IBM Security Verify Access
Version 10.0.3
December 2021

Error Message Reference

Contents

Chapter 1. Message overview

Messages indicate events that occur during the operation of the system. Depending on their purpose, messages might be displayed on the screen. By default, all informational, warning, and error messages are written to the message logs. The logs can be reviewed later to determine what events occurred, to see what corrective actions were taken, and to audit all the actions performed. For more information about message logs, see the Troubleshooting topics in the IBM® Knowledge Center.

Message types

IBM Security Verify Access uses messages of specific types.

The following types of messages are used:

Informational messages
Indicate conditions that are worthy of noting but do not require you to take any precautions or perform an action.

Warning messages
Indicate that a condition is detected that you must be aware of, but does not necessarily require that you take any action.

Error messages
Indicates that a condition occurred that requires you to take action.

Message format

Messages that are logged by IBM Security Verify Access adhere to message standards. Each message consists of a message identifier (ID) and accompanying message text.

Message ID format

A message ID consists of 10 alphanumeric characters that uniquely identify the message.

A message ID is composed of:

- Three-character product identifier
- Two-character or three-character component or subsystem identifier
- Three-digit or four-digit serial or message number
- One-character type code that indicates the severity of the message

The figure that follows shows a graphical representation of a possible message ID and identifies its different parts. (Some messages might use 2 characters for the component ID and 4 digits for the serial number.)

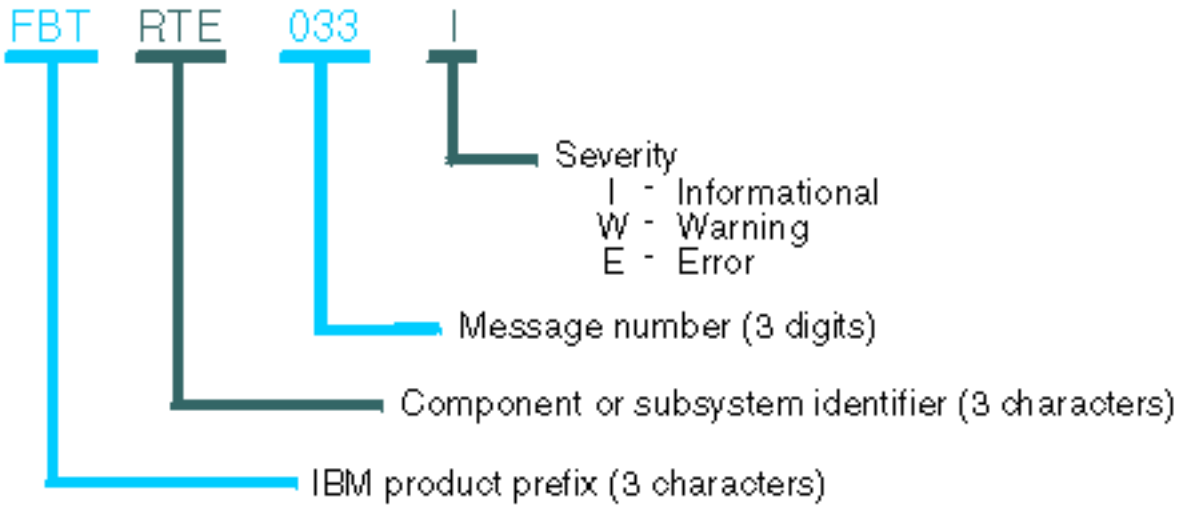

Figure 1. Message ID format

Component identifiers

The component identifier indicates which component or subsystem produced the message.

ADM
Administration commands

AUD
Audit

AUT
Authentication service

CC
Common Auditing and Reporting Service disk cache

CE
Common Auditing and Reporting Service emitter

CFG
Configuration properties

CO
Common Audit Service Configuration Console

CON
Security Verify Access console

CTG
Authorization service

CTJ
Single Sign On for Bluemix service

DIS
Directory Integrator component used by Single Sign On

DPW
Secure reverse proxy

FBT
Protocol service

FDB
Database

FMS
Management service

ELA
End-user license agreement

HRD
HTTP redirect

IAS
Single sign-on administration

IDA
Single sign-on administration

IDS
Identity service

IN
Common Auditing and Reporting Service installation

ISJ
Alias service JDBC component

ISL
Alias service LDAP component

KES
Key encryption and signature service

KJK
Key encryption and signature service Java KeyStore

KQA
Knowledge questions

LOG
Logging

MB
Common Audit Service Configuration MBean

MET
Metadata handling

MGT
Management

MOD
Module

OAU
OAuth 2.0

OTP
One-time password

PWD
Password handling

RBA
Context-based access

RPT
Report messages

RTE
Runtime environment component configuration

SDK
Software development kit

SO
Single Sign On service

SOC
SOAP client

SPS
Single sign-on protocol service

STM
Secure token service

STS
Secure token service modules

STZ
RACF® PassTicket tokens

SU
Common Audit Staging Utility

SYS
System alert messages

TAC
Security Verify Access configuration

TRC
Trust client

UPD
Username password

UTI
Utility

WS
Common Auditing and Reporting Service Mobile service

WSS
Mobile services security management

XS
Common Audit Service XML data store

XU
Common Audit Service XML store utilities

Severity

Associated with each message is a severity level that indicates whether corrective action must be taken.

Table 1. Severity level

Severity	Description

I (Informational)	Provides information or feedback about normal events that occur. In general, no action needs to be performed in response to an informational message.
	`FBTRTE033I The domain default was successfully created.`
	`FBTSTM066I The Trust Service has been disabled.`

W (Warning)	Indicates that a potentially undesirable condition has occurred, but processing can continue. Intervention or corrective action might be necessary in response to a warning message.
	`FBTLOG002W An integer was expected.`
	`FBTTRC004W The returned RequestSecurityTokenResponse did not have a wsu:Id`

Table 1. Severity level (continued)	
Severity	**Description**

E (Error)	Indicates that a problem has occurred that requires intervention or correction before processing can continue. An error message might be accompanied by one or more warning or informational messages that provide additional details about the problem.
	
	`FBTCON013E The federation with ID insert could not be retrieved from the single sign-on protocol service. Explanation: This error can occur if the console is unable to communicate with the single sign-on protocol service.`
	
	`FBTSML260E The binding value value for attribute attr is not valid for profile profile.`

Message text

The text of the message, in the system locale, also is recorded in the log file. If the message text is not available in the language that you want, the English language text is used.

Events that are generated by the events framework

Use the Event Log management page in the appliance to view system events. In the local management interface, select **Monitor** > **Logs** > **Event Log**.

All of the following events are generated by the events framework. These events are displayed in the event log or broadcasted to an external collector, such as SNMP, if configured.

Informational messages

These events are generated to indicate conditions that are worthy of noting but do not require you to do anything.

Event ID	Description
See WGASY0000I.	This message is an identifier for generic information messages. It includes an informational message and the name of the server that generated the message.

CPU usage

These events are generated when the CPU usage of the system reaches certain thresholds.

Event ID	Description
See WGAWA0643W.	This warning message is generated when the CPU usage exceeds the warning threshold.
See WGAWA0043W.	This error message is generated when the CPU usage exceeds the error threshold.
See WGAWA0650I.	This informational message is generated when the CPU utilization falls below the configured threshold.

Disk usage

These events are generated when the disk usage of the system reaches certain thresholds.

Event ID	Description
See WGAWA0644W.	This warning message is generated when the disk usage exceeds the warning threshold.
See WGAWA0044W.	This error message is generated when the disk usage exceeds the error threshold.
See WGAWA0649I.	This informational message is generated when the disk utilization falls below the configured threshold.

Certificate expiry

These events are generated when there are expired or soon to expire certificates in the SSL certificate database.

Event ID	Description
See WGAWA0645W.	This warning message is generated when a certificate will expire within the warning threshold.
See WGAWA0045W.	This error message is generated when a certificate will expire within the error threshold.
See WGAWA0046W.	This error message is generated when a certificate has expired. The message includes the certificate label of the expired certificate.

Stopped reverse proxy instances

These events are generated when there are configured reverse proxy instances in the appliance that are currently not running or has recovered.

Event ID	Description
See WGAWA0047W.	This error message is generated when a reverse proxy instance is configured but not running. The message includes the name of the reverse proxy instance.
See WGAWA0648I.	This informational message is generated when the reverse proxy has recovered.

Runtime database size

These events are generated when the disk usage of the runtime database reaches certain thresholds.

Event ID	Description
See WGAWA0055W.	This error message is generated when the disk usage reaches the error threshold.
See WGAWA0646W.	This warning message is generated when the disk usage reaches the warning threshold.
See WGAWA0649I.	This informational message is generated when the disk usage for the runtime database falls below the configured threshold.

Pending changes

These events are generated when there are changes in the local management interface or web services that are not yet deployed or have been deployed.

Event ID	Description
See WGAWA0642W.	The error message is generated when pending changes did not complete deploying within the command timeout.
See WGAWA0640W.	This informational message is generated when changes that are made by using the LMI/Web services are not active because they have not yet been deployed.
See WGAWA0653I.	This informational message is generated when pending changes have been deployed.

Time synchronization

These events are generated when the NTP server is not configured or configured for the appliance.

Event ID	Description
See WGAWA0647W.	This warning message is generated when the clock on the appliance is not currently synchronized.
See WGAWA0652I.	This informational message is generated when the appliance has been updated with NTP configuration information.

Related concepts

“Appliance messages” on page 9

Chapter 2. Appliance messages

These messages are provided by the appliance.

Authentication messages

These messages are provided by the authentication component.

GLGAU0001I

User *user_name* logged on to the appliance *interface_name* from *remote_host* (*protocol_name* connection).

Explanation
This message is generated when user logs on to the appliance.

Administrator response
This is an audit event. No action is required.

GLGAU0002I

User *user_name* logged out of the appliance *interface_name* from *remote_host* (*protocol_name* connection).

Explanation
This message is generated when user logs out of the appliance.

Administrator response
This is an audit event. No action is required.

GLGAU0003W

User *user_name* failed to login to the appliance *interface_name* from *remote_host* (*protocol_name* connection).

Explanation
This message is generated when authentication fails for a user.

Administrator response
This is an audit event. No action is required.

GLGAU0004I

User *user_name* logged on to the appliance CLI.

Explanation
This message is generated when user logs on to the appliance via serial console.

Administrator response
This is an audit event. No action is required.

GLGAU0005I

User *user_name* logged out of the appliance CLI.

Explanation
This message is generated when user logs out of the appliance serial console.

Administrator response
This is an audit event. No action is required.

GLGAU0006W

User *user_name* failed to login to the appliance CLI.

Explanation
This message is generated when user tries to log on to the appliance serial console with invalid credentials.

Administrator response
This is an audit event. No action is required.

GLGAU0007W

The user *user_name* was locked out because the maximum amount of login attempts exceeded. The number of failed attempts is *tally_name*.

Explanation
This message is generated when a user logs on to the appliance with invalid credentials and exceeds the account lockout threshold.

Administrator response
This is an audit event. No action is required.

GLGAU0008I

User *user_name* has more than one active session logged on to the appliance.

Explanation
This message is generated when the user has more than one active session logged on to the appliance.

Administrator response
This is an audit event. No action is required.

GLGAU0008W

User *user_name* password will expire in *days* days.

Explanation
This message is generated when the user password is going to expire.

Administrator response
Please login to the system to change the user password.

GLGAU0009W

User *user_name* password expired.

Explanation
This message is generated when the user password expired.

Administrator response
Please login to the system to change the user password.

GLGAU9001I

User *user_name* logged on to the appliance *interface_name* from *remote_host* (*protocol_name* connection).

Explanation
This message is generated when user logs on to the appliance.

Administrator response
This is an audit event. No action is required.

GLGAU9002I

User *user_name* logged out of the appliance *interface_name* from *remote_host* (*protocol_name* connection).

Explanation
This message is generated when user logs out of the appliance.

Administrator response
This is an audit event. No action is required.

GLGAU9003W

User *user_name* failed to login to the appliance *interface_name* from *remote_host* (*protocol_name* connection).

Explanation
This message is generated when authentication fails for a user.

Administrator response
This is an audit event. No action is required.

GLGAU9004I

User *user_name* logged on to the appliance CLI.

Explanation
This message is generated when user logs on to the appliance via serial console.

Administrator response
This is an audit event. No action is required.

GLGAU9005I

User *user_name* logged out of the appliance CLI.

Explanation
This message is generated when user logs out of the appliance serial console.

Administrator response
This is an audit event. No action is required.

GLGAU9006W

User *user_name* failed to login to the appliance CLI.

Explanation
This message is generated when user tries to log on to the appliance serial console with invalid credentials.

Administrator response
This is an audit event. No action is required.

GLGAU9007W

The user *user_name* was locked out because the maximum amount of login attempts exceeded. The number of failed attempts is *tally_name*.

Explanation
This message is generated when a user logs on to the appliance with invalid credentials and exceeds the account lockout threshold.

Administrator response
This is an audit event. No action is required.

GLGAU9008I

User *user_name* has more than one active session logged on to the appliance.

Explanation
This message is generated when the user has more than one active session logged on to the appliance.

Administrator response
This is an audit event. No action is required.

GLGAU9008W

User *user_name* password will expire in *days* day(s).

Explanation
This message is generated when the user password is going to expire.

Administrator response
Please login to the system to change the user password.

GLGAU9009W

User *user_name* password expired.

Explanation
This message is generated when the user password expired.

Administrator response
Please login to the system to change the user password.

GLGAU9010W

User *user_name* has reset the admin account.

Explanation
This message is generated when the user has reset the admin account.

Administrator response
This is an audit event. No action is required.

GLGAU9011W

User *user_name* who is logging on to the appliance *interface_name* from *remote_host* has forced the preceding user with the same account to log off.

Explanation
This message is generated when the single-session limit is enabled and the new session forces another session to be closed.

Administrator response
This is an audit event. No action is required.

GLGAU9012I

User *user_name* who is trying to log on to the appliance *interface_name* from *remote_host* has triggered the single-session limit.

Explanation
The single-session limit has been enabled. The user logged in with the account currently being used, and a dialog to cancel login or to log off current user was initiated.

Administrator response
This is an audit event. No action is required.

GLGAU9013W

User *user_name* who is logging on to the appliance CLI has forced the preceding user with the same account to log off.

Explanation
This message is generated when the single-session limit is enabled and the new session via serial console forces another session to be closed.

Administrator response
This is an audit event. No action is required.

GLGAU9014I

User *user_name* who is trying to log on to the appliance CLI has triggered the single-session limit.

Explanation
The single-session limit has been enabled. The user logged in via serial console with the account currently being used, and a dialog to cancel login or to log off current user was initiated.

Administrator response
This is an audit event. No action is required.

Backup restore messages

These messages are provided by the backup restore component.

GLGBK1002E

An attempt by the *interface_name* operator, *user_name*, to back up partition, *partition_number* has failed.

Explanation
This message is generated when an attempt to back up a partition has failed. The message includes the partition number that was to be duplicated.

Administrator response
Review subsequent log messages to determine why the operation failed.

GLGBK1003I

The *interface_name* operator *user_name* has swapped the active partition to partition, *partition_number*.

Explanation
This message is generated as part of a configuration change. It informs the administrator when the active disk partition has been swapped.

Administrator response
This is an informational message. No action is required.

GLGBK1004E

An attempt by the *interface_name* operator, *user_name*, to swap the active partition to partition, *partition_number* has failed.

Explanation
This message is generated when an attempt to swap the active partition has failed. The message includes the partition number that was to be swapped.

Administrator response
Review subsequent log messages to determine why the operation failed.

GLGBK1001I

The *interface_name* operator *user_name* has performed a backup operation on partition, *partition_number*.

Explanation
This message is generated as part of a configuration change. It informs the administrator when a backup operation has been performed on a disk partition.

Administrator response
This is an informational message. No action is required.

GLGBK9001I

The *interface_name* operator *user_name* has performed a backup operation on partition, *partition_number*.

Explanation
This message is generated as part of a configuration change. It informs the administrator when a backup operation has been performed on a disk partition.

Administrator response
This is an informational message. No action is required.

GLGBK9003I

The *interface_name* operator *user_name* has swapped the active partition to partition, *partition_number*.

Explanation
This message is generated as part of a configuration change. It informs the administrator when the active disk partition has been swapped.

Administrator response
This is an informational message. No action is required.

Date and time messages

These messages are provided by the date and time component.

GLGDT1001I

The time changed from *old_time* to *new_time* by *user_name* from *origin*.

Explanation
The time was changed by a user from the LMI, CLI, or by NTP server.

Administrator response
This is an informational message. No action is required.

GLGDT1002I

The time changed from *old_hour* to *new_hour* by *user_name* from *origin*.

Explanation
The time (hour, minute, second) was changed by a user from the LMI, CLI, or by NTP server.

Administrator response
This is an informational message. No action is required.

GLGDT1003I

The date changed from *old_date* to *new_date* by *user_name* from *origin*.

Explanation
The date was changed by a user from the LMI, CLI, or by NTP server.

Administrator response
This is an informational message. No action is required.

GLGDT1004W

NTP was unable to set the system clock. The time correction value (*skew*) exceeds the sanity limit (*sanity_limit*).

Explanation
The NTP time correction value is outside the allowed range.

Administrator response
The system clock must be configured manually.

GLGDT1005E

An attempt to set the system time by user *user_name* from *origin* has failed.

Explanation
The system has rejected the attempt to change the system time.

Administrator response
Contact Software Support.

GLGDT9001I

The time changed from *old_time* to *new_time* by *user_name* from *origin*.

Explanation
The time was changed by a user from the LMI, CLI, or by NTP server.

Administrator response
This is an informational message. No action is required.

GLGDT9002I

The time changed from *old_hour* to *new_hour* by *user_name* from *origin*.

Explanation
The time (hour, minute, second) was changed by a user from the LMI, CLI, or by NTP server.

Administrator response
This is an informational message. No action is required.

GLGDT9003I

The date changed from *old_date* to *new_date* by *user_name* from *origin*.

Explanation
The date was changed by a user from the LMI, CLI, or by NTP server.

Administrator response
This is an informational message. No action is required.

GLGDT9006I

NTP server configuration was changed by *user_name*.

Explanation
NTP server configuration was changed by user from LMI or CLI.

Administrator response
This is an informational message. No action is required.

Event messages

These messages are provided by the event component.

GLGSY0000W

The *service* was terminated and restarted unexpectedly.

Explanation
System service was terminated unexpectedly and subsequently restarted.

Administrator response
Contact Software Support.

GLGSY0001E

The configuration component has failed to apply a configuration change. A reboot is required.

Explanation
Configuration failed unexpectedly whilst applying changes.

GLGSY0002E

The configuration component has failed to apply the appliance configuration during appliance startup. A reboot is required.

Explanation
Configuration failed unexpectedly during startup.

GLGSY0003E

The configuration component has failed to successfully validate policy during appliance startup. A reboot is required.

Explanation

Administrator response
No action required.

GLGSY0004E

An unexpected failure has occurred in the configuration component.

Explanation
Configuration failed unexpectedly.

GLGSY0005E

The attempted policy migration has failed.

Explanation
The previous configuration did not migrate to the new partition successfully.

GLGSY0006E

An attempt to locate and copy specified files to new partition during policy migration has failed.

Explanation
The previous configuration did not migrate to the new partition successfully.

GLGSY0007E

The directory, *directory_name*, is not valid. The creation of a support information file has failed.

Explanation
An internal error occurred whilst generating the support information file.

GLGSY0008W

Information needed for a support information file has not been found.

Explanation
An internal error occurred whilst generating the support information file.

GLGSY0009W

An attempt to add a comment to a support information file has failed

Explanation

An internal error occurred whilst adding a comment to a support information file.

GLGSY0010E

An attempt to apply a configuration change using a settings snapshot has failed. The previous policy has been restored.

Explanation

The configuration contained within the snapshot could not be successfully applied.

GLGSY0011E

Restoring the previous policy after a failed attempt to apply a configuration from a settings snapshot file has resulted in at least one failure.

Explanation

The policy contained within the snapshot could not be successfully applied.

GLGSY0012E

The policy was not validated by the configuration component. The configuration was rolled back and the Local Management Interface was restarted.

Explanation

The previous configuration could not be validated successfully.

GLGSY0013E

The configuration was not reset to the factory defaults.

Explanation

The configuration could not be reset to factory defaults.

GLGSY0014I

The configuration was reset to the factory defaults.

Explanation

The configuration has been reset to factory defaults.

GLGSY0015I

The startup configuration is complete.

Explanation

The previous configuration was validated and applied successfully.

GLGSY0016E

The appliance was automatically restarted to recover from a startup configuration attempt that failed.

Explanation
After encountering an error, the appliance has restarted to retry booting.

Administrator response
This is an informational message. No action is required.

GLGSY0017E

Restart the appliance manually to recover from a startup configuration attempt that failed.

Explanation
An error occurred during startup and the appliance must be rebooted manually.

GLGSY0018E

An unrecoverable error has occurred while attempting to configure network interfaces.

Explanation
The configuration of the appliance network interfaces has failed.

Administrator response
Contact Software Support.

GLGSY0019W

The *component_name* has stopped unexpectedly.

Explanation
A required component has stopped without warning.

Administrator response
Contact Software Support.

GLGSY0020I

User *user_name* logged on to the appliance.

Explanation
This message is generated when user logs on to the appliance. (This event is deprecated. Use GLGAU messages for authentication events.)

Administrator response
This is an audit event. No action is required.

GLGSY0021W

Authentication failed for user *user_name*.

Explanation
This message is generated when user tries to log on to the appliance with invalid credentials. (This event is deprecated. Use GLGAU messages for authentication events.)

Administrator response
This is an audit event. No action is required.

GLGSY0022E

FIPS error detected. Checksum validation failed for file *file_name*.

Explanation
This message is generated if a checksummed file is modified in an unauthorized manner when running in FIPS mode.

Administrator response
Contact Software Support.

GLGSY0023E

FIPS error detected. File *file_name* has been deleted.

Explanation
This message is generated if a checksummed file is removed in an unauthorized manner when running in FIPS mode.

Administrator response
Contact Software Support.

GLGSY0024E

FIPS error detected. Component *component_name* has failed to enter FIPS mode.

Explanation
This message is generated if a component fails to enter FIPS mode.

Administrator response
Contact Software Support.

GLGSY0025I

Component *component_name* has successfully entered FIPS mode.

Explanation
This message is generated when a component successfully enables FIPS mode.

Administrator response
This is an audit event. No action is required.

GLGSY0026I

Component sshd has successfully entered FIPS mode.

Explanation
This message is generated when sshd successfully enables FIPS mode at startup.

Administrator response
This is an audit event. No action is required.

GLGSY0027W

Invalid SNMP alert configuration: *algorithm_name* is not allowed in FIPS mode.

Explanation
This message is generated in FIPS mode when an SNMPv3 alert is configured to use a cryptographic algorithm that's not FIPS 140-2 approved.

Administrator response
Update the SNMP alert configuration to use FIPS 140-2 approved cryptographic algorithms.

GLGSY0028E

FIPS error detected. Component sshd has failed to enter FIPS mode.

Explanation
This message is generated if sshd fails to enter FIPS mode.

Administrator response
Contact Software Support.

GLGSY0029I

Appliance has entered FIPS mode.

Explanation
This message is generated when appliance boots into FIPS mode.

Administrator response
This is an audit event. No action is required.

GLGSY0030I

The default CA certificate was automatically renewed. The new expiration date is *expire_date*.

Explanation
This message is generated when the appliance automatically renews the default Certificate Authority Certificate.

Administrator response
This is an audit event. No action is required.

GLGSY0031W

The Certificate Authority with subject name, *subject_name*, expires in less than *num_days* days.

Explanation
A Certificate Authority will expire soon.

Administrator response
Update the Certificate Authority certificate.

GLGSY0032E

The attempt to update the route, *route_detail*, has failed.

Explanation
The route specified is invalid.

Administrator response
Verify that the static route specified in the policy are correct for the current network configuration of the appliance.

GLGSY0033W

The certificate with subject name, *subject_name*, expires in less than *num_days* days.

Explanation
A certificate will expire soon.

Administrator response
Update the certificate.

GLGSY0034I

The LMI has been configured to use the default self-signed certificate.

Explanation
The certificate used to secure connections to the LMI has been changed to use the default self-signed certificate created when the appliance was deployed.

Administrator response
This is an informational message. No action is required.

GLGSY0034W

A problem was detected in the security content installed on this appliance and certain signatures may not operate properly.

Explanation
The system will continue to operate with the currently installed security content, however, certain signatures may not operate properly.

Administrator response
Contact Software Support.

GLGSY0035I

The LMI has been configured to use a custom user provided certificate.

Explanation
The certificate used to secure connections to the appliance LMI has been changed to use a certificate provided by the appliance administrator.

Administrator response
This is an informational message. No action is required.

GLGSY0036W

The certificate with subject name, *subject_name*, has expired.

Explanation
A certificate has expired.

Administrator response
Update the certificate.

GLGSY0037W

The Certificate Authority with subject name, *subject_name*, has expired.

Explanation
A Certificate Authority certificate has expired.

Administrator response
Update the Certificate Authority certificate.

GLGSY0038W

The hardware watchdog timer did not initialize properly.

Explanation
The hardware watchdog timer, which automatically reboots the appliance when the operating system fails, did not initialize properly.

Administrator response
Contact Software Support.

GLGSY0039W

The system memory use of *value* percent has exceeded the specified limit of *limit* percent.

Explanation
The system memory used has exceeded the specified limit.

Administrator response
Contact Software Support.

GLGSY0040W

The disk consumption of *value* percent of the root partition has exceeded the specified limit of *limit* percent.

Explanation
The disk consumption of the root partition has exceeded the specified limit.

Administrator response
Temporary files such as packet captures or support files should be deleted to free up some space.

GLGSY0041E

Network interface module in bank *bank* is below the minimum supported firmware version for this appliance. This network interface module will be disabled. Current firmware version is *currentVersion*. Minimum required firmware version is *minimumVersion*.

Explanation
The specified network interface module is not supported on this system. It must be replaced with another module with the minimum required firmware version.

Administrator response
Power off the appliance and replace the network interface module.

GLGSY0042I

Call Home service has started.

Explanation
Call Home service will now submit all unprocessed failure cases to support systems. This may take some time to finish.

Administrator response
This is an informational message. No action is required.

GLGSY0043I

Call Home service has successfully submitted: *problem_desc* PMR *pmr_id*.

Administrator response
This is an informational message. No action is required.

GLGSY0044I

IPS events log database has been cleared.

Explanation
IPS events log database has been cleared.

Administrator response
This is an informational message. No action is required.

GLGSY0044W

Call Home service was unable to submit a service request for: *problem_desc* (on *problem_timestamp*)

Explanation
Call Home service has detected a system failure, but was unable to submit a service request.

Administrator response
Contact software support.

GLGSY0045I

Network access events log database has been cleared.

Explanation
Network access events log database has been cleared.

Administrator response
This is an informational message. No action is required.

GLGSY0046W

Network interface module in bank *bank*, with serial number *serial*, is not compatible with this appliance. This network interface module will be disabled.

Explanation
The specified network interface module is not compatible with this appliance and cannot be used.

Administrator response
The specific network interface module cannot be used on this appliance. Please power off the appliance and remove it during the next maintenance period.

GLGSY0047I

All hardware bypass controllers have switched to connected mode.

Explanation
All network segments with built-in hardware bypass controllers have switched to connected mode. The appliance can now inspect traffic on these segments.

Administrator response
This is an informational message. No action required here.

GLGSY0048I

All hardware bypass controllers have switched to fail mode.

Explanation
All network segments with built-in hardware bypass controllers have switched to fail mode. The appliance can no longer inspect traffic on these segments.

Administrator response
This is an informational message. No action required here.

GLGSY0049E

System reboot due to a fatal error in root file system.

Explanation
File system is corrupted and may change to read-only mode due to disk failure or bad blocks.

Administrator response
If the persists, restart the appliance or contact technical support.

GLGSY0050I

Malware analysis status database has been cleared.

Explanation
Malware analysis status database has been cleared.

Administrator response
This is an informational message. No action is required.

GLGSY0100W

An attempt was made to log on using an unknown user, '*user_name*', from '*remote_host*'.

Explanation
This message is generated when an unknown user tries to log on to the appliance.

Administrator response
This is an audit event. No action is required.

GLGSY0101W

An incorrect password was provided for the user, '*user_name*', from '*remote_host*'.

Explanation
This message is generated when the wrong password is provided for a user trying to log on to the appliance.

Administrator response
This is an audit event. No action is required.

GLGSY0102I

The user, '*user_name*' from '*remote_host*', was logged out of the system.

Explanation
This message is generated when a user logs off the appliance.

Administrator response
This is an audit event. No action is required.

GLGSY0103I

The user, '*user_name*' from '*remote_host*', was successfully authenticated.

Explanation
This message is generated when a user logs on to the appliance.

Administrator response
This is an audit event. No action is required.

GLGSY0104W

The account for user, '*user_name*' from '*remote_host*', has been locked.

Explanation
This message is generated when a user tries to log on to the appliance when their account is locked.

Administrator response
This is an audit event. No action is required.

GLGSY0105W

The login was rejected for the unprivileged user, '*user_name*' from '*remote_host*'.

Explanation
This message is generated when a user tries to log on to the appliance that does not have the required privileges.

Administrator response
This is an audit event. No action is required.

GLGSY0106W

The account has not been enabled for the user '*user_name*' from '*remote_host*'.

Explanation
This message is generated when a user tries to log on to the appliance when their account is not enabled.

Administrator response
This is an audit event. No action is required.

GLGSY0107W

The account has expired for the user '*user_name*' from '*remote_host*'.

Explanation
This message is generated when a user tries to log on to the appliance when their account is expired.

Administrator response
This is an audit event. No action is required.

GLGSY0108I

The user '*user_name*' from '*remote_host*' reset their own password.

Explanation
This message is generated when a user resets their password.

Administrator response
This is an audit event. No action is required.

GLGSY9025I

Component *component_name* has successfully entered FIPS mode.

Explanation
This message is generated when a component successfully enables FIPS mode.

Administrator response
This is an audit event. No action is required.

GLGSY9026I

Component sshd has successfully entered FIPS mode.

Explanation
This message is generated when sshd successfully enables FIPS mode at startup.

Administrator response
This is an audit event. No action is required.

GLGSY9029I

Appliance has entered FIPS mode.

Explanation
This message is generated when appliance boots into FIPS mode.

Administrator response
This is an audit event. No action is required.

GLGSY9030I

The default CA certificate was automatically renewed. The new expiration date is *expire_date*.

Explanation
This message is generated when the appliance automatically renews the default Certificate Authority Certificate.

Administrator response
This is an audit event. No action is required.

GLGSY9034I

The LMI has been configured to use the default self-signed certificate.

Explanation

The certificate used to secure connections to the LMI has been changed to use the default self-signed certificate created when the appliance was deployed.

Administrator response

This is an informational message. No action is required.

GLGSY9035I

The LMI has been configured to use a custom user provided certificate.

Explanation

The certificate used to secure connections to the appliance LMI has been changed to use a certificate provided by the appliance administrator.

Administrator response

This is an informational message. No action is required.

GLGSY9042I

The appliance has been configured to use the default self-signed certificate for *central_management_entity* bi-directional authentication.

Explanation

The certificate used to authenticate as a client to a central management IT entity has been changed to use the default self-signed certificate created when the appliance was deployed.

Administrator response

This is an informational message. No action is required.

GLGSY9043I

The appliance has been configured to use a custom user provided certificate for *central_management_entity* bi-directional authentication.

Explanation

The certificate used to authenticate as a client to a central management IT entity has been changed to use a certificate provided by the appliance administrator.

Administrator response

This is an informational message. No action is required.

Event framework messages

These messages are provided by the event framework component.

GLGEV1001I

The system has resumed processing events after encountering an internal error. Events may have been lost.

Explanation
This message is generated when the internal error results in the event message queue to be reset.

Administrator response
This is an informational message. No action is required.

Fixpack messages

These messages are provided by the fixpack component.

GLGFP1001I

The *interface_name* operator, *user_name*, has installed a fix pack file, *file_name*.

Explanation
This message is generated when a user installs a fix pack file. The message includes the name of the file and who installed it.

Administrator response
This is an informational message. No action is required.

GLGFP1002E

An attempt by the *interface_name* operator, *user_name*, to install the fix pack file, *file_name*, has failed.

Explanation
This message is generated when a fix pack file fails to install successfully. The message lists the uploaded file name and the name of the user who requested the installation.

Administrator response
Review subsequent log messages to determine why the operation failed.

GLGFP1003E

The fix pack file, *file_name*, was not found.

Explanation
This message is generated when a fix pack file cannot be found.

Administrator response
Contact Software Support.

GLGFP1004E

The fix pack file, *file_name*, does not have a valid digital signature.

Explanation
This message is generated when a fix pack file does not contain the correct digital signature.

Administrator response
Contact Software Support.

GLGFP1005E

The fix pack file, *file_name*, is not a valid fix pack file.

Explanation
This message is generated when a fix pack file is not in the correct format. The file might be corrupt.

Administrator response
Contact Software Support.

GLGFP1006I

The *interface_name* operator, *user_name*, has uninstalled the fix pack file *file_name*.

Explanation
This message is generated when a user uninstalls a fix pack file.

Administrator response
This is an informational message. No action is required.

GLGFP1007E

An attempt by the *interface_name* operator, *user_name*, to uninstall the fix pack file, *file_name*, has failed.

Explanation
This message is generated when a fix pack file fails to uninstall.

Administrator response
Review subsequent log messages to determine why the operation failed.

GLGFP1008I

The system is not allowed to uninstall the fix pack file *file_name*.

Explanation
The system attempted to uninstall a fix pack file that it is not allowed to be uninstalled.

Administrator response
The administrator may restore to a previous firmware version to remove a fix pack that is not allowed to be uninstalled.

GLGFP1009E

The fix pack file, *file_name*, is not supported by the currently installed firmware.

Explanation
This message is generated when a fix pack file is not supported by the currently installed firmware.

Administrator response
Contact Software Support.

GLGFP9001I

The *interface_name* operator, *user_name*, has installed a fix pack file, *file_name*.

Explanation
This message is generated when a user installs a fix pack file. The message includes the name of the file and which user installed it.

Administrator response
This is an informational message. No action is required.

GLGFP9006I

The *interface_name* operator, *user_name*, has uninstalled the fix pack file *file_name*.

Explanation
This message is generated when a user uninstalls a fix pack file.

Administrator response
This is an informational message. No action is required.

Hardware messages

These messages are provided by the hardware component.

GLGHW0001I

USB device, *manufacturer product*, was added as device number *device_number*. The USB device transfer rate is *speed* Mbit/s.

Explanation
This message is generated when a USB device is connected to the appliance.

Administrator response
This is an audit event. No action is required.

GLGHW0002I

USB device number *device_number* was disconnected.

Explanation
This message is generated when a USB device is removed from the appliance.

Administrator response
This is an audit event. No action is required.

GLGHW0003I

NIM with serial number, *serial_number*, was added to bank *bank_number*.

Explanation
This message is generated when a network interface module (NIM) is added to the appliance.

Administrator response
This is an audit event. No action is required.

GLGHW0004I

NIM with serial number, *serial_number*, was removed from bank *bank_number*.

Explanation
This message is generated when a network interface module (NIM) is removed from the appliance.

Administrator response
This is an audit event. No action is required.

GLGHW0005I

PCI device number *pci_id_number* was added to PCI bus *bus_number*.

Explanation
This message is generated when a PCI device is added to the appliance.

Administrator response
This is an audit event. No action is required.

GLGHW0006I

PCI device number *pci_id_number* was removed from PCI bus *bus_number*.

Explanation
This message is generated when a PCI device is removed from the appliance.

Administrator response
This is an audit event. No action is required.

GLGHW0101E

Hardware component *module* has failed to operate properly.

Explanation
This message is generated when a platform hardware sensor has signaled a failure.

Administrator response
Contact Support.

GLGHW0102E

NIM with serial number, *serial_number*, in bank *bank_number*, has failed to operate properly.

Explanation
This message is generated when failures have been detected on an NIM

Administrator response
Contact Software Support.

GLGHW0103W

LCD has failed to operate properly.

Explanation
This message is generated when the LCD fails to operate.

Administrator response
Restart and run Hardware Diagnostics to check the LCD.

GLGHW0104W

Hardware component power supply unit #*id* has failed to operate properly due to power loss.

Explanation
This message is generated when a power supply sensor has signaled a power loss.

Administrator response
Reattach power core and check power source

GLGHW0105I

Hardware component power supply unit #*id* has restored from power loss.

Explanation
This message is generated when a power supply sensor has reset power loss signal.

Administrator response
This is an informational message. No action is required.

GLGHW0106I

Hardware component power supply unit #*id* has been removed.

Explanation
This message is generated when a power supply sensor has signaled a power module absence.

Administrator response
This is an informational message. No action is required.

GLGHW0107I

Hardware component power supply unit #*id* has been inserted.

Explanation
This message is generated when a power supply sensor has signaled a power module presence.

Administrator response
This is an informational message. No action is required.

GLGHW0108E

Hardware component *module* has failed to operate properly because *failure*.

Explanation
This message is generated when a platform hardware inventory checking failure occurred.

Administrator response
Contact Support.

GLGHW0109W

Hardware component *module* has failed to operate properly because *failure*.

Explanation
This message is generated when a platform hardware inventory checking failure occurred.

Administrator response
Contact Support.

GLGHW1101E

Hardware component fan #*id* has failed to operate properly.

Explanation
This message is generated when a platform hardware sensor has signaled a failure.

Administrator response
Contact Support.

GLGHW1102E

Hardware component power supply unit #*id* has failed to operate properly.

Explanation
This message is generated when a platform hardware sensor has signaled a failure.

Administrator response
Contact Support.

GLGHW9001I

USB device, *manufacturer product*, was added as device number *device_number*. The USB device transfer rate is *speed* Mbit/s.

Explanation
This message is generated when a USB device is connected to the appliance.

Administrator response
This is an audit event. No action is required.

GLGHW9002I

USB device number *device_number* was disconnected.

Explanation
This message is generated when a USB device is removed from the appliance.

Administrator response
This is an audit event. No action is required.

GLGHW9003I

NIM with serial number, *serial_number*, was added to bank *bank_number*.

Explanation
This message is generated when a network interface module (NIM) is added to the appliance.

Administrator response
This is an audit event. No action is required.

GLGHW9004I

NIM with serial number, *serial_number*, was removed from bank *bank_number*.

Explanation
This message is generated when a network interface module (NIM) is removed from the appliance.

Administrator response
This is an audit event. No action is required.

GLGHW9005I

PCI device number *pci_id_number* was added to PCI bus *bus_number*.

Explanation
This message is generated when a PCI device is added to the appliance.

Administrator response
This is an audit event. No action is required.

GLGHW9006I

PCI device number *pci_id_number* was removed from PCI bus *bus_number*.

Explanation
This message is generated when a PCI device is removed from the appliance.

Administrator response
This is an audit event. No action is required.

GLGHW9101E

Hardware component processor has failed to operate properly because socket #*id* cores doesn't match .

Explanation
This message is generated when a platform hardware inventory checking failure occurred.

Administrator response
Contact Support.

GLGHW9102E

Hardware component memory has failed to operate properly because total size doesn't match.

Explanation
This message is generated when a platform hardware inventory checking failure occurred.

Administrator response
Contact Support.

GLGHW9103E

Hardware component storage has failed to operate properly because slot #*id*: SSD life left is low.

Explanation
This message is generated when a platform hardware inventory checking failure occurred.

Administrator response
Contact Support.

GLGHW9104E

Hardware component storage has failed to operate properly because slot #*id*: S.M.A.R.T. overall assessment failed.

Explanation
This message is generated when a platform hardware inventory checking failure occurred.

Administrator response
Contact Support.

GLGHW9105W

Hardware component processor has failed to operate properly because model name doesn't match.

Explanation
This message is generated when a platform hardware inventory checking failure occurred.

Administrator response
Contact Support.

GLGHW9106W

Hardware component processor has failed to operate properly because clock rate doesn't match.

Explanation
This message is generated when a platform hardware inventory checking failure occurred.

Administrator response
Contact Support.

GLGHW9107W

Hardware component processor has failed to operate properly because caches size doesn't match.

Explanation
This message is generated when a platform hardware inventory checking failure occurred.

Administrator response
Contact Support.

Licensing messages

These messages are provided by the licensing component.

GLGLI0001W

The *type* license expires in less than *num_days* days.

Explanation
A license will expire soon. The system might not receive updates after the license expires.

Administrator response
Update the system license to continue receiving updates after the expiry date.

GLGLI0002E

The *type* license has expired.

Explanation
A license has expired. The system might not receive updates because of this.

Administrator response
Update the system license to continue receiving updates.

GLGLI0003E

The flexible performance level (*performance_level*) has been set to exceed the licensed performance level (*license_level*).

Explanation
A user has set the flexible performance level to a level higher than what the appliance is licensed for.

Administrator response
This audit information requires no operator response.

GLGLI0004E

SSL rules have been configured without a valid SSL Inspection feature license.

Explanation

A user has configured SSL Inspection rules but the appliance is not licensed for SSL inspection.

Administrator response

This audit information requires no operator response.

GLGLI0005E

Application Identification rules have been configured without a valid Application Identification feature license.

Explanation

A user has configured Application Identification rules but the appliance is not licensed for Application Identification feature.

Administrator response

This audit information requires no operator response.

GLGLI0006E

A user configured the appliance to include IP Reputation information in IPS events without a valid IP Reputation license.

Explanation

A user has configured the appliance to include IP Reputation information in IPS events without a valid IP Reputation license.

Administrator response

To prevent this warning buy or renew your IP Reputation license or disable the IP Reputation feature.

GLGLI0007E

A user configured the appliance to include IP Reputation objects in the Network Access policy without a valid IP Reputation license.

Explanation

A user configured the appliance to include IP Reputation objects in the Network Access policy without a valid IP Reputation license.

Administrator response

To prevent this warning buy or renew your IP Reputation license or edit the Network Access policy to stop using Geolocation or IP Reputation objects.

GLGLI0008E

A user configured the appliance to use Inline Protection Mode without a valid Intrusion Prevention license.

Explanation

A user configured the appliance to use Inline Protection Mode without a valid Intrusion Prevention license.

Administrator response

To prevent this warning buy or renew your Intrusion Prevention license or edit the Inspection Mode to stop using Inline Protection mode.

GLGLI9000I

The administrator, *user_name*, has installed the *type* license.

Explanation

A license was successfully applied to the system.

Administrator response

This is an informational message. No action is required.

GLGPL1004E

An error was detected while processing the System Alerts Policy. The policy will not be applied until the problem is corrected.

Explanation

This message indicates that the System Alerts Policy contains an error that must be corrected before the policy can be used.

Administrator response

Review the Network Objects in use in the System Alerts Policy. Look for any Invalid Object References and remove those objects from the policy. Then re-apply the policy.

GLGPL1005W

The Protection Interfaces policy contains an unsupported speed/duplex setting, *LinkMode*, for interface *Interface* Interface will default to Auto.

Explanation

This message indicates that one or more network interface modules were changed and the Protection Interfaces policy no longer matches the hardware.

Administrator response

Review the Protection Interfaces policy. Correct the speed/duplex setting for the specified interface. Re-apply the policy.

Remote syslog messages

These messages are provided by the remote syslog component.

GLGRL1001I

Communications with remote syslog server, *server*, have been restored.

Explanation
This message indicates the communications to a remote syslog server have been restored after previously encountering an error.

Administrator response
No action is required.

GLGRL1002W

An error occurred attempting to send an event to a remote syslog server, *server*. The server refused the event.

Explanation
The remote syslog response configuration may be incorrect. The remote syslog server may not have been running the syslog service, or it may be misconfigured. An intermediate firewall may have blocked the event.

Administrator response
Verify the remote syslog server parameters are specified correctly. Verify the remote syslog server itself is configured correctly.

Restart shutdown messages

These messages are provided by the restart shutdown component.

GLGRS1001I

The *interface_name* operator *user_name* has restarted the appliance.

Explanation
This message is generated when the appliance is restarted. The message includes the user who requested the restart operation.

Administrator response
This is an informational message. No action is required.

GLGRS1002E

An attempt by the *interface_name* operator *user_name* to restart the appliance has failed.

Explanation
This message is generated when an attempt to restart the appliance has failed. The message includes the user who requested the restart operation.

Administrator response
Review subsequent log messages to determine why the operation failed.

GLGRS1003I

The *interface_name* operator *user_name* has shut down the appliance.

Explanation
This message is generated when the appliance has been shut down. The message includes the user who requested the shutdown operation.

Administrator response
This is an informational message. No action is required.

GLGRS1004E

An attempt by the *interface_name* operator *user_name* to shut down the appliance has failed.

Explanation
This message is generated when an attempt to shut down the appliance has failed. The message includes the user who requested the shutdown operation.

Administrator response
Review subsequent log messages to determine why the operation failed.

GLGRS9001I

The *interface_name* operator *user_name* has restarted the appliance.

Explanation
This message is generated when the appliance is restarted. The message includes the user who requested the restart operation.

Administrator response
This is an informational message. No action is required.

GLGRS9003I

The *interface_name* operator *user_name* has shut down the appliance.

Explanation
This message is generated when the appliance has been shut down. The message includes the user who requested the shutdown operation.

Administrator response
This is an informational message. No action is required.

GLGRS9005I

The *service* service was restarted by the *interface_name* operator *user_name*.

Explanation
A system service was restarted by a user.

Administrator response
This is an informational message. No action is required.

Snapshot messages

These messages are provided by the snapshot component.

GLGSS1001I

The *interface_name* operator *user_name* has created a setting snapshot file: *file_name*.

Explanation

This message is generated when a settings snapshot file has been created. The message includes the name of the file and who created it.

Administrator response

This is an informational message. No action is required.

GLGSS1002E

An attempt by the *interface_name* operator *user_name* to create a settings snapshot file has failed.

Explanation

This message is generated when an attempt to create a settings snapshot file has failed. The message includes the user who requested the settings snapshot.

Administrator response

Review subsequent log messages to determine why the operation failed.

GLGSS1003I

The *interface_name* operator *user_name* has deleted a setting snapshot file: *file_name*.

Explanation

This message is generated when a settings snapshot file has been deleted. The message includes the name of the file and who deleted it.

Administrator response

This is an informational message. No action is required.

GLGSS1004E

An attempt by the *interface_name* operator *user_name* to delete a settings snapshot file, *file_name*, has failed.

Explanation

This message is generated when an attempt to delete a settings snapshot file has failed. The message includes the user who requested the settings snapshot deletion and the name of the file.

Administrator response

Review subsequent log messages to determine why the operation failed.

GLGSS1005I

The *interface_name* operator, *user_name*, has applied a configuration change using setting snapshot file, *file_name*.

Explanation
This message is generated when a user applies a configuration change using a settings snapshot file. The message includes the name of the file and who applied it.

Administrator response
This is an informational message. No action is required.

GLGSS1006E

An attempt by the *interface_name* operator, *user_name*, apply a configuration change from the settings snapshot file, *file_name*, has failed.

Explanation
This message is generated when an attempt to apply a configuration change using a settings snapshot file has failed. The message includes the user who requested the configuration change and the name of the file.

Administrator response
Review subsequent log messages to determine why the operation failed.

GLGSS1007I

The *interface_name* operator, *user_name*, has uploaded a setting snapshot file, *file_name*.

Explanation
This message is generated when a user uploads a settings snapshot file. The message includes the name of the file and who uploaded it.

Administrator response
This is an informational message. No action is required.

GLGSS1008E

An attempt by the *interface_name* operator, *user_name*, to upload a settings snapshot file has failed.

Explanation
This message is generated when an attempt to upload a settings snapshot file has failed. The message includes the user who requested the file upload.

Administrator response
Review subsequent log messages to determine why the operation failed.

GLGSS1009E

The settings snapshot file, *file_name*, uploaded by the *interface_name* user, *user_name*, has failed validation.

Explanation
This message is generated when a settings snapshot file was uploaded but failed validation. The message includes the user who requested the upload and the name of the file.

Administrator response
Review subsequent log messages to determine why the operation failed.

GLGSS1010E

An attempt to set comment, *comment*, to a settings snapshot file, *file_name*, has failed.

Explanation
This message is generated when the operation to set comment to a settings snapshot file has failed. The message includes the comment and the name of the settings snapshot file.

Administrator response
Review subsequent log messages to determine why the operation failed.

GLGSS1011I

The *interface_name* operator *user_name* has modified the comment of a settings snapshot file: *file_name*.

Explanation
This message is generated when the operation to modify the comment of a settings snapshot file has completed.

Administrator response
This is an informational message. No action is required.

GLGSS9001I

The *interface_name* operator *user_name* has created a setting snapshot file: *file_name*.

Explanation
This message is generated when a settings snapshot file has been created. The message includes the name of the file and who created it.

Administrator response
This is an informational message. No action is required.

GLGSS9003I

The *interface_name* operator *user_name* has deleted a setting snapshot file: *file_name*.

Explanation
This message is generated when a settings snapshot file has been deleted. The message includes the name of the file and who deleted it.

Administrator response
This is an informational message. No action is required.

GLGSS9005I

The *interface_name* operator, *user_name*, has applied a configuration change using setting snapshot file, *file_name*.

Explanation
This message is generated when a user applies a configuration change using a settings snapshot file. The message includes the name of the file and who applied it.

Administrator response
This is an informational message. No action is required.

GLGSS9007I

The *interface_name* operator, *user_name*, has uploaded a setting snapshot file, *file_name*.

Explanation
This message is generated when a user uploads a settings snapshot file. The message includes the name of the file and who uploaded it.

Administrator response
This is an informational message. No action is required.

Support messages

These messages are provided by the support component.

GLGSI1001I

The *interface_name* operator *user_name* has created a new support information file: *file_name*.

Explanation
This message is generated when a new support information file has been created. The message includes the name of the file and who created it.

Administrator response
This is an informational message. No action is required.

GLGSI1002E

An attempt by the *interface_name* operator *user_name* to create a new support information file has failed.

Explanation
This message is generated when an attempt to create a new support information has failed. The message includes the user who requested the support information file creation.

Administrator response
Review subsequent log messages to determine why the operation failed.

GLGSI1003I

The *interface_name* operator *user_name* has deleted a support information file: *file_name*.

Explanation

This message is generated when a support information file has been deleted. The message includes the name of the file and who deleted it.

Administrator response

This is an informational message. No action is required.

GLGSI1004E

An attempt by the *interface_name* operator *user_name* to delete a support information file, *file_name*, has failed.

Explanation

This message is generated when an attempt to delete a support information has failed. The message includes the name of the file and who requested its deletion.

Administrator response

Review subsequent log messages to determine why the operation failed.

GLGSI9001I

The *interface_name* operator *user_name* has created a new support information file: *file_name*.

Explanation

This message is generated when a new support information file has been created. The message includes the name of the file and who created it.

Administrator response

This is an informational message. No action is required.

GLGSI9003I

The *interface_name* operator *user_name* has deleted a support information file: *file_name*.

Explanation

This message is generated when a support information file has been deleted. The message includes the name of the file and who deleted it.

Administrator response

This is an informational message. No action is required.

Update messages

These messages are provided by the update component.

GLGUP1001I

The *interface_name* operator, *user_name*, has started the installation of the update *module_name* update version *version_number*.

Explanation
This message is generated when a user starts the installation of an update. The message includes the update type, the version number, and the user who started the installation.

Administrator response
This is an informational message. No action is required.

GLGUP1002E

An attempt by the *interface_name* operator, *user_name*, to install *module_name* update version *version_number* has failed.

Explanation
This message is generated when an attempt to install an update has failed. The message includes the update type, the update version number, and includes the user who attempted to install it.

Administrator response
Review subsequent log messages to determine why the operation failed.

GLGUP1003I

The *interface_name* operator, *user_name*, has scheduled the installation of the update *module_name* update version *version_number* at *date_value*.

Explanation
This message is generated when a user schedules the installation of an update. The message includes the update type, the version number, and the date it will occur.

Administrator response
This is an informational message. No action is required.

GLGUP1004I

The *interface_name* operator, *user_name*, has removed a scheduled installation of the update *module_name* update version *version_number*.

Explanation
This message is generated when a user removes a scheduled installation of an update. The message includes the update type and the version number.

Administrator response
This is an informational message. No action is required.

GLGUP1005I

The *interface_name* operator, *user_name*, has started the installation of the update *module_name* update version *version_number* from a USB device.

Explanation
A user has started an installation of an update to the appliance using a USB device.

Administrator response
This is an informational message. No action is required.

GLGUP1006I

The *interface_name* operator, *user_name*, has started the uninstallation of the update *module_name* update version *version_number*.

Explanation
A user has started an uninstallation of an update to the appliance.

Administrator response
This is an informational message. No action is required.

GLGUP1007I

The update *id* was installed.

Explanation
An update was installed. The system is operating with the updated content.

Administrator response
This is an informational message. No action is required.

GLGUP1008I

The update *id* was uninstalled.

Explanation
An update was uninstalled. The system is operating with the content it was using before this update was applied.

Administrator response
This is an informational message. No action is required.

GLGUP1009E

An attempt to apply the update, *id*, has failed.

Explanation
An attempt to update the system has failed. The system will continue to operate with the current content.

Administrator response
Review subsequent log messages to determine why the operation failed.

GLGUP1010E

An attempt to uninstall the update, *id*, has failed.

Explanation
An attempt to uninstall an update has failed. The system will continue to operate with the current content.

Administrator response
Review subsequent log messages to determine why the operation failed.

GLGUP1011E

An attempt to download the secondary update catalog has failed.

Explanation
An attempt to download the secondary update catalog has failed. The system will try to download it again at the next scheduled interval.

Administrator response
Check network connectivity between the appliance and the internet.

GLGUP1012E

An attempt to download the primary update catalog has failed. Common causes of this failure are not having a license installed and DNS errors.

Explanation
An attempt to download the primary update catalog has failed. The system will try to download it again at the next scheduled interval.

Administrator response
Check network connectivity between the appliance and the internet.

GLGUP1013E

The digital signature of the downloaded update, *file*, could not be verified.

Explanation
The digital signature of the downloaded update could not be verified. The system will delete the update and attempt to download it again at the next scheduled interval.

Administrator response
Check network connectivity between the appliance and the internet.

GLGUP1014E

An attempt to download an update, *file*, has failed.

Explanation
An attempt to download an update has failed. The system will delete the update and attempt to download it again at the next scheduled interval.

Administrator response
Check network connectivity between the appliance and the internet.

GLGUP1015E

An attempt to install the update, *id*, has failed because the required dependency, *requiredId*, has not been met.

Explanation
An attempt to install the update has failed because the required dependency has not been met.

Administrator response
The required dependency must be installed before this update can be installed.

GLGUP9001I

The *interface_name* operator, *user_name*, has started the installation of the update *module_name* update version *version_number*.

Explanation
This message is generated when a user starts the installation of an update. The message includes the update type, the version number, and the user who started the installation.

Administrator response
This is an informational message. No action is required.

GLGUP9003I

The *interface_name* operator, *user_name*, has scheduled the installation of the update *module_name* update version *version_number* at *date_value*.

Explanation
This message is generated when a user schedules the installation of an update. The message includes the update type, the version number, and the date it will occur.

Administrator response
This is an informational message. No action is required.

GLGUP9004I

The *interface_name* operator, *user_name*, has removed a scheduled installation of the update *module_name* update version *version_number*.

Explanation
This message is generated when a user removes a scheduled installation of an update. The message includes the update type and the version number.

Administrator response
This is an informational message. No action is required.

GLGUP9005I

The *interface_name* operator, *user_name*, has started the installation of the update *module_name* update version *version_number* from a USB device.

Explanation
A user has started an installation of an update to the appliance using a USB device.

Administrator response
This is an informational message. No action is required.

GLGUP9006I

The *interface_name* operator, *user_name*, has started the uninstallation of the update *module_name* update version *version_number*.

Explanation
A user has started an uninstallation of an update to the appliance.

Administrator response
This is an informational message. No action is required.

GLGUP9007I

The update *id* was installed.

Explanation
An update was installed. The system is operating with the updated content.

Administrator response
This is an informational message. No action is required.

GLGUP9008I

The update *id* was uninstalled.

Explanation
An update was uninstalled. The system is operating with the content it was using before this update was applied.

Administrator response
This is an informational message. No action is required.

Chapter 3. Audit messages

These messages are provided by the audit component.

FBTAUD001E

Check the audit configuration to ensure that it is correct.

Explanation
The audit configuration settings might contain errors or ommissions.

System action
System will not audit.

Administrator response
Check the audit properties or try restarting the server.

FBTAUD002E

The passed-in audit provider is not supported.

Explanation
This error occurs due to problems in the audit configuration.

System action
System will not audit.

Administrator response
Check the audit properties or try restarting the server.

FBTAUD003E

The audit configuration property *insert* is not defined or is incorrect.

Explanation
This error occurs due to problems in the audit configuration.

System action
System will not audit.

Administrator response
Correctly specify the property and restart the server.

FBTAUD004E

An error was encountered while initializing the file logger.

Explanation
This error occurs due to problems in the audit configuration.

System action
System will not audit.

Administrator response
Check the file logger properties and the encapsulated exception to solve the problem.

FBTAUD005E

An error was encountered while initializing context to the Common Audit Serivice server. Check the JNDI connection property and emitter profile for possible errors.

Explanation
This error occurs due to problems in the audit configuration.

System action
System will not audit.

Administrator response
Check the properties mentioned in the error and the encapsulated exception to solve the problem.

FBTAUD006E

An error was encountered while sending the audit event to the Common Audit Service server.

Explanation
This error occurs because of problems in the audit configuration, or because of connectivity problems with the Common Audit Service server.

System action
System will not audit this particular event.

Administrator response
Ensure that the Common Audit Service server is running and check the encapsulated exception to solve the problem.

FBTAUD007E

An error was encountered while initializing the audit component.

Explanation
This error occurs because of problems in the audit configuration, or because of connectivity problems with the Common Audit Service server.

System action
System will not audit this particular event.

Administrator response
Ensure that the Common Audit Service server is running and check the previous exceptions in the log to determine the cause of the problem.

FBTAUD008E

An event completion exception was encountered because all of the event data is not filled in correctly.

Explanation
This error occurs if any of the required elements in the event are not set.

System action
System will not audit this particular event and will log an exception.

Administrator response
Check the encapsulated exception to solve the problem.

FBTAUD009E

System could not audit a call because a required parameter to the API is not available.

Explanation
This error occurs if any of the required elements in the event are not set.

System action
System will not audit this particular event and will log an exception.

Administrator response
Check the parameter that is not being passed correctly.

FBTAUD010E

An event validation exception was encountered because all of the event data is not correctly filled in.

Explanation
This error occurs if any of the required elements in the event are not set.

System action
System will not audit this particular event and log an exception.

Administrator response
Check the encapsulated exception to solve the problem.

Chapter 4. Authentication service messages

These messages are provided by the authentication service component.

FBTAUT001E

The request does not contain any of the these required parameters [*parameters*]. Please re-access the protected resource.

Explanation
This problem happens because the request does not contain any of the required parameters.

System action
The request is not processed.

Administrator response
None.

FBTAUT002E

Authentication service receives invalid transaction ID [*id*]. Ensure that the transaction with the specified ID exist and has not been processed. Please re-access the protected resource.

Explanation
This problem happens because the transaction with the specified ID does not exist or has been processed.

System action
The request is not processed.

Administrator response
None.

FBTAUT003E

Authentication service receives invalid policy ID [*id*]. Ensure that the policy with the specified ID exist. Please re-access the protected resource.

Explanation
This problem happens because the policy with the specified ID does not exist.

System action
The request is not processed.

Administrator response
None.

FBTAUT004E

Authentication service receives invalid state ID [*id*]. Ensure that you do not use back button on the browser or perform multiple authentication processes in the same browser. Please re-access the protected resource.

Explanation
This problem happens happens because (1) the user uses back button on the browser, (2) the user performs multiple authentication processes in the same browser, (3) the user modifies the state ID parameter value, or (4) the user's session has expired.

System action
The request is not processed.

Administrator response
None.

FBTAUT005E

Authentication service encounters error while executing [*name*] mapping rule.

Explanation
This problem happens happens because (1) the mapping rule is not syntactically correct, or (2) the mapping rule contains logic error.

System action
The request is not processed.

Administrator response
Ensure that the mapping rule is syntactically correct, and does not contain any logic error.

FBTAUT006E

Authentication service cannot perform TOTP authentication because the username parameter is missing. If you specify the username parameter using literal value, ensure that it is not NULL. If you specify the username parameter using context attribute reference, ensure that the referenced context attribute is not NULL. If you do not specify the username parameter, ensure that the authentication policy requires the user to login before they are challenged by TOTP authentication.

Explanation
See message.

System action
The request is not processed.

Administrator response
See message.

FBTAUT007E

Authentication service cannot perform HOTP authentication because the username parameter is missing. If you specify the username parameter using literal value, ensure that it is not NULL. If you specify the username parameter using context attribute reference, ensure that the referenced context attribute is not

NULL. If you do not specify the username parameter, ensure that the authentication policy requires the user to login before they are challenged by HOTP authentication.

Explanation
See message.

System action
The request is not processed.

Administrator response
See message.

FBTAUT008E

Authentication service cannot perform RSA authentication because the username parameter is missing. If you specify the username parameter using literal value, ensure that it is not NULL. If you specify the username parameter using context attribute reference, ensure that the referenced context attribute is not NULL. If you do not specify the username parameter, ensure that the authentication policy requires the user to login before they are challenged by RSA authentication.

Explanation
See message.

System action
The request is not processed.

Administrator response
See message.

FBTAUT009E

Authentication service cannot perform MAC one-time password authentication because the supplied delivery type is invalid. The valid values for the deliveryType are parameter are Email and SMS.

Explanation
The delivery type should be set to Email or SMS.

System action
The request is not processed.

Administrator response
Modify the deliveryType value to one of the supported values.

FBTAUT010E

Authentication service cannot perform MAC one-time password authentication because the username parameter is missing. If you specify the username parameter using literal value, ensure that it is not NULL. If you specify the username parameter using context attribute reference, ensure that the referenced context attribute is not NULL. If you do not specify the username parameter, ensure that the authentication policy requires the user to login before they are challenged by MAC one-time password authentication.

Explanation
See message.

System action
The request is not processed.

Administrator response
See message.

FBTAUT011E

Authentication service cannot perform one-time password authentication because the username parameter is missing. If you specify the username parameter using literal value, ensure that it is not NULL. If you specify the username parameter using context attribute reference, ensure that the referenced context attribute is not NULL. If you do not specify the username parameter, ensure that the authentication policy requires the user to login before they are challenged by one-time password authentication.

Explanation
See message.

System action
The request is not processed.

Administrator response
See message.

FBTAUT012E

Authentication service receives invalid target URL [*url*]. Ensure that the target URL is specified. Please re-access the protected resource.

Explanation
This problem happens because the target URL is not specified.

System action
The request is not processed.

Administrator response
None.

FBTAUT013E

Authentication service cannot create a user credential because there is a duplicate credential attribute [*attribute*] specified for authentication policy [*policy*].

Explanation
This problem happens because there is a duplicate credential attribute.

System action
The request is not processed.

Administrator response
None.

FBTAUT014E

Authentication service cannot perform EULA authentication because the username parameter is missing. If you specify the username parameter using literal value, ensure that it is not NULL. If you specify the username parameter using context attribute reference, ensure that the referenced context attribute is not NULL. If you do not specify the username parameter, ensure that the authentication policy requires the user to login before they are challenged by EULA authentication.

Explanation
See message.

System action
The request is not processed.

Administrator response
See message.

FBTAUT015E

Authentication service cannot perform knowledge questions based authentication because the username parameter is missing. If you specify the username parameter using literal value, ensure that it is not NULL. If you specify the username parameter using context attribute reference, ensure that the referenced context attribute is not NULL. If you do not specify the username parameter, ensure that the authentication policy requires the user to login before they are challenged by the knowledge questions based authentication.

Explanation
See message.

System action
The request is not processed.

Administrator response
See message.

FBTAUT016E

Authentication service cannot parse the request data content.

Explanation
This happens if the request does not contain any JSON data, the JSON data in not valid, or the content-type header was not application/json.

System action
The request is not processed.

Administrator response
Modify the client request.

FBTAUT017E

Authentication service received an invalid state ID [*id*].

Explanation
This problem happens happens because (1) the requester performs multiple authentication processes in the same session, (2) the requester supplied the wrong or modified state ID parameter value, or (3) the requester's session has expired.

System action
The request is not processed.

Administrator response
None.

FBTAUT018E

Authentication service received an invalid JSON request. This request could not be processed.

Explanation
This problem happens happens because (1) the request is not valid for the given authentication policy (2) the request is not valid for the current authentication mechanism or authentication state, or (3) The JSON data could not be parsed or read, or contained too many levels of nested objects.

System action
The request is not processed.

Administrator response
None.

FBTAUT019E

Authentication service cannot perform Mobile User Approval authentication because an OAuth access token is missing. Ensure that the authentication policy requires the user to obtain an OAuth access token before they are challenged by Mobile User Approval authentication.

Explanation
See message.

System action
The request is not processed.

Administrator response
See message.

FBTAUT020E

Authentication service cannot perform Mobile User Approval authentication because the username parameter is missing. If you specify the username parameter using literal value, ensure that it is not NULL. If you specify the username parameter using context attribute reference, ensure that the referenced context attribute is not NULL. If you do not specify the username parameter, ensure that the authentication policy requires the user to login before they are challenged by Mobile User Approval authentication.

Explanation
See message.

System action
The request is not processed.

Administrator response
See message.

FBTAUT021E

Authentication service cannot perform Mobile Multi Factor authentication because the username parameter is missing. If you specify the username parameter using literal value, ensure that it is not NULL. If you specify the username parameter using context attribute reference, ensure that the referenced context attribute is not NULL. If you do not specify the username parameter, ensure that the authentication policy requires the user to login before they are challenged by Mobile Multi Factor authentication.

Explanation
See message.

System action
The request is not processed.

Administrator response
See message.

FBTAUT022E

The target URL *targetURL* is not whitelisted.

Explanation
The target URL received by the system is rejected because it is not whitelisted.

System action
The flow is stopped.

Administrator response
Check if the target URL should be whitelisted.

FBTAUT023E

Authentication service cannot perform Universal 2nd Factor authentication because the username parameter is missing. If you specify the username parameter using literal value, ensure that it is not NULL. If you specify the username parameter using context attribute reference, ensure that the referenced context attribute is not NULL. If you do not specify the username parameter, ensure that the authentication policy requires the user to login before they are challenged by Universal 2nd Factor authentication.

Explanation
See message.

System action
The request is not processed.

Administrator response
See message.

Chapter 5. Context-based access messages

These messages are provided by the context-based access component.

FBTRBA001E

A database error occurred.

Explanation
An unrecoverable database error occurred.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTRBA002E

An error occurred when managing the policy.

Explanation
See message.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTRBA003E

An error occurred during command execution.

Explanation
See message.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTRBA005E

A required parameter *parameter name* is missing or invalid.

Explanation
See message.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTRBA007E

The policy file does not exist.

Explanation
See message.

System action
Command execution is halted.

Administrator response
Specify a policy file that exists and run the command again.

FBTRBA008E

Creation of database connection failed. Check the database configuration and network connectivity to the database server.

Explanation
The database connection could not be created.

System action
Command execution is halted.

Administrator response
Ensure that the database is configured correctly. Also check that the network connectivity to the database server is available.

FBTRBA009E

Unable to modify the application parameter *task or role name*.

Explanation
An attempt to locate and modify a particular set of application parameters failed during deployment.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTRBA0100E

The action: *action* failed because the resource [*resource*] was not found.

Explanation
The requested action on the specified resource could not be completed because the resource was not found.

System action
No action necessary.

Administrator response
Ensure that the resource and action requested are valid.

FBTRBA0101E

The import cannot be performed while another import is in progress.

Explanation
The system can only perform one import operation at a time.

System action
The new import operation request was ignored.

Administrator response
Retry the new import operation after the original import operation is completed.

FBTRBA0106E

The action *action* failed because the resource ID [*id*] is not valid for a resource of type: [*type*].

Explanation
The requested action on the specified resource could not be completed because the resource ID is invalid.

System action
No action is necessary.

Administrator response
Ensure that the resource and action requested are valid.

FBTRBA0107E

The action *action* failed for resource [] because the request body contains improperly structured JSON.

Explanation
The requested action on the specified resource could not be completed because the request body contains malformed or improperly structured JSON.

System action
No action is necessary.

Administrator response
Ensure that the request body contains the appropriately structured JSON for the requested action.

FBTRBA0108W

The update failed because the resource was not found.

Explanation
The requested action on the specified resource could not be completed because the resource was not found.

System action
No action necessary.

Administrator response
Ensure that the resource and action requested are valid.

FBTRBA0109W

The resource already exists.

Explanation
The requested action on the specified resource could not be completed because the resource already exists.

System action
No action necessary.

Administrator response
Ensure that the resource and action requested are valid.

FBTRBA010E

The IBM Tivoli Federated Identity Manager runtime is not deployed. Deploy the IBM Tivoli Federated Identity Manager runtime before continuing.

Explanation
The risk-based access runtime requires that the IBM Tivoli Federated Identity Manager runtime be deployed first.

System action
Command execution is halted.

Administrator response
Deploy the IBM Tivoli Federated Identity Manager runtime before proceeding.

FBTRBA0110E

The device *id* was not found.

Explanation
The requested device does not exist.

System action
No action necessary.

Administrator response
Ensure that the resource and action requested are valid.

FBTRBA0111E

The user *userID* does not have any registered devices.

Explanation
The requested user does not have any devices registered.

System action
No action necessary.

Administrator response
Ensure that the resource and action requested are valid.

FBTRBA0112E

Devices with IDs *ids* were not found.

Explanation
One or more of the requested devices does not exist.

System action
No action necessary.

Administrator response
Ensure that the resource and action requested are valid.

FBTRBA0113E

No devices last used before *timestamp* were found.

Explanation
No devices last used before the requested timestamp were found.

System action
No action necessary.

Administrator response
Ensure that the resource and action requested are valid.

FBTRBA0114E

The file export failed.

Explanation
The file export failed. This can occur if the file does not exist, there are access permissions either at the source or destination, or because there was an I/O error.

System action
No action is necessary.

Administrator response
Examine the logs for the cause of the exception. Ensure that the file exists, that access permissions are set properly, and that there is sufficient space to export the file.

FBTRBA0115E

The file import failed.

Explanation
The file import failed. This can occur if the file does not exist, there are access permissions either at the source or destination, or because there was an I/O error.

System action
No action is necessary.

Administrator response
Examine the logs for the cause of the exception. Ensure that the file exists, that access permissions are set properly, and that there is sufficient space to import the file.

FBTRBA0116E

The filter string is empty.

Explanation
The filter query parameter has an empty value.

System action
No action is necessary.

Administrator response
If filtering is required add valid content to the value of the filter field.

FBTRBA0117E

The filter contains unknown java.sql.Types [*filterObj*]. Supported values are *supportedValues*.

Explanation
An unknown or unsupported java.sql.Types type was passed into the filter.

System action
No action is necessary.

Administrator response
If filtering is required use supported java.sql.Types.

FBTRBA0118E

The filter format is not valid. Filters should be in the format of *supportedValues*.

Explanation
An invalid filter syntax was used.

System action
No action is necessary.

Administrator response
If filtering is required use supported format.

FBTRBA0119E

No matching field name for [*jsonFieldName*] was found.

Explanation
An invalid filter syntax was used.

System action
No action is necessary.

Administrator response
If filtering is required use supported format.

FBTRBA011E

The risk-based access deployment failed.

Explanation
An error occurred during risk-based access deployment.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTRBA0120E

The filter function: *function* is not valid. Supported functions are: *supportedFunctions* .

Explanation
An invalid filter type was used.

System action
No action is necessary.

Administrator response
If filtering is required use supported format.

FBTRBA0121E

The action failed because the policy is contained in one or more policy sets. The policy sets are [*policySetNames*].

Explanation
The action is not allowed when the policy is referenced by another resource.

System action
No action necessary.

Administrator response
Remove references to the policy and retry the action.

FBTRBA0122E

The action failed because the policy set is attached to one or more resources. The resources are [*policySetName*].

Explanation
The action is not allowed when the policy set is referenced by another resource.

System action
No action necessary.

Administrator response
>Remove references to the policy set and retry the action.

FBTRBA0123E

Returned improper datatype of: *passedDataType*. Expected a JavaScript object.

Explanation
The specified data type was returned, but was incorrect. A JavaScript object was expected.

System action
No action is necessary.

Administrator response
Ensure that the getMetadata function returns the JavaScript object in the authentication rule JavaScript.

FBTRBA0124E

The *fieldWithIssue* object has experienced *exceptionType*. Cannot convert *passedDataType* object type to a *newDataType* object type.

Explanation
Conversion to the new data type did not complete because of an exception.

System action
No action is necessary.

Administrator response
Ensure that the data types in authentication rule JavaScript match the required specifications.

FBTRBA0125E

Expected key, *missingKey*, was not found in the JavaScript.

Explanation
At least one expected key was not found in the Javascript getMetadata function.

System action
No action is necessary.

Administrator response
Ensure that the getMetadata function in the authentication rule JavaScript contains the appropriate keys and fields.

FBTRBA0126E

The authentication rule JavaScript must contain the getMetadata function with the metadata values stored inside.

Explanation
The program expected the getMetadata function in the JavaScript, and it was not found.

System action
No action is necessary.

Administrator response
Ensure that the getMetadata function in the athentication rule JavaScript exists.

FBTRBA0127E

The table type *unsupportedTable* is not supported. Supported types are: *supportedTables*.

Explanation
An unsupported table type was specified.

System action
No action necessary.

Administrator response
Specify a supported table type.

FBTRBA0128E

The resource ID *resourceId* does not exist within the table *supportedTables*.

Explanation
A resource relationship was specified with a resource that does not exist.

System action
No action necessary.

Administrator response
Specify an existing resource.

FBTRBA0129E

The obligation with the URI *obligationUri* does not exist.

Explanation
The specified obligation URI does not exist.

System action
No action necessary.

Administrator response
Specify an existing obligation URI.

FBTRBA012E

The risk-based access deployment failed because it could not determine the directory in which IBM Tivoli Federated Identity Manager is installed.

Explanation
See message.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTRBA0130E

The attribute with the combination of URI: *attrUri*, datatype: *dataType*, and issuer: *issuer* does not exist.

Explanation
The specified combination of URI, datatype and issuer does not exist.

System action
No action necessary.

Administrator response
Specify an existing URI, datatype and issuer combination.

FBTRBA0131E

The attribute with the combination of URI: *attrUri*, and datatype: *dataType* does not exist.

Explanation
The specified combination of URI and datatype does not exist.

System action
No action necessary.

Administrator response
Specify an existing URI and datatype combination.

FBTRBA0132E

The action failed because the attribute is used in one or more policies. The policies are [*policyNames*].

Explanation
The action is not allowed when the attribute is referenced by another resource.

System action
No action necessary.

Administrator response
Remove references to the attribute and retry the action.

FBTRBA0133E

The metadata from the JavaScript that was included in the JSON file was not retrieved properly.

Explanation
The getMetadata function in the JavaScript that contains the metadata of the script could not be retrieved.

System action
No action is necessary.

Administrator response
Ensure that the getMetadata function in the authentication rule JavaScript exists and is formatted properly.

FBTRBA0134E

The action failed because the obligation is used in one or more policies. The policies are [*policyNames*].

Explanation
The action is not allowed when the obligation is referenced by another resource.

System action
No action necessary.

Administrator response
Remove references to the obligation and retry the action.

FBTRBA0135E

Authentication rules with the names: *authnRuleNames* are currently using this obligation. An obligation that is being referenced by another resource cannot be deleted.

Explanation
A delete operation of an obligation that is being referenced by other resources is not allowed.

System action
No action necessary.

Administrator response
Remove references to this obligation, and then try deleting it again.

FBTRBA0136E

No obligation URI associated with the ID: *oblId*.

Explanation
A delete operation of an obligation that does not exist is not allowed.

System action
No action necessary.

Administrator response
Specify a valid obligation ID to delete.

FBTRBA0137E

Authentication rule with the name: *authnRuleName* and policies with the names: *policyNames* are currently using this obligation. An obligation that is being referenced by another resource cannot be deleted.

Explanation
A delete operation of an obligation that is being referenced by other resources is not allowed.

System action
No action necessary.

Administrator response
Remove references to this obligation, and then try deleting it again.

FBTRBA0138E

The action failed because the attribute is included in a risk profile or policy. The risk profiles are [*profileNames*]. The policies are [*policyNames*].

Explanation
The action is not allowed when the attribute is referenced by another resource.

System action
No action necessary.

Administrator response
Remove references to the attribute and retry the action.

FBTRBA0139E

The action failed because the attribute is included in one or more risk profiles. The risk profiles are [*profileNames*].

Explanation
The action is not allowed when the attribute is referenced by another resource.

System action
No action necessary.

Administrator response
Remove references to the attribute and retry the action.

FBTRBA013E

The risk-based access deployment failed because the runtime security services EAR is not found at the following location: *RTSS Ear path*.

Explanation
See message.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTRBA0140E

No mapping found between the authentication rule and obligation with the URI value of: *oblUri*.

Explanation
There should be a one to one mapping between the obligation and authentication URIs.

System action
If this error is encountered the database needs to be cleaned up manually.

Administrator response
Manually remove the obligation from the back end data store.

FBTRBA0141E

A predefined resource cannot be deleted or modified. The resource is [*resourceName*].

Explanation
Predefined resources cannot be modified or deleted.

System action
No action necessary.

Administrator response
No action necessary.

FBTRBA0142E

The action failed because the policy is contained in a policy set or attached to a resource. The policy sets are [*policySetNames*]. The resources are [*policyAttachmentNames*].

Explanation
The action is not allowed when the policy is referenced by another resource.

System action
No action necessary.

Administrator response
Remove references to the policy and retry the action.

FBTRBA0143E

The action failed because the policy is attached to one or more resources. The resources are [*policyAttachmentNames*].

Explanation
The action is not allowed when the policy is referenced by another resource.

System action
No action necessary.

Administrator response
Remove references to the policy and retry the action.

FBTRBA0144E

The action failed because the policy set is attached to one or more resources. The resources are [*policyAttachmentNames*].

Explanation
The action is not allowed when the policy set is referenced by another resource.

System action
No action necessary.

Administrator response
Remove references to the policy set and retry the action.

FBTRBA0145W

Unable to obtain authenticated user name. Setting user name to: *unauthnUser*.

Explanation
Failed to get a value while attempting to get the authenticated user from the Subject or Principal objects

System action
No action necessary.

Administrator response
Try authenticating with a valid user.

FBTRBA0146E

The JavaScript mapping rule that you submitted is not valid. The JavaScript validator reported a syntax error at line *line* and column *column* with the message: *message*.

Explanation
The JavaScript mapping rule that you submitted is not valid. You can only submit a valid JavaScript mapping rule.

System action
The JavaScript mapping rule is rejected.

Administrator response
Submit a valid JavaScript mapping rule.

FBTRBA0147E

The data type [*type*] in the XACML policy is not supported. Supported types are: *dataTypes*.

Explanation
The data type passed in is not supported.

System action
The XACML string is rejected.

Administrator response
Submit a valid data type within the XACML string.

FBTRBA0148E

A predefined resource cannot be deleted. The resource is [*resourceName*].

Explanation
Predefined resources of this type cannot be deleted.

System action
No action necessary.

Administrator response
No action necessary.

FBTRBA0149E

The configuration property cannot be modified because it is a read-only property.

Explanation
Read-only configuration cannot be modified.

System action
The modification operation is rejected.

Administrator response
No action necessary.

FBTRBA014E

The risk-based access deployment failed because the following configuration directory could not be created: *Configuration Directory*.

Explanation
See message.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTRBA0150E

The data type of the configuration property is not valid. The data type is: *dataType*.

Explanation
The configuration property data type is not supported.

System action
The modification operation is rejected.

Administrator response
No action necessary.

FBTRBA0151E

The configuration property value is not valid. Valid values are: *validValues*.

Explanation
The configuration property value is not valid.

System action
The modification operation is rejected.

Administrator response
No action necessary.

FBTRBA0152E

The field [*inputFieldName*] is not valid for sorting. Valid fields are: *validFields*.

Explanation
An invalid field name was used for sorting.

System action
No action necessary.

Administrator response
No action necessary.

FBTRBA0160E

A delete cannot be performed while another delete is in progress.

Explanation
The system can perform only one delete operation at a time.

System action
The new delete operation request was ignored.

Administrator response
Retry the new delete operation after the original delete operation is completed.

FBTRBA017E

The risk-based access deployment failed because the configuration repository directory could not be determined.

Explanation
See message.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTRBA018E

The risk-based access deployment failed because the runtime security services archive file is not found at the following location: *RTSS archive path*.

Explanation
See message.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTRBA019E

The risk-based access deployment task failed because the risk-based access runtime security services plugins directory is not found at the following location: *rba plugins path*.

Explanation
See message.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTRBA020E

The risk-based access deployment failed because a required file is not found at the following location: *path to file*.

Explanation
See message.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTRBA021E

An error occurred during the risk-based access redeployment. Check the application server logs for more details.

Explanation
See message.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTRBA028E

Deserialization of the response file failed.

Explanation
See message.

System action
Command execution is halted.

Administrator response
Check the XML response file to verify that it is valid and try again.

FBTRBA0294E

No matching field name for [*jsonFieldName*] was found. Valid filter field values for this resource are [*validFields*].

Explanation
An invalid filter syntax was used.

System action
No action is necessary.

Administrator response
If filtering is required use supported format.

FBTRBA029E

The risk-based access deployment failed because the risk-based access JavaScript directory is not found at the following location: *rbajavascript path*.

Explanation
See message.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTRBA049E

The runtime property ac.request.server is not configured.

Explanation
To make cross-domain AJAX requests, the runtime property ac.request.server must be configured.

System action
The CORS headers are not set in the HTTP response.

Administrator response
Configure the runtime property ac.request.server.

FBTRBA057E

The attribute string is formatted incorrectly.

Explanation
Attributes must be formatted as key=value and separated by the specified delimiter or a percent symbol (%).

System action
Command execution is halted.

Administrator response
Ensure that the attribute string is formatted correctly.

FBTRBA058E

The attribute name, *name*, is invalid and is not configured.

Explanation
The attribute validation failed because the attribute is not configured.

System action
Command execution is halted.

Administrator response
Configure the attribute.

FBTRBA060E

The policies are not exported to *location*.

Explanation
An error occurred when exporting policies to the specified location.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTRBA061E

An error occurred when parsing the XACML rules file.

Explanation
The XACML rules file could not be parsed successfully, probably due to improper syntax.

System action
Command execution is halted.

Administrator response
Check the syntax of the XACML rules file and try again. Also check the server logs for more details to trace the cause of the error.

FBTRBA062E

An unknown operation *operation name* is specified.

Explanation
An invalid operation is specified by the user.

System action
Command execution is halted.

Administrator response
Run the command with a correct operation as specified in the documentation.

FBTRBA065E

Reloading of the configuration failed.

Explanation
A subcomponent returned an error during the reload attempt.

System action
Command execution is halted.

Administrator response
Check the logs for more details to trace the cause of the error.

FBTRBA066E

The device ID is invalid.

Explanation
The device ID is not formatted correctly. It must be an integer value.

System action
Command execution is halted.

Administrator response
Verify the device ID.

FBTRBA069E

The type for the attribute *id* is not specified.

Explanation
An attribute and its type must be specified must be specified before referencing the attribute. Valid types are integer, double, string, time, or date.

System action
Command execution is halted.

Administrator response
Specify the type for the attribute in the XACML rules file.

FBTRBA075E

The *operation* operation is not allowed because runtime security service was installed by IBM Tivoli Security Policy Manager.

Explanation
The runtime security service was deployed by IBM Tivoli Security Policy Manager; so policy management must be done using IBM Tivoli Security Policy Manager.

System action
Command execution is halted.

Administrator response
Use IBM Tivoli Security Policy Manager to manage policies.

FBTRBA077E

Service name missing. To specify the service name, use the -serviceName parameter, or add *serviceNameConfigPropertyName* to the risk-based access configuration.

Explanation
The default service name was not configured, and a value was not provided through the serviceName parameter.

System action
Command execution is halted.

Administrator response
Add a default service name to the risk-based access configuration, or specify one using the the serviceName parameter.

FBTRBA078E

The risk-based access deployment task failed because the risk-based access matchers directory was not found at this location: *rba matchers path*

Explanation
The risk-based access deployment encountered an error and could not continue.

System action
The risk-based access deployment task is halted.

Administrator response
Check the system logs for more details and ensure that the risk-based access installation step has completed.

FBTRBA079E

The attribute collection service GET method is not enabled.

Explanation
The property ac.get.attributes.enabled must be set to true in order to use the attribute collection service's GET method.

System action
No attributes were retrieved from the database.

Administrator response
Set the property ac.get.attributes.enabled to true in order to use the attribute collection service's GET method.

FBTRBA080E

This client is not allowed to access the attribute collection service's GET method.

Explanation
Only clients listed in the ac.get.attributes.allowed.clients property may access the attribute collection service's GET method.

System action
No attributes were retrieved from the database.

Administrator response
Add this client to the list of allowed clients or reaccess from an allowed client.

FBTRBA085E

Line number: *line number* Lines must be formatted as country,region,city,postal code,metro code,start IP,end IP.

Explanation
An invalid format was found in the custom location data file on the specified line number. Lines must be formatted as country,region,city,postal code,metro code,start IP,end IP.

System action
Custom location data was not loaded.

Administrator response
Fix the custom location file and redeploy.

FBTRBA086E

Line number: *line number* Start IP and end IP must be valid IP addresses.

Explanation
An invalid value was found for start IP or end IP on the specified line number. The value must be a valid IPv4 or IPv6 address.

System action
Custom location data was not loaded.

Administrator response
Fix the custom location file and redeploy.

FBTRBA086W

The IP reputation threshold configuration property is not valid. The default value of *default value* will be used in place of the invalid value.

Explanation
An invalid value was found for the ip.reputation.threshold configuration property. Valid values include any integer from 0 to 100.

System action
The default value was used.

Administrator response
Set the ip.reputation.threshold property to any valid value and reload risk-based access.

FBTRBA087E

The update of this resource requires the *field name* field to have an *value type* value present.

Explanation
There was a required value missing in one of the fields. Refer to the exception for which fields and types are missing.

System action
Add the required input to payload.

Administrator response
Add a value of the correct type to the update to request payload.

FBTRBA088E

The update of the resource [*name*] failed.

Explanation
During the update operation of the resource, a database exception was encountered.

System action
Ensure that the database is running correctly.

Administrator response
See the exception in the logs for the cause.

FBTRBA089E

The delete of the resource failed.

Explanation
During the delete operation of the resource, a database exception was encountered.

System action
Ensure that the database is running correctly.

Administrator response
See the exception in the logs for the cause.

FBTRBA090E

The delete failed because the resource cannot be found.

Explanation
During the delete operation, the specified resource was not found.

System action
See the exception in the logs for the cause.

Administrator response
Verify that the resource exists.

FBTRBA091E

The retrieval failed because the resource cannot be found.

Explanation
During the get operation, the specified resource was not found.

System action
See the exception in the logs for the cause.

Administrator response
Contact your system administrator regarding the database exception.

FBTRBA092E

The retrieval of the [*resourceType*] resources failed.

Explanation
During the retrieval operation, the specified resource was not found.

System action
See the exception in the logs for the cause.

Administrator response
Contact your system administrator regarding the database exception.

FBTRBA093E

The creation of the [*resourceType*] resources failed.

Explanation
During the create operation, there was either a key violation or an internal server error.

System action
See the exception in the logs for the cause.

Administrator response
Contact your system administrator regarding the database exception.

FBTRBA094E

The generation of an ID from the KEYS table for resource type [*resourceType*] failed.

Explanation
During the creation of the resource ID, there was an internal server error.

System action
See the exception in the logs for the cause.

Administrator response
Contact your system administrator regarding the database exception.

FBTRBA095E

The value [*constraintValue*] for [*constraintName*] already exists.

Explanation
The creation or update of the resource failed because a value within your request, that is required to be unique, already exists.

System action
See the exception in the logs for more details.

Administrator response
Specify a different value for the resource constraint.

FBTRBA096E

The profile [*nameValue*] is active. Active profiles cannot be deleted.

Explanation
Attempted to delete an active profile. An active profile cannot be deleted.

System action
No action necessary.

Administrator response
Update the profile so that it is not active, and then delete it.

FBTRBA097E

The database connection failed. Check the logs for more information.

Explanation
The connection object was null. There might be a data source or database problem.

System action
Check the data source and database configuration. Also, check the help information for your database.

Administrator response
Check the data source and database configuration.

FBTRBA098E

The value [*value*] for [*propertyName*] is not valid. Valid values are: *validValues*

Explanation
The specified value is not valid.

System action
No action necessary.

Administrator response
Ensure that you are using the allowed values for this column.

FBTRBA099E

The delete of the attribute failed because it is included in one or more risk profiles. The risk profiles are: *profileNames*.

Explanation
The delete of the attribute failed because it is used by another risk profile.

System action
No action necessary.

Administrator response
To delete this attribute, first remove this attribute from all risk profiles.

FBTRBA102E

The geolocation file must be a .zip file.

Explanation
The import only supports .zip files.

System action
The geolocation data in the database was not changed.

Administrator response
Import the geolocation data in a .zip file.

FBTRBA103E

The data within the geolocation .zip file is not valid.

Explanation
The .zip file must contain two files. The name of one of the files must contain the word Location. The name of the other file must contain the word Blocks.

System action
The geolocation data in the database was not changed.

Administrator response
Upload a .zip file that contains two properly named files.

FBTRBA153E

The update of the resource [*resourceRequestUri*] failed.

Explanation
During the update operation of the resource, a database exception was encountered.

System action
Ensure that the database is running correctly.

Administrator response
See the exception in the logs for the cause.

FBTRBA154E

An attribute with the internal ID of [*attrId*] was not found.

Explanation
An attribute with the specified attribute ID does not exist.

System action
No action necessary.

Administrator response
No action necessary.

FBTRBA155E

The resource request did not include a valid CSRF token or the request CSRF token did not match the server CSRF token.

Explanation
The CSRF token parsed from the request was either null or did not match with the stored version on the server.

System action
No action necessary.

Administrator response
No action necessary.

FBTRBA156E

An exception was encountered while parsing the CSRF token from the resource request.

Explanation
The resource request did not match the format expected and caused a CSRF parsing error.

System action
No action necessary.

Administrator response
No action necessary.

FBTRBA164E

The device *name* was not removed.

Explanation
The device could not be deleted.

System action
No devices were deleted.

Administrator response
No action necessary.

FBTRBA166E

The device *name* could not be updated.

Explanation
The device could not be updated.

System action
No devices were updated.

Administrator response
No action necessary.

FBTRBA168E

The HMAC OTP secret key could not be reset.

Explanation
The secret key could not be reset.

System action
The secret key was not reset.

Administrator response
No action necessary.

FBTRBA169E

The value [*uri*] is not a valid URI.

Explanation
The requested value is not a valid URI.

System action
The requested action was not performed.

Administrator response
Ensure the requested value is a valid URI.

FBTRBA179E

Communication with the policy server failed with the following command error: *cmdErr*.

Explanation
Communication with the policy server failed.

System action
Ensure that all back end servers are running.

Administrator response
The database, policy manager and webseal server(s) could be down.

FBTRBA180E

The http method used to submit the request is not valid. The valid method is [*valid HTTP Method*].

Explanation
Submit the request using the supported http method.

System action
The request has been halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTRBA181E

The consent to register device process failed.

Explanation
The consent to register device process did not complete.

System action
The request has been halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTRBA182E

The value [*value*] is not valid.

Explanation
The specified value is not valid.

System action
The requested action was not performed.

Administrator response
Ensure the requested value is valid.

FBTRBA183E

The value [*value*] for [*propertyName*] is not valid.

Explanation
The specified value is not valid.

System action
The requested action was not performed.

Administrator response
Ensure the requested value is valid.

FBTRBA184E

The value for [*propertyName*] is missing.

Explanation
A required property value is missing.

System action
No action necessary.

Administrator response
Ensure that the property value is specified

FBTRBA185E

A request *method uri* was denied due to the cluster configuration.

Explanation
The requested URL value is not a master node.

System action
The requested URL value is not a master node.

Administrator response
To perform management operations please make requests to the management nodes URL.

FBTRBA186E

A device named [*device name*] already exists.

Explanation
Device names must be unique.

System action
No action necessary.

Administrator response
Specify a unique name for the device.

FBTRBA187E

The value for [*propertyName*] is too long.

Explanation
The length of the string for the property is too long.

System action
No action necessary.

Administrator response
Specify a shorter length string

FBTRBA188E

The value specified for device name is too long.

Explanation
The length of the string for the device name is too long.

System action
No action necessary.

Administrator response
Specify a shorter length string

FBTRBA189E

The value [*value*] specified for device name is not valid.

Explanation
The specified value is not valid.

System action
The requested action was not performed.

Administrator response
Ensure the requested value is valid.

FBTRBA190W

The device registration process failed for user [*value*];

Explanation
The device registration process did not complete.

System action
The device will not be registered.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTRBA191E

The definition does not exist.

Explanation
The definition does not exist.

System action
No action necessary.

Administrator response
Ensure that the definition exists.

FBTRBA192E

The minimum length for the client shared-secret is *<number>* characters.

Explanation
The length of the client shared-secret in the response file does not meet the required length.

System action
No action taken.

Administrator response
Ensure that the client shared-secret meets the minimum length requirement.

FBTRBA193E

The value for [*propertyName*] is not valid.

Explanation
The specified value is not valid.

System action
The requested action was not performed.

Administrator response
Ensure the requested value is valid.

FBTRBA194E

The policy type [*inputFieldName*] is not valid. Valid types are: *validFields*.

Explanation
The policy type is invalid.

System action
The requested action was not performed.

Administrator response
Ensure the policy type is valid.

FBTRBA195E

The action failed because the definition is referenced by a client or attached to a resource. The clients are [*clientNames*]. The resources are [*policyAttachmentNames*].

Explanation
The action is not allowed when the definition is referenced by another resource.

System action
No action necessary.

Administrator response
Remove references to the definition and retry the action.

FBTRBA196E

The action failed because the definition is referenced by one or more clients. The clients are [*clientNames*].

Explanation
The action is not allowed when the definition is referenced by another resource.

System action
No action necessary.

Administrator response
Remove references to the definition and retry the action.

FBTRBA197E

The action failed because the definition is attached to one or more resources. The resources are [*policyAttachmentNames*].

Explanation
The action is not allowed when the definition is referenced by another resource.

System action
No action necessary.

Administrator response
Remove references to the definition and retry the action.

FBTRBA198E

The authorization grant *state_id* could not be updated.

Explanation
The authorization grant could not be updated.

System action
No authorization grants were updated.

Administrator response
No action necessary.

FBTRBA200E

The authorization grant *state_id* was not removed.

Explanation
The authorization grant could not be deleted.

System action
No authorization grants were deleted.

Administrator response
No action necessary.

FBTRBA202E

The policy information point property *pipProperty* cannot be modified because it is a read-only property.

Explanation
Read-only policy information point property cannot be modified.

System action
The modification operation is rejected.

Administrator response
No action necessary.

FBTRBA203E

The action failed because the policy information point is associated with one or more attributes. The attributes are [*attributeNames*]. Remove the Issuer from the attributes before you delete the policy information point.

Explanation
The action is not allowed when the policy information point is referenced by another resource.

System action
No action necessary.

Administrator response
Remove references to the policy information point and retry the action.

FBTRBA204E

The REST service returned an unexpected error code: [*error code*]

Explanation
An error was received while calling the REST service.

System action
Processing of the attribute was halted.

Administrator response
Verify that the REST service is functioning properly.

FBTRBA205E

The attribute finder for attribute [*attribute name*] returned no values.

Explanation
The REST service did not return a value for the requested attribute.

System action
The attribute value was set to the empty string.

Administrator response
Verify that the REST service is functioning properly.

FBTRBA206E

The required property [*configuration property*] does not exist in the configuration.

Explanation
The configuration for a required property is missing.

System action
PIP initialization could not complete, so the PIP was disabled.

Administrator response
Configure the missing property.

FBTRBA207E

The required property [*configuration property*] for instance [*instance name*] contains an HTTP header delimiter, but it is not in the correct format.

Explanation
The format for HTTP headers is incorrect.

System action
PIP initialization could not complete, so the PIP was disabled.

Administrator response
Verify the HTTP header configuration.

FBTRBA210E

The property [*configuration property*] for instance [*instance name*] contains an unsupported URI scheme.

Explanation
The specified URI scheme is invalid.

System action
PIP initialization could not complete, so the PIP was disabled.

Administrator response
Verify the URI scheme in the REST service URL.

FBTRBA211E

The property [*configuration property*] for instance [*instance name*] is not a valid URL.

Explanation
A properly formatted URL must be specified for the REST service.

System action
PIP initialization could not complete, so the PIP was disabled.

Administrator response
Verify the REST service URL configuration.

FBTRBA212E

The property [*configuration property*] for instance [*instance name*] has an invalid value.

Explanation
A property is configured with an invalid value.

System action
PIP initialization could not complete, so the PIP was disabled.

Administrator response
Verify the PIP instance configuration.

FBTRBA213E

The property [*configuration property*] for instance [*instance name*] has an invalid integer value.

Explanation
The property must be configured to a valid integer value.

System action
PIP initialization could not complete, so the PIP was disabled.

Administrator response
Verify the PIP instance configuration.

FBTRBA214E

The policy information point could not be created or updated because the attribute [*attribute*] was not found.

Explanation
The requested action on the policy information point could not be completed because an attribute was not found.

System action
No action necessary.

Administrator response
Ensure that the attribute is valid and exists.

FBTRBA215E

The action failed because the policy information point type is associated with one or more policy information points. The policy information points are [*pips*].

Explanation
The action is not allowed when the policy information point type is referenced by another resource.

System action
No action necessary.

Administrator response
Remove references to the policy information point type and retry the action.

FBTRBA216E

The policy information point could not be created or updated because the policy information point type [*pipType*] was not found.

Explanation
The requested action on the policy information point could not be completed because a policy information point type was not found.

System action
No action necessary.

Administrator response
Ensure that the policy information point type is valid and exists.

FBTRBA217E

The XPath expression [*xpath*] for attribute [*attribute*] is invalid.

Explanation
The XML response from the REST service could not be parsed because an invalid XPath expression was specified.

System action
No attributes were returned.

Administrator response
Verify that the XPath expression is correct.

FBTRBA218E

The authentication mechanism property *authMechProperty* cannot be modified because it is a read-only property.

Explanation
Read-only authentication mechanism property cannot be modified.

System action
The modification operation is rejected.

Administrator response
No action necessary.

FBTRBA219E

The authentication mechanism could not be created or updated because the authentication mechanism type ID [*authMechTypeId*] was not found.

Explanation
The requested action on the authentication mechanism could not be completed because an authentication mechanism type ID was not found.

System action
No action necessary.

Administrator response
Ensure that the authentication mechanism type ID is valid and exists.

FBTRBA220E

The action failed because the authentication mechanism type is associated with one or more authentication mechanisms. The authentication mechanisms are [*authMechs*].

Explanation
The action is not allowed when the authentication mechanism type is referenced by another resource.

System action
No action necessary.

Administrator response
Remove references to the authentication mechanism type and retry the action.

FBTRBA221E

The authentication mechanism instance property *property* value *value* is not valid. Valid values are: *validValues*.

Explanation
The authentication mechanism instance property value is not valid.

System action
The modification operation is rejected.

Administrator response
No action necessary.

FBTRBA222E

The authentication mechanism instance property *property* data type *dataType* is not valid.

Explanation
The authentication mechanism instance property data type is not valid.

System action
The modification operation is rejected.

Administrator response
No action necessary.

FBTRBA223E

The authentication mechanism instance property *property* value *value* is not valid for the data type *dataType*.

Explanation
The authentication mechanism instance property value is not valid.

System action
The modification operation is rejected.

Administrator response
No action necessary.

FBTRBA224E

The action failed because the attribute is used in one or more policy information points. The policy information points are [*pipNames*]. Remove the attribute from the policy information points before you delete the attribute.

Explanation
The action is not allowed when the attribute is referenced by another resource.

System action
No action necessary.

Administrator response
Remove references to the attribute and retry the action.

FBTRBA225E

The authentication mechanism instance property *property* was not found.

Explanation
The authentication mechanism instance property being updated was not found for the specified authentication mechanism instance.

System action
The modification operation is rejected.

Administrator response
No action necessary.

FBTRBA226E

The file name [*fileName*] is not valid. A valid file name must contain only the character set A-Z, a-z, 0-9, underscore (_), period (.) and dash (-). It must not start with 0-9, underscore (_), period (.) or dash (-). It must end with a .jar extension.

Explanation
The file name that is used was not valid.

System action
No action is necessary.

Administrator response
Ensure that the file name is valid.

FBTRBA227E

The JavaScript that you submitted is not valid. The JavaScript validator reported a syntax error at line *line* and column *column* with the message: *message*.

Explanation
The JavaScript that you submitted is not valid. You can only submit valid JavaScript.

System action
The JavaScript is rejected.

Administrator response
Submit valid JavaScript.

FBTRBA228E

The data type [*dataType*] of property [*propertyKey*] in the extension [*extensionId*] is not supported. Supported data types are: [*dataTypes*].

Explanation
The property data type in the extension of the bundle is not supported.

System action
The uploading of the bundle file is rejected.

Administrator response
Ensure that the property data type in the extension is valid.

FBTRBA229E

The bundle file [*filename*] was not found.

Explanation
The requested bundle file does not exist.

System action
No action necessary.

Administrator response
Ensure that the resource and requested action are valid.

FBTRBA230E

The extension [*extensionId*] was not found.

Explanation
The extension was not found.

System action
The request is rejected.

Administrator response
Ensure that the extension exists.

FBTRBA231E

The required property [*propertyKey*] was not found.

Explanation
The required property was not found.

System action
The request is rejected.

Administrator response
Ensure that the request contains the required property.

FBTRBA232E

The value for property [*propertyKey*] is not valid. The data type must be [*dataType*].

Explanation
The passed in property value does not match the specific data type.

System action
The request is rejected.

Administrator response
Ensure that the property value meets the data type requirement.

FBTRBA233E

The value for JSON property [*value*] is null. Null values are not allowed.

Explanation
The JSON property value that was passed in is not allowed.

System action
The request is rejected.

Administrator response
Ensure that the JSON property value is not null.

FBTRBA234E

The value entered for the pagination query parameter [start] was either non-numeric or less than 0. The query parameter sent in the request for 'start' was [*start*].

Explanation
The query parameter value passed in the request was not valid.

System action
The request is rejected.

Administrator response
Ensure that the value is a valid integer.

FBTRBA235E

The value entered for the pagination query parameter [count] was either non-numeric or less than 0. The query parameter sent in the request for 'count' was [*count*].

Explanation
The query parameter value passed in the request was not valid.

System action
The request is rejected.

Administrator response
Ensure that the value is a valid integer.

FBTRBA236E

The extension ID [*extensionId*] for extension point [*extensionPoint*] exists.

Explanation
An extension with the same ID exists for the extension point.

System action
The uploading of the bundle file is rejected.

Administrator response
Specify a different value for the extension ID.

FBTRBA237E

Duplicate property [*propertyKey*] is found for extension [*extensionName*].

Explanation
A duplicate property is found for an extension.

System action
The uploading of the bundle file is rejected.

Administrator response
Remove the duplicate property.

FBTRBA238E

The property [*extensionId*] is not valid.

Explanation
The property is not valid.

System action
The request is rejected.

Administrator response
Ensure that the property is valid.

FBTRBA239E

The property [*configKey*] clashes with the reserved keys for the extension [*extensionId*] that extends [*extensionPoint*].

Explanation
The property clashes with the reserved keys for the extension that extends the particular extension point.

System action
The uploading of the bundle file is rejected.

Administrator response
Remove or rename the property.

FBTRBA240E

The authentication policy could not be created or updated because the authentication policy identifier *authPolicyUri* must start with the prefix urn:ibm:security:authentication:asf:.

Explanation
The requested action on the authentication policy could not be completed because the authentication policy identifier is not valid.

System action
No action necessary.

Administrator response
Ensure that the authentication policy identifier is valid and has the prefix urn:ibm:security:authentication:asf:.

FBTRBA241E

The JSON property [*property*] received an invalid type of [*type*]. The expected type was [*expectedType*].

Explanation
An invalid type was passed in for this property.

System action
There was a JSON validation failure.

Administrator response
Send the JSON payload with the expected type value.

FBTRBA242E

The additional JSON property [*property*] is not allowed. Send only known properties in the request.

Explanation
An invalid property was sent in the request.

System action
There was a JSON validation failure.

Administrator response
Send the JSON payload with known properties.

FBTRBA243E

The required JSON property [*property*] is missing from the request.

Explanation
A required property is missing from the request.

System action
There was a JSON validation failure.

Administrator response
Send the JSON payload with the required properties.

FBTRBA244E

The JSON property [*property*] requires the property [*requiredProperty*] to be included in the JSON. This property is missing from the request.

Explanation
A required property is missing from the request.

System action
There was a JSON validation failure.

Administrator response
Send the JSON payload with the required properties.

FBTRBA245E

The JSON property [*property*] was received with a value of [*value*]. The minimum value allowed is [*minimumValue*].

Explanation
The specified value was less than the allowable minimum value.

System action
There was a JSON validation failure.

Administrator response
Send the JSON payload with at least the minimum property value.

FBTRBA246E

The JSON property [*property*] was received with a value of [*value*]. The maximum value allowed is [*maximumValue*].

Explanation
The specified value exceeded the allowable maximum value.

System action
There was a JSON validation failure.

Administrator response
Send the JSON payload with the maximum property value or less.

FBTRBA247E

The JSON property [*property*] was received with a value of [*value*]. The minimum number of items allowed is [*minimumItems*].

Explanation
The minimum number of items was not received.

System action
There was a JSON validation failure.

Administrator response
Send the JSON payload with at least the minimum number of items.

FBTRBA248E

The JSON property [*property*] was received with a value of [*value*]. The maximum number of items allowed is [*maximumItems*].

Explanation
The maximum number of items was exceeded.

System action
There was a JSON validation failure.

Administrator response
Send the JSON payload with no more than the maximum number of items.

FBTRBA249E

The JSON property [*property*] has an invalid schema pattern of [*pattern*].

Explanation
A regular expression pattern was entered in the schema that is invalid.

System action
The schema developer needs to correct this.

Administrator response
Use valid regular expression patterns.

FBTRBA250E

The string for JSON property [*property*] with a value of [*value*] does not match the pattern of [*pattern*].

Explanation
A regular expression pattern was entered in the schema that is invalid.

System action
The schema developer needs to correct this.

Administrator response
Use valid regular expression patterns.

FBTRBA251E

The length of string property [*property*] is less than the allowed minimum length. The length received was [*length*]. The minimum allowed length is [*minimumLength*].

Explanation
The minimum required string length for this property was not met.

System action
There was a JSON validation failure.

Administrator response
Provide a string value for this property with at least the minimum length.

FBTRBA252E

The length of string property [*property*] is more than the allowed maximum length. The length received was [*length*]. The maximum allowed length is [*maximumLength*].

Explanation
The maximum required string length for this property was exceeded.

System action
There was a JSON validation failure.

Administrator response
Provide a string value for this property that is less than the maximum length.

FBTRBA253E

The property [*property*] contains a value with an unsupported value type of [*value*]. Supported values are [*expectedValues*].

Explanation
The value type entered is not supported.

System action
There was a JSON validation failure.

Administrator response
Provide a supported value type for this property.

FBTRBA254E

The string property [*property*] is not in the correct format. The correct format is [*format*].

Explanation
The value of the string property is not in the correct format.

System action
There was a JSON validation failure.

Administrator response
Provide the correct format for this string property.

FBTRBA255E

The number of decimal places in property [*property*] with a value of [*value*] is greater than the allowed maximum of [*maximum*].

Explanation
The maximum number of decimal places was exceeded.

System action
There was a JSON validation failure.

Administrator response
Provide a value that has less than the maximum amount of decimal places.

FBTRBA256E

The instance type of [*type*] specified for property [*value*] is not allowed.

Explanation
The specified instance type is not allowed.

System action
There was a JSON validation failure.

Administrator response
Provide an instance type that is allowed for the property.

FBTRBA257E

The URI for the property [*property*] does not start with [*value*].

Explanation
The property value specified does not start with the constraining URI.

System action
There was a JSON validation failure.

Administrator response
Provide a property value that starts with the required URI.

FBTRBA258E

The property array [*property*] can only contain unique items.

Explanation
The array contained items that were not all unique.

System action
There was a JSON validation failure.

Administrator response
Pass property array items that are unique.

FBTRBA259E

The value [*value*] specified for property [*property*] is not divisible by [*expectedNumber*].

Explanation
A value was entered that is not divisible by the assigned number.

System action
There was a JSON validation failure.

Administrator response
Pass a value that is divisible by the assigned number.

FBTRBA260E

The value [*value*] specified for property [*property*] exceeded the maximum allowed amount of [*maximumAllowed*].

Explanation
A value was entered that is greater than the maximum allowed value.

System action
There was a JSON validation failure.

Administrator response
Pass a value that is less than the maximum allowed value.

FBTRBA261E

The action failed because the authentication policy is used in one or more access control policies. The access control policies are [*policyNames*].

Explanation
The action is not allowed when the authentication policy is referenced by another resource.

System action
No action necessary.

Administrator response
Remove references to the authentication policy and retry the action.

FBTRBA262E

The consent to register device process failed. The user is not authenticated.

Explanation
The consent to register device process did not complete because the user is not authenticated.

System action
The request has been halted.

Administrator response
Ensure that the user authenticates prior to the consent to register device process.

FBTRBA263E

The value of [*value*] is not valid for key [*key*]. Valid values are one of [*validValues*].

Explanation
The value entered for the specified key was not one of the allowed values.

System action
There was a validation failure.

Administrator response
Pass one of the allowed values.

FBTRBA264E

The value of [*value*] entered is invalid for the datatype [*datatype*].

Explanation
The value entered for the specified datatype was invalid.

System action
There was a validation failure.

Administrator response
Pass a valid value for the specified datatype.

FBTRBA265E

An unknown data type of [*datatype*] was entered.

Explanation
The value entered for the specified datatype was not known.

System action
There was a validation failure.

Administrator response
Pass a known datatype into the request.

FBTRBA266E

An invalid date format of [*date*] was entered. Supported date formats are [*formats*].

Explanation
An unsupported date format was entered.

System action
There was a validation failure.

Administrator response
Pass a supported date format string.

FBTRBA267E

The attribute specified with the id [*id*] cannot be used within a risk profile. The attribute specified was of type [*type*]. The attribute needs to be at least 'risk': true or 'risk': true, 'policy': true to be valid.

Explanation
An attribute id that is not of type 'risk' or 'both' was specified.

System action
There was a validation failure.

Administrator response
Specify an attribute that is of type 'risk': true or 'risk': true, 'policy': true.

FBTRBA268E

The attribute with id [*id*] was entered more than once. Duplicate attributes are not allowed.

Explanation
The is a duplicate attribute id specified within the risk profile. Duplicates are not allowed.

System action
There was a validation failure.

Administrator response
Specify an attribute only once.

FBTRBA269E

The attribute matcher with id [*id*] is invalid. The id of the attribute matcher needs to be passed in as a numerical string.

Explanation
The attribute matcher identity is invalid.

System action
There was a validation failure.

Administrator response
Specify a valid attribute matcher.

FBTRBA270E

The attribute matcher with the id of [*matcherId*] was not found.

Explanation
An attribute matcher with the specified attribute matcher ID does not exist.

System action
No action necessary.

Administrator response
No action necessary.

FBTRBA271E

The attribute with id [*id*] is invalid. The id of the attribute needs to be passed in as a numerical string.

Explanation
The attribute identity is invalid.

System action
There was a validation failure.

Administrator response
Specify a valid attribute.

FBTRBA272E

The JavaScript Policy Information Point file cannot be empty.

Explanation
The uploaded JavaScript Policy Information Point file is invalid because it does contain any data.

System action
There was a validation failure.

Administrator response
Upload a valid JavaScript Policy Information Point file.

FBTRBA273E

The uploaded JavaScript Policy Information Point is missing the required function [*function name*].

Explanation
The uploaded JavaScript Policy Information Point file must contain a function named getAttributes and a function named hasAttribute

System action
There was a validation failure.

Administrator response
Upload a valid JavaScript Policy Information Point file.

FBTRBA274E

The uploaded file [*function name*] is invalid or empty.

Explanation
The uploaded file must be valid and non-empty.

System action
There was a validation failure.

Administrator response
Upload a valid file.

FBTRBA275E

The SQL query returned an unexpected error.

Explanation
An error was received while invoking the SQL query.

System action
Processing of the attribute was halted.

Administrator response
Verify that the database is functioning properly.

FBTRBA276E

The attribute finder for attribute [*attribute name*] returned no values.

Explanation
The SQL query did not return a value for the requested attribute.

System action
The attribute value was set to the empty string.

Administrator response
Verify that the database is functioning properly.

FBTRBA277E

The required property [*configuration property*] does not exist in the configuration.

Explanation
The configuration for a required property is missing.

System action
PIP initialization could not complete, so the PIP was disabled.

Administrator response
Configure the missing property.

FBTRBA279E

The property [*configuration property*] with value [*instance name*] is not a valid SQL query.

Explanation
A properly formatted SQL query must be specified for the database.

System action
PIP initialization could not complete, so the PIP was disabled.

Administrator response
Verify the database SQL query configuration.

FBTRBA280E

The property [*configuration property*] for instance [*instance name*] has an invalid value.

Explanation
A property is configured with an invalid value.

System action
PIP initialization could not complete, so the PIP was disabled.

Administrator response
Verify the PIP instance configuration.

FBTRBA281E

The attribute selector column [*column*] must be specified in the SQL query [*query*].

Explanation
An attribute selector is configured with an invalid value.

System action
No action necessary.

Administrator response
Modify the SQL query or specify a different attribute selector column name.

FBTRBA282E

No column selected in the SQL query [*query*].

Explanation
At least one column must be selected in the SQL query.

System action
No action necessary.

Administrator response
Correct the SQL query.

FBTRBA283E

The property key [*propertyKey*] is not valid. The property key must not end with [.obf].

Explanation
A property key that is not valid was used.

System action
The uploading of the bundle file is rejected.

Administrator response
Remove or rename the property key.

FBTRBA284E

The specified obligation URI is not valid. An obligation URI must not start with [urn:ibm:security:authentication:asf] and it must not be [*].

Explanation
An obligation URI that is not valid was used.

System action
The obligation creation is rejected.

Administrator response
Rename the obligation URI.

FBTRBA285E

At least one attribute selector must be specified.

Explanation
An attribute selector is required for the policy information point.

System action
No action necessary.

Administrator response
Specify an attribute selector.

FBTRBA286E

To publish multiple policy attachments you must specify the property [*propertyKey*] within the requests JSON payload. There must be at least one value and if more than one value, the values must be comma-separated.

Explanation
A JSON payload property or value was missing for this request.

System action
No action necessary.

Administrator response
Specify at least one policy attachment ID within the requests JSON payload.

FBTRBA287E

The specified policy attachments with the identifiers [*publishedAttachments*] have been published. However, the specified policy attachments with the identifiers [*dneAttachments*] do not exist.

Explanation
A JSON payload property or value was missing for this request.

System action
No action necessary.

Administrator response
Specify at least one policy attachment ID within the requests JSON payload.

FBTRBA288E

the specified policy attachments with the identifiers [*ids*] do not exist.

Explanation
A JSON payload property or value was missing for this request.

System action
No action necessary.

Administrator response
Specify at least one policy attachment ID within the requests JSON payload.

FBTRBA289E

The extension point [*extensionPoint*] is not supported.

Explanation
The bundle file contains an implementation of an extension point that is not supported.

System action
The uploading of the bundle file is rejected.

Administrator response
Remove the implementation of the unsupported extension point from the bundle file.

FBTRBA290E

The obligations specified within the policy with the URIs [*uris*] do not exist.

Explanation
The obligations with the uris specified within the XACML policy do not exist.

System action
Policy creation fail.

Administrator response
Create obligations with the uris specified within the XACML policy prior to trying to create this policy.

FBTRBA291E

The attributes specified within the policy with the uri, datatype and issuer combinations [*attrProps*] do not exist.

Explanation
The attributes with the specified uri, datatype and issuer within the XACML policy do not exist.

System action
Policy creation fail.

Administrator response
Create attributes with the uri, datatype and issuer combinations specified within the XACML policy prior to trying to create this policy.

FBTRBA292E

The filter property of [*prop*] cannot use the comparator [*comp*] because it is of type [*recType*]. Valid comparators for this property are [*supCompar*].

Explanation
The comparator for this property is not valid because of the data type of the property.

System action
There was a validation failure.

Administrator response
Specify a valid comparator for this data type.

FBTRBA293E

Unsupported java.sql.Types [*type*].

Explanation
The database data type passed in is unknown.

System action
There was a validation failure.

Administrator response
Specify a valid, known database data type.

FBTRBA295E

The authentication policies specified within the policy with the URIs [*uris*] do not exist.

Explanation
The authentication policies with the uris specified within the XACML policy do not exist.

System action
Policy creation fail.

Administrator response
Create authentication policies with the uris specified within the XACML policy prior to trying to create this policy.

FBTRBA296E

The attribute [*attribute name*] is not valid for the specified grant.

Explanation
The grant attributes that is specified is not part of the existing attributes.

System action
The request is rejected.

Administrator response
Remove the invalid attribute from the request.

FBTRBA297E

The attribute [*attribute name*] cannot be modified because it is a read-only attribute.

Explanation
A read-only attribute cannot be modified.

System action
The request is rejected.

Administrator response
Remove the read-only attribute from the request.

FBTRBA299E

The user knowledge questions could not be reset for user [*user*].

Explanation
The user knowledge questions could not be reset.

System action
The user knowledge questions were not reset.

Administrator response
No action necessary.

FBTRBA300E

The action failed because the obligation type [*obligationTypeName*] is associated with one or more obligations. The obligations are [*obligationNames*].

Explanation
The action is not allowed when the obligation type is referenced by another resource.

System action
The action is rejected.

Administrator response
Remove references to the obligation type and try again.

FBTRBA301E

The action failed because the authentication mechanism is used in one or more policies. The policies are [*policyNames*].

Explanation
The action is not allowed when the authentication mechanism is referenced by another resource.

System action
The action is rejected.

Administrator response
Remove references to the authentication mechanism and try again.

FBTRBA302E

You cannot create multiple instances of the authentication mechanism type [*typeName*]. An instance of this type exists.

Explanation
The authentication mechanism type does not allow multiple instances to be created.

System action
The action is rejected.

Administrator response
Specify another authentication mechanism type that allows multiple instances to be created.

FBTRBA303E

You cannot create multiple instances of the obligation type [*typeName*]. An instance of this type exists.

Explanation
The obligation type does not allow multiple instances to be created.

System action
The action is rejected.

Administrator response
Specify another obligation type that allows multiple instances to be created.

FBTRBA305E

The user knowledge questions could not be stored for user [*user*].

Explanation
The user knowledge questions could not be stored.

System action
The user knowledge questions were not stored.

Administrator response
No action necessary.

FBTRBA306E

The user management operation failed because the user is not authenticated.

Explanation
The user management process did not complete because the user is not authenticated.

System action
The request has been halted.

Administrator response
Ensure that the user authenticates prior to performing the user management operation.

FBTRBA307E

The user knowledge questions could not be retrieved for user [*user*].

Explanation
The user knowledge questions could not be retrieved.

System action
The user knowledge questions were not retrieved.

Administrator response
No action necessary.

FBTRBA308E

The user knowledge questions answer(s) submitted are not valid.

Explanation
The user knowledge questions could not be stored because the answer(s) provided by the user are not valid.

System action
The user knowledge questions were not stored.

Administrator response
Submit valid knowledge questions answers.

FBTRBA309E

The user knowledge questions answer(s) could not be updated because a question with unique identifier [*uniqueid*] was not found.

Explanation
The user knowledge questions could not be updated because the question unique identifier provided by the user was not found.

System action
The user knowledge questions were not updated.

Administrator response
Submit valid knowledge question unique identifier.

FBTRBA310E

The user knowledge questions answer(s) could not be stored because a duplicate question unique identifier [*uniqueid*] was included on the user questions.

Explanation
The user knowledge questions could not be stored because a duplicate question unique identifier was included on the user questions.

System action
The user knowledge questions were not stored.

Administrator response
Submit valid knowledge questions unique identifiers.

FBTRBA311E

The import policies file specified does not contain valid JSON.

Explanation
An error occurred while parsing the JSON files contents.

System action
No action taken.

Administrator response
Submit a valid policies JSON file.

FBTRBA312E

The query for object [*object*] returned no results. Ensure that the runtime and at least one reverse proxy server is configured.

Explanation
No reverse proxy servers were returned from the query.

System action
No action taken.

Administrator response
Make sure the runtime is configured and the reverse proxy is configured.

FBTRBA313E

The extension bundle file is not valid.

Explanation
The bundle file that is used is not valid.

System action
The importing of the bundle file is rejected.

Administrator response
Ensure that the extension bundle file is valid.

FBTRBA314E

The length of the attribute [*attributeName*] must be [*characterLength*] characters.

Explanation
The length of the attribute does not meet the length requirement.

System action
The request is rejected.

Administrator response
Ensure that the attribute meets the length requirement.

FBTRBA315E

The user knowledge questions answer(s) could not be stored because [*numAnswers*] answer(s) were provided while the authentication mechanism is configured to only allow [*maxNumAnswers*] answer(s) to be stored.

Explanation
The user knowledge questions could not be stored because the amount of user questions answer(s) provided exceeds the maximum amount allowed to be stored.

System action
The user knowledge questions were not stored.

Administrator response
Submit valid amount of knowledge questions.

FBTRBA316E

The user knowledge questions answer(s) could not be stored because the user defined question [*userDefinedQuestion*] was included on the request while the authentication mechanism is not configured to allow user defined questions to be stored.

Explanation
The user knowledge questions could not be stored because user defined questions are not allowed.

System action
The user knowledge questions were not stored.

Administrator response
Enable user defined questions on the authentication mechanism configuration.

FBTRBA317E

The user [*user*] does not exist in the database.

Explanation
An invalid username was specified.

System action
Nothing was deleted from the runtime database.

Administrator response
Verify the username.

FBTRBA318E

The services list is empty.

Explanation
The services list cannot be empty.Specify endpoints in the services list

System action
Federation/partner not created.

Administrator response
Verify that endpoints are specified in the services list.

FBTRBA319E

The services must be specified.

Explanation
The services must be specified .

System action
Federation/partner not created.

Administrator response
Verify that services is present in JSON.

FBTRBA320E

The sessionTimeout parameter cannot be negative.

Explanation
The sessionTimeout parameter cannot be negative.

System action
Federation/partner not created.

Administrator response
Verify that sessionTimeout parameter is non-negative.

FBTRBA321E

The artifactLifeTime parameter cannot be negative.

Explanation
The artifactLifeTime parameter cannot be negative.

System action
Federation/partner not created.

Administrator response
Verify that artifactLifeTime parameter is non-negative.

FBTRBA322E

The assertionValidBefore parameter cannot be negative.

Explanation
The assertionValidBefore parameter cannot be negative.

System action
Federation/partner not created.

Administrator response
Verify that assertionValidBefore parameter is non-negative.

FBTRBA323E

The assertionValidAfter parameter cannot be negative.

Explanation
The assertionValidAfter parameter cannot be negative.

System action
Federation/partner not created.

Administrator response
Verify that assertionValidAfter parameter is non-negative.

FBTRBA324E

The logoutRequestNotOnOrAfter parameter value cannot be negative.

Explanation
The logoutRequestNotOnOrAfter parameter value cannot be negative.

System action
Federation/partner not created.

Administrator response
Verify that logoutRequestNotOnOrAfter parameter value is non-negative.

FBTRBA325E

The binding parameter value cannot be empty.

Explanation
The binding parameter value cannot be empty.

System action
Federation/partner not created.

Administrator response
Verify binding parameter value is present.

FBTRBA326E

The binding type parameter should be present in JSON.

Explanation
The binding type parameter should be present in JSON.

System action
Federation/partner not created.

Administrator response
Verify binding type parameter is present in JSON.

FBTRBA327E

The services parameter should be present under services.

Explanation
The services parameter should be present in JSON .

System action
Federation/partner not created.

Administrator response
Verify services parameter is present in JSON.

FBTRBA329E

The username password authentication mechanism configuration is invalid.

Explanation
The username password authentication mechanism configuration encountered an error and could not continue.

System action
No action taken.

Administrator response
Modify the username password authentication mechanism configuration.

FBTRBA330E

The signing and encryption key label must be different.

Explanation
The signing and encryption key label must be different.

System action
The partner is not created.

Administrator response
Ensure that the signing and encryption key label are different.

FBTRBA331E

The action: Import Metadata failed because the metadata file or federation role is invalid.

Explanation
The metadata file import failed. This can occur if the file is not a valid import file or federation role is invalid.

System action
No action is necessary.

Administrator response
Examine the logs for the cause of the exception. Ensure that the file is a valid import file.

FBTRBA332E

The action: Export Metadata failed because the keystore or certificate is invalid/not exist.

Explanation
The metadata file export failed. This can occur if the keystore or certificate is invalid/not exist.

System action
No action is necessary.

Administrator response
Examine the logs for the cause of the exception. Ensure that the keystore or certificate is valid.

FBTRBA333E

Federation name must be specified.

Explanation
Federation name must be specified.

System action
Federation was not created.

Administrator response
Federation name must be specified.

FBTRBA334E

The policy id [*id*] is invalid.

Explanation
The policy id is invalid.

System action
There was a validation failure.

Administrator response
Specify a valid policy id.

FBTRBA335E

The URL provided is invalid.

Explanation
The URL provided is invalid.

System action
There was a validation failure.

Administrator response
Specify a valid URL.

FBTRBA336E

The parameter sessionNotOnOrAfter must be positive.

Explanation
The parameter sessionNotOnOrAfter must be positive.

System action
There was a validation failure.

Administrator response
Specify a positive value for sessionNotOnOrAfter parameter .

FBTRBA337E

The tenant type *tenant type* is not valid. Supported tenant types are *supported tenant types*.

Explanation
The tenant type is not valid.

System action
The request is rejected.

Administrator response
Specify a valid tenant type.

FBTRBA338E

One or more required properties are missing. Required properties for tenant type *tenant type* are *required properties*.

Explanation
One or more required properties for the specific tenant type are missing.

System action
The request is rejected.

Administrator response
Supply all the required properties for the specific tenant type.

FBTRBA339E

The User Registry Type Id provided is invalid.

Explanation
The User Registry Type Id provided is invalid.

System action
There was a validation failure.

Administrator response
Specify a valid User Registry Type Id.

FBTRBA340E

The User Registry Id provided is invalid.

Explanation
The User Registry Id provided is invalid.

System action
There was a validation failure.

Administrator response
Specify a valid User Registry Id.

FBTRBA341E

The Tenant Type Id provided is invalid.

Explanation
The Tenant Type Id provided is invalid.

System action
There was a validation failure.

Administrator response
Specify a valid Tenant Type Id.

FBTRBA343E

The connection failed. - *server error*

Explanation
The connection test to the server failed. The configuration supplied is not valid or the server is down.

System action
None

Administrator response
None

FBTRBA344E

The connection failed. - [No further information available].

Explanation
The connection test to the server failed. The configuration supplied is not valid or the server is down.

System action
None

Administrator response
None

FBTRBA345E

The federationID provided in URL is invalid.

Explanation
The federationID provided is invalid.

System action
None.

Administrator response
Verify federationId is valid.

FBTRBA346E

The partnerID provided is invalid.

Explanation
The partnerID provided is invalid.

System action
Federation/partner not created.

Administrator response
Verify partnerID is valid.

FBTRBA347E

The integer value is out of range.

Explanation
The integer value is out of range.

System action
Federation/partner not created.

Administrator response
Verify that integer is within the range.

FBTRBA348E

The msgLifeTime parameter cannot be negative.

Explanation
The msgLifeTime parameter cannot be negative.

System action
Federation/partner not created.

Administrator response
Verify that msgLifeTime parameter is non-negative.

FBTRBA349E

The action: Import Metadata failed because there is syntax error in the metatdata input.

Explanation
The metadata file import failed. This can occur if the file has syntax error.

System action
No action is necessary.

Administrator response
Examine the logs for the cause of the exception. Ensure that the file is a valid import file.

FBTRBA350E

The action: Import Metadata failed becacuse IDPSSODescriptor is not found in the metadatafile.

Explanation
The metadata file import failed. This can occur if there is no IDPSSODescriptor in the metadatafile.

System action
No action is necessary.

Administrator response
Examine the logs for the cause of the exception. Ensure that the file is a valid import file.

FBTRBA351E

The action: Import Metadata failed becacuse the metadata file either does not have KeyDescriptor of type signing or signing key value is empty.

Explanation
The metadata file import failed. This can occur if there is no IDPSSO-KeyDescriptor of type signing in the metadatafile.

System action
No action is necessary.

Administrator response
Examine the logs for the cause of the exception. Ensure that the file is a valid import file.

FBTRBA352E

The action: Import Metadata failed becacuse NameIDFormat tag with value as emailAddress is mandatory in the metadatafile.

Explanation
The metadata file import failed. This can occur if the file does not have NameIDFormat tag with emailAddress value.

System action
No action is necessary.

Administrator response
Examine the logs for the cause of the exception. Ensure that the file is a valid import file.

FBTRBA353E

The email server is not configured.

Explanation
An attempt was made to send an email and it failed because the email server is not configured.

System action
No action is necessary.

Administrator response
Configure the email server connection properties to fix the problem.

FBTRBA354E

An exception occurred when sending an email notification. Email delivery failed.

Explanation
An attempt was made to send an email and it failed.

System action
No action is necessary.

Administrator response
Check the logs for more information. Check the email server configuration properties for valid authentication settings.

FBTRBA355E

The email template with identifier [*identifier*] is missing the subject. Email delivery failed.

Explanation
An attempt was made to send an email and it failed because the email template is missing a subject field.

System action
No action is necessary.

Administrator response
Check the email server template file and fix the subject field.

FBTRBA356E

The email template page with identifier [*identifier*] is missing the the message content. Email delivery failed.

Explanation
An attempt was made to send an email and it failed because the email template is missing the message to send.

System action
No action is necessary.

Administrator response
Check the email server template file and fix the message content.

FBTRBA357E

An email template page with identifier [*identifier*] was not found. Email delivery failed.

Explanation
An attempt was made to send an email and it failed because the email template cannot be found.

System action
No action is necessary.

Administrator response
Check the email server template files and add the email template.

FBTRBA358E

User [*user*] was not found in the registry.

Explanation
An attempt was made to call the User Self Care REST API and the authenticated user was not found in the registry.

System action
No action is necessary.

Administrator response
Check that the user exists in the registry.

FBTRBA359E

Audit tracing is disabled. Enable Audit trace in Local Management Interface.

Explanation
Audit is disabled.

System action
Turn on Audit trace.

Administrator response
Turn on Audit trace.

FBTRBA360E

Remote audit server is not enabled. Local syslog is enabled.

Explanation
Remote audit server is not enabled.

System action
Turn on remote Audit server.

Administrator response
Turn on remote Audit server.

FBTRBA361E

The email address is not valid.

Explanation
Email address is not valid. Email delivery failed.

System action
None.

Administrator response
Specify a proper email address.

FBTRBA362E

The process cannot be completed. The request is missing or contains invalid required data.

Explanation
A REST API was called and the request sent is incomplete.

System action
None.

Administrator response
Check the REST API for proper usage. Check the trace logs for more information.

FBTRBA363E

An account with that email address already exists.

Explanation
A request to register a new user was made, but an account with the specified email address already exists.

System action
None.

Administrator response
None.

FBTRBA364E

Token validation failed.

Explanation
The token is missing or expired. The REST API cannot be completed.

System action
None.

Administrator response
None.

FBTRBA365E

Remote audit server credential (idaas.audit.serverHostname or idaas.audit.serverPort or idaas.audit.secToken) not found in advanced config in Local Management Interface.

Explanation
Remote audit server credentials not found.

System action
Provide remote audit server credentials.

Administrator response
Provide remote audit server credentials in advanced configuartion in Local Management Interface.

FBTRBA366E

Audit configuration error as UDP protocol is not supported .

Explanation
Audit configuration error as UDP protocol is not supported.

System action
Configure TLS protocol in audit configuration in Local Management Interface.

Administrator response
Configure TLS protocol in audit configuration in Local Management Interface.

FBTRBA367E

No user exists for the provided email *emailAddress*.

Explanation
A user was not found in the registry for the provided email address.

System action
None.

Administrator response
Use an email address for an existing user.

FBTRBA368E

An different account with that email address already exists.

Explanation
A request to modify a user's email address was made, but a different account with the specified email address already exists.

System action
None.

Administrator response
None.

FBTRBA369E

The identity source with ID *id* was not updated.

Explanation
An error occurred while the identity source was being updated.

System action
None.

Administrator response
Check the REST API for appropriate identity source specifications.

FBTRBA370E

EndDate cannot be before StartDate.

Explanation
EndDate cannot be before StartDate.

System action
None.

Administrator response
Use an email address for an existing user.

FBTRBA371E

StartDate more than 90 days. Audit report is stored only for last 90 days.

Explanation
StartDate more than 90 days. Audit report is stored only for last 90 days.

System action
None.

Administrator response
StartDate more than 90 days.

FBTRBA372E

Start date or End date could not be parsed.

Explanation
Start date or End date could not be parsed.

System action
None.

Administrator response
Start date or End date could not be parsed.

FBTRBA373E

This user does not have *action* permission for this resource.

Explanation
This user does not have permission for this resource.

System action
None.

Administrator response
For more information about the permissions that are granted for your user account, see your administrator.

FBTRBA374E

There are multiple users registered for the email address *email*.

Explanation
There are multiple accounts using the provided email address.

System action
None.

Administrator response
Multiple accounts are using this email address. Only one account can use this address. Contact your administrator to delete the additional accounts so that you can continue this operation.

FBTRBA375E

StartDate and/or EndDate is missing in the query param.

Explanation
StartDate and/or EndDate is missing in the query param.

System action
None.

Administrator response
StartDate and/or EndDate is missing in the query param.

FBTRBA376E

We are unable to renew your password at this time.

Explanation
An attempt was made to renew the password but the user id does not exist.

System action
None.

Administrator response
None.

FBTRBA377E

An unknown parameter *property* was specified.

Explanation
An invalid property is specified by the user.

System action
Command execution is halted.

Administrator response
Run the command with a correct properties as specified in the documentation.

FBTRBA378E

The property *property* must be provided when the property *property2* contains value *value*

Explanation
A required property is missing.

System action
Command execution is halted.

Administrator response
Run the command with a correct properties as specified in the documentation.

FBTRBA379E

The resource *resource* was not found.

Explanation
The specified resource could not be found.

System action
No action necessary.

Administrator response
Ensure that the resource exists.

FBTRBA380E

The property *property* is read only and cannot be changed.

Explanation
An invalid property is specified by the user.

System action
Command execution is halted.

Administrator response
Run the command with the correct properties as specified in the documentation.

FBTRBA381E

Cannot specify both *property1* and *property2*.

Explanation
It is only valid to provide one of the two properties.

System action
Command execution is halted.

Administrator response
Run the command with only one of the specified properties.

FBTRBA382E

The property *property* or property *property2* must be provided when the property *property3* has value *value*

Explanation
A required property is missing.

System action
Command execution is halted.

Administrator response
Run the command with one of the required properties as specified in the documentation.

FBTRBA383E

The property *key* should have value *property*.

Explanation
A required property is invalid.

System action
Command execution is halted.

Administrator response
Run the command with one of the required properties as specified in the documentation.

FBTRBA384E

The attribute matcher with id *id* is not valid for the attribute datatype *datatype*.

Explanation
The supplied attribute matcher cannot be used for attributes with the specified datatype.

System action
Command execution is halted.

Administrator response
Change the datatype of the attribute or the attribute matcher, or use the exact matcher.

FBTRBA385E

The device [*device*] was not found.

Explanation
An attempt was made to retreive a registered device for more information and the device was not found.

System action
No action is necessary.

Administrator response
None

FBTRBA386E

The attribute *name* is predefined and can not be used or issued by this PIP.

Explanation
The attribute referenced by the attribute matcher is predefined within the product. It can not issued by this custom PIP.

System action
Command execution is halted.

Administrator response
Change the attribute selector.

FBTRBA387E

An error occured while validating the specified trust store *name*.

Explanation
This is an internal error

System action
Command execution is halted.

Administrator response
Review system logs.

FBTRBA388E

The specified key store [*name*] does not exist.

Explanation
The trust specified in the request is not valid or does not exist on the appliance

System action
Command execution is halted.

Administrator response
Check the SSL settings on the appliance or change the trust store in the request.

FBTRBA389E

The property scope must contain value openid

Explanation
A required property is invalid.

System action
Command execution is halted.

Administrator response
Run the command with the required value as specified in the documentation.

FBTRBA390E

The property *key* is not valid when the property *property* has value *value*.

Explanation
A provided property is invalid.

System action
Command execution is halted.

Administrator response
Run the command without the property.

FBTRBA391E

The property *key* has a maximum length of *key*.

Explanation
A provided property is invalid.

System action
Command execution is halted.

Administrator response
Run the command with a shorter value.

FBTRBA392E

The value associated with the JSON field name *property* is read only and cannot be changed.

Explanation
The JSON property value cannot be changed.

System action
The request is rejected.

Administrator response
Ensure that the JSON property value does not differ from the existing value.

FBTRBA393E

The creation of this resource requires the *field name* field to have an *value type* value present.

Explanation
There was a required value missing in one of the fields. Refer to the exception for which fields and types are missing.

System action
Add the required input to payload.

Administrator response
Add a value of the correct type to the request payload.

FBTRBA394E

The uri value not assigned.

Explanation
There was a required value missing in one of the fields. Refer to the exception for which fields and types are missing.

System action
Add the required input to payload.

Administrator response
Add a value of the correct type to the request payload.

FBTRBA395E

Invalid uri value. Uri must begin with http or https.

Explanation
The required value is invalid. Refer to the exception for which fields and types are missing.

System action
Add the required input to payload.

Administrator response
Add a value of the correct type to the request payload.

FBTRBA396E

The authType value not assigned.

Explanation
The required value is invalid. Refer to the exception for which fields and types are missing.

System action
Add the required input to payload.

Administrator response
Add a value of the correct type to the request payload.

FBTRBA397E

The authentication type not supported. Supported types are NONE, BASIC or CERTIFICATE.

Explanation
The authType value is invalid. Refer to the exception for which fields and types are missing.

System action
Add the required input to payload.

Administrator response
Add a value of the correct type to the request payload.

FBTRBA398E

The username value for Basic Authentication not assigned.

Explanation
The required value is invalid. Refer to the exception for which fields and types are missing.

System action
Add the required input to payload.

Administrator response
Add a value of the correct type to the request payload.

FBTRBA399E

The password value for Basic Authentication not assigned.

Explanation
The required value is invalid. Refer to the exception for which fields and types are missing.

System action
Add the required input to payload.

Administrator response
Add a value of the correct type to the request payload.

FBTRBA400E

The client keystore value for Certificate Authentication not assigned.

Explanation
The required value is invalid. Refer to the exception for which fields and types are missing.

System action
Add the required input to payload.

Administrator response
Add a value of the correct type to the request payload.

FBTRBA401E

The client alias value for Certificate Authentication not assigned.

Explanation
The required value is invalid. Refer to the exception for which fields and types are missing.

System action
Add the required input to payload.

Administrator response
Add a value of the correct type to the request payload.

FBTRBA402E

The message format value not supported. Supported types are XML or WSTRUST.

Explanation
The required value is invalid. Refer to the exception for which fields and types are missing.

System action
Add the required input to payload.

Administrator response
Add a value of the correct type to the request payload.

FBTRBA403E

The AppliesTo value required for WS-Trust message.

Explanation
The required value is invalid. Refer to the exception for which fields and types are missing.

System action
Add the required input to payload.

Administrator response
Add a value of the correct type to the request payload.

FBTRBA404E

The export operation is not supported by this protocol.

Explanation
A request to export the configuration data has been made against a protocol which does not provide this support.

System action
Ensure that you only make this request against protocols which do support the export operation.

Administrator response
Ensure that the correct federation has been selected.

FBTRBA405E

The combination of username, federation_id, and type already exists with ID: *id*. Update the aliases using this ID instead.

Explanation
When attempting to create a new alias it was found that the username, federation_id, and type combination had already been configured and assigned an ID. This ID should be used instead.

System action
The request is rejected.

Administrator response
Update the aliases with the given ID instead of attemping to create a new alias association.

FBTRBA406E

The alias ID provided does not exist.

Explanation
The provided alias ID could not be found when trying to process the request.

System action
The request is rejected.

Administrator response
Verify that the provided alias ID is correct.

FBTRBA407E

The values for username, federation_id, and type are read-only. Create a new alias association instead.

Explanation
When attempting to update an alias, new values were provided for fields that are read-only. A new alias association should be configured instead.

System action
The request is rejected.

Administrator response
Create a new alias association with the given values instead of attempting to update read-only values.

FBTRBA408E

The provided attribute id is not valid [id=*attrId*]

Explanation
The provided id is not valid. Accepts integer only.

System action
Ensure source id is integer only

Administrator response
Ensure source id is integer only.

FBTRBA409E

Cannot find attribute with given source id [id=*attrId*]

Explanation
The attribute source cannot be found using the provided id.

System action
Ensure attribute source has been defined.

Administrator response
Ensure attribute source has been defined.

FBTRBA410E

The federation name [*federationName*] can contain only the character set A-Z, a-z, 0-9, underscore (_) and hyphen (-). Specify a different name using only the valid characters.

Explanation
The federation name that is used was not valid.

System action
No action is necessary.

Administrator response
Ensure that the federation name is valid.

FBTRBA411E

The JSON property [*property*] value, [*value*], cannot be changed.

Explanation
A different value was passed in for this property.

System action
There was a JSON validation failure.

Administrator response
Send the JSON payload with the expected value.

FBTRBA412E

The PIP update request included an attempt to change the current PIP type from [*property*] to [*value*]. This modification is not allowed.

Explanation
The type of an existing PIP instance cannot be changed.

System action
There was validation failure.

Administrator response
Correct the request and resend.

FBTRBA413E

The protocol, *protocolName*, is not supported. The supported protocols are *supportedProtocols*.

Explanation
The specified protocol is invalid.

System action
The JSON validation failed.

Administrator response
Provide a valid protocol name.

FBTRBA414E

[*value*] is not a valid [*property*].

Explanation
An invalid value was passed in for this property.

System action
There was a JSON validation failure.

Administrator response
Send the JSON payload with the valid property value.

FBTRBA415E

The role, *roleName*, is not supported. The supported roles for *protocolName* protocol are *supportedRoles*.

Explanation
The specified role is invalid.

System action
The JSON validation failed.

Administrator response
Provide a valid role name.

FBTRBA416E

The aliases array must not contain duplicates. A duplicate alias was found: *alias*.

Explanation
When attempting to add aliases it was found that a duplicate alias exists in the array. Remove the duplicate and attempt the request again.

System action
The request is rejected.

Administrator response
Remove duplicates from the aliases array.

FBTRBA417E

A chain mapping with the specified RequestType, AppliesTo, Issuer and TokenType values already exists.

Explanation
A chain mapping with the specified RequestType, AppliesTo, Issuer and TokenType values already exists. Remove the existing mapping or choose a different combination of RequestType, AppliesTo, Issuer and TokenType values.

System action
No action taken

Administrator response
Determine if the new chain mapping is different from the one that already exists. Resolve the error by either removing the current mapping or using the current mapping.

FBTRBA418E

An invalid value caused a JSON validation failure.

Explanation
An invalid value was passed in for this JSON.

System action
The JSON validation failed and the action was not completed.

Administrator response
Update the JSON payload with a valid value.

FBTRBA419E

An invalid value caused a JSON formatting failure.

Explanation
An invalid value was passed in for this JSON.

System action
The JSON formatting failed and the action was not completed.

Administrator response
Update the JSON payload with a valid value.

FBTRBA420E

The create failed because the domain value was not supplied.

Explanation
During the create operation, the domain value was not provided.

System action
See the exception in the logs for the cause.

Administrator response
Ensure that the domain is provided.

FBTRBA421E

The action *action* failed because the resource with the ID [*id*] is read-only for a resource of type: [*type*].

Explanation
The requested action on the specified resource could not be completed because the resource with the ID is read-only.

System action
The operation failed.

Administrator response
Create a new resource with the given values. Do not attempt to update the read-only resource.

FBTRBA422E

The action *action* failed because the value for sign in or local identity callbacks was empty.

Explanation
The creation or update of the resource failed because a required value within the request was not provided.

System action
The JSON validation failed.

Administrator response
Specify the required value for the resource.

FBTRBA423E

The action *action* failed because the value [*constraintValue*] for [*constraintName*] is not valid for resource with the ID [*id*].

Explanation
The requested action on the specified resource was not completed because an invalid value was provided for a property of the resource.

System action
The JSON validation failed.

Administrator response
Specify a valid value for the property to update the resource.

FBTRBA424E

The action *action* failed because the point of contact profile with the ID [*id*] is currently used by the system and cannot be deleted.

Explanation
The operation failed because you cannot delete a point of contact profile that is being used by the system.

System action
The operation failed.

Administrator response
Set another point of contact profile as the current profile. Then, delete this resource.

FBTRBA425E

The action *action* failed because the point of contact profile name [*federationName*] can contain only the character set A-Z, a-z, 0-9, underscore (_), space( ), and hyphen (-). Specify a different name using only the valid characters.

Explanation
The point of contact profile name used was not valid.

System action
The operation failed.

Administrator response
Ensure that the point of contact profile name is valid.

FBTRBA426E

The action *action* failed because it requires the *field name* field to have an *value type* value present.

Explanation
There was a required value missing in one of the fields. Refer to the exception for which fields and types are missing.

System action
The operation failed.

Administrator response
Add a value of the correct type to the request payload.

FBTRBA427E

The action *action* failed because the index value of *callback type* is not valid.

Explanation
The index value of the point of contact callback is not valid.

System action
The operation failed.

Administrator response
Ensure the index value of the point of contact callback is valid.

FBTRBA428E

The action *action* failed because more than one callback of type *callback type* are provided.

Explanation
More than one callback is provided for the callback type.

System action
The operation failed.

Administrator response
Ensure only one callback is provided for the callback type.

FBTRBA429E

The configuration of MMFA settings failed.

Explanation
During the MMFA configuration operation, a database exception was encountered.

System action
Ensure that the database is running correctly.

Administrator response
See the exception in the logs for the cause.

FBTRBA430E

The unconfiguration of MMFA settings failed.

Explanation
During the MMFA unconfiguration operation, a database exception was encountered.

System action
Ensure that the database is running correctly.

Administrator response
See the exception in the logs for the cause.

FBTRBA432E

The list of users who have stored knowledge questions could not be retrieved.

Explanation
The users who have stored knowledge questions could not be listed.

System action
See the exception in the logs for the cause.

Administrator response
No action necessary.

FBTRBA433E

Provider push notification service is not supported for *platform*.

Explanation
The specified push notification service is not supported for the given platform.

System action
See the exception in the logs for the cause.

Administrator response
No action necessary.

FBTRBA434E

The certificate *label* was not found in *store*.

Explanation
The certificate was not found in the database, ensure the certificate has been imported successfully.

System action
See the exception in the logs for the cause.

Administrator response
No action necessary.

FBTRBA435E

The action failed because the STS template is used in one or more STS chains. The STS chains are [*chainNames*].

Explanation
The action is not allowed when the STS template is referenced by another resource.

System action
No action necessary.

Administrator response
Remove references to the STS template and retry the action.

FBTRBA436E

The value for [*propertyName*] does not conform to naming rules.

Explanation
The string does not conform to naming rules. Ensure that the string contains no non-standard substrings or characters.

System action
No action necessary.

Administrator response
Use other value that conforms to naming rules, using only standard substrings and characters.

FBTRBA437E

An invalid number, *number*, of entries were defined in *propertyName*. A single entry must be defined.

Explanation
Multipl

System action
No action necessary.

Administrator response
No action necessary.

FBTRBA438E

The provided key identifier is invalid because the required JSON property [*property*] is missing from the request.

Explanation
A required property of a key identifier is missing from the request.

System action
There was a JSON validation failure.

Administrator response
Send the JSON payload with the required properties.

FBTRBA439E

A policy attachment with the server [*server*] and resource [*resource*] already exists.

Explanation
The creation or update of the policy attachment failed because a value within your request, that is required to be unique, already exists.

System action
See the exception in the logs for more details.

Administrator response
Specify a different value for the server or resource constraint.

FBTRBA440E

Unexpected error occured while connecting IBM Security Verify Access to IBM Security Verify.

Explanation
The connect operation should typically succeed. Unexpected error probably happens due to incorrect SAML 2.0 metadata provided by IBM Security Verify. Please see the logs to find the cause of the problem, and contact IBM support.

System action
The connect operation was aborted.

Administrator response
See the logs for more information, and contact IBM support.

FBTRBA441E

Unable to successfully complete connecting IBM Security Verify Access to IBM Security Verify.

Explanation
To successfully connect IBM Security Verify Access to IBM Security Verify, you must not abort the flow.

System action
The connect operation was aborted.

Administrator response
None.

FBTRBA442E

The Issuer Identifier [*value*] is not valid. An Issuer Identifier must be a URL with the protocol 'https://' and cannot contain any trailing query or fragment parts.

Explanation
The specified value is not valid.

System action
The requested action was not performed.

Administrator response
Ensure the requested value is valid.

FBTRBA443E

Invalid uri value for parameter [*parameter*]. Uri must begin with 'https://'.

Explanation
The required value is invalid. Refer to the exception for which fields and types are missing.

System action
Add the required input to payload.

Administrator response
Add a value of the correct type to the request payload.

FBTRBA444E

The JSON property [*property*] contains duplicate values.

Explanation
A property contains incorrectly duplicated values.

System action
There was a JSON validation failure.

Administrator response
Send the JSON payload without duplicates.

FBTRBA445E

The issuerUri value is required for the WS-Trust message format.

Explanation
The required value is invalid. Refer to the exception for which fields and types are missing.

System action
Add the required input to payload.

Administrator response
Add a value of the correct type to the request payload.

FBTRBA446E

The federation already has a partner with the specified realm and endpoint.

Explanation
The specified partner is invalid. All WS-Federation partners must have a unique realm and endpoint combination.

System action
Ensure that the realm and endpoint combination is unique for the partners of the federation.

Administrator response
Ensure that the realm and endpoint combination is unique for the partners of the federation.

FBTRBA447E

The federation already has a partner with the specified name.

Explanation
The specified partner is invalid. All partners must have a unique name.

System action
Ensure that the name is unique for the partners of the federation.

Administrator response
Ensure that the name is unique for the partners of the federation.

FBTRBA448E

The federation already has a partner with the specified realm.

Explanation
The specified partner is invalid. All WS-Federation partners must have a unique realm.

System action
Ensure that the realm is unique for the partners of the federation.

Administrator response
Ensure that the realm is unique for the partners of the federation.

FBTRBA449E

The federation already has a partner with the specified endpoint.

Explanation
The specified partner is invalid. All WS-Federation partners must have a unique endpoint.

System action
Ensure that the endpoint is unique for the partners of the federation.

Administrator response
Ensure that the endpoint is unique for the partners of the federation.

FBTRBA450E

The type of this access policy is not valid.

Explanation
The valid types for an access policy are: JavaScript, Simple, or XACML.

System action
The type of this access policy is not valid.

Administrator response
Submit a valid access policy.

FBTRBA451E

The JavaScript access policy that you submitted is not valid. The JavaScript validator reported a syntax error at line *line* and column *column* with the message: *message*.

Explanation
The JavaScript access policy that you submitted is not valid. You can only submit a valid JavaScript access policy.

System action
The JavaScript access policy is rejected.

Administrator response
Submit a valid JavaScript access policy.

FBTRBA452E

The category of this access policy is not valid.

Explanation
The category of this access policy is not valid.

System action
The category of this access policy is not valid.

Administrator response
Submit a valid access policy.

FBTRBA453E

Access policy with ID [*line*] does not exist.

Explanation
Access policy does not exist.

System action
The operation was aborted.

Administrator response
Submit a valid access policy.

FBTRBA454E

The property, [*property* is not supported in a Docker environment.

Explanation
A field was specified in the update operation which is not supported in a Docker environment.

System action
See the exception in the logs for the cause.

Administrator response
Verify that the field was not updated.

FBTREC001E

Internal Error. Contact the System Administrator.

Explanation
An internal error occurred.

System action
The end-user license agreement application encountered an error, process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTREC101E

There was an error contacting *ServiceLocation*.

Explanation
The service could not be contacted, or didn't provide a response body.

System action
The mechanism encountered an error, process has been halted.

Administrator response
Check the logs and the connection to the service.

FBTREC102E

There was an error parsing the response from the serivce.

Explanation
The service didn't provide a valid response body.

System action
The mechanism encountered an error, process has been halted.

Administrator response
Check the logs and the connection to the service.

FBTREC103E

The captcha provided was not valid.

Explanation
The request didn't contain a valid captcha.

System action
The mechanism did not contain a valid caputre in the request, peform a captcha again to proceed.

Administrator response

FBTREC104E

The mechanism property *property* is invalid.

Explanation
The mechanism configuration isn't valid.

System action
The mechanism is not properly configured, process has been halted.

Administrator response
Check the value of the incorrecly set property.

Chapter 6. Database messages

These messages are provided by the database component.

FBTFDB001E

Creation of database connection failed. Check the database configuration and network connectivity to the database server.

Explanation
The database connection could not be created.

System action
Command execution is halted.

Administrator response
Ensure that the database is configured correctly. Also check that the network connectivity to the database server is available.

FBTFDB002E

A database error occurred.

Explanation
An unrecoverable database error occurred.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTFDB003E

A file database error has ocurred.

Explanation
An unrecoverable file database error occurred.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTFDB004E

The database file does not exist.

Explanation
An unrecoverable database error occurred.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTFDB005E

Unable to reach Database.

Explanation
The database cannot be reached

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTFDB006E

Unable to get Data Access Object.

Explanation
An instance of the Data Access Object cannot be retrieved

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTFDB007E

Unable to retrieve transaction.

Explanation
A Transaction object cannot be retrieved from the Data Access Object

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTFDB008E

An invalid SQL statement was executed.

Explanation
The result from a SQL statement showed invalid execution.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTFDB009E

An invalid cleanup interval of *VALUE_0* was defined.

Explanation
The clean up interval is invalid, it must be a valid integer above 60000.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTFDB010E

The datasource *VALUE_0*, could not be retrieved.

Explanation
The JNDI lookup to get a datasource failed.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTFDB011E

An error occured during deserialization as part of a database operation.

Explanation
The deserialization failed for a stored data object.

System action
Command execution is halted.

Administrator response
Check the server logs for more details to trace the cause of the error.

FBTFDB012E

An invalid configuration parameter was specified for either the retry limit, retry delay or default TTL of the distributed map.

Explanation

One or more of the following parameters values is invalid; retryLimit, retryDelay, or defaultTTL.

System action

Command execution is halted.

Administrator response

Check the server logs for more details to trace the cause of the error.

Chapter 7. End-user license agreement messages

These messages are provided by the end-user license agreement component.

FBTELA000E

Internal Error. Contact the System Administrator.

Explanation
An internal error occurred.

System action
The end-user license agreement application encountered an error, process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTELA001E

Internal Error. Contact the System Administrator.

Explanation
An internal error occurred.

System action
The InfoMap mechanism encountered an error, process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTELA100E

The license agreement was declined. Processing cannot continue.

Explanation
The user must accept the license agreement to continue.

System action
The end-user license agreement application encountered an error, process has been halted.

Administrator response
None.

Chapter 8. HTTP redirect messages

These messages are provided by the HTTP redirect component.

FBTHRD000E

Internal Error. Contact the System Administrator.

Explanation
An internal error occurred.

System action
The application encountered an error. The process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTHRD100E

The configuration properties for the HTTP Redirect authentication mechanism is missing or not valid.

Explanation
The HTTP Redirect authentication mechanism requires configuration to process a redirect to an external authentication application.

System action
The authentication process encountered an error. The process has been halted.

Administrator response
Check the configuration properties for the HTTP Redirect authentication mechanism.

FBTHRD101E

The external authentication application did not return a successful authentication result. The process has been halted.

Explanation
The external authentication application must return a credential attribute that matches the configuration to flag a successful authentication result.

System action
The authentication process encountered an error. The process has been halted.

Administrator response
Check the configuration properties for the HTTP Redirect authentication mechanism.

Chapter 9. IDasS admin messages

These messages are provided by the IDasS admin component.

FBTIDA001E

The user entry was not found.

Explanation
No SCIM entry exists with that user identifier.

System action
The service did not return a value.

Administrator response
Validate the input parameters, then try the operation again.

FBTIDA002E

The configured SCIM service is not responding

Explanation
The SCIM server does not respond properly to requests.

System action
The service did not return a value.

Administrator response
Verify the SCIM service is available, then try the operation again.

FBTIDA003E

Unable to read the configuration because of an internal server error.

Explanation
The system is unable to fulfill the request because of an internal server error.

System action
The request is stopped.

Administrator response
Ensure that the server configuration is valid and try again.

FBTIDA004E

You must enter the minimum number of characters required.

Explanation
You must enter the minimum number of characters required.

System action
The request is stopped.

Administrator response
Ensure that the password is valid and try again.

FBTIDA005E

You must not use the username when creating a password.

Explanation
You must not use the username when creating a password.

System action
The request is stopped.

Administrator response
Ensure that the password is valid and try again.

FBTIDA006E

You must enter the minimum number of numeric and special characters required.

Explanation
You must enter the minimum number of numeric and special characters required.

System action
The request is stopped.

Administrator response
Ensure that the password is valid and try again.

FBTIDA007E

Your password has expired and must be changed.

Explanation
Your password has expired and must be changed.

System action
The request is stopped.

Administrator response
Ensure that the password is valid and try again.

FBTIDA008E

Your password expires in *days* days. Consider changing your password.

Explanation
Your password will expire soon. Consider changing your password.

System action
The request is stopped.

Administrator response
Ensure that the password is valid and try again.

FBTIDA009E

You have reached the maximum number of attempts to use an expired password to change your password.

Explanation
You have reached the maximum number of attempts to use an expired password to change your password.

System action
The request is stopped.

Administrator response
Ensure that the password is valid and try again.

FBTIDA010E

You have reached the maximum number of failed password attempts.Your account is locked.

Explanation
You have reached the maximum number of failed password attempts.Your account is locked.

System action
The request is stopped.

Administrator response
Ensure that the password is valid and try again.

FBTIDA011E

Password has been used before. You must use a different password.

Explanation
Password has been used before. You must use a different password.

System action
The request is stopped.

Administrator response
Ensure that the password is valid and try again.

FBTIDA012E

Too many similar characters from a previous password used. Use a different set of characters.

Explanation
Too many similar characters from a previous password used. Use a different set of characters.

System action
The request is stopped.

Administrator response
Ensure that the password is valid and try again.

FBTIDA013E

The request does not contain a syntactically correct JSON.

Explanation
The request must contain a syntactically correct JSON before it can be processed.

System action
The request is rejected.

Administrator response
None.

FBTIDA014E

Tenant type *id* does not exist.

Explanation
Tenant type with the specified ID does not exist.

System action
The request is rejected.

Administrator response
None.

FBTIDA015E

Tenant page *id* does not exist.

Explanation
Tenant page with the specified ID does not exist.

System action
The request is rejected.

Administrator response
None.

FBTIDA016E

The SCIM service is not properly configured

Explanation
The SCIM configuration has either missing or incorrect parameters.

System action
Verify SCIM configuration parameters.

Administrator response
None.

FBTIDA017E

The configuration is not completed due to an internal REST API error.

Explanation
The internal REST API call did not return a valid response.

System action
The request is canceled.

Administrator response
Try again later. If the problem persists, contact your system administrator.

FBTIDA018E

Tenant with identifier [*id*] does not exist.

Explanation
Tenant with the specified identifier does not exist.

System action
The request is rejected.

Administrator response
None.

FBTIDA019E

Tenant with identifier [*id*] already exist. Please use a different identifier.

Explanation
Tenant with the specified identifier already exist.

System action
The request is rejected.

Administrator response
None.

FBTIDA020E

The tenant identifier [*id*] is not valid. Ensure that it is not empty, and contains only characters from the following set [*characters*].

Explanation
Tenant identifier must only contain allowed characters.

System action
The request is rejected.

Administrator response
None.

FBTIDA021E

The tenant type [*type*] is not valid.

Explanation
Tenant type does not exist.

System action
The request is rejected.

Administrator response
None.

FBTIDA022E

The tenant friendly name [*id*] is not valid. Ensure that it is not empty, and contains only characters from the following set [*characters*].

Explanation
Tenant friendly name must only contain allowed characters.

System action
The request is rejected.

Administrator response
None.

FBTIDA023E

The credential type [*type*] is not valid.

Explanation
The credential type is not valid.

System action
The request is rejected.

Administrator response
None.

FBTIDA024E

The credential [*credential*] is not valid.

Explanation
The old credential is not valid.

System action
The request is rejected.

Administrator response
None.

FBTIDA025E

The old credential type [*type*] is not valid.

Explanation
The old credential type is not valid.

System action
The request is rejected.

Administrator response
None.

FBTIDA026E

The old credential [*credential*] is not valid.

Explanation
The old credential is not valid.

System action
The request is rejected.

Administrator response
None.

FBTIDA027E

The new credential type [*type*] is not valid.

Explanation
The new credential type is not valid.

System action
The request is rejected.

Administrator response
None.

FBTIDA028E

The new credential [*credential*] is not valid.

Explanation
The new credential is not valid.

System action
The request is rejected.

Administrator response
None.

FBTIDA029E

Unable to parse the input file.

Explanation
The bulk upload parse resulted in no records. File is invalid.

System action
None

Administrator response
Upload a proper CSV file.

FBTIDA030E

Incorrect record. The input values do not match the headers.

Explanation
The bulk upload parse resulted in an invalid record. The values did not match the headers.

System action
None

Administrator response
Check the record values and ensure that they match the headers.

FBTIDA031E

An upload request cannot be performed while another request is in progress.

Explanation
The system can perform only one bulk upload operation at a time.

System action
The new upload operation request was ignored.

Administrator response
Try the new upload operation again after the original upload operation is complete.

FBTIDA034E

The required input fields are missing for the record.

Explanation
The input records have required fields.

System action
None

Administrator response
Add all required fields and try again.

FBTIDA035E

Internal error. Contact the System Administrator.

Explanation
An internal error occurred.

System action
The application encountered an error. The process is halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTIDA036E

The file size exceeds the limit of [*limit*]MB.

Explanation
The input file size is exceeding limit.

System action
Reduce the size of input file.

Administrator response
Reduce the size of input file and try again.

FBTIDA037E

A required property is missing: [*property*]

Explanation
The posted JSON payload does not contain all required properties.

System action
Provide the missing property.

Administrator response

Provide the missing property.

Chapter 10. Key encryption and signature service messages

These messages are provided by the key encryption and signature service component.

FBTKES001E

The global configuration properties file is not in the classpath of the server.

Explanation
The global configuration properties file could not be found in the server's classpath. The file is typically created at installation time for the installer and is required for the server to successfully start.

System action
The request is halted.

Administrator response
Ensure that the system was installed correctly, locate the global configuration properties file, and ensure that the file is located in the server's classpath.

FBTKES002E

No keystore or keystore password was provided.

Explanation
A keystore or keystore password or both must be provided for the server to start.

System action
The request is halted.

Administrator response
Ensure that the keystore has the correct file permissions for the server to read and write.

FBTKES003E

The password could not be unobfuscated.

Explanation
The obfuscated password could not successfully be unobfuscated.

System action
The request is halted.

Administrator response
Check that the Java that supports the A.E.S. 128-cipher algorithm is being used.

FBTKES005E

A problem was encountered while creating the keystore at location: *filename*.

Explanation
Because the keystore at the given location did not exist, the server attempted to create a new keystore but failed.

System action
The keystore was not created.

Administrator response
Ensure that the directory path up to the given file exists and that the correct read and write file permissions are set. Check the cause exception to get more specific details about what caused the problem.

FBTKES006E

The key type for the given alias *alias* is an unknown key.

Explanation
An attempt was made to use a key that has an unknown type.

System action
No action taken.

Administrator response
Ensure that the key for the given alias is a supported key type.

FBTKES007E

A key was not found with the given alias (*alias*).

Explanation
The server could not find a key with the provided alias.

System action
No action taken.

Administrator response
Ensure that you have the correct keystore configured.

FBTKES008E

The required input was not given.

Explanation
The required input was not given to process the request.

System action
The request is halted.

Administrator response
Ensure that the correct input is given.

FBTKES009E

The document owner was not given. The signature template could not be generated.

Explanation
For the signature template to generate correctly, the document owner must be provided.

System action
The request is halted.

Administrator response
Ensure that the caller provides the correct document owner.

FBTKES010E

A reference list of elements to be signed was not given. The signature template cannot be generated without a reference list.

Explanation
For a signature template to be generated, a reference list must be provided.

System action
The request is halted.

Administrator response
Ensure that the caller provides the correct reference list of elements to be referenced in the generated signature template.

FBTKES011E

A context was not provided by caller.

Explanation
The caller did not provide a context.

System action
The request is halted.

Administrator response
Ensure that a context is provided.

FBTKES012E

A key alias was not provided by the caller.

Explanation
The caller did not provide a key alias.

System action
The request is halted.

Administrator response
Ensure that a key alias is provided.

FBTKES013E

No data was provided to be signed.

Explanation
The caller did not provide any data to be signed.

System action
The request is halted.

Administrator response
Ensure that there is data provided.

FBTKES014E

A certificate was not found with the given alias (*alias*).

Explanation
The server could not find a certificate with the provided alias.

System action
The request is halted.

Administrator response
Ensure that you have the correct keystore configured.

FBTKES015E

The signature validation failed.

Explanation
The server encountered an error while attempting to validate a signature.

System action
The request is halted.

Administrator response
Check the cause exception to find more details about why the validation failed.

FBTKES016E

No document was given.

Explanation
An XML document is required to perform the operation.

System action
The request is halted.

Administrator response
Ensure that a document is provided.

FBTKES017E

The signature creation operation failed.

Explanation
The server encountered an error while attempting to sign the given data.

System action
The request is halted.

Administrator response
Check the cause exception to find more details about why the signing failed.

FBTKES020E

The signature was not valid.

Explanation
The signature was determined to be invalid while attempting to validate the byte array of the signature.

System action
The request is halted.

Administrator response
No response required.

FBTKES021E

No keystore directory was provided.

Explanation
A keystore directory must be provided for the server to start.

System action
The request is halted.

Administrator response
Ensure that the keystore directory is provided.

FBTKES022E

The keystore directory provided (*alias*) does not exist or is not a directory.

Explanation
The keystore directory provided in the configuration does not exist or is not a directory.

System action
The request is halted.

Administrator response
Ensure that the given directory exists.

FBTKES023E

The required path element was not provided.

Explanation
For the given request, a path that points to the specific XML element is required.

System action
The request is halted.

Administrator response
Ensure that the caller is passing all required parameters.

FBTKES024E

The given element path did not point to an XML element.

Explanation
For the given request, a path that points to the specific XML element is required.

System action
The request is halted.

Administrator response
Ensure that the caller is passing all required parameters.

FBTKES025E

The key encryption and signature service client factory could not locate the key encryption and signature service module.

Explanation
The modules or module directory could not be located in the current environment configuration.

System action
The request is halted.

Administrator response
Ensure that the caller is passing all required parameters and that the configuration is correct.

FBTKES026E

An alias was not given.

Explanation
The caller did not pass an alias.

System action
The request is halted.

Administrator response
Ensure that the key configuration has all the correct key alias names configured.

FBTKES027E

The given key profile does not have a cipher assigned or an error occurred when getting an instance of the cipher.

Explanation
The key profile given did not return a cipher.

System action
The request is halted.

Administrator response
Ensure that the key profile configuration has the cipher configured correctly.

FBTKES028E

The raw key bytes for key *id* were not specified.

Explanation
The key bytes were not specified in the configuration file for the given key ID.

System action
The key given was not generated, process continued to the next key in the configuration file.

Administrator response
Ensure that the key configuration has the required configuration item.

FBTKES029E

The type for key *id* was not specified.

Explanation
The type was not specified in the configuration file for the given key ID.

System action
The key given was not generated, process continued to the next key in the configuration file.

Administrator response
Ensure that the key configuration has the required configuration item.

FBTKES030E

An unknown error occurred, the cipher returned no data but data was expected.

Explanation
Data was given to the cipher engine but it did not return any data.

System action
The request is halted.

Administrator response
Ensure that key profile, the cipher and the key are configured correctly.

FBTKES031E

During the decryption an error was encountered. It appears the given cipher text is corrupt.

Explanation
The given cipher text could not be decrypted and parsed into a valid XML document.

System action
The operation will return a failure.

Administrator response
Confirm that the message is not being altered.

FBTKES032W

The certificate with the subject's distinguished name of [*dn*] and serial of [*number*] has expired, therefore it was not used for runtime operations.

Explanation
The given certificate has expired and will not be used for runtime operations.

System action
The system will not use the certificate.

Administrator response
Only use certificates that are still valid.

FBTKES033E

The block cipher algorithm URI provided [*URI*] is not supported by the XML security API.

Explanation
The block cipher algorithm URI provided from configuration is not supported by the XML security API.

System action
The system will not complete the request.

Administrator response
Change the configuration to a supported block cipher algorithm URI.

FBTKES034E

The key transport algorithm URI provided [*URI*] is not supported by the XML security API.

Explanation
The key transport algorithm URI provided from configuration is not supported by the XML security API.

System action
The system will not complete the request.

Administrator response
Change the configuration to a supported key transport algorithm URI.

FBTKES035E

The provided message contained too many EncryptedKey elements, the process is unable to determine the correct key to use.

Explanation
The provided message did not have a KeyInfo element as a child of the EncryptedData element. Because there was no KeyInfo element, the service has to look for EncryptedKey elements under the parent node of the EncryptedData. If there is more than one EncryptedKey element under the parent, this error is returned.

System action
The system will not complete the request.

Administrator response
Ensure the given message contains a KeyInfo element as a child of the EncryptedData element, which includes either the EncryptedKey or references the EncryptedKey if there is more then one EncryptedKey in the message.

FBTKES036E

No EncryptedKey element found, the process cannot decrypt the given message.

Explanation
The given message did not contain a EncryptedKey element, the EncryptedKey element contains the key material to decrypt the EncryptedData element.

System action
The system will not complete the request.

Administrator response
Ensure that messages contain at least one EncryptedKey element for every EncryptedData element.

FBTKES037E

The key encryption and signature service client factory could not locate a certificate path validator module.

Explanation
The modules or module directory could not be located in the current environment configuration.

System action
The request is halted.

Administrator response
Ensure that the required certificate path validator module is properly configured and installed.

FBTKES038W

Certificate path validation is disabled because no keystores of type CA Certificates are configured.

Explanation
There are no keystores of type CA Certificates configured.

System action
The request is halted.

Administrator response
Ensure that at least one keystore containing CA certificates is configured with a type of CA Certificates.

FBTKES039E

The configuration file *file* could not be read.

Explanation
The configured file might not exist, might not be readable by this user, or might not be a valid file.

System action
The server cannot perform initialization of the hardware device.

Administrator response
Correct the configuration for the hardware provider in etc/kessjks.xml and restart the server.

FBTKES040E

A <HardwareProviderType> element could not be found with reference ID *idref* in etc/kessjks.xml.

Explanation
The configuration file contains a reference to an element that does not exit.

System action
The server cannot perform initialization of the hardware device.

Administrator response
Correct the configuration for the hardware provider in etc/kessjks.xml and restart the server.

FBTKES041E

A <ModuleReference> element could not be found with reference ID *idref* in etc/kessjks.xml.

Explanation
The configuration file contains a reference to an element that does not exit.

System action
The server will skip initialization of the module referenced by the ID.

Administrator response
Correct the configuration for the hardware provider in etc/kessjks.xml and restart the server.

FBTKES042E

The hardware cryptographic device could not be initialized.

Explanation
The hardware cryptographic device failed to initialize. See previous messages.

System action
The server will not be able to perform signing and cryptography services.

Administrator response
Verify that the hardware device is installed correctly and is operating properly.

FBTKES043E

There is no provider available to perform the requested operation.

Explanation
The signature and cryptographic provider failed to initialize. See previous messages.

System action
The server cannot perform the requested operation.

Administrator response
Check the message log for related errors and take corrective action accordingly.

FBTKES044E

The key encryption and signature service configuration is missing the required parameter *parameter*.

Explanation
An error has occurred while validating the server configuration. This error is due to the absence of a required parameter.

System action
The server will not function with a missing configuration.

Administrator response
Ensure that the missing configuration entry is specified.

FBTKES045E

The hardware cryptography feature is not supported by Tivoli Federated Identity Manager on this version of WebSphere Application Server.

Explanation
The installed version of WebSphere Application Server does not provide the proper support for the hardware cryptography feature.

System action
The server will not function with a missing configuration.

Administrator response
Either upgrade to WebSphere Application Server version 6.1 or greater, or disable the hardware cryptography feature.

FBTKES046E

The key profile with alias *alias* requires an initialization vector.

Explanation
The mode of the cipher in the key profile requires an initialization vector to be configured.

System action
The key profile is discarded.

Administrator response
Correct the configuration and restart the server.

FBTKES047E

The key profile with alias *alias* has an incomplete initialization vector.

Explanation
The initialization vector must include a size or initialization data to be configured.

System action
The key profile is discarded.

Administrator response
Correct the configuration and restart the server.

FBTKES048E

An exception occurred while processing the keystore on the hardware device. The exception message text is: *message*.

Explanation
An exception was encountered while processing the keystore provided by the hardware device.

System action
The keys and certificates not already processed will be unavailable.

Administrator response
Correct the configuration and restart the server.

FBTKES049E

The message signature did not include the required KeyInfo data to find a validation certificate.

Explanation
The server is configured to use the KeyInfo data in the message signature to locate a key for signature validation but the signature does not have the required data.

System action
The request is rejected.

Administrator response
Ensure that the sender includes either a Public Key, X509 Certificate data, X509 Subject Key Identifier or X509 Subject Name in the KeyInfo element of the signature.

FBTKES050E

The message signature did not include any KeyInfo data that matches the configured DN expression [*alias*].

Explanation
The server is configured to use the KeyInfo data in the message signature to locate a key for signature validation but the DN of the certificate does not match the allowable names in the configuration.

System action
The request is rejected.

Administrator response
Ensure that the configured DN expression is correct and retry the operation.

FBTKES051E

There are no certificates available that match the KeyInfo data in the message signature for the DN [*alias*].

Explanation
The server is configured to use the KeyInfo data in the message signature to locate a key for signature validation but a certificate could not be found in any keystore.

System action
The request is rejected.

Administrator response
Ensure that the public key certificate is imported into the Tivoli Federated Identity Manager keystore.

FBTKES052E

The signature algorithm URI provided [*URI*] is not supported.

Explanation
The system does not support the signature algorithm URI provided from the configuration.

System action
The system will not complete the request.

Administrator response
Change the configuration to the supported signature algorithm URI.

FBTKES053E

The digest algorithm URI provided [*URI*] is not supported.

Explanation
The system does not support the digest algorithm URI provided from the configuration.

System action
The system will not complete the request.

Administrator response
Change the configuration to the supported digest algorithm URI.

FBTKES054E

The signing key type [*KeyType*] does not match the signature algorithm [*URI*].

Explanation
The signing key type does not match the signature algorithm provided from the configuration.

System action
The system will not complete the request.

Administrator response
Change the configuration to match the key type and signature algorithm.

FBTKES055E

The key type [*KeyType*] does not support encryption.

Explanation
The key type provided from configuration does not support encryption.

System action
The system cannot complete the request.

Administrator response
Change the configuration to a supported encryption key type.

Chapter 11. Key encryption and signature service Java KeyStore messages

These messages are provided by the key encryption and signature service Java™ KeyStore component.

FBTKJK001E

A manager could not be created on this node. This result might not be an error if the system is running in a clustered environment. Confirm configuration and startup on the appropriate node.

FBTKJK002E

The global configuration properties file is not in the classpath of the server.

Explanation
The global configuration properties file could not be found in the server's classpath. The file is typically created at installation time for the installer and is required for the server to successfully start.

System action
The global configuration properties file could not be found.

Administrator response
Ensure that the system was installed correctly, locate the global configuration properties file, and ensure that the file is located in the server's classpath.

FBTKJK006E

The Key Encryption and Signature Service Java Keystore management bean cannot be registered.

Explanation
An error has occurred registering the management bean for the Key Encryption and Signature Service Java Keystore provider.

System action
The server will start with no management interface.

Administrator response
Enable a trace and check for errors leading up to this failure.

FBTKJK007E

The configuration file for the Key Encryption and Signature Service Java Keystore, *filename*, cannot be read.

Explanation
An error has occurred reading the configuration for the Key Encryption and Signature Service Java Keystore provider.

System action
The server will not be able to start unless the configuration file is located on another node.

Administrator response
Enable a trace and check for errors leading up to this failure.

FBTKJK008E

The bootstrap of the Key Encryption and Signature Service Java Keystore provider has failed.

Explanation
The bootstrap process of the Key Encryption and Signature Service Java Keystore did not complete successfully.

System action
Check earlier error and trace messages for problems leading up to this failure.

Administrator response
Validate the configuration of the Key Encryption and Signature Service Java Keystore provider.

FBTKJK009E

The input provided to the management operation is not valid.

Explanation
This error is typically due to null input values, missing input values, or input values of the wrong type.

System action
The management operation will be halted.

Administrator response
Check the trace for the input to the management operation.

FBTKJK010E

The input provided to the management operation is not valid. The parameter *parameter* is missing.

Explanation
This error is typically due to null input values, missing input values, or input values of the wrong type.

System action
The management operation will be halted.

Administrator response
Check the trace for the input to the management operation.

FBTKJK011E

The input provided to the management operation is not valid. The type *type* for parameter *parameter* is not valid. A value of *expectedType* was expected.

Explanation
This error is typically due to null input values, missing input values, or input values of the wrong type.

System action
The management operation will be halted.

Administrator response
Check the trace for the input to the management operation.

FBTKJK012E

The configuration update failed.

Explanation
An error has occurred while updating the server configuration.

System action
The server will continue running with the existing configuration.

Administrator response
Enable a trace and check for errors leading up to this failure.

FBTKJK015E

The key encryption and signature service configuration could not be discovered because no configuration store was found.

Explanation
An error has occurred discovering the server configuration. This error occurred because the distributed map instance could not be located.

System action
The server will not function without configuration information.

Administrator response
Ensure that the configuration store is running on the application server and enable the trace to check for errors leading up to this failure.

FBTKJK016E

The key encryption and signature service configuration is missing the required parameter *parameter*.

Explanation
An error has occurred while validating the server configuration. This error is due to the absence of a required parameter.

System action
The server will not function with a missing configuration.

Administrator response
Ensure that the missing configuration entry is specified.

FBTKJK017E

The configured Java key store configuration directory *directory* could not be read.

Explanation
The configured directory might not exist, might not be readable by this user, or might not be a directory.

System action
The server will not function with a missing configuration.

Administrator response
Ensure that the configured entry is valid.

FBTKJK018E

The configured Java key store configuration directory contains a file *file* that could not be read.

Explanation
The configured file might not exist, might not be readable by this user, or might not be a valid.

System action
The server will attempt to read the remaining files in the directory.

Administrator response
Ensure that the file is valid.

FBTKJK021E

The required input was not given.

Explanation
The required input was not given to process the request.

System action
The request could not be processed because the required input is missing.

Administrator response
Ensure that the correct input is given.

FBTKJK022E

The document owner was not given and the signature template could not be generated.

Explanation
For the signature template to generate correctly, the document owner must be provided.

System action
The signature template was not generated.

Administrator response
Ensure that the caller provides the correct document owner.

FBTKJK023E

A reference list of elements to be signed was not given. The signature template cannot be generated without a reference list.

Explanation
For a signature template to be generated, a reference list must be provided.

System action
Ensure that the caller provides the correct list of elements to be referenced in the generated signature template.

Administrator response
Ensure that the caller provides the correct list of elements to be referenced in the generated signature template.

FBTKJK024E

A context was not provided by the caller.

Explanation
The caller did not provide a context.

System action
The request is halted.

Administrator response
Ensure that a context is provided.

FBTKJK025E

A key alias was not provided by caller.

Explanation
The caller did not provide a key alias.

System action
The request is halted.

Administrator response
Ensure that a key alias is provided.

FBTKJK026E

There was no data provided to be signed.

Explanation
The caller did not provide any data to be signed.

System action
The request is halted.

Administrator response
Ensure that data is provided.

FBTKJK027E

A certificate with given alias (*alias*) was not found.

Explanation
The server could not find a certificate with the provided alias.

System action
Ensure that you have the correct keystore configured.

Administrator response
Ensure that you have the correct keystore configured.

FBTKJK028E

Signature validation failed.

Explanation
The server encountered an error while attempting to validate a signature.

System action

Administrator response
Check the cause exception to determine why the validation failed.

FBTKJK029E

No document was given.

Explanation
An XML document is required to perform the operation.

System action
The request is halted.

Administrator response
Ensure that a document is provided.

FBTKJK030E

The signature creation operation failed.

Explanation
The server encountered an error while attempting to sign the given data.

System action
The request is halted.

Administrator response
Check the cause exception to determine why the signing failed.

FBTKJK031E

The signature is not valid.

Explanation
See message.

System action
The request is halted.

Administrator response
Check the logs for exceptions to determine why signature validation failed.

FBTKJK032E

A key was not found with the given alias (*alias*).

Explanation
The server could not find a key with the provided alias.

System action
Ensure that you have the correct keystore configured.

Administrator response
Ensure that you have the correct keystore configured.

FBTKJK033E

The required path element was not provided.

Explanation
For the given request, a path that points to the specific XML element is required.

System action
The request is halted.

Administrator response
Ensure that the caller is passing all required parameters.

FBTKJK034E

The given element path did not point to an XML element.

Explanation
For the given request, a path that points to the specific XML element is required.

System action
The request is halted.

Administrator response
Ensure that the caller is passing all required parameters.

FBTKJK035E

The key type for a given alias *alias* is an unknown key.

Explanation
An attempt was made to use a key that has an unknown type.

System action
An attempt was made to use a key that has an unknown type.

Administrator response
Ensure that the key for given alias is a supported key type.

FBTKJK036E

The key encryption and signature service Java keystore was unable to find a worker to complete the task. This error is likely due to an incorrect configuration.

Explanation
No configuration worker instance could be found.

System action
The operation returned failure.

Administrator response
Enable a trace and check the logs for errors that might have lead up to this action.

FBTKJK037E

The key encryption and signature service Java keystore EJB client could not create the remote interface, *remote*

Explanation
No remote EJB instance could be created.

System action
The operation will return a failure.

Administrator response
Enable a trace and check the logs for errors that might have lead up to this action.

FBTKJK038E

The key encryption and signature service Java keystore EJB client encountered an error with the EJB invocation.

Explanation
An exception was thrown while communicating with the remote EJB.

System action
The operation will return a failure.

Administrator response
Enable a trace and check the logs for errors that might have lead up to this action.

FBTKJK039E

The SignedInfo signature value does not match the calculated value.

Explanation
The SignedInfo portion of the signature did not match the calculated value. This error is usually caused by the SignedInfo digest not matching or the public key used to validate does not match the private key used to sign.

System action
The operation will return a failure.

Administrator response
Ensure that the correct certificate is used to validate the message.

FBTKJK040E

The Reference with the identifier *identifier* calculated a different digest value.

Explanation
The given Reference digest did not match the calculated digest. This error is usually caused by the message changing after being signed.

System action
The operation will return a failure.

Administrator response
Ensure that the message does not change after being signed.

FBTKJK041E

While writing out the updated file *filename*, an error was encountered. The update to the file did not occur.

Explanation
An error was encountered when making an update to the given file.

System action
The operation will return a failure.

Administrator response
Ensure that the given file exists and has the correct file permissions to allow updates to occur. See the corresponding exception in the trace file for more details.

FBTKJK042E

The directory *directory* cannot be read.

Explanation
An error was encountered when attempting to read the directory given.

System action
The operation will return a failure.

Administrator response
Ensure that the given directory exists and that the correct file permissions are enabled.

FBTKJK043E

The backup operation failed. The backup JAR file *filename* for directory *directory* cannot be created.

Explanation
An error was encountered when attempting to create a backup.

System action
The operation will return a failure.

Administrator response
Ensure that the given directory exists and that the correct file permissions are enabled.

FBTKJK045E

The management operation is missing required input values. The management operation has failed to complete.

Explanation
The management operation is missing required input.

System action
The operation will return a failure.

Administrator response
The management operation being called requires specific input to complete the operation. Check the documentation for all the required input.

FBTKJK046E

The provided password is incorrect or the *keystore* keystore does not exist. The management operation has failed to complete.

Explanation
The provided password was not correct, or the keystore does not exist.

System action
The operation will return a failure.

Administrator response
Ensure that the keystore exists and ensure that the correct password was entered.

FBTKJK047E

An error was encountered when retrieving the encoded format of the certificate.

Explanation
An attempt was made to encode a certificate that returned errors.

System action
The operation will return a failure.

Administrator response
Check the trace logs to find out a more specific exception error.

FBTKJK048E

An error was encountered while creating the keystore for export. The export operation failed.

Explanation
During the generation of the keystore to export, the server encountered a error.

System action
The operation will return a failure.

Administrator response
Check the logs for an exception that will give a more specific reason for the error.

FBTKJK049E

An error was encountered while importing the given keystore. The import operation failed.

Explanation
During the importing of the keystore, the server encountered a error.

System action
The operation will return a failure.

Administrator response
Check the logs for an exception that will give a more specific reason for the error.

FBTKJK050E

The store *storename* does not exist. The operation failed to complete.

Explanation
The given store does not exist.

System action
The operation will return a failure.

Administrator response
Ensure that the given store exists.

FBTKJK051E

The import into store *storename* failed. The operation failed to complete. Check the trace logs for more specific errors.

Explanation
An error was encountered when the key or certificate or both were being imported.

System action
The operation will return a failure.

Administrator response
Check the trace logs for a more specific error message.

FBTKJK052E

The password for the given keystore is incorrect. The operation failed to complete.

Explanation
An error was encountered while validating the password for the given keystore.

System action
The operation will return a failure.

Administrator response
Ensure that the correct password is entered for the keystore or for the key entry.

FBTKJK053E

An error occurred when attempting to update the store (*storename*) with the new data. The operation failed to complete.

Explanation
An error occurred when updating the store listed.

System action
The operation will return a failure.

Administrator response
Check the trace logs for a more specific error message.

FBTKJK054E

The key alias *alias name* returned no data for the keystore provided. Confirm that the key alias given exists. The operation failed to complete.

Explanation
There are no keys or certificates located at the key alias given.

System action
The operation will return a failure.

Administrator response
Confirm that the given key alias exists in the provided keystore.

FBTKJK055E

The key alias *alias name* already exists in the store *store name*. The operation failed to complete.

Explanation
The import operation was asked to not overwrite existing key aliases and the alias provided already existed in the store.

System action
The operation will return a failure.

Administrator response
Confirm that the given key alias does not exist in the provided store.

FBTKJK056W

The certificate with the subject's distinguished name of [*dn*] and serial of [*number*] has expired therefore it was not used for runtime operations.

Explanation
The given certificate has expired and will not be used for runtime operations.

System action
The system will not use the certificate.

Administrator response
Only use certificates that are still valid.

FBTKJK057E

The block cipher algorithm URI provided [*URI*] is not supported by the XML security API.

Explanation
The block cipher algorithm URI provided from configuration is not supported by the XML security API.

System action
The system will not complete the request.

Administrator response
Change the configuration to a supported block cipher algorithm URI.

FBTKJK058E

The key transport algorithm URI provided [*URI*] is not supported by the XML security API.

Explanation
The key transport algorithm URI provided from configuration is not supported by the XML security API.

System action
The system will not complete the request.

Administrator response
Change the configuration to a supported key transport algorithm URI.

FBTKJK059E

The provided message contained too many EncryptedKey elements, we are unable to determine the correct key to use.

Explanation
The provided message did not have a KeyInfo element as a child of the EncryptedData element. Since there was no KeyInfo element the service has to look for EncryptedKey elements under the parent node of the EncryptedData. If there is more then one EncryptedKey element under the parent, this error is returned.

System action
The system will not complete the request.

Administrator response
Ensure the given message contains a KeyInfo element as a child of the EncryptedData element which includes either the EncryptedKey, or which references the EncryptedKey if there is more then one EncryptedKey in the message.

FBTKJK060E

No EncryptedKey element found, we are unable to decrypt the given message.

Explanation
The given message did not contain a EncryptedKey element, the EncryptedKey element contains the key material to decrypt the EncryptedData element.

System action
The system will not complete the request.

Administrator response
Ensure that messages contain at least one EncryptedKey element for every EncryptedData element.

Chapter 12. Knowledge questions messages

These messages are provided by the knowledge questions component.

FBTKQA000E

Internal Error. Contact the System Administrator.

Explanation
An internal error occurred.

System action
The application encountered an error. The process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTKQA100E

The user [*user*] attempting to authenticate using the knowledge questions authentication mechanism does not have enough questions registered. The knowledge questions authentication mechanism is configured to require *answer* questions answered to authenticate. At this time only *number* questions have been registered.

Explanation
The user needs to register enough knowledge questions prior to authenticating using the knowledge questions authentication mechanism.

System action
The authentication process encountered an error. The process will continue if a grace period has been granted to authenticate without supplying any knowledge questions.

Administrator response
None.

FBTKQA101E

The knowledge questions authentication mechanism failed to retrieve the user questions.

Explanation
The knowledge questions authentication mechanism failed to obtain the user questions from the repository.

System action
The authentication process encountered an error. The process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTKQA102E

The knowledge questions authentication mechanism failed to validate the submitted answers.

Explanation
The knowledge questions authentication mechanism failed to validate the submitted answers.

System action
The authentication process encountered an error. The process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTKQA103W

The user [*user*] attempting to authenticate using the knowledge questions authentication mechanism does not have any questions registered.

Explanation
The user needs to register knowledge questions prior to authenticating using the knowledge questions authentication mechanism.

System action
The authentication process encountered an error. The process will continue if a grace period has been granted to authenticate without supplying knowledge questions.

Administrator response
None.

FBTKQA104E

The request sent to the knowledge questions authentication mechanism is not valid. The request is missing attribute [*parameter*].

Explanation
The knowledge questions authentication mechanism failed because the request did not include a required parameter.

System action
The authentication process encountered an error. The process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTKQA105E

The request sent to the knowledge questions authentication mechanism is not valid. The value [*value*] specified for attribute [*parameter*] is not valid.

Explanation
The knowledge questions authentication mechanism failed because the request included an invalid value for a required parameter.

System action
The authentication process encountered an error. The process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTKQA107E

The answer(s) submitted for the knowledge questions are not valid.

Explanation
At least one of the answers submitted for the knowledge question is not valid.

System action
None.

Administrator response
None.

FBTKQA108E

The knowledge questions authentication mechanism failed to retrieve the grace period authentication count.

Explanation
The knowledge questions authentication mechanism failed to obtain the user grace period authentication count from the repository.

System action
The authentication process encountered an error. The process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTKQA109E

The knowledge questions authentication mechanism failed to store the grace period authentication count.

Explanation
The knowledge questions authentication mechanism failed to store the user grace period authentication count in the repository.

System action
The authentication process encountered an error. The process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTKQA110E

The answer(s) submitted for the knowledge questions are not valid. *incorrect* incorrect attempt(s) have been made. You have *remaining* attempts remaining.

Explanation
The entered answers are not valid.

System action
The request has been halted.

Administrator response
Correct the answers and resubmit the form.

FBTKQA111E

incorrect incorrect attempt(s) have been made. You have no attempts remaining. Please try again in *time* seconds.

Explanation
There are no more remaining attempts.

System action
The request has been halted.

Administrator response
Wait until the attempts have expired before trying again.

FBTKQA112E

The knowledge questions authentication user management failed to reset the knowledge questions.

Explanation
The knowledge questions authentication user management failed to reset the knowledge questions in the repository.

System action
The knowledge questions user management process encountered an error. The process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTKQA113E

The knowledge questions authentication user management failed to store the knowledge questions.

Explanation
The knowledge questions authentication user management failed to store the knowledge questions in the repository.

System action
The knowledge questions user management process encountered an error. The process has been halted.

Administrator response

Check the log file for more information about the cause of the problem.

Chapter 13. Liberty messages

These messages are provided by the Liberty Profile component.

FBTLIB001E

A configuration error has occurred.

Explanation
A configuration error has occurred due to invalid configuration.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages and validate the configuration.

FBTLIB002E

Internal Error: The delegate protocol was unable to retrieve the Liberty Request Context.

Explanation
Internal Error: The delegate protocol was unable to retrieve the Liberty Request Context.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages and validate the configuration.

FBTLIB003E

The Liberty plug-in is not able to route the incoming request correctly.

Explanation
The Liberty plug-in is not able to determine the protocol that must be used for the incoming request.

System action
The request has been halted.

Administrator response
Make sure that the endpoint that is configured is correct. Enable a trace for detailed messages about the error.

FBTLIB004E

Internal Error: The delegate protocol cannot retrieve the AuthnRequest from incoming HTTP GET.

Explanation
The delegate protocol cannot retrieve the AuthnRequest from incoming HTTP GET.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB005E

Internal Error: The delegate protocol cannot retrieve the AuthnResponse from incoming HTTP POST.

Explanation
The delegate protocol cannot retrieve the AuthnResponse from incoming HTTP POST.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB006E

Internal Error: The delegate protocol cannot decode the incoming AuthnResponse from BASE64.

Explanation
The delegate protocol cannot decode the incoming AuthnResponse from BASE64.

System action
The request has been halted.

Administrator response
Make sure that the AuthnResponse was encoded correctly by the partner. Enable a trace for detailed messages about the error.

FBTLIB007E

Internal Error: The delegate protocol cannot retrieve the value in the LARES field in the incoming AuthnReponse POST.

Explanation
The delegate protocol cannot retrieve the value in the LARES field in the incoming AuthnReponse POST.

System action
The request has been halted.

Administrator response
Make sure that the AuthnResponse was sent by the partner adhering to Liberty specifications. Enable a trace for detailed messages about the error.

FBTLIB008E

Internal Error: An error was encountered in the execution of protocol chain.

Explanation
An error was encountered in the execution of protocol chain.

System action
Contact your IBM support representative.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB009E

Internal Error: The Delegate protocol is unable to process the response because it could not retrieve the AuthnRequest from LibertyContext.

Explanation
The Delegate protocol is unable to process the response because it could not retrieve the AuthnRequest from LibertyContext.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB010E

Internal Error: The Delegate protocol is unable to obtain the SingleSignOnUrl from the context.

Explanation
The Delegate protocol is unable to obtain the SingleSignOnUrl from the context.

System action
The request has been halted.

Administrator response
Make sure all the endpoints are configured correctly. Enable a trace for detailed messages about the error.

FBTLIB011E

Internal Error: The Delegate protocol is unable to process the response because it could not retrieve the AuthnResponse from LibertyContext.

Explanation
The Delegate protocol is unable to process the response because it could not retrieve the AuthnResponse from LibertyContext.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB012E

Internal Error: The Delegate protocol is unable to process the response because it could not convert the AuthnResponse to an XML string.

Explanation
The Delegate protocol is unable to process the response because it could not convert the AuthnResponse to an XML string.

System action
The request has been halted.

Administrator response
The AuthnResponse message might not be formatted correctly. Enable a trace for detailed messages about the error.

FBTLIB013E

Internal Error: The Delegate protocol is unable to convert the response from an XML string to BASE64 encoded data.

Explanation
The Delegate protocol is unable to convert the response from an XML string to BASE64 encoded data.

System action
Contact your IBM support representative.

Administrator response
The AuthnResponse message might not be formatted correctly. Enable a trace for detailed messages about the error.

FBTLIB014E

Internal Error: The Delegate protocol is unable to obtain the AssertionConsumerUrl from the context.

Explanation
The Delegate protocol is unable to obtain the AssertionConsumerUrl from the context.

System action
The request has been halted.

Administrator response
Make sure that all the endpoints are configured correctly. Enable a trace for detailed messages about the error.

FBTLIB015E

Internal Error: The Delegate protocol is unable to obtain the RelayState from the AuthnResponse.

Explanation
The Delegate protocol is unable to obtain the RelayState from the AuthnResponse.

System action
The request has been halted.

Administrator response
RelayState might not be set correctly in the AuthnResponse. Enable a trace for detailed messages about the error.

FBTLIB016E

Internal Error: The Delegate protocol is unable to find the template page *PageTemplate*.

Explanation
The delegate protocol is unable to find the specified page template.

System action
Contact your IBM support representative.

Administrator response
Make sure that the product is installed and configured correctly. Enable a trace for detailed messages about the error.

FBTLIB017E

Internal Error: The delegate protocol cannot retrieve the LogoutRequest from incoming HTTP GET.

Explanation
The delegate protocol cannot retrieve the LogoutRequest from incoming HTTP GET.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB018E

The delegate protocol cannot retrieve the *EndPointType* from the defined federations.

Explanation
The specified endpoint is not configured.

System action
The request has been halted.

Administrator response
Make sure that all the endpoints are configured correctly. Enable a trace for detailed messages about the error.

FBTLIB019E

The delegate protocol cannot convert the logout response to a URL encoded string.

Explanation
The delegate protocol cannot convert the logout response to a URL encoded string.

System action
Contact your IBM support representative.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB020E

Internal Error: The delegate protocol could not find the session ID *SessionId* in the global session.

Explanation
The specified session ID was not found in the global session.

System action
Contact your IBM support representative.

Administrator response
The session ID might not have been stored or it might have expired. Enable a trace for detailed messages about the error.

FBTLIB021E

The delegate protocol configuration determined that no federations are defined.

Explanation
The delegate protocol configuration determined that no federations are defined.

System action
Contact your IBM support representative.

Administrator response
Make sure that the federations are defined. Enable a trace for detailed messages about the error.

FBTLIB022E

The required attribute *VariableName* was not found in the defined self-federation entity.

Explanation
The specified attribute is not defined in the self-federation entity.

System action
Contact your IBM support representative.

Administrator response
Make sure that the specified required attribute is defined in the self-federation entity. Enable a trace for detailed messages about the error.

FBTLIB023E

The Delegate protocol configuration could not find the Provider ID in the defined self-federation entity.

Explanation
The Delegate protocol configuration could not find the Provider ID in the defined self-federation entity.

System action
Contact your IBM support representative.

Administrator response
Make sure that the Provider ID is defined in the self-federation entity. Enable a trace for detailed messages about the error.

FBTLIB024E

The Delegate protocol configuration could not find the Key identifier in the defined self-federation entity.

Explanation
The Delegate protocol configuration could not find the Key identifier in the defined self-federation entity.

System action
The request has been halted.

Administrator response
Make sure the Key identifier is defined in the defined self-federation entity. Enable a trace for detailed messages about the error.

FBTLIB025E

The SOAPEndpoint URL is malformed. SoapEndpoint = *SoapEndpoint*

Explanation
The specified SOAPEndpoint URL is not valid.

System action
The request has been halted.

Administrator response
Make sure that the correct SOAPEndpoint is configured. Enable a trace for detailed messages about the error.

FBTLIB026E

The Liberty plug-in cannot connect to SOAPEndpoint *SoapEndpoint*

Explanation
The Liberty plug-in cannot connect to the specified SOAPEndpoint.

System action
The request has been halted.

Administrator response
Make sure that the SOAPEndpoint accepts connections. Enable a trace for detailed messages about the error.

FBTLIB027E

The Liberty plug-in caught an unexpected exception when sending the SOAP message.

Explanation
The Liberty plug-in caught an unexpected exception when sending the SOAP message.

System action
Contact your IBM support representative.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB028E

The Liberty plug-in received a SOAP request that is not valid.

Explanation
The Liberty plug-in received a SOAP request that is not valid.

System action
The request is halted.

Administrator response
Make sure that the received SOAP request is formatted correctly. Enable a trace for detailed messages about the error.

FBTLIB029E

The keystore is not initialized for SSL communication for the SOAP client.

Explanation
The keystore is not initialized for SSL communication for the SOAP client.

System action
Contact your IBM support representative.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB030E

The Liberty plug-in caught an exception during SSL initialization.

Explanation
The Liberty plug-in caught an exception during SSL initialization.

System action
Contact your IBM support representative.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB031E

The Liberty plug-in configuration failed to find the key *Key* in the SPS configuration.

Explanation
The Liberty plug-in configuration failed to find the specified key in the SPS configuration.

System action
Contact your IBM support representative.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB032E

The Liberty SOAP client failed to initialize due to an unexpected exception.

Explanation
The Liberty SOAP client failed to initialize due to an unexpected exception.

System action
The request has been halted.

Administrator response
Make sure that the SOAP back channel configuration is correct. Enable a trace for detailed messages about the error.

FBTLIB033E

The Liberty plug-in is unable to get an artifact from the context.

Explanation
The Liberty plug-in is unable to get an artifact from the context.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB034E

The Liberty plug-in is unable to get an artifact from the incoming HTTP GET query parameters.

Explanation
The Liberty plug-in is unable to get an artifact from the incoming HTTP GET query parameters.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB035E

The Liberty plug-in is unable to get a SAML response from the context.

Explanation
The Liberty plug-in is unable to get a SAML response from the context.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB036E

Internal Error: The Delegate protocol is unable to get the logout response from the received HTTP GET.

Explanation
The Delegate protocol is unable to get the logout response from the received HTTP GET.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB037E

Internal Error: The delegate protocol cannot retrieve the Logout response from the context.

Explanation
The delegate protocol cannot retrieve the Logout response from the context.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB038E

The delegate protocol cannot convert a logout request to a URL-encoded string.

Explanation
The delegate protocol cannot convert a logout request to a URL-encoded string.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB039E

Internal Error: The Delegate protocol is unable to process the request because it could not retrieve a LogoutRequest from LibertyContext.

Explanation
The Delegate protocol is unable to process the request because it could not retrieve a LogoutRequest from LibertyContext.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB040E

An incorrect LECP header was received in the incoming request.

Explanation
An incorrect LECP header was received in the incoming request.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB041E

The Delegate protocol is unable to get the AuthnRequest from the incoming SOAP message.

Explanation
The Delegate protocol is unable to get the AuthnRequest from the incoming SOAP message.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB042E

The Delegate protocol is unable to get the AuthnResponse from the received HTTP POST.

Explanation
The Delegate protocol is unable to get the AuthnResponse from the received HTTP POST.

System action
The request has been halted.

Administrator response
Make sure that the partner is configured to send the AuthnResponse. Enable a trace for detailed messages about the error.

FBTLIB043E

The Delegate protocol is unable to find an AuthnRequest in the received SOAP message.

Explanation
The Delegate protocol is unable to find an AuthnRequest in the received SOAP message.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB044E

Internal Error: The Delegate protocol is unable to get the AuthnRequestEnvelope from the Context.

Explanation
The Delegate protocol is unable to get the AuthnRequestEnvelope from the Context.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB045E

Internal Error: The Delegate protocol is unable to get the AuthnResponseEnvelope from the Context.

Explanation
The Delegate protocol is unable to get the AuthnResponseEnvelope from the Context.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB046E

A common domain name has not been configured.

Explanation
An attempt was made to perform an Identity Provider introduction but a common domain name was not configured.

System action
The operation was not performed.

Administrator response
Configure a common domain name and restart the server.

FBTLIB047E

An MSISDN header was not found in the incoming LECP request.

Explanation
The incoming LECP request does not contain an MSISDN header.

System action
The request was rejected.

Administrator response
Configure the LECP provider ID correctly and restart the server.

FBTLIB048E

An error was encountered while unobfuscating the password *ObfuscatedPassword* for key *Key* from the configuration.

Explanation
Liberty plug-in tried to unobfuscate the specified password set in the configuration, but failed to do so.

System action
The Liberty plug-in failed to initialize SSL for the SOAP backchannel.

Administrator response
Configure SSL for the SOAP backchannel correctly and restart the server.

FBTLIB049E

Partner provider ID cannot be determined for checking signature configuration options.

Explanation
Liberty plug-in tried to find the partner this message was sent to or received from, but failed to do so.

System action
The Liberty plug-in failed to determine the partner from the configuration.

Administrator response
Enable a trace for detailed messages and validate the configuration.

FBTLIB050E

Request to create an unsolicited AuthnResponse was received but the request does not contain all the required parameters.

Explanation
The required parameters are missing in the request.

System action
The request was rejected.

Administrator response
The request must have the TargetURL and ProviderID parameters set.

FBTLIB200E

The protocol action caught an unexpected exception while building a Liberty assertion.

Explanation
The protocol action caught an unexpected exception from outside of Liberty while building a Liberty assertion.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB201E

The protocol action cannot retrieve the SAML status from the Liberty context.

Explanation
No SAML_STATUS attribute was found in the Liberty context. This attribute is typically set by a previous protocol action.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB202E

The protocol action cannot find a request ID in the request object.

Explanation
No RequestID attribute was found in the request message being processed. This attribute is required.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB203E

The protocol action cannot determine the current provider identifier.

Explanation
The configuration did not return an identifier for the current provider.

Administrator response
Verify that configuration files are present and have not been corrupted. If the files appear good, enable a trace for detailed messages about the error.

FBTLIB204E

No federation exists for this principal.

Explanation
Single sign-on is not possible for this principal because the account cannot be federated. The following conditions can prevent account federation: the user does not consent to federation when queried, the authentication request Federate element is set to false, the authentication request IsPassive element is set to true and the user cannot be queried for consent.

Administrator response
Verify that the authentication request provides proper values for the Federate and IsPassive elements, and that the user answers affirmatively if queried for consent to federate. In addition, enable a trace for detailed messages about the error.

FBTLIB205E

The protocol action caught an unexpected exception while determining consent to federate.

Explanation
The protocol action caught an unexpected exception outside of Liberty while determining if the user consents to account federation.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB206E

The protocol action cannot determine the identity of a locally authenticated user.

Explanation
No local user information was available in the Liberty context. This information is typically set by a previous protocol action by querying the local execution environment for user identity and credentials.

User response
Verify that the user has logged on successfully.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB207E

The protocol action cannot determine the value of the name identifier provided by the identity provider.

Explanation
No IDP_NAME_ID attribute was found in the Liberty context. This value is typically set by a previous protocol action.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB208E

The protocol action caught an unexpected exception while federating the principal.

Explanation
The protocol action caught an unexpected exception outside of Liberty while attempting to federate the principal.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB209E

The protocol action caught an unexpected exception while executing ForceAuthn logic.

Explanation
The protocol action caught an unexpected exception outside of Liberty while executing ForceAuthn logic.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB210E

The protocol action cannot obtain a local token from the Liberty context.

Explanation
Local authentication is not possible because the protocol action requires a LOCAL_TOKEN attribute in the Liberty context. This attribute is typically set by a previous protocol action.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB211E

The protocol action caught an unexpected exception while attempting to set the user's local credentials.

Explanation
The protocol action caught an unexpected exception outside of Liberty while attempting to set the user's local credentials.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB212E

SAML error in response: *SamlStatus*.

Explanation
The response message contains a SAML error indicating that the request was not successful.

Administrator response
Enable a trace on the message provider for information about why the error was returned.

FBTLIB213E

No Liberty assertion was returned in the authentication response message.

Explanation
The identity provider did not return any Liberty assertions in the authentication response. Single sign-on failed.

Administrator response
Enable a trace on the identity provider for information about why no Liberty assertions were included in the authentication response.

FBTLIB214E

No RelayState element was found in the authentication response.

Explanation
The authentication response message did not contain a RelayState element, which is required for single sign-on. The RelayState should have been provided in the original authentication request.

Administrator response
Enable a trace on both the service provider and identity provider for more information. On the service provider, verify that the original authentication request contains the appropriate RelayState element.

FBTLIB215E

No request with identifier *InResponseTo* was found. The response is ignored.

Explanation
The response message contained an InResponseTo attribute whose value did not correspond to any request identifiers in the current session.

Administrator response
Enable a trace on both the service provider and identity provider for more information. On the service provider, verify that the original request contains a RequestID attribute. On the identity provider, verify that the response references that same value in the InResponseTo attribute.

FBTLIB216E

The protocol action caught an unexpected exception while processing the Liberty message.

Explanation
The protocol action caught an unexpected exception outside of Liberty while processing the Liberty message.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB217E

The Liberty assertion could not be exchanged for a local credential.

Explanation
The protocol action caught an unexpected exception from the token exchange service while exchanging a Liberty assertion for a local credential.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB218E

The protocol action caught an unexpected exception while querying the user who wants to federate his identity.

Explanation
The protocol action caught an unexpected exception outside of Liberty while querying the user who wants to federate his identity.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB219E

The protocol action caught an unexpected exception while querying the execution environment for the user's current federation state.

Explanation
The protocol action caught an unexpected exception outside of Liberty while querying the execution environment for the user's current federation state.

System action
Contact your IBM support representative.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB220E

The protocol action caught an unexpected exception while querying the execution environment for the user's current login state.

Explanation
The protocol action caught an unexpected, non-Liberty exception while querying the execution environment for the user's current login state.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB221E

A Liberty version mismatch occurred: runtime = *LibertyRuntimeMajorVersion.LibertyRuntimeMinorVersion*; message = *MessageMajorVersion.MessageMinorVersion*.

Explanation
The Liberty version of the message is not supported by the Liberty runtime.

Administrator response
Verify that the providers in this provider's circle of trust operate at a compatible level of the Liberty protocol.

FBTLIB222E

The protocol action caught an unexpected exception while validating a Liberty message.

Explanation
The protocol action caught an unexpected exception outside of Liberty while validating a Liberty message.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB223E

The identity provider (*IdentityProvider*) does not have a configured federation with the requesting service provider (*ServiceProvider*).

Explanation
There are no configured federations that include the service provider who issued the request.

Administrator response
Verify that configuration files are present and have not been corrupted. If necessary, establish a partnership with the service provider in question.

FBTLIB224E

The user has no local credentials.

Explanation
The protocol being executed by this action requires that the user is locally authenticated. No local credentials could be found; therefore, the protocol cannot be completed.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB225E

The protocol action caught an unexpected exception while verifying that the user has local credentials.

Explanation
The protocol action caught an unexpected exception outside of Liberty while verifying that the user has local credentials.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB226E

The protocol action caught an unexpected exception while building a Liberty request or response message.

Explanation
The protocol action caught an unexpected exception outside of Liberty while building a Liberty request or response message.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB227E

No destination URL was found in the Liberty context.

Explanation
The protocol action cannot find the APPLIES_TO_URL attribute in the Liberty context. This attribute is typically set by a previous action that sets it to the value of a service provider's AssertionConsumerServiceURL.

Administrator response
Verify that configuration files are present and have not been corrupted. Enable a trace for detailed messages about the error.

FBTLIB228E

The local credential could not be exchanged for a Liberty assertion.

Explanation
The protocol action caught an unexpected exception from the token exchange service while exchanging a local credential for a Liberty assertion.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB229E

The identity provider is passive and cannot authenticate the user.

Explanation
The identity provider must interact with the user for local authentication, but it cannot because the authentication request's IsPassive element is set to 'true'.

Administrator response
Retry the authentication request with the IsPassive element set to 'false'.

FBTLIB230E

The ForceAuthn element is not supported.

Explanation
Forced authentication is not supported in this release, and the authentication request's ForceAuthn element is set to 'true'.

Administrator response
Retry the authentication request with the ForceAuthn element set to 'false'.

FBTLIB231E

The ReauthenticateOnOrAfter attribute is not supported.

Explanation
Reauthentication requirements specified in the Liberty assertion is not supported in this release. Therefore, the assertion cannot be used for single sign-on.

Administrator response
Retry the authentication request, sending it to an identity provider that does not specify a reauthentication time.

FBTLIB232E

The provider identifier cannot be retrieved from configuration.

Explanation
Configuration did not return a value for the provider identifier.

Administrator response
Verify that configuration files are present and have not been corrupted. If necessary, add the needed configuration data.

FBTLIB233E

The protocol profile could not be retrieved from the Liberty context.

Explanation
The Liberty context did not contain a LIB_PROTOCOL_PROFILE attribute. This attribute is typically set by the delegate protocol.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB234E

The protocol action caught an unexpected exception while generating claims for the token exchange between a local credential and a Liberty assertion.

Explanation
The protocol action caught an unexpected exception outside of Liberty while generating a LibertyClaims object for the token exchange.

Administrator response
Enable trace for detailed messages about the error.

FBTLIB235E

No provider identifier was found in the Liberty message.

Explanation
The protocol action could not find a provider identifier in the message being processed.

Administrator response
Enable a trace for detailed messages about the error, including format of the message in question.

FBTLIB236E

No identity service was found.

Explanation
No identity service was found.

Administrator response
Check the identity service configuration. Enable a trace for detailed messages about the error.

FBTLIB237E

No token request information was found.

Explanation
Token exchange requires Issuer information, AppliesTo information, or both. Neither Issuer information nor AppliesTo information could be found.

Administrator response
If the error is seen on an identity provider, check the configuration and make sure that the self-provider is configured properly; this configuration is needed to determine the Issuer information. Enable a trace for detailed messages about the error, including the contents of the message, which should contain the ProviderID. The ProviderID is needed to determine the AppliesTo information. If the error is seen on a service provider, enable a trace for detailed messages about the error; Issuer information is determined from information in the Liberty assertion, and AppliesTo information is determined from the RelayState in the original authentication request.

FBTLIB238E

No alias was found for user *User* and provider *PartnerProvider*.

Explanation
There was no alias found for the currently authenticated user for the specified partner provider.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB239E

The timestamp (IssueInstant attribute) in a received Liberty request or response was out of range.

Explanation
Validation failed for a received Liberty message because the timestamp in the message did not fall within a configured range from the current system's time.

Administrator response
Synchronize the clocks of the sending and receiving machines, if possible. Also check that the configured time skew tolerance is acceptable.

FBTLIB240E

The protocol action caught an unexpected exception while executing a local logout.

Explanation
The protocol action caught an unexpected exception outside of Liberty while executing a local logout.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB241E

The local logout operation failed.

Explanation
The local logout operation failed.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB242E

The protocol action could not build a list of service providers that were sent Liberty assertions on this session.

Explanation
The protocol action could not build a list of service providers that were sent Liberty assertions on this session.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB243E

The response does not correlate to the current request.

Explanation
Validation failed for a Liberty or SAML response because the InResponseTo attribute in a received Liberty response did not match the current request identifier.

Administrator response
Enable a trace on both the responding and requesting machines for detailed messages about the error.

FBTLIB244E

The service provider (*ServiceProvider*) does not have a configured federation with the responding identity provider (*IdentityProvider*).

Explanation
No configured federations include the identity provider that issued the response.

Administrator response
Verify that configuration files are present and have not been corrupted. If necessary, establish a partnership with the identity provider in question.

FBTLIB245E

The service provider (*ServiceProvider*) making the logout request was not issued an assertion by this session in the identity provider.

Explanation
The identity provider session information does not indicate that this service provider has been issued an assertion. Therefore, the service provider cannot initiate a logout request.

Administrator response
This error might mean that the identity provider has received an inappropriate logout message. Examine the configuration and enable a trace to investigate which service providers can request authentication and which actually have requested authentication.

FBTLIB246E

The provider (*ServiceOrIdentityProvider*) does not have a required endpoint URL configured (*EndpointURL*).

Explanation
A required endpoint URL was not found in the configuration for the specified provider.

Administrator response
Verify that configuration files are present and have not been corrupted. If necessary, define the required endpoint URL for the provider in question.

FBTLIB247E

Bad SAML status.

Explanation
A previous protocol action set the SAML_STATUS Liberty attribute to a value other than Success, indicating that subsequent actions should not execute.

Administrator response
Enable a trace to determine which action set the SAML_STATUS value, and why the value is not samlp:Success.

FBTLIB248E

No LogoutRequest was found for the responding service provider (*ServiceProvider*).

Explanation
A LogoutResponse was received from a service provider and no corresponding LogoutRequest could be found. The LogoutResponse is ignored.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB249E

No audience entry was found for self-service provider (*ServiceProvider*).

Explanation
The Liberty assertion did not contain an audience entry for the current self-provider. The assertion is ignored.

Administrator response
Enable trace for detailed messages on the issuing identity provider to determine why the self-provider was not included in the assertion audience.

FBTLIB250E

The protocol action caught an unexpected exception while validating a Liberty assertion.

Explanation
The protocol action caught an unexpected exception outside of Liberty while validating a Liberty assertion.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB251E

The Liberty assertion failed validation.

Explanation
The Liberty assertion did not pass validation checks of the ReauthenticationOnOrAfter attribute, the InResponseTo attribute, or the AudienceRestrictionCondition element.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB252E

Required data could not be found from configuration.

Explanation
A required data item was not found in the provider's configuration, so the operation cannot be performed.

Administrator response
Enable a trace for detailed messages about the error, including which data item could not be found. Then verify that the provider's configuration files are not incorrect or unreadable and that they contain the proper data.

FBTLIB253E

Required data could not be found in a Liberty request or response message.

Explanation
A required data item was not found in a Liberty request or response message, so the operation cannot be performed.

Administrator response
Enable a trace for detailed messages about the error, including which data item could not be found. Note that trace might need to be enabled on the provider of the Liberty message as well to determine why the message lacks the required data.

FBTLIB254E

Required data could not be found in the Liberty context.

Explanation
A required data item was not found in the Liberty context, so the operation cannot be performed.

Administrator response
Enable a trace for detailed messages about the error, including which data item could not be found.

FBTLIB255E

The issuer of the Liberty assertion (*AssertionIsuer*) did not match the issuer of the Liberty artifact (*ArtifactIssuer*).

Explanation
The Liberty assertion's issuer did not match the Liberty artifact's issuer. The assertion is ignored.

Administrator response
Enable a trace for detailed messages about the error. Verify that the configuration maps the succinct ID in the artifact to the correct provider.

FBTLIB256E

The Liberty Service implementation class (*ClassName*) is not valid.

Explanation
The Liberty Service implementation parameter is not valid.

Administrator response
Update the configuration. Ensure that the implementation class is a fully qualified Java class.

FBTLIB257E

The Liberty Service failed to validate the configuration.

Explanation
The Liberty Service failed to validate the configuration information.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB258E

The Liberty Service Factory failed to instantiate the service with the implementation class (*ClassName*).

Explanation
The Liberty Service Factory failed to instantiate the service implementation class.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB259E

No assertion or status information was found for artifact (*LibertyArtifact*).

Explanation
No information related to the specified artifact could be found.

Administrator response
Verify that the artifact is specified properly and that it has been used within the allowed assertion store timeout.

FBTLIB260E

The Liberty module failed to retrieve the service factory for the specified service key (*Service Key*).

Explanation
The Liberty module failed to retrieve the service factory.

Administrator response
Enable trace for detailed messages about the error. Verify that the configuration has the correct entry for the service factory and retry the operation.

FBTLIB261E

The Liberty module failed to retrieve a service instance using the service factory. (*ServiceFactory*).

Explanation
The Liberty module failed to retrieve a service instance.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB262E

The succinct ID in the artifact does not correspond to a configured provider.

Explanation
No provider was mapped to the succinct ID in the artifact. The artifact is ignored.

Administrator response
Enable a trace for detailed messages about the error, including which succinct ID is in the artifact. Verify that configuration has correct mappings for providers and their succinct IDs.

FBTLIB263E

The provider referenced by the succinct ID in the Liberty artifact (*ArtifactSuucinctIDProvider*) did not match the current provider (*SelfProvider*).

Explanation

The provider mapped to the succinct ID in the Liberty artifact did not match the current identity provider. The assertion request is ignored.

Administrator response

Enable a trace for detailed messages about the error. Verify that the configuration has the correct mappings for providers and their succinct IDs.

FBTLIB264E

The protocol action caught an unexpected exception while validating a Liberty artifact.

Explanation

The protocol action caught an unexpected exception outside of Liberty while validating a Liberty artifact.

Administrator response

Enable a trace for detailed messages about the error.

FBTLIB265E

The protocol action caught an unexpected exception while building a Liberty artifact.

Explanation

The protocol action caught an unexpected exception outside of Liberty while building a Liberty artifact.

Administrator response

Enable a trace for detailed messages about the error.

FBTLIB266E

The Liberty module caught an unexpected exception while serializing an object.

Explanation

The Liberty module caught an unexpected exception while serializing an object.

Administrator response

Enable a trace for detailed messages about the error.

FBTLIB267E

The Liberty module caught an unexpected exception while deserializing an object.

Explanation

The Liberty module caught an unexpected exception while deserializing an object.

Administrator response

Enable a trace for detailed messages about the error.

FBTLIB268E

The Liberty LogoutRequest could not be found.

Explanation
The Liberty LogoutRequest object, which is required to complete the operation, could not be found. If the operation was being performed on a service provider, the LogoutRequest should be in the Liberty context. If the operation was being performed on an identity provider, the LogoutRequest should be in the Liberty session.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB269E

The Protected Resource URL value could not be found in the Liberty Context object.

Explanation
The Protected Resource URL value, which is required to complete the operation, could not be found in the Liberty Context object.

Administrator response
Verify that the point of contact at the service provider is configured properly.

FBTLIB270E

The requested provider *provider* does not exist.

Explanation
The provider ID, which is required to initiate federation termination, could not be found.

Administrator response
Verify that the provider ID is correct and that the configuration specifies that provider ID.

FBTLIB271E

The profile specified for termination *profile* is not valid.

Explanation
The profile specified is not present or supported.

Administrator response
Verify that the profile URI is correct and that the configuration specifies that provider URI.

FBTLIB272E

The federation termination service URL specified for termination *url* is not valid.

Explanation
The URL specified is not present or supported.

Administrator response
Verify that the URL is correct and that the configuration specifies that provider URL.

FBTLIB273E

The federation termination service SOAP endpoint specified for termination *endpoint* is not valid.

Explanation
The URL specified is not present or supported.

Administrator response
Verify that the URL is correct and that the configuration specifies that provider URL.

FBTLIB274E

The federation termination service is missing a notification message.

Explanation
The notification message specified is not present or supported.

Administrator response
Verify that the message is correct and that the configuration specifies the provider URL and correct notification profile.

FBTLIB275E

The federation partner's service return URL, *endpoint* is missing or not valid.

Explanation
The termination service return URL specified is not present or supported.

Administrator response
Verify that the message is correct and that the configuration specifies the provider URL and service return URL.

FBTLIB276E

A response to an unsolicited federation termination was received.

Explanation
A request was received as a response to an unsolicited federation termination. This request will be ignored but could be due to the requestor not having cookies enabled. The configuration can override this default behavior.

Administrator response
Verify that the message is correct and that the configuration specifies the provider URL and service return URL.

FBTLIB277E

The ID service request to remove an alias for *userId* and provider *providerId* failed.

Explanation
The ID service operation was not successful.

Administrator response
Validate that the identity and provider are valid and check the log for messages returned from the ID service.

FBTLIB279E

The user's response to the consent to federate was not found in the browser query string.

Explanation
Internal Error: The Delegate protocol is unable to process the response because it could not retrieve the AuthnRequest from LibertyContext.

System action
The operation will be halted.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB280E

The register name identifier could not be performed. The user *user* does not have a required name identifier configured for provider *provider*.

Explanation
For a register name identifier request to be created, it is a requirement that the user has a name identifier for the partner.

Administrator response
Validate that the given user has a name identifier configured.

FBTLIB281E

The register name identifier request failed. The provider *provider* did not provide a name identifier in the register name identifier request.

Explanation
A name identifier is required in a register name identifier request.

Administrator response
Validate that the given provider is correctly formatting its register name identifier requests.

FBTLIB282E

The register name identifier could not be performed. The provider *provider* did not provide an old name identifier in the register name identifier request.

Explanation
A old name identifier is required in a register name identifier request.

Administrator response
Validate that the given provider is correctly formatting its register name identifier requests.

FBTLIB283E

Register name identifier request failed. The provider *provider* provided the old name identifier *old identifier* but the expected one was *expected old identifier*.

Explanation
The provided old name identifier did not match the current name identifier. The register name identifier request failed.

Administrator response
Validate that the given provider is correctly formatting its register name identifier requests.

FBTLIB284E

The register name identifier could not be performed. The provider *provider* does not have the required register name identifier endpoint configured.

Explanation
The given provider does not have the required register name identifier endpoint configured.

Administrator response
Validate that the given provider has a register name identifier endpoint configured.

FBTLIB285E

The register name identifier request for *userid* could not complete because the identity service was unavailable.

Explanation
The identity service was not available to complete the register name identifier request.

Administrator response
Validate that the identity service is configured into the environment and is functioning correctly.

FBTLIB286E

The register name identifier request for *userid* could not complete because an error was encountered during the modification of the alias in the registry.

Explanation
The identity service was not able to make the alias modification in the registry.

Administrator response
Check a trace log for a more specific error that will indicate what caused the problem.

FBTLIB287E

No register name identifier response message was given.

Explanation
The partner did not respond with a register name identifier message.

Administrator response
Ensure that the partner responds with correctly formatted messages.

FBTLIB288E

No provider identifier was given in the register name identifier response.

Explanation
The provider did not respond with a provider identifier.

Administrator response
Ensure that the provider responds with correctly formatted messages.

FBTLIB289E

The provider *provider* did not include a status in the register name identifier response.

Explanation
The provider given did not include a status or a correctly formatted status in its response.

Administrator response
Ensure that the provider responds with correctly formatted messages.

FBTLIB290E

No register name identifier request found in the session.

Explanation
When the provider returns a response, the original request is needed to complete the transaction.

Administrator response
Ensure that the browser has cookies enabled.

FBTLIB291E

The protocol action caught an unexpected exception while executing a local login.

Explanation
The protocol action caught an unexpected exception outside of Liberty while executing a local login.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB292E

The name identifier provided for federation termination, *identifier*, is not valid.

Explanation
The requestor sent a name identifier that was not valid for the principal.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB293E

A federation termination notification that was not valid was received.

Explanation
An attempt to decode the federation termination notification failed either because of schema violation or a signature failure.

Administrator response
Check a trace log for the message and ensure that it is correctly formatted, and validate the configured keys for the partner sending the notification.

FBTLIB294E

The federation termination notification could not be created because '*schemaMessage*'. The federation termination has not been performed.

Explanation
An attempt to encode the federation termination notification failed either because of schema violation or a signature failure.

Administrator response
Check a trace log for the message and ensure that it is correctly formatted, and validate the configured private key aliases.

FBTLIB295E

The register name identifier provided is not valid or could not be understood, because [*reason*]. The register name identifier has not been performed.

Explanation
An attempt to encode the register name identifier failed either because of a schema violation or a signature failure.

Administrator response
Check a trace log for the message and ensure that it is correctly formatted, and validate the configured private key aliases.

FBTLIB296E

There was no register name identifier request provided. The register name identifier has not been performed.

Explanation
There was no register name identifier request provided.

Administrator response
Ensure that the provider making the register name identifier request provides a request message.

FBTLIB297E

The register name identifier message could not be created because [*schemaMessage*]. The federation termination has not been performed.

Explanation
No register name identifier request was created because an error occurred.

Administrator response
Check a trace log for the message and ensure that it is correctly formatted, and validate the configured private key aliases.

FBTLIB300E

The identity service could not set the self or partner alias for user *user* and partner provider *provider*.

Explanation
The identity service encountered an error while storing alias data for the current local user.

Administrator response
Validate that the identity service is configured into the environment and is functioning correctly.

FBTLIB301E

A Liberty message was not included in the request to the SOAP endpoint.

Explanation
The message that was received by the SOAP endpoint did not include a Liberty message as a child of the SOAP body.

Administrator response
Validate that the partner that is sending messages to the SOAP endpoint is sending correctly formatted Liberty requests.

FBTLIB304E

The Delegate protocol is unable to obtain the AuthenticationURL endpoint.

Explanation
A required endpoint URL was not found in the configuration for the specified provider.

Administrator response
Verify that configuration files are present and have not been corrupted. If necessary, define the required endpoint URL for the provider in question.

FBTLIB305E

The name identifier to be used to determine the local user cannot be obtained from Liberty context.

Explanation
The name identifier that comes in the request is needed to determine the local identity of user. It might not have come in the request.

Administrator response
Turn on the provider tracing to check if the incoming request had name identifiers set.

FBTLIB306E

The protocol action caught an unexpected exception while attempting to get the user's local credentials.

Explanation
The protocol action caught an unexpected exception outside of Liberty while attempting to get the user's local credentials.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB307E

The protocol action caught an unexpected exception while executing.

Explanation
The protocol action caught an unexpected exception outside Liberty while executing.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB308E

The Liberty plug-in caught an unexpected exception when building the SOAP message.

Explanation
The Liberty plug-in caught an unexpected exception when building the SOAP message.

System action
Contact your IBM support representative.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB309E

The received message failed signature verification. The message was not signed by a trusted signer or was modified after signing.

Explanation
The received message was signed but signature verification failed.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages and validate configuration.

FBTLIB310E

The configured Liberty version is valid for the federation *federationId* with display name *federationName*.

Explanation
The Liberty version of the message is not supported by the Liberty runtime.

Administrator response
Verify that the providers in this provider's circle of trust operate at a compatible level of the Liberty protocol.

FBTLIB311E

The provider *provider* does not have an AssertionConsumerServiceURL endpoint configured with an ID of *id*.

Explanation
The configuration does not contain an AssertionConsumerServiceURL endpoint with the given identifier for the given provider.

System action
The request has been halted.

Administrator response
Ensure that the configuration is correct.

FBTLIB312E

The user *user* has authenticated with a one-time name identifier and cannot execute a register name identifier action.

Explanation
The user was issued a one-time name identifier during authentication. Register name identifier actions can be executed only when a user has been issued federated name identifiers.

System action
The request has been halted.

Administrator response
No action is required.

FBTLIB313E

The user *user* has authenticated with a one-time name identifier and cannot execute a defederation action.

Explanation
The user was issued a one-time name identifier during authentication. Federation termination actions can be executed only when a user has been issued federated name identifiers.

System action
The request has been halted.

Administrator response
No action is required.

FBTLIB314E

The user was not authenticated because a pre-existing logout request was found.

Explanation
The user was not authenticated because a pre-existing logout request was detected. This can happen if a user logs in but logs out of another federated site, and the logout message arrives before the authentication credentials.

System action
The request has been halted.

Administrator response
The user should log in again.

FBTLIB315E

No authentication request was found in the session.

Explanation
When a user authenticates, the authentication request message is stored and used to validate the corresponding response message. A response message was received, but there was not a request message, and so the unsolicited response is rejected.

System action
The request has been halted.

Administrator response
Enable a trace for detailed messages.

FBTLIB316E

The calculated proxy count value, *count*, is invalid.

Explanation
The calculated proxy count value must be at least one less than the original proxy count value. A pluggable proxy service has returned an invalid value. This limitation is specified by the Liberty Architecture.

System action
The request has been halted.

Administrator response
Install and configure a proxy service that will return a valid proxy count value, such as the default proxy service plug-in that is delivered with the product.

FBTLIB317E

The user cannot be authenticated directly or by proxy.

Explanation
The incoming authentication request forbids proxying of the request, and the identity provider cannot authenticate the user directly.

System action
The request has been halted.

Administrator response
The request should be retried permitting proxying, if possible. Otherwise, the request should be directed to another identity provider that is configured to authenticate users directly.

FBTLIB318E

No identity provider was found in configuration.

Explanation
No identity provider was configured as a partner to this provider.

System action
The request has been halted.

Administrator response
Verify that configuration files are present and have not been corrupted. If necessary, define one or more identity provider partners for this provider.

FBTLIB319E

The liberty version specified in the federation group configuration '*groupId*', self entity '*entity*' is invalid. Specify the correct values in the '*majorVersionProperty*' and '*minorVersionProperty*' properties. Current values MajorVersion: '*majorVersion*' MinorVersion: '*minorVersion*'

Explanation
An invalid liberty version is specified in the configuration.

System action
The liberty module could not be initialized.

Administrator response
Specify a valid liberty version in the configuration.

FBTLIB320E

The federation group type specified in the configuration is not supported. Group id: '*id*', Group display name: '*id*', federation group type '*type*'.

Explanation
The federation group defined is not a supported type.

System action
The Liberty Module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify a supported group type in the configuration.

FBTLIB321E

The *partnerEndpointType* endpoint for partner '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is invalid. Endpoint value '*displayName*'.

Explanation
The specified partner endpoint is invalid.

System action
The Liberty Module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify a valid endpoint value in the configuration.

FBTLIB322E

The *partnerEndpointType* endpoint for self '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is invalid. Endpoint value '*displayName*'.

Explanation
The specified self endpoint is invalid.

System action
The Liberty Module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify a valid endpoint value in the configuration.

FBTLIB323E

The *partnerEndpointType* endpoint is missing from the provider '*id*' and display name '*displayName*' configuration for federation group with ID '*id*' and display name '*displayName*'.

Explanation
A required endpoint is missing from the provider's configuration.

System action
The Liberty Module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify the required endpoint in the provider's configuration.

FBTLIB324E

The *propertyName* property is missing from the provider '*id*' and display name '*displayName*' configuration for federation group with ID '*id*' and display name '*displayName*'.

Explanation
A required property is missing from the provider's configuration.

System action
The Liberty Module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify the required property in the provider's configuration.

FBTLIB325E

The protocol profile value '*protocolProfileValue*' for protocol type '*protocolProfile*' specified for partner '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is invalid.

Explanation
The specified protocol profile value is invalid.

System action
The Liberty Module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify a valid protocol profile value in the configuration.

FBTLIB326E

The property value '*propertyValue*' for property '*propertyName*' specified for provider '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is invalid.

Explanation
The specified property value is invalid.

System action
The Liberty Module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify a valid property value in the configuration.

FBTLIB327E

The boolean property value '*propertyValue*' for property '*propertyName*' specified for provider '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is invalid. For boolean properties the permitted values are 'true' or 'false'.

Explanation
The specified boolean property value is invalid.

System action
The Liberty Module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify a valid boolean property value in the configuration.

FBTLIB328E

The numeric property value '*propertyValue*' for property '*propertyName*' specified for provider '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is invalid. The minimum value for this property is '*displayName*'.

Explanation
The specified numeric property value is invalid.

System action
The Liberty Module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify a valid numeric property value in the configuration.

FBTLIB329E

The Identity provider succinct id value '*propertyValue*' specified under property '*propertyName*' for provider '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is invalid. The identity provider succinct ID is a required property.

Explanation
The specified numeric property value is invalid.

System action
The Liberty Module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify a valid identity provider succinct ID value in the configuration.

FBTLIB330E

The common domain service host value '*commonDomainServiceHost*' specified using property '*propertyName*' for partner '*id*' and display name '*displayName*' for federation group with ID '*id*' and

display name '*displayName*' is invalid. The common domain service host must start with http:// or https:// and end with the common domain value '*displayName*'.

Explanation
The specified common domain service host is invalid.

System action
The Liberty Module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify a valid common domain service host in the configuration.

FBTLIB331E

The Identity provider succinct ID value '*propertyValue*' specified under property '*propertyName*' for provider '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' does not match the message digest of the provider ID.

Explanation
The specified identity provider succinct ID value is invalid.

System action
The Liberty Module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify a valid identity provider succinct ID value in the configuration.

FBTLIB332E

The proxy list is invalid.

Explanation
The proxy list used in a proxy authentication request must adhere to the Liberty specifications. A pluggable proxy service has returned an invalid proxy list.

System action
The request has been halted.

Administrator response
Install and configure a proxy service that will return a valid proxy list, such as the default proxy service plug-in that is delivered with the product.

FBTLIB333E

The '*propertyValue*' property is missing from the partner with provider ID '*providerId*' configuration.

Explanation
The specified property is missing from the partner configuration.

System action
The SOAP client could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Include the missing property in the partner configuration.

FBTLIB334E

The authentication request contained a RequestAuthnContext element which is not supported by this identity provider.

Explanation
This version of the product does not support RequestAuthnContext elements in authentication requests. Any request containing a RequestAuthnContext cannot be processed.

System action
The request has been halted.

Administrator response
No action is necessary on the identity provider. If possible, configure the service provider to issue authentication requests that do not include a RequestAuthnContext element.

FBTLIB335E

Internal Error: The delegate protocol cannot retrieve the AuthnRequest from incoming HTTP POST.

Explanation
Internal Error: The delegate protocol cannot retrieve the AuthnRequest from incoming HTTP POST.

System action
Contact your IBM support representative.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB336E

Internal Error: The Delegate protocol is unable to process the request because it could not convert the liberty request to an XML string.

Explanation
Internal Error: The Delegate protocol is unable to process the request because it could not convert the liberty request to an XML string.

System action
Contact your IBM support representative.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB337E

Internal Error: The Delegate protocol is unable to convert the request from an XML string to BASE64 encoded data.

Explanation
Internal Error: The Delegate protocol is unable to convert the request from an XML string to BASE64 encoded data.

System action
Contact your IBM support representative.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB338E

Internal Error: The Delegate protocol is unable to convert the request from BASE64 encoded data to an XML string.

Explanation
Internal Error: The Delegate protocol is unable to convert the request from BASE64 encoded data to an XML string.

System action
Contact your IBM support representative.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB339E

Internal Error: The Delegate protocol is unable to process the request because it couldn't parse the liberty request XML string.

Explanation
Internal Error: The Delegate protocol is unable to process the request because it couldn't parse the liberty request XML string.

System action
Contact your IBM support representative.

Administrator response
Enable a trace for detailed messages about the error.

FBTLIB340E

The maximum amount of authentication attempts *authenticationAttempts* has been reached. Please verify that the Access Control Lists are specified correctly. The *authenticationURL* URL needs to be a protected endpoint.

Explanation
The user has exhausted the amount of attempts to authenticate.

System action
Verify the point of contact configuration.

Administrator response
Verify that the Access Control Lists are specified correctly.

Chapter 14. Logging messages

These messages are provided by the logging component.

FBTLOG001E

The logging configuration file was not found.

Explanation
The system could not find the file containing the logging configuration data.

System action
The system will revert to default settings.

Administrator response
Ensure that the configuration file exists and is in the classpath of the application.

FBTLOG002W

An integer was expected.

Explanation
The system expected an argument of integer type.

System action
The system will revert to a hardcoded value (5000).

Administrator response
Ensure that the argument is the correct type.

FBTLOG003W

An EventLevel was expected.

Explanation
The system expected one of the following: DEBUG_MIN, DEBUG_MID, DEBUG_MAX.

System action
The system will revert to DEBUG_MIN.

Administrator response
Ensure that the argument is valid.

FBTLOG004W

An EventType was expected.

Explanation
The system expected one of the following: INFO_TYPE, WARN_TYPE, ERROR_TYPE, ALL_MSG_TYPE, TRACE_TYPE, AUDIT_TYPE.

System action
The system will revert to ALL_MSG_TYPE.

Administrator response
Ensure that the argument is valid.

FBTLOG005E

An error occurred while saving the configuration.

Explanation
The system could not write the configuration file.

System action
The configuration will not be saved.

Administrator response
Ensure that the configuration file is in the correct location and is writable.

FBTLOG006E

An error occurred during the loading of the logging configuration.

Explanation
The system could not read from the file containing the logging configuration data.

System action
The system will revert to default settings.

Administrator response
Ensure that the configuration file exists and is in the classpath of the application.

FBTLOG007E

The management context was not valid. The changes could not be committed during this session.

Explanation
The management context was invalidated probably because a commit occurred elsewhere.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG008E

An exception was received during the commit process. The changes could not be committed during this session.

Explanation
The management component caught an exception thrown while trying to commit the changes.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG009E

An exception was received during a getMaxMsgFileSize operation.

Explanation
An exception was received during the retrieveMaxMsgFileSize operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG010E

An exception was received during a retrieveMaxTraceFileSize operation.

Explanation
An exception was received during the retrieveMaxMsgFileSize operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG011E

An exception was received during a retrieveMsgType operation.

Explanation
An exception was received during the retrieveMsgType operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG012E

An exception was received during a retrieveTraceLevel operation.

Explanation
An exception was received during the retrieveTraceLevel operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG013E

Required parameters were missing.

Explanation
A required parameter was missing from the argument map.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG014E

An exception was received during a retrieveTracing operation.

Explanation
An exception was received during a retrieveTracing operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG015E

An exception was received during a retrieveAuditLevel operation.

Explanation
An exception was received during a retrieveAuditLevel operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG016E

An exception was received during a retrieveMaxAuditFileSize operation.

Explanation
An exception was received during the retrieveMaxAuditFileSize operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG017E

An exception was received during a retrieveLogHomeDir operation.

Explanation
An exception was received during the retrieveLogHomeDir operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG018E

An exception was retrieved during a retrieveProductName operation.

Explanation
An exception was received during the retrieveProductName operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG019E

An exception was received during a retrieveTivoliCommonDir operation.

Explanation
An exception was received during the retrieveTivoliCommonDir operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG020E

An exception was received during a modifyMaxMsgFileSize operation.

Explanation
An exception was received during the modifyMaxMsgFileSize operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG021E

An exception was received during a modifyMaxTraceFileSize operation.

Explanation
An exception was received during the modifyMaxTraceFileSize operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG022E

An exception was received during a modifyMsgType operation.

Explanation
An exception was received during the modifyMsgType operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG023E

An exception was received during a modifyTraceLevel operation.

Explanation
An exception was received during the modifyTraceLevel operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG024E

An exception was received during a modifyTracing operation.

Explanation
An exception was received during the modifyTracing operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG025E

An exception was received during a modifyAuditLevel operation.

Explanation
An exception was received during the modifyAuditLevel operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG026E

An exception was received during a modifyMaxAuditFileSize operation.

Explanation
An exception was received during the modifyMaxAuditFileSize operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG027E

An exception was received during a modifyLogHomeDir operation.

Explanation
An exception was received during the modifyLogHomeDir operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG028E

An exception was received during a modifyProductName operation.

Explanation
An exception was received during the modifyProductName operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG029E

An exception was received during a modifyTivoliCommonDir operation.

Explanation
An exception was received during the modifyTivoliCommonDir operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG030E

An exception was received during a retrieveComponentList operation.

Explanation
An exception was received during the retrieveComponentList operation.

System action
The system will revert back to the previous settings.

Administrator response
Create a new session and attempt the operation again.

FBTLOG037E

The component identifier is null.

Explanation
The component identifier specified in a request to initialize logging is null.

System action
The logging initialization request is ignored.

Administrator response
This is an internal programming error. Report this problem and the invocation stack dump found in SystemErr.log to your IBM service representative.

FBTLOG038E

Invalid class name provided for constructing a logger: *parameter*

Explanation

The class name provided for constructing a logger should be a full package-qualified class name beginning with com.tivoli.am.fim.

System action

The logger has not been created.

Administrator response

This is an internal programming error. Report this problem and the invocation stack dump found in SystemErr.log to your IBM service representative.

Chapter 15. Multi-Factor Authentication messages

These messages are provided by the Mobile Multi-Factor Authentication component.

FBTMFA001E

A required parameter *parameter name* is missing or invalid.

Explanation
The current request is not valid.

System action
The request is rejected.

Administrator response
Ensure that the JSON parameter value is present and valid.

FBTMFA002E

The authenticator [*authenticator*] was not found.

Explanation
An attempt was made to retreive or modify authenticator information and the authenticator was not found.

System action
The request is rejected.

Administrator response
Verify that the authenticator exists.

FBTMFA003E

The authentication method [*authenticator*] was not found.

Explanation
An attempt was made to retreive or modify authentication method information and the authentication method was not found.

System action
The request is rejected.

Administrator response
Verify that the authentication method exists.

FBTMFA004E

There was no authenticator found for the given access token.

Explanation
An attempt was made to retreive or modify authenticator information and no authenticator was found.

System action
The request is rejected.

Administrator response
Verify that the authenticator exists.

FBTMFA005E

The retrieval of the resource failed.

Explanation
During the retrieval operation an internal server error occured.

System action
See the exception in the logs for the cause.

Administrator response
Ensure that the resource and action requested are valid.

FBTMFA006E

The delete of the resource failed.

Explanation
During the delete operation an internal server error occured.

System action
See the exception in the logs for the cause.

Administrator response
Ensure that the resource and action requested are valid.

FBTMFA007E

The update of the resource failed.

Explanation
During the update operation an internal server error occured.

System action
See the exception in the logs for the cause.

Administrator response
Ensure that the resource and action requested are valid.

FBTMFA008E

The creation of the resource failed.

Explanation
During the creation operation an internal server error occured.

System action
See the exception in the logs for the cause.

Administrator response
Ensure that the resource and action requested are valid.

FBTMFA009E

The signature validation failed.

Explanation
The server encountered an error while attempting to validate a signature.

System action
See the exception in the logs for the cause.

Administrator response
Ensure that the resource and action requested are valid.

FBTMFA010E

The request failed because the request body contains improperly structured JSON.

Explanation
The request could not be processed because the request body contains malformed or improperly structured JSON.

System action
See the exception in the logs for the cause.

Administrator response
Ensure that the request body contains the appropriately structured JSON for the requested action.

FBTMFA011E

The authenticator was not found.

Explanation
An attempt was made to retreive or modify authenticator information and the authenticator was not found.

System action
The request is rejected.

Administrator response
Verify that the authenticator exists.

FBTMFA012E

The authentication method was not found.

Explanation
An attempt was made to retreive or modify authentication method information and the authentication method was not found.

System action
The request is rejected.

Administrator response
Verify that the authentication method exists.

FBTMFA013E

An authentication method of type *type* already exists.

Explanation
An attempt was made to add an authentication method but a method with that type already exists.

System action
The request is rejected.

Administrator response
Ensure that the resource and action requested are valid.

FBTMFA014E

No push notification API credential registration exists for mobile app identifier *appId* and platform *platform*.

Explanation
An attempt was made to read push notification service credentials that do not exist.

System action
The request is rejected and no mobile push notifcation can be sent.

Administrator response
Ensure that the push notification API credentials have been configured for the mobile application.

FBTMFA015E

A database error occurred trying to read push notification service credential data for mobile app identifier *appId* and platform *platform*.

Explanation
A database error occurred trying to read push notification service credential data.

System action
The request is rejected.

Administrator response
Ensure that the push notification API credentials have been configured for the mobile application and that the database is available.

FBTMFA016E

An attempt has been made to create a *platform* notification service client object with null configuration data.

Explanation
A push notification service client requires configuration data.

System action
The request is rejected.

Administrator response
Ensure that the push notification API credentials have been configured for the mobile application and that the database is available.

FBTMFA017E

The *platform* push notification service data attribute *attribute* is missing or is not valid.

Explanation
A push notification service client requires configuration data.

System action
The request is rejected.

Administrator response
Ensure that the push notification API credentials have been configured for the mobile application and that the database is available.

FBTMFA018E

An attempt has been made to send a mobile push notification with an invalid notification object.

Explanation
A push notification object must not be null.

System action
The request is rejected.

Administrator response
Ensure the notification has been correctly created.

FBTMFA019E

The mobile push notification does not contain a valid target device object.

Explanation
The target device data object identifies the mobile device to be notified and must not be null.

System action
The request is rejected.

Administrator response
Ensure the notification has been correctly created and that mobile device registrations are correct.

FBTMFA020E

The mobile push notification does not contain a valid payload.

Explanation
The notification payload must not be null.

System action
The request is rejected.

Administrator response
Ensure the notification has been correctly created.

FBTMFA021E

The mobile push notification target device data attribute *attribute* is missing or is not valid.

Explanation
A push notification requires a correctly identified target device.

System action
The request is rejected.

Administrator response
Ensure that the mobile device registrations are valid.

FBTMFA022E

The mobile push notification payload attribute *attribute* is missing or is not valid.

Explanation
A push notification requires a correctly formated payload.

System action
The request is rejected.

Administrator response
Ensure that the mobile push notification payload is valid.

FBTMFA023E

The mobile push notification with identifier *attribute* does not match response identifier *attribute*.

Explanation
The push notification and response identifier do not match.

System action
The request is rejected.

Administrator response
Enable additional diagnostic trace.

FBTMFA024E

An internal error has occurred while performing the requested operation: *internalMsg*.

Explanation
An internal error occurred while performing an action for MMFA. The error message and previous log message indicate the cause.

System action
The request is rejected.

Administrator response
Enable additional diagnostic trace.

FBTMFA025E

A push notifcation was requested but an authenticator to receive the notification has not been selected. Please select a registered authenticator.

Explanation
A push notification can only be sent to a registered authenticator that has been selected to received the notification.

System action
The request is rejected.

Administrator response
Enable additional diagnostic trace.

FBTMFA026E

The authenticator *deviceId*: *description* has not registered a valid push notification service token.

Explanation
A push notification can only be sent to a registered authenticator that has been selected to received the notification.

System action
The request is rejected.

Administrator response
Reregister the authenticator.

FBTMFA027E

The authenticator *deviceId*: *description* has not registered a valid mobile application identifier.

Explanation
A push notification can only be sent to a registered authenticator that has been selected to received the notification and has registered its application identifier.

System action
The request is rejected.

Administrator response
Reregister the authenticator.

FBTMFA028E

The authenticator *deviceId*: *description* has not registered a valid or supported device type: *type* .

Explanation
A push notification can only be sent to a registered authenticator that has been selected to received the notification and has registered its device type.

System action
The request is rejected.

Administrator response
Reregister the authenticator.

FBTMFA029E

An error occurred while preparing to send a notification to device *deviceId*: *description* : *error*.

Explanation
An error occurred during preparation for push notification. See the error message for details

System action
The request is rejected.

Administrator response
Enable additional diagnostic trace.

FBTMFA030E

The push notification API credential registration for for mobile app identifier *appId* and platform *platform* does not include a supported provider type: *provType*.

Explanation
The provider type must be set to a supported type. Currently supported provider types are 'apple', 'firebase'.

System action
The request is rejected and no mobile push notifcation can be sent.

Administrator response
Ensure that the push notification API credentials have been configured correctly for the mobile application.

FBTMFA031E

An attempt to send a push notification to mobile device ID *deviceId deviceDesc* has failed with the following error message: *msg*.

Explanation
A call to the push notification provider API has failed.

System action
The request is rejected and no mobile push notifcation can be sent.

Administrator response
Ensure that the push notification API credentials have been configured correctly for the mobile application.

FBTMFA032E

An attempt to send a push notification to mobile device ID *deviceId* with application ID *appId* has failed because the HTTP response is null. This can be the result of invalid configuration of push notification service providers or network connectivity problems.

Explanation
A call to the push notification provider API has failed.

System action
The request is rejected and no mobile push notifcation can be sent.

Administrator response
Ensure that the push notification API credentials have been configured correctly for the mobile application and network connectivity exists to the push notification service provider.

FBTMUA000E

Internal Error. Contact the System Administrator.

Explanation
An internal error occurred.

System action
The application encountered an error, process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTMUA100E

The authentication method type for the mobile user approval mechanism is missing or not valid.

Explanation
The mobile user approval mechanism requires an authentication method type to retrieve registered methods.

System action
None.

Administrator response
None.

FBTMUA101E

No [*type*] authentication methods have been registered or enabled on the authenticator.

Explanation
An attempt was made to authenticate via the mobile user approval authentication mechanism and no registered or enabled authentication methods were found.

System action
None.

Administrator response
None.

FBTMUA102E

The mobile user approval authentication mechanism failed to decode the signed challenge.

Explanation
The signed challenge must be represented in Base64 format.

System action
None.

Administrator response
None.

FBTMUA103E

The mobile user approval authentication mechanism failed to validate the submitted signed challenge.

Explanation
The server challenge must be signed by the user's private key associated with one of the registered key handles.

System action
None.

Administrator response
None.

FBTMUA104E

No authenticator has been registered or enabled for the given access token.

Explanation
An attempt was made to authenticate via the mobile user approval authentication mechanism and no registered or enabled authenticator was found.

System action
None.

Administrator response
None.

FBTMUA105E

The pending transaction expired before verification was completed.

Explanation
An attempt was made to authenticate via the mobile user approval authentication mechanism but the pending transaction expired.

System action
None.

Administrator response
None.

FBTSAR100E

The mechanism property *property* is invalid.

Explanation
The mechanism configuration isn't valid.

System action
The mechanism is not properly configured, process has been halted.

Administrator response
Check the value of the incorrectly set property.

FBTSAR101E

User session invalid. Attribute *property* doesn't exist.

Explanation
The mechanism configuration isn't valid.

System action
The session is not valid, process has been halted.

Administrator response
Check the user credential to ensure the correct attribute exists.

FBTSAR102E

The SMTP connection had the error: *property*.

Explanation
The SMTP configuration isn't valid.

System action
The SMTP server connection is not properly configured, process has been halted.

Administrator response
Check the value of the incorrectly set SMTP connection.

FBTU2F012E

The authentication validation failed.

Explanation
The server encountered an error while attempting to validate an authentication.

System action
See the exception in the logs for the cause.

Administrator response
Ensure that the resource and action requested are valid.

FBTRBA455E

The account locked status could not be retrieved for user [*user*].

Explanation
The user account locked status could not be retrieved.

System action
The user account locked status was not retrieved.

Administrator response
No action necessary.

FBTRBA456E

The user account locked status could not be updated for user [*user*].

Explanation
The user account locked status could not be updated.

System action
The user account locked status was not updated.

Administrator response
No action necessary.

FBTU2F001E

A required parameter *parameter name* is missing or invalid.

Explanation
The current request is not valid.

System action
The request is rejected.

Administrator response
Ensure that the JSON parameter value is present and valid.

FBTU2F002E

The token [*token*] was not found.

Explanation
An attempt was made to retreive or modify token information and the token was not found.

System action
The request is rejected.

Administrator response
Verify that the token exists.

FBTU2F003E

The retrieval of the resource failed.

Explanation
During the retrieval operation an internal server error occured.

System action
See the exception in the logs for the cause.

Administrator response
Ensure that the resource and action requested are valid.

FBTU2F004E

The delete of the resource failed.

Explanation
During the delete operation an internal server error occured.

System action
See the exception in the logs for the cause.

Administrator response
Ensure that the resource and action requested are valid.

FBTU2F005E

The update of the resource failed.

Explanation
During the update operation an internal server error occured.

System action
See the exception in the logs for the cause.

Administrator response
Ensure that the resource and action requested are valid.

FBTU2F006E

The creation of the resource failed.

Explanation
During the creation operation an internal server error occured.

System action
See the exception in the logs for the cause.

Administrator response
Ensure that the resource and action requested are valid.

FBTU2F007E

The signature validation failed.

Explanation
The server encountered an error while attempting to validate a signature.

System action
See the exception in the logs for the cause.

Administrator response
Ensure that the resource and action requested are valid.

FBTU2F008E

The registration validation failed.

Explanation
The server encountered an error while attempting to validate a registration.

System action
See the exception in the logs for the cause.

Administrator response
Ensure that the resource and action requested are valid.

FBTU2F009E

The request failed because the request body contains improperly structured JSON.

Explanation
The request could not be processed because the request body contains malformed or improperly structured JSON.

System action
See the exception in the logs for the cause.

Administrator response
Ensure that the request body contains the appropriately structured JSON for the requested action.

FBTU2F010E

The attestation certificate validation failed.

Explanation
The server encountered an error while attempting to validate an attestation certificate.

System action
See the exception in the logs for the cause.

Administrator response
Ensure that the resource and action requested are valid.

FBTU2F011E

An internal error has occurred while performing the requested operation: *internalMsg*.

Explanation
An internal error occurred while performing an action for U2F. The error message and previous log message indicate the cause.

System action
The request is rejected.

Administrator response
Enable additional diagnostic trace.

FBTOAU256E

Pending. The user code is not yet verified.

Explanation
The user code has not yet been approved by a user. Visit the verification URI to verify the user code.

System action
The request is not processed.

Administrator response
Verify the user code and retry.

SCIIS0020E

The LDAP connection has not been defined. (0x370d8014)

Explanation
A request was made with an invalid SCIM configuration. An LDAP connection is required.

Administrator response
Check to ensure that an LDAP connection has been defined in the SCIM configuration.

SCIIS0021E

There are no LDAP server connections defined. (0x370d8015)

Explanation
A request was made with an invalid SCIM configuration. A server connection is required.

Administrator response
Check to ensure that an LDAP server connection has been defined.

SCIIS0022E

The configured server connection contains no LDAP servers. (0x370d8016)

Explanation
A request was made with an invalid SCIM configuration. An LDAP server is required in the server connection.

Administrator response
Check to ensure that an LDAP server has been defined in the server connections.

SCIIS0023E

The configured LDAP connection was not found in the server connection list. (0x370d8017)

Explanation
A request was made with an invalid SCIM configuration. The configured LDAP connection is not a valid server connection.

Administrator response
Check to ensure that the LDAP connection defined in the SCIM configuration is valid.

SCIIS0024E

The server referenced by the specified LDAP connection could not be contacted. (0x370d8018)

Explanation
The LDAP server referenced by the SCIM configuration is not available.

Administrator response
Check to ensure that the LDAP server defined in the SCIM configuration is available.

FBTCID001E

User not found.

Explanation
The user was not found

System action
See the logs for the cause.

Administrator response
Ensure that the user exists in IBM Security Verify.

FBTCID002E

Retrieving authentication methods failed.

Explanation
An attempt was made to retreive authentication methods but the request failed.

System action
See the logs for the cause.

Administrator response
Verify connection to IBM Security Verify.

FBTCID003E

Registration failed.

Explanation
An attempt was made to perform registration but the request failed.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTCID004E

Registration failed:

Explanation
An attempt was made to perform registration but the request failed.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTCID005E

No OTP delivery detail provided.

Explanation
An attempt was made to perform a request but the OTP delivery detail was missing.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTCID006E

No type provided.

Explanation
An attempt was made to perform a request but the type was missing.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTCID007E

Validation failed.

Explanation
An attempt was made to perform validation but the request failed.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTCID008E

Validation failed:

Explanation
An attempt was made to perform validation but the request failed.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTCID009E

No OTP provided.

Explanation
An attempt was made to perform a request but the OTP was missing.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTCID010E

No ID provided.

Explanation
An attempt was made to perform a request but the ID was missing.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTCID011E

No validation ID provided.

Explanation
An attempt was made to perform a request but the validation ID was missing.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTCID012E

No verification ID provided.

Explanation
An attempt was made to perform a request but the verification ID was missing.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTCID013E

Update failed.

Explanation
An attempt was made to perform an update but the request failed.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTCID014E

Update failed:

Explanation
An attempt was made to perform an update but the request failed.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTCID015E

Removal failed.

Explanation
An attempt was made to perform removal but the request failed.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTCID016E

Removal failed:

Explanation
An attempt was made to perform removal but the request failed.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTCID017E

Verification failed.

Explanation
An attempt was made to perform verification but the request failed.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTCID018E

Verification failed:

Explanation
An attempt was made to perform verification but the request failed.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTCID019E

Could not create transacton.

Explanation
An attempt was made to create a transaction but the request failed.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTCID020E

Could not create verification.

Explanation
An attempt was made to create a verification but the request failed.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTCID021E

Could not create validation.

Explanation
An attempt was made to create a validation but the request failed.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTCID022E

Login failed. You have used an invalid user name or password.

Explanation
An attempt was made to login but the request failed.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTCID023E

The action provided was invalid for this mechanism.

Explanation
An attempt was made with an action that was not valid.

System action
See the logs for the cause.

Administrator response
Ensure that the request and action requested are valid.

FBTKQA114E

incorrect incorrect attempt(s) have been made. You have no attempts remaining. Please contact administrator to unlock your account.

Explanation
There are no more remaining attempts and account has been locked indefinitely.

System action
The request has been halted.

Administrator response
Contact an administrator to unlock the account.

FBTMUA106E

The authenticator attempting to complete the transaction does not match the selected authenticator.

Explanation
An attempt was made to authenticate via the mobile user approval authentication mechanism with an authenticator which is different to the authenticator previously selected.

System action
None.

Administrator response
None.

FBTOAU254E

The presented URI to be registered is not valid.

Explanation
Present a correctly formatted URI, ensure it includes a scheme.

System action
The request is rejected.

Administrator response
Correctly form the request.

FBTOAU255E

The client registration request failed. Check the log for details.

Explanation
Check the format of the request and connectivity to the database. Check that the clientId was not already registered.

System action
The request is rejected.

Administrator response

Correctly form the request.

Chapter 16. OAuth 2.0 messages

These messages are provided by the OAuth 2.0 component.

FBTOAU201E

The response type is not supported.

Explanation
The response_type parameter received in the request has an unsupported value.

System action
The request is rejected.

Administrator response
Ensure that the response_type parameter is one of the following: - code - token - a valid extension response type

FBTOAU202E

The required parameter: [*name*] was not found in the request.

Explanation
A required parameter for this request type was not found in the received request

System action
The request is rejected.

Administrator response
Ensure that the request contains all of the required parameters.

FBTOAU203E

The client identifier could not be found.

Explanation
The client identifier in the request does not match any registered client.

System action
The request is rejected.

Administrator response
Ensure that the client is valid and is registered correctly.

FBTOAU204E

An invalid client assertion or client secret was provided for the client identifier.

Explanation
The client secret in the request does not match the secret registered for this client.

System action
The request is rejected.

Administrator response
Ensure that the client secret is valid for this client.

FBTOAU205E

The preferred client provider class: [*preferred_provider*] could not be loaded, falling back on the default client provider class: [*default_provider*].

Explanation
The preferred client provider class could not be found.

System action
The default client provider class is used.

Administrator response
Check that the preferred client provider class is present.

FBTOAU207E

The browser request could not be converted into an STSUU because: [*message*].

Explanation
The process of converting an HTTP request to an STSUU failed.

System action
The request is rejected.

Administrator response
Ensure that the request has been properly constructed.

FBTOAU209E

The token request with applies to: [*applies_to*] and issuer: [*issuer*] failed.

Explanation
The token exchange failed.

System action
The request is rejected.

Administrator response
Ensure that your OAuth 2.0 trust chains have been correctly configured.

FBTOAU210E

The redirection URI provided in the request is either invalid, or does not meet matching criteria against the registered redirection URI.

Explanation
An invalid redirection URI was provided.

System action
The request is rejected.

Administrator response
Ensure that you have provided the correct redirection URI.

FBTOAU211E

The [*type*] received of type [*sub_type*] does not exist.

Explanation
An invalid grant/token was provided.

System action
The request is rejected.

Administrator response
Check that the grant/token being provided is valid.

FBTOAU214E

The [*type*] received of type [*sub_type*] does not belong to the client attempting to use it.

Explanation
An invalid grant/token was provided.

System action
The request is rejected.

Administrator response
Check that the grant/token being provided is valid.

FBTOAU215E

The grant type is not supported.

Explanation
The grant_type parameter received in the request has an unsupported value.

System action
The request is rejected.

Administrator response
Ensure that the grant_type parameter is one of the following: - authorization_code - refresh_token - a valid extension grant type

FBTOAU216E

The runtime could not load the OAuth 2.0 extension module with ID: [*moduleID*] for the extension point: [*extension*] . Instead the default module will be loaded with ID: [*defaultID*].

Explanation
The configuration specifies a module ID which could not be loaded by the runtime plugin manager.

System action
A default module will be loaded instead.

Administrator response
Validate that the plugin containing the specified module is deployed to the runtime.

FBTOAU217E

You are not authorized to access this protected resource.

Explanation
This resource can only be access by an authorized user.

System action
The request is rejected.

Administrator response
Ensure that the authorization endpoint has been properly configured and secured.

FBTOAU218E

The user denied consent to the protected resource.

Explanation
The user denied authorization to the OAuth 2.0 client.

System action
Inform the client of the decision.

Administrator response
None.

FBTOAU219E

The scope requested in the access token request exceeds the scope granted by the resource owner.

Explanation
The client has requested an access token with greater scope then that granted.

System action
The request is rejected.

Administrator response
Ensure the client is not requesting too great a scope in it's token request.

FBTOAU220E

The authenticated client id: [*username*] does not match the client id in the request body.

Explanation
The client's authenticated username does not match the client id it provided in the request body.

System action
The request is rejected.

Administrator response
Ensure that the authenticated username matches the client id.

FBTOAU222E

The client's registered redirection URI is not a valid absolute URI.

Explanation
The client's configured redirection URI is invalid.

System action
The request is rejected.

Administrator response
Ensure that your client is configured correctly.

FBTOAU223E

The received redirection URI does not match the redirection URI that this grant was issued to.

Explanation
The redirection URI in the request is no the same as the redirection URI used in the request for the authorization grant.

System action
The request is rejected.

Administrator response
Ensure the same redirection URI is used when requesting an authorization grant and using an authorization grant.

FBTOAU224E

The runtime cannot load the OAuth 2.0 trusted clients manager module with ID: [*moduleID*]. The default module with ID: [*defaultModuleID*] loads instead.

Explanation
The runtime plug-in manager cannot load the module ID specified during configuration.

System action
A default trusted clients manager module loads instead.

Administrator response
Validate that the module ID configured for the OAuth trusted clients manager and plug-in which contains the specified module are deployed to the runtime.

FBTOAU225E

The authorization delegate received a consent page form verifier that was not valid compared to the verifier in the user's session.

Explanation
The consent page form verifier sent to the authorization delegate was not valid compared to the verifier contained in the user's session.

System action
The browser displays an error page and the operation stops.

Administrator response
Ensure that the consent page form verifier parameter submitted matches that set by the intial authorization delegate request.

FBTOAU226E

The authorization delegate received consent form data that contained OAuth 2.0 parameters.

Explanation
The consent page form returned one or more OAuth 2.0 parameters such as client_id, redirect_uri, response_type or state.

System action
The browser displays an error page and the operation stops.

Administrator response
Ensure that the consent page form does not contain OAuth 2.0 parameters such as client_id, redirect_uri, response_type or state.

FBTOAU227E

Multiple values of the OAuth 2.0 protocol parameter: [*request_parameter*] were found in the request.

Explanation
OAuth 2.0 protocol parameters may not occur more then once in the request.

System action
The request is rejected.

Administrator response
Make sure that OAuth 2.0 request parameters do not occur more then once in the request.

FBTOAU228E

The request included multiple client credentials.

Explanation
OAuth 2.0 protocol requests may not include multiple client credentials, for example client credentials in both the BA header and the request body.

System action
The request is rejected.

Administrator response
Make sure that OAuth 2.0 request did not include client credentials in more then one place, for example, in the BA header and the request body.

FBTOAU229E

Confidential clients accessing the token endpoint must authenticate using their registered credentials.

Explanation
A confidential client attempted to access the token endpoint without authenticating.

System action
The request is rejected.

Administrator response
Ensure any confidential clients accessing the token endpoint present their client credentials.

FBTOAU230E

The client credentials flow is restricted to confidential clients.

Explanation
A public client attempted to use the client credentials grant type, this grant type is restricted to confidential clients.

System action
The request is rejected.

Administrator response
Ensure public clients are not attempting to use the client credentials grant type.

FBTOAU231E

The token endpoint is not configured to allow public client access.

Explanation
A public client attempted to access a token endpoint that has been configured to only allow confidential clients.

System action
The request is rejected.

Administrator response
If you wish to allow public clients to access the token endpoint, it must be configured on the federation page in the TFIM management console.

FBTOAU232E

The client MUST use the HTTP POST method when making access token requests.

Explanation
A client attempted to make an access token request without using the HTTP POST method.

System action
The request is rejected.

Administrator response
Ensure that all requests to the OAuth 2.0 token endpoint use the HTTP POST method.

FBTOAU233E

Maximum number of access token per user per client was reached

Explanation
There is limit on the number of access token distributed per user per client. You can set the limit in the API Protection definition.

System action
The request is rejected.

Administrator response
Increase the access token per user per client limit in the API Protection definition of the client.

FBTOAU234E

Submitted PIN is wrong.

Explanation
PIN policy is enabled for the refresh token. PIN received in the request does not match.

System action
The request is rejected.

Administrator response
Prompt the user to enter the correct password.

FBTOAU235E

The provided PIN does not match the PIN length setting in API Protection definition.

Explanation
The PIN length is different from the PIN length setting in API Protection definition.

System action
The request is rejected.

Administrator response
Submit a PIN with the correct length.

FBTOAU236E

A PIN must be provided to protect the refresh token.

Explanation
PIN policy is enabled in the API Protection definition, but a PIN was not provided.

System action
The request is rejected.

Administrator response
Submit a PIN in the request.

FBTOAU237E

The provided PIN contains invalid characters.

Explanation
A PIN should only contain numbers.

System action
The request is rejected.

Administrator response
Submit a PIN containing only numbers.

FBTOAU238E

The API Protection definition is not attached to the requested resource.

Explanation
The API Protection definition should be attached to the resource.

System action
The request is rejected.

Administrator response
Attach the API Protection definition to the resource.

FBTOAU239E

An invalid token was provided for the client: [*username*].

Explanation
The token in the request was not valid for this client.

System action
The request is rejected.

Administrator response
Ensure that the token is valid for this client.

FBTOAU240E

The client MUST use the HTTP POST OR GET method when making requests to this endpoint.

Explanation
A client attempted to make an endpoint without using the HTTP POST or GET method.

System action
The request is rejected.

Administrator response
Ensure that all requests to the OAuth 2.0 endpoint use the HTTP POST or GET method.

FBTOAU241E

An error was encountered building a JWT: *jwt_error*

Explanation
The call to the STS returned an error.

System action
The browser displays an error page and the operation stops.

Administrator response
Ensure that JWT configuration for this OAuth definition is correct.

FBTOAU242E

The required parameter: [*name*] was invalid or not found in the STSUU when building a JWT.

Explanation
A required parameter for this request type was not found in the STSUU when building a JWT.

System action
The request is rejected.

Administrator response
Ensure that the request contains all of the required parameters.

FBTOAU243E

Prompt parameter value none cannot be combined with other value.

Explanation
Prompt parameter must not contain none with any other value.

System action
The request is rejected.

Administrator response
Ensure that the request prompt parameter none is not combined with any other value.

FBTOAU244E

An invalid prompt value was provided.

Explanation
The prompt parameter value is not valid.

System action
The request is rejected.

Administrator response
Ensure that the request prompt parameter value is either none, login or consent.

FBTOAU245E

Login is required.

Explanation
The request cannot be processed further without authentication.

System action
The request is rejected.

Administrator response
This is expected behavior when prompt value is none and user is not authenticated.

FBTOAU246E

Consent is required.

Explanation
The request cannot be processed futher without user consent.

System action
The request is rejected.

Administrator response
Check on the request prompt parameter value and Trusted Client behavior setting.

FBTOAU247E

Unable to determine which redirection URI to use at runtime.

Explanation
The request does not specify redirection URI and there are more than one registered redirection URI to choose from.

System action
The request is rejected.

Administrator response
Provide redirection URI to avoid this confusion.

FBTOAU248E

Scope openid is required for id_token to be generated.

Explanation
The client has requested for id_token to be generated without openid scope specified.

System action
The request is rejected.

Administrator response
Specify the openid scope in the request.

FBTOAU249E

Not an OIDC Provider.

Explanation
The client has requested an OIDC request against OAuth Provider.

System action
The request is rejected.

Administrator response
Please configure and enable OIDC configuration.

FBTOAU250E

Response Type parameter value none cannot be combined with other value.

Explanation
Response Type parameter must not contain none with any other value.

System action
The request is rejected.

Administrator response
Ensure that the request response_type parameter none is not combined with any other value.

FBTOAU251E

The code_challenge_method is not valid, supported values include: *goodValues*.

Explanation
The code_challenge_method presented is not supported by this Authorization Server.

System action
The request is rejected.

Administrator response
Ensure a valid code_challenge_method is presented

FBTOAU252E

PKCE validation failed. The code_challenge [*badValue*] did not match the computed value: [*goodValue*].

Explanation
The code_challenge and code_verifier did not match.

System action
The request is rejected.

Administrator response
Ensure a valid code_challenge and code_verifer are used

FBTOAU253E

The client assertion is not valid, *exception*.

Explanation
The value of the assertion is not valid.

System action
The operation stops.

Administrator response
Ensure that the parameter values in the request message has the correct type and format.

FBTOIC001E

The request does not contain [*name*] parameter.

Explanation
This problem happens because the request does not contain consentData parameter.

System action
The request is not processed.

Administrator response
Ensure that the OpenID Connect template page consent_redirect.html sends consentData parameter.

FBTOIC002E

The request does not contain valid [*name*] request parameter.

Explanation
This problem happens because the request does not contain valid consentData parameter.

System action
The request is not processed.

Administrator response
Ensure that the OpenID Connect template page consent_redirect.html sends consentData parameter without any modification.

FBTOIC101E

The client ID [*name*] that you provide is not valid.

Explanation
Ensure that you supply a valid client ID.

System action
The request is not processed.

Administrator response
None.

FBTOIC102E

The target URL *targetURL* is not whitelisted.

Explanation
The target URL received by the system is rejected because it is not whitelisted.

System action
The flow is stopped.

Administrator response
Check if the target URL should be whitelisted.

FBTOIC103E

The relying party specified does not exist.

Explanation
The request received by the system is rejected because the relying party was not found.

System action
The flow is stopped.

Administrator response
Check the partner name in the kickoff url.

FBTOIC104E

The parameter *parameterName* is unset or null.

Explanation
The request received by the system is rejected because the value of the parameter is invalid.

System action
The flow is stopped.

Administrator response
Check that the advanced mapping rule isn't unsetting the value.

FBTOIC105E

The required parameter *parameterName* is missing from the request.

Explanation
The request received by the system is rejected because the required parameter is missing or null.

System action
The flow is stopped.

Administrator response
Check that the OpenID Connect Provider formatted the redirect correctly.

FBTOIC106E

Invalid state.

Explanation
The state parameter received did not match the expected value.

System action
The flow is stopped.

Administrator response
Check the value that was returned from the OP was correct.

FBTOIC107E

The token request with applies to: [*applies_to*] and issuer: [*issuer*] failed. Reason: [*reason*]

Explanation
The token exchange failed.

System action
The request is rejected.

Administrator response
Check that the trust chains are correctly configured

FBTOIC108E

The parameter [*parameter*] was duplicated in the Bearer token.

Explanation
The parameter occurred more than once in the bearer token in the response from the OP

System action
The request is rejected.

Administrator response
Check the response from the OP.

FBTOIC109E

The parameter [*parameter*] was duplicated in the request.

Explanation
The parameter occurred more than once in the request

System action
The request is rejected.

Administrator response
Check the request.

FBTOIC110E

The OpenID provider returned the following error code: [*error_code*]. Description: [*error_description*]. Error Uri: [*error_uri*] Op Endpoint: [*endpoint*]

Explanation
The an error occurred at the OP

System action
The authentication is halted.

Administrator response
Check the error at the OP.

FBTOIC111E

The redirect from the OpenID Connect Provider did not contain the required parameters [*parameter*], for the response_type:[*response_type*]

Explanation
The redirect didn't contain some expected parameters in the redirect

System action
The authentication is halted.

Administrator response
Check the redirect from the OP.

FBTOIC112E

The parameter in the metadata [*parameter*] is not supported by this Relying Party.

Explanation
The metadata did not contain a parameter suitable for this RP

System action
The authentication is halted.

Administrator response
Check the metadata and change the RP configuration to suit.

FBTOIC113E

The JSON response from the endpoint was not properly formatted.

Explanation
The response was not valid JSON

System action
The authentication is halted.

Administrator response
Check the response.

FBTOIC114E

An error occurred while invoking the advanced mapping rule.

Explanation
The rule encountered a runtime exception

System action
The authentication is halted.

Administrator response
Check the rule content and stacktrace.

FBTOIC115E

The mapping rule identified by id [*rule_id*] was not found.

Explanation
The mapping rule wasn't found.

System action
The authentication is halted.

Administrator response
Check the federation and partner configuration and that the rule exists.

FBTOIC116E

There was an error contacting the [*endpoint*]. The HTTP Status was: [*http_code*]. The JSON error code was: [*error_code*], with the description [*error_description*]

Explanation
There was an error contacting the OP, or the OP returned an error.

System action
The authentication is halted.

Administrator response
Check connectivity to the OP and that the request was valid.

FBTOIC117E

The claim [*name*] with the value [*value*] is invalid.

Explanation
The JWT was not considered valid for the purposes of an OpenID Connect Authentication.

System action
The authentication is halted.

Administrator response
Check the trace for an exact reason why the claim was rejected.

FBTOIC118E

There was an error retrieving the metadata from the OpenID connect provider

Explanation
An error occured making the HTTP request to the OpenID connect provider.

System action
The process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

DPWAD1061E

Failed to connect to the server: *%s*. (0x38983425)

Explanation
An attempt to contact a server failed. The server is required to be able to correctly service the Web request.

Administrator response
Ensure that the configuration for the server is correct and that the server is available. Check the log file for additional errors.

DPWAD1062E

Failed to connect to a required server. (0x38983426)

Explanation
An attempt to contact a server failed. The server is required to be able to correctly service the Web request.

Administrator response
Ensure that the configuration for the server is correct and that the server is available. Check the log file for additional errors.

DPWAD1063E

An invalid URL has been specified: *%s* (0x38983427)

Explanation
A URL has been supplied which does not conform to the standard URL specification (http[s]://<host>{:<port}).

Administrator response
Correct the URL, ensuring that it is of the correct format.

DPWAD1064E

An invalid HTTP status code, *%d*, was received in response to a request sent to *%s*. (0x38983428)

Explanation
A request was sent to a URL, and the status code received in the response was not the expected status code.

Administrator response
Ensure that the URL is correct and is responding with the correct data.

DPWAD1065E

An unexpected content type, *%s*, was received in response to a request sent to *%s*. (0x38983429)

Explanation
A request was sent to a URL, and the response content received was unexpected.

Administrator response
Ensure that the URL is correct and is responding with the correct data.

DPWAD1066E

An error occurred while parsing the JSON data: *%s*. (0x3898342a)

Explanation
The JSON data which has been supplied is not correctly formatted.

Administrator response
Ensure that the JSON data which is being supplied is correctly formatted.

DPWAD1067E

The element, *%s*, was not found in the JSON data. (0x3898342b)

Explanation
The JSON data which has been supplied is missing a required piece of data.

Administrator response
Ensure that the JSON data which is being supplied is correct.

DPWAD1068E

The element, *%s*, was found in the JSON data but is not of the correct type. (0x3898342c)

Explanation
The JSON data which has been supplied contains a required piece of data, but it is of an incorrect type.

Administrator response
Ensure that the JSON data which is being supplied is correct.

DPWAD1069E

A matching key for '*%s*' was not found. (0x3898342d)

Explanation
A search was made for a key which does not exist.

Administrator response
Ensure that the correct key has been specified.

DPWAD1071E

An error was returned from the OIDC OP. (0x3898342f)

Explanation
An error was returned from the OIDC OP during an authentication operation.

Administrator response
Ensure that the configuration for the OIDC OP server is correct and that the OIDC OP server is available. Check the log file for additional errors.

DPWAD1072E

An OIDC authentication request was received for an unknown issuer: *%s*. (0x38983430)

Explanation
A request was received which contained an unknown issuer identifier.

Administrator response
Ensure that the OIDC configuration is correct. Check the log file for additional errors.

DPWAD1073E

An OIDC authentication request was received for an unknown issuer. (0x38983431)

Explanation
A request was received which contained an unknown issuer identifier.

Administrator response
Ensure that the OIDC configuration is correct. Check the log file for additional errors.

DPWAD1074E

The OIDC RP authentication flow failed due to some missing data: *%s* (0x38983432)

Explanation
An OIDC RP flow failed because some required data is missing.

Administrator response
Ensure that the OIDC configuration is correct. Check the log file for additional errors.

DPWAD1075E

The authentication failed because the server has not yet been fully initialized. (0x38983433)

Explanation
An OIDC RP authentication flow because the OP is still to provide some required information.

Administrator response
Ensure that the OIDC configuration is correct. Check the log file for additional errors.

DPWAD1076E

The authentication failed because invalid authentication data was received. (0x38983434)

Explanation
An OIDC RP authentication flow because an invalid request was received.

Administrator response
Ensure that the OIDC configuration is correct. Check the log file for additional errors.

DPWAD1077E

The OIDC RP authentication flow failed due to invalid data being received for '*%s*'. '*%s*' is expected, but '*%s*' was received. (0x38983435)

Explanation
An OIDC RP flow failed because some provided data was invalid.

Administrator response
Ensure that the OIDC configuration is correct. Check the log file for additional errors.

DPWAD1078E

The OIDC RP authentication flow failed due to a missing header in the ID token. (0x38983436)

Explanation
An OIDC RP flow failed because the ID token was missing a header.

Administrator response
Ensure that the OIDC configuration is correct. Check the log file for additional errors.

DPWAD1079E

The OIDC RP authentication flow failed due to a missing field in the ID token: *%s*. (0x38983437)

Explanation
An OIDC RP flow failed a field was missing from the ID token header.

Administrator response
Ensure that the OIDC configuration is correct. Check the log file for additional errors.

DPWAD1080E

The OIDC RP authentication flow failed as the supplied token was not successfully validated. (0x38983438)

Explanation
An OIDC RP flow failed because the ID token failed the verification check.

Administrator response
Ensure that the OIDC configuration is correct. Check the log file for additional errors.

Chapter 17. One-time password messages

These messages are provided by the one-time password component.

FBTOTP000E

Internal Error. Contact the System Administrator.

Explanation
An internal error occurred.

System action
The one-time password manager encountered an error, process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTOTP100E

The plugin *pluginName* is missing the required parameter *parameter*

Explanation
A required plugin is missing from the plugin configuration.

System action
The one-time password plugin initialization encountered an error, process has been halted.

Administrator response
Provide the required parameter in the plugin configuration.

FBTOTP101E

The value [*value*] of the plugin parameter *parameter* is not valid.

Explanation
Some of the values in the plugin configuration are not valid.

System action
The one-time password plugin initialization encountered an error, process has been halted.

Administrator response
Fix the parameter value in the plugin configuration.

FBTOTP200E

The one-time password provider for type *type* is not found.

Explanation
The one-time password provider for the specified type is not found.

System action
Process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTOTP201E

The one-time password delivery for delivery type *type* is not found.

Explanation
The one-time password delivery for the specified delivery type is not found.

System action
Process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTOTP202E

One-time password manager not initialized.

Explanation
An internal error occurred.

System action
The one-time password manager encountered an error, process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTOTP300E

The required input parameter *param* is not found in the STSUU.

Explanation
A required input is missing from the input parameter.

System action
Process has been halted.

Administrator response
Provide the required parameter in the incoming STSUU.

FBTOTP301E

Cannot obtain one-time password delivery option.

Explanation
There was an error in obtaining the one-time password delivery option.

System action
The request has been halted.

Administrator response
Examine the log to determine the cause of the failure.

FBTOTP302E

The one-time password cannot be generated.

Explanation
There was an error in generating the one-time password.

System action
The request has been halted.

Administrator response
Examine the log to determine the cause of the failure.

FBTOTP303E

The one-time password cannot be delivered to *deliveryAttribute*.

Explanation
There was an error in delivering the one-time password.

System action
The request has been halted.

Administrator response
Examine the log to determine the cause of the failure.

FBTOTP304E

The submitted one-time password is not valid.

Explanation
The entered one-time password is not valid.

System action
The request has been halted.

Administrator response
Correct the one-time password and resubmit the form.

FBTOTP305E

The required service handle *handleName* was not provided to the STS module.

Explanation
The required service handle was not available.

System action
The STS request processing has been halted.

Administrator response
This error is a significant internal error. Check the logs for error messages indicating why the required service was not properly created.

FBTOTP306E

An error occurred during the construction of the contents of a message.

Explanation
The messaging component failed to build a message to send to the user.

System action
The one-time password operation could not be completed.

Administrator response
The one-time password application could not send a message due to a problem constructing the message contents. If details are required, enable trace logging and examine the nested exception.

FBTOTP307E

An internal error occurred. Contact the System Administrator.

Explanation
An internal error occurred.

System action
The one-time password application encountered an error, process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTOTP308E

The page contents might be missing the required information such as [*requiredInfo*] that is used to process an e-mail message request.

Explanation
The one-time password email delivery module requires certain information to process the request. The required information is missing.

System action
The request has been halted.

Administrator response
Examine the logs to determine the cause of the problem.

FBTOTP309E

The page contents might be missing the required information such as [*requiredInfo*] that is used to process an SMS message request.

Explanation
The one-time password SMS delivery module requires certain information to process the request. The required information is missing.

System action
The request has been halted.

Administrator response
Examine the logs to determine the cause of the problem.

FBTOTP310E

The one-time password that you submitted is not valid. Please submit a valid one-time password.

Explanation
You must use a valid one-time password.

System action
The one-time password is rejected.

Administrator response
None.

FBTOTP311E

The one-time password is submitted after the one-time password has expired. Please generate another one-time password, and submit it before it expires.

Explanation
One-time passwords are only valid for a certain amount of time. Ensure that you submit the one-time password before it expires.

System action
The one-time password is rejected.

Administrator response
None.

FBTOTP312E

The one-time password cannot be delivered to the email address: *toEmail*. Verify that the email address is correct.

Explanation
There was an error in delivering the one-time password to the specified email address.

System action
The request has been halted.

Administrator response
Examine the log to determine the cause of the failure.

FBTOTP313E

The one-time password authenticate callback could not invoke the trust service to perform token exchange for operation id [*operation id*] .

Explanation
The one-time password authenticate callback could not invoke the trust service to perform the one-time password operation.

System action
The request has been halted.

Administrator response
Examine the logs to determine the cause of the problem.

FBTOTP314E

The one-time password authenticate callback could not retrieve the one-time password delivery options.

Explanation
The one-time password authenticate callback could not to retrieve the one-time password delivery options.

System action
The request has been halted.

Administrator response
Examine the logs to determine the cause of the problem.

FBTOTP315E

The one-time password cannot be generated or delivered.

Explanation
There was an error in generating and delivering the one-time password.

System action
The request has been halted.

Administrator response
Examine the log to determine the cause of the failure.

FBTOTP316E

The request received by the one-time password authentication callback was sent using a transport that is not valid.

Explanation
The request received by the one-time password authentication callback was sent using a transport that is not valid. The request was sent using the SOAP binding.

System action
The one-time password request processing stopped.

Administrator response
Examine the logs to determine the cause of the problem. Ensure that the request is being sent using the appropriate binding.

FBTOTP317E

The submitted one-time password could not be validated.

Explanation
The one-time password module could not validate the submitted one-time password value.

System action
The request has been halted.

Administrator response
Examine the log to determine the cause of the failure.

FBTOTP318E

Unable to send the message to [*phoneNumber*] with username [*username*] because the SMS gateway provider returned a response HTTP status code [*statusCode*] which does not match the value that is configured in the response file for the parameter SuccessHTTPReturnCode: [*successCode*].

Explanation
The response HTTP status code returned by the SMS gateway provider does not match the value that is configured in the response file for the parameter SuccessHTTPReturnCode.

System action
The request has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTOTP319E

Unable to send the message to [*phoneNumber*] with username [*username*] because the SMS gateway provider returned an HTTP response body: [*responseBody*] which does not match

the Java regular-expression pattern that is configured in the response file for the parameter SuccessHTTPResponseBodyRegexPattern: *regexPattern*

Explanation
The HTTP response body returned by the SMS gateway provider does not match the Java regular-expression pattern that is configured in the response file for the parameter SuccessHTTPResponseBodyRegexPattern.

System action
The request has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTOTP320E

The list of methods for generating, delivering, and verifying one-time password returned from OTPGetDeliveryMethods mapping rule is invalid.

Explanation
OTPGetDeliveryMethods mapping rule must return at least one method for generating, delivering, and verifying one-time password.

System action
The request has been halted.

Administrator response
Ensure that OTPGetDeliveryMethods mapping rule returns a valid list of methods for generating, delivering, and verifying one-time password.

FBTOTP321E

The submitted ID of the method for generating, delivering, and verifying one-time password is invalid.

Explanation
The submitted ID must refer to one of the methods for generating, delivering, and verifying one-time password returned by OTPGetDeliveryMethods mapping rule.

System action
The request has been halted.

Administrator response
None.

FBTOTP322E

The one-time password based authentication failed. The user is not authenticated or the authentication level in the credential is not equal or higher to the supported authentication level [*authentication level*].

Explanation
The authentication process failed to generate a credential that supports the configured authentication level.

System action
The one-time password application encountered an error, process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTOTP323E

The value [*action*] received on the one-time password action query string parameter is not valid.

Explanation
The value submitted using the action query string parameter is not valid.

System action
The one-time password application encountered an error, process has been halted.

Administrator response
None.

FBTOTP324E

The value [*action*] received on the one-time password action query string parameter is not allowed when the previous step was [*previousPhase*].

Explanation
The authentication process failed because an invalid action value was specified.

System action
The one-time password application encountered an error, process has been halted.

Administrator response
None.

FBTOTP325E

The method for generating, delivering, and verifying one-time password was not found in the session.

Explanation
The method for generating, delivering, and verifying one-time password needs to be available in the session.

System action
The request has been halted.

Administrator response
None.

FBTOTP326E

The submitted CSRF token is invalid.

Explanation
The submitted CSRF token must match the last generated CSRF token.

System action
The request has been halted.

Administrator response
None.

FBTOTP328E

The configured parameter [*parameterName*] with value [*value*] is outside of the range [*lowRange* - *highRange*]

Explanation
The parameter is outside of the expected range.

System action
The configuration is invalid. The one-time passwords cannot be verified.

Administrator response
Update the configuration so that the configuration parameter is in a valid range.

FBTOTP329E

The configured parameter [*parameterName*] with value [*value*] is below the minimum value of [*lowRange*]

Explanation
The parameter is below the minimum accepted value.

System action
The configuration is invalid. The one-time passwords cannot be verified.

Administrator response
Update the configuration so that the configuration parameter is at least the minimum value.

FBTOTP330E

Unable to locate the HMAC secret key

Explanation
The user's secret key for one-time password generation cannot be located.

System action
Unable to verify

Administrator response
Ensure that the secret key is being provided to the user through the STSUU

FBTOTP331E

The specified algorithm [*parameterName*] is not supported on this system

Explanation
The algorithm chosen to generate the OTPs is not supported on this system. It is possible that the algorithm was not named correctly, or a newer version of Java is required.

System action
The algorithm specified is not supported, so OTPs cannot be verified.

Administrator response
Check the configuration to make sure the algorithm is specified correctly. It is possible that the algorithm is supported in a later version of Java than the one currently installed.

FBTOTP332E

The one time use enforcement store [*parameterName*] could not be loaded or was not found.

Explanation
The one time use enforcement store implementing the OTPReplayStore interface was not found.

System action
Due to the configuration error, OTPs will not be generated or verified.

Administrator response
Check that the one time use enforcement store is available to be loaded. Also check that it implements the OTPReplayStore interface.

FBTOTP333E

The one time use enforcement store [*parameterName*] implemented OTPStore, but not OTPReplayStore.

Explanation
The one time use enforcement store must implement the OTPReplayStore interface.

System action
Due to the configuration error, OTPs will not be generated or verified.

Administrator response
Specify a store that implements the OTPReplayStore interface.

FBTOTP334E

The one time password provider failed to store the counter that corresponds to the user [*username*].

Explanation
The one time password provider failed to store the counter value that corresponds to the user.

System action
The request to authenticate the user using the one time password will fail.

Administrator response
Validate the one time password provider configuration .

FBTOTP335E

The submitted PIN did not satisfy all requirements.

Explanation
The submitted PIN did not meet all of the requirements of the RSA Manager.

System action
The request to authenticate the user using the one time password and attempt to change the PIN will fail.

Administrator response
None.

FBTOTP336E

The ID obtained from the obligation URI for the method for generating, delivering, and verifying one-time password is invalid.

Explanation
The ID obtained from the obligation URI must refer to one of the methods for generating, delivering, and verifying one-time password returned by OTPGetDeliveryMethods mapping rule.

System action
The request has been halted.

Administrator response
None.

FBTOTP337E

The submitted one time password is invalid. *incorrect* incorrect attempt(s) have been made. You have *remaining* attempts remaining.

Explanation
The entered one-time password is not valid.

System action
The request has been halted.

Administrator response
Correct the one-time password and resubmit the form.

FBTOTP338E

incorrect incorrect attempt(s) have been made. You have no attempts remaining. Please try again in *time* seconds.

Explanation
There are no more remaining attempts.

System action
The request has been halted.

Administrator response
Wait until the attempts have expired before trying again.

Chapter 18. Policy messages

These messages are provided by the policy component.

GLGPL1004E

An error was detected while processing the System Alerts Policy. The policy will not be applied until the problem is corrected.

Explanation

This message indicates that the System Alerts Policy contains an error that must be corrected before the policy can be used.

Administrator response

Review the Network Objects in use in the System Alerts Policy. Look for any Invalid Object References and remove those objects from the policy. Then re-apply the policy.

GLGPL1005W

The Protection Interfaces policy contains an unsupported speed/duplex setting, *LinkMode*, for interface *Interface* Interface will default to Auto.

Explanation

This message indicates that one or more network interface modules were changed and the Protection Interfaces policy no longer matches the hardware.

Administrator response

Review the Protection Interfaces policy. Correct the speed/duplex setting for the specified interface. Re-apply the policy.

GLGPL9004W

Some OpenSignatures rules did not pass the rule validation check. Please verify the syntax in your rules. Detail: *detail*.

Explanation

This message alerts to invalid Open Signature rules that may be due to an incompatible XPU update.

Administrator response

Review Open Signature rules on LMI or Site Protector, and save them to check if any errors occurred.

GLGPY0001E

An error was detected while processing the Address Object Group. Policies will not be applied until the problem is corrected.

Explanation

This message indicates that the Address Object Group contains an error that must be corrected before policies can be applied.

Administrator response

Review the Address Objects in use in the Address Object Group. Look for any Invalid Object References and remove those objects from the group. Then re-apply the policy.

Chapter 19. Reporting messages

These messages are provided by the report component.

FBTRPT001E

Check that all required report parameters are set correctly.

Explanation
This error occurs when a required report parameter is missing or has been set incorrectly in a report design file.

System action
System cannot execute reporting functionality.

Administrator response
Check report parameter settings in report design file.

FBTRPT002E

The Report engine cannot be started.

Explanation
This error occurs due to problems in the reports configuration.

System action
System cannot execute reporting functionality.

Administrator response
Check that the reports configuration has been defined properly.

FBTRPT003E

Detected invalid or nonexistent directory for report designs.

Explanation
This error occurs when the report designs directory for the reports configuration is invalid or does not exist.

System action
System cannot execute reporting functionality.

Administrator response
Check that the report designs directory has been specified correctly in the reports configuration.

FBTRPT004E

Detected invalid or nonexistent directory for report designs.

Explanation
This error occurs when the report archives directory for the reports configuration is invalid or does not exist.

System action
System cannot execute reporting functionality.

Administrator response
Check that the report archives directory has been specified correctly in the reports configuration.

FBTRPT005E

Could not find report design.

Explanation
This error occurs when a report design cannot be found in the report designs directory.

System action
System cannot execute reporting functionality.

Administrator response
Check that the appropriate report design is located in the report designs directory as defined in the reports configuration.

FBTRPT006E

Could not find archived report.

Explanation
This error occurs when an archived report cannot be found in the report archives directory.

System action
System cannot execute reporting functionality.

Administrator response
Check that the appropriate archived report is located in the report archives directory as defined in the reports configuration.

FBTRPT007E

Could not create archive report directory for render type.

Explanation
This error occurs when a invalid or unsupported render type has been specified.

System action
System cannot execute reporting functionality.

Administrator response
Specify pdf or html as a render type.

FBTRPT008E

An error has occurred while running report.

Explanation
This error occurs when an unexpected error has occurred while running a report.

System action
System cannot execute reporting functionality.

Administrator response
Check the system logs for error details.

FBTRPT009E

Detected invalid report file name.

Explanation
This error occurs when the required naming convention for report design files is not followed.

System action
System cannot execute reporting functionality.

Administrator response
Check that report design file is named properly.

FBTRPT010E

Detected invalid parameter with no selection choices.

Explanation
There was a problem retrieving selection choices for a list box, check box, or radio button parameter.

System action
System cannot execute reporting functionality.

Administrator response
Check that the list box, check box, or radio button parameter has been defined correctly in the report design.

FBTRPT011E

Detected unsupported or invalid parameter. Parameter must be a scalar type.

Explanation
This error occurs when a parameter is not a scalar parameter.

System action
System cannot execute reporting functionality.

Administrator response

Check that the parameter has been defined as a scalar type in the report design. Only scalar parameters are supported in this release. Check the TFIM documentation for details on defining report parameters.

Chapter 20. SCIM messages

These messages are from the SCIM component.

SCIIS0001E

The resource '{0}' was not found. (0x370d8001)

Explanation
A request was made for a resource which is not known to the system.

Administrator response
Check to ensure that the resource which has been specified is correct.

SCIIS0002E

The JSON data element '{0}' is missing from the request. (0x370d8002)

Explanation
The JSON data which was supplied with the request is missing some required data elements.

Administrator response
Ensure that the correct JSON data is supplied with the request.

SCIIS0003E

The JSON data element '{0}' is invalid. (0x370d8003)

Explanation
The JSON data which was supplied with the request contains invalid data.

Administrator response
Ensure that the correct JSON data is supplied with the request.

SCIIS0004E

The path '{0}', included in the request, is not valid. (0x370d8004)

Explanation
The path supplied with the request is invalid.

Administrator response
Ensure that the correct path is specified for the request.

SCIIS0005E

The schema, '{0}', is not a known or supported schema. (0x370d8005)

Explanation
The JSON data which was supplied with the request contains the name of a schema which is not known.

Administrator response
Ensure that the correct JSON data is supplied with the request.

SCIIS0006E

The resource '{0}' already exists. (0x370d8006)

Explanation
A request was made for a resource which already exists.

Administrator response
Check to ensure that the resource which has been specified is correct.

SCIIS0007E

The field '{0}' cannot be updated. (0x370d8007)

Explanation
The JSON data which was supplied with the request contains data which cannot be updated.

Administrator response
Ensure that the correct JSON data is supplied with the request.

SCIIS0008E

An internal error occurred. (0x370d8008)

Explanation
An unexpected internal error occurred.

Administrator response
Check the logs.

SCIIS0009E

An unknown attribute, '{0}', has been specified. (0x370d8009)

Explanation
The request contains an attribute name which is not known to the system.

Administrator response
Ensure that only known attributes are included in the request.

SCIIS0010E

An invalid attribute, '{0}', has been specified. (0x370d800a)

Explanation
The request contains an attribute name which is not valid in the context of the request.

Administrator response
Ensure that only valid attributes are included in the request.

SCIIS0011E

The path '{0}', included in the request, did not match known data. (0x370d800b)

Explanation
The path supplied with the request did not match any known data.

Administrator response
Ensure that the correct path is specified for the request.

SCIIS0012E

The filtering capability for the '{0}' schema has not been implemented. (0x370d800c)

Explanation
A request which contains a filter string has been sent to the application, but the corresponding schema for the request does not support filtering.

Administrator response
Ensure that only supported requests are sent to the application.

SCIIS0013E

The filter operation '{0}' for the '{1}' schema is not supported. (0x370d800d)

Explanation
A request which contains a filter string has been sent to the application, but the filter operation specified in the string is not supported.

Administrator response
Ensure that only supported requests are sent to the application.

SCIIS0014E

The filter attribute '{0}' for the '{1}' schema is not supported. (0x370d800e)

Explanation
A request which contains a filter string has been sent to the application, but the filter attribute specified in the string is not supported in the context of the request.

Administrator response
Ensure that only supported requests are sent to the application.

SCIIS0015E

The field '{0}' cannot be removed. (0x370d800f)

Explanation
The JSON data which was supplied with the request contains data which cannot be removed.

Administrator response
Ensure that the correct JSON data is supplied with the request.

SCIIS0016E

The path '{0}', included in the request, is not valid. A filter is required to reference multi-valued attributes. (0x370d8010)

Explanation
The path supplied with the request is invalid.

Administrator response
Ensure that a filter is specified in the request.

SCIIS0017E

The attribute '{0}', included in the request, is not valid. The attribute structure was invalid or did not conform to the request schema. (0x370d8011)

Explanation
The JSON data which was supplied with the request did not conform to the request schema.

Administrator response
Ensure that the correct JSON data is supplied with the request.

SCIIS0018E

The SCIM integration with Verify Access has not been enabled. (0x370d8012)

Explanation
A SCIM request was received which contained data which is specific to the Verify Access schema. The Verify Access integration point is currently disabled and so the SCIM application is unable to process the request.

Administrator response
Check the data associated with the Web Service request and ensure that no data for the Verify Access schema is being supplied.

SCIIS0019E

Multiple entries were found for the resource '{0}'. (0x370d8013)

Explanation
A request was made for resource which has multipe entries.

Administrator response
Check to ensure that the resource which has been specified is correct.

SCIIS0064E

The user with the DN of '{0}' was not found. (0x370d8040)

Explanation
An attempt was made to access a user DN which was not located in the user registry.

Administrator response
Check to ensure that the resource which has been specified is correct.

SCIIS0065E

The Verify Access user with the identity of '{0}' was not found. (0x370d8041)

Explanation
An attempt was made to access an Verify Access user which was not located in the user registry.

Administrator response
Check to ensure that the resource which has been specified is correct.

SCIIS0066E

The group with the DN of '{0}' was not found. (0x370d8042)

Explanation
An attempt was made to access a group DN which was not located in the user registry.

Administrator response
Check to ensure that the resource which has been specified is correct.

SCIIS0067E

Authentication mechanism identified by '{0}' was not found. (0x370d8043)

Explanation
The ID was not found in the database.

Administrator response
Check that the mechanism ID is correct.

SCIIS0068E

The JSON response from the external server was malformed. (0x370d8044)

Explanation
The response from the server could not successfully be parsed as JSON.

Administrator response
Check the external server.

SCIIS0069E

The JSON response from the external server was of type {0} rather than {1}. (0x370d8045)

Explanation
The response from the server contained an unexpected type.

Administrator response
Check the external server.

SCIIS0070E

The response from the server did not contain a Content-Type header. (0x370d8046)

Explanation
The response from the server was missing the Content-Type header.

Administrator response
Check the external server.

SCIIS0071E

The response from the server contained a Content-Type header with value '{0}', '{1}' was expected. (0x370d8047)

Explanation
The response from the server had an incorrect value for the Content-Type header.

Administrator response
Check the external server.

SCIIS0072E

The response from the server was considered bad, Status code: {0}, Body: {1} (0x370d8048)

Explanation
The response from the server was an error.

Administrator response
Check the external server.

SCIIS0073E

The configured server connection, {0}, could not be found. (0x370d8049)

Explanation
The SCIM application configuration refers to a server connection which could not be located.

Administrator response
Check the configuration of the SCIM application.

SCIIS0074E

The user with the DN of '{0}' was not found. (0x370d804a)

Explanation
An attempt was made to access a user DN which was not located in the user registry.

Administrator response
Check to ensure that the resource which has been specified is correct.

SCIIS0075E

The ISAM user with the identity of '{0}' was not found. (0x370d804b)

Explanation
An attempt was made to access an ISAM user which was not located in the user registry.

Administrator response
Check to ensure that the resource which has been specified is correct.

SCIIS0076E

The group with the DN of '{0}' was not found. (0x370d804c)

Explanation
An attempt was made to access a group DN which was not located in the user registry.

Administrator response
Check to ensure that the resource which has been specified is correct.

SCIIS0128E

The attribute '{0}' could not be removed. To unset this attribute, remove or replace the parent attribute. (0x370d8080)

Explanation
The JSON data which was supplied with the request contains data which cannot be removed.

Administrator response
Ensure that the correct JSON data is supplied with the request.

SCIIS0129E

The operation could not be performed. An attempt was made to modify or remove attributes that can only be updated from a registered device. (0x370d8081)

Explanation
The JSON data which was supplied with the request contains data which can only be removed or modified from a registered device.

Administrator response
Ensure that the correct JSON data is supplied with the request.

SCIIS0130E

The operation could not be performed. An attempt was made to modify or remove attributes that can only be updated by the owner. (0x370d8082)

Explanation
The JSON data which was supplied with the request contains data which can only be removed or modified by the owner of the data.

Administrator response
Ensure that the correct JSON data is supplied with the request.

SCIIS0131E

The operation could not be performed. An attempt was made to add attributes that can only be updated from a registered device. (0x370d8083)

Explanation
The JSON data which was supplied with the request contains data which can only be added from a registered device.

Administrator response
Ensure that the correct JSON data is supplied with the request.

Chapter 21. Secure reverse proxy messages

These messages are provided by the secure reverse proxy component.

CTGSI0301E

Initialization of the distributed session cache server failed. (0x38c5812d)

Explanation
The distributed session cache server was unable to initialize and cannot function until the cause of the failure is corrected.

Administrator response
Inspect the application server log files for details, take any necessary corrective action, and restart the distributed session cache server.

CTGSI0302W

The client is not registered with the distributed session cache server. (0x38c5812e)

Explanation
The client is not registered with the distributed session cache server. Clients must register before performing any operations.

Administrator response
No action is necessary.

CTGSI0303E

The client is not authorized to perform the requested operation. (0x38c5812f)

Explanation
The client attempted to perform an operation that it is not authorized to perform.

Administrator response
If the client is expected to be authorized to perform the requested operation then correct the security policy that applies to the distributed session cache server.

CTGSI0304W

The concurrent session limit for the user has been reached. (0x38c58130)

Explanation
The attempt to create a new session for the user failed because creating another session would exceed the concurrent session limit for the user.

Administrator response
No action is necessary.

CTGSI0305W

The client attempted to create a session with a session ID that is already in use. (0x38c58131)

Explanation
The session ID specified for the new session already exists in the shared session cache. The client must choose a new ID for the session.

Administrator response
No action is necessary.

CTGSI0306E

The client attempted to use a replica set that does not exist in the distributed session cache server configuration. (0x38c58132)

Explanation
The client attempted to use a replica set that has not been specified in the distributed session cache server configuration. All replica set names must be specified in the distributed session cache server configuration.

Administrator response
Verify the client's configuration specifies all replica set names correctly and the distributed session cache server's configuration includes all any necessary replica sets.

CTGSI0307E

The client attempted to perform an operation on a replica set that it has not joined. (0x38c58133)

Explanation
When clients connect to the distributed session cache server they must specify the names of all replica sets they will use. This error indicates a client has not done so.

Administrator response
Verify the client is correctly configured.

CTGSI0308E

The client attempted to create or modify a session such that its concurrent session key would not be valid. (0x38c58134)

Explanation
Sessions stored by the distributed session cache server can include session data items indicating the concurrent session key. Either all of these session data items must be present and valid, or none of them. This error indicates that some, but not all, of the session data items were present.

Administrator response
This error indicates a problem with the configuration of the client or a programming error. Examine the sections of the client configuration relating to concurrent session limits and session displacement. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSI0309W

The client's version of the session is out of date. (0x38c58135)

Explanation
The client issued a session modification request based on an out of date version of the session. The client must retrieve the current version of the session and retry the request.

Administrator response
No action is necessary.

CTGSI0310W

The client specified a capability mask that does not match the active capability mask. (0x38c58136)

Explanation
The client specified a capability mask that does not match the active capability mask. The client will not be able to register until the distributed session cache server is restarted and initialized with a matching capability mask.

Administrator response
Ensure all clients accessing the distributed session cache server are compatible with the version of the distributed session cache server. It may be necessary to restart the distributed session cache server and all active clients to correct this condition. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSI0311E

The distributed session cache server was unable to generate a new key. (0x38c58137)

Explanation
The distributed session cache server was unable to generate a new key.

Administrator response
Examine the distributed session cache server logs for further details. It may be necessary to restart the distributed session cache server completely to correct this condition.

CTGSI0312W

The session was not found. (0x38c58138)

Explanation
The distributed session cache server was unable to find a session with the session ID specified by the client.

Administrator response
No action is necessary.

CTGSI0313E

A parameter value was not valid. (0x38c58139)

Explanation
The client specified a parameter value that was not valid to the distributed session cache server.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSI0314E

The specified client instance ID has already been registered by another client. (0x38c5813a)

Explanation
Each client that makes use of the distributed session cache server must register a unique instance ID. This message indicates a client attempted to use an instance ID that another client had already registered.

Administrator response
Restart the client. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSI0315E

The distributed session cache server encountered an error and was unable to complete the operation. (0x38c5813b)

Explanation
While processing the client's request, the distributed session cache server encountered an error that prevented it from completing the operation.

Administrator response
Inspect the distributed session cache server logs to identify the nature and cause of the error. Take any necessary corrective measures. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSI0316E

The client attempted to register using an active client name from a different IP address than was used to register the active instance. (0x38c5813c)

Explanation
The client attempted to register using an active client name from a different IP address than was used to register the active instance.

Administrator response
Inspect the client's configuration to ensure each client uses a unique replica name. The distributed session cache server logs indicate the IP addresses of the clients using the same client name. If the IP address of the client has recently changed, wait until the distributed session cache server expires the previous registration before restarting the client. The amount of time to wait is controlled by the distributed session cache server's client idle timeout configuration parameter.

CTGSI0317W

The client attempted an idle timeout operation but the capabilities required to support idle timeouts have not been enabled. (0x38c5813d)

Explanation
The first client to start-up requested a set of capabilities from the distributed session cache server that did not include the session interest list capability. This capability is required to support idle timeout of sessions.

Administrator response
Examine any client configuration options relating to distributed session cache server capabilities. To change the active set of capabilities, all clients must be shut-down, and the distributed session cache server restarted. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSI0319E

The client issued a change session request with no session data changes. (0x38c5813f)

Explanation
The client issued a change session request with no session data changes.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSI0320E

The interface version requested by the client is not supported by this server. (0x38c58140)

Explanation
The interface version requested by the client is not supported by this server.

Administrator response
Ensure the versions of client software and server software are compatible.

CTGSI0321W

The distributed session cache server detected a conflict resulting from replication of the changes. (0x38c58141)

Explanation
The distributed session cache server detected a conflict resulting from replication of the changes.

Administrator response
No action is necessary.

CTGSI0322E

An invalid request parameter was passed to the session administration interface. (0x38c58142)

Explanation
An invalid request parameter was passed to the session administration interface.

Administrator response
Retry the operation specifying valid parameters. Consult the IBM Security Verify Access Shared Session Administration Guide for information about valid request parameters.

CTGSI0323E

An unrecognized administration operation was passed to the distributed session cache server's administration interface. (0x38c58143)

Explanation
The distributed session cache server's administration interface can only handle known request types from its clients. An unrecognized request type was sent from a client.

Administrator response
Ensure the requested administration operation is currently enabled and that the version of the client software in use is supported by this version of the distributed session cache server.

CTGSI0324E

The request from the client requires a capability of the distributed session cache server that is not enabled by the distributed session cache server. (0x38c58144)

Explanation
The request from the client requires a capability of the distributed session cache server that is not enabled by the distributed session cache server.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSI0325E

The client attempted to use a session realm that does not exist in the distributed session cache server configuration. (0x38c58145)

Explanation
The client attempted to use a session realm that does not exist in the distributed session cache server configuration. All session realm names must be specified in the distributed session cache server configuration.

Administrator response
Retry the operation specifying a defined session realm.

CTGSI0327W

The distributed session cache server was not able to replicate the changes across the cluster. (0x38c58147)

Explanation
The distributed session cache server was not able to replicate the changes resulting from the request across the cluster.

Administrator response
Check the distributed session cache server logs for more information concerning this error. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSI0328E

Authentication failed. You have used an invalid user name or password. (0x38c58148)

Explanation
An invalid user name or password was supplied.

Administrator response
Check your authentication information and try again.

CTGSI0329E

Authentication failed. The account associated with the user has expired. (0x38c58149)

Explanation
The users account has expired.

Administrator response
Contact your system administrator to have the account reactivated.

CTGSI0330E

Authentication failed. The credential associated with the user has expired. (0x38c5814a)

Explanation
The user's credential has expired. This error might indicate that the user's password has expired.

Administrator response
Contact your system administrator to renew the users credential.

CTGSI0331W

The session limit for this session realm has been reached. (0x38c5814b)

Explanation
The attempt to create a new session for the user failed because creating another session would exceed the session limit for the session realm.

Administrator response
No action is necessary.

CTGSI0332E

The client is attempting a switch user operation while already switched, this is not valid. (0x38c5814c)

Explanation
A client, such as WebSEAL, is attempting to switch user while already switched. The Distributed Session Cache server does not support this.

Administrator response
Do not attempt a switch-user operation from a session which has already been switched.

CTGSI0333E

The client is attempting revert from a switched user session when there is no prior session. (0x38c5814d)

Explanation
A client, such as WebSEAL, is attempting to switch back from a switched user session when there is no prior session to switch back to.

Administrator response
If the problem persists, check IBM Electronic Support for additional information.

CTGSM0301E

The new instance, *%s*, of the client, *%s*, could not be stored. (0x38c5c12d)

Explanation
The session management server was unable to store the details of the client.

Administrator response
Examine the log for further detailed messages regarding the error, take any necessary corrective action, and restart the client. It may also be necessary to restart the session management server.

CTGSM0303E

The list of keys stored in the session list store, *%s*, for the replica set, *%s*, could not be retrieved. (0x38c5c12f)

Explanation
The session management server was unable to retrieve the list of keys stored in the given session list.

Administrator response
Examine the log for earlier messages regarding this error and take any necessary corrective action. If the problem persists, restart the session management server.

CTGSM0304E

The session, *%s*, in the replica set, *%s*, does not have a concurrent session key. (0x38c5c130)

Explanation
Every session must include the data item used as the key for maintaining concurrent session counts. A session was either created without the data item, or the data item was removed as part of a session update.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0305E

The session, *%s*, in replica set, *%s*, could not be stored. (0x38c5c131)

Explanation
A session could not be stored in the session cache.

Administrator response
Examine the log for other messages regarding the error and take any necessary corrective action. The error might indicate resource exhaustion.

CTGSM0306W

The session management server has rejected a session modification request from the client, *%s*, for the session, *%s*, in the replica set, *%s*, based on an outdated version of the session. The client has version number *%s*, while *%s* is the current version number. (0x38c5c132)

Explanation
A client has issued a session update request based on an outdated version of the session. The request has been rejected.

Administrator response
This condition can sometimes occur during normal operation of the session management server. The client can correct the condition by first requesting the current version of the session, and then re-issuing the update request based on that version. This error could also indicate a problem with the client.

CTGSM0310W

The client, *%s*, is not registered. (0x38c5c136)

Explanation
The client attempted the perform an operation without first registering with the session management server.

Administrator response
No action is necessary.

CTGSM0311W

Returning result: *%s* (code: 0x*%s*). (0x38c5c137)

Explanation
The specified result is being returned to the client. This message is usually only logged when an error result is returned.

Administrator response
If the result indicates an error has occurred, examine the log for further details and take any necessary corrective action.

CTGSM0312E

A new instance of the client, *%s*, has attempted to start-up. The existing instance ID is *%s*, with the client ID of *%s*. The second instance ID is *%s*, with IP address *%s*. (0x38c5c138)

Explanation

A replica attempted to register with the session management server using a replica name that was already active, and its client ID was different to that used to register the active instance. The replica's registration was denied by the session management server.

Administrator response

This message indicates two replicas are configured with the same replica name, and both are attempting to register with the session management server. If this message coincides with a planned client ID change for a replica machine, the replica cannot be restarted until its previous instance is expired. Otherwise, examine the configuration on the machines with the client ID's given to determine whether they have been configured to use the same replica name. If so, change the replica name on one machine. It may be necessary to explicitly configure the replica name on both machines to avoid a conflict.

CTGSM0316E

Single sign-on was requested in session realm, *%s*, but there is no single sign-on mapping configured. (0x38c5c13c)

Explanation

A client requested a session be created using single sign-on within a session realm, but the session management server configuration does not specify a single sign-on mapping for the session realm.

Administrator response

Modify the session management server configuration so it specifies a single sign-on mapping to use within the session realm. The session management server must be restarted for this change to take effect.

CTGSM0317E

An error occurred during statistics gathering setup: *%s*. (0x38c5c13d)

Explanation

An error occurred during statistics gathering setup. Statistics will not be recorded until the error is corrected and the session management server application is restarted.

Administrator response

Examine this and earlier log messages for more information regarding the error. Once the error has been corrected, restart the session management server.

CTGSM0318E

Initialization of the event timer class, *%s*, failed: *%s* (0x38c5c13e)

Explanation

The session management server uses different event timer classes in different runtime environments. This message indicates the event timer class for this environment is not available. The session management server will not function without an event timer.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0319E

The database, *%s*, could not be opened. (0x38c5c13f)

Explanation
The database may not exist or may have other problems.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0321E

The event does not specify a session. (0x38c5c141)

Explanation
The event may be corrupt or incorrectly created because it does not specify a session.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0322E

The session management server could not copy the file *%s* to *%s*: *%s* (0x38c5c142)

Explanation
The session management server could not copy a file.

Administrator response
Examine the error message for more information on the error. Restart the session management server application to retry the operation. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0323E

The administration interface version, *%s*, requested by the client is not supported by the server. The server supports the following versions of the administration interface: *%s*. (0x38c5c143)

Explanation
The interface version requested by the client is not supported by this server.

Administrator response
Ensure the versions of client software and server software are compatible.

CTGSM0324W

J2EE security is disabled for this application server. No security checks will be performed by the session management server administration interface. (0x38c5c144)

Explanation
The session management server administration interface security depends on J2EE security being enabled in the application server.

Administrator response
If security is required for the session management server administration interface then enable J2EE security and restart the application server.

CTGSM0325E

Unable to retrieve message text for message code {0}. (0x38c5c145)

Explanation
The message text for the specified message code could not be retrieved.

Administrator response
Verify the files that make up the session management server application are present in the WebSphere application server installed applications directory. The session management server will not function correctly until this problem is corrected. It may be necessary to reinstall the session management server application to correct this problem.

CTGSM0326E

The file, *%s*, could not be deleted. (0x38c5c146)

Explanation
A file could not be deleted.

Administrator response
Check that the file system is writable, and that the file system permissions allow the file to be deleted.

CTGSM0327E

An error occurred during initialization of the class, *%s*, specified by property, *%s*: *%s* (0x38c5c147)

Explanation
An error occurred during initialization of an event handler class.

Administrator response
Examine the error message for information regarding the error and take any necessary corrective action. The session management server application must be restarted.

CTGSM0328E

An error occurred while replicating session management server data: *%s* (0x38c5c148)

Explanation
An error occurred while replicating session management server data. This error may indicate communication problems between cluster members.

Administrator response
Examine the error message for information regarding the error and take any necessary corrective action. It may be necessary to restart the session management server application. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0329E

The session management server was not able to replicate an operation on the key, *%s*, in the map, *%s*. (0x38c5c149)

Explanation
The session management server was not able to replicate an operation on an entry in a storage map to other nodes in the cluster. The client issuing the request that resulted in the operation will be notified of the failure.

Administrator response
Check that all WebSphere cluster members are running correctly, and that the network connections between each node are functioning. Multiple instances of this error may indicate resource starvation or server availability problems. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0330E

The session management server instance was not able to establish communication with other instances in the cluster: *%s*. (0x38c5c14a)

Explanation
The session management server instance was not able to establish communication with other instances in the cluster.

Administrator response
Restart the server on which this instance of the session management server runs. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0332E

The session management server was not able to obtain a cluster-wide lock on the item, *%s*: *%s* (0x38c5c14c)

Explanation
The session management server was not able to obtain a cluster-wide lock on a data item in order to update it.

Administrator response
Check that all WebSphere cluster members are running correctly, and that the network connections between each node are functioning. Multiple instances of this error may indicate resource starvation

or server availability problems. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0333E

The session management server was not able to release a lock on the item, *%s*: *%s* (0x38c5c14d)

Explanation

The session management server was not able to release a cluster-wide lock on a data item after updating it.

Administrator response

Check that all WebSphere cluster members are running correctly, and that the network connections between each node are functioning. Multiple instances of this error may indicate resource starvation or server availability problems. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0334E

Transfer of existing session management server data to a new instance, *%s*, failed: *%s*. (0x38c5c14e)

Explanation

Transfer of existing session management server data to a new instance failed. The new instance will not process requests until it is restarted.

Administrator response

Restart the server on which the new instance runs. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0335E

An error occurred while receiving session management server data from another instance: *%s* (0x38c5c14f)

Explanation

An error occurred while receiving session management server data. This error may indicate communication problems between cluster members.

Administrator response

Examine the error message for information regarding the error and take any necessary corrective action. It may be necessary to restart the session management server application. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0336E

The replication operation message was badly formed. (0x38c5c150)

Explanation

A replication operation message, used to transfer data between session management server instances, was badly formed.

Administrator response
This message indicates a serious problem relating to session management server data replication. Restart the session management server application. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0337E

Initialization of the event worker class, *%s*, failed: *%s* (0x38c5c151)

Explanation
The session management server uses different event worker classes in different runtime environments. This message indicates the event worker class for this environment is not available.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0450E

An SQL error has occurred: *%s* (SQL error code: *%s*, SQL state: *%s*). (0x38c5c1c2)

Explanation
The session management server has encountered an SQL error during a database operation.

Administrator response
This message may indicate resource starvation problems, such as disk space or memory exhaustion. Examine the system's resource usage to see if this is the case. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0451E

The JDBC driver could not be initialized: *%s* (0x38c5c1c3)

Explanation
The JDBC driver required to access the session management server database tables could not be initialized.

Administrator response
Check the properties of the JDBC data source configured for use by the session management server and restart the session management server.

CTGSM0452E

The database table, *%s*, was not found. (0x38c5c1c4)

Explanation
One of the session management server database tables is missing.

Administrator response
Correct the database configuration and restart the session management server. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0453E

The column, *%s*, in the database table, *%s*, was not found. (0x38c5c1c5)

Explanation
A column in one of the session management server database tables is missing.

Administrator response
Correct the database configuration and restart the session management server. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0454E

The column, *%s*, in the database table, *%s*, has the wrong type. The expected type is *%s*, but the type in the database is *%s*. (0x38c5c1c6)

Explanation
A column in one of the session management server database tables has the wrong type.

Administrator response
Correct the database configuration and restart the session management server. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0457E

The column, *%s*, in the database table, *%s*, is not a primary key. (0x38c5c1c9)

Explanation
A column in one of the session management server database tables is not a primary key.

Administrator response
Correct the database configuration and restart the session management server. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0458E

The column, *%s*, in the database table, *%s*, is not configured to use a foreign key. (0x38c5c1ca)

Explanation
A column in one of the session management server database tables is not configured to use a foreign key.

Administrator response
Correct the database configuration and restart the session management server. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0459E

The foreign key column, *%s*, in the database table, *%s*, imports its key from the table, *%s*, but it should import from the table, *%s*. (0x38c5c1cb)

Explanation
A column in one of the session management server database tables has a misconfigured foreign key.

Administrator response
Correct the database configuration and restart the session management server. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0460E

The foreign key column, *%s*, in the database table, *%s*, imports its key from the column, *%s*, but it should import from the column, *%s*. (0x38c5c1cc)

Explanation
A column in one of the session management server database tables has a misconfigured foreign key.

Administrator response
Correct the database configuration and restart the session management server. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0461E

The foreign key column, *%s*, in the database table, *%s*, uses the update rule, *%s*, but it should use the update rule, *%s*. (0x38c5c1cd)

Explanation
A column in one of the session management server database tables has a misconfigured foreign key.

Administrator response
Correct the database configuration and restart the session management server. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0462E

The foreign key column, *%s*, in the database table, *%s*, uses the delete rule, *%s*, but it should use the delete rule, *%s*. (0x38c5c1ce)

Explanation
A column in one of the session management server database tables has a misconfigured foreign key.

Administrator response
Correct the database configuration and restart the session management server. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0463E

No index was found for the column, *%s*, in the database table, *%s*. (0x38c5c1cf)

Explanation
The database does not contain an index for the specified column.

Administrator response
Correct the database configuration and restart the session management server. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0464E

The JDBC driver could not be initialized. (0x38c5c1d0)

Explanation
The JDBC driver required to access the session management server database tables could not be initialized.

Administrator response
Check the properties of the JDBC data source configured for use by the session management server. The session management server may need to be restarted.

CTGSM0602E

The session management server was not able to load the class *%s*: *%s*. (0x38c5c25a)

Explanation
The session management server configuration specifies that it must load the given class for SSO mapping, session data inspection, or data replication. The class could not be loaded, for the given reason.

Administrator response
Verify all class names specified in the session management server configuration are spelled correctly, and all necessary files are present in the application's class path.

CTGSM0603E

The session management server was not able to create an instance of the class *%s*: *%s*. (0x38c5c25b)

Explanation
The session management server encountered an error while trying to instantiate the class.

Administrator response
Check the class name is correct, and the Java security policy allows the session management server to instantiate the class, then restart the application. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0604E

The session management server configuration specifies an illegal value for the *%s* property: *%s*. (0x38c5c25c)

Explanation
The property value must be a positive integer, but the configuration file specifies either a non-integer or a negative value.

Administrator response
Modify the configuration file so a positive integer is specified for the named property, and restart the session management server.

CTGSM0617E

An unknown single sign-on mapping, *%s*, was specified for the session realm, *%s*. (0x38c5c269)

Explanation
The single sign-on mapping name specified in the configuration for a session realm does not match any of the configured single sign-on mappings.

Administrator response
Verify the single sign-on mapping name is correctly specified and restart the session management server.

CTGSM0618E

The session management server was unable to identify the version of WebSphere application server. (0x38c5c26a)

Explanation
The session management server application needs to identify the application server version in order to perform statistics gathering. This message indicates that it was not able to do so.

Administrator response
Ensure you are running the session management server application on a supported version of WebSphere application server. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0619E

A Java class name is required to be specified in the session management server configuration by property *%s*. (0x38c5c26b)

Explanation
Each extension specified in the session management server configuration must include the name of a Java class implementing the extension functionality. The specified property does not specify a class name.

Administrator response
Examine the session management server configuration. Verify all extension names and property names are specified correctly, and each extension configuration includes the correct Java class name. Restart the session management server application.

CTGSM0620E

The Java class, *%s*, specified by property, *%s*, is not a valid session management server *%s* class. (0x38c5c26c)

Explanation
The Java class configured for the specified property name does not an implementation of the expected interface.

Administrator response
Ensure all Java class names specified in the session management server configuration are correct. Restart the session management server application.

CTGSM0622W

The session management server was unable to read the Tivoli Common Directory configuration file: *%s* (0x38c5c26e)

Explanation
The session management server was unable to read the Tivoli Common Directory configuration file. The Tivoli Common Directory can be used in the logging destination configuration. Any log handlers configured to use the Tivoli Common Directory variable will write to an incorrect location until the problem is corrected.

Administrator response
Verify the Tivoli Common Directory configuration file exists and is readable. Restart the session management server once the problem has been corrected

CTGSM0626E

An error occurred while reading the configuration file *%s*: *%s* (0x38c5c272)

Explanation
An error occurred while attempting to read the configuration file.

Administrator response
Examine the error message to determine the cause of the problem. Once the problem has been corrected, restart the session management server.

CTGSM0627E

An error occurred while writing the configuration file *%s*: *%s* (0x38c5c273)

Explanation
An error occurred while attempting to write the configuration file.

Administrator response
Examine the error message to determine the cause of the problem. Once the problem has been corrected, restart the session management server.

CTGSM0633W

The session management server was unable to access the Windows registry: *%s* (0x38c5c279)

Explanation
The session management server attempts to access the Windows registry in order to locate the Tivoli Common Directory configuration file and the product installation directory. In this case the session management server was unable to access the Windows registry.

Administrator response
Examine the error message to determine the cause of the problem. Verify the WebSphere application server configuration includes a shared library definition for the session management server registry access library. Check the session management server deployment descriptor includes a reference to this shared library. If Java 2 security policy is enforced, ensure the session management server policy file includes the permissions required to load the registry access shared library. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0634E

The session management server installation directory could not be determined: *%s* (0x38c5c27a)

Explanation

The session management server was unable to determine the directory in which it is stored under the WebSphere application server install applications directory.

Administrator response

Examine the error message to determine the cause of the problem. If Java 2 security policy is enforced, ensure the session management server policy file includes the permissions required to read files in the WebSphere application server configuration directory. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0637W

An error was encountered while reading output from the process, *%s*: *%s* (0x38c5c27d)

Explanation

An error was encountered while reading output from a process run during session management server configuration.

Administrator response

No action is necessary. If the configuration process failed, not all of the output from the process will be available.

CTGSM0638E

The command, *%s*, run during session management server configuration has exceeded the time limit of *%s* seconds and has been terminated. (0x38c5c27e)

Explanation

A process run during session management server configuration has exceeded the time limit. The process has been terminated, and session management server configuration will fail as a result. The captured output from the process will be included in a later log message.

Administrator response

Examine the output from the process, which is included in a later log message, to determine the reason the process did not complete within the time limit. Restart the session management server to retry the configuration process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0639E

An error was encountered while attempting to execute the command, *%s*, during session management server configuration: *%s* (0x38c5c27f)

Explanation

An error was encountered while attempting to execute a process during session management server configuration.

Administrator response
Examine the error message to determine the cause of the problem. Restart the session management server application to retry the configuration process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0640E

The directory, *%s*, could not be created. (0x38c5c280)

Explanation
A directory could not be created.

Administrator response
Check that the file system is writable and has sufficient free space, and that the file system permissions allow the directory to be created.

CTGSM0641E

An error was encountered while configuring the Tivoli Common Directory: *%s* (0x38c5c281)

Explanation
An error was encountered while configuring the Tivoli Common Directory.

Administrator response
Examine the error message to determine the cause of the error. Restart the session management server application to retry the configuration process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0642E

Activation of the session management server configuration MBean failed: *%s* (0x38c5c282)

Explanation
Activation of the session management server configuration MBean failed.

Administrator response
Examine the error message to determine the cause of the error. It may be necessary to restart the WebSphere application server deployment manager to correct the problem.

CTGSM0644E

The session management server configuration application could not create a new WebSphere application server SSL configuration: *%s* (0x38c5c284)

Explanation
The session management server could not create a new WebSphere application server SSL configuration.

Administrator response
Examine the error message to determine the cause of the error. Run the session management server configuration program again to retry the operation. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0645E

The session management server configuration application could not remove the WebSphere application server SSL configuration, *%s*: *%s* (0x38c5c285)

Explanation

The session management server configuration application could not remove the WebSphere application server SSL configuration.

Administrator response

Examine the error message to determine the cause of the error. Attempt to remove the SSL configuration manually through the WebSphere application server administration console. Run the session management server configuration program again to retry the operation. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0648E

Failed to access the WebSphere application server configuration service. (0x38c5c288)

Explanation

The session management server could not access the WebSphere application server configuration service in order to complete its configuration.

Administrator response

If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0649E

Failed to locate the WebSphere application server security configuration. (0x38c5c289)

Explanation

The session management server could not locate the WebSphere application server security configuration in order to complete its configuration.

Administrator response

If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0651W

An error occurred while parsing the WebSphere application server configuration: *%s* (0x38c5c28b)

Explanation

An error occurred while parsing the WebSphere application server configuration. The logging for the Session management server may not function correctly until the problem is resolved.

Administrator response

The message shown describes the error condition that occurred. Take the appropriate corrective action based on the details contained within the message.

CTGSM0652E

An error occurred while retrieving the list of applications installed on the WebSphere application server: *%s* (0x38c5c28c)

Explanation
An error occurred while retrieving the list of applications installed on the WebSphere application server. The session management server configuration application will not function correctly until the problem is resolved.

Administrator response
The message shown describes the error condition that occurred. Take the appropriate corrective action based on the details contained within the message.

CTGSM0653E

An error occurred while parsing the configuration of the application, *%s*: *%s* (0x38c5c28d)

Explanation
An error occurred while parsing the configuration of the named application. The session management server configuration application will not function correctly until the problem is resolved.

Administrator response
The message shown describes the error condition that occurred. Take the appropriate corrective action based on the details contained within the message.

CTGSM0654E

An error occurred while attempting to restart the application, *%s*: *%s* (0x38c5c28e)

Explanation
An error occurred while attempting to restart the named application.

Administrator response
The message shown describes the error condition that occurred. Take the appropriate corrective action based on the details contained within the message. The session management server configuration process will not proceed until the session management server application is restarted. If the session management server application is restarted manually, the configuration process will proceed, but the results will not be reported to the configuration program.

CTGSM0659E

The deployment descriptor for the session management server application could not be located. (0x38c5c293)

Explanation
The deployment descriptor for the session management server application could not be located.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0663E

The session management server was not able to create an instance of the class *%s*. (0x38c5c297)

Explanation
The session management server encountered an error while trying to instantiate the class.

Administrator response
Examine the log for earlier messages indicating why the class could not be instantiated. Check the class name is correct, and the Java security policy allows the session management server to instantiate the class, then restart the application. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0666E

The specified configuration session is not active. (0x38c5c29a)

Explanation
The specified configuration session is not active. This may mean that the target session management server instance has been restarted, or that the configuration session has been displaced by a newer session.

Administrator response
Retry the configuration action.

CTGSM0667E

The session management server was not able to lock the distributed configuration: *%s* (0x38c5c29b)

Explanation
Before updating its configuration, the session management server first locks the configuration to protect against concurrent updates. This failure may indicate there are communication problems between the WebSphere application servers hosting the session management server.

Administrator response
Examine the detailed error message and previous entries in the WebSphere application server logs for more information about the error.

CTGSM0668E

The session management server was not able to unlock the distributed configuration: *%s* (0x38c5c29c)

Explanation
Before updating its configuration, the session management server first locks the configuration to protect against concurrent updates. This failure may indicate there are communication problems between the WebSphere application servers hosting the session management server.

Administrator response
Examine the detailed error message and previous entries in the WebSphere application server logs for more information about the error.

CTGSM0669E

The session management server was not able to retrieve the configuration state from other instances in the cluster: *%s* (0x38c5c29d)

Explanation

This may indicate there are communication problems between the WebSphere application servers hosting the session management server.

Administrator response

Examine the detailed error message and previous entries in the WebSphere application server logs for more information about the error.

CTGSM0670E

The session management server was not able to distribute the updated configuration across the cluster: *%s* (0x38c5c29e)

Explanation

The session management server was not able to distribute the updated configuration to other instances in the cluster. This may indicate that there are communication problems between the WebSphere application servers hosting the session management server. Unless this problem is corrected, future configuration operations may operate on an outdated version of the configuration.

Administrator response

Examine the detailed error message and previous entries in the WebSphere application server logs for more information about the error. It may be necessary to restart the application server instance that logged this message.

CTGSM0671E

The session management server was not able to distribute configuration result information across the cluster: *%s* (0x38c5c29f)

Explanation

The session management server was not able to distribute the updated configuration to other instances in the cluster. This may indicate that there are communication problems between the WebSphere application servers hosting the session management server.

Administrator response

Examine the detailed error message and previous entries in the WebSphere application server logs for more information about the error. It may be necessary to restart the application server instance that logged this message.

CTGSM0672E

The new configuration is based on a previous version of the configuration. The current configuration is version *%d* and the new configuration is version *%d*. (0x38c5c2a0)

Explanation

An update to the session management server configuration has a version number older than or equal to that of the current configuration.

Administrator response
Retry the configuration operation.

CTGSM0673E

A component with the name *%s* already exists in the *%s* component set. (0x38c5c2a1)

Explanation
An attempt was made to add a component to a set using a name already present in that component set.

Administrator response
Retry the operation using a different name for the component.

CTGSM0674E

The component *%s* from component set *%s* failed to initialize: *%s* (0x38c5c2a2)

Explanation
An SMS component failed to initialize. The component will not be available until the problem is fixed. This may make the session management server unavailable until the problem is fixed.

Administrator response
Examine the error message for details of the failure. It may be necessary to reconfigure or restart the session management server.

CTGSM0675E

The component *%s* was not found in the component set *%s*. (0x38c5c2a3)

Explanation
The specified component does not exist in the configuration.

Administrator response
Check the component name and retry the configuration operation.

CTGSM0676E

An unknown configuration component set identifier, *%d*, was specified. (0x38c5c2a4)

Explanation
The configuration component set specified does not match any of the known component sets.

Administrator response
Check the component set identifier and retry the configuration operation.

CTGSM0677E

The session realm, *%s*, cannot be removed because it still contains replica sets. (0x38c5c2a5)

Explanation
Session realms cannot be removed while they still contain replica sets.

Administrator response
Remove the replica sets that are still in the session realm before removing the session realm.

CTGSM0678E

An unknown session realm name, *%s*, is specified in the configuration for the replica set, *%s*. (0x38c5c2a6)

Explanation
The configuration for the replica set specifies a session realm name that does not match any configured session realm.

Administrator response
Check the session realm name for the replica set. Either create a session realm matching the name specified in the replica set configuration or change the replica set configuration to match an existing session realm. The replica set will not be available until the problem is corrected.

CTGSM0679E

An attempt to process an SMS event failed: *%s*. (0x38c5c2a7)

Explanation
The session management server encountered an error while trying to process an event.

Administrator response
Examine the log for other messages relating to this error, and take any necessary corrective action. If the problem persists, restart the session management server.

CTGSM0750E

The SecureRandom algorithm, *%s*, could not be loaded: *%s* (0x38c5c2ee)

Explanation
The SecureRandom algorithm specified in the session management server configuration could not be loaded.

Administrator response
Verify the SecureRandom algorithm specified in the session management server configuration is correct, and restart the application.

CTGSM0751E

The SecureRandom provider, *%s*, was not found: *%s* (0x38c5c2ef)

Explanation
The SecureRandom provider specified in the session management server configuration could not be found.

Administrator response
Verify the SecureRandom provider specified in the session management server configuration is correct, and restart the application.

CTGSM0752E

The session management server was unable to determine the current key details. (0x38c5c2f0)

Explanation
The session management server was unable to determine the current key details. The key information may have become corrupted.

Administrator response
Request a change of key using the administration interface. If the problem persists, restart the session management server.

CTGSM0753E

The session management server was unable to find the key with ID: *%s*. (0x38c5c2f1)

Explanation
The session management server was unable to find the key. The key information may have become corrupted.

Administrator response
Request a change of key using the administration interface. If the problem persists, restart the session management server.

CTGSM0754E

An error occurred while updating the key distribution information. The parameter, *%s*, could not be associated with the value: *%s*. (0x38c5c2f2)

Explanation
While updating the key distribution information, the session management server encountered an error.

Administrator response
Examine the log for other messages relating to this error, and take any necessary corrective action. Request a key change using the administration interface. If the problem persists, restart the session management server.

CTGSM0755W

An error occurred while updating the key distribution information. The expired key, *%s*, could not be removed. (0x38c5c2f3)

Explanation
While updating the key distribution information, the session management server encountered an error. This condition does not effect the operation of the session management server, but it may indicate future errors.

Administrator response
Examine the log for other messages relating to this error, and take any necessary corrective action. Unless the other messages indicate a serious problem, it is not necessary to request a new key or restart the session management server.

CTGSM0901E

The session management server was not able to initialize the IBM Security Verify Access Runtime for Java: *%s* (0x38c5c385)

Explanation
The session management server must initialize the IBM Security Verify Access Runtime for Java. This message indicates the initialization failed

Administrator response
Examine this and earlier log messages for information regarding the error and take any necessary corrective action. Verify the IBM Security Verify Access Runtime for Java configuration URL is specified correctly. The session management server application must be restarted.

CTGSM0902W

An error occurred while accessing a IBM Security Verify Access credential: *%s* (0x38c5c386)

Explanation
An error occurred while accessing a IBM Security Verify Access credential.

Administrator response
Examine the error message for specific details of the error. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0903W

The session, *%s*, does not contain a IBM Security Verify Access credential. (0x38c5c387)

Explanation
The identified session does not contain a IBM Security Verify Access credential. All authenticated sessions stored in the session management server must contain a credential.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0904E

A configuration value required to configure the IBM Security Verify Access Runtime for Java is missing: *%s*. (0x38c5c388)

Explanation
One of the configuration values required to configure the IBM Security Verify Access Runtime for Java is missing.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM0905E

Configuration of the IBM Security Verify Access Runtime for Java failed: *%s* (0x38c5c389)

Explanation
Configuration of the IBM Security Verify Access Runtime for Java has failed.

Administrator response
Examine the error message for information regarding the error and take any necessary corrective action. Verify that the IBM Security Verify Access policy server and the user registry server are available. The session management server application must be restarted.

CTGSM0906E

Unconfiguration of the IBM Security Verify Access Runtime for Java failed: *%s* (0x38c5c38a)

Explanation
Unconfiguration of the IBM Security Verify Access Runtime for Java has failed.

Administrator response
Examine the error message for information regarding the error and take any necessary corrective action. Verify that the IBM Security Verify Access policy server and the user registry server are available. The session management server application must be restarted.

CTGSM0907E

An error was encountered while creating the key and trust store files used to authenticate clients of the session management server: *%s* (0x38c5c38b)

Explanation
An error was encountered while creating the key and trust store files used to authenticate clients of the session management server.

Administrator response
Examine the error message for information regarding the error and take any necessary corrective action. Verify that the necessary Java security providers are available. The session management server application must be restarted.

CTGSM0908E

IBM Security Verify Access integration has not been enabled for the session management server. (0x38c5c38c)

Explanation
A Security Verify Access configuration operation was requested, but Security Verify Access integration has not been enabled.

Administrator response
Enable Security Verify Access integration before attempting further Security Verify Access configuration.

CTGSM0909E

The IBM Security Verify Access Runtime for Java is not currently available. (0x38c5c38d)

Explanation
The IBM Security Verify Access Runtime for Java is not currently available.

Administrator response
Examine earlier log messages to determine the cause of the problem. This may indicate a problem with the IBM Security Verify Access policy server. The session management server may need to be restarted.

CTGSM0910W

The session, *%s*, does not contain a user UUID. (0x38c5c38e)

Explanation
The identified session does not contain a user UUID. This information is required for the recording of last login information. The information should be supplied either as session data, or as a part of a IBM Security Verify Access credential.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM1050E

Multiple values for the *%s* attribute of the *%s* session management server administration interface request were specified but no more than one value may be specified. (0x38c5c41a)

Explanation
The client sent multiple values for the indicated request attribute but the attribute may only have a single value.

Administrator response
Ensure the version of the client software in use is supported by this version of the session management server.

CTGSM1051E

The *%s* attribute of the *%s* session management server administration interface request must be an integer value - the *%s* value cannot be parsed as an integer. (0x38c5c41b)

Explanation
The specified request attribute must be an integer but the value provided by the client cannot be parsed as an integer value.

Administrator response
Ensure the version of the client software in use is supported by this version of the session management server.

CTGSM1052E

The *%s* attribute of the *%s* session management server administration interface request has a lower bound of *%s* - the value *%s* is too low. (0x38c5c41c)

Explanation

The client specified a value for the specified request attribute that is less than the identified attribute's minimum valid value.

Administrator response

Ensure the version of the client software in use is supported by this version of the session management server.

CTGSM1053E

The *%s* attribute of the *%s* session management server administration interface request has an upper bound of *%s* - the value *%s* is too high. (0x38c5c41d)

Explanation

The client specified a value for the specified request attribute that is greater than the identified attribute's maximum valid value.

Administrator response

Ensure the version of the client software in use is supported by this version of the session management server.

CTGSM1054E

The required *%s* attribute of the *%s* session management server administration interface request was not provided by the client. (0x38c5c41e)

Explanation

A required request attribute was not sent by the session management server administration interface client.

Administrator response

Ensure the version of the client software in use is supported by this version of the session management server.

CTGSM1055E

The value (*%s*) of the *%s* attribute of the *%s* session management server administration interface request could not be processed. Error: *%s*. (0x38c5c41f)

Explanation

The indicated value of the indicated attribute is not valid when specified as part of the indicated session management server administration interface request.

Administrator response

If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM1059E

The session realm *%s* specified in a *%s* request of the session management server's administration interface is not recognized by the session management server. (0x38c5c423)

Explanation
The request from the client specified an undefined session realm name.

Administrator response
Retry the operation specifying a defined session realm name.

CTGSM1060E

The *%s* request failed with error: *%s* (0x38c5c424)

Explanation
The request from the client could not be executed.

Administrator response
Examine the log for further detailed messages regarding the error and take any necessary corrective action.

CTGSM1061E

The *%s* request caused an exception: *%s*Exception stack trace:*%s* (0x38c5c425)

Explanation
The request from the client caused the indicated exception.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM1062E

No HTTP request for administration service authorization. (0x38c5c426)

Explanation
The HTTP request object could not be accessed while authorizing an administration service operation.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM1063E

The user *%s* is not permitted to delegate access to the administration service. (0x38c5c427)

Explanation
The identified user is not permitted to delegate access to the administration service.

Administrator response
If the identified user is expected to be able to delegate access to the administration service ensure they have the sms-delegator role.

CTGSM1064E

Unable to authorize access for the *%s* operation requiring the *%s* role for user *%s* delegated by user *%s*. (0x38c5c428)

Explanation
Authorization of a user for this operation has failed. For further detailed information about the failure examine earlier messages in the log containing this message. Correct any problems and retry the operation.

Administrator response
Examine the log containing this message for more information describing the error that occurred and take the appropriate corrective action.

CTGSM1065E

Authorization of user *%s* for role *%s* failed. *%s* exception: *%s* (0x38c5c429)

Explanation
The specified exception occurred while attempting to authorize the user for the role.

Administrator response
The message shown describes the error condition that occurred. Take the appropriate corrective action.

CTGSM1066E

The administration request type, *%s*, cannot be handled by class, *%s*, as specified by handler, *%s*, as it is already configured to be handled by the class, *%s*. (0x38c5c42a)

Explanation
The session management server administration requests may only be configured to be handled by one handler. This message indicates that a single request type is configured to be handled by more than one handler.

Administrator response
Ensure the session management server administration request handlers are configured correctly and restart the application.

CTGSM1067E

Failed to locate the DSessAdmin request dispatcher. (0x38c5c42b)

Explanation
The request from the client could not be executed.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM1363E

Validation of the last login information database table failed. (0x38c5c553)

Explanation
The last login information database table has not been correctly created.

Administrator response
Refer to earlier log messages regarding the creation of the last login information database table. Check that the table exists in the database. It may be necessary to modify the table manually to allow the table validation to succeed.

CTGSM1369E

An error occurred while installing a component into the WebSphere application server runtime. The file, *%s*, could not be copied to the target location, *%s*. (0x38c5c559)

Explanation
An error occurred while installing a component into the WebSphere application server runtime.

Administrator response
Check that the permissions on the target directory permit the file to be copied and that there is sufficient disk space. The file may also be copied into place manually. Restart the session management server application.

CTGSM1500W

The host name of this machine could not be determined. (0x38c5c5dc)

Explanation
The host name of the machine on which the session management server is running could not be determined.

Administrator response
Check that the system host name and network devices have been configured correctly. Restart the session management server application.

CTGSM1501E

User information is required to report an audit event but no session information is available. (0x38c5c5dd)

Explanation
User information is required to report an audit event but no session information is available.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM1505W

The session creation time, *%s*, is in the future. Check time synchronization between SMS and client *%s*. (0x38c5c5e1)

Explanation
The session creation timestamp associated with the session being terminated is later than the current time. This indicates clock skew between the SMS and the client that created the session.

Administrator response
Synchronize the clocks of the SMS system and its clients and restart the SMS.

CTGSM1506E

The auditing emitter configuration has been set to debug mode. Events will not be sent to a CARS emitter, they will be written to the log file. (0x38c5c5e2)

Explanation
The auditing emitter configuration has been set to debug mode. Events will not be sent to a CARS emitter, they will be written to the log file.

Administrator response
No action is necessary.

CTGSM1507E

The CARS Security Event Factory reported an error while constructing an event: *%s* (0x38c5c5e3)

Explanation
The common audit reporting service (CARS) Security Event Factory reported an error while constructing an event for the reported reason.

Administrator response
Examine the reason for the failure and take any necessary corrective action.

CTGSM1509E

The CARS emitter reported an error while sending an event: *%s* (0x38c5c5e5)

Explanation
The common audit reporting service (CARS) emitter reported an error while sending an event for the reported reason.

Administrator response
Examine the reason for the failure and take any necessary corrective action.

CTGSM1514E

The common audit and reporting service (CARS) encountered a severe error when initializing: Error: *%s*, cause: *%s*Error stack trace:*%s*Cause stack trace:*%s* (0x38c5c5ea)

Explanation
The common audit and reporting service (CARS) encountered a severe error when initializing.

Administrator response
Examine the reason for the failure and take any necessary corrective action.

CTGSM1515E

The common auditing service encountered a severe error when shutting down: Error: *%s*, cause: *%s*Error stack trace:*%s*Cause stack trace:*%s* (0x38c5c5eb)

Explanation
The common auditing service encountered a severe error when shutting down.

Administrator response
No action is necessary.

CTGSM1654E

The command line option, *%s*, is not recognized. (0x38c5c676)

Explanation
The identified command line option of the smsbackup command is not recognized by the smsbackup command.

Administrator response
Re-run the smsbackup command with correct command line options.

CTGSM1655E

The *%s* command line option requires an argument. (0x38c5c677)

Explanation
The identified smsbackup command line option requires an argument.

Administrator response
Consult the documentation for the smsbackup command and re-run it specifying a valid argument for the option.

CTGSM1656E

The argument to the -list option must be a readable file. The value provided, *%s*, is not a readable file. (0x38c5c678)

Explanation
The value provided for the -list option of the smsbackup command does not identify a readable file.

Administrator response
Re-run the smsbackup command specifying a valid value for the -list option.

CTGSM1657E

The file, *%s*, could not be opened: *%s* (0x38c5c679)

Explanation
The identified file could not be opened for the specified reason.

Administrator response
Ensure that the name of the file is correct, that it exists and is that it is readable.

CTGSM1658W

Line *%s* of the list file *%s*, *%s*, cannot be interpreted. (0x38c5c67a)

Explanation
Not all of the contents of the file specified by the -list option could be interpreted correctly.

Administrator response
Ensure the list file name is specified correctly and that the contents of the file are not corrupt.

CTGSM1659E

The file, *%s*, could not be backed up: *%s* (0x38c5c67b)

Explanation
The file was indicated to be backed up by the list file and does exist but could not be backed for the reason indicated by the exception shown.

Administrator response
Ensure that all files required to be backed up are accessible to the smsbackup program.

CTGSM1660E

The command, *%s*, could not be executed: *%s* (0x38c5c67c)

Explanation
The command was indicated to be executed by the list file but execution failed for the reason indicated by the exception shown.

Administrator response
Ensure that all programs required to be executed are accessible to the smsbackup program.

CTGSM1662E

The directory, *%s*, could not be created: *%s* (0x38c5c67e)

Explanation
The directory specified as the output path does not exist and could not be created.

Administrator response
Re-run the smsbackup command specifying a different value for -path option or ensuring that you have permission to create the specified directory.

CTGSM1663E

An error occurred writing to the file, *%s*: *%s* (0x38c5c67f)

Explanation
The file specified could not be written to for the reason indicated.

Administrator response
Ensure that the file system containing the file has sufficient space and that the directory containing the file may be written to.

CTGSM1800E

The property, *%s*, which is required to configure the Java client API is missing. (0x38c5c708)

Explanation
One of the configuration values required to configure the Java client API is missing.

Administrator response
Add the property to the supplied properties object.

CTGSM1801E

A configuration value required to configure the Java client API is missing: *%s*. (0x38c5c709)

Explanation
The specified configuration item has not been supplied to the DSessClientConfig class.

Administrator response
Ensure that the specified configuration item is passed into the DSessClientConfig class.

CTGSM1802E

The session management interface of any configured session management server could not be accessed. (0x38c5c70a)

Explanation
An unsuccessful attempt has been made to communicate with the session management interface of each configured session management server.

Administrator response
Ensure the session management interface of at least one configured session management server is available and can be reached by the client. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM1803E

An internal error occurred within the Java client API: *%s*. (0x38c5c70b)

Explanation
An internal error occurred within the Java client API.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM1804E

The MAC algorithm, *%s*, could not be loaded: *%s* (0x38c5c70c)

Explanation
The MAC algorithm which is used for Session ID generation and validation could not be loaded.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM1805E

The provided session ID, *%s*, is invalid. (0x38c5c70d)

Explanation
The session ID that was provided to the Java client API failed the cyrpographic check which is used to validate ID's.

Administrator response
The client of the API should disregard the locally cached session and should return an error back to the client.

CTGSM1806E

The provided session ID, *%s*, was incorrectly formatted. (0x38c5c70e)

Explanation
The session ID that was provided to the Java client API was of an incorrect format.

Administrator response
The client of the API should disregard the locally cached session and should return an error back to the client.

CTGSM1807E

A request was made to send a session which contained no data to the SMS. (0x38c5c70f)

Explanation
The session which was to be sent to the SMS contains no session data.

Administrator response
The client of the API should not be sending any empty sessions to the SMS. A review of the client code should be conducted.

CTGSM1950E

An exception occurred while performing a WebSphere eXtreme Scale data replication operation: *%s* (0x38c5c79e)

Explanation
An exception occurred while performing a WebSphere eXtreme Scale data replication operation.

Administrator response
Examine the details of the WebSphere eXtreme Scale error to determine the cause and take appropriate action. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM1951E

The session management server was unable to initialize the WebSphere eXtreme Scale data replication service. (0x38c5c79f)

Explanation
The session management server was unable to initialize the WebSphere eXtreme Scale data replication service.

Administrator response
Examine previous log messages for more details of the underlying cause of the failure. Once the underlying problem has been corrected, restart the application server.

CTGSM1952E

Initialization of the WebSphere eXtreme Scale data replication service failed: *%s* (0x38c5c7a0)

Explanation
Initialization of the WebSphere eXtreme Scale data replication service failed. The session management server will not function until this problem is corrected.

Administrator response
Examine the details of the WebSphere eXtreme Scale error to determine the cause. Once the underlying problem has been corrected, restart the application server. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

CTGSM1954E

An exception occurred during a remote WebSphere eXtreme Scale operation on server *%s*: *%s* (0x38c5c7a2)

Explanation
An exception occurred during a WebSphere eXtreme Scale operation on a remote server.

Administrator response
Examine the details of this message and the logs on the named server for more information on the cause of the problem and take any appropriate action.

DPWAD0309E

The WebSEAL administration service has not been initalized. (0x38983135)

Explanation
The WebSEAL administration service plug-in failed to initialize properly.

Administrator response
Check for other initialization errors and/or configuration problems that may have previously occurred.

DPWAD0312E

Object list failed: %s (0x38983138)

Explanation
The object list command failed to complete correctly.

Administrator response
This is a generic error which will contain further details when output.

DPWAD0328E

The junction import command received invalid data (0x38983148)

Explanation
An error occurred when trying to extract one or more of the junction attributes sent in the admin command.

Administrator response
Check that the data being passed into the junction import command is valid.

DPWAD0329E

The junction import command received an invalid version (0x38983149)

Explanation
The version in the junction definition is not supported by this version of WebSEAL

Administrator response
Check the version of the junction in the XML definition

DPWAD0330E

The junction import could not create the junction file (0x3898314a)

Explanation
WebSEAL can not create the junction file.

Administrator response
Check the filesystem to make sure there is space available, or that the WebSEAL server has permissions to create/write the file.

DPWAD0331E

The junction import could not write the junction file (0x3898314b)

Explanation
An error occurred writing the junction definition.

Administrator response
Check the filesystem to make sure there is space available, or that the WebSEAL server has permissions to create/write the file.

DPWAD0332E

The junction export could not read the junction directory (0x3898314c)

Explanation
An error occurred while trying to read the contents of the junction database directory.

Administrator response
Check to make sure that WebSEAL is able to read the contents of the directory which is configured to contain the junction definitions.

DPWAD0333E

Unable to add junction attributes into command handler (0x3898314d)

Explanation
An error occurred returning the junction data to the client

Administrator response
This is an internal error which occurs when WebSEAL is marshalling the junction data to the export command. Check for other errors occurring previously.

DPWAD0334E

An invalid junction point was specified. (0x3898314e)

Explanation
WebSEAL was unable to build the junction filename.

Administrator response
An internal error occurred in WebSEAL when trying to build the encoded filename. Check for previous errors.

DPWAD0335E

Error reading junction point *%s*. (0x3898314f)

Explanation
The file name representing the junction could not constructed.

Administrator response
An internal error occurred in WebSEAL when trying to build the encoded filename. Check for previous errors.

DPWAD0336E

Error reading junction file *%s*. (0x38983150)

Explanation
There was an error opening or parsing the junction definition file.

Administrator response
Verify the .xml file exists, is readable, and has valid data.

DPWAD0342E

Error reading input user session id. (0x38983156)

Explanation
There was an error parsing the user session id.

Administrator response
Verify that the input is being passed correctly.

DPWAD0343E

Error reading input user id. (0x38983157)

Explanation
There was an error parsing the user ID.

Administrator response
Verify that user ID is being input correctly.

DPWAD0345E

No matching User Session found. (0x38983159)

Explanation
Bad input, or User session was already terminated.

Administrator response
Verify validity of input, or assume session was already terminated.

DPWAD0362E

The dynurl configuration file *%s* cannot be opened for reading. (0x3898316a)

Explanation
An attempt to open the dynurl configuration file for reading failed

Administrator response
Ensure that the file exists on the WebSEAL server and is readable

DPWAD0363E

The jmt configuration file *%s* cannot be opened for reading. (0x3898316b)

Explanation
An attempt to open the jmt configuration file for reading failed

Administrator response
Ensure that the file exists on the WebSEAL server and is readable

DPWAD0364E

You must specify a junction point to read or write an fsso configuration file. (0x3898316c)

Explanation
A junction point is necessary to determine which fsso configuration file to read or write

Administrator response
Add the junction point to the junction attribute of the indata attribute list

DPWAD0365E

The junction: *%s* is not a valid junction on this WebSEAL server. (0x3898316d)

Explanation
An invalid junction point was provided.

Administrator response
Ensure that the junction attribute in indata is a valid junction

DPWAD0366E

The junction: *%s* is not an fsso junction on this WebSEAL server. (0x3898316e)

Explanation
The junction specified is not an FSSO junction.

Administrator response
Ensure that the junction specified is an FSSO junction.

DPWAD0367E

The fsso configuration file: *%s* could not be opened for reading. (0x3898316f)

Explanation
The junction specified could not be opened.

Administrator response
Ensure that the fsso configuration file for the junction specified exists and is readable.

DPWAD0368E

Could not create dynurl configuration file: *%s* (0x38983170)

Explanation
WebSEAL was unable to create the dynurl conf file.

Administrator response
Ensure that ivmgr has filesystem permissions to create a file in the directory where the dynurl configuration file will be stored

DPWAD0369E

Reloading the in memory dynurl table failed (0x38983171)

Explanation
An error occurred while trying to read the dynurl configuration file.

Administrator response
Ensure that the new file specified is in the proper format

DPWAD0370E

Could not create jmt configuration file: *%s* (0x38983172)

Explanation
An error occurred while trying to open the jmt configuration file.

Administrator response
Ensure that ivmgr has filesystem permissions to create a file in the directory where the jmt configuration file will be stored

DPWAD0371E

Reloading the in memory jmt table failed (0x38983173)

Explanation
An error occurred while trying to read in the new jmt configuration file.

Administrator response
Ensure that the new file specified is in the proper format.

DPWAD0372W

The junction specified does not exist. The configuration file: *%s* was created. (0x38983174)

Explanation
An fsso junction may not be created without the configuration file being inplace. This allows the file to be created before the junction

Administrator response
The junction may now be created using this new configuration file

DPWAD0373E

Could not create fsso configuration file: *%s* (0x38983175)

Explanation
An error occurred while trying to read in the new fsso configuration file.

Administrator response
Ensure that ivmgr has filesystem permissions to create a file in the directory where the fsso configuration file will be stored

DPWAD0374E

The backup operation failed for *%s* (0x38983176)

Explanation
An error occurred while attempting to create a backup copy of the original configuration file.

Administrator response
Ensure that ivmgr has filesystem permissions to create a file in the directory where the configuration file resides.

DPWAD0375E

Reloading junction: *%s* failed (0x38983177)

Explanation
An error occurred while trying to load the fsso configuration file.

Administrator response
Ensure that the new file specified is in the proper format.

DPWAD0376E

The restore operation failed for *%s* (0x38983178)

Explanation
An error occurred while trying to restore a backed up version of a configuration file.

Administrator response
Ensure that ivmgr has filesystem permissions to create a file in the directory where the configuration file resides.

DPWAD0386E

Failed to open the supplied junction archive file. (0x38983182)

Explanation
An error occurred when trying to access a junction archive file.

Administrator response
Ensure that the specified file name is correct and that the WebSEAL server can access the file.

DPWAD0387E

The supplied junction archive file contains an invalid junction definition. (0x38983183)

Explanation
An error occurred while trying to access a junction archive file.

Administrator response
Ensure that the supplied file is correctly formatted.

DPWAD0391W

Failed to execute the program (*%s*). (Errno = *%d*). (0x38983187)

Explanation
An error occurred when attempting to run the specified program.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWAD0394W

The requested file segment contained binary characters. (0x3898318a)

Explanation
A request to display a binary file was submitted. A binary file can be displayed only if the '-encode' option is supplied.

Administrator response
Ensure that the correct file has been requested and if so that the '-encode' option is supplied to the command.

DPWAD0404E

Failed to locate the authorization server password, required for the server sync command. (0x38983194)

Explanation
The server sync command is not available because the authorization server password could not be determined.

Administrator response
Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Verify Access for Web Troubleshooting Guide.

DPWAD0405E

Failed to synchronize the WebSEAL server. (0x38983195)

Explanation
The server sync command did not complete successfully.

Administrator response
Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Verify Access for Web Troubleshooting Guide.

DPWAD0406E

The server name supplied was not valid. (0x38983196)

Explanation
The server name supplied to the server sync command was not valid.

Administrator response
Ensure that a valid server name is supplied with the server sync command. The server name must not be the same as the name of the server that runs the command.

DPWAD0411E

The TCP/IP host information could not be determined from the server hostname: *%s*. Ensure that the server hostname is correct and that the domain name server is functioning correctly. (0x3898319b)

Explanation
The TCP/IP address for the specified host could not be determined.

Administrator response
Ensure that the IP address for the specified host name can be resolved. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWAD0412E

The configuration entry found within the *%s* stanza was not valid: *%s* = *%s*. (0x3898319c)

Explanation
The specified configuration entry contained a value that must be corrected.

Administrator response
Correct the configuration entry which is not valid.

DPWAD0413E

An attempt to create a temporary file failed. (0x3898319d)

Explanation
An attempt was made to create a temporary file and the file could not be created.

Administrator response
Check the log file for additional errors. Also check the file system to ensure that there is adequate disk space available.

DPWAD0415E

An ICAP Server for the '*%s*' resource was not found. (0x3898319f)

Explanation
An unknown ICAP resource was specified.

Administrator response
Check the ICAP configuration within both the WebSEAL configuration file and the policy database.

DPWAD0416E

An ICAP Server for the specified resource was not found. (0x389831a0)

Explanation
An unknown ICAP resource was specified.

Administrator response
Check the log file for additional errors.

DPWAD0417E

A bad response was received from the ICAP server. (0x389831a1)

Explanation
The response which was received from the ICAP server was incorrectly formatted.

Administrator response
Check the configuration of the ICAP server.

DPWAD0418E

Failed to connect to the ICAP server: *%s*. (0x389831a2)

Explanation
An attempt to contact an ICAP server failed. The ICAP server is required to be able to correctly service the Web request.

Administrator response
Ensure that the configuration for the ICAP server is correct and that the ICAP server is available. Check the log file for additional errors.

DPWAD0419E

Failed to connect to a required ICAP server. (0x389831a3)

Explanation
An attempt to contact an ICAP server failed. The ICAP server is required to be able to correctly service the Web request.

Administrator response
Ensure that the configuration for the ICAP server is correct and that the ICAP server is available. Check the log file for additional errors.

DPWAD0420E

The maximum number of concurrent requests which can be processed for this session has been reached. (0x389831a4)

Explanation
The user session has reached the maximum number of simultaneous requests which can be processed by WebSEAL.

Administrator response
Either increase the configured maximum number of requests which can be processed by a session, or wait for existing requests for the user session to complete.

DPWAD0421W

The session, owned by *%s*, has reached it's soft limit of *%d* concurrent requests. (0x389831a5)

Explanation
The user session has reached the warning point for the number of simultaneous requests which can be processed by WebSEAL.

Administrator response
Prepare to increase the hard limit of concurrent requests for a user session, or wait for existing requests for the user session to complete.

DPWAD0431E

Failed to locate the authorization server password, required for the cluster functionality. (0x389831af)

Explanation
The cluster support is not available because the authorization server password could not be determined.

Administrator response
Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Verify Access for Web Troubleshooting Guide.

DPWAD0432E

Failed to execute the server task '*%s*' on *%s*: *%s* (0x389831b0)

Explanation
An attempt to execute a server task command failed.

Administrator response
Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Verify Access for Web Troubleshooting Guide.

DPWAD0433E

Failed to execute a server task command (0x389831b1)

Explanation
An attempt to execute a server task command failed.

Administrator response
Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Verify Access for Web Troubleshooting Guide.

DPWAD0434E

Failed to create the administration context for *%s*: *%s* (0x389831b2)

Explanation
An attempt to create an administration context failed.

Administrator response
Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Verify Access for Web Troubleshooting Guide.

DPWAD0435E

Failed to create an administration context (0x389831b3)

Explanation
An attempt to create an administration context failed.

Administrator response
Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Verify Access for Web Troubleshooting Guide.

DPWAD0436E

An unexpected result was received from the server task command: *%s* (*%s*) (0x389831b4)

Explanation
An unexpected result was received from the server task command.

Administrator response
Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Verify Access for Web Troubleshooting Guide.

DPWAD0438E

Failed to synchronize with the cluster master (0x389831b6)

Explanation
An attempt to synchronize the local configuration with the cluster master server failed.

Administrator response
Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Verify Access for Web Troubleshooting Guide.

DPWAD0439E

Failed to restart the cluster (0x389831b7)

Explanation
An attempt to restart the cluster failed.

Administrator response
Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Verify Access for Web Troubleshooting Guide.

DPWAD0440E

Failed to restart the cluster: 0x*%lx* (0x389831b8)

Explanation
An attempt to restart the cluster failed.

Administrator response
Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Verify Access for Web Troubleshooting Guide.

DPWAD0441E

Failed to restart the cluster as a cluster restart is already in progress (0x389831b9)

Explanation
An attempt to restart the cluster failed as a prior request to restart the cluster is still in progress.

Administrator response
Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Verify Access for Web Troubleshooting Guide.

DPWAD0442E

The server, *%s*, failed to restart within a reasonable period of time. (0x389831ba)

Explanation
The specified server did not restart within the allocated period of time. This restart was performed as a part of the cluster synchronisation.

Administrator response
Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Verify Access for Web Troubleshooting Guide.

DPWAD0445E

%s (0x389831bd)

Explanation
An unspecified error has occurred.

Administrator response
Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Verify Access for Web Troubleshooting Guide.

DPWAD0446E

Both the '-ripple' and '-status' options cannot be specified at the same time. (0x389831be)

Explanation
The cluster restart command cannot have both the '-ripple' and '-status' options specified in the same command.

Administrator response
Re-issue the command with either of the options, but not both.

DPWAD0447E

The server is not fully initialized. (0x389831bf)

Explanation
An attempt to access the server failed due to the fact that it is not fully initialized. This can occur during server start-up or shutdown.

Administrator response
Allow extra time for the server to finish initialization and then retry the operation. If the problem persists check the log file for additional errors.

DPWAD0448E

The new user identity (*%s*) does not match the current authenticated user identity (*%s*). (0x389831c0)

Explanation
The identity which is provided in a subsequent authentication operation must match the identity which was used during the original authentication operation.

Administrator response
The user must present the same user ID provided in the previous authentication operation.

DPWAD0449E

The new user identity does not match the current authenticated user identity. (0x389831c1)

Explanation
The identity which is provided in a subsequent authentication operation must match the identity which was used during the original authentication operation.

Administrator response
The user must present the same user ID provided in the previous authentication operation.

DPWAD0452E

eCSSO authentication is enabled but no Master Authorization Server is defined. (0x389831c4)

Explanation
The e-community-sso-auth has been set without setting a master authorization server.

Administrator response
Update the configuration file and set a master authorization server in the master-authn-server value under the [e-community-sso] stanza.

DPWAD0453E

Duplicate eCSSO domain '*%s*' defined under the [e-community-domains] stanza. (0x389831c5)

Explanation
Each domain under the [e-community-domains] stanza must be unique.

Administrator response
Remove the duplicate entry and retry.

DPWAD0454E

Unable to configure the eCSSO authentication module for domain/host '*%s*': status 0x*%lx*. (0x389831c6)

Explanation
The eCSSO (consume or create) authentication module configured for the domain/host specified returned an error while being initialised.

Administrator response
Either a bad shared library was specified for the authentication module or the configuration is incorrect, for example the key files specified are missing or inaccessible.

DPWAD0455E

The value '*%s*' is not a valid option for ip-support-level. Use one of 'displaced-only', 'generic-only', or 'displaced-and-generic'. (0x389831c7)

Explanation
An invalid setting was set for the webseald configuration file option ip-support-level.

Administrator response
Change the setting for ip-support-level to a valid one.

DPWAD0456E

The value displaced-only is not a valid option for ip-support-level when ipv6-support is enabled. (0x389831c8)

Explanation
displaced-only can not be set when ipv6-support = yes.

Administrator response
Change the setting for ip-support-level to generic-only or displaced-and-generic.

DPWAD0457E

The authentication challenge type specified is not valid: *%s* (0x389831c9)

Explanation
The challenge type string located in the WebSEAL configuration file was not valid.

Administrator response
Change the setting for auth-challenge-type to be a valid challenge type.

DPWAD0458E

The corresponding authentication method for the challenge type, *%s*, is not enabled. (0x389831ca)

Explanation
The corresponding authentication method for the specified challenge type is not enabled.

Administrator response
Either remove the failing challenge type from the auth-challenge-type configuration entry, or enable the corresponding authentication method.

DPWAD0459E

The authentication challenge type contains multiple entries for *%s*. (0x389831cb)

Explanation
The challenge type string located in the WebSEAL configuration file contains multiple rule sets for a single mechanism.

Administrator response
Remove the duplicate entries in the auth-challenge-type configuration entry.

DPWAD0460E

The following authentication challenge type contains a syntax error or invalid pattern.*%s* (0x389831cc)

Explanation
The challenge type string located in the WebSEAL configuration file contains a syntax error.

Administrator response
Correct the syntax error for the auth-challenge-type configuration entry.

DPWAD0600E

An error occurred attempting to determine the current installed version of WebSEAL. WebSEAL cannot start. (0x38983258)

Explanation
This error occurs if the current installed version of WebSEAL cannot be determined. This indicates a severe problem.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWAD0601E

The version string '*%s*' is invalid. (0x38983259)

Explanation
This error occurs if an invalid version number is found.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWAD0602E

An error occurred attempting to determine the originally installed version of WebSEAL to verify that the configuration file is up-to-date. WebSEAL cannot start. (0x3898325a)

Explanation
This error occurs if the originally installed version of WebSEAL cannot be determined. This indicates a severe problem.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWAD0603E

An error occurred attempting to backup the configuration file. (0x3898325b)

Explanation
This error occurs when WebSEAL is trying to make a backup copy of the original configuration file before upgrade.

Administrator response
Examine the log file for additional errors. More information about the problem that occurred will be present.

DPWAD0604E

An error occurred attempting to restore the configuration file. (0x3898325c)

Explanation
This error occurs when WebSEAL is trying to restore a backed up copy of the configuration file.

Administrator response
Examine the log file for additional errors. More information about the problem that occurred will be present.

DPWAD0605W

The configuration file entry [*%s*]*%s* was not found. (0x3898325d)

Explanation
This error occurs when WebSEAL is trying to determine the version of the WebSEAL server that created the configuration file.

Administrator response
No action is necessary - the WebSEAL server will try another method to determine the original version of WebSEAL installed, and update the configuration file as necessary.

DPWAD0606E

An error occurred attempting to migrate the configuration file entry [*%s*]*%s*. (0x3898325e)

Explanation
This error occurs when WebSEAL is trying to perform migration of a configuration file entry.

Administrator response
You may need to manually update the entry to allow migration to proceed. Examine the configuration file and documentation for more information on the particular entry.

DPWAD0607E

An error occurred attempting to migrate the configuration file entry [*%s*]. (0x3898325f)

Explanation
This error occurs when WebSEAL is trying to perform migration of a configuration file stanza.

Administrator response
You may need to manually update the entry to allow migration to proceed. Examine the configuration file and documentation for more information on the particular entry.

DPWAD0611E

A serious error occurred performing configuration file migration. You may need to perform manual migration of some configuration options. (0x38983263)

Explanation
This message indicates that a serious problem occurred while attempting to update the configuration file.

Administrator response
Refer to other log messages to attempt to determine the problem. You may be able to perform manual migration of configuration file entries. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport. If you wish to attempt to manual migration, comment the problematic entries out of the WebSEAL configuration file and restart the WebSEAL server. Once the WebSEAL server has started successfully, manually modify the configuration file to restore the functionality you have disabled, refering to the WebSEAL Administration Guide where necessary.

DPWAD0752E

A replica set must be specified for the virtual host junction '*%s*'. (0x389832f0)

Explanation
When the SMS is used for session storage, all virtual host junctions must have a replica set specified with the -z junction option.

Administrator response
Create the junction using the -z <replica-set> option. The <replica-set> must be one of the replica sets listed in the WebSEAL configuration file.

DPWAD0753E

A replica set must be specified for the junction. (0x389832f1)

Explanation
When the SMS is used for session storage, all virtual host junctions must have a replica set specified with the -z junction option.

Administrator response
Create the junction using the -z <replica-set> option. The <replica-set> must be one of the replica sets listed in the WebSEAL configuration file.

DPWAD0754E

The Virtual Host junction '*%s*' must have an eCSSO domain key in the configuation file for it's virtual host name '*%s*'. (0x389832f2)

Explanation
When the Virtual Host junction was created or restored from the junction database it's virtual host name was discovered not to have a eCSSO domain key. These are configured using [e-community-domains] and [e-community-domain-keys:<domain>]

Administrator response
Add a eCSSO key for the domain the Virtual Host junction is in using the [e-community-domains] and [e-community-domain-keys:<domain>] stanzas and restart WebSEAL so it recognises the changes. Then retry creating the Virtual Host junction.

DPWAD0755E

The Virtual Host junction must have an eCSSO domain key in the configuration file for it's virtual host name. (0x389832f3)

Explanation
When the Virtual Host junction was created or restored from the junction database it's virtual host name was discovered not to have a eCSSO domain key. These are configured using [e-community-domains] and [e-community-domain-keys:<domain>]

Administrator response
Add a eCSSO key for the domain the Virtual Host junction is in using the [e-community-domains] and [e-community-domain-keys:<domain>] stanzas and restart WebSEAL so it recognises the changes. Then retry creating the Virtual Host junction.

DPWAD0756W

The junction reload command did not complete for regular junctions as a previous reload is still in effect. Try again later. (0x389832f4)

Explanation
A reload command issued earlier is still waiting for some requests using the older junction definitions to complete. New reload commands will not have an effect until these requests complete. Virtual Host junctions are independent and you should look for a separate message if they are busy too.

Administrator response
The command has had no effect on junctions, retry the command at a later time.

DPWAD0757W

The junction reload command did not complete for Virtual Host junctions as a previous reload is still in effect. Try again later. (0x389832f5)

Explanation
A reload command issued earlier is still waiting for some requests using the older Virtual Host junction definitions to complete. New reload commands will not have an effect until these requests complete. Regular junctions are independent and you should look for a separate message if they are busy too.

Administrator response
The command has had no effect on Virtual Host junctions, retry the command at a later time.

DPWAD0782E

Could not take junction offline (0x3898330e)

Explanation
This message is followed by an explanation of why the junction could not be taken offline.

Administrator response
Correct the problem described in the message displayed after this message.

DPWAD0783E

Could not take Virtual Host junction offline (0x3898330f)

Explanation
This message is followed by an explanation of why the Virtual Host junction could not be taken offline.

Administrator response
Correct the problem described in the message displayed after this message.

DPWAD0784E

Could not throttle junction (0x38983310)

Explanation
This message is followed by an explanation of why the junction could not be throttled.

Administrator response
Correct the problem described in the message displayed after this message.

DPWAD0785E

Could not throttle Virtual Host junction (0x38983311)

Explanation
This message is followed by an explanation of why the Virtual Host junction could not be throttled.

Administrator response
Correct the problem described in the message displayed after this message.

DPWAD0786E

Could not bring junction online (0x38983312)

Explanation
This message is followed by an explanation of why the junction could not be brought online.

Administrator response
Correct the problem described in the message displayed after this message.

DPWAD0787E

Could not bring Virtual Host junction online (0x38983313)

Explanation
This message is followed by an explanation of why the Virtual Host junction could not be brought online.

Administrator response
Correct the problem described in the message displayed after this message.

DPWAD0788E

You can only change the operation state of TCP, SSL, TCP Proxy, and SSL Proxy junctions. (0x38983314)

Explanation
Not all junction types support operational state changes.

Administrator response
Ensure you are applying the command to the correct junction.

DPWAD0789E

You can only change the operation state of TCP, SSL, TCP Proxy, and SSL Proxy Virtual Host junctions. (0x38983315)

Explanation
Not all Virtual Host junction types support operational state changes.

Administrator response
Ensure you are applying the command to the correct Virtual Host junction.

DPWAD0790E

Invalid server ID (0x38983316)

Explanation
The argument passed to -i was not a valid server UUID.

Administrator response
Obtain the correct UUID by using the 'show' command.

DPWAD0791E

Invalid server ID (0x38983317)

Explanation
The argument passed to -i was not a valid server UUID.

Administrator response
Obtain the correct UUID by using the 'virtualhost show' command.

DPWAD0792E

Server *%s* not found at junction *%s* (0x38983318)

Explanation
An attempt was made to change the operational state of a junction server based on a UUID which did not match any of the servers of the junction.

Administrator response
Use the 'show' command to find the correct UUID.

DPWAD0793E

Server *%s* not found at Virtual Host junction *%s* (0x38983319)

Explanation
An attempt was made to change the operational state of a Virtual Host junction server based on a UUID which did not match any of the servers of the Virtual Host junction.

Administrator response
Use the 'virtualhost show' command to find the correct UUID.

DPWAD1050E

The filename must not contain any path information. (0x3898341a)

Explanation
A base path for the database files has been statically configured and as such the supplied file name should not contain any path information.

Administrator response
Specify the name of the database without any path information.

DPWAD1053E

An error occurred while writing the WebSEAL flow data to disk. (0x3898341d)

Explanation
An error occurred while WebSEAL was committing the collected flow data to disk. One or more records may be missing for the last time period.

Administrator response
No action is required.

DPWAD1054E

The *%s* system routine failed: *%d*. (0x3898341e)

Explanation
An error occurred when WebSEAL attempted to execute a system routine.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWAD1055E

A system routine failed. (0x3898341f)

Explanation
An error occurred when WebSEAL attempted to execute a system routine.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWAD1056E

A process terminated unexpectedly: *%d*. (0x38983420)

Explanation
A process which was currently being monitored terminated unexpectedly. This process will be automatically restarted.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWAD1059E

The validation of the secret token for the request failed. (0x38983423)

Explanation
To help prevent cross-site request forgery attacks the requests for certain management pages need to contain a token which can be compared against data contained within the user session. The validation of this token failed because either the token was missing from the request, or the token did not match the value contained in the user session.

Administrator response
Ensure that the resource request contains the correct secret token for the user session.

DPWAD1060E

Unsolicited authentication requests are not permitted. (0x38983424)

Explanation
The server is configured to deny unsolicited authentication requests. The authentication information must first be requested by WebSEAL in response to an unauthenticated request for a protected resource.

Administrator response
First request a resource which requires authentication and then supply the authentication information to the server.

DPWAD1200E

The incoming connection from *%s* has been blocked. (0x389834b0)

Explanation
The incoming connection has been temporarily blocked by the Web Application Firewall functionality.

Administrator response
Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Verify Access for Web Troubleshooting Guide.

DPWAD1201E

An invalid csv field was provided: *%s* (0x389834b1)

Explanation
An invalid field was provided.

Administrator response
Examine the configuration and correct the offending field.

DPWAD1202E

An invalid configuration value was provided: *%s* (0x389834b2)

Explanation
An invalid configuration value was provided.

Administrator response
Examine the configuration and correct the offending value.

DPWAD1203E

An invalid number of fields were provided within the csv file: *%s* (0x389834b3)

Explanation
An invalid number of fields were discovered in a csv file.

Administrator response
Examine the configuration and correct the offending csv file.

DPWAD1204E

An unknown issue was discovered, *%d*, and as such no action was taken. (0x389834b4)

Explanation
An issue was discovered for which there was no configured action.

Administrator response
Examine the configuration and ensure that an action exists for the specified issue.

DPWAD1206E

An incompatible ISS protocol analysis module library was found. (0x389834b6)

Explanation
An incompatible ISS protocol analysis module was specified within the WebSEAL configuration.

Administrator response
Install a compatible ISS protocol analysis module distribution, or disable this functionality within WebSEAL.

DPWAD1207E

An internal error was encountered within the ISS protocol analysis module. (0x389834b7)

Explanation
An error was returned from the ISS protocol analysis module.

Administrator response
Check the log file for additional errors. If necessary, look up the error code from the message in the IBM Security Verify Access for Web Troubleshooting Guide for additional troubleshooting steps.

DPWAD1208E

An unrecoverable error was encountered within the ISS protocol analysis module : *%s*. (0x389834b8)

Explanation
An error was returned from the ISS protocol analysis module.

Administrator response
Check the log file for additional errors. If necessary, look up the error code from the message in the IBM Security Verify Access for Web Troubleshooting Guide for additional troubleshooting steps.

DPWAD1209E

An insufficient amount of memory was supplied to an internal WAF routine. (0x389834b9)

Explanation
An insufficient amount of memory was supplied to one of the internal WAF routines.

Administrator response
Check the log file for additional errors. If necessary, look up the error code from the message in the IBM Security Verify Access for Web Troubleshooting Guide for additional troubleshooting steps.

DPWAD1210E

The client connection has been blocked due to a security attack which was detected by the protocol analysis module. (0x389834ba)

Explanation
The protocol analysis module detected a potential attack in a prior request from the client and as such has blocked all connections from this client for a period of time.

Administrator response
Check the log file for additional errors. If necessary, look up the error code from the message in the IBM Security Verify Access for Web Troubleshooting Guide for additional troubleshooting steps.

DPWAD1211E

An error occurred while saving the WAF statistics data to the disk. (0x389834bb)

Explanation
An error occurred while WebSEAL was saving the collected WAF statistics to the disk. One or more records might be missing for the last time period.

Administrator response
No action is required.

DPWAD1212E

Initialization of Kerberos authentication failed. (0x389834bc)

Explanation
Initialization of Kerberos authentication failed.

Administrator response
Check for additional error messages in log files. Check your Kerberos related junction configuration entries to make sure they match the documentation.

DPWAD1213E

An error occurred when creating the Kerberos token: *%s* (0x389834bd)

Explanation
An error occurred when creating the Kerberos token.

Administrator response
This problem is most likely due to an internal error or misconfiguration. Check for additional error messages in log files. Check the Kerberos related junction configuration items in your server for errors.

DPWAD1214E

No Kerberos single sign-on tokens were available. (0x389834be)

Explanation
WebSEAL is correctly retrieving SSO tokens from the KDC, but these tokens have expired. The problem is most likely caused by the clocks on the WebSEAL server and the KDC being set to different times.

Administrator response
Check the time synchronization between the KDC and the WebSEAL server.

DPWAD1215E

An error occurred when creating the Kerberos token. (0x389834bf)

Explanation
An error occurred when creating the Kerberos token.

Administrator response
This problem is most likely due to an internal error or misconfiguration. Check for additional error messages in log files. Check the Kerberos related junction configuration items in your server for errors.

DPWAP0002E

Error accessing the database file: *%s* (*%s*:0x*%x*) (0x3898f002)

Explanation
An attempt to access a database file failed.

Administrator response
Check that the database file exists and that the file permissions allow access.

DPWAP0004E

The data which was passed into the program is not valid: *%s* (0x3898f004)

Explanation
The supplied data is not valid.

Administrator response
Check the provided data to ensure that it is being used in the correct context.

DPWAP0005E

The file, *%s*, contains data which is not valid. (0x3898f005)

Explanation
The specified file contains unexpected content.

Administrator response
Examine the file for the data which is not valid, or specify a different file.

DPWAP0006E

The file, *%s*, already exists. (0x3898f006)

Explanation
The supplied file name matches a file which already exists on the file system.

Administrator response
Either remove the specified file or select a different file name.

DPWAP0007E

The file, *%s*, does not exist. (0x3898f007)

Explanation
The supplied file name does not match a file which exists on the file system.

Administrator response
Check the supplied file name to ensure that it is correct.

DPWAP0008E

An internal error has occurred (*%s*:*%d*). (0x3898f008)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWAP0009E

The configuration entry, '*%s*', in the [*%s*] stanza does not exist. (0x3898f009)

Explanation
The requested configuration entry does not exist in the configuration file.

Administrator response
Check the supplied information to ensure that it is correct.

DPWAP0010E

Failed to establish a secure connection to the policy server (0x3898f00a)

Explanation
An attempt to establish a secure connection to the policy server failed.

Administrator response
Check the TAM policy server to ensure that it is running.

DPWAP0011E

The administration command, *%s*, failed (0x3898f00b)

Explanation
An attempt to execute an administration command failed.

Administrator response
Check the TAM servers to ensure that they are running.

DPWAP0012E

An unsupported configuration entry was supplied. (0x3898f00c)

Explanation
An attempt to supply an unsupported configuration entry was encountered.

Administrator response
Ensure that the correct configuration data is supplied.

DPWAP0013E

The [*%s*] stanza is an unsupported configuration stanza. (0x3898f00d)

Explanation
An attempt to supply an unsupported configuration entry was encountered.

Administrator response
Ensure that the correct configuration data is supplied.

DPWAP0014E

The '*%s*' configuration entry, in the [*%s*] stanza, is an unsupported configuration entry. (0x3898f00e)

Explanation
An attempt to supply an unsupported configuration entry was encountered.

Administrator response
Ensure that the correct configuration data is supplied.

DPWAP0015E

An value which is not valid, '*%s*', was supplied for the configuration entry, '*%s*', in the [*%s*] stanza. (0x3898f00f)

Explanation
An attempt was made to supply data which is not valid for a configuration entry.

Administrator response
Ensure that the correct configuration data is supplied.

DPWAP0016E

A prior configuration does not exist for this resource. (0x3898f010)

Explanation
An attempt to revert the configuration was made when there were no changes to revert.

Administrator response
Ensure that the correct resource has been specified.

DPWAP0017E

An instance name is required when referencing the ftype: *%s*. (0x3898f011)

Explanation
The supplied ftype is instance specific and an instance name was not specified.

Administrator response
Retry the command, specifying an instance name.

DPWAP0018E

An instance name should not be supplied when referencing the ftype: *%s*. (0x3898f012)

Explanation
The supplied ftype is not instance specific and an instance name was specified.

Administrator response
Retry the command, without specifying an instance name.

DPWAP0019E

The supplied instance name, *%s*, is not a configured instance. (0x3898f013)

Explanation
The supplied instance name does not match a configured instance on this appliance.

Administrator response
Retry the command, specifying the correct instance name.

DPWAP0020E

The supplied ftype, *%s*, was not recognized. (0x3898f014)

Explanation
The supplied ftype was not recognized and the command cannot be completed.

Administrator response
Retry the command, ensuring that the ftype given is correct.

DPWAP0021E

The [*%s*] stanza was not found in the configuration file. (0x3898f015)

Explanation
An attempt was made to delete a stanza which does not exist.

Administrator response
Ensure that the correct stanza name is supplied.

DPWAP0022E

Cannot allocate memory (0x3898f016)

Explanation
Memory allocation operation failed.

Administrator response
Check memory limits on your machine, and increase available memory if possible.

DPWAP0023E

The file, *%s*, contains data which is not valid at line *%d*. (0x3898f017)

Explanation
The specified file contains unexpected content.

Administrator response
Examine the file for the data which is not valid, or specify a different file.

DPWAP0024E

An error occurred in the *%s* system function: 0x*%x* (0x3898f018)

Explanation
An error occurred while attempting to execute a system function.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWAP0025E

An error occurred while executing the system call: *%s* (0x*%x*) (0x3898f019)

Explanation
An attempt to execute a system call failed.

Administrator response
Check the system log for further information.

DPWAP0026E

The file, *%s*, cannot be opened (0x*%x*) (0x3898f01a)

Explanation
An attempt to access a file failed.

Administrator response
Check that the file permissions allow access.

DPWAP0028E

The '%s' configuration entry, in the [%s] stanza, is a read only configuration entry and should not be modified. (0x3898f01c)

Explanation
An attempt was made to change a configuration entry which is not allowed to be modified.

Administrator response
Ensure that the configuration entry has not been modified.

DPWAP0029E

A read only configuration entry was supplied. (0x3898f01d)

Explanation
An attempt to supply a read only configuration entry was encountered.

Administrator response
Ensure that the correct configuration data is supplied.

DPWAP0031E

The process, *%s*, was terminated by the signal, *%d*. The process will be automatically restarted. (0x3898f01f)

Explanation
A process terminated unexpectedly. The process will be automatically restarted by the system.

Administrator response
Check the system log for further information.

DPWAP0032E

Failed to stop the *%s* process (pid: *%d*). (0x3898f020)

Explanation
An attempt to stop a running process failed.

Administrator response
Check the system log for further information. If the problem persists reboot the system.

DPWAP0033E

The *%s* operation for the ldap server, *%s*:*%d*, failed: (*%s*). (0x3898f021)

Explanation
An attempt to perform an operation on the LDAP server failed.

Administrator response
Ensure that the LDAP server information has been supplied correctly and that the LDAP server is currently contactable.

DPWAP0034E

Cannot obtain a unique DN for the user: *%s*. (0x3898f022)

Explanation
An attempt to locate the DN for a user has failed.

Administrator response
Ensure that the correct user information has been supplied, and that the LDAP server information has been supplied correctly.

DPWAP0035E

An error occurred while executing the command: *%s* (0x*%x*) *%s* (0x3898f023)

Explanation
An attempt to execute a system command failed.

Administrator response
Check the system log for further information.

DPWAP0036E

The directory, *%s*, does not exist. (0x3898f024)

Explanation
The supplied directory name does not match a directory which exists on the file system.

Administrator response
Check the supplied directory name to ensure that it is correct.

DPWAP0037E

A file or directory which is not valid was encountered: *%s* (0x3898f025)

Explanation
The specified file is not valid.

Administrator response
Check the provided data to ensure that it is being used in the correct context.

DPWAP0038E

The following files already exist: *%s* (0x3898f026)

Explanation
The specified files already exist on the system.

Administrator response
Check the system log for further information.

DPWAP0039E

An error occurred in the *%s* system function: *%s* (0x3898f027)

Explanation
An error occurred while attempting to execute a system function.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWAP0045E

Invalid configuration for the *%s* notifications module. Reverting to default values. (0x3898f02d)

Explanation
The configured advanced tuning parameters for the notifications module are invalid. The default values will be used until this is corrected.

Administrator response
No action is required

DPWAP0046E

An error occurred while executing an SQL statement at *%s*:*%d*. (*%d*:*%s*) (0x3898f02e)

Explanation
There was an error writing the FlowData information to disk. If the problem persists, see the IBM Electronic Support for additional information - https://www.ibm.com/mysupport

Administrator response
No action is required

DPWAP0047E

The requested configuration data was not found. (0x3898f02f)

Explanation
A request for specific configuration data failed as the configuration data does not exist.

Administrator response
Ensure that the correct data has been specified, and that the configuration file contains this data.

DPWAP0048E

An ICC toolkit failure occurred while calling *%s*. Error: *%s*. (0x3898f030)

Explanation
An internal ICC error occurred.

Administrator response
The action to correct this problem depends on details in the error message. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWAP0049E

An ICC toolkit failure occurred while calling *%s*. No further details are known. (0x3898f031)

Explanation
An internal ICC error occurred. However, no details about the error were able to be determined beyond the name of the ICC function which failed.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWAP0050E

The library, *%s*, cannot be opened: *%s* (0x3898f032)

Explanation
An attempt to load a library file failed.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWAP0051E

An error occurred while executing the system call: *%s* (0x*%x*) *%s* (0x3898f033)

Explanation
An attempt to execute a system call failed.

Administrator response
Check the system log for further information.

DPWAP0053E

Failed to write to the file, *%s* (0x*%x*) (0x3898f035)

Explanation
An attempt to write to a file failed.

Administrator response
Check that the file permissions allow access and that the disk is not full.

DPWAP0054E

The database is not yet available. (0x3898f036)

Explanation
The database is in the process of being updated and is not yet available for use.

Administrator response
Wait a period of time and then retry the operation.

DPWAP0058E

The command, '*%s*', did not complete within the allotted time. (0x3898f03a)

Explanation
A command which was executed did not complete in the allotted time.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWAP0059E

The supplied authorization server name, *%s*, is not a known server. (0x3898f03b)

Explanation
The supplied authorization server name does not match a configured authorization server.

Administrator response
Retry the command, specifying a valid server name.

DPWAP0060E

The specified authorization server, *%s*, could not be deleted. (0x3898f03c)

Explanation
An attempt to delete an authorization server has failed.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWAP0061E

The server certificate could not be retrieved from *%s* at port *%s*. (0x3898f03d)

Explanation
An attempt to load the server certificate from a server has failed.

Administrator response
Ensure that the specified server is running and can be reached by the appliance.

DPWAP0064E

Incorrect usage for the mesa_config *%s* command. (0x3898f040)

Explanation
The command line options which were supplied to the mesa_config program were not valid.

Administrator response
Retry the command, supplying the correct command line options.

DPWAP0065E

A path which is not valid has been specified. (0x3898f041)

Explanation
The command is only authorized to perform an action on specific file paths. The supplied path does not match one of these supported paths.

Administrator response
Retry the command, supplying a supported path.

DPWAP0066E

Failed to copy the file (error code: *%d*). (0x3898f042)

Explanation
An attempt to copy a file failed.

Administrator response
Check the supplied file names for accuracy and then retry the command.

DPWAP0067E

Authorization for the requested command has been denied. (0x3898f043)

Explanation
A command request has been denied.

Administrator response
Examine the requested command and ensure that the necessary rules have been met.

DPWAP0068E

The IBM Security Verify Access runtime environment is not configured. (0x3898f044)

Explanation
The IBM Security Verify Access runtime is not currently configured. It must be configured to execute the requested operation.

Administrator response
Configure the IBM Security Verify Access runtime environment and then retry the operation.

DPWAP0069E

A web reverse proxy instance with the name *%s* has already been configured. (0x3898f045)

Explanation
An attempt to configure a new web reverse proxy instance has failed because the supplied instance name matches the name of a pre-existing instance.

Administrator response
Either unconfigure the existing existance or select a new instance name.

DPWAP0070E

The runtime environment has already been configured. (0x3898f046)

Explanation
An attempt to configure the runtime environment has been made while the environment is still configured.

Administrator response
Unconfigure the runtime environment before attempting to reconfigured it.

DPWAP0071E

The supplied file name, *%s*, must have a file extension of '*%s*'. (0x3898f047)

Explanation
A file name was supplied with an unexpected extenions.

Administrator response
Specify a file name with the correct extension.

DPWAP0072E

The key database, *%s*, does not exist. (0x3898f048)

Explanation
The supplied database does not match one which exists on the file system.

Administrator response
Check the supplied database name to ensure that it is correct.

DPWAP0073E

An IP address which is not valid was located in the supplied entry: *%s* (0x3898f049)

Explanation
The supplied IP address does not match one of the IP addresses of the protected interfaces.

Administrator response
Check the supplied IP address to ensure that it is correct.

DPWAP0074E

A matching interface was not found. (0x3898f04a)

Explanation
The supplied IP address does not match one of the IP addresses of the protected interfaces.

Administrator response
Check the supplied IP address to ensure that it is correct.

DPWAP0075E

The *%s* parameter is required. (0x3898f04b)

Explanation
A required parameter was missing from the supplied information.

Administrator response
Check the supplied information and ensure that the missing data is supplied.

DPWAP0076E

The supplied starting value of *%ld* is larger than the number of lines contained in the file (*%ld*) (0x3898f04c)

Explanation
The starting line number is greater than the current number of lines in the file.

Administrator response
Check the supplied information and ensure that a start value which is less than the number of lines in the file is supplied.

DPWAP0077E

An incorrect range was specified. The starting value (*%ld*) must be less than the ending value (*%ld*) (0x3898f04d)

Explanation
The start value is greater than the end value.

Administrator response
Check the supplied information and ensure that a start value which is less than the end value is supplied.

DPWAP0078E

The pending changes cannot be committed as conflicts have been discovered between the staged and production files. (0x3898f04e)

Explanation
Conflicts have been discovered between the pending changes and production files. This will only occur if the production file has been modified by a source outside of the appliance.

Administrator response
Manually apply the changes again.

DPWAP0079E

The IP address, *%s*, is already in use. (0x3898f04f)

Explanation
The supplied IP address is already in use by the system.

Administrator response
Choose an IP address which is not already in use by the system.

DPWAP0080E

The *%s* interface is not a configured interface. (0x3898f050)

Explanation
The supplied interface name does not match one of the configured interfaces.

Administrator response
Check the supplied interface name to ensure that it is correct.

DPWAP0081E

One or more instances of the Web reverse proxy is still configured. These instances must be unconfigured first. (0x3898f051)

Explanation
An attempt to unconfigure the runtime environment has been made while Web reverse proxy instances remain configured.

Administrator response
Unconfigure the Web reverse proxy instances and then retry the operation.

DPWAP0087E

An incorrect user name or password has been supplied. (0x3898f057)

Explanation
An authentication attempt has failed. Either an incorrect user name or password was supplied.

Administrator response
Ensure that the correct user name and password have been used.

DPWAP0088E

Examine the log of the Web Reverse Proxy instance for further information on the failure. (0x3898f058)

Explanation
A request to start or stop the Web Reverse Proxy has failed. The log for the instance should contain more information on this failure.

Administrator response
Examine the log of the Web Reverse Proxy instance for further information on the failure.

DPWAP0090E

The key database, *%s*, already exists. (0x3898f05a)

Explanation
The supplied database name already matches one which exists on the file system.

Administrator response
Check the supplied database name to ensure that it is correct.

DPWAP0091E

The requested operation cannot proceed as there are pending changes which first need to be committed. (0x3898f05b)

Explanation
The requested operation cannot be performed while there are pending changes. These changes need to be deployed, or rolled back, before the operation can be processed.

Administrator response
Either deploy or rollback the changes and then attempt the operation again.

DPWAP0092E

The configuration file for the *%s* instance is missing from the migration zip file. (0x3898f05c)

Explanation
The migration functionality only supports the migration to an instance of the same name. The supplied migration zip file does not contain the configuration file for the specified instance.

Administrator response
Check the migration zip file to ensure that the configuration file for the specified instance is present.

DPWAP0093E

An invalid filter rule was specified (*%s*) (0x3898f05d)

Explanation
An attempt to capture packet data failed as an invalid filter rule was provided.

Administrator response
Check the filter rule and ensure that it is a valid rule.

DPWAP0094E

The specified maximum file size exceeds the available space of *%ld* MB. (0x3898f05e)

Explanation
The specified maximum file size will exceed the amount of available disk space.

Administrator response
Ensure that the maximum file size is less than the remaining available disk space.

DPWAP0095E

The system is already capturing network packets. The current capture operation must be stopped before the requested operation can be completed. (0x3898f05f)

Explanation
The system can only perform a single capture operation at a time.

Administrator response
Stop the current capture operation and then attempt the request again.

DPWAP0096E

A packet capture file already exists on the system. The current file must be deleted before a new capture operation can be started. (0x3898f060)

Explanation
A capture file already exists and it must be deleted before a new capture operation can be started.

Administrator response
Delete the current capture file and then retry the operation.

DPWAP0097E

The maximum capture file size has been reached. (0x3898f061)

Explanation
The maximum file size for the capture file has been reached. This file size was specified when the capture operation was started.

Administrator response
Ensure that the specified maximum file size is adequate for the packets which are being captured.

DPWAP0098W

The log file, *%s*, has been automatically purged from the system. (0x3898f062)

Explanation
The disk utilisation has reached the maximum threshold and as such the system has deleted the specified log file.

Administrator response
Check the system to ensure that all unnecessary files are deleted.

DPWAP0099E

A management interface has already been configured with the same IP address: *%s*. (0x3898f063)

Explanation
An attempt was made to configure an application interface with the same address as a management interface. This configuration is not supported.

Administrator response
Either change the corresponding management interface address, or change the configured application interface address.

DPWAP0100E

An invalid activation code has been supplied. (0x3898f064)

Explanation
The supplied activation code is not valid.

Administrator response
Check the provided activation code to ensure that it has been entered correctly.

DPWAP0102E

The server failed to start correctly. (0x3898f066)

Explanation
The attempt to start the server failed.

Administrator response
Check the system log for further information.

DPWAP0104E

The server could not be stopped. (0x3898f068)

Explanation
The attempt to stop the server failed.

Administrator response
Check the system log for further information.

DPWAP0105E

The command is not supported with the current configuration. (0x3898f069)

Explanation
An invalid command was attempted.

Administrator response
Check the configuration of the system to see if the specified command should be supported.

DPWAP0108E

The supplied database name, *%s*, does not match any known databases. (0x3898f06c)

Explanation
The supplied database name does not match a configured database on this appliance.

Administrator response
Retry the command, specifying the correct database name.

DPWAP0109E

The user identity for the local database cannot be modified after the database has been created. (0x3898f06d)

Explanation
The new configuration data could not be applied because the user identity for a local database has been modified.

Administrator response
Ensure that the user identity which is associated with the local databases have not been changed.

DPWAP0110E

The database, *%s*, is not currently enabled. (0x3898f06e)

Explanation
The specified database is not currently enabled.

Administrator response
Enable the database or select a different database and then retry the command.

DPWAP0111E

Failed to obtain the state of the specified database: *%s*. (0x3898f06f)

Explanation
The program could not obtain the state of the specified database.

Administrator response
Check the system log for further information.

DPWAP0112E

The server has already been started. (0x3898f070)

Explanation
An attempt was made to start a server when it was already running.

Administrator response
Ensure that the server is not running before attempting the operation again.

DPWAP0113E

The cluster signature file could not be created. (0x3898f071)

Explanation
An attempt to create the cluster signature file failed.

Administrator response
Check the system log for further information.

DPWAP0114E

The cluster signature file could not be validated. (0x3898f072)

Explanation
An attempt to validate the cluster signature file failed.

Administrator response
Ensure that a valid signature file is used.

DPWAP0115E

The cluster master cannot currently be reached, and must be reachable in order to complete the operation. (0x3898f073)

Explanation
The operation failed because the cluster master cannot currently be reached.

Administrator response
Ensure that the cluster master is running and can be reached.

DPWAP0116W

The specified node cannot currently be reached. (0x3898f074)

Explanation
The operation could not be fully completed because the cluster node cannot currently be reached.

Administrator response
Ensure that the node is running and can be reached.

DPWAP0117E

The database server failed to start within the allocated time. (0x3898f075)

Explanation
The database server did not start within the allocated time.

Administrator response
Check the system log for further information.

DPWAP0118W

The specified node, *%s*, is not a member of the cluster. (0x3898f076)

Explanation
The operation could not be fully completed because the specified node is not a member of the cluster.

Administrator response
Ensure that the specified node is a recognised member of the cluster.

DPWAP0119E

A cluster master cannot be deregistered from the cluster. (0x3898f077)

Explanation
A cluster master cannot be deleted from the cluster.

Administrator response
Change the cluster policy so that the local appliance is not a master and then delete the appliance from the cluster.

DPWAP0120E

A cluster must be defined before this request can be processed. To define a cluster the primary master must be set to something other than 127.0.0.1. (0x3898f078)

Explanation
A cluster must be defined before the request can be processed.

Administrator response
Configure a primary master and then retry the operation.

DPWAP0121E

The port which has been specified for the cluster cannot be used because another service is already using one of the range of required ports. (0x3898f079)

Explanation
The cluster utilises a range of network ports, starting at a port which is specified as a part of the cluster configuration. One or more ports within this range is currently being used by a different service of the appliance.

Administrator response
Select another range of ports which can be used by the cluster.

DPWAP0122E

The signature file could not be created. (0x3898f07a)

Explanation
An attempt to create the signature file failed.

Administrator response
Check the system log for further information.

DPWAP0123E

The signature file could not be validated. (0x3898f07b)

Explanation
An attempt to validate the signature file failed.

Administrator response
Ensure that a valid signature file is used.

DPWAP0124E

The supplied signature file is not compatible with the local server. (0x3898f07c)

Explanation
An attempt to apply the configuration data from the supplied signature file failed.

Administrator response
Ensure that the signature file was generated from a server which has a compatible configuration with the local server.

DPWAP0125E

One or more Authorization server instances are still configured. These instances must be unconfigured first. (0x3898f07d)

Explanation
An attempt to unconfigure the runtime environment has been made while Authorization server instances remain configured.

Administrator response
Unconfigure the Authorization server instances and then retry the operation.

DPWAP0126W

Failed to attach the ACL which is used to allow unauthenticated access to the favicon.ico resource. (0x3898f07e)

Explanation
An attempt to attach an ACL to an object on the new Web Reverse Proxy instance failed. This usually occurs when the policy server cannot connect to the Web Reverse Proxy instance.

Administrator response
Check the environment to ensure that the policy server can communicate with the new Web Reverse Proxy instance.

DPWAP0127E

The operation is not permitted on this key database. (0x3898f07f)

Explanation
The attempted operation on the key database is not permitted.

Administrator response
No action is required. The requested operation is not allowed.

DPWAP0128E

The file, *%s*, cannot be removed as it is still in use. (0x3898f080)

Explanation
An attempt to delete a file failed as it is currently in use by another process.

Administrator response
Determine what is using the file and take the appropriate action before attempting to delete the file again.

DPWAP0129E

The stash file contains an invalid password. (0x3898f081)

Explanation
The contents of the stash file was not valid.

Administrator response
Check the stash file.

DPWAP0130E

The username for the logged in UID could not be determined (0x3898f082)

Explanation
The name of the user running the current process could not be determined.

Administrator response
Ensure that process is being run by a valid user.

DPWAP0131E

The UID of the calling process could not be found (0x3898f083)

Explanation
The UID of the user running the current process could not be determined.

Administrator response
Ensure that process is being run by a valid user.

DPWAP0132E

Failed to write to the configuration file. (0x3898f084)

Explanation
An attempt to write to a file failed.

Administrator response
Check that the file permissions allow access and that the disk is not full.

DPWAP0133E

Failed to load the configuration file. (0x3898f085)

Explanation
An attempt to load a file failed.

Administrator response
Check that the file permissions allow access.

DPWBA0300W

A general error occurred: *%s*. (0x36a6812c)

Explanation
An error occurred when attempting to process the authorization decision request. The WebSEAL logs might contain more information.

Administrator response
Check the WebSEAL logs for more details.

DPWBA0303E

A required configuration entry, *%s*, under the *%s* stanza is missing from the configuration file. (0x36a6812f)

Explanation
See message.

Administrator response
Add the specified missing entry to the configuration file.

DPWBA0304E

Unable to determine whether the IBM Security Verify Access policy needs to be applied: 0x*%x*. (0x36a68130)

Explanation
An error occurred when parsing the IBM Security Verify Access policy value as Boolean. The WebSEAL trace logs might contain more details.

Administrator response
Ensure that the configuration value for setting the IBM Security Verify Access policy is set to either true or false.

DPWBA0305E

Initialization of cluster manager failed: 0x*%x*. (0x36a68131)

Explanation
This error might be due to a missing configuration entry for the runtime security services cluster definition.

Administrator response
Check if all configuration entries are present, and have correct values.

DPWBA0306E

Failed to add cluster to cluster manager: 0x%x. (0x36a68132)

Explanation
This error might be due to a missing configuration entry for the runtime security services cluster definition.

Administrator response
Verify that all configuration entries are present and have correct values.

DPWBA0307W

The stanza %s in file %s is not found. (0x36a68133)

Explanation
An error occurred when looking up the specified stanza in the file.

Administrator response
Ensure that the specified stanza is present.

DPWBA0308W

The header key name is missing for the app_context_data key: %s (0x36a68134)

Explanation
A header key name (the custom ones specified on the LHS by users) is missing in the configuration file, but is present in an IBM Security Verify Access structure.

Administrator response
Check the WebSEAL logs for more details.

DPWBA0309W

The authentication level is missing for the obligation: %s. (0x36a68135)

Explanation
An entry is missing in the [obligations-levels-mapping] stanza in WebSEAL.

Administrator response
Add the missing entry that maps the obligation to its authentication level and restart WebSEAL.

DPWBA0310W

An error occurred when trying to retrieve the obligation ID from the runtime security services response. (0x36a68136)

Explanation

The obligation ID sent by runtime security services could not be parsed successfully. This error is due to an issue either with the runtime security services server or the runtime security services external authorization service (EAS).

Administrator response

If the problem persists, contact IBM support.

DPWBA0311W

Unable to contact runtime security services. (0x36a68137)

Explanation

EAS is unable to contact any of the runtime security services servers for an access decision because the service is down.

Administrator response

Verify that the runtime security services server is up and running. Check the WebSEAL logs for more details. Also, you can update the WebSEAL configuration file with the following [rtss-eas] stanza entry to permit access decisions even when the servers are down: permit-when-no-rtss-available = true

DPWBA0312W

The *%s* attribute could not be extracted from a credential: API error: *%s* (API error code [*%x*:*%x*]). (0x36a68138)

Explanation

The specified attribute could not be extracted from a credential. This error might be due to resource exhaustion, and as such be transient.

Administrator response

If the problem persists, check IBM Electronic Support for additional information at https://www.ibm.com/mysupport.

DPWBA0313E

An error occurred when attempting to communicate with the SOAP server URL *%s*: *%s* (error code: *%d*/0x*%x*). (0x36a68139)

Explanation

An attempt to communicate with the SOAP server failed within the underlying communications layer.

Administrator response

Check additional messages to determine the cause of the error and correct the problem. Ensure that the SOAP server is running and reachable. If the problem persists, check IBM Electronic Support for additional information at https://www.ibm.com/mysupport.

DPWBA0314E

The URL is invalid. (0x36a6813a)

Explanation
A client request contained a URL that does not conform to HTTP specifications.

Administrator response
Verify the request from the client and ensure that it conforms to HTTP specifications.

DPWBA0315E

Cannot allocate memory (0x36a6813b)

Explanation
Memory allocation operation failed.

Administrator response
Check memory limits on your machine, and increase available memory if possible.

DPWBA0316W

Config entry for context-id is set to context-inherited-pop but special-eas entry is not set. (0x36a6813c)

Explanation
When attempting to find the policy ID for the pretected resource being accessed, it was found that the user configured the context-id to be context-inherited-pop but this setting also requires the special-eas setting in the aznapi-configuration stanza to be set. This is a configuration error.

Administrator response
Set the special-eas entry in the WebSEAL configuration file to the aznapi-external-authzn-services entry for the RBA EAS (eg. special-eas = trigger_rba_eas).

DPWBA0317W

The credential used is missing the tagvalue_user_session_id attribute. (0x36a6813d)

Explanation
The protected object attribute CBACacheResult has been set to a non-zero value which enables caching within the RTSS EAS module. The caching functionality requires the tagvalue_user_session_id attribute to be present in the user credential.

Administrator response
Set the [session] user-session-ids=yes entry in the WebSEAL configuration file.

DPWCA0150E

Invalid UNIX user name (*%s*) (0x389d0096)

Explanation
See message.

Administrator response
Use a valid user name

DPWCA0151E

Invalid UNIX group name (*%s*) (0x389d0097)

Explanation
See message

Administrator response
Put user in a valid group.

DPWCA0152E

Could not change process GID (*%s*) (0x389d0098)

Explanation
See message.

Administrator response
Contact support.

DPWCA0153E

Could not change process UID (*%s*) (0x389d0099)

Explanation
See message.

Administrator response
Contact support.

DPWCA0154E

Could not become background process (*%d*) (0x389d009a)

Explanation
See message.

Administrator response
Contact support.

DPWCA0155W

Could not start background process (0x389d009b)

Explanation
See message.

Administrator response
Contact support.

DPWCA0156E

Could not use RPC protocol sequence (*%s*,*%s*,0x*%8.8lx*) (0x389d009c)

Explanation
See message.

Administrator response
Contact support.

DPWCA0157E

Could not fetch RPC bindings (0x*%8.8lx*) (0x389d009d)

Explanation
See message.

Administrator response
Contact support.

DPWCA0158E

Could not release RPC bindings (0x*%8.8lx*) (0x389d009e)

Explanation
See message.

Administrator response
Contact Support.

DPWCA0159E

Caught signal (*%d*) (0x389d009f)

Explanation
See message.

Administrator response
Contact Support.

DPWCA0160E

Could not create new thread (*%d*) (0x389d00a0)

Explanation
See message.

Administrator response
Contact support.

DPWCA0161E

Could not cancel thread (*%d*) (0x389d00a1)

Explanation
See message.

Administrator response
Contact support.

DPWCA0162E

Could not join thread (*%d*) (0x389d00a2)

Explanation
See message.

Administrator response
Contact Support.

DPWCA0163E

Could not set RPC authorization function (0x*%8.8lx*) (0x389d00a3)

Explanation
See message.

Administrator response
Contact support.

DPWCA0164E

Could not setup authentication info (0x*%8.8lx*) (0x389d00a4)

Explanation
Unable to perform login.

Administrator response
Check login parameters.

DPWCA0165E

Could not set server login context (0x*%8.8lx*) (0x389d00a5)

Explanation
Unable to set the network credentials to those specified by login context.

Administrator response
Check that network credentials are correct.

DPWCA0166E

Could not perform network login (*%s*,*%s*,0x*%8.8lx*) (0x389d00a6)

Explanation
See message.

Administrator response
Verify that user/password is correct.

DPWCA0167E

Could not fetch key from keytab file (*%s*,*%s*,0x*%8.8lx*) (0x389d00a7)

Explanation
See message.

Administrator response
Check that the keyfile is set up correctly, and the user information is valid.

DPWCA0168E

Could not refresh login context (0x*%8.8lx*) (0x389d00a8)

Explanation
WebSEAL was unable to refresh the login based on existing login information.

Administrator response
Check validity of login information

DPWCA0169E

Could not determine login context expiration (0x*%8.8lx*) (0x389d00a9)

Explanation
See message.

Administrator response
Check validity of login information.

DPWCA0170E

Could not set RPC interface (0x*%8.8lx*) (0x389d00aa)

Explanation
See message.

Administrator response
Check interfaces.

DPWCA0171E

Could not register RPC endpoints (*%s*,0x*%8.8lx*) (0x389d00ab)

Explanation
See message.

Administrator response
Check endpoints.

DPWCA0172E

Could not unregister RPC interface (0x*%8.8lx*) (0x389d00ac)

Explanation
See message.

Administrator response
Check validity and status of interfaces.

DPWCA0173E

Could not export bindings to name service (*%s*,*%s*,0x*%8.8lx*) (0x389d00ad)

Explanation
See message.

Administrator response
Check status of name service.

DPWCA0174E

Could not unregister RPC endpoints (0x*%8.8lx*) (0x389d00ae)

Explanation
See message.

Administrator response
Check validity and status of endpoints.

DPWCA0175E

Could not unexport bindings from name service (*%s*,0x*%8.8lx*) (0x389d00af)

Explanation
See message.

Administrator response
Check validity of interfaces and name service.

DPWCA0176E

Malloc failure (0x*%8.8lx*) (0x389d00b0)

Explanation
See message.

Administrator response
Check status of memory on the system.

DPWCA0177E

This CDAS does not support this authentication style: (*%d*) (0x389d00b1)

Explanation
See message.

Administrator response
Check validity of authentication style

DPWCA0178E

General CDAS (Cross Domain Authentication Service) failure (*%s*, 0x*%8.8lx*) (0x389d00b2)

Explanation
See message.

Administrator response
See message.

DPWCA0179E

Pthread error occurred: *%d* (0x389d00b3)

Explanation
See message.

Administrator response
Check system resources.

DPWCA0180E

An invalid rule was supplied: *%s* (0x389d00b4)

Explanation
An invalid rule was retrieved from the rules file.

Administrator response
Correct the rule within the specified rules file.

DPWCA0181E

No rules were found in the rules file (0x389d00b5)

Explanation
No valid rules were found in the rules file.

Administrator response
Add a valid rule to the rules file, or specify a different rules file.

DPWCA0182W

The cache entries have exceeded the maximum cache size. (0x389d00b6)

Explanation
The cache has reached its configured limit.

Administrator response
Increase the permitted size of the cache.

DPWCA0300E

API internal error: (*%s*, *%d*) (0x389d012c)

Explanation
See message.

Administrator response
See message.

DPWCA0301W

A timeout occurred while waiting for authentication information from *%s*. (0x389d012d)

Explanation
A requested authentication operation required further authentication information. This information was not received in a timely fashion.

Administrator response
No action is required.

DPWCA0458E

malloc() failure (0x389d01ca)

Explanation
The application was unable to allocate the required memory.

Administrator response
Ensure that there is enough system memory.

DPWCA0751E

There is no user authentication information available. (0x389d02ef)

Explanation
The user did not provide their information for authentication

Administrator response
Check user information for authentication

DPWCA0753E

Unable to encode certificate data (0x389d02f1)

Explanation
See message.

Administrator response
Verify that xauthn_cert is valid

DPWCA0754E

Failure reading string key or value of replacementString from WebSEAL configuration file. (0x389d02f2)

Explanation
See message.

Administrator response
Ensure the value exists for the replacementString in the WebSEAL configuration file.

DPWCA0755E

Unable to perform DN mapping. (0x389d02f3)

Explanation
An internal error has occurred. A function was called with invalid parameters.

Administrator response
Contact support.

DPWCA0756E

Error building replacement string. (0x389d02f4)

Explanation
An error occurred while preparing an LDAP search filter.

Administrator response
Check for other errors in the configuration file which may provide more information. If no other errors are found, call support.

DPWCA0757E

Failure extracting key-value pairs from CERT-DN. (0x389d02f5)

Explanation
An error occurred while parsing the DN from a certificate.

Administrator response
Check that the certificate DN is valid.

DPWCA0759E

Invalid parameter passed to get_name_value (0x389d02f7)

Explanation
An internal error has occurred.

Administrator response
Call support.

DPWCA0760E

Invalid replacement string entry found (0x389d02f8)

Explanation
The entries in the replacement string stanza must contain '=' characters.

Administrator response
Check that all entries in the replacement string stanza contain an equals sign.

DPWCA0761E

Out of memory in get_name_value function (0x389d02f9)

Explanation
Memory allocation failed.

Administrator response
Check per process memory allocation limits.

DPWCA0762E

Calloc function could not allocate memory (0x389d02fa)

Explanation
Memory allocation failed.

Administrator response
Check per process memory allocation limits.

DPWCA0763E

The last character in the DN was the = following the name (0x389d02fb)

Explanation
The format of the certificate DN was not valid.

Administrator response
Make sure the certificate DN is valid.

DPWCA0764E

Unexpected end of string encountered parsing certificate DN (0x389d02fc)

Explanation
See message.

Administrator response
Check the format of the last string in certifcate DN

DPWCA0765E

The search string is NULL (0x389d02fd)

Explanation
An internal error has occurred.

Administrator response
Call support.

DPWCA0766E

The return dn is NULL (0x389d02fe)

Explanation
An internal error has occurred.

Administrator response
Call support.

DPWCA0768E

Error loading XKMS CDAS configuration file. (0x389d0300)

Explanation
There was an error in the XKMS CDAS configuration file.

Administrator response
Look for other log messages indicating which entries were not found.

DPWCA0769E

Error searching suffix '*%s*', return status = 0x*%x* (0x389d0301)

Explanation
An LDAP search failed.

Administrator response
Verify the LDAP server is running and that the suffix exists.

DPWCA0770E

Bad Parameters passed to build_search_filter function. (0x389d0302)

Explanation
An internal error has occurred.

Administrator response
Call support

DPWCA0771E

Error retrieving value from certificate DN. (0x389d0303)

Explanation
Make sure that the DN contains all of the strings specified in the replacement strings list.

Administrator response
An error occurred while trying to replace a value from the certificate DN.

DPWCA0774E

Unable to attach thread to existing JVM. (0x389d0306)

Explanation
An error occurred when trying to attach a thread to a JVM.

Administrator response
Make sure the JVM being used is a supported JVM.

DPWCA0775E

Unable to create JVM or attach to an existing JVM. (0x389d0307)

Explanation
An error occurred when trying to discover whether or not a JVM already existed in the current process.

Administrator response
Make sure the JVM being used is a supported JVM.

DPWCA0778E

Unable to attach thread in shutdown. Aborting cleanup. (0x389d030a)

Explanation
An error occurred while trying to attach to the JVM to perform clean up activities.

Administrator response
None necessary.

DPWCA0779E

Cannot load class: *%s* (0x389d030b)

Explanation
An error occurred while trying to load a java class.

Administrator response
Make sure the classpath in webseald.conf is correct and that the class can be found in a jar file in the classpath.

DPWCA0780E

Cannot create new object: *%s* (0x389d030c)

Explanation
An error occurred while creating a new object.

Administrator response
Make sure the classpath in webseald.conf is correct and that the class can be found in a jar file in the classpath.

DPWCA0781E

Cannot load class method: *%s*.init (0x389d030d)

Explanation
An error occurred while trying to load the init method for the class.

Administrator response
Make sure that the class is valid and implements the 'init' method.

DPWCA0782E

Exception occurred in *%s*.init(*%s*) (0x389d030e)

Explanation
An exception occurred while invoking the init method of a class.

Administrator response
Check the log file for other details about the exception and make sure the properties file contains no errors.

DPWCA0783E

Cannot load class method: *%s*.validate (0x389d030f)

Explanation
An error occurred while trying to load the validate method for the class.

Administrator response
Make sure that the class is valid and implements the 'validate' method.

DPWCA0785E

Exception occurred in validate, certificate DN = *%s* (0x389d0311)

Explanation
An exception occurred while invoking the validate method of a class with the specified certificate DN.

Administrator response
Check the log file for other details about the exception.

DPWCA0787E

DN of first entry is NULL. (0x389d0313)

Explanation
An LDAP search returned an entry without a DN.

Administrator response
Call support.

DPWCA0788E

Parsing the names and values for replacement string failed. (0x389d0314)

Explanation
An error occurred retrieving values needed to certificate DN mapping.

Administrator response
Check the log file for additional errors. Verify the replacement strings in webseald.conf are correct.

DPWCA0900E

Unable to open ITIM CDAS configuration file. (0x389d0384)

Explanation
An error occurred while opening the ITIM CDAS configuration file.

Administrator response
Check the file path in the WebSEAL configuration file and verify that the ITIM CDAS configuration file exists.

DPWCA0901E

Incorrect number of arguments used for ITIM CDAS initialization. (0x389d0385)

Explanation
Bad number of arguments used in ITIM CDAS configuration.

Administrator response
Verify that the correct number of arguments are specified in the WebSEAL configuration file for initializaion of the ITIM CDAS.

DPWCA0902E

No ITIM CDAS configuration file or action in the WebSEAL configuration file. (0x389d0386)

Explanation
Bad parameter for ITIM CDAS configuration file name or action type.

Administrator response
Verify that the ITIM CDAS configuration file name path are correct in the WebSEAL configuration file and that the CDAS action type is either 'check' or 'sync'.

DPWCA0904E

Could not create the sending message to ITIM. (0x389d0388)

Explanation
See message.

Administrator response
Contact support.

DPWCA0905W

Function call, *func*, failed error: *error code error text*. (0x389d0389)

Explanation
The specified GSKit function failed while setting up for SSL connections to junctions or from browsers. Or perhaps the initial handshake failed due to invalid certificates or the browser simply closed the connection abruptly.

Administrator response
Examine the error text for details. Typical problems might be that the PKCS#11 library is incorrectly specified, or the PKCS#11 token or token password is incorrect, or the PKCS#11 token is not set up.

DPWCA0906E

Could not create socket (*%d*) (0x389d038a)

Explanation
This message is overloaded in its meaning. It can mean there was a failure in creating a socket for connecting, setting socket options on it, or creating sockets for HTTP and HTTPS connections.

Administrator response
Check WebSEAL has not exceeded system resource limits. Examine the errno in the system error header file for details.

DPWCA0907E

Could not connect socket (*%d*) (0x389d038b)

Explanation
This message means that there was a failture to connect to a specific socket.

Administrator response
Examine the errno in the system error header file for details.

DPWCA0908E

Could not get the ITIM server host address (0x389d038c)

Explanation
See the message.

Administrator response
Check whether ITIM server is already running. If ITIM is running, check the ITIM CDAS configuration file to verify the ITIM server URL is specified correctly.

DPWCA0909E

Windows library call failed. Could not call the function WSAStartup. (0x389d038d)

Explanation
The WSAStartup function must be the first Windows Sockets function called by an application or DLL. It allows an application or DLL to specify the version of Windows Sockets required and to retrieve details of the specific Windows Sockets implementation. The application or DLL can only issue further Windows Sockets functions after a successfully calling WSAStartup.

Administrator response
Check WS2_32.DLL in the system environment.

DPWCA0910E

Unable to allocate memory (0x389d038e)

Explanation
Memory allocation failed.

Administrator response
Check per process memory allocation limits.

DPWCA0911E

Could not find host name or IP address of ITIM server in the ITIM CDAS configuration file. (0x389d038f)

Explanation
See the message.

Administrator response
Check the ITIM Password URL part in the ITIM CDAS configuration file.

DPWCA0912E

Could not find KeyDataBase in the ITIM CDAS configuration file. (0x389d0390)

Explanation
See the message.

Administrator response
Verify that the KeyDataBase entry exists in the ITIM CDAS configuration file.

DPWCA0913E

Could not find KeyDataBase Password in the ITIM CDAS configuration file. (0x389d0391)

Explanation
See the message.

Administrator response
Verify that the KeyDataBase Password entry exists in the ITIM CDAS configuration file.

DPWCA0914E

Could not find Source DN in the ITIM CDAS configuration file. (0x389d0392)

Explanation
See the message.

Administrator response
Verify that the Source DN entry exists in the ITIM CDAS configuration file.

DPWCA0915E

Could not find ITIM Principal Name in the ITIM CDAS configuration file. (0x389d0393)

Explanation
See the message.

Administrator response
Verify that the ITIM Principal Name entry exists in the ITIM CDAS configuration file.

DPWCA0916E

Could not find ITIM Principal Password in the ITIM CDAS configuration file. (0x389d0394)

Explanation
See the message.

Administrator response
Verify that the ITIM Principal Password entry exists in the ITIM CDAS configuration file.

DPWCA0917E

Could not find ITIM message header. (0x389d0395)

Explanation
ITIM server replied with an invalid HTTP message header.

Administrator response
Check ITIM server for error message details. Verify the version of the reverse password server component.

DPWCA0922E

The password could not be changed in ITIM. The password has beeen changed in Verify Access. (0x389d039a)

Explanation
Message indicates that module failed to change the password in ITIM. Password in Verify Access has been changed.

Administrator response
No action is required.

DPWCF0450E

The IBM Security Verify Access Runtime installation directory could not be found. Install IBM Security Verify Access Runtime. (0x389d51c2)

Explanation
The installation directory for AMRTE could not be found in the registry. This is probably because AMRTE is not installed.

Administrator response
Make sure that AMRTE is installed.

DPWCF0451E

The IBM Security Verify Access WebSEAL installation directory could not be found. Install IBM Security Verify Access WebSEAL. (0x389d51c3)

Explanation
The installation directory for AMWeb could not be found in the registry. This is probably because AMWeb is not installed.

Administrator response
Make sure that IBM Security Verify Access WebSEAL is installed.

DPWCF0452E

The configuration file '*%s*' could not be opened. (0x389d51c4)

Explanation
The configuration file may not exist, or file system permissions may prevent it from being opened.

Administrator response
Make sure that the configuration file exists and can be read and written.

DPWCF0453E

The file '*%s*' could not be opened. Error code: *%d* (0x389d51c5)

Explanation
The file could not be opened. The system function returned the indicated error code

Administrator response
Make sure that the file exists in the system, and that it is readable and writable. If necessary, look up the system error code to determine the problem.

DPWCF0454E

The file '*%s*' could not be closed. Error code *%d*. (0x389d51c6)

Explanation
A file could not be closed because of the indicated system error.

Administrator response
Make sure that the file system on which the file is located is not full. Also make sure that the directory for the file exists and is writable. If necessary, look up the system error code to identify the problem.

DPWCF0455E

The directory '*%s*' could not be opened. Error code: *%d* (0x389d51c7)

Explanation
The directory could not be opened because of the indicated system error code.

Administrator response
Make sure that the directory exists and file system permissions allow it to be read.

DPWCF0456E

The directory '*%s*' could not be closed. Error code: *%d* (0x389d51c8)

Explanation
Closing a directory failed because of the indicated system error code.

Administrator response
Make sure that the directory exists and is writable.

DPWCF0457E

The instance name '*%s*' is already in use. (0x389d51c9)

Explanation
The instance name is already in use.

Administrator response
Use a different instance name.

DPWCF0458E

The length of the instance name '*%s*' is more than *%d* characters. (0x389d51ca)

Explanation
The provided instance name is more than 20 characters.

Administrator response
Use an instance name that has less than 20 characters.

DPWCF0459E

The instance name '*%s*' contains invalid characters. Instance names must consist of alphanumeric characters plus the symbols: '-' '_' '.' (0x389d51cb)

Explanation
The provided instance name contains illegal characters.

Administrator response
Use an instance name that contains only valid characters.

DPWCF0460E

The IP address '*%s*' does not exist in the system. (0x389d51cc)

Explanation
The provided IP address does not exist in the system.

Administrator response
Make sure that the provided IP address exists in the system.

DPWCF0461E

The key file '*%s*' does not exist in the system. (0x389d51cd)

Explanation
The provided key file does not exist in the system.

Administrator response
Make sure the provided key file exists in the system.

DPWCF0462E

The key file password is incorrect. (0x389d51ce)

Explanation
The key file password may have been entered incorrectly.

Administrator response
Make sure that the key file password is entered correctly.

DPWCF0463E

The LDAP server could not be contacted through SSL on port *%d*. (0x389d51cf)

Explanation
The SSL LDAP port may have been entered incorrectly, or the LDAP server may not be running.

Administrator response
Make sure the LDAP server is running. Correct the SSL LDAP port if necessary.

DPWCF0464E

The key file for SSL communcation with the LDAP server is invalid. (0x389d51d0)

Explanation
The wrong key file may have been entered.

Administrator response
Make sure that the provided key file is a valid key file for SSL communication with the LDAP server

DPWCF0465E

SSL environment could not be opened. Error: *%s*. (0x389d51d1)

Explanation
An internal SSL error occurred.

Administrator response
The action to correct this problem depends on details in the error message.

DPWCF0466E

Port '*%s*' is already in use. (0x389d51d2)

Explanation
The provided port is already in use.

Administrator response
Use a different port, or remove the service that is using the port.

DPWCF0467E

Fields marked with an asterisk (*) are required. (0x389d51d3)

Explanation
Not all required inputs were provided.

Administrator response
Fill in values for all of the required fields.

DPWCF0468E

The Policy Server could not be contacted. Make sure the Policy Server is running and try again. (0x389d51d4)

Explanation
The Policy Server must be running in order to configure WebSEAL.

Administrator response
Make sure the Policy Server is functioning properly. Restart the Policy Server if necessary.

DPWCF0469E

The file '*%s*' could not be copied to '*%s*' (0x389d51d5)

Explanation
An error occurred when trying to copy a file.

Administrator response
Make sure the orginal file exists and the directory for the new file exists. Make sure the file system has sufficient space to copy the file. Make sure the destination directory is writable.

DPWCF0470E

The directory '*%s*' could not be copied to the directory '*%s*'. (0x389d51d6)

Explanation
The original directory or the path of the new directory may not be existed.

Administrator response
Make sure the orginal directory exists and the path of the new directory also exists.

DPWCF0471E

The directory '*%s*' could not be created. (0x389d51d7)

Explanation
The path to the directory that want to be created may be not existed in the system.

Administrator response
Make sure the path to the directory that want to be created exists in the system.

DPWCF0472E

The random password could not be generated. (0x389d51d8)

Explanation
Memory allocation operation failed.

Administrator response
Check memory limits on your machine, and increase availabel memory if possible

DPWCF0473E

The WebSEAL instance '*%s*' failed to configure. (0x389d51d9)

Explanation
WebSEAL instance cannot be configured due to the error that displayed before this message

Administrator response
Unconfigure this WebSEAL instance and run configuration program again.

DPWCF0474E

The WebSEAL instance '*%s*' failed to unconfigure. (0x389d51da)

Explanation
WebSEAL instance cannot be unconfigured due to the error that displayed before this message

Administrator response
Run unconfiguration program again.

DPWCF0475E

The specified document root directory '*%s*' does not exist. (0x389d51db)

Explanation
The provided document root directory does not exist.

Administrator response
Make sure the document root directory exists in the system.

DPWCF0476E

The specified option '*%s*' is invalid. (0x389d51dc)

Explanation
The specified option is invalid. Only the flags in the usage message are valid.

Administrator response
The specified option is invalid. Use one of the options from the usage and try again.

DPWCF0477E

The specified option '*%s*' needs a parameter. (0x389d51dd)

Explanation
The specified option must have a parameter.

Administrator response
Need to specify a parameter for the specified action.

DPWCF0478E

The action option needs to be specified. (0x389d51de)

Explanation
The "action" option needs to be specified to configure or unconfigure WebSEAL instance from command line.

Administrator response
Need to specify the "action" option in the command line inputs.

DPWCF0479E

The specified certificate label '*%s*' is invalid. (0x389d51df)

Explanation
The provided certificate label is incorrect.

Administrator response
Make sure the certificate label is entered correctly.

DPWCF0480E

The response file '*%s*' could not be opened. (0x389d51e0)

Explanation
The provided response file does not exist.

Administrator response
Make sure the response file exists.

DPWCF0481E

The instance name '*%s*' does not exist to unconfigure. (0x389d51e1)

Explanation
No instance with the provided name was found on the system.

Administrator response
Make sure the instance name was typed correctly.

DPWCF0482E

Could not determine the hostname of the machine. Error code: *%d* (0x389d51e2)

Explanation
An error occurred when attempting to determine the host name of the local system.

Administrator response
Make sure the network configuration on the machine is correct.

DPWCF0483E

The entry '*%s*' in the response file does not have a value (0x389d51e3)

Explanation
A needed entry in the response file did not have a value.

Administrator response
Make sure that the value of the entry exists in the response file.

DPWCF0484E

Error: the configuration program must be run as root. (0x389d51e4)

Explanation
The configuration program needs to be run as the root user in order to be able to function properly.

Administrator response
Run the configuration program as the root user.

DPWCF0485E

The ownership of '*%s*' cannot be changed to user ivmgr, group ivmgr. Error code: *%d*. (0x389d51e5)

Explanation
An attempt to change the ownership of a file or directory failed. The system error number can be used to determine the cause of the failure.

Administrator response
Make sure the file or directory exists.

DPWCF0486E

Could not create symbolic link from '*%s*' to '*%s*'. Error code: *%d*. (0x389d51e6)

Explanation
An attempt to create a symbolic link failed.

Administrator response
Make sure the destination directory for the symlink exists, and no file or directory exists in that location already. Look up the system error code for further information if necessary.

DPWCF0487E

The hash table for configuration options cannot be initialized. (0x389d51e7)

Explanation
The hash table can not be initialized because the allocation of the options failed.

Administrator response
Check memory limits on your machine, and increase available memory if possible

DPWCF0488E

The file '*%s*' could not be moved to '*%s*' (0x389d51e8)

Explanation
An error occurred when trying to move a file.

Administrator response
Make sure the orginal file exists and the directory for the new file exists. Make sure the file system has sufficient space to move the file. Make sure the destination directory is writable.

DPWCF0489E

ERROR: For WebSEAL to function correctly the maximum number of threads per process should be at least 96. This value can be increased by modifying the MAXTHREADPROC or MAX_THREAD_PROC kernel parameter through the sam utility. (0x389d51e9)

Explanation
The MAXTHREADPROC or MAX_THREAD_PROC must be greater than 96 for WebSEAL to function correctly.

Administrator response
Use the sam utility to increase the MAXTHREADPROC or MAX_THREAD_PROC and run the configuration program again.

DPWCF0490E

The configuration status could not be set. (0x389d51ea)

Explanation
This problem should not occur. If it does happen, the machine should be restarted and run the configuration program again.

Administrator response
Restart the machine and run the configuration program again.

DPWCF0491E

The file '*%s*' could not be deleted. Error code: *%d*. (0x389d51eb)

Explanation
An attempt to delete a file failed.

Administrator response
Make sure that the file and the directory containing the file are both writable.

DPWCF0492E

The socket could not be created. Error code: *%d* (0x389d51ec)

Explanation
An error occurred when attempting to initialize a socket.

Administrator response
Look up the system error code for additional information. Check system resource limits on the number of file descriptors, and increase the limits if necessary.

DPWCF0493E

The -interactive option is not supported on this platform. (0x389d51ed)

Explanation
The amwebcfg utility does not support the -interactive flag on Windows.

Administrator response
Should not use interactive option for the amwebcfg utility on windows

DPWCF0494E

The executable file 'ldapsearch' could not be found. (0x389d51ee)

Explanation
The installlation directory for the LDAP client could not be found.

Administrator response
Make sure the LDAP client is installed correctly.

DPWCF0495E

The configuration value of an entry [*%s*] '*%s*' could not be retrieved from the configuration file '*%s*'. (0x389d51ef)

Explanation
An attempt to retrieve an entry from a configuration file failed.

Administrator response
Check logs for additional errors. The configuration file may not exist or might not be readable. The entry might not exist in the configuration file.

DPWCF0496E

The user '*%s*' does not have permission to unconfigure the server. (0x389d51f0)

Explanation
Only IBM Security Verify Access Administrators are allowed to configure or unconfigure WebSEAL.

Administrator response
Run the configuration program again, supplying the ID and password of an Administrative user.

DPWCF0497E

The response file '*%s*' does not exist. (0x389d51f1)

Explanation
The provided response file does not exist or is not readable.

Administrator response
Make sure the response file exists and is readable.

DPWCF0498E

The user '*%s*' could not be removed from the group '*%s*'. Error message: '*%s*' (0x389d51f2)

Explanation
The function ivadmin_group_removemember failed to remove the user from the group because of the indicated error.

Administrator response
Fix the problem indicated by the error message.

DPWCF0499E

The objectspace '*%s*' could not be created. Error message: '*%s*' (0x389d51f3)

Explanation
The function ivadmin_objectspace_create failed to create the objectspace because of the indicated error.

Administrator response
Fix the problem indicated by the error message.

DPWCF0500E

The ACL '*%s*' could not be created with an error: '*%s*' (0x389d51f4)

Explanation
The function ivadmin_acl_create failed to create the ACL because of the indicated error.

Administrator response
Fix the problem indicated by the error message.

DPWCF0501E

The description of ACL '*%s*' could not be set to '*%s*'. Error message: '*%s*' (0x389d51f5)

Explanation
The function ivadmin_acl_setdescription failed because of the indicated error.

Administrator response
Fix the problem indicated by the error message.

DPWCF0502E

The permissions for group '*%s*' in the ACL '*%s*' could not be set. Error message: '*%s*' (0x389d51f6)

Explanation
The function ivadmin_acl_setgroup failed to set the group permissions because of the indicated error.

Administrator response
Fix the problem indicated by the error message.

DPWCF0503E

The permissions for user '*%s*' in the ACL '*%s*' could not be set. Error message: '*%s*' (0x389d51f7)

Explanation
The function ivadmin_acl_setuser failed to set the user permissions because of the indicated error.

Administrator response
Fix the problem indicated by the error message.

DPWCF0504E

The permissions for anyother in the ACL '*%s*' could not be set. Error message: '*%s*' (0x389d51f8)

Explanation
The function ivadmin_acl_setanyother failed to set the permissions for anyother because of the indicated error.

Administrator response
Fix the problem indicated by the error message.

DPWCF0505E

The permissions for unauthenticated in the ACL '*%s*' could not be set to '*%s*'. Error message: '*%s*' (0x389d51f9)

Explanation
The function ivadmin_acl_setunauth failed to set the permissions for unauthenticated because of the indicated error.

Administrator response
Fix the problem indicated by the error message.

DPWCF0506E

The ACL '*%s*' could not be attached to the protected object '*%s*'. Error message: '*%s*' (0x389d51fa)

Explanation
The function ivadmin_protobj_attachacl failed to attach the acl to a protected object because of the indicated error.

Administrator response
Fix the problem indicated by the error message.

DPWCF0507E

The protected object '*%s*' could not be created. Error message: '*%s*' (0x389d51fb)

Explanation
The function ivadmin_protobj_create failed to create a protected object because of the indicated error.

Administrator response
Fix the problem indicated by the error message.

DPWCF0508E

The protected object '*%s*' could not be deleted. Error message: '*%s*' (0x389d51fc)

Explanation
The function ivadmin_protobj_create failed to delete the protected object because of the indicated error.

Administrator response
Fix the problem indicated by the error message.

DPWCF0509E

The group '*%s*' could not be retrieved. Error message: '*%s*' (0x389d51fd)

Explanation
The function ivadmin_group_get fails to retrieve the group because of the indicated error.

Administrator response
Fix the problem indicated by the error message.

DPWCF0510E

The group '*%s*' could not be created. Error message: '*%s*' (0x389d51fe)

Explanation
The function ivadmin_group_create failed to create a group because of the indicated error.

Administrator response
Fix the problem indicated by the error message.

DPWCF0511E

The descript for group '*%s*' could not be set to '*%s*'. Error message: '*%s*' (0x389d51ff)

Explanation
The function ivadmin_group_setdescription failed because of the indicated error.

Administrator response
Fix the problem indicated by the error message.

DPWCF0512E

The DN of the group '*%s*' could not be retrieved. Error message: '*%s*' (0x389d5200)

Explanation
The function ivadmin_group_getdn failed because of the indicated error.

Administrator response
Fix the problem indicated by the error message.

DPWCF0513E

The directory '*%s*' could not be deleted. (0x389d5201)

Explanation
The directory may not exist.

Administrator response
Make sure the directory exists.

DPWCF0514E

The ivadmin context could not be created. Error message '*%s*'. Use pdadmin to manually create 'su-admins' and 'su-excluded' groups as instructed in the appendix of WebSEAL upgrade document. (0x389d5202)

Explanation
The function ivadmin_context_createdefault2 failed because of the indicated error.

Administrator response
Fix the problem indicated by the error message.

DPWCF0515E

Use pdadmin to manually create 'su-admins' or 'su-excluded' groups as instructed in the appendix of WebSEAL upgrade document. (0x389d5203)

Explanation
The 'su-admins' or 'su-groups' could not be created in the upgrade process. It should be created manually.

Administrator response
Fix the problem indicated by the message.

DPWCF0516E

The tivoli_common_dir entry in the log.properties file has an empty value. (0x389d5204)

Explanation
The tivoli_common_dir entry must contain Tivoli Common Directory in log.properties file if Tivoli Common Directory is used.

Administrator response
Add a Tivoli Common Directory to tivoli_common_dir entry in log.properties file.

DPWCF0517E

The log.properties file does not exist. (0x389d5205)

Explanation
The log.properties file must exist in Tivoli Common Directory if Tivoli Common Directory is used.

Administrator response
Make sure the log.properties file exists in Tivoli Common Directory.

DPWCF0518E

Failed to create Tivoli Common Directory for WebSEAL. (0x389d5206)

Explanation
An error occurred when creating Tivoli Common Directory for WebSEAL.

Administrator response
The action to correct this problem depends on details displayed in previous error messages.

DPWCF0519E

Failed to relocate Tivoli Common Directory for WebSEAL. (0x389d5207)

Explanation
An error occurred when relocating the Tivoli Common Directory for WebSEAL.

Administrator response
The action to correct this problem depends on details displayed in previous error messages.

DPWCF0520E

The '*%s*' option must be provided on the command line. (0x389d5208)

Explanation
The option displayed in the message must be provided in the command line in order to successfully configure WebSEAL.

Administrator response
Provide the option displayed in the message on the command line.

DPWCF0521E

The '*%s*' option only uses 'y' or 'n' for its parameter. (0x389d5209)

Explanation
The option displayed in the message requires 'y' or 'n' for its value.

Administrator response
Need to provide 'y' or 'n' as the value of the option displayed in the message on the command line.

DPWCF0522E

The administrator ID or password is invalid. (0x389d520a)

Explanation
A valid administrator ID and valid password are required to configure WebSEAL.

Administrator response
Make sure that the administrator ID and password provided are correct.

DPWCF0523E

The request-log-format entry in the logging stanza contains an invalid directive: *%s* (0x389d520b)

Explanation
The request-log-format value is invalid.

Administrator response
Correct the invalid request-log-format configuration value.

DPWCF0524E

The request-log-format entry in the logging stanza contains an invalid parameter for a directive. (0x389d520c)

Explanation
The request-log-format value is invalid.

Administrator response
Correct the invalid request-log-format configuration value.

DPWCF0525W

The ping-method value of '*%s*' is not a valid ping-method, defaulting to HEAD. (0x389d520d)

Explanation
The ping-method specified is not supported. A default value of 'HEAD' has been used.

Administrator response
No action is necessary.

DPWCF0527W

The configuration item (*%s*, *%s*) is missing, defaulting to a value of: '*%s*'. (0x389d520f)

Explanation
The required configuration entry is missing, a default value will be used.

Administrator response
Add the required configuration entry to the configuration file.

DPWCF0528W

The configuration file entry encountered is not valid. (0x389d5210)

Explanation
A configuration entry was retrieved from the configuration file which was not of the expected type or formatting.

Administrator response
Examine the log files for additional information.

DPWCF0529E

Domain cookies cannot be shared when the session management server has been configured. (0x389d5211)

Explanation
The configuration items [session] shared-cookie-name and [session] dsess-enabled are mutually exclusive. If you are attempting to acheive single sign-on in an SMS environment, Disable the shared-cookie-name configuration entry. If you are in an environment without the SMS, disable the dsess-enabled configuration entry.

Administrator response
Correct the configuration as needed and restart the WebSEAL daemon.

DPWCF0530E

A login redirect page cannot be specified when JavaScript redirection is enabled. (0x389d5212)

Explanation
The configuration items [acnt-mgt] enable-js-redirect and [acnt-mgt] login-redirect-page are mutually exclusive.

Administrator response
Correct the configuration as needed and restart the WebSEAL daemon.

DPWCF0531E

The configured single sign-off resource is invalid. The resource must reside on a standard junction. (0x389d5213)

Explanation
The single sign-off resource must reside on a standard junction and the URI specified must begin with a '/'.

Administrator response
Correct the configuration as needed and restart the WebSEAL daemon.

DPWCF0532E

The configured list of user-agent patterns will not match all user-agent strings. The list must contain a match-all pattern. (0x389d5214)

Explanation
The configured list of user-agent patterns will not match against all possible user-agent strings. Add a new entry to the [user-agents] stanza with the pattern '*'.

Administrator response
Correct the configuration as needed and restart the WebSEAL daemon.

DPWCF0533E

The [user-agents] stanza must be configured when flow data is enabled. (0x389d5215)

Explanation
The configuration stanza [user-agents] must be configured and contain at least one entry when using the flow data functionality.

Administrator response
Correct the configuration as needed and restart the WebSEAL daemon.

DPWCF0534E

No default HTTP method permission map has been specified under the [http-method-perms] stanza in the configuration file. (0x389d5216)

Explanation
A default HTTP method permission map must be specified in the WebSEAL configuration file, but it has not been.

Administrator response
Specify a value for the default HTTP method permission map in the WebSEAL configuration file.

DPWCF0535E

No default HTTP method permission map has been specified under the [http-method-perms:*%s*] stanza in the configuration file. (0x389d5217)

Explanation
A default HTTP method permission map must be specified in the WebSEAL configuration file, but it has not been.

Administrator response
Specify a value for the default HTTP method permission map in the WebSEAL configuration file.

DPWCF0536E

HTTP method permission map validation failed. (0x389d5218)

Explanation
Invalid permission sets are mapped to HTTP methods in the configuration file.

Administrator response
Ensure that the permission sets mapped to each HTTP method in the [http-method-perms] stanzas of the WebSEAL configuration file are valid.

DPWCF0537W

The provided global HTTP method permission map in [http-method-perms] is invalid and will not be used. (0x389d5219)

Explanation
Invalid configuration was provided in the [http-method-perms] stanza. This configuration will be ignored.

Administrator response
Correct the configuration of the [http-method-perms] stanza in the WebSEAL configuration file.

DPWCF0538W

The provided junction HTTP method permission map in [http-method-perms:*%s*] is invalid and will not be used. (0x389d521a)

Explanation
Invalid configuration was provided in the [http-method-perms] stanza. This configuration will be ignored.

Administrator response
Correct the configuration of the [http-method-perms] stanza in the WebSEAL configuration file.

DPWDS0150E

An attempt to create a UUID has failed with the following error: *%s* (error code: 0x*%x*) (0x38a0a096)

Explanation
An attempt to create a UUID has failed.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0151E

An attempt to retrieve the machine address code (MAC) failed: *%s* (error code: 0x*%lx*) (0x38a0a097)

Explanation
An attempt to retrieve the MAC of the server failed.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0152E

Memory could not be allocated. (0x38a0a098)

Explanation
An error occurred when the process attempted to allocate memory. There is not enough free memory available to complete the request.

Administrator response
Examine the system for processes consuming excessive memory and restart them. Ensure the system has sufficient physical and virtual memory for its expected load. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0153E

No more entries were found in the specified list. (0x38a0a099)

Explanation
An operation requested another entry from a list when there were no remaining entries.

Administrator response
This message is logged as a clarifying addition to another error message. Refer to the recommended action for that error message. For further detailed information about the failure examine earlier messages in the log containing this message. Correct any problems and retry the operation.

DPWDS0154E

An invalid number was supplied. (0x38a0a09a)

Explanation
The system was expecting a number to be supplied, but something else was supplied instead.

Administrator response
Examine other error messages for more detail, correct any problem, and retry the operation.

DPWDS0155E

The number which was supplied is too large. (0x38a0a09b)

Explanation
The number which was supplied to the system was too large to fit into the allocated memory.

Administrator response
Examine other error messages for more detail, correct any problem, and retry the operation.

DPWDS0156E

A system routine failed. (0x38a0a09c)

Explanation
A system routine failed.

Administrator response
Examine the log for additional information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0157E

The *%s* system routine failed: system error code: *%d* (0x38a0a09d)

Explanation
A system routine failed for the reason indicated by the system error code.

Administrator response
Examine the log for additional information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0158E

The requested data is not available. (0x38a0a09e)

Explanation
An operation requested data that was not available.

Administrator response
This message is logged as the reason part of an error message. Refer to the recommended action for that error message. For further detailed information about the failure examine earlier messages in the log containing this message. Correct any problems and retry the operation.

DPWDS0159E

A command line option was not of the correct format. (0x38a0a09f)

Explanation
A command line option was not specified correctly.

Administrator response
Re-run the configuration program ensuring the correct command line options are provided.

DPWDS0160E

The supplied configuration data was not valid. (0x38a0a0a0)

Explanation
A configuration entry was found to be invalid.

Administrator response
Examine the log for further details of the error, correct the configuration, and retry the operation.

DPWDS0161E

The command line option, *-%s*, is not valid. (0x38a0a0a1)

Explanation
The command line option is not valid for the current program.

Administrator response
Check the usage of the program and re-run it with the correct options.

DPWDS0162E

A binary has been executed with incorrect arguments. (0x38a0a0a2)

Explanation
A binary has been executed with incorrect arguments.

Administrator response
Examine the log files for further error messages, correct any problem, and retry the operation.

DPWDS0163W

The '*%s*' parameter of the command is invalid. (0x38a0a0a3)

Explanation
The specified parameter, supplied for an administration task, was invalid.

Administrator response
Review the format of the command text to ensure all parameters are correct.

DPWDS0164W

An invalid command parameter was supplied. (0x38a0a0a4)

Explanation
One of the command parameters, supplied for an administration task, was invalid.

Administrator response
Review the format of the command text to ensure all parameters are correct.

DPWDS0165E

Could not open file *%s* (system error code: *%d*). (0x38a0a0a5)

Explanation
The identified file could not be opened for the specified reason.

Administrator response
Check to ensure that the file exists and has the correct permissions.

DPWDS0166E

The configuration file could not be opened. (0x38a0a0a6)

Explanation
The specified file could not be opened.

Administrator response
Check that the file exists and has the correct permissions.

DPWDS0167E

Expected configuration data could not be located in the configuration file. (0x38a0a0a7)

Explanation
An expected configuration item is not present in the configuration file.

Administrator response
Examine the log for further details of the error, correct the configuration, and retry the operation.

DPWDS0168E

The *%s* stanza of *%s* requires specification of the *%s* configuration parameter. (0x38a0a0a8)

Explanation
An expected configuration item is not present in the configuration file.

Administrator response
Correct the configuration and retry the operation.

DPWDS0169E

Could not open configuration file '*%s*' due to error: '*%s*'. (0x38a0a0a9)

Explanation
The identified file could not be opened for the specified reason.

Administrator response
Check to ensure that the file exists and has the correct permissions.

DPWDS0300E

The distributed session cache client failed to initialized. (0x38a0a12c)

Explanation
The client for the distributed session cache interface could not be initialized.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0301E

A general failure has occurred within the distributed session cache client. (0x38a0a12d)

Explanation
An error has occurred within the distributed session cache client.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0302E

A replica set which is unknown to the distributed session cache client has been supplied (*%s*). (0x38a0a12e)

Explanation
An operation on a unknown distributed session cache replica set has been requested.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0303E

A replica set which is unknown to the distributed session cache client has been supplied. (0x38a0a12f)

Explanation
An operation on a unknown distributed session cache replica set has been requested.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0304E

The requested version *%d* of the session key was not found for replica *%s* in replica set *%s*. (0x38a0a130)

Explanation
A request was made for a session key which is not currently stored. This error occurs when an old session ID is used.

Administrator response
Either increment the key expiration time within the configuration file, or ensure that old session ID's are not used.

DPWDS0305E

The requested key was not found. (0x38a0a131)

Explanation
A request was made for a session key which is not currently stored. This will usually occur when an old session ID is used.

Administrator response
Either increment the key expiration time within the configuration file, or ensure that old session ID's are not used.

DPWDS0306E

No session keys are currently available. (0x38a0a132)

Explanation
A request was made for the current session key, but no key has been stored in the key table .

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0307E

An error occurred when attempting to communicate with the SOAP server URL *%s*: *%s* (error code: *%d*/0x*%x*). (0x38a0a133)

Explanation
An attempt was made to communicate with the SOAP server and a failure occurred within the underlying communications layer.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. Ensure that the SOAP server is running and reachable. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0309E

An error was returned from the SOAP server in cluster *%s* when calling the *%s* interface: *%s* (code: 0x*%x*). (0x38a0a135)

Explanation
The distributed session cache server returned an error.

Administrator response
Examine messages within the distributed session cache server log. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0310E

An invalid key size was returned by the distributed session cache server: *%d*, whereas it should be: *%d*. (0x38a0a136)

Explanation
The distributed session cache server has passed a key to the client which is not the expected key size.

Administrator response
Examine messages within the distributed session cache server log. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0311E

An incorrect key version was returned by the distributed session cache server to replica *%s* in replica set *%s*: *%d*, whereas it should be: *%d*. (0x38a0a137)

Explanation
The distributed session cache server has passed a key to the client which is not the expected version.

Administrator response
Examine messages within the distributed session cache server log. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0312E

The distributed session cache server could not be reached. (0x38a0a138)

Explanation
An unsuccessful attempt has been made to communicate with an interface of the distributed session cache server.

Administrator response
Ensure that the distributed session cache server is running and can be reached by the client. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0313E

The cryptographic routine, *%s*, failed : *%s* (error code: 0x*%x*). (0x38a0a139)

Explanation
A call in to a cryptographic routine has failed.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0314E

The cryptographic routine, *%s*, failed. (0x38a0a13a)

Explanation
A call in to a cryptographic routine has failed.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0315W

An invalid session key was provided to the distributed session cache server client. (0x38a0a13b)

Explanation
A session key with an invalid format was provided to the distributed session cache server client.

Administrator response
Ensure that the distributed session cache server is running and can be reached by the client. Restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0316E

The distributed session cache server did not return a response. (0x38a0a13c)

Explanation
The distributed session cache server did not return a response to a request made by the shared distributed session cache client.

Administrator response
Ensure that the distributed session cache server is running and can be reached by the client. Examine the distributed session cache server's logs for error messages relating to this failure. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0319E

The distributed session cache server client attempted to join the replica set '*%s*' twice with the replica name '*%s*'. (0x38a0a13f)

Explanation
The distributed session cache server client has been configured to join a replica set twice using the same replica name. The client must use different replica names for each server instance in a replica set.

Administrator response
Modify the configuration file to specify different replica names for each server instance joining the same replica set. Restart the server.

DPWDS0320E

The DN contained within the server certificate, *%s*, is not recognised by replica *%s* in replica set *%s*. (0x38a0a140)

Explanation
The DN found within the server certificate was not listed as a valid DN within the configuration file.

Administrator response
Ensure that the correct server certificate is supplied, or modify the list of valid DN's within the configuration file.

DPWDS0321E

The replica *%s* in replica set *%s* does not have permission to access the distributed session cache server. (0x38a0a141)

Explanation
The distributed session cache server has been configured to require authentication, but the distributed session cache client either did not authenticate, or authenticated using an identity that does not have permission to access the distributed session cache server.

Administrator response
Ensure the distributed session cache client has been configured to use HTTPS to access the distributed session cache server, and that the configuration file specifies the correct client certificate. Check that the distributed session cache server security role mappings are correct. It may be necessary to restart the client.

DPWDS0322E

The distributed session cache server for the replica set, *%s*, of the replica, *%s*, could not be reached. (0x38a0a142)

Explanation
An unsuccessful attempt has been made to communicate with an interface of the distributed session cache server.

Administrator response
Ensure that the distributed session cache server is running and can be reached by the client. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0323E

No session keys are currently available for replica *%s* in replica set *%s*. (0x38a0a143)

Explanation
A request was made for the current session key, but no key has been stored in the key table .

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0450E

Error parsing STS response element line *%d*, column *%d*: '*%s*'. The element text was '*%s*'. (0x38a0a1c2)

Explanation
The STS returned an unintelligible XML response.

Administrator response
If other elements of the STS response are complete, SSO will continue. Otherwise, SSO will fail. If SSO fails, exmaine the element to determine why the STS response was invalid.

DPWDS0451E

Unable to parse timestamp '*%s*' (0x38a0a1c3)

Explanation
The timestamp returned from the STS was unintelligible.

Administrator response
Examine the element to determine why the timestamp was invalid.

DPWDS0452E

Unable to parse timestamp. (0x38a0a1c4)

Explanation
The timestamp returned from the STS was unintelligible.

Administrator response
Examine the element to determine why the timestamp was invalid.

DPWDS0453E

The STS response did not contain the element '*%s*' (0x38a0a1c5)

Explanation
The STS response was incomplete.

Administrator response
The TFIM server may not be functioning properly, or the STS module may need to be modified to return the necessary data.

DPWDS0454E

The STS response did not contain a necessary element. (0x38a0a1c6)

Explanation
The STS response was incomplete.

Administrator response
Examine other entries in the logs to determine which element was missing. The TFIM server may not be functioning properly, or the STS module may need to be modified to return the necessary data.

DPWDS0455E

Token types other than 'kerberos' require that you specify an HTTP header name with the 'header-name' configuration option or an HTTP cookie name with the 'cookie-name' configuration option. (0x38a0a1c7)

Explanation
A configuration option was missing from the configuration file

Administrator response
Add the needed entries to the configuration file.

DPWDS0456E

Error *%08x* occurred when retrieving a token for user '*%s*' to access '*%s*'. Refer to other log messages for additional detail. (0x38a0a1c8)

Explanation
An attempt to retrieve a token to access a resource failed. Other messages with greater detail have been logged.

Administrator response
Examine other entries in the logs to determine the root cause of the failure.

DPWDS0600E

An unexpected AXIS exception was caught while processing a client request. Error message *%s* (0x*%x*) was returned with the exception. (0x38a0a258)

Explanation
AXIS returned an exception condition while process a client request.

Administrator response
Refer to the error log to determine if an error message accompanied the exception.

DPWDS0601E

A failure occurred while processing a received distributed session request. (0x38a0a259)

Explanation
An error occurred when processing a distributed session request.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0602E

The server could not bind to the configured address: *%s* (0x38a0a25a)

Explanation
An error occurred when the server attempted to bind to the configured IP address.

Administrator response
Check the configured IP address to ensure that it is a valid local address on the server.

DPWDS0604W

The distributed session cache server has started. (0x38a0a25c)

Explanation
The distributed session cache server has started.

Administrator response
No action required.

DPWDS0605W

The distributed session cache server has been stopped. (0x38a0a25d)

Explanation
The distributed session cache server has been stopped by the administrator.

Administrator response
No action required.

DPWDS0606E

Could not accept incoming connection on '*%s*:*%d*': system error number = *%d* (0x38a0a25e)

Explanation
The Operating System returned an error when the server attempted to accept an incoming connection.

Administrator response
Check the server has not exceeded system resource limits. For further details on the problem refer to the system error number in the operating system documentation.

DPWDS0607E

Could not accept incoming connection (0x38a0a25f)

Explanation
The Operating System returned an error when the server attempted to accept an incoming connection.

Administrator response
Check the server has not exceeded system resource limits.

DPWDS0608E

Could not poll for any incoming connections: system error number = *%d* (0x38a0a260)

Explanation
The Operating System returned an error when the server attempted to poll for an incoming connection on the configured addresses and port.

Administrator response
Check the server has not exceeded system resource limits. For further details on the problem refer to the system error number in the operating system documentation.

DPWDS0609E

Could not poll for incoming connection (0x38a0a261)

Explanation
The Operating System returned an error when the server attempted to poll for an incoming connection on the configured addresses and port.

Administrator response
Check the server has not exceeded system resource limits.

DPWDS0610E

Could not determine the local network address of a connection: system error number = *%d* (0x38a0a262)

Explanation
The Operating System returned an error when the server attempted to determine the network interface over which the incoming connection was received.

Administrator response
Check the server has not exceeded system resource limits. For further details on the problem refer to the system error number in the operating system documentation.

DPWDS0611E

Could not determine the local network address of a connection (0x38a0a263)

Explanation
The Operating System returned an error when the server attempted to determine the network interface over which the incoming connection was received.

Administrator response
Check the server has not exceeded system resource limits.

DPWDS0612E

The *%s* '*%s*' is a duplicate or a subset of another configured *%s* entry. (0x38a0a264)

Explanation
It is not valid to specify the same address twice, or to specify an address like '::' or 0.0.0.0 with additional addresses as they cover all addresses.

Administrator response
Modify the server configuration file and remove the listen-address configuration entry which is causing the problem.

DPWDS0613E

A configured address is a duplicate or a subset of another. (0x38a0a265)

Explanation
It is not valid to specify the same address twice, or to specify an address like '::' or '0.0.0.0' with additional addresses as they cover all addresses.

Administrator response
Modify the server configuration file and remove the address causing the problem.

DPWDS0614E

accept-admin-address values must be a subset of the listen-address addresses. (0x38a0a266)

Explanation
It is not valid to specify an accept-admin-address that is not also included by the listen-address configuration.

Administrator response
Modify the server configuration file and correct the accept-admin-address configuration entry which is causing the problem.

DPWDS0615E

Could not determine the remote network address of a connection: system error number = *%d* (0x38a0a267)

Explanation
The Operating System returned an error when the server attempted to determine the remote network address from which the incoming connection was received.

Administrator response
Check the server has not exceeded system resource limits. For further details on the problem refer to the system error number in the operating system documentation.

DPWDS0616E

Could not determine the remote network address of a connection (0x38a0a268)

Explanation
The Operating System returned an error when the server attempted to determine the remote network address from which the incoming connection was received.

Administrator response
Check the server has not exceeded system resource limits.

DPWDS0617W

Entering standby mode. (0x38a0a269)

Explanation
The DSC server is changing mode, or starting up in standby mode. This is likely expected behavior caused by the startup of the server, or by the changing of the server mode by an administrator.

Administrator response
This is likely expected behavior and no action is required.

DPWDS0618W

Entering active mode. (0x38a0a26a)

Explanation
The DSC server is changing mode into active mode. At startup the server begins in standby mode and if appropriate will change to active mode. Or the active Distributed Session Cache server may have failed and this server is taking over as the active. Or the administrator has changed the mode of the server.

Administrator response
If this is not a startup mode change, then check the previous primary DSC server for failure.

DPWDS0619E

A database operation failed on line *%d* with error *%d*: '*%s*'. Native error *%d*. SQL state: '*%s*' (0x38a0a26b)

Explanation
An error was encountered while saving or reading session data to or from the database.

Administrator response
Check the SQL error message for the possible cause.

DPWDS0620E

A database operation failed. (0x38a0a26c)

Explanation
An error was encountered while saving or reading session data to or from the database.

Administrator response
Check the log for an SQL error message which contains a possible cause.

DPWDS0621E

The command 'ADMIN COMMAND 'hsb state' failed with an error *%d*: '*%s*'. (0x38a0a26d)

Explanation
An error was encountered while attempting to determine the HSB state of the embedded SolidDB server.

Administrator response
Check the error code and message for a possible cause.

DPWDS0622E

Unable to start the embedded SolidDB server. Error *%d*. (0x38a0a26e)

Explanation
An error was encountered while attempting to start the embedded SolidDB server.

Administrator response
Check the error code for the possible cause, such as invalid permissions on the database and log files.

DPWDS0623E

Unable to start the embedded SolidDB server. (0x38a0a26f)

Explanation
An error was encountered while attempting to start the embedded SolidDB server.

Administrator response
Check the error code in the log for a possible cause, such as invalid permissions on the database and log files.

DPWDS0624E

Unable to register a shutdown notifier function with the SolidDB server. Error *%d*. (0x38a0a270)

Explanation
An error was encountered while attempting to register a call back function with the embedded SolidDB server. This call back is required for detection of the shutdown of the embedded SolidDB server.

Administrator response
Check the error code for the possible cause.

DPWDS0625E

Unable to register a shutdown notifier function with the embedded SolidDB server. (0x38a0a271)

Explanation
An error was encountered while attempting to register a call back function with the embedded SolidDB server. This call back is required for detection of the shutdown of the embedded SolidDB server.

Administrator response
Check the error code in the log for the possible cause.

DPWDS0626E

Unable to load and extract functions from the SolidDB shared library. (0x38a0a272)

Explanation
An error was encountered while attempting to load the library containing the embedded SolidDB server.

Administrator response
Check the log for additional error messages.

DPWDS0627E

The configuration value of *%d* for number-of-nodes is not valid. It must be 0, 1, 2 or 4. (0x38a0a273)

Explanation
The number-of-nodes configuration value has an incorrect value.

Administrator response
Change the configuration file value to be correct and retry.

DPWDS0628E

The configuration value for number-of-nodes is not valid. It must be 0, 1, 2 or 4. (0x38a0a274)

Explanation
The number-of-nodes configuration value has an incorrect value.

Administrator response
Change the configuration file value to be correct and retry.

DPWDS0629E

The configuration value of *%d* for node-number is not valid. It must be a value from 1 to 4. (0x38a0a275)

Explanation
The node-number configuration value has an incorrect value.

Administrator response
Change the configuration file value to be correct and retry.

DPWDS0630E

The configuration value for node-number is not valid. It must be a value from 1 to 4. (0x38a0a276)

Explanation
The node-number configuration value has an incorrect value.

Administrator response
Change the configuration file value to be correct and retry.

DPWDS0631E

The option -n '*%s*' is not valid or missing. It must be a value from 1 to 4. (0x38a0a277)

Explanation
The -n command line option value has an incorrect value.

Administrator response
Correct the command line option and retry.

DPWDS0632E

The password option -p must be supplied and must not be an empty string. (0x38a0a278)

Explanation
The -p command line option value was not provided or was an empty string.

Administrator response
Correct the command line option and retry.

DPWDS0633E

The option '*%s*' must be supplied. (0x38a0a279)

Explanation
A required command line option value was not provided.

Administrator response
Add the missing option to the command line and then retry.

DPWDS0634E

The option -N '*%s*' is not valid. It must be one of 0, 1, 2 or 4. (0x38a0a27a)

Explanation
The -N command line option value has an incorrect value.

Administrator response
Correct the -N command line option and retry.

DPWDS0636E

Only one of the '-C' or '-U' options must be provided. (0x38a0a27c)

Explanation
Either none of -C or -U options were provided, or more than one was provided.

Administrator response
Either ensure that only one of -C or -U options are provided.

DPWDS0637E

The Distributed Session Cache server is already configured or there is an unexpected problem with the configuration file '*%s*' (0x38a0a27d)

Explanation
Either the Distributed Session Cache server configuration file exists, indicating it is already configured, or there was a problem attempting to check if the file exists.

Administrator response
Unconfigure the Distributed Session Cache server before attempting to configure it again. If the specified configuration file does not exist then ensure the directory which would contain the file is valid.

DPWDS0638E

Unable to contact the remote DSC server at '*%s*'. (0x38a0a27e)

Explanation
A test probe of the specified Distributed Session Cache server failed. This indicates that it may not be operational, the network connection is down, or the address and port used to access it are not correct.

Administrator response
Ensure that the specified Distributed Session Cache server is running.

DPWDS0639E

Unable to open the file '*%s*' error *%d*: '*%s*'. (0x38a0a27f)

Explanation
The configuration process failed to open the template configuration file.

Administrator response
Examine the error code and message for the cause of the failure and correct it.

DPWDS0640E

Unable to create the file '*%s*' error *%d*: '*%s*'. (0x38a0a280)

Explanation
The configuration process failed to create a new configuration file.

Administrator response
Examine the error code and message for the cause of the create failure and correct it.

DPWDS0641E

Error processing the configuration file '*%s*' line *%d*: '*%s*'. (0x38a0a281)

Explanation
An error occurred while processing the configuration file.

Administrator response
Examine the specified line for the cause of the error and correct it.

DPWDS0642E

Unable to remove the file '*%s*' error *%d*: '*%s*'. (0x38a0a282)

Explanation
The unconfiguration process failed to remove a file.

Administrator response
Examine the error code and message for the cause of the failure and correct it.

DPWDS0643E

Failed to create and initialize the backing database. (0x38a0a283)

Explanation
The DSC uses a backing SolidDB database to replicate session data for failover scenarios. The configuration tool was unable to create and initialize the database.

Administrator response
Retry the operation to see if the problem persists.

DPWDS0644E

Failed to put the backing database into a writable mode. (0x38a0a284)

Explanation
The DSC uses a backing SolidDB database to replicate session data for failover scenarios. The configuration tool was unable to put the database into a mode which will allow the data to be modified.

Administrator response
Retry the operation to see if the problem persists.

DPWDS0645E

Failed to cleanly shutdown the backing database. (0x38a0a285)

Explanation
The DSC uses a backing SolidDB database to replicate session data for failover scenarios. The configuration tool was unable cleanly shutdown the database.

Administrator response
Retry the operation to see if the problem persists.

DPWDS0646E

Failed to copy the data from the primary distributed session cache backing database to the secondary. (0x38a0a286)

Explanation
The DSC uses a backing SolidDB database to replicate session data for failover scenarios. The configuration tool failed to perform the initial copy of the data from the primary database to the secondary.

Administrator response
Ensure that the primary distributed session cache server is running and correctly configured as the primary node for replication.

DPWDS0647E

Failed to change the ownership of the backing database or configuration files. (0x38a0a287)

Explanation
The ownership of the DSC backing SolidDB database or configuration files could not be changed to the user and group ID specified in the template configuration file.

Administrator response
Retry the operation to see if the problem persists.

DPWDS0648E

Failed to send updates to the master Distributed Session Cache server. State *%d* with error *%d* '*%s*'. Attempting to recover. (0x38a0a288)

Explanation

When an isolated Replica Distribute Session Cache server reconnects with the Master it will send it's updates to the Master. This error message indicates that the send failed and an attempt is being made to recover automatically.

Administrator response

The server will attempt to recover. Monitor for additional message in case recovery is not successful. Ensure the network and all Distribute Session Cache servers are functioning correctly.

DPWDS0651W

The Distribute Session Cache server is waiting for the initial copy of the database to be send to it. (0x38a0a28b)

Explanation

The embedded SolidDB server is configured as a Secondary in a Highly Available pair and is waiting for the Primary in the pair to send the initial copy of the database.

Administrator response

If the copy does not occur then ensure the associated Distributed Session Cache servers are running so they can provide the database.

DPWDS0653W

The Distribute Session Cache server has applied the updated copy of database. (0x38a0a28d)

Explanation

The embedded SolidDB server has received a complete replacement copy of the database from the primary and is now using it.

Administrator response

No action is required.

DPWDS0654E

Failed to unregister this replica from the master database. (0x38a0a28e)

Explanation

While unconfiguring the node the tool was not able to unregister it from the master database.

Administrator response

If the master node will also be unconfigured you can ignore this error. If the master node is not running then start it and attempt to clear this issue by configuring and unconfiguring this node. The configure may experience an error as the node may have been left registered, but this can be ignored and the unconfigure should clear the issue.

DPWDS0655E

The tool was not able to create the tempory file '*%s*', error: '*%s*'. (0x38a0a28f)

Explanation
While unconfiguring the node the tool was not able to create a tempory file of SQL commands to unregister it from the master database.

Administrator response
If the master node will also be unconfigured you can ignore this error.

DPWDS0656W

Unable to connect to destination *%s*:*%d* (0x38a0a290)

Explanation
An error occurred when the client attempted to connect to the configured IP address and port.

Administrator response
Check the configured IP address and port to ensure that it is a valid and the destination server is running and listening.

DPWDS0657E

Both -K and -F option must be provided. (0x38a0a291)

Explanation
Either none, or only one, of -K and -F options were provided.

Administrator response
Rerun the command with the -K and -F options specified.

DPWDS0658E

Both -R and -Q option must be provided. (0x38a0a292)

Explanation
Either none, or only one, of -R and -Q options were provided.

Administrator response
Rerun the command with the -R and -Q options specified.

DPWDS0659E

It is not valid to provide the -b option with -n 1. (0x38a0a293)

Explanation
It is not valid for the first node to have a node before it.

Administrator response
Rerun the command without the -b option or change the -n option.

DPWDS0660E

You must provide the -b option when the -n option is not 1. (0x38a0a294)

Explanation
If the node being configured is not node 1, then the address and port of the node before it must be provided.

Administrator response
Rerun the command providing the -b option or change the -n option.

DPWDS0661E

It is not valid to provide the -a option with -n 4. (0x38a0a295)

Explanation
It is not valid for the last node to have a node after it.

Administrator response
Rerun the command without the -a option or change the -n option.

DPWDS0662E

The '*%s*' option value of '*%s*' is not valid. (0x38a0a296)

Explanation
The -b or -a option value must be of the form 'addr port'.

Administrator response
Rerun the command with a valid option value.

DPWDS0663W

Waiting for catchup before entering standby mode. (0x38a0a297)

Explanation
The DSC server is active and has just discovered it's sibling node has recovered. Before changing to standby mode it waits for the sibling to catchup with the lastest session changes.

Administrator response
This is likely expected behavior and no action is required.

DPWDS0664E

The node-number configuration value of '*%d*' is not valid. (0x38a0a298)

Explanation
The node-number configuration value must a value from 1 to 4.

Administrator response
Correct the configuration file value and Rerun the command.

DPWDS0665E

The node-number configuration value is not valid. (0x38a0a299)

Explanation
The node-number configuration value must a value from 1 to 4.

Administrator response
Correct the configuration file value and Rerun the command.

DPWDS0666E

The configuration settings node-before-port can not be set when the value of node-number is 1. (0x38a0a29a)

Explanation
It is not valid for the first node to have a node before it.

Administrator response
Remove the node-before-port setting and rerun the command.

DPWDS0667E

The configuration settings node-after-port can not be set when the value of node-number is 4. (0x38a0a29b)

Explanation
It is not valid for the last node to have a node after it.

Administrator response
Remove the node-after-port setting and rerun the command.

DPWDS0668E

Unable to read replicator protocol header from the remote node. (0x38a0a29c)

Explanation
The local node was unable to read the replicator protocol header.

Administrator response
Check the server on the other node, the configuration of the before and after nodes and the network setup.

DPWDS0669E

The replicator protocol header version *%d* received from the remote node is invalid. (0x38a0a29d)

Explanation
The version number read from the connection was not valid.

Administrator response
Ensure other applications are not incorrectly confgured to use the replicator port.

DPWDS0670E

The replicator protocol header operation *%d* received from the remote node is invalid. (0x38a0a29e)

Explanation
The operation number read from the connection was not valid.

Administrator response
Ensure other applications are not incorrectly confgured to use the replicator port.

DPWDS0671E

The replicator protocol header length *%d* received from the remote node is out of range. (0x38a0a29f)

Explanation
The length value read from the connection was out of range.

Administrator response
Ensure other applications are not incorrectly confgured to use the replicator port.

DPWDS0672E

Unable to read replicator protocol body (request) from the remote node. (0x38a0a2a0)

Explanation
The local node was unable to read the replicator protocol body (request).

Administrator response
Check the server on the other node, the configuration of the before and after nodes and the network setup.

DPWDS0673E

Unable to decode the replicator protocol body (request). (0x38a0a2a1)

Explanation
The request body received did not contain the correct data.

Administrator response
Ensure other applications are not incorrectly confgured to use the replicator port.

DPWDS0674E

The replicator protocol request node number *%d* is not valid. (0x38a0a2a2)

Explanation
The decoded request received contains a node number that is not valid.

Administrator response
Ensure other applications are not incorrectly confgured to use the replicator port.

DPWDS0675E

The replicator protocol request timeout value *%d* is not valid. (0x38a0a2a3)

Explanation
The decoded request received contains a timeout value that is not valid.

Administrator response
Ensure other applications are not incorrectly confgured to use the replicator port.

DPWDS0676E

Unable to write replicator protocol header to the remote node. (0x38a0a2a4)

Explanation
The local node was unable to write the replicator protocol header.

Administrator response
Check the server on the other node, the configuration of the before and after nodes and the network setup.

DPWDS0677E

Unable to write replicator protocol body (request) to the remote node. (0x38a0a2a5)

Explanation
The local node was unable to write the replicator protocol body (request).

Administrator response
Check the server on the other node, the configuration of the before and after nodes and the network setup.

DPWDS0678E

Unable to encode the replicator protocol body (response). (0x38a0a2a6)

Explanation
It is likely the process ran out of memory encoding the data to be send.

Administrator response
Ensure all memory has not been depleted.

DPWDS0679E

Unable to write replicator protocol body (response) to the remote node. (0x38a0a2a7)

Explanation
The local node was unable to write the replicator protocol body (response).

Administrator response
Check the server on the other node, the configuration of the before and after nodes and the network setup.

DPWDS0680E

Unable to read replicator protocol body (response) of length *%d* from the remote node. (0x38a0a2a8)

Explanation
The local node was unable to read the replicator protocol body (response).

Administrator response
Check the server on the other node, the configuration of the before and after nodes and the network setup.

DPWDS0681E

Unable to decode the replicator protocol body (response). (0x38a0a2a9)

Explanation
The request body received did not contain the correct data.

Administrator response
Ensure other applications are not incorrectly confgured to use the replicator port.

DPWDS0682E

Unable to encode the replicator protocol body (request). (0x38a0a2aa)

Explanation
It is likely the process ran out of memory encoding the data to be send.

Administrator response
Ensure all memory has not been depleted.

DPWDS0683W

This server node *%d*, has detected node *%d* has started with time offset *%d*. (0x38a0a2ab)

Explanation
This server has noticed it's neighbor node has started.

Administrator response
No action required.

DPWDS0684E

The replicator protocol response node number *%d* is not valid. (0x38a0a2ac)

Explanation
The decoded response received contains a node number that is not valid.

Administrator response
Ensure other applications are not incorrectly confgured to use the replicator port.

DPWDS0685E

Expecting to connect to node *%d*, but reported node is *%d*. (0x38a0a2ad)

Explanation
The neighbor node's reported node number is not the expected one.

Administrator response
Fix the neighbor node configuration, or this nodes configuration.

DPWDS0686E

Unable to set the trace level '*%s*'. Error *%d* (0x38a0a2ae)

Explanation
The internal trace API did not accept the trace level provided.

Administrator response
Ensure the trace level value in the configuration file is valid (0 -> 9).

DPWDS0750E

The administration interface of the distributed session cache server did not return all expected data. (0x38a0a2ee)

Explanation
Return data from a distributed session cache server administration operation was missing.

Administrator response
Ensure the correct version of the distributed session cache server and client is being used. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0751E

The administration interface of the distributed session cache server returned some unexpected data. (0x38a0a2ef)

Explanation
The return data from a distributed session cache server administration operation was of an unexpected format.

Administrator response
Ensure the correct version of the distributed session cache server and client is being used. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0752E

The *%s* operation of the distributed session cache server administration interface did not return all expected data: *%s*. (0x38a0a2f0)

Explanation
The indicated return data from a distributed session cache server administration operation is missing.

Administrator response
Ensure the correct version of the distributed session cache server and client is being used. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0753E

The *%s* operation of the distributed session cache server administration interface returned some data for the *%s* attribute which was not in the expected format. (0x38a0a2f1)

Explanation
The return data from a distributed session cache server administration operation was of an unexpected format.

Administrator response
Ensure the correct version of the distributed session cache server and client is being used. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0754E

An error occurred when attempting to communicate with the administration interface of the distributed session cache server using the URL *%s*: *%s* (0x*%x*). (0x38a0a2f2)

Explanation
An attempt was made to communicate with the administration interface of the distributed session cache server and a failure occurred within the underlying communications layer.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. Ensure the administration interface of the distributed session cache server is available and reachable. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0755E

The administration interface of the distributed session cache server could not be accessed. (0x38a0a2f3)

Explanation
An unsuccessful attempt has been made to communicate with the administration interface of the distributed session cache server.

Administrator response
Ensure the administration interface of the distributed session cache server is available and can be reached by the client. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWDS0762W

No replicas were found for the specified replica set. (0x38a0a2fa)

Explanation
A request was made to display a specified replica set, but no replicas are currently registered with the replica set.

Administrator response
No action is required, this is a status message.

DPWDS0766W

No sessions were found which match the specified search criteria. (0x38a0a2fe)

Explanation
A request was made to list sessions which match specified criteria, but no matching sessions were found.

Administrator response
No action is required, this is a status message.

DPWDS0767W

The '*%s*' instance is invalid. (0x38a0a2ff)

Explanation
The specified instance, supplied for an administration task, was invalid.

Administrator response
Review the format of the command text to ensure all parameters are correct.

DPWDS0768E

The administration operation is not permitted on the interface which was used to contact the distributed session cache server. (0x38a0a300)

Explanation
The Distributed Session Cache server can be configured to restrict access for administration commands to a subset of the network interfaces it is configured to use. The administration request was not received on one of the permitted interfaces.

Administrator response
Change the interface of the Distributed Session Cache server being addressed, or adjust the configuration of the Distributed Session Cache server.

DPWDS0769E

The administration operation from '*%s*' is not permitted on the interface '*%s*'. (0x38a0a301)

Explanation
The Distributed Session Cache server can be configured to restrict access for administration commands to a subset of the network interfaces it is configured to use. The administration request was not received on one of the permitted interfaces.

Administrator response
Change the interface of the Distributed Session Cache server being addressed, or adjust the configuration of the Distributed Session Cache server.

DPWDS0770E

Function call, *func*, failed error: *error code error text*. (0x38a0a302)

Explanation
The specified GSKit function failed while setting up for SSL connections to the Distributed Session Cache server. Or perhaps the initial handshake failed due to invalid certificates or the client simply closed the connection abruptly.

Administrator response
Examine the error text to gain insight on the problem.

DPWIV0151E

Could not initialize serviceability component (*%s*, 0x*%8.8lx*) (0x38ad5097)

Explanation
WebSEAL was unable to register the service component with the serviceibility subsystem or register an in memory catalog. The error code output in the message will give finer details as to why. Most likely it will be due to a lack of memory or a design flaw.

Administrator response
Check memory ulimit on UNIX platforms, and available memory on all types of platforms. Increase available memory to the WebSEAL process if applicable.

DPWIV0152E

Could not register serviceability message table (*%s*, 0x*%8.8lx*) (0x38ad5098)

Explanation
WebSEAL was unable to register an in memory catalog. The error code output in the message will give finer details as to why. Most likely it will be due to a lack of memory or a program design flaw.

Administrator response
Check memory ulimit on UNIX platforms, and available memory on all types of platforms. Increase available memory to the WebSEAL process if applicable.

DPWIV0155E

Configuration stanza missing (*%s*) (0x38ad509b)

Explanation
A necessary configuration file stanza was not found.

Administrator response
Make sure the name of the stanza is spelled correctly in the configuration file.

DPWIV0172E

Unexpected end of byte stream (0x38ad50ac)

Explanation
Message is not used. This is purely used as in internal status code.

Administrator response
No action is required

DPWIV0173E

Could not stop background process (errno *%d*) (0x38ad50ad)

Explanation
Message is not used. This is purely used as in internal status code.

Administrator response
No action is required

DPWIV0175E

Could not open a pipe (errno *%d*) (0x38ad50af)

Explanation
WebSEAL failed to create a pipe for communicating to a child CGI process of WebSEAL. The meaning of the errno value can typically be found in /usr/include/sys/errno.h and will give finer details on the cause.

Administrator response
Lookup the errno in /usr/include/sys/errno.h for the cause.

DPWIV0176E

Could not fork (errno *%d*) (0x38ad50b0)

Explanation
WebSEAL failed for fork so that it could execute a CGI. This could be due to insufficent operating system resources.

Administrator response
Lookup the errno in /usr/include/sys/errno.h for the cause.

DPWIV0178E

Operation forbidden by the operating system (0x38ad50b2)

Explanation
Message is not used. This is purely used as in internal status code.

Administrator response
No action is required

DPWIV0179E

Unknown user (0x38ad50b3)

Explanation
Message is not used. This is purely used as in internal status code.

Administrator response
No action is required

DPWIV0194E

Could not become background process because pipe failed. (*%d*) (0x38ad50c2)

Explanation
The pipe() function failed. This error value can typically be found in /usr/include/sys/errno.h and will give finer details on the cause.

Administrator response
Make sure server has the permission to create interprocess pipes.

DPWIV0195E

Could not become background process because fork failed. (*%d*) (0x38ad50c3)

Explanation
The fork() function failed. This function fails when insufficient memory is available, or machine process limit is reached. The error value can typically be found in /usr/include/sys/errno.h and will give finer details on the cause.

Administrator response
Make sure server machine resources are available.

DPWIV0196W

Could not start background process: *%s* (0x38ad50c4)

Explanation
This is due to the failure to execute a CGI program. Either the program is not executable, or system resources are not available to run the program.

Administrator response
WebSEAL could not successfully start a child process. Most likely the program does not exist or is not executable.

DPWIV0197E

Error in stanza file *%s* on line *%d*: *%s* (0x38ad50c5)

Explanation
An error occurred while attempting to read data from a stanza file.

Administrator response
Correct the problem in the stanza file.

DPWIV0198E

Error in stanza file. (0x38ad50c6)

Explanation
An error occurred while attempting to read data from a stanza f ile. Log files will contain more information.

Administrator response
Examine log files to identify the error in the stanza file.

DPWIV0199E

An unexpected exception occurred at line *%s*:*%d* (0x38ad50c7)

Explanation
An internal error occurred.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWIV0200E

An unexpected exception occurred (0x38ad50c8)

Explanation
An internal error occurred.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWIV0201E

The azn-api function '*%s*' returned 0x*%lx* (0x38ad50c9)

Explanation
An unexpected azn-api function failure occurred.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWIV0202E

An azn-api function unexpectedly failed (0x38ad50ca)

Explanation
An unexpected azn-api function failure occurred.

Administrator response
Check log files for additional details. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWIV0203E

Additional information from azn-api: *%s* = *%s* (0x38ad50cb)

Explanation
An azn-api error occurred, and this message contains more detail about the error.

Administrator response
Check log files for additional details. The exact action to take depends on the context of the error.

DPWIV0204E

An invalid permission string, *%s*, was located for the *%s* method within the *%s* stanza. (0x38ad50cc)

Explanation
A configured permission string is invalid and not recognized by the IBM Security Verify Access Authorization engine.

Administrator response
Correct the specified permission string within the configuration file and ensure that the permission string is valid.

DPWIV0205E

The system function '*%s*' returned 0x*%lx*. (0x38ad50cd)

Explanation
An unexpected system function failure occurred.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWIV0465E

Error msg returned from stanza function: (*%s*).For entry: *%s*/*%s*. (0x38ad51d1)

Explanation
The migrate tool has had an error while manipulating a configuration file full of stanzas and entries. The bracketted error string within the error message gives more detail.

Administrator response
Correct the error specified by the bracketted error string.

DPWIV0466E

Unsupported configuration item type (*%d*) (0x38ad51d2)

Explanation
The migrate tool has had an unrecoverable internal error. It has encountered an unknown entry type.

Administrator response
Contact technical support, this is an unexpected internal error.

DPWIV0467E

Could not create new pthread key (*%d*) (0x38ad51d3)

Explanation
See message.

Administrator response
Contact product support.

DPWIV0468E

Could not create default pthread attributes. (0x38ad51d4)

Explanation
WebSEAL failed to create pthread attributes.

Administrator response
Check available memory for the process.

DPWIV0469E

pthread_attr_setdetachstate() failed (*%d*) (0x38ad51d5)

Explanation
This message indicates a serious internal error involving the threading library.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWIV0470E

Could not destroy pthread attributes. (0x38ad51d6)

Explanation
WebSEAL failed to delete pthread attributes.

Administrator response
Check available memory for the process.

DPWIV0471E

pthread_rwlock_init() failed (*%d*) (0x38ad51d7)

Explanation
This message indicates a serious internal error involving the threading library.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWIV0756E

Could not deallocate file descriptor *%d*. (errno: *%d*) (0x38ad52f4)

Explanation
Unable to close unused file handles in child CGI process.

Administrator response
This is unexpected and if it persists should be reported to technical support. The error number in this message can be looked up in /usr/include/sys/errno.h for additional details on the cause.

DPWIV0759W

Directory (*%s*) could not be created. (Errno = *%d*) (0x38ad52f7)

Explanation
Unable to create the directory specified in the error message. The directory is created to store content from a PUT HTTP request.

Administrator response
This may be due to lack of disk space or permissions on parent directories. For more details on the cause lookup the errno in /usr/include/sys/errno.h

DPWIV0760W

The specified path is invalid. (*%s*) (0x38ad52f8)

Explanation
The path specified to the DELETE HTTP request is not valid on the local junction.

Administrator response
Correct the HTTP URL to contain a valid path on the local junction.

DPWIV0761W

The file (*%s*) attributes cannot be obtained. (Errno = *%d*) (0x38ad52f9)

Explanation
Unable to fetch information on the file specified in the error message. This file is possibly going to be the target of a HTTP PUT request.

Administrator response
This may be due to permissions on the file. For more details on the cause lookup the errno in /usr/include/sys/errno.h

DPWIV0762W

Can't delete non-empty directory (*%s*) (0x38ad52fa)

Explanation
This is only used as an internal status. It occurs either during a PUT or DELETE HTTP request when the replaced or deleted directory is not empty.

Administrator response
Don't PUT or DELETE on this directory until it is empty.

DPWIV0763W

Failed to delete file (*%s*) (Errno = *%d*) (0x38ad52fb)

Explanation
A HTTP PUT or DELETE request is either replacing or deleting a file on a local junction. This failed.

Administrator response
This may be due to permissions on the file. For more details on the cause lookup the errno in /usr/include/sys/errno.h

DPWIV0766W

Write to file (*%s*) failed. (Errno = *%d*) (0x38ad52fe)

Explanation
The server failed to write to an open file.

Administrator response
This may be due to permissions on the file or because there is insufficient room in the file system. For more details on the cause lookup the errno in /usr/include/sys/errno.h

DPWIV0767E

List of directory (*%s*) failed. (Errno = *%d*) (0x38ad52ff)

Explanation
A system error occurred while trying to read a directory's contents.

Administrator response
Examine the directory specified and attempt to determine and correct the problem that caused the system error.

DPWIV0768E

Could not copy file (*%s*, *%s*, *%d*) (0x38ad5300)

Explanation
Unable to copy the file to the destination. The source of this error depends on the context of the operation that failed.

Administrator response
This may be due to permissions on the source or destination file or their directories. For more details on the cause lookup the errno in /usr/include/sys/errno.h

DPWIV0769W

Read from file (*%s*) failed. (Errno = *%d*) (0x38ad5301)

Explanation
The server was unable to read from the file specified.

Administrator response
This may be due to permissions on the file. For more details on the cause lookup the errno in /usr/include/sys/errno.h

DPWIV0770W

Could not close file (*%s*). (Errno = *%d*) (0x38ad5302)

Explanation
The server was unable to close an open file.

Administrator response
This may be due to insufficient file system space. For more details on the cause lookup the errno in /usr/include/sys/errno.h

DPWIV1060E

Could not read from socket (*%d*) (0x38ad5424)

Explanation
A timeout occurred when WebSEAL was attempting to read from a socket.

Administrator response
No action required.

DPWIV1061E

Could not write to socket (*%d*) (0x38ad5425)

Explanation
An unexpected error occurred while writing to a socket.

Administrator response
No action required.

DPWIV1062E

Unable to resolve IP address for hostname '*%s*' (Error *%d*: *%s*) (0x38ad5426)

Explanation
An attempt to resolve a hostname to an IP address failed. There are many possible reasons for failure, and the system error code and error text can be used to isolate the problem.

Administrator response
The source for this error depends on the exact context of the error. Administrators should verify that the hostname specified is correct, and that DNS can resolve the hostname properly. Check the DNS

configuration the server logging this error. The system error code and error text may provide more detail about the problem.

DPWIV1063E

Unable to resolve IP address for hostname. (0x38ad5427)

Explanation
An attempt to resolve a hostname to an IP address failed.

Administrator response
Check the logs for additional error messages. Other messages will contain more detail about the problem.

DPWIV1064E

Could not set socket options (*%d*) (0x38ad5428)

Explanation
There was a failure in setting socket options.

Administrator response
Check that WebSEAL has not exceeded system resource limits. For more details on the cause, lookup the errno in /usr/include/sys/errno.h.

DPWIV1065E

Could not get socket options (*%d*) (0x38ad5429)

Explanation
There was a failure trying to get socket options.

Administrator response
Check that WebSEAL has not exceeded system resource limits. For more details on the cause, look up the errno in /usr/include/sys/errno.h.

DPWIV1066E

Could not obtain the socket details: ERRNO = *%d* (0x38ad542a)

Explanation
WebSEAL failed to obtain the connection details for a connected socket.

Administrator response
Check WebSEAL has not exceeded system resource limits. For more details on the cause lookup the errno in /usr/include/sys/errno.h.

DPWIV1200E

Could not write to SSL connection (0x38ad54b0)

Explanation
This is used only as an internal error code. It should not be visible.

Administrator response
No action required.

DPWIV1201E

Could not read from SSL connection (0x38ad54b1)

Explanation
This is used only as an internal error code. It should not be visible.

Administrator response
No action required.

DPWIV1203E

Could not create new SSL connection (0x38ad54b3)

Explanation
This is used only as an internal error code. It should not be visible.

Administrator response
No action required.

DPWIV1210W

Function call, *func*, failed error: *error code error text*. (0x38ad54ba)

Explanation
The specified GSKit function failed while setting up for SSL connections to junctions or from browsers. Or perhaps the initial handshake failed due to invalid certificates or the browser simply closed the connection abruptly.

Administrator response
Examine the error text to gain insite on the problem. Typical problems might be that the PKCS#11 library is incorrectly specified, or the PKCS#11 token or token password is incorrect, or the PKCS#11 token is not setup.

DPWIV1212W

No server DN is defined for '*%s*'. The junctioned server DN verification is not performed. (0x38ad54bc)

Explanation
No server DN is defined in the junction database. DN verification against server certificate will be ignored.

Administrator response
Recreate the junction specifying the junctioned servers certificate DN or turn off mutual authentication on the junction.

DPWIV1213E

Could not get junctioned server (*%s*) certificate (0x38ad54bd)

Explanation
The SSL connection to the specified junction did not have a certificate presented from the junctioned server.

Administrator response
Check the server side's certificate has been configured.

DPWIV1214E

Could not get junctioned server (*%s*) certificate's DN (0x38ad54be)

Explanation
See message.

Administrator response
Check the junctioned server is presenting a certificate that has a printable DN present

DPWIV1215E

Error in junctioned server DN verification (*%s*) (0x38ad54bf)

Explanation
The DN in the certificate presented by the junctioned server contains a DN that does not match the one specified when the junction was created.

Administrator response
Check the junctioned server's DN with the one specified during the junction creation.

DPWIV1216E

The junctioned server presented an invalid certificate. (0x38ad54c0)

Explanation
The certificate presented by the backend server failed validation.

Administrator response
Install the CA root certificate in the WebSEAL certificate key database.

DPWIV1217W

SSL connection error. (0x38ad54c1)

Explanation
This is an internal error status not visible. Error code returned when an ssl connection failed

Administrator response
Check logs for more details.

DPWIV1218E

Error in junctioned server DN verification. (0x38ad54c2)

Explanation
The DN specified when the junction was created did not match the DN in the certificate presented by the server.

Administrator response
Check the junctioned server's DN with the one specified during the junction creation.

DPWIV1219E

An SSL toolkit failure occurred while calling *%s*. Error: *%s*. (0x38ad54c3)

Explanation
An internal SSL error occurred.

Administrator response
The action to correct this problem depends on details in the error message.

DPWIV1220E

An ICC toolkit failure occurred. (0x38ad54c4)

Explanation
An internal ICC error occurred.

Administrator response
This error is always accompanied with a serviceability log error message detailing the ICC routine which failed and the reason for the failure. The action to correct this problem depends on details in the serviceability log message. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWIV1221E

An ICC toolkit failure occurred while calling *%s*. Error: *%s*. (0x38ad54c5)

Explanation
An internal ICC error occurred.

Administrator response
The action to correct this problem depends on details in the error message. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWIV1222E

An ICC toolkit failure occurred while calling *%s*. No further details are known. (0x38ad54c6)

Explanation
An internal ICC error occurred. However, no details about the error we able to be determined beyond the name of the ICC function which failed.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWIV1223E

HTTP/2 could not be selected during the TLS negotiation with junction server '*%s*'. (0x38ad54c7)

Explanation
The Junction is configured for HTTP/2 but the TLS connection to the specified junction server could not negotiate HTTP/2 protocol.

Administrator response
Ensure the junctioned HTTP server has HTTP/2 enabled for TLS connections.

DPWIV1224E

The configured value for http2-max-connections has been exceeded '*%llu*' times for interface '*%s*'. (0x38ad54c8)

Explanation
The configuration setting, http2-max-connections, limits the number of simultaneous HTTP/2 connections. This error is reported when this limit has been exceeded. The new connection that triggered this event will be abruptly closed.

Administrator response
Increase the value for http2-max-connections or reduce the HTTP/2 load.

DPWIV1225E

WebSEAL is not able to negotiate the HTTP/2 protocol with the server '*%s*'. (0x38ad54c9)

Explanation
WebSEAL is configured to use HTTP/2 protocol with the Junction or Proxy server, but the server did not respond correctly to the expected HTTP/2 protocol negotiation sequence. For HTTP/2 cleartext TCP connections the server must support the direct (prior knowledge) method. For HTTP/2 TLS the server must support the application-layer protocol negotiation (ALPN) method.

Administrator response
Ensure the junction or proxy server has the HTTP/2 protocol enabled for the connection.

DPWIV1226E

HTTP/2 could not be selected during the TLS negotiation with the junctioned server. (0x38ad54ca)

Explanation
The Junction is configured for HTTP/2 but the TLS connection to the specified junction server could not negotiate HTTP/2 protocol.

Administrator response
Ensure the junctioned HTTP server has HTTP/2 enabled for TLS connections.

DPWIV1350E

An error occurred when loading a shared library. (0x38ad5546)

Explanation
This message indicates that a problem occurred when loading a shared library. Other log messages will have additional information.

Administrator response
Examine log files for more detailed error messages.

DPWIV1351E

The shared library '*%s*' could not be loaded because of system error code *%d*. System error text: *%s*. (0x38ad5547)

Explanation
Opening a shared library failed. The shared library may not exist, permissions on the library may be incorrect, or it may contain other errors that prevent it from loading.

Administrator response
Examine the system error code and text to determine the nature of the problem. Make sure the shared library exists and is readable. Make sure all of the symbols in the library can be resolved.

DPWIV1352E

The symbol '*%s*' in the shared library '*%s*' could not be loaded because of system error code *%d*. System error text: *%s*. (0x38ad5548)

Explanation
Resolving a symbol from a shared library failed after the library was initially loaded. The symbol may not exist in the library or other symbols on which this symbol depends might not be available.

Administrator response
Examine the system error code and text to determine the nature of the problem. Make sure the shared library implements and exports the function being resolved. Make sure all of the symbols required by the shared library can be resolved.

DPWNS0150E

Process can't access directory '*%s*', error: 0x*%8.8lx* (0x38b9a096)

Explanation
The process is trying to change it's working directory

Administrator response
Check the UID running the process has the correct permissions

DPWNS0165E

The certificate revocation check result was undetermined. The subject issuer is '*%s*'. (0x38b9a0a5)

Explanation
An OCSP CRL check could not determine if the certificate is revoked. This is usually due to an unresponsive OCSP responder.

Administrator response
Check the OCSP responder is operating.

DPWNS0166E

The junction server, '*%s*', certificate revocation check result was undetermined. The subject issuer is '*%s*'. (0x38b9a0a6)

Explanation
An OCSP CRL check could not determine if the junctions certificate is revoked. This is usually due to an unresponsive OCSP responder.

Administrator response
Check the OCSP responder is operating.

DPWNS0301W

Junction server '*%s*:*%d*' is renegotiating SSL sessions at a rate of *%ld* per minute. (0x38b9a12d)

Explanation
The SSL server junctioned behind WebSEAL is forcing WebSEAL to renegotiate new SSL Sessions at a rate higher than specified by [junction] jct-ssl-reneg-warning-rate.

Administrator response
Ensure the junctioned SSL server has SSL session caching enabled and functioning correctly, or check that any intervening load balancers are not causing this issue by forcing WebSEAL to alternate between two SSL servers.

DPWNS0450E

The pattern '*%s*' is not a valid MIME type matching pattern. (0x38b9a1c2)

Explanation
MIME type patterns must be either exact (type/subtype), subtype wild cards (type/*), or type and subtype wildcards (*/*).

Administrator response
Make sure the mime type specified is valid.

DPWNS0451E

Invalid MIME matching pattern. (0x38b9a1c3)

Explanation
Mime type patterns must be either exact (type/subtype), subtype wild cards (type/*), or type and subtype wildcards (*/*).

Administrator response
Make sure the mime type specified is valid.

DPWNS0452E

Invalid MIME type '*%s*'. (0x38b9a1c4)

Explanation
An attempt was made to lookup a match for a MIME type that did not contain a '/'.

Administrator response
Check the MIME type configuration of your servers to verify that they are returning valid MIME types for all documents.

DPWNS0453E

Invalid MIME type. (0x38b9a1c5)

Explanation
An attempt was made to lookup a match for a MIME type that did not contain a '/'.

Administrator response
Check the MIME type configuration of your servers to verify that they are returning valid MIME types for all documents.

DPWNS0600E

Compression initialization failed with error code *%d* (*%s*). (0x38b9a258)

Explanation
Initialization of compression failed. This error should never occur.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWNS0601E

Compression failed with error code *%d* (*%s*). (0x38b9a259)

Explanation
Compression of a document failed. This error should never occur.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWNS0602E

Completion of compression failed with error code *%d* (*%s*). (0x38b9a25a)

Explanation
The completion of document compression failed. This error should never occur.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWNS0603E

An error occurred during document compression. (0x38b9a25b)

Explanation
This error is returned when a problem was encountered during document compression.

Administrator response
Examine log files for additional information.

DPWNS0750E

The HTTP header key '*%d*' is invalid. (0x38b9a2ee)

Explanation
This message indicates an internal error. An attempt was made to reference an HTTP header using an invalid key.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWNS0900E

The client certificate EAI request failed: *%s* (0x*%lx*) (0x38b9a384)

Explanation
This error is returned when the EAI request which has been generated by WebSEAL does not return a valid HTTP response.

Administrator response
Examine log files for additional information.

DPWNS0901E

No EAI authentication data was provided with the EAI response. (0x38b9a385)

Explanation
This error is returned when the EAI response lacks all of the configured EAI authentication headers.

Administrator response
Examine the log files for additional information. Check the EAI application to ensure that valid authentication headers are being set.

DPWNS0902E

Attempted OAuth authentication has failed. (0x38b9a386)

Explanation
This error is returned when an attempt to perform an OAuth authentication has failed. A typical reason for this is providing an access token that has expired.

Administrator response
Examine the log files for additional information. Also examine the OAuth server log files.

DPWNS0903E

Failed to find user identity attribute named *%s* in RSTR returned from OAuth server. (0x38b9a387)

Explanation
This error is returned when a required value is not returned from a call to the OAuth server. The webseald.conf file has an entry named user-identity-attribute in the oauth stanza. The value of this entry, username by default, provides the name of an attribute that must be present in the RSTR returned by the OAuth server. The value of that entry is used when creating a credential. That entry is not found.

Administrator response
Examine the log files for additional information. Make sure that the user-identity-attribute entry in the oauth stanza of webseald.conf names the attribute that is returned by the OAuth server.

DPWNS1050E

Session cache creation failed. (0x38b9a41a)

Explanation
This message can indicate a failure due to system resource limitations.

Administrator response
Check available system memory and process resource usage limits.

DPWNS1051E

Addition or update of a session cache entry failed. (0x38b9a41b)

Explanation
This message indicates an internal error.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWNS1052W

A session cache entry was not found. (0x38b9a41c)

Explanation
This message indicates that an expected session cache entry was not found.

Administrator response
No action is necessary unless other problems are experienced.

DPWNS1053E

Session owner tracking is not supported in this configuration. (0x38b9a41d)

Explanation
This message indicates that an attempt was made to get a list of the sessions associated with a user when session owner tracking was not enabled.

Administrator response
Refer to the WebSEAL Administration Guide for instructions on how to enable tracking of session owners.

DPWNS1054E

Invalid session ID. (0x38b9a41e)

Explanation
This message indicates that an invalid session ID was encountered when trying to generate an internal representation of the ID. The most likely cause of this error is a malformed session cookie from a browser.

Administrator response
No action is necessary. A new session and session cookie is created as needed.

DPWNS1055E

You are already logged in from another client. You can either wait for the other login to end or contact your local support personnel to cancel the existing login. (0x38b9a41f)

Explanation
This message indicates that the maximum number of concurrent sessions for the user has been reached and no new sessions will be permitted until one of the existing sessions has ended.

Administrator response
Refer to the WebSEAL Administration Guide discussion of concurrent login sessions for more complete information.

DPWNS1056W

You are already logged in from another client. Do you want to terminate your existing login or cancel this new login request? (0x38b9a420)

Explanation

This message indicates that the maximum number of concurrent sessions for the user has been reached, and that the user can choose to replace an existing session.

Administrator response

The action depends on the reason for the previous session. If the user closed their browser without properly logging out or does not need their old session, they can press the 'Terminate existing login' button. If the user does need their old session, they should press the 'Cancel this new login' button.

DPWNS1057E

Unable to intialize the distributed session API (error code 0x*%08lx*) (0x38b9a421)

Explanation

Initialization of the distributed session API failed. This error should never occur. The error code in the message might reveal more information about the problem.

Administrator response

Look up the error code included in the message in the IBM Security Verify Access for Web Troubleshooting Guide.

DPWNS1058E

Unable to join the replica set '*%s*' (error code 0x*%08lx*) (0x38b9a422)

Explanation

The WebSEAL server attempted to join a particular replica set but the operation failed. The SMS might not be available, or may have prevented the WebSEAL server from joining the replica set for some reason.

Administrator response

Make sure the correct protocol, host name, and port for the SMS in the WebSEAL configuration file are correct. Make sure the SMS server is running and can be reached from the WebSEAL server machine. Make sure the SMS server is configured to host the specified replica set. Check the log file for additional errors. If necessary, look up the error code from the message in the IBM Security Verify Access for Web Troubleshooting Guide for additional troubleshooting steps.

DPWNS1059E

Unable to shut down the distributed session API (error code 0x*%08lx*) (0x38b9a423)

Explanation

Shutdown of the distributed session API failed. This error should never occur. The error code in the message might reveal more information about the problem.

Administrator response

Look up the error code included in the message in the IBM Security Verify Access for Web Troubleshooting Guide.

DPWNS1060E

Unable to leave the replica set '*%s*' (error code 0x*%08lx*) (0x38b9a424)

Explanation
The WebSEAL server attempted to leave a particular replica set but the operation failed. The SMS might not be available or there might have been another problem when leaving the replica set.

Administrator response
Look up the error code included in the message in the IBM Security Verify Access for Web Troubleshooting Guide.

DPWNS1061E

An attempt to create a session failed with error code 0x*%08lx*. (0x38b9a425)

Explanation
An attempt to create a session at the SMS failed.

Administrator response
Repeat the operation. If the problem continues to occur, look up the error code included in the message in the IBM Security Verify Access for Web Troubleshooting Guide. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWNS1062E

An attempt to update a session failed with error code 0x*%08lx*. (0x38b9a426)

Explanation
An attempt to update a session at the SMS failed.

Administrator response
Repeat the operation. If the problem continues to occur, look up the error code included in the message in the IBM Security Verify Access for Web Troubleshooting Guide. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWNS1063E

An attempt to delete a session failed with error code 0x*%08lx*. (0x38b9a427)

Explanation
An attempt to delete a session at the SMS failed.

Administrator response
Repeat the operation. If the problem continues to occur, look up the error code included in the message in the IBM Security Verify Access for Web Troubleshooting Guide. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWNS1064E

Unknown replica set '*%s*' (0x38b9a428)

Explanation
An attempt was made to locate a replica set that was not configured.

Administrator response
Check that the replica set requested is included in the WebSEAL configuration file as a replica set that the WebSEAL server should join.

DPWNS1065E

Unknown replica set. (0x38b9a429)

Explanation
An attempt was made to locate a replica set that was not configured.

Administrator response
Check that the replica set requested is included in the WebSEAL configuration file as a replica set that the WebSEAL server should join.

DPWNS1066E

An error with code 0x*%08lx* occurred when decoding a session from the SMS. (0x38b9a42a)

Explanation
An attempt to decode a session from the SMS failed.

Administrator response
Look up the error code included in the message in the IBM Security Verify Access for Web Troubleshooting Guide.

DPWNS1067E

An attempt to generate a new external session ID failed with error code 0x*%08lx*. (0x38b9a42b)

Explanation
An attempt to generate a new external session ID for a session failed.

Administrator response
Repeat the operation. If the problem continues to occur, look up the error code included in the message in the IBM Security Verify Access for Web Troubleshooting Guide. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWNS1068E

An attempt to register an authentication failure for user '*%s*' failed with status code 0x*%08lx*. (0x38b9a42c)

Explanation
An attempt to notify the SMS of an authentication failure was unsuccessful.

Administrator response
Check the log file for additional errors. If necessary, look up the error code from the message in the IBM Security Verify Access for Web Troubleshooting Guide for additional troubleshooting steps.

DPWNS1070E

Session version mismatch while deserializing session data. (0x38b9a42e)

Explanation
WebSEAL attempted to deserialize session data but encountered an invalid session version. This indicates that the session was not compatible with the WebSEAL server that generated this error. The session was discarded.

Administrator response
No action is necessary. A new session will be created as needed. Refer to the documentation for the server that generated the invalid session version for information on compatibility with the WebSEAL server that generated this error.

DPWNS1071E

The max-concurrent-web-sessions policy value of '*%d*' is invalid. (0x38b9a42f)

Explanation
The max-concurrent-web-sessions policy returned from the IBM Security Verify Access Runtime had an unexpected value. A default value of 'unlimited' has been assumed.

Administrator response
Reset the max-concurrent-web-sessions policy for the user. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWNS1072W

WebSEAL received notification that the distributed session cache for replica-set '*%s*' was cleared. All local references to sessions are being discarded to synchronize the local session cache with the distributed session cache. (0x38b9a430)

Explanation
The DSC server notified the WebSEAL server that the distributed session cache was lost. Any sessions remaining on the WebSEAL server are no longer valid and will be removed. This message will also be displayed when the WebSEAL server first regains contact with the DSC server after WebSEAL is restarted.

Administrator response
No action is necessary.

DPWNS1074E

The single sign-off attempt for the user '*%s*' failed because the single sign-off resource is unavailable. (0x38b9a432)

Explanation
The single sign-off attempt failed because the configured single sign-off resource is not accessible by WebSEAL.

Administrator response
Check that the configured single sign-off resource URI points to a resource on a junction which is accessible by WebSEAL.

DPWNS1075E

The single sign-off attempt to *%s* for user '*%s*' failed because the configured single sign-off resource is not responding. (0x38b9a433)

Explanation
A single sign-off request was sent to the configured single sign-off resource but no response was received.

Administrator response
Check that the configured single sign-off application is running and functioning correctly.

DPWNS1076E

The single sign-off attempt to *%s* for user '*%s*' failed because the configured single sign-off resource returned a response with the HTTP status code *%d*. (0x38b9a434)

Explanation
An unexpected response was received from the configured single sign-off resource. WebSEAL expects a response with the HTTP status code 200.

Administrator response
Check that the configured single sign-off application is running and functioning correctly.

DPWNS1200W

The application server you are accessing has been taken offline by the system administrator. (0x38b9a4b0)

Explanation
The application server being accessed has been taken offline or throttled by the system administrator.

Administrator response
Try again at a later time or contact the system administrator for more information.

DPWNS1201E

The server is temporarily unable to service your request. Try again later. (0x38b9a4b1)

Explanation
The WebSEAL server is unable to service a request because a needed resource is unavailable.

Administrator response
The WebSEAL server log file will have more detailed information about why the WebSEAL server is unable to service the request. Check the WebSEAL server log file and correct the problem.

DPWNS1202E

An error occurred processing a HTTP transformation. (0x38b9a4b2)

Explanation
The WebSEAL server is unable to service a request because a HTTP transformation rule caused an error.

Administrator response
The WebSEAL server log file will have more detailed information about why the HTTP transformation failed. Check the WebSEAL server log file and correct the HTTP transformation rule.

DPWNS1203E

An invalid XML message document was used as part of a HTTP transformation operation. (0x38b9a4b3)

Explanation
The WebSEAL server is unable to service a request because an invalid XML message document was used as part of a HTTP transformation operation.

Administrator response
The WebSEAL server log file will have more detailed information about the XML object used. Check the WebSEAL server log file and correct the HTTP transformation rule.

DPWNS1204E

The XML element *%s* was missing from the document generated by a HTTP transformation operation. (0x38b9a4b4)

Explanation
The WebSEAL server is unable to service a request because an expected XML element was missing from the output document of a HTTP transformation operation.

Administrator response
Correct the HTTP transformation rule to ensure the rule includes all required elements.

DPWNS1205E

The XML attribute *%s* was missing from the *%s* element for the document generated by a HTTP transformation operation. (0x38b9a4b5)

Explanation
The WebSEAL server is unable to service a request because an expected XML attribute was missing from the output document of a HTTP transformation operation.

Administrator response
Correct the HTTP transformation rule to ensure the rule includes all required elements.

DPWNS1206E

The XML element *%s* was missing from the request change document generated by a HTTP transformation operation. (0x38b9a4b6)

Explanation

The WebSEAL server is unable to service a request because an expected XML element was missing from the request change document as part of a HTTP transformation operation.

Administrator response

Correct the HTTP transformation rule to ensure the rule includes all required elements.

DPWNS1207E

The XML element *%s* was missing from the response change document generated by a HTTP transformation operation. (0x38b9a4b7)

Explanation

The WebSEAL server is usable to service a request because an expected XML element was missing from the response change document as part of a HTTP transformation operation.

Administrator response

Correct the HTTP transformation rule to ensure the rule includes all required elements.

DPWNS1208E

The action attribute *%s* is unknown and therefore cannot be used by a HTTP transformation operation. (0x38b9a4b8)

Explanation

The WebSEAL server is unable to service a request because an unexpected action attribute was found as part of a HTTP transformation operation.

Administrator response

Correct the HTTP transformation rule to ensure the rule outputs supported actions.

DPWNS1209W

A configuration entry for the resource *%s* was not defined in the http-transformation stanza of the WebSEAL configuration file and therefore HTTP transformation cannot take place. (0x38b9a4b9)

Explanation

A HTTPTransformation resource was defined as an extended attribute on a POP but the WebSEAL configuration does not include a transformation rule for this resource.

Administrator response

Correct the WebSEAL configuration or the POP HTTPTransformation attribute to ensure the resource references an appropriate transformation rule.

DPWNS1210E

The cookie attribute *%s* is unknown and therefore cannot be used by a HTTP transformation operation. (0x38b9a4ba)

Explanation
The WebSEAL server is unable to service a request because an unexpected cookie attribute was found as part of a HTTP transformation operation.

Administrator response
Correct the HTTP transformation rule so that it does not reference unsupported cookie attributes.

DPWNS1211W

The cookie *%s* already exists in the HTTP message and as such it cannot be added by the transformation rule. (0x38b9a4bb)

Explanation
The WebSEAL server is unable to add a cookie to a HTTP message as it already exists in the HTTP message being transformed.

Administrator response
Modify the HTTP transformation so that it either checks for the existence of the cookie before adding the new cookie, or specifies the update action so that the cookie is updated.

DPWNS1212W

The authentication challenge type rules could not be applied because WebSEAL received a request without the User-Agent HTTP header. (0x38b9a4bc)

Explanation
A client which did not present a User Agent header in their request has made a request to authenticate with WebSEAL. WebSEAL was unable to determine the authentication challenge type for this request.

Administrator response
No action required.

DPWNS1350W

Failed to load ARM library '*%s*': error code *%d*: error message '*%s*'. ARM support will be disabled. (0x38b9a546)

Explanation
WebSEAL attempted to dynamically load the ARM shared library and failed.

Administrator response
Check the shared library name is correct and present on the system. Refer to the error message for more specific information. The shared library name is specified by the library entry under the [arm] stanza. If loading the ARM library is not desired set enable = no under the [arm] stanza.

DPWNS1351W

ARM library is missing function '*%s*': error code *%d*: error message '*%s*'. ARM support will be disabled. (0x38b9a547)

Explanation
WebSEAL dynamically loaded the ARM shared library and can not find a required function in it.

Administrator response
Check the shared library name is correct. Refer to the error message for more specific information. The shared library name is specified by the library entry under the [arm] stanza.

DPWNS1352W

Failed to register the WebSEAL application with ARM: error code *%d*: error message '*%s*'. ARM support will be disabled. (0x38b9a548)

Explanation
WebSEAL was unable to register itself with ARM.

Administrator response
Check ARM setup is operational. Refer to the error message for more specific information.

DPWNS1353W

Failed to register WebSEAL transaction '*%s*' with ARM: error code *%d*: error message '*%s*'. ARM support will be disabled. (0x38b9a549)

Explanation
WebSEAL was unable to register the transaction with ARM.

Administrator response
Check ARM setup. Refer to the error message for more specific information.

DPWNS1354W

Failed to start WebSEAL as an ARM application: error code *%d*: error message '*%s*'. ARM support will be disabled. (0x38b9a54a)

Explanation
WebSEAL was unable to start as an ARM application.

Administrator response
Check ARM setup. Refer to the error message for more specific information.

DPWNS1356W

Failed to stop WebSEAL running as an ARM application: error code *%d*: error message '*%s*'. (0x38b9a54c)

Explanation
WebSEAL was unable to stop running as an ARM application using arm_stop_application().

Administrator response
Refer to the error message for more specific information.

DPWNS1357W

Failed to unregister the WebSEAL application from ARM: error code *%d*: error message '*%s*'. (0x38b9a54d)

Explanation
WebSEAL was unable to unregister as an ARM application using arm_destroy_application().

Administrator response
Refer to the error message for more specific information.

DPWNS1358W

Failed to get ARM transaction '*%s*' arrival time: error code *%d*: error message '*%s*'. (0x38b9a54e)

Explanation
The call to ARM function arm_get_arrival_time() failed unexpectedly. The transaction will not be reported.

Administrator response
Refer to the error message for more specific information.

DPWNS1359W

Failed to get the length of an ARM correlator: error code *%d*: error message '*%s*'. (0x38b9a54f)

Explanation
The call to ARM function arm_get_correlator_length() failed unexpectedly. The correlator will not be used.

Administrator response
Refer to the error message for more specific information.

DPWNS1360W

An invalid correlator string was passed to WebSEAL: '*%s*'. It will not be used for subsequent transactions. (0x38b9a550)

Explanation
An ARMCorrelator header was received by WebSEAL with an invalid value.

Administrator response
Check the application making the request to WebSEAL. Or disable WebSEAL from using incoming ARM Correlator by setting accept-correlators = no in the [arm] stanza.

DPWNS1361W

Failed to start ARM transaction '*%s*': error code *%d*: error message '*%s*'. The transaction will not be reported. (0x38b9a551)

Explanation
The call to ARM function arm_start_transaction() failed unexpectedly. The transaction will not be reported.

Administrator response
ARM can limit the number of concurrent transactions being reported. It may be possible to increase the limit. Also refer to the error message for more specific information.

DPWNS1362W

Failed to stop ARM transaction '*%s*': error code *%d*: error message '*%s*'. (0x38b9a552)

Explanation
The call to ARM function arm_stop_transaction() failed unexpectedly.

Administrator response
Refer to the error message for more specific information.

DPWNS1363W

Unable to start ARM transaction reporting as ARM initialization failed. See log files for more information. (0x38b9a553)

Explanation
The 'arm on' command cannot complete as the ARM initialization failed.

Administrator response
Examine the log files for the reason ARM initization failed. Correct this, restart WebSEAL and try again.

DPWNS1364W

Unable to start ARM transaction reporting as WebSEAL ARM support has been disabled. (0x38b9a554)

Explanation
The 'arm on' command cannot complete as the WebSEAL ARM support has been disabled in the configuration file.

Administrator response
To enable ARM support set enable = yes in the [arm] stanza and restart WebSEAL.

DPWNS1365W

ARM transaction reporting is already on. (0x38b9a555)

Explanation
The 'arm on' command is redundant and will be ignored as arm transaction reporting is already on.

Administrator response
Don't run the 'arm on' command while transaction reporting is on.

DPWNS1366W

ARM transaction reporting is already off. (0x38b9a556)

Explanation
The 'arm off' command is redundant and will be ignored as arm transaction reporting is already off.

Administrator response
Don't run the 'arm off' command while transaction reporting is off.

DPWNS1367W

Failed to load ARM library '*%s*': error code *%d*: error message '*%s*'. ARM support will be disabled. (0x38b9a557)

Explanation
WebSEAL attempted to dynamically load the ARM shared library and failed.

Administrator response
Check the shared library name is correct and present on the system. Refer to the error message for more specific information. The shared library name is specified by the library entry under the [arm] stanza. If loading the ARM library is not desired set enable-arm = no under the [arm] stanza.

DPWNS1368W

Unable to start ARM transaction reporting as WebSEAL ARM support has been disabled. (0x38b9a558)

Explanation
The 'arm on' command cannot complete as the WebSEAL ARM support has been disabled in the configuration file.

Administrator response
To enable ARM support set enable-arm = yes in the [arm] stanza and restart WebSEAL.

DPWNS1500E

The interface '*%s*', defined in the [*%s*] stanza, contains an invalid value for '*%s*'. You must specify either 'http' or 'https'. (0x38b9a5dc)

Explanation
The web-http-protocol and web-https-protocol interface settings can only contain 'http' or 'https'.

Administrator response
Set the value to either 'http' or 'https'

DPWNS1501E

The option '*%s*', defined in the [*%s*] stanza, contains an invalid value. You must specify either 'http' or 'https'. (0x38b9a5dd)

Explanation
The web-http-protocol and web-https-protocol settings can only contain 'http' or 'https'.

Administrator response
Set the value to either 'http' or 'https'

DPWNS1502E

The option '*%s*' defined in the [*%s*] stanza contains an invalid port value. (0x38b9a5de)

Explanation
The port value provided is either out of the valid range, or is not a number.

Administrator response
Provide a valid value for a TCP/IP port in the range 1 to 65535.

DPWWA0150E

Cannot allocate memory (0x38cf0096)

Explanation
Memory allocation operation failed.

Administrator response
Check memory limits on your machine, and increase available memory if possible.

DPWWA0151E

An insufficient amount of memory was supplied. (0x38cf0097)

Explanation
An insufficient amount of memory was passed into a function.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA0305E

The '*%s*' routine failed for '*%s*', errno = *%ld* (0x38cf0131)

Explanation
This is a major internal server failure. An internal function call failed.

Administrator response
Contact customer support.

DPWWA0306E

Error in configuration file: *%s* (0x38cf0132)

Explanation
The configuration file contained an error.

Administrator response
Edit the configuration file to correct the error.

DPWWA0308W

Function *name* failed with errno *value* (0x38cf0134)

Explanation
This is a generic message used to identify specific non-fatal function calls failing.

Administrator response
Determine why the function call failed.

DPWWA0309E

Badly formatted config entry for *%s* cache (0x38cf0135)

Explanation
The configuration defined in the [content-cache] stanza was incorrect.

Administrator response
Correct the values in the [content-cache] stanza of the configuration file.

DPWWA0310E

Could not open IBM Security Verify Access WebSEAL configuration file (*%s*) (0x38cf0136)

Explanation
See message.

Administrator response
Correct problem preventing configuration file from being opened.

DPWWA0314E

Initialization of authorization API failed. Major status=0x*%x*, minor status = 0x*%x* (0x38cf013a)

Explanation
See message.

Administrator response
Look up the specified major/minor status codes either through the Error Message Reference Book or the pdadmin errtxt command. Analyze and fix the error based on that information.

DPWWA0315E

Initialization of authentication layer failed: *%s* (0x38cf013b)

Explanation
One of the authentication libraries failed to load.

Administrator response
Correct the entries for the authentication libraries in webseald.conf

DPWWA0316W

Configuration item value has been assumed for *%s* (0x38cf013c)

Explanation
The configuration item value did not make sense and a default value was assumed

Administrator response
Correct the configuration variable in webseald.conf

DPWWA0318E

Error in configuration file, invalid accept-client-certs value: *%s* (0x38cf013e)

Explanation
See message.

Administrator response
Correct the accept-client-certs parameter in webseald.conf

DPWWA0319E

Error in configuration file. When accept-client-certs is set to optional or required, you must specify a library with the cert-ssl option, or you must specify an eai-uri option. (0x38cf013f)

Explanation
See message.

Administrator response
Set the cert-ssl parameter in webseald.conf

DPWWA0320W

Error in configuration. Clients and MPAs cannot use the same session types. (0x38cf0140)

Explanation
Clients and MPAs cannot use the same session types.

Administrator response
Configure clients and MPAs to use different session types.

DPWWA0321E

Value for stanza [*%s*] entry '*%s*' contains an illegal trailing backslash character. (0x38cf0141)

Explanation
Backslash characters are used to remove any special meaning of the character following it. The end of line cannot be treated this way.

Administrator response
Remove the trailing \\ character from the the entries value.

DPWWA0322E

Value for stanza [*%s*] entry '*%s*' contains an unmatched quote. (0x38cf0142)

Explanation
Quote characters are used to allows values to have leading and trailing space characters. The values that have this requirement must have a quote at the begining and end of the region of chars. A unpaired quote is not legal unless its special meaning is removed using the backslash character.

Administrator response
Remove the unmatched " character from the the entries value or place a \\ char before it to remove its special meaning.

DPWWA0323E

Value for stanza [*%s*] entry '*%s*' contains a 'name = value' with a missing name. (0x38cf0143)

Explanation
Stanza entries of this type have a special format. This format consists of multiple name = value pairs separated by semicolon characters. In this case the name part of a pair is missing or empty.

Administrator response
Provide a name before the = character.

DPWWA0324E

Value for stanza [*%s*] entry '*%s*' contains a 'name = value' with a missing = character. (0x38cf0144)

Explanation
Stanza entries of this type have a special format. This format consists of multiple 'name = value' pairs separated by semicolon characters. In this case the = separating the pair is missing.

Administrator response
Insert the missing = character.

DPWWA0325E

Value for stanza [*%s*] entry '*%s*' contains two name value pairs with the same name '*%s*'. (0x38cf0145)

Explanation
Stanza entries of this type have a special format. This format consists of multiple 'name = value' pairs separated by semicolon characters. In this case there are two of these pairs with the same name. This is illegal as all names must be unique.

Administrator response
Remove or rename one of the name value pair with the duplicate name.

DPWWA0326E

Stanza [*%s*] contains an illegal duplicate entry '*%s*'. (0x38cf0146)

Explanation
This stanza expects entries with unique names.

Administrator response
Remove or rename one of the entry names.

DPWWA0327W

The default WebSEAL TCP and SSL interfaces have both been disabled, which also disables the default WebSEAL worker threads. (0x38cf0147)

Explanation
When both the default WebSEAL interfaces are disabled using [server] https = no and http = no the default worker threads are also not created. This will make WebSEAL unaccessable unless additional interfaces are defined under [interfaces] stanza. Note that these additional interfaces will not be able to share the 'default' worker threads as they will not have been created.

Administrator response
No action required, it just an unusual situation.

DPWWA0328E

The interface '*%s*' defined in the [*%s*] stanza contains an illegal empty value for '*%s*'. (0x38cf0148)

Explanation
The worker threads setting in the configuration of an interface must be set to either the number of worker threads to create, or the name of another interface to share worker threads with. Typically this entry will look like 'worker-threads = 50'

Administrator response
Supply a non-empty value for worker-threads.

DPWWA0329E

The interface '*%s*' defined in the [*%s*] stanza contains an illegal value for '*%s*'. (0x38cf0149)

Explanation
The worker threads setting in the configuration of an interface must be set to either the number of worker threads to create, or the name of another interface to share worker threads with. Typically this entry will look like 'worker-threads = 50'

Administrator response
Provide the name of an interface that has it's own worker threads or provide the number of worker threads it should create for itself.

DPWWA0330E

The interface '*%s*' defined in the [*%s*] stanza contains an invalid value for '*%s*'. (0x38cf014a)

Explanation
The port value provided is either out of the legal range or is not a number.

Administrator response
Provide a legal value for a TCP/IP port in the range 1 to 65535.

DPWWA0331E

The interface '*%s*' defined in the [*%s*] stanza contains an illegal TCP/IP address value for '*%s*'. (0x38cf014b)

Explanation
The TCP/IP value provided is either 255.255.255.255 or not a valid string for an TCP/IP address

Administrator response
Provide a legal value for a TCP/IP port.

DPWWA0332E

Invalid certificate authentication configuration for interface '*%s*' defined in the [*%s*] stanza. Incompatible combination of accept-client-certs and ssl-id-sessions values. (0x38cf014c)

Explanation
See message.

Administrator response
Change the accept-client-certs or ssl-id-sessions parameter in webseald.conf.

DPWWA0333E

Invalid certificate cache configuration to support interface '*%s*' defined in the [*%s*] stanza. (0x38cf014d)

Explanation
See message.

Administrator response
Change the values of the certificate cache configuration items.

DPWWA0334E

There is an error in the configuration file. An invalid accept-client-certs value (*%s*) for the '*%s*' interface has been defined in the [*%s*] stanza. (0x38cf014e)

Explanation
See message.

Administrator response
Correct the accept-client-certs parameter in webseald.conf

DPWWA0335E

Error in configuration file relating to interface '*%s*' defined in the [*%s*] stanza. When accept-client-certs is set to optional, required, or prompt_as_needed, specify a library with the cert-ssl option or the eai-uri option. (0x38cf014f)

Explanation
See message.

Administrator response
Set the cert-ssl parameter in webseald.conf

DPWWA0336E

The interface '*%s*' defined in the [*%s*] stanza must have one of http-port or https-port enabled. (0x38cf0150)

Explanation
An interface has no function unless at least one port is defined.

Administrator response
Assign a port to either or both of http-port or https-port.

DPWWA0337W

The '*%s*' routine failed in '*%s*' for interface *%s*:*%d*, errno = *%d* (0x38cf0151)

Explanation
A non-fatal error was reported from the specified function, called in a specified function in relation to the specified interface and port. The system error code is given to help diagnose the reason. WebSEAL will continue to function. Typically this occurs when a connection from a browser is ended abnormally.

Administrator response
Keep an eye on this and if this occurs too often contact WebSEAL customer support.

DPWWA0338E

Not enough free file descriptors in the process to configure even one of the worker threads wanted by the worker pool named '*%s*'. (0x38cf0152)

Explanation
Each interface defined can have it's own worker thread pool. If previous definintions have consumed all available resources in creating their own worker thread pools then there may be nothing left for this interface. Each worker thread requires 2 file descriptors. The number of available file descriptors is dependent on the Operating System WebSEAL is run on and is fixed when WebSEAL is constructed.

Administrator response
Reduce the number of worker threads used by other worker pools.

DPWWA0339W

Worker list '*%s*' has configured *%d* worker threads which is greater than the system can support. It has automatically been reduced to *%d*. (0x38cf0153)

Explanation
Each operation system has different levels of support for threads and open files. That combined with compile time options will provide limits on the configurable number of worker threads.

Administrator response
The software automatically reduced the value. However to stop this message appearing you may set the value in the configuration file lower.

DPWWA0340E

Unable to listen on interface *%s*:*%d*, errno = *%d* (0x38cf0154)

Explanation
The attempt to listen for connections on the specified interface and port failed. The system error code is given to help diagnose the reason.

Administrator response
It is likely the reason for failure is that another process or WebSEAL interface is already listening on the same port and network address. Change the port and/or network address to one not in use.

DPWWA0341E

Error in configuration file, unknown setting '*%s*' for interface '*%s*' defined in the [*%s*] stanza. (0x38cf0155)

Explanation
The interface has an unknown name=value pair in it's configuration. This could be due to a spelling error.

Administrator response
Remove the unknown setting in the WebSEAL configuration file

DPWWA0342W

The configuration data for this WebSEAL instance has been logged in '*%s*' (0x38cf0156)

Explanation
This is an informational message.

Administrator response
Informational. No action is required.

DPWWA0343E

An error occurred trying to log the WebSEAL configuration data at startup. (0x38cf0157)

Explanation
Check the server's error log file for specific error conditions that could have led to this failure. It is possible that there are permission issues with the configuration data log file or there are space limitations in the filesystem.

Administrator response
It is likely that logging the server's configuration data failed because the desired location for the log file is missing or was specified incorrectly in the server's configuration file.

DPWWA0345E

The request was too large to store in the session cache. (0x38cf0159)

Explanation
The request size exceeded request-max-cache or the message body exceeded request-body-max-read, so the request could not be stored in the session cache.

Administrator response
Re-submit the request after authentication or increase request-max-cache and/or request-body-max-read

DPWWA0346E

Invalid certificate data has been supplied. (0x38cf015a)

Explanation
The client certificate which has been supplied to WebSEAL during the authentication operation cannot be decoded correctly.

Administrator response
Ensure that the client certificate which is being used to authenticate to WebSEAL is valid.

DPWWA0347E

There is an error in the configuration setting '*%s*' (min=*%d* max=*%d*), for interface '*%s*', as defined in the [*%s*] stanza. (0x38cf015b)

Explanation
The interface has a configuration with an invalid name=value pair.

Administrator response
Correct the setting's value in the WebSEAL configuration file

DPWWA0600E

The requested single sign-on service is not supported by this server (0x38cf0258)

Explanation
Junction created with an SSO specification that the server was not built to support

Administrator response
Do not use the single-sign-on service specified by the junction definition

DPWWA0601E

Could not fetch SSO info for user (*%s*,0x*%8lx*) (0x38cf0259)

Explanation
Could not map from username/pwd to principal/target in SSO

Administrator response
Check mappings from principal/target to username/pwd in SSO

DPWWA0602E

User '*%s*' does not have any associated SSO info (0x38cf025a)

Explanation
SSO data either does not exist or is incorrect.

Administrator response
Check that SSO data for this user exists and is correct.

DPWWA0603E

User '*%s*' does not have a matching SSO target (0x38cf025b)

Explanation
The user was found in SSO, but no target exists for them.

Administrator response
Create a target in SSO for this user.

DPWWA0605E

Can't perform single sign-on. User '*%s*' is not logged in (0x38cf025d)

Explanation
User must be authenticated to use SSO.

Administrator response
Informative only. User must be logged in.

DPWWA0606E

Could not sign user '*%s*' on due to incorrect target (0x38cf025e)

Explanation
Could not sign user on due to incorrect target in SSO.

Administrator response
Check the target in SSO for this user

DPWWA0607E

Received basic authentication challenge for junction where filtering is being applied (0x38cf025f)

Explanation
The junction type filters out Basic Authentication data, but the junctioned server sent a BA challenge.

Administrator response
Either create the junction without the -filter flag or modify the junctioned server to not use Basic Authentication.

DPWWA0608E

Unable to obtain binding to LDAP server (0x38cf0260)

Explanation
Unable to obtain binding to LDAP server

Administrator response
Check that LDAP server is running and can be accessed.

DPWWA0609E

Unable to obtain binding to LDAP-GSO server (0x*%8lx*) (0x38cf0261)

Explanation
Unable to obtain binding to LDAP-GSO server

Administrator response
Check that LDAP-GSO server is running and can be accessed.

DPWWA0625E

Either the configuration file is missing or it has errors. (0x38cf0271)

Explanation
The iv.conf file is either missing, or the LDAP stanza does not have enough information to bind to the LDAP server.

Administrator response
Make sure that the configuration file has the ldap stanza and all the LDAP information is included in the stanza.

DPWWA0626E

This script can only be used to decode form results. (0x38cf0272)

Explanation
This error occurs when the user invokes the update password URL directly from the browser.

Administrator response
The user needs to invoke the cgi-bin program and change the password from the browser.

DPWWA0627E

Could not get the LDAP distinguished name (DN) for the remote user. (0x38cf0273)

Explanation
The ira_get_dn(), to get the distinguished name, failed.

Administrator response
Make sure that the LDAP entry is set for the remote user.

DPWWA0628E

The selected resource or resource group does not exist. (0x38cf0274)

Explanation
The user selected a resource or a resource group that does not exist in the LDAP database.

Administrator response
Make sure that the resource or the resource group exists for the user.

DPWWA0629E

Could not bind to the LDAP server. (0x38cf0275)

Explanation
The ira_rgy_init call failed. Contact your Administrator.

Administrator response
Make sure that the LDAP server can be reached and try again.

DPWWA0630E

This script should be referenced with a METHOD of POST. (0x38cf0276)

Explanation
This error occurs when the user invokes the update password URL directly from the browser.

Administrator response
The user needs to invoke the cgi-bin program and change the password from the browser.

DPWWA0631E

Passwords don't match. (0x38cf0277)

Explanation
The user attempted to change their GSO target password and failed to confirm the new password.

Administrator response
The user must correct their entries in the update password form, ensuring that the passwords match.

DPWWA0632E

Unable to retrieve user identity. (0x38cf0278)

Explanation
This error occurs because the REMOTE_USER cgi environment variable was not passed to the GSO chpwd program by WebSEAL.

Administrator response
Verify that the cgi-program is being invoked by WebSEAL and not called directly.

DPWWA0633E

Either a user ID or a password must be specified. (0x38cf0279)

Explanation
Either the user ID or a password must be specified to update the resource.

Administrator response
Enter the user ID or password and try again.

DPWWA0634E

Select a resource or resource group. (0x38cf027a)

Explanation
The required resource information was missing from the cgi form used to update a user's GSO target information.

Administrator response
The user must specify the proper resource information in the cgi form.

DPWWA0635E

Completed successfully. (0x38cf027b)

Explanation
Operation completed successfully.

Administrator response
No action required.

DPWWA0636E

No TFIM single sign-on tokens were available. (0x38cf027c)

Explanation
WebSEAL is correctly retrieving SSO tokens from TFIM, but these tokens have expired. The problem is most likely caused by the clocks on the WebSEAL server and the TFIM server being set to different times.

Administrator response
Check the time synchronization between the TFIM server and the WebSEAL server.

DPWWA0637E

The credential information could not be stored. (0x38cf027d)

Explanation
The call to GSO to store credentials failed.

Administrator response

DPWWA0638E

An attempt to obtain credential information from a GSO Web service invoked a call to another GSO Web service. This is an invalid configuration. (0x38cf027e)

Explanation
The junction on which a GSO Web service resides also requires GSO style authentication using another GSO Web service. This is not a supported configuration.

Administrator response
Ensure that the junction on which the initiating GSO Web service resides does not also require GSO style authentication.

DPWWA0639E

An unexpected HTTP status code was returned from the GSO Web service: *%d* (0x38cf027f)

Explanation
A request was made to a configured GSO Web service and the response contained an unexpected HTTP status code.

Administrator response
Ensure that the GSO Web service is functioning correctly and that it conforms to the specification contained in the Verify Access documentation.

DPWWA0640E

The response which has been received from a GSO Web service is invalid. (0x38cf0280)

Explanation
A request was made to a configured GSO Web service but the response contained invalid JSON data.

Administrator response
Ensure that the GSO Web service is functioning correctly and that it conforms to the specification contained in the Verify Access documentation.

DPWWA1055E

Operation has insufficient Quality of Protection (0x1005b41f)

Explanation
This error occurs when a person tries to access an object that requires a secure communications channel over an insecure channel such as TCP.

Administrator response
Either access the object over SSL/TLS or modify the policy associated with the object to reduce the QOP required.

DPWWA1061E

Provide your authentication details for method: (0x1005b425)

Explanation
This error is printed when a user attempts to access an object that requires a higher level of authentication than they have provided.

Administrator response
The user should either provide the higher level of authentication, or the policy associated with the object should be modified to reduce the level of authentication required.

DPWWA1062E

An invalid authentication level has been detected in a POP object. (0x1005b426)

Explanation
A POP object specified an authentication level that is not supported by the current WebSEAL configuration.

Administrator response
Either modify the POP object to correct the authentication level, or modify the WebSEAL configuration file to specify an authentication method that can provide the required level.

DPWWA1076E

Privacy required (0x38cf0434)

Explanation
Indicates that requested object has the privacy bit set, but the request is not using privacy

Administrator response
The user must connect using privacy to access the resource.

DPWWA1082E

Invalid HTTP status code present in response. The response could have been sent either by a third-party server or by a local resource, such as a CGI program. (0x38cf043a)

Explanation

An invalid status code was received in a response. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

Administrator response

Check the status code in the response. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

DPWWA1083E

Could not read HTTP status line in response. Possible causes: non-spec HTTP response, connection timeout, no data returned. The response could have been sent either by a third-party server or by a local resource, such as a CGI program. (0x38cf043b)

Explanation

Data read failure. Possible causes: non-spec HTTP response, connection timeout, no data returned. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

Administrator response

Check response for a missing HTTP status line. Also investigate a possible connection timeout problem. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

DPWWA1084E

Could not read HTTP headers in response. Possible causes: non-spec HTTP headers, connection timeout, no data returned. The response could have been sent either by a third-party server or by a local resource, such as a CGI program. (0x38cf043c)

Explanation

Data read failure. Possible causes: non-spec HTTP headers, connection timeout, no data returned. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

Administrator response

Check response for bad HTTP headers. Also investigate a possible connection timeout problem. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

DPWWA1085E

An HTTP message body sent in a response is too short. The response could have been sent either by a third-party server or by a local resource, such as a CGI program. (0x38cf043d)

Explanation

The actual length of the response body is shorter that indicated by the Content-length HTTP header in the response.

Administrator response
Correct problem with the response. The actual length of the response body is shorter that indicated by the Content-length HTTP header of the response.

DPWWA1086E

Could not read request line. Possible causes: non-spec HTTP headers, connection timeout, no data returned (0x38cf043e)

Explanation
Data read failure. Possible causes: non-spec HTTP data, connection timeout, no data returned

Administrator response
Check client request. Could contain bad HTTP headers or there might be a connection timeout problem.

DPWWA1087E

Invalid URL (0x38cf043f)

Explanation
A client request contained a URL that does not conform to HTTP specifications.

Administrator response
Check request from client. Does not conform to HTTP specifications.

DPWWA1088E

Bad cookie header (or data read failure) (0x38cf0440)

Explanation
Data read failure. Possible causes: timeout, connection problems, no data returned

Administrator response
Check response from either junctioned server or client. Could be bad Cookie header, Set-cookie header or a connection timeout problem.

DPWWA1089E

Invalid date string in HTTP header (0x38cf0441)

Explanation
Invalid date string in HTTP header in client request.

Administrator response
Check request from client. Contains invalid date string in HTTP header.

DPWWA1091W

Failed to load portal map (0x*%8lx*) (0x38cf0443)

Explanation
The portal service failed to load correctly due to a problem with the information in the [portal-map] stanza of the configuration file.

Administrator response
Correct errors in the [portal-map] stanza of the configuration file.

DPWWA1092E

Unable to open stanza file to read portal information (0x38cf0444)

Explanation
The configuration file containing the portal mapping service information could not be opened for reading.

Administrator response
Ensure that the configuration file exists and is readable.

DPWWA1093W

Unable to find [portal-map] stanza (0x38cf0445)

Explanation
The [portal-map] stanza was not found in the configuration file.

Administrator response
Ensure that the [portal-map] stanza has been added to the configuration file.

DPWWA1094E

Unable to read the URL field of the portal map (0x38cf0446)

Explanation
The URL attribute of a portal map entry in the configuration file was not found.

Administrator response
Ensure that the [portal-map] stanza of the configuration file contains the URL field.

DPWWA1095E

Unable to read the Protected Object field of the portal map (0x38cf0447)

Explanation
The Protected Object field of a portal map entry in the configuration file was not found.

Administrator response
Ensure that the [portal-map] stanza of the configuration file contains the Protected Object field.

DPWWA1096E

Unable to read the Action field of the portal map (0x38cf0448)

Explanation
The Action field of a portal map entry in the configuration file was not found.

Administrator response
Ensure that the [portal-map] stanza of the configuration file contains the Action field.

DPWWA1097E

the Protected Object supplied to the portal map is invalid (0x38cf0449)

Explanation
The Protected Object field in the [portal-map] stanza of the configuration file is not a valid Protected Object name

Administrator response
Correct the value entered in the Protected Object field of the [portal-map] stanza of the configuration file.

DPWWA1100W

POST request larger than request-body-max-read, cannot apply dynurl matching. (0x38cf044c)

Explanation
WebSEAL attempted to apply dynurl matching to a request, but received too much POST data from the client.

Administrator response
Increase the request-body-max-read in the configuration file or rearchitect your site so that WebSEAL does not need to apply dynurl rules to large POSTs.

DPWWA1110E

Unable to build original URL for Attribute Retrieval Service (0x38cf0456)

Explanation
WebSEAL was unable to obtain the hostname of the URL that client has requested. The result of this is that the original URL cannot be constructed for consumption by the Attribute Retrieval Service.

Administrator response
Ensure that configuraion is complete.

DPWWA1111E

The SOAP client returned the error code: *%d* (0x38cf0457)

Explanation
The SOAP request failed, and the gSOAP client returned the error code contained in the message text.

Administrator response
Consult gSOAP documentation for error code definitions.

DPWWA1112E

Attribute Retrieval Service internal error: *%s* (0x38cf0458)

Explanation
The SOAP request succeeded, but the Attribute Retrieval Service returned the error contained in the message text.

Administrator response
Ensure that the Attribute Retrieval Service is configured correctly.

DPWWA1113E

URL specifies an invalid Win32 object name (0x38cf0459)

Explanation
The client request specifies the object name using a Win32 alias that points to the actual object. The authorization check will have been performed on the alias, and not the actual object, so the request cannot be allowed.

Administrator response
Ensure that client requests do not use Win32 aliases.

DPWWA1114E

URL contains invalid Win32 characters or abbreviations (0x38cf045a)

Explanation
The client request contains Win32 abbreviations or '\' characters that are invalid.

Administrator response
Ensure that client requests do not contain invalid Win32 characters or abbreviations.

DPWWA1115E

URL contains an illegal byte sequence (0x38cf045b)

Explanation
The client request contains an illegal byte sequence, possibly from an attempted multibyte character encoding.

Administrator response
Ensure that client requests do not contain illegal byte sequences.

DPWWA1116E

The requested method is not supported (0x38cf045c)

Explanation
One of the supported HTTP methods (that is: GET, PUT, POST, etc...) must be specified by each client request. This request either contains an unsupported method, or none at all.

Administrator response
Ensure that client requests contain a valid method.

DPWWA1117E

The content-length of the client request is invalid (0x38cf045d)

Explanation
The content-length is either less than zero, or it doesn't accurately describe the length of the POST-body, or it should not be provided with the request.

Administrator response
Ensure that the content-length specified correctly describes the characteristics of the request, and that this is not a chunked request.

DPWWA1118E

The 'host' header is not present in the client request (0x38cf045e)

Explanation
The client request specifies an HTTP version of 1.1, but doesn't include the host header that is required for this version.

Administrator response
Ensure that the host header is present in request who's HTTP version is 1.1.

DPWWA1119E

The HTTP version specified by the client request is not supported (0x38cf045f)

Explanation
See Message.

Administrator response
Ensure that the HTTP version of the request is correct and supported.

DPWWA1120E

The POST body of the client request contains misformated or invalid data (0x38cf0460)

Explanation
See Message.

Administrator response
Ensure that the POST bodies of client requests contain valid data.

DPWWA1121E

An error occurred while reading the POST body of the request (0x38cf0461)

Explanation
See Message.

Administrator response
Ensure that the POST bodies of client requests are valid.

DPWWA1122W

Corrupted session cookie: *%s*. (0x38cf0462)

Explanation
A session cookie was presented that was corrupted. This could be a spoof attempt, a browser or network problem, or a WebSEAL internal problem.

Administrator response
Investigate spoof attempt or source of corruption.

DPWWA1123W

The login data entered could not be mapped to an IBM Security Verify Access user (0x38cf0463)

Explanation
A mapping function, such as that in a library or CDAS, failed to map the login information to an IBM Security Verify Access user.

Administrator response
Check the login data, registry, or mapping function.

DPWWA1124W

A client certificate could not be authenticated (0x38cf0464)

Explanation
A client certificate could not be authenticated

Administrator response
Check the client certificate

DPWWA1125W

The data contained in the HTTP header *%s* failed authentication (0x38cf0465)

Explanation
The request an HTTP header that IBM Security Verify Access was configured to use as authentication data. This data failed authentication.

Administrator response
Check the request, the proxy server (if one is used), and the mapping library

DPWWA1126W

IP address based authentication failed with IP address: *%s* (0x38cf0466)

Explanation
IBM Security Verify Access is configured to authenticate using the client IP address, which was either unavailable or invalid

Administrator response
Check IBM Security Verify Access configuration and/or authentication library

DPWWA1128E

The current authentication method does not support reauthentication. Contact the IBM Security Verify Access WebSEAL Administrator. (0x38cf0468)

Explanation

Reauthentication is not supported by the current WebSEAL authentication method. The user can abort the reauthentication process (by accessing another URL) and still participate in the secure domain by accessing other resources that do not require reauthentication.

Administrator response

Notify the IBM Security Verify Access WebSEAL Administrator.

DPWWA1129E

A reauthentication operation was attempted with an initial authentication method for which reauthentication is not supported. (0x38cf0469)

Explanation

A reauthentication misconfiguration has occurred. Administrators should not put a reauthentication POP on a resource for clients who cannot actually perform a reauthentication.

Administrator response

The resource requested requires reauthentication but reauthentication is supported only by Forms, Token, and EAI authentication.

DPWWA1130E

Authentication level mismatch when performing reauthentication (0x38cf046a)

Explanation

The authentication level supplied while reauthenticating does not match the authentication level of the existing authenticated user.

Administrator response

The user's authentication level must be the same when reauthenticating as when they originally authenticated.

DPWWA1131W

An entry in the [portal-map] stanza is invalid. (0x38cf046b)

Explanation

[portal-map] stanza in the configuration file contains an invalid entry.

Administrator response

Ensure that all entries in the [portal-map] stanza are valid.

DPWWA1132W

Entry '*%s* = *%s*' in the [portal-map] stanza is invalid. (0x38cf046c)

Explanation
[portal-map] stanza in the configuration file contains an invalid entry.

Administrator response
Correct the entry in the [portal-map] stanza.

DPWWA1133E

The 'host' header presented in the client request does not conform to HTTP specifications. (0x38cf046d)

Explanation
The client request contains a host header which does not conform to the HTTP specification.

Administrator response
Ensure that the host header conforms to the HTTP specification.

DPWWA1200E

The requested junction type is not supported by this server (0x38cf04b0)

Explanation
The requested junction type is not supported by this server

Administrator response
Change junction definition.

DPWWA1201E

Junction not found (0x38cf04b1)

Explanation
The named junction does not exist.

Administrator response
Verify the name, and if incorrect try the operation again.

DPWWA1202E

Requested object does not exist (0x38cf04b2)

Explanation
Object on junctioned server does not exist.

Administrator response
Informational only.

DPWWA1203E

Permission denied (0x38cf04b3)

Explanation
You do not have permission to mount or unmount at this location.

Administrator response
Check the acl at this location for mount or unmount permissions.

DPWWA1204E

Requested object is not a directory (0x38cf04b4)

Explanation
Requested object is not a directory

Administrator response
Informational only.

DPWWA1205E

No query-contents on this server (0x38cf04b5)

Explanation
To list object space, a query_contents cgi program must be configured on the junctioned server.

Administrator response
To list object space, configure a query_contents cgi program on the junctioned server.

DPWWA1206E

Illegal name for a junction point (0x38cf04b6)

Explanation
The junction point is illegal.

Administrator response
Use a different junction point for the new junction.

DPWWA1207E

Trying to add wrong type of server at this junction point (0x38cf04b7)

Explanation
Trying to add wrong type of server at this junction point

Administrator response
Change junction definition.

DPWWA1208E

Trying to add two servers with the same UUID at a junction point (0x38cf04b8)

Explanation
Trying to add two servers with the same UUID at a junction point

Administrator response
Change junction definition

DPWWA1209E

Trying to add the same server twice at the same junction point (0x38cf04b9)

Explanation
Trying to add the same server twice at the same junction point

Administrator response
Change junction definition

DPWWA1210E

Could not open junction database (*%s*,0x*%8x*) (0x38cf04ba)

Explanation
Indicates a problem accessing the junction database maintained by the IBM Security Verify Access server.

Administrator response
Check junction database directory existance and permissions.

DPWWA1211E

Could not load junction database (*%s*,0x*%8lx*) (0x38cf04bb)

Explanation
An error occurred when loading the junction database.

Administrator response
Check that all of the files in the junction database can be read by the ivmgr user and are not corrupted. Check other error messages for other information about the error. If necessary, remove all of the files in the junction database and then add them back one by one to isolate the problem to a specific file.

DPWWA1212E

Could not delete entry from junction database (*%s*,0x*%8lx*) (0x38cf04bc)

Explanation
The XML File representing the junction could not be deleted.

Administrator response
Check the file permissions on the junction XML file

DPWWA1213E

Could not write entry to junction database (*%s*,0x*%8lx*) (0x38cf04bd)

Explanation
Internal status code only. Database was opened, but could not be written to.

Administrator response
Check system memory and disk space.

DPWWA1214W

Could not fetch entry from junction database (*%s*,0x*%8lx*) (0x38cf04be)

Explanation
Internal status code only. Database was opened, but this junction could not be read.

Administrator response
Check that the xml file representing the junction is not corrupt.

DPWWA1215E

Invalid junction flags for this junction type (0x38cf04bf)

Explanation
Invalid junction flags for this junction type

Administrator response
Correct junction definition.

DPWWA1216E

Invalid parameters for junction (0x38cf04c0)

Explanation
Invalid parameters for junction

Administrator response
Correct junction definition.

DPWWA1217E

An error occurred when writing a request to a junction. WebSEAL was unable to dispatch the request to another junction server. (0x38cf04c1)

Explanation
WebSEAL tried to send a request to a junction server. Sending the request failed. When WebSEAL is unable to send a request to a junction, WebSEAL attempts to 'rewind' the request from the client so that it can be sent to another junction server. If the request from the client is large, it may not be possible to retry the request. In that case, this error is returned to the client.

Administrator response
Retry the request. If the problem continues to occur, attempt to discover why the request could not be written to the junction server. Check WebSEAL and junction server log files for unusual error messages. Try sending the request directly to the junction.

DPWWA1218E

Unknown junction server host (0x38cf04c2)

Explanation
Could not resolve a hostname using gethostbyname()

Administrator response
Check the hostname in the junction configuration and make sure it is resolveable.

DPWWA1219E

Could not build junction server URL mappings (0x*%8lx*) (0x38cf04c3)

Explanation
See message

Administrator response
Contact support.

DPWWA1220E

Cannot delete the junction at the root of the Web space. Try replacing it instead (0x38cf04c4)

Explanation
Cannot delete the junction at the root of the Web space. Try replacing it instead

Administrator response
Cannot delete the junction at the root of the Web space. Try replacing it instead

DPWWA1221E

Cannot add two servers with different options (case-sensitive, etc) at the same junction (0x38cf04c5)

Explanation
Cannot add two servers with different options (case-sensitive, etc) at the same junction

Administrator response
Change junction definition

DPWWA1222E

A third-party server is not responding. Possible causes: the server is down, there is a hung application on the server, or network problems. This is not a problem with the WebSEAL server. (0x38cf04c6)

Explanation
A junctioned server is not responding to requests. Possible causes: junctioned server down, network problems, hung application on junctioned server.

Administrator response
Determine why the junctioned server is not responding and fix it.

DPWWA1224E

Could not load junction database (0x38cf04c8)

Explanation
The database couldn't be loaded for some reason.

Administrator response
Check the log files for more details.

DPWWA1225E

Could not delete entry from junction database (0x38cf04c9)

Explanation
The file representing the junction could not be deleted from the filesystem.

Administrator response
Check the log files for more details.

DPWWA1226E

Could not write entry to junction database (0x38cf04ca)

Explanation
Internal status code only. Database was opened, but could not be written to.

Administrator response
Check system memory and disk space.

DPWWA1227W

Could not fetch entry from junction database (0x38cf04cb)

Explanation
Internal status code only. Database was opened, but this junctio n could not be read.

Administrator response
Check that the xml file representing the junction is not corrupt.

DPWWA1228E

Unable to contact junction server host at mount point: *%s* (0x38cf04cc)

Explanation
Could not resolve a hostname using gethostbyname()

Administrator response
Check for network conectivity with the junctioned server

DPWWA1229E

Unable to load junction file *%s*: *%s* (0x38cf04cd)

Explanation
An error occurred while loading a file from the junction database. The reason for the error is included in the message.

Administrator response
Correct the error.

DPWWA1230E

Error building junction *%s* from file *%s*: *%s* (0x38cf04ce)

Explanation
An error occurred while building a junction from an XML file loaded from the junction database. The XML file may have specified invalid junction options.

Administrator response
Fix the problem in the XML file.

DPWWA1231E

No such junction. (0x38cf04cf)

Explanation
A particular junction was not found in the junction database.

Administrator response
Verify that the junction file exists.

DPWWA1232E

Could not remove file. (0x38cf04d0)

Explanation
The junction database was unable to remove a file.

Administrator response
Verify that all files in the junction database are writable by the ivmgr user and group.

DPWWA1233E

Invalid junction file name. (0x38cf04d1)

Explanation
The junction file name specified did not map to a valid junction name.

Administrator response
Make sure the junction file name ends with .xml and is a valid mime 64 encoding.

DPWWA1234E

An invalid status code was received in a response sent by a third-party server. This is not a problem with the WebSEAL system. (0x38cf04d2)

Explanation
A junctioned server has sent an invalid status code in a response.

Administrator response
Check status code returned from junctioned server.

DPWWA1235E

Could not read the response status line sent by a third-party server. Possible causes: non-spec HTTP headers, connection timeout, no data returned. This is not a problem with the WebSEAL server. (0x38cf04d3)

Explanation
Data read failure. Possible causes: non-spec HTTP headers, connection timeout, no data returned

Administrator response
Check response from junctioned server. Could be bad HTTP headers or a connection timeout problem.

DPWWA1236E

Could not read the response headers sent by a third-party server. Possible causes: non-spec HTTP headers, connection timeout, no data returned. This is not a problem with the WebSEAL server. (0x38cf04d4)

Explanation
Data read failure. Possible causes: non-spec HTTP headers, connection timeout, no data returned

Administrator response
Check response from junctioned server. Could be bad HTTP headers or a connection timeout problem.

DPWWA1237E

An invalid HTTP header was sent by a third-party server. This is not a problem with the WebSEAL server. (0x38cf04d5)

Explanation
An HTTP response from a junctioned server does not conform to HTTP specs.

Administrator response
Check response from junctioned server for non-spec HTTP headers.

DPWWA1238E

An HTTP message body sent in a response by a third-party server is too short. This is not a problem with the WebSEAL server. (0x38cf04d6)

Explanation
The actual length of the response body sent by a junctioned server is shorter that indicated by the Content-length HTTP header in the response.

Administrator response
Correct problem with junctioned server response. The actual length of the response body is shorter that indicated by the Content-length HTTP header of the response.

DPWWA1239E

A third-party server is not responding. Possible causes: the server is down, there is a hung application on the server, or network problems. This is not a problem with the WebSEAL server. (0x38cf04d7)

Explanation
A junctioned server is not responding to requests. Possible causes: junctioned server down, network problems, hung application on junctioned server.

Administrator response
Determine why the junctioned server is not responding and fix it.

DPWWA1240E

Could not build Virtual Host Junction host mappings (0x*%8lx*) (0x38cf04d8)

Explanation
See message

Administrator response
Contact support.

DPWWA1241E

Virtual Host Junction '*%s*' loaded from database illegally partners Virtual Host Junction '*%s*'. Virtual Host Junction skipped. (0x38cf04d9)

Explanation
An error occurred when loading the Virtual Host Junction from it's database file. It may have been incorrectly manually modified. The problem is the the Virtual Host Junction being loaded refers to one that also refers to another.

Administrator response
Manually edit the offending Virtual Host Junction Database file and correct it.

DPWWA1242E

Virtual Host Junction '*%s*' loaded from database illegally partners Virtual Host Junction '*%s*' that already has partner '*%s*'. Virtual Host Junction skipped. (0x38cf04da)

Explanation
An error occurred when loading the Virtual Host Junction from it's database file. It may have been incorrectly manually modified.

Administrator response
Manually edit the offending Virtual Host Junction Database file and correct it.

DPWWA1243E

Virtual Host Junction '*%s*' loaded from database illegally partners Virtual Host Junction '*%s*' with different virtual hostname. Virtual Host Junction skipped. (0x38cf04db)

Explanation
An error occurred when loading the Virtual Host Junction from it's database file. It may have been incorrectly manually modified. Virtual Host Junctions that are partnered must have the same virtual hostname (excluding the ports).

Administrator response
Manually edit the offending Virtual Host Junction Database file and correct it.

DPWWA1244E

Virtual Host Junction attempted to partner (-g) non-existant Virtual Host Junction (0x38cf04dc)

Explanation
See text.

Administrator response
Use 'virtualhost list' command to find a valid partner.

DPWWA1245E

Virtual Host Junction attempted to partner (-g) a Virtual Host Junction with a different virtual hostname. (0x38cf04dd)

Explanation
See text.

Administrator response
Use 'virtualhost show' command to help match virtual hostnames.

DPWWA1246E

Virtual Host Junction illegally attempted to partner (-g) itself. (0x38cf04de)

Explanation
See text.

Administrator response
Choose another partner.

DPWWA1247E

Virtual Host Junction can not be changed to partner (-g) another as it is currently being partnered. (0x38cf04df)

Explanation
See text.

Administrator response
Do not use -g for this operation.

DPWWA1248E

Could not write entry to Virtual Host Junction database (0x38cf04e0)

Explanation
Internal status code only. Database was opened, but could not be written to.

Administrator response
Check system memory and disk space.

DPWWA1249E

Could not write entry to Virtual Host Junction database (*%s*,0x*%8lx*) (0x38cf04e1)

Explanation
Internal status code only. Database was opened, but could not be written to.

Administrator response
Check system memory and disk space.

DPWWA1250E

Virtual Host Junction can not be deleted until it's partner is deleted. (0x38cf04e2)

Explanation
See text.

Administrator response
Delete the Partner Virtual Host Junction first.

DPWWA1251E

Virtual Host Junctions created using -g don't have their own object space. List the partner's object space instead. (0x38cf04e3)

Explanation
Virtual Host Junctions created using -g share their partnered Virtual Host Junction's protected object space. They don't have their own.

Administrator response
List the partnered Virtual Host Junctions object space instead as this Virtual Host Junction uses it for access control.

DPWWA1252E

Virtual Host Junctions partnered using -g must have different protocol types (TCP and SSL). (0x38cf04e4)

Explanation
The concept of -g is to have the same content but opposite protocol, this was violated in this attempt to create a Virtual Host junction using -g.

Administrator response
Either don't use -g or ensure the type of the Virtual Host junction are of complementry protocols. For example localtcp and localssl will partner successfully.

DPWWA1253E

The Virtual Host junction you are attempting to partner with using -g is already in a partnership. (0x38cf04e5)

Explanation
The concept of -g is to have only two Virtual host junctions in partnership, a third is not permitted.

Administrator response
Either don't use -g or ensure the Virtual Host junction being partnered to is not already in a partnership.

DPWWA1254E

Can't replace a Virtual Host junction being partnered too with a new junction having a different protocol type (TCP and SSL). (0x38cf04e6)

Explanation
The concept of -g is to have the same content but opposite protocol, this was violated in this attempt to replace an existing Virtual Host junction.

Administrator response
Ensure the type of the Virtual Host junction is the same protocol as the Virtual Host juntion being replaced.

DPWWA1255E

Can't replace a Virtual Host junction being partnered too with a new junction having a different virtual hostname. (0x38cf04e7)

Explanation
See text.

Administrator response
Use 'virtualhost show' command to help match virtual hostnames.

DPWWA1256E

Virtual Host junction has duplicate virtual hostname (specificed by -v) as another Virtual Host junction. (0x38cf04e8)

Explanation
Virtual Host junctions are selected based on the host header in the client request matching the virtual hostname (specified by -v) of the Virtual Host junction. Thus the virtual hostname must be unique to be able to uniquely identify a Virtual Host junction.

Administrator response
Remove the Virtual Host junction with the duplicate virtual hostname before adding this one.

DPWWA1257E

Could not load the local junction, *%s*, as the local junction functionality has been disabled. (0x38cf04e9)

Explanation
Local Junctions are disabled for this instance and a previously configured local junction, "%s", could not be loaded.

Administrator response
Remove the local junction or enable local junctions in the WebSEAL configuration file.

DPWWA1258E

Could not build the server which is used to retrieve HTTP updates: *%s* (0x38cf04ea)

Explanation
An attempt has been made to communicate with a HTTP update server. This operation failed while trying to set up the internal framework which will be used.

Administrator response
Verify that the configuration of the HTTP update server is correct. Pay particular attention to the SSL settings.

DPWWA1259E

Could not connect to the server which is used to retrieve HTTP updates: *%s* (0x38cf04eb)

Explanation
An attempt to communicate with a HTTP update server failed.

Administrator response
Verify that the configuration of the HTTP update server is correct, and that the HTTP update server can be reached.

DPWWA1260E

The command, *%s*, failed. (0x38cf04ec)

Explanation
An attempt to execute a configured command failed.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA1350E

Could not initialize mutex (0x38cf0546)

Explanation
A resource required for proper concurrency could not be created. The global variable errno may provide more specific information.

Administrator response
This is a fatal error. No recovery is possible.

DPWWA1352E

Could not lock mutex (0x38cf0548)

Explanation
A resource required for proper concurrency could not be locked. The global variable errno may provide more specific information.

Administrator response
This is a fatal error. No recovery is possible.

DPWWA1353E

Could not unlock mutex (0x38cf0549)

Explanation
A resource required for proper concurrency could not be unlocked. The global variable errno may provide more specific information.

Administrator response
This is a fatal error. No recovery is possible.

DPWWA1503E

SSL function *function* failed, error 0x*error code* (0x38cf05df)

Explanation
An SSL toolkit function has failed.

Administrator response
This is a fatal error. No recovery is possible. Contact Support

DPWWA1504W

SSL function *function* failed, error 0x*error code* (0x38cf05e0)

Explanation
An SSL toolkit function failed.

Administrator response
This is a warning message. Operation continues. If the warning persists contact support.

DPWWA1505W

HTTP request does not contain authentication information (0x38cf05e1)

Explanation
HTTP request does not contain authentication information

Administrator response
Internal status code only.

DPWWA1506E

Unknown HTTP authentication scheme (0x38cf05e2)

Explanation
An authorization header contained an invalid authentication scheme.

Administrator response
Check Authorization header in request.

DPWWA1507E

No password supplied in HTTP authentication header (0x38cf05e3)

Explanation
No password supplied in HTTP Authorization header

Administrator response
Check Authorization header in request.

DPWWA1518W

The specified certificate key label *%s* is incorrect. The default one will be used instead. (0x38cf05ee)

Explanation
The specified certificate key label cannot be retrieved from the key database

Administrator response
check the webseald.conf ssl-keyfile-label option and the key database

DPWWA1519E

The SSL session cache has become full and because of this existing SSL sessions will be displaced. (0x38cf05ef)

Explanation

The SSL session cache is now full which means that existing sessions will be displaced to make room for new sessions.

Administrator response

Consider increasing the size of the SSL session cache size, using the ssl-max-entries configuration parameter.

DPWWA1520W

The SSL session cache has reached *%d*%% capacity. If this warning persists it might indicate that the size of the SSL session cache should be increased. (0x38cf05f0)

Explanation

The SSL session cache is becoming full. When the cache does become full it will mean that existing sessions will be displaced to make room for new sessions.

Administrator response

Consider increasing the size of the SSL session cache size, using the ssl-max-entries configuration parameter.

DPWWA1521E

The password could not be updated because the user record could not be located (0x38cf05f1)

Explanation

The call to the search endpoint did not return a valid result.

Administrator response

Check the response from the configured password-callout search endpoint. One way to do this is to enable the pdweb.snoop.passwd trace component.

DPWWA1522E

The password could not be updated because of the following error [*%s*:*%s*] (0x38cf05f2)

Explanation

The call to the pre endpoint did not return a valid result.

Administrator response

Check the response from the configured password-callout pre-update endpoint. One way to do this is to enable the pdweb.snoop.passwd trace component.

DPWWA1523E

The password was successfully updated but the following error occurred [*%s*:*%s*] (0x38cf05f3)

Explanation
The call to the post endpoint did not return a valid result.

Administrator response
Check the response from the configured password-callout post-update endpoint. One way to do this is to enable the pdweb.snoop.passwd trace component.

DPWWA1524E

The password could not be updated due to an error with an external service (0x38cf05f4)

Explanation
The call to a password callout endpoint did not return a valid result.

Administrator response
Check the response from the configured password-callout endpoints. One way to do this is to enable the pdweb.snoop.passwd trace component.

DPWWA1950E

Stanza '*%s*' is missing from configuration file (0x38cf079e)

Explanation
A necessary stanza is missing from configuration file

Administrator response
The stanza should be added to the configuration file

DPWWA1951E

Configuration item '[*%s*]*%s*' is missing from configuration file (0x38cf079f)

Explanation
A necessary configuration item is missing from configuration file

Administrator response
The configuration item should be added to the configuration file

DPWWA1952E

Received invalid HTTP header in response. The response could have been sent either by a third-party server or by a local resource, such as a CGI program. (0x38cf07a0)

Explanation
Response HTTP headers do not conform to HTTP specs. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

Administrator response
Check HTTP headers in response. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

DPWWA1953E

HTTP document fetch failed with status *%d* (0x38cf07a1)

Explanation
Could not retrieve requested resource.

Administrator response
Check request for correctness.

DPWWA1954E

HTTP list request failed (0x38cf07a2)

Explanation
Could not list directory on junctioned server

Administrator response
Check permissions and existence of directory being listed

DPWWA1955E

Field missing from HTTP header (0x38cf07a3)

Explanation
Internal status code only.

Administrator response
No action is required.

DPWWA1962W

CGI Script Failed (0x38cf07aa)

Explanation
Internal status code only.

Administrator response
No action is required.

DPWWA1964E

Invalid Content-Length header returned by TCP junction server (0x38cf07ac)

Explanation
The content-length is either less than zero, or it doesn't accurately describe the length of the POST-body.

Administrator response
Ensure that the content-length specified correctly describes the characteristics of the request.

DPWWA1965E

Overflow of output buffer (0x38cf07ad)

Explanation
Internal status code only.

Administrator response
No action is required.

DPWWA1966E

Overflow of HTML filter workspace (0x38cf07ae)

Explanation
Internal status code only.

Administrator response
No action is required.

DPWWA1967E

Overflow of HTTP filter workspace (0x38cf07af)

Explanation
Internal status code only.

Administrator response
No action is required.

DPWWA1968E

HTTP response truncated (0x38cf07b0)

Explanation
Internal status code only.

Administrator response
No action is required.

DPWWA1969E

HTTP request truncated (0x38cf07b1)

Explanation
Internal status code only.

Administrator response
No action is required.

DPWWA1970E

Cannot rewind HTTP response to write error message (*%lx*) (0x38cf07b2)

Explanation
An internal error has occoured trying to rewing the HTTP response.

Administrator response
MRQ Contact support

DPWWA1971E

Cannot write HTTP error response to client (*%lx*,*%lx*) (0x38cf07b3)

Explanation
An internal error has occoured trying to write the error response to the client.

Administrator response
MRQ Contact support

DPWWA1972E

Cannot read HTTP request from client (0x38cf07b4)

Explanation
Internal status code only.

Administrator response
No action is required.

DPWWA1973E

HTTP response aborted (0x38cf07b5)

Explanation
Internal status code only.

Administrator response
No action is required.

DPWWA1975W

Unable to decode *%s* (0x38cf07b7)

Explanation
The decode of the specified token has failed.

Administrator response
Contact support.

DPWWA1976W

Unable to encode *%s* (0x38cf07b8)

Explanation
The encode of the specified token has failed. This is an unexpected internal error.

Administrator response
Contact support.

DPWWA1977W

%s for user *%s*, in domain *%s* has expired (0x38cf07b9)

Explanation
cdsso authentication token for a user has expired

Administrator response
The token has expired. This could be due to clock skew, in which case fix the clocks or change the authentication token lifetime in configuration file. But beware of replay attacks

DPWWA1978W

Badly formed single-sign-on URL (0x38cf07ba)

Explanation
Badly formed single-sign-on URL

Administrator response
Fix the cdsso link on the web page.

DPWWA1979W

Failover cookie contents have expired (0x38cf07bb)

Explanation
Failover cookie contents for a user has expired

Administrator response
No action is required.

DPWWA1980W

Could not retrieve key for failover cookie (0x38cf07bc)

Explanation
Internal status code only.

Administrator response
No action is required.

DPWWA1981W

An internal error occurred while encoding/decoding the *%s* (0x38cf07bd)

Explanation
Internal status code only.

Administrator response
No action is required.

DPWWA1982W

Could not find SSO key for server/domain *%s* (0x38cf07be)

Explanation
The SSO key file has not been correctly configured for the server

Administrator response
Set up configuration to provide correct key file for the specified server.

DPWWA1983W

CDSSO cryptography error *%d* occurred (0x38cf07bf)

Explanation
Internal status code only.

Administrator response
No action is required.

DPWWA1984W

Unable to use failover cookies. No failover cookie key configured (0x38cf07c0)

Explanation
Failover cookies have been enabled, but no keyfile has been specified.

Administrator response
Either turn failover cookies off, or specify the keyfile for the failover cookie.

DPWWA1985W

Unable to retrieve CDSSO referer from request (0x38cf07c1)

Explanation
Either the agent has not provided the referer header or the client has directly typed in the link and not been directed by a link

Administrator response
No action is required.

DPWWA1986W

Error reading key file *%s* (0x38cf07c2)

Explanation
The CDSSO keyfile could not be read from

Administrator response
Check the keyfile for existence and permissions.

DPWWA1987W

Error writing key file *%s* (0x38cf07c3)

Explanation
The CDSSO keyfile could not be written to

Administrator response
Check the keyfile for permissions.

DPWWA1988E

This action requires HTTP forms to be enabled in the configuration file (0x38cf07c4)

Explanation
HTTP forms are required for this action but are not enabled in the configuration file

Administrator response
The forms-auth configuration item should be set to both

DPWWA1989W

Invalid protection level for *%s* (0x38cf07c5)

Explanation
The received token is of an insufficent protection level

Administrator response
Ensure that vf-token-privacy and vf-token-integrity have the same settings on both WebSEAL servers.

DPWWA1990W

The e-community name *%s* does not match the configured name *%s* (0x38cf07c6)

Explanation
Another WebSEAL has passed an e-community name which does not match this servers configured e-community name

Administrator response
Synchronize the e-community names

DPWWA1991W

The e-community cookie passed has expired (0x38cf07c7)

Explanation
The contents of the e-community cookie passed have expired

Administrator response
No action is required.

DPWWA1992E

Can't retrieve fully qualified host name for server. Disabling e-community single-sign-on (0x38cf07c8)

Explanation
The fully qualified host name could not be retrieved

Administrator response
Ensure that network configuration allows gethostbyname to retrieve the fully qualified name

DPWWA1993E

Can't determine server domain name. Disabling e-community single-sign-on (0x38cf07c9)

Explanation
The domain name could not be determined

Administrator response
Specify value for ec-cookie-domain setting or ensure that gethostbyname returns the fully qualified host name

DPWWA1994E

Disabling e-community single-sign-on (0x38cf07ca)

Explanation
An error occurred when looking up the key associated with the domain name for this server.

Administrator response
Ensure that network configuration allows gethostbyname to retrieve the fully qualified name. You may need to place the fully qualified host name of this server first in the hosts file.

DPWWA1995E

Invalid master authentication server configuration. Disabling e-community single-sign-on (0x38cf07cb)

Explanation
master-authentication-server and is-master-authentication-serverare mutually exclusive settings

Administrator response
Correctly configure the settings for master authentication server

DPWWA1996E

e-community-name has not been specified. Disabling e-community single-sign-on (0x38cf07cc)

Explanation
An e-community name was not specified. This is mandatory

Administrator response
Correctly configure an e-community name

DPWWA1997W

The machine *%s* could not vouch for the user's identity (0x38cf07cd)

Explanation
The specified machine returned a token indicating that it could not vouch for the user's identity

Administrator response
Correct e-community configuration

DPWWA1998W

Unable to open the LTPA key file for reading (0x38cf07ce)

Explanation
The LTPA key file configured for a junction could not be opened for reading

Administrator response
Check junction configuration

DPWWA1999W

The version of the LTPA key file is not supported (0x38cf07cf)

Explanation
Only certain versions of LTPA keyfiles are supported

Administrator response
Obtain right version of the key file

DPWWA2000W

Error parsing LTPA key file (0x38cf07d0)

Explanation
The LTPA Keyfile is either corrupt or the wrong version

Administrator response
Obtain new copy of keyfile

DPWWA2001W

LTPA key file: password invalid or file is corrupt (0x38cf07d1)

Explanation
The password specified could not decrypt keyfile

Administrator response
Use correct key file password or ensure file is not corrupted

DPWWA2002W

The LTPA cookie passed has expired (0x38cf07d2)

Explanation
An expired LTPA cookie was passed

Administrator response
No action is required

DPWWA2004W

LTPA text conversion error (0x38cf07d4)

Explanation
An iconv routine failed

Administrator response
Check locale settings

DPWWA2005W

An error occurred while encoding an LTPA token (0x38cf07d5)

Explanation
Internal Error

Administrator response
Contact support.

DPWWA2006W

An error occurred while decoding an LTPA token (0x38cf07d6)

Explanation
Internal Error

Administrator response
Contact support.

DPWWA2008E

Error reading stanza '[*%s*]': *%s* (0x38cf07d8)

Explanation
One of the entries in the stanza couldn't be parsed.

Administrator response
Fix the malformed entry in the stanza.

DPWWA2009E

The forms single-sign-on argument '*%s*' needs a colon. (0x38cf07d9)

Explanation
One of the request arguments isn't formatted properly.

Administrator response
Fix the argument.

DPWWA2010E

Forms single-sign-on GSO argument '*%s*' is not valid. GSO arguments must be either 'gso:username' or 'gso:password.' (0x38cf07da)

Explanation
One of the request arguments isn't formatted properly.

Administrator response
Fix the argument.

DPWWA2011E

The forms single-sign-on argument '*%s*' is not valid. (0x38cf07db)

Explanation
Most likely a typo in the config file.

Administrator response
Fix the argument.

DPWWA2012E

Forms single-sign-on configuration error. (0x38cf07dc)

Explanation
This is a summary of the problem, and will be preceded by a better explanation of the error.

Administrator response
Fix the configuration problem.

DPWWA2013E

Forms single-sign-on URLs must be relative to the junction point. (0x38cf07dd)

Explanation
The fsso URL from the configuration file does not begin with a / character.

Administrator response
Make the fsso URL relative to the junction point.

DPWWA2014E

An internal error in the forms single-sign-on module occurred. (0x38cf07de)

Explanation
This should never happen - perhaps some kind of unexpected configuration problem has resulted in an internal error.

Administrator response
Call tech support.

DPWWA2015E

A forms SSO authentication request would have been dispatched to a different junction than the login request. The request has been aborted. (0x38cf07df)

Explanation
For security reasons, forms SSO does not allow an authentication request to be dispatched to a different junction than the login page was returned from.

Administrator response
Make sure that the application does not dispatch the authentication request to a different junction than returned the login page.

DPWWA2016E

No HTML form for single-sign-on was found. (0x38cf07e0)

Explanation
This occurs when no HTML form with an action URI matching the login-form-action was found in the document returned from the junction.

Administrator response
Examine the login page being returned from the junction. Is it an HTML or WML document? Does it contain an HTML form? Does the form action URI match the login-form-action entry in the forms SSO configuration file?

DPWWA2017E

The login form returned by the junction did not contain all required form attributes. (0x38cf07e1)

Explanation
This occurs when the login form returned from a junction did not cpontain an 'action' or 'method' attribute in the form start tag.

Administrator response
Examine the login form being returned from the junction. Did the login form contain both the action and method attributes? Does the form action URI match the form action URI specified in the configuration file?

DPWWA2018E

The action URI in the login form returned by the junction did not match any WebSEAL junction. (0x38cf07e2)

Explanation
In order to dispatch a forms SSO authentication request, WebSEAL must match the action URI returned with the login form to a WebSEAL junction. That match could not be made.

Administrator response
Examine the login form being returned by the junction. You may need to create a junction to the host referenced by the actoin URI.

DPWWA2019E

The action URI in the login form returned by the junction was invalid. (0x38cf07e3)

Explanation
An action URI such as '/../foo' will be rejected by WebSEAL because /.. is not a valid location.

Administrator response
Examine the login form. Does it contain any invalid characters, or is the path invalid?

DPWWA2020E

One or more of the arguments passed to the SU authentication module were invalid. (0x38cf07e4)

Explanation
The suauthn library can take an argument to specify the authentication level for the credential. It prints this error if the arguments are incorrect.

Administrator response
Check the flags being passed to the authentication library.

DPWWA2021E

The SU authentication method specified is not enabled. (0x38cf07e5)

Explanation
The POST to /pkmssu.form takes an auth_method parameter. This must correspond to an authentication mechanism that is enabled in the configuration file.

Administrator response
Check the auth_method field in the SU form submission.

DPWWA2023E

Configuration item '[*%s*]*%s*' has an invalid value '*%s*' (0x38cf07e7)

Explanation
A configuration item in the configuration file has a bad value. For example it is expecting an integer and was provided with a string

Administrator response
The configuration item should be changed to a valid entry

DPWWA2024E

%s [*%s*] *%s*: Value is out of range. It must be value from 0 to 100. (0x38cf07e8)

Explanation
WebSEAL will not start if the worker-thread-hard-limit or worker-thread-soft-limit is not in the range 0 to 100 inclusive

Administrator response
You must edit the configuration file and adjust the value to a valid one

DPWWA2025W

IBM Security Verify Access WebSEAL has lost contact with junction (*%s*) server: *%s* (0x38cf07e9)

Explanation
See message.

Administrator response
Check the network conection between WebSEAL and the junctioned server, and that the backend application server is running.

DPWWA2026W

IBM Security Verify Access WebSEAL has regained contact with junction (*%s*) server: *%s* (0x38cf07ea)

Explanation
WebSEAL has regained contact with a junctioned server that was previously unreachable.

Administrator response
No action is required.

DPWWA2027E

One or more of the form arguments is either missing or invalid. (0x38cf07eb)

Explanation
One or more of the arguments passed in the form submission is either missing or invalid.

Administrator response
Check the completed fields in the form submission.

DPWWA2028E

New password verification failed. Make sure both new password fields contain the same data. (0x38cf07ec)

Explanation
New password double-check failed. Make sure both new passwords are the same.

Administrator response
Check the new password fields in the form submission.

DPWWA2029E

Pam Module Internal Error (0x38cf07ed)

Explanation
Error with the Pam Handle. This is an unexpected internal error.

Administrator response
Notifiy the IBM Security Verify Access WebSEAL Administrator.

DPWWA2030W

Mismatch of Auth Token versions, check pre-410-compatible-tokens setting. (0x38cf07ee)

Explanation
A new encoding method for Auth tokens was introduced in version 4.1.0 which is enabled by default. This can be overridden and made compatable with earlier versions using the webseald.conf file entry, [server] pre-410-compatible. All WebSEAL servers must be using the same version.

Administrator response
Update all WebSEAL servers to use the same setting for [server] pre-410-compatible-tokens.

DPWWA2031W

Mismatch of *%s* Auth Token versions, check pre-410-compatible-tokens setting. (0x38cf07ef)

Explanation
A new encoding method for Auth tokens was introduced in version 4.1.0 which is enabled by default. This can be overridden and made compatable with earlier versions using the webseald.conf file entry, [server] pre-410-compatible. All WebSEAL servers must be using the same version.

Administrator response
Update all WebSEAL servers to use the same setting for [server] pre-410-compatible-tokens.

DPWWA2032E

CDSSO library error. (0x38cf07f0)

Explanation
The CDSSO library returned a failing status.

Administrator response
Check configuration and usage. See msg__webseald.log for details.

DPWWA2033E

Invalid configuration file name. (0x38cf07f1)

Explanation
An invalid parameter was passed to a function, indicating an internal error.

Administrator response
Call support.

DPWWA2034E

Some PKCS#11 options are missing. You must specify either all or none of the the options: pkcs11-driver-path, pkcs11-token-label, pkcs11-token-pwd (0x38cf07f2)

Explanation
WebSEAL will not start if only some of the PKCS#11 options are specified.

Administrator response
You must edit the configuration file and set all PKCS#11 settings

DPWWA2035E

Credential generation failed during the credential refresh operation. Error code 0x*%lx* (0x38cf07f3)

Explanation
The azn-api function azn_id_get_creds was called to retrieve a new credential for a user. The operation failed.

Administrator response
Use the pdadmin 'errtext' command to look up the corresponding error code, and take further action from there.

DPWWA2036E

Credential generation failed during the credential refresh operation. (0x38cf07f4)

Explanation
The azn-api function azn_id_get_creds was called to retrieve a new credential for a user. The operation failed.

Administrator response
Check error logs for further information on the failure.

DPWWA2037E

An invalid result for a credential refresh rule was specified. (0x38cf07f5)

Explanation
Credential refresh rules require that the rule result be either 'preserve' or 'refresh.'

Administrator response
Verify that the syntax of credential refresh configuration in configuration files is correct.

DPWWA2038E

An internal error occurred during the credential refresh operation. (0x38cf07f6)

Explanation
This error should not occur.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2039W

A credential attribute value of type *%lu* not supported by credential refresh was found. The value was removed from the new credential. (0x38cf07f7)

Explanation
Credential attribute values can be of several types. Credential refresh is able to preserve string, buffer, unsigned long, and protected object values. Other value types are removed from the credential.

Administrator response
You may ignore this warning if you are not experiencing other difficulties involving credential refresh. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2040E

User session IDs must be enabled in order to use the credential refresh feature. (0x38cf07f8)

Explanation
Refreshing a user's credential based on their username requires that user session IDs are enabled.

Administrator response
Enable User Session IDs in the WebSEAL configuration file.

DPWWA2041E

An invalid session cache entry was found while refreshing a user's credential. (0x38cf07f9)

Explanation
This message indicates that the user session cache and the credential cache are inconsistent.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2042W

The user is not logged in to the web server. (0x38cf07fa)

Explanation
If a user is not logged in to the web server, their credential cannot be refreshed. There is also no need to refresh their credential, since the next time they log in to the web server they will receive a new credential.

Administrator response
No action is necessary.

DPWWA2044E

Invalid certificate authentication configuration. Incompatible combination of accept-client-certs and ssl-id-sessions values. (0x38cf07fc)

Explanation
See message.

Administrator response
Change the accept-client-certs or ssl-id-sessions parameter in webseald.conf

DPWWA2045W

A client attempted to Step-up to certificates, but the server is not configured for Step-up to certificates. (0x38cf07fd)

Explanation
See message.

Administrator response
Change the accept-client-certs parameter to prompt_as_needed in webseald.conf or unconfigure the step-up POPs.

DPWWA2046E

Invalid certificate cache configuration. (0x38cf07fe)

Explanation
See message.

Administrator response
Change the values of the certificate cache configuration items.

DPWWA2047E

The activity timestamp is missing from the failover cookie. (0x38cf07ff)

Explanation
A request was made to update the last activity timestamp of the failover cookie, but the attribute was not found in the cookie.

Administrator response
An internal error occurred. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2048E

The original authentication method in the failover cookie is not recognized for failover authentication on this server. The value *%s* is invalid. (0x38cf0800)

Explanation
A request could not be authenticated using the supplied failover cookie because the authentication level specified in the cookie is not valid for this server.

Administrator response
Update the supported failover authentication methods in the configuration file or correct the configuration of the server that generated the failover cookie.

DPWWA2049E

The original authentication method in the failover cookie is not recognized for failover authentication on this server. (0x38cf0801)

Explanation
A request could not be authenticated using the supplied failover cookie because the authentication level specified in the cookie is not valid for this server.

Administrator response
Update the supported failover authentication methods in the configuration file or correct the configuration of the server that generated the failover cookie.

DPWWA2050E

An authentication system failure has occurred. (0x38cf0802)

Explanation
A call to the authentication system failed with an unexpected error.

Administrator response
Examine the log for the context of the failure and correct any indicated problem. In particular, ensure that your user registry is available and accessible. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2051E

An authentication system failure has occurred: error: *%s* (error code: *%#lx*). (0x38cf0803)

Explanation
A call to the authentication system failed with an unexpected error.

Administrator response
Examine the log for the context of the failure and correct any indicated problem. In particular, ensure that your user registry is available and accessible. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2052E

The cross domain single sign-on operation failed. (0x38cf0804)

Explanation
A call into the cross domain single sign-on system failed with an unexpected error.

Administrator response
Examine the log for the context of the failure. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2053E

The cross domain single sign-on system failed with an unexpected error: *%#x* (0x38cf0805)

Explanation
A call into the cross domain single sign-on system failed with an unexpected error.

Administrator response
Examine the log for the context of the failure. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2054E

No default HTTP method permission map has been specified. (0x38cf0806)

Explanation
A default HTTP method permission map must be specified in the configuration file but none has been.

Administrator response
Specify a value for the default HTTP method permission map in the configuration file.

DPWWA2055E

The HTTP method permission map configuration information could not be found in the configuration file. (0x38cf0807)

Explanation
No HTTP method permission map configuration information could be found in the configuration file.

Administrator response
Ensure that HTTP method permission map configuration information is present in the configuration file.

DPWWA2056E

HTTP method permission map validation failed: API error: *%s* (API error code: [*%#x*:*%#x*]). (0x38cf0808)

Explanation
The authorization API failed while validating the configured HTTP method permission map.

Administrator response
Perform the action required to resolve the problem indicated by the identified API error. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2057E

The SSO token module configuration data was missing or invalid. (0x38cf0809)

Explanation
The process using the SSO token modules must provide some input data to configure the modules. This data was not provided correctly. This is an unexpected internal error.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2058E

The integer value '*%s*' for the '*%s*' entry in the '*%s* stanza is not valid. (0x38cf080a)

Explanation
The specified value is required to be a non-negative integer.

Administrator response
Correct the invalid configuration value.

DPWWA2059W

The *%s* attribute could not be extracted from a credential: API error: *%s* (API error code [*%x*:*%x*]). (0x38cf080b)

Explanation
The specified attribute could not be extracted from a credential. This may be due to resource exhaustion, and as such be transient.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2060W

The *%s* attribute could not be extracted from a credential: API error code [*%x*:*%x*]. (0x38cf080c)

Explanation
The specified attribute could not be extracted from a credential. This may be due to resource exhaustion, and as such be transient.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2061W

The number of values for the *%s* attribute could not be retrieved from an attribute list: API error: *%s* (API error code [*%x*:*%x*]). (0x38cf080d)

Explanation
The number of values for the specified attribute could not be retrieved from an attribute list. This may be due to resource exhaustion, and as such be transient.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2062W

The number of values for the *%s* attribute could not be retrieved from an attribute list: API error code [*%x*:*%x*]. (0x38cf080e)

Explanation
The number of values for the specified attribute could not be retrieved from an attribute list. This may be due to resource exhaustion, and as such be transient.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2063W

The type of value *%d* for the *%s* attribute from an attribute list could not be determined: API error: *%s* (API error code [*%x*:*%x*]). (0x38cf080f)

Explanation
The type of a values for the specified attribute in an attribute list could not be determined. This may be due to resource exhaustion, and as such be transient.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2064W

The type of value *%d* for the *%s* attribute from an attribute list could not be determined: API error code [*%x*:*%x*]. (0x38cf0810)

Explanation
The type of a values for the specified attribute in an attribute list could not be determined. This may be due to resource exhaustion, and as such be transient.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2065W

Value *%d* of the *%s* attribute cannot be included in an SSO token, as it is of type *%s*. (0x38cf0811)

Explanation
The specified attribute value cannot be included in an SSO token, because it is of the wrong type. Only string and unsigned long data types can be included in SSO tokens.

Administrator response
Remove the token attribute specification which matched this attribute, or, for custom attributes, change the attribute type to one suitable for inclusion in tokens.

DPWWA2066W

The *%s* attribute could not be extracted from an attribute list: API error: *%s* (API error code [*%x*:*%x*]). (0x38cf0812)

Explanation
The specified attribute could not be extracted from an attribute list. This may be due to resource exhaustion, and as such be transient.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2067W

The *%s* attribute could not be extracted from an attribute list: API error code [*%x*:*%x*]. (0x38cf0813)

Explanation
The specified attribute could not be extracted from an attribute list. This may be due to resource exhaustion, and as such be transient.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2068W

The attribute list could not be retrieved from a credential: API error: *%s* (API error code [*%x*:*%x*]). (0x38cf0814)

Explanation
The attribute list could not be extracted from a credential. This may be due to resource exhaustion, and as such be transient.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2069W

The attribute list could not be retrieved from a credential: API error code [*%x*:*%x*]. (0x38cf0815)

Explanation
The attribute list could not be extracted from a credential. This may be due to resource exhaustion, and as such be transient.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2070W

The list of entry names could not be retrieved from an attribute list: API error: *%s* (API error code: [*%x*:*%x*]). (0x38cf0816)

Explanation
The list of entry names could not be extracted from an attribute list. This may be due to resource exhaustion, and as such be transient.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2071W

The list of entry names could not be retrieved from an attribute list: API error code [*%x*:*%x*]. (0x38cf0817)

Explanation
The list of entry names could not be extracted from an attribute list. This may be due to resource exhaustion, and as such be transient.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2072E

No cryptographic keys are configured for cross domain single sign-on in the stanza '*%s*'. (0x38cf0818)

Explanation
No keys are configured for Cross Domain Single Sign-On in the specified stanza. For Cross Domain Single Sign-On to operate, keys must be configured in this stanza.

Administrator response
Correct the configuration, or use the cdsso_key_gen utility to create keys for use by CDSSO. CDSSO keys must be securely shared by, and installed on, all CDSSO participant servers.

DPWWA2073E

No cryptographic keys are configured for e-community single sign-on in the stanza '*%s*'. (0x38cf0819)

Explanation
No keys are configured for e-Community Single Sign-On in the specified stanza. For e-Community Single Sign-On to operate, keys must be configured in this stanza.

Administrator response
Correct the configuration, or use the cdsso_key_gen utility to create keys for use by eCSSO. eCSSO keys must be securely shared by and installed on all servers participating in the e-Community.

DPWWA2074W

The machine '*%s*' could not vouch for the user's identity: error: *%s* (error code: *%#lx*) (0x38cf081a)

Explanation
The specified machine returned a token indicating that it could not vouch for the user's identity. This means that either the user's account is disabled, or that the user was unable to authenticate to the specified machine.

Administrator response
If the message indicates that the user's account is disabled, check whether this should be the case. If the message indicates an authentication failure, the user may need to have their password changed. If possible, check the log messages on the specified machine for more information.

DPWWA2075E

The stanza '*%s*' contains an invalid SSO token incoming attribute configuration item: '*%s* = *%s*'. (0x38cf081b)

Explanation
The SSO token incoming attribute stanzas specify attributes that are accepted and rejected from incoming eCSSO or CDSSO tokens. The right hand side of the items in this stanza must be either 'accept' or 'reject'.

Administrator response
Locate and correct the invalid configuration item and try again.

DPWWA2076E

Failed to construct a credential from a PAC supplied by an EAI server. Major status = 0x*%x*, minor status = 0x*%x*. (0x38cf081c)

Explanation
An EAI server constructed a PAC to authenticate a user, but the PAC could not be converted to a credential.

Administrator response
Investigate the PAC construction and verify that the PAC data is valid for IBM Security Verify Access.

DPWWA2077E

Could not authenticate user. An EAI server returned invalid authentication data. (0x38cf081d)

Explanation
An EAI server failed to return proper authentication data in an authentication response. This is typically due to a misconfigured EAI server.

Administrator response
Investigate and correct any problems with the authentication headers returned by the EAI server.

DPWWA2078E

Could not authenticate user. An external authentication service did not return required authentication data. (0x38cf081e)

Explanation
An EAI server did not return required authentication data in an authentication response. This is typically due to a misconfigured EAI server not returning attributes that it must return.

Administrator response
Investigate and correct any problems with the authentication headers returned by the EAI server.

DPWWA2079E

Configuration of the SSO create and/or consume authentication module(s) failed: *%s*'. (0x38cf081f)

Explanation
ECSSO and/or CDSSO is configured to create and/or consume authentication tokens, but the modules could not be configured. This means that they are either not properly loaded, or there is a fatal problem with the current configuration settings.

Administrator response
Ensure that the sso-create/sso-consume libraries are properly specified in the configuration file.

DPWWA2080E

The session inactivity timestamp is missing from the failover cookie. (0x38cf0820)

Explanation
WebSEAL is configured to require inactivity timestamps in all received failover cookies, and a failover cookie was received that did not have the session inactivity timestamp.

Administrator response
Set failover-validate-inactivity-timestamp to optional.

DPWWA2081E

The session lifetime timestamp is missing from the failover cookie. (0x38cf0821)

Explanation
WebSEAL is configured to require lifetime timestamps in all received failover cookies, and a failover cookie was received that did not have the session inactivity timestamp.

Administrator response
Set failover-validate-lifetime-timestamp to optional.

DPWWA2082E

This system error code could not be converted to an error string. (0x38cf0822)

Explanation
The system error code has no equivalent error string.

Administrator response
No action is required.

DPWWA2083E

The shared library could not be opened. (0x38cf0823)

Explanation
The shared library could not be opened.

Administrator response
Examine earlier messages in the log containing this message to identify the module that could not be opened. Check that the identified library exists and is found within the configured library path.

DPWWA2084E

Could not find the requested symbol. (0x38cf0824)

Explanation
The requested symbol was not found within the shared library.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2085E

The shared library file '*%s*' could not be opened: *%s* (0x38cf0825)

Explanation
The specified shared library file could not be opened. The system error string is given.

Administrator response
Ensure the specified shared library file exists and has appropriate permissions. Restart the process.

DPWWA2086E

The symbol '*%s*' could not be resolved in the shared library '*%s*': *%s* (0x38cf0826)

Explanation
The specified symbol could not be resolved. The system error string is given.

Administrator response
Ensure the specified shared library file is the appropriate type of library file. Restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2087E

The '*%s*' flag to the authentication module requires an argument. (0x38cf0827)

Explanation
The authentication module flag must have an argument.

Administrator response
Add an argument to the specified flag.

DPWWA2088E

Unknown authentication module flag '*%s*'. (0x38cf0828)

Explanation
An invalid option was provided to the authentication module.

Administrator response
Provide correct authentication module option.

DPWWA2089E

The authentication module flag '*%s*' requires an integer argument. (0x38cf0829)

Explanation
The argument of the authentication module flag must be an integer.

Administrator response
Ensure that the argument of the authentication module flag is an integer.

DPWWA2090E

The session activity timestamp is missing from the failover cookie. (0x38cf082a)

Explanation
WebSEAL is configured to require activity timestamps in all received failover cookies, and a failover cookie was received that did not have the session activity timestamp.

Administrator response
Set failover-require-activity-timestamp-validation to no.

DPWWA2091E

Bad EAI trigger URL pattern '*%s*' in configuration file. (0x38cf082b)

Explanation
The EAI trigger is not formatted correctly. If it is a Virtual Host junction trigger it must begin with HTTP[S]://hostname[:port]/.

Administrator response
Correct the syntax of the EAI trigger.

DPWWA2092E

Could not reset the cache session lifetime because the EAI server provided a bad value ('*%s*') in the 'am_eai_xattr_session_lifetime' header. (0x38cf082c)

Explanation
WebSEAL could not reset the cache session lifetime because the header value returned by the EAI server is invalid. The value must contain only numeric digits.

Administrator response
Investigate and correct any problems with the 'am_eai_xattr_session_lifetime' extended attribute header returned by the EAI server.

DPWWA2093E

Configuration item '[*%s*]*%s*' has an invalid value '*%s*' (0x38cf082d)

Explanation
A configuration item in the configuration file has a bad value. For example it is expecting an integer and was provided with a string

Administrator response
The configuration item should be changed to a valid entry

DPWWA2094E

The login-success-pattern with the header pattern '*%s*' is invalid (0x38cf082e)

Explanation
Check the value of the login-success-pattern configuration entry and ensure all rules are well formed.

Administrator response
Provide a correct value for the login-success-pattern

DPWWA2095E

The login-success-pattern with the pattern '*%s*' is invalid (0x38cf082f)

Explanation
Check the value of the login-success-pattern configuration entry and ensure all rules are well formed.

Administrator response
Provide a correct value for the login-success-pattern

DPWWA2096E

At least one login success rule must be defined (0x38cf0830)

Explanation
No login success rules were defined in the configuration file

Administrator response
Provide a value for the login-success-pattern

DPWWA2100E

The new user ID does not match the user ID previously presented to authenticate. (0x38cf0834)

Explanation
In the event of a step-up operation with verify-step-up-user set to true, the user ID presented to this authentication level must match the user ID authenticated to the previous level.

Administrator response
The user must present the same user ID provided in the previous authentication level.

DPWWA2101E

The new user ID (*%s*) does not match the user ID (*%s*)previously presented to authenticate. (0x38cf0835)

Explanation
In the event of a step-up operation with verify-step-up-user set to true, the user ID presented to this authentication level must match the user ID authenticated to the previous level.

Administrator response
The user must present the same user ID provided in the previous authentication level.

DPWWA2250E

The ACL attached to the requested resource does not permit the Traverse operation. (0x38cf08ca)

Explanation
The ACL attached to the requested resource does not permit the Traverse operation.

Administrator response
Modify the ACL if necessary, or inform the user that they are not permitted to access the resource.

DPWWA2251E

The ACL attached to the requested resource does not allow access by this user. (0x38cf08cb)

Explanation
The ACL attached to the requested resource does not allow access by the client.

Administrator response
Modify the ACL if necessary, or inform the user that they are not permitted to access the resource.

DPWWA2252E

The requested resource is protected by a policy that restricts access to specific time periods. This request is prohibited at this time. (0x38cf08cc)

Explanation
A time-of-day POP is attached to the requested resource that has prohibited access at the time of the request.

Administrator response
Modify the POP if necessary, or inform the user of the policy details.

DPWWA2253E

An External Authorization Server has denied access to the requested resource. (0x38cf08cd)

Explanation
An External Authorization Server has denied access to the requested resource.

Administrator response
Modify the EAS if necessary, or inform the user that they are not permitted to access the resource.

DPWWA2254E

The requested resource is protected by a policy that restricts access to specific clients. This request is prohibited for this client. (0x38cf08ce)

Explanation
Step-up is configured for the requested resource, but the client IP address is forbidden to step-up.

Administrator response
Modify the POP if necessary, or inform the user that they are not permitted to access the resource.

DPWWA2255E

This user does not have permissions to perform a delegated operation. (0x38cf08cf)

Explanation
This user does not have permissions to perform a delegated operation.

Administrator response
Modify the ACL attached to the resource to grant the user delegation permissions, or inform the user that they are not permitted to perform the requested operation.

DPWWA2400E

Invalid challenge header (0x38cf0960)

Explanation
SPNEGO Authentication requires decoding a challenge header from the client. That header had an invalid format.

Administrator response
Make sure that the client is one supported by WebSEAL.

DPWWA2401E

An internal error occurred during SPNEGO processing. (0x38cf0961)

Explanation
SPNEGO authentication failed because of an internal error. This indicates a serious problem.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2402E

Initialization of Kerberos authentication failed. (0x38cf0962)

Explanation
Initialization of Kerberos authentication failed.

Administrator response
Check for additional error messages in log files. Check your SPNEGO configuration entries to make sure they match the documentation.

DPWWA2403E

Your browser supplied NTLM authentication data. NTLM is not supported by WebSEAL. Make sure your browser is configured to use Integrated Windows Authentication. (0x38cf0963)

Explanation
If a browser is improperly unconfigured, it will supply NTLM authentication data instead of SPNEGO data.

Administrator response
Make sure that the browser is located in the same domain as the WebSEAL server. Refer to your browser documentation to make sure it is configured properly for Integrated Windows Authentication.

DPWWA2404E

An error occurred when creating the SPNEGO token. (0x38cf0964)

Explanation
An error occurred when creating the SPNEGO token for the GSS-API token.

Administrator response
This problem is most likely due to an internal error or misconfiguration. Check the SPNEGO related configuration items in your server for errors.

DPWWA2405W

Cannot update failover cookie for switch-user admins (0x38cf0965)

Explanation
A switch-user admin cannot get a failover cookie for the user impersonated; this is a known limitation of failover with switch-user

Administrator response
No action is required.

DPWWA2406W

Could not find the failover session ID in the user's failover token (0x38cf0966)

Explanation
A user is trying to authenticate with a failover token that should have a session ID encoded from another WebSEAL replica. The session ID is missing from the token, indicating a configuration error at one of the replicas.

Administrator response
Ensure failover-include-session-id configuration settings are correct.

DPWWA2407W

The failover session ID in the user's failover token does not match the session ID in the user's session cookie. (0x38cf0967)

Explanation
When trying to establish a session with failover-include-session-id enabled, the session ID stored in the session cookie and the user's failover token must match. A mismatch indicates a possible security breach. WebSEAL will issue new session and failover cookies for the user.

Administrator response
Ensure failover-include-session-id configuration settings are correct.

DPWWA2408W

Cannot find the session cookie in the user's request for use in comparing with the failover cookie. (0x38cf0968)

Explanation
When attempting to establish a nonsticky failover session, WebSEAL could not find the user's session cookie. The cookie is required for a comparison with the session id in the failover token. Ensure configuration settings are correct.

Administrator response
Check cookie and nonsticky failover settings.

DPWWA2409W

Reverse lookup for host '*%s*' returned an alternate host name '*%s*'. This might prevent SPNEGO authentication from functioning properly. (0x38cf0969)

Explanation
The SPNEGO authentication module attempted to validate the SPNEGO principal name by checking that the reverse lookup for the specified host name resolves to the same host name as the original. The host name returned for the reverse lookup did not match the original host name.

Administrator response
If server startup succeeds and SPNEGO authentication functions properly, no action need be taken. If there are problems with SPNEGO authentication, make sure that your host name resolution is properly configured. Refer to the Verify Access WebSEAL Administration Guide for additional information about the problem.

DPWWA2410E

Initialization of Kerberos authentication for server principal '*%s*' failed. (0x38cf096a)

Explanation
Initialization of Kerberos authentication for the specified principal failed.

Administrator response
Check for additional error messages in log files. Refer to the Verify Access WebSEAL Administration Guide for additional information.

DPWWA2411E

No SPNEGO service principal credential found for Virtual Host Junction '*%s*'. (0x38cf096b)

Explanation
SPNEGO authentication cannot complete unless the SPNEGO keytab file contains a service principal matching the host name of the virtual host junction and the service principal is listed in the WebSEAL configuration file.

Administrator response
Verify that the client is using the correct hostname to contact the virtual host. Verify that the WebSEAL configuration file contains an entry '[spnego]spnego-krb-service-name = HTTP@<hostname>' for the virtual host. The SPNEGO keytab file must contain a key for the principal.

DPWWA2550E

Error initializing the credential policy entitlements service (0x38cf09f6)

Explanation
An error occurred when loading the credential policy entitlements service.

Administrator response
Check the log file for additional error messages. The other error messages contain more information about the problem.

DPWWA2551E

Policy retrieval for user *%s* failed: *%s* (error code: 0x*%lx*) (0x38cf09f7)

Explanation
An error occurred when trying to retrieve credential policy attributes for the specified user.

Administrator response
Examine the status message and code embedded in this message to identify the root cause of the problem.

DPWWA2734W

The authentication type is unknown. The audit event will not be recorded. (0x38cf0aae)

Explanation
An authentication event has occurred. However, the authentication type utilized is not a known value and, as such, the audit event will not be recorded.

Administrator response
No action is required

DPWWA2735W

The reason for the session termination is unknown. The audit event will not be recorded. (0x38cf0aaf)

Explanation
A session has been terminated. The reason for this termination, however, is unknown. Because of this the audit record of this event could be considered broken and, as such, will not be audited.

Administrator response
No action is required

DPWWA2850E

A general failure has occurred within the SOAP client. (0x38cf0b22)

Explanation
An error has occurred within the SOAP client.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2851E

An error was returned from the SOAP server in cluster *%s* when calling the *%s* interface: *%s* (code: 0x*%x*). (0x38cf0b23)

Explanation
The web service returned an error.

Administrator response
Examine messages within the session management server log. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2852E

An error occurred when attempting to communicate with the SOAP server URL *%s*: *%s* (error code: *%d*/0x*%x*). (0x38cf0b24)

Explanation
An attempt was made to communicate with the SOAP server and a failure occurred within the underlying communications layer.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. Ensure that the SOAP server is running and reachable. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWA2853E

The SOAP client failed to initialized. (0x38cf0b25)

Explanation
The SOAP client for a Web service could not be initialized.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

DPWWM1299E

Invalid flag '-*%c*' (0x38cfc513)

Explanation
An invalid flag was passed to a command.

Administrator response
Read the manual to identify the flag you want to use.

DPWWM1300E

Flag '-*%c*' does not take an argument (0x38cfc514)

Explanation
An invalid argument was passed to a command.

Administrator response
Correct the syntax of the command.

DPWWM1301E

Missing argument for '-*%c*' flag (0x38cfc515)

Explanation
An argument is required for the option used.

Administrator response
Correct the syntax of the command.

DPWWM1302E

Basic authentication type must be one of: ignore, filter,supply or gso (0x38cfc516)

Explanation
An invalid argument followed the -b flag.

Administrator response
Correct the syntax of the command.

DPWWM1314E

Must specify the junction type using the '-t' flag (0x38cfc522)

Explanation
The junction type was not passed with the create command.

Administrator response
Pass the junction type as an argument to the -t flag.

DPWWM1315E

Must specify a junction point (0x38cfc523)

Explanation
No junction point was passed as an argument.

Administrator response
Correct the syntax of the command.

DPWWM1316W

WARNING: A junction already exists at *%s* (0x38cfc524)

Explanation
A junction already exists at the specified junction point.

Administrator response
Either replace the existing junction or specify a different junction point.

DPWWM1318E

Cannot create junction (0x38cfc526)

Explanation
A junction create command failed.

Administrator response
This message is preceded by a detailed explanation of why the junction could not be created. Correct the problem and try to create the junction again.

DPWWM1320E

Must specify the junction server hostname using the '-h' flag (0x38cfc528)

Explanation
No hostname was passed to the add or create command.

Administrator response
Include the hostname in the command.

DPWWM1321E

Invalid port *%s* (0x38cfc529)

Explanation
The port number specified was invalid. Port numbers must be integers greater than zero.

Administrator response
Specify a valid port number.

DPWWM1322E

Invalid proxy port *%s* (0x38cfc52a)

Explanation
An invalid port number was passed using the -P flag. Port numbers must be integers greater than zero.

Administrator response
Pass a valid port number to the create or add command.

DPWWM1323E

A proxy TCP port must be supplied with the -P option (0x38cfc52b)

Explanation
No -P argument was specified to the add or create command even though the -H argument was specified.

Administrator response
Include the -P argument in the command.

DPWWM1324E

Can only use -T flag when using '-b gso' (0x38cfc52c)

Explanation
The -T flag was specified to the create command without the -b flag.

Administrator response
If you want to use GSO for the junction, pass -b gso as an argument to the junction create command. If you do not want to use GSO, then do not pass the -T flag to the create command.

DPWWM1325E

Must also use -T flag when using '-b gso' (0x38cfc52d)

Explanation
The -b gso flag was passed to the create command without a corresponding -T flag.

Administrator response
Include the name of the GSO target which should be used for the junction.

DPWWM1327E

Must specify a file system directory using the '-d' flag (0x38cfc52f)

Explanation
No directory was specified when trying to create a local junction.

Administrator response
If you want to create a local junction, pass the full path to the directory to use with the -d flag. If you want to create another type of junction, pass the correct type using the -t flag.

DPWWM1330E

Must specify a server to remove using the '-i' flag (0x38cfc532)

Explanation
No -i flag was passed to the 'remove' command.

Administrator response
If you want to delete the junction entirely, use the 'delete' command. If you want to remove a particular server, use the 'show' command to loook up the UUID of the server to remove, and then pass the UUID as the argument to the -i flag.

DPWWM1332E

Invalid server ID (0x38cfc534)

Explanation
The argument passed to -i was not a valid UUID.

Administrator response
Obtain the correct UUID by using the 'show' command and pass a valid UUID as an argument to the 'remove' command.

DPWWM1333E

Could not fetch junction definition (0x38cfc535)

Explanation
This message is followed by an explanation of the problem.

Administrator response
Correct the problem described by the following message.

DPWWM1334E

Can only remove servers from a TCP, SSL or mutual junction (0x38cfc536)

Explanation
It is not possible to remove a server from a local junction.

Administrator response
Correct the junction point specified in the remove command. The junction point should belong to a TCP, SSL or mutual junction.

DPWWM1335E

Server *%s* not found at junction *%s* (0x38cfc537)

Explanation
An attempt was made to remove a junction server based on a UUID which did not match any of the servers on the junction point.

Administrator response
Use the 'show' command to find the correct UUID and pass the correct UUID to the 'remove' command.

DPWWM1336E

Could not delete junction (0x38cfc538)

Explanation
This message is followed by an explanation of why the junction could not be deleted.

Administrator response
Correct the problem described in the message displayed after this message.

DPWWM1337E

Could not update junction (0x38cfc539)

Explanation
This message is followed by an explanation of why the junction could not be modified.

Administrator response
Correct the problem described in the message displayed after this message.

DPWWM1339E

Junction not found at *%s*. (0x38cfc53b)

Explanation
An attempt was made to add or remove a server from a junction point which does not exist.

Administrator response
Use the 'list' and 'show' commands to figure out which junction point you should use.

DPWWM1341E

Create junction (0x38cfc53d)

Explanation
This message is followed by an explanation of why the creation failed.

Administrator response
Fix the problem described in the message following this message.

DPWWM1342E

Can't add servers to this type of junction (0x38cfc53e)

Explanation
It is not possible to add servers to local junctions.

Administrator response
Only add servers to TCP, SSL, TCP proxy, SSL proxy or mutual junctions. Figure out which junction you wish to add a server to using the 'list' and 'show' commands, and then pass the correct junction point to the 'add' command.

DPWWM1343E

Add server (0x38cfc53f)

Explanation
An attempt to add a server failed.

Administrator response
This message is followed by an explanation of why the server could not be added. Correct the problem.

DPWWM1345E

Cannot list junctions (0x38cfc541)

Explanation
This message is followed by an explanation of why junctions could not be listed. Correct the problem described in that message.

Administrator response
Correct the problem described in the following message.

DPWWM1346E

Cannot show junction (0x38cfc542)

Explanation
This message is followed by an explanation of the problem. Correct the problem described in that message.

Administrator response
Correct the problem described in the following message.

DPWWM1392E

Bad value for path attribute. (0x38cfc570)

Explanation
An item from a configuration file which should be set to a path name is an empty string instead.

Administrator response
Add the path to the configuration file.

DPWWM1416E

Error: No filename specified in request. (0x38cfc588)

Explanation
WebSEAL was unable to locate a template file to return to the user. The file may have been specified using the /pkms.....?filename=name.html construct or may have been one of the default response files.

Administrator response
If the link which produced this error was a PKMS page that included a ?filename=-name- query, make sure the format of the query portion of the link is correct. If the link which produced this error was not a PKMS page that included a file name specification, make sure that all files in the www/lib/-lang- directories are readable by the ivmgr user (on UNIX systems) or by all users (on Windows systems.)

DPWWM1417E

Error: Could not retrieve file data. (0x38cfc589)

Explanation
WebSEAL was unable to locate a template file to return to the user. The file may have been specified using the /pkms.....?filename=name.html construct or may have been one of the default response files.

Administrator response
If the link which produced this error was a PKMS page that included a ?filename=-name- query, verify that the file specified by -name- is located in the www/lib/-lang- (where -lang- is the language appropriate to the user's browser) directory and is readable by the ivmgr user (on UNIX systems) or by all users (on Windows systems.) If the link which produced this error was not a PKMS page that included a file name specification, make sure that all files in the www/lib/-lang- directories are readable by the ivmgr user (on UNIX systems) or by all users (on Windows systems.)

DPWWM1419E

You can only use the -u flag with a stateful junction. (0x38cfc58b)

Explanation
The -u flag was passed to the add or create command without the -s flag. UUIDs can only be specified for stateful junctions.

Administrator response
If you wish to specify the UUID of the junction, then specify the -s flag as well as the -u flag.

DPWWM1420E

The UUID specified with the -u flag is in an invalid format. (0x38cfc58c)

Explanation
An invalid UUID was specified with the -u flag to the 'add' or 'create' commands.

Administrator response
Correct the format of the UUID. If you are unsure of the proper format for a UUID, examine the output of the 'show' command for a junction. The 'ID' entry will contain a valid UUID.

DPWWM1427E

-D flag only supported with ssl, sslproxy or mutual junctions. (0x38cfc593)

Explanation
The -D flag can only be used for SSL, SSL proxy or mutual junctions.

Administrator response
Either make this an SSL/SSL Proxy or Mutual junction or do not specify the DN of the junctioned server.

DPWWM1432W

NOTE: Ensure the CA root certificate used to sign the junctioned server certificate is installed in the WebSEAL certificate key database. (0x38cfc598)

Explanation
WebSEAL was unable to communicate with an SSL junction because the junction presented a certificate WebSEAL could not validate.

Administrator response
See message.

DPWWM1435E

-C flag only supported with ssl or sslproxy junctions. (0x38cfc59b)

Explanation
The -C flag can only be used for SSL or SSL proxy junctions.

Administrator response
Either make this an SSL or SSL Proxy junction or do not make the junction a WebSEAL to WebSEAL junction.

DPWWM1436E

Either -K or -B can be defined for a junction. (0x38cfc59c)

Explanation
Both -K and -B were specified in the junction creation command. The two options cannot be used simultaneously on the same junction.

Administrator response
Read the manual and figure out whether you want to use -K, -B, or neither.

DPWWM1437E

Both -K and -B flag only supported with ssl, sslproxy or mutual junctions. (0x38cfc59d)

Explanation
The -K and -B flags can only be used for SSL, SSL proxy or mutual junctions.

Administrator response
Either make this an SSL/SSL Proxy or Mutual junction or do not make the junction mutually authenticated.

DPWWM1438E

The -b option cannot be specified with the -B option. (0x38cfc59e)

Explanation
Both -b and -B were specified in the junction creation command. The two options cannot be used simultaneously on the same junction.

Administrator response
Read the manual and figure out whether you want to use -b, -B, or neither.

DPWWM1439E

-U <username> and -W <password> must be supplied with the -B option. (0x38cfc59f)

Explanation
The -B flag was specified without the -U and -W flags.

Administrator response
Specify the username and password for the junction with the -U and -W flags.

DPWWM1451W

Too few authentication methods configured. (0x38cfc5ab)

Explanation
Too few authentication methods have been specified.

Administrator response
Add 1 or more authentication methods to the authentication levels stanza configuration.

DPWWM1452W

No unauthenticated method configured. (0x38cfc5ac)

Explanation
The unauthenticated method has not been specified

Administrator response
Ensure that the unauthenticated method occurs first in the authentication levels stanza configuration.

DPWWM1453E

Invalid authentication method. (0x38cfc5ad)

Explanation
The specified authentication method is either invalid or unsupported in the current product configuration.

Administrator response
Verify the validity of the specified authentication method.

DPWWM1454E

The requested operation is not valid (0x38cfc5ae)

Explanation
IBM Security Verify Access was unable to perform a requested operation beca use it is not valid. An example would be a token authentication user attempting to change their password

Administrator response
Consult documentation for operation.

DPWWM1461E

Failed loading JMT table (0x38cfc5b5)

Explanation
The JMT file could not be read from disk.

Administrator response
Make sure the JMT file specifed in webseald.conf is present in the installation directory and is readable by the ivmgr user.

DPWWM1490E

No dynurl.conf file found. No changes were made. (0x38cfc5d2)

Explanation
No dynurl.conf file was present when the dynurl update command was issued.

Administrator response
Create the dynurl.conf file.

DPWWM1493E

Junction '*%s*' has reached it's worker thread hard limit. (0x38cfc5d5)

Explanation
The configured maximum number of worker threads for this junction has been reached. The overloaded requests are being retured with 503, Service Unavailable. This could be due to either a slow junction or too many requests.

Administrator response
Increase number of worker threads, increase hard limit or decrease load.

DPWWM1494W

Junction '*%s*' has reached it's worker thread soft limit (0x38cfc5d6)

Explanation
A configured warning level has been reached for this junction on the number of worker threads currently active on it. This could be due to either a slow junction or too many requests.

Administrator response
Prepare to increase number of worker threads, increase soft limit or decrease load.

DPWWM1499W

The configured number of worker threads, *%d*, is greater than the system can support, *%d*. It has automatically been reduced. (0x38cfc5db)

Explanation
Each operation system has different levels of support for threads and open files. That combined with compile time options will provide limits on the configurable number of worker threads.

Administrator response
The software automatically reduced the value. However to stop this message appearing you may set the value in the configuration file lower.

DPWWM1510E

One or more entries in dynurl.conf do not specify URLs (0x38cfc5e6)

Explanation
See message.

Administrator response
Examine dynadi.conf for formatting and content errors.

DPWWM1513W

The stanza '*%s*' in the configuration file contains an unrecognised P3P compact policy element: '*%s*'. (0x38cfc5e9)

Explanation
The given entry is not a valid P3P HTTP header configuration entry.

Administrator response
Correct the configuration file entry. The list of valid P3P compact policy elements is given in the documentation.

DPWWM1514W

The stanza '*%s*' in the configuration file contains an unrecognised value for the P3P compact policy element '*%s*': '*%s*'. (0x38cfc5ea)

Explanation
The specified P3P HTTP header configuration entry contains an invalid value.

Administrator response
Correct the configuration file entry. The list of accepted values for each P3P compact policy element is given in the documentation.

DPWWM1515E

The configuration for P3P HTTP header insertion is invalid. (0x38cfc5eb)

Explanation
One or more aspects of the P3P HTTP header configuration are invalid. Earlier log messages give more specific details.

Administrator response
Examine other log messages to determine the specific error or errors in the configuration file, and correct the configuration.

DPWWM1516W

No P3P policy elements are configured in the stanza '*%s*', but P3P header insertion has been enabled. (0x38cfc5ec)

Explanation
P3P header insertion has been enabled in the configuration file, but no P3P policy has been configured. P3P headers cannot be inserted until the P3P policy is configured.

Administrator response
Either add P3P policy elements to the stanza, or disable P3P header insertion.

DPWWM1517E

The -H and -P flags are valid only for tcpproxy and sslproxy type junctions. (0x38cfc5ed)

Explanation
The -H and -P parameters are only valid for tcpproxy or sslproxy type junctions. Either create one of those types of junctions or remove the -H and -P parameters from this command.

Administrator response
Create a tcpproxy or sslproxy type junction.

DPWWM1518E

A proxy hostname must be supplied with the -H option (0x38cfc5ee)

Explanation
No -H argument was specified to the add or create command even though the -P argument was specified.

Administrator response
Include the -H argument in the command.

DPWWM1522E

Only 'onfocus', 'inhead', 'xhtml10' and 'trailer' are supported with the -J option. (0x38cfc5f2)

Explanation
An invalid option was supplied with the -J flag.

Administrator response
Correct the syntax of the command.

DPWWM1523E

You can not specify both -C and -B flags when creating a junction. (0x38cfc5f3)

Explanation
The -C and -B flags use the same method to transmit authentication data and thus would overwrite each other if used together.

Administrator response
Do not specify both flags when creating the junction.

DPWWM1524E

The -P flag is valid only for mutual, tcpproxy and sslproxy type junctions. (0x38cfc5f4)

Explanation
The -P parameter is only valid for mutual, tcpproxy or sslproxy type junctions. Either create one of those types of junctions or remove the -P parameter from this command.

Administrator response
Create a mutual, tcpproxy or sslproxy type junction.

DPWWM1527E

The supplied TCP and SSL ports must be different. (0x38cfc5f7)

Explanation
The TCP and SSL port values which have been supplied point to the same port. This is not a valid configuration.

Administrator response
Specify different port values for the TCP and SSL port options.

DPWWM1528E

The -V flag is valid only for mutual junctions. (0x38cfc5f8)

Explanation
The -V parameter is only valid for mutual type junctions. Either create one of those types of junctions or remove the -V parameter from this command.

Administrator response
Remove the -V flag or create a mutual type of junction.

DPWWM1531W

Error: The supplied keyfile must not contain any path information. (0x38cfc5fb)

Explanation
A base path for LTPA keyfiles has been statically configured and as such the supplied file name should not contain any path information.

Administrator response
Specify the name of the keyfile without any path information.

DPWWM1532W

Error: The supplied FSSO configuration file must not contain any path information. (0x38cfc5fc)

Explanation
A base path for FSSO configuration files has been statically configured and as such the supplied file name should not contain any path information.

Administrator response
Specify the name of the FSSO configuration file without any path information.

DPWWM2041E

Cannot create Virtual Host Junction (0x38cfc7f9)

Explanation
A virtualhost create command failed.

Administrator response
This message is preceded by a detailed explanation of why the Virtual Host Junction could not be created. Correct the problem and try to create the Virtual Host Junction again.

DPWWM2044E

Create Virtual Host Junction (0x38cfc7fc)

Explanation
This message is followed by an explanation of why the creation failed.

Administrator response
Fix the problem described in the message following this message.

DPWWM2045E

Can't add servers to this type of Virtual Host Junction (0x38cfc7fd)

Explanation
It is not possible to add servers to local Virtual Host Junctions.

Administrator response
Only add servers to TCP, SSL, TCP proxy, or SSL proxy Virtual Host Junctions. Figure out which Virtual Host Junction you wish to add a server to using the 'virtualhost list' and 'virtualhost show' commands, and then pass the correct Virtual Host Junction label to the 'virtualhost add' command.

DPWWM2047E

Must specify the Virtual Host Junction type using the '-t' flag (0x38cfc7ff)

Explanation
The Virtual Host Junction type was not passed with the create command.

Administrator response
Pass the Virtual Host Junction type as an argument to the -t flag.

DPWWM2050W

WARNING: A Virtual Host Junction already exists using label *%s* (0x38cfc802)

Explanation
A Virtual Host Junction already exists using the specified Virtual Host Junction label.

Administrator response
Either replace the existing Virtual Host Junction or specify a different Virtual Host Junction label.

DPWWM2051E

-C flag only supported with ssl or sslproxy Virtual Host Junctions. (0x38cfc803)

Explanation
The -C flag can only be used for SSL or SSL proxy Virtual Host Junctions.

Administrator response
Either make this an SSL/SSL Proxy Virtual Host Junction or do not make the Virtual Host Junction a WebSEAL to WebSEAL Virtual Host Junction.

DPWWM2052E

Can only use -T flag when using '-b gso' (0x38cfc804)

Explanation
The -T flag was specified to the virtualhost create command without the -b flag.

Administrator response
If you want to use GSO for the Virtual Host Junction, pass -b gso as an argument to the virtualhost create command. If you do not want to use GSO, then do not pass the -T flag to the virtualhost create command.

DPWWM2053E

Must also use -T flag when using '-b gso' (0x38cfc805)

Explanation
The -b gso flag was passed to the virtualhost create command without a corresponding -T flag.

Administrator response
Include the name of the GSO target which should be used for the Virtual Host Junction.

DPWWM2054E

Either -K or -B can be defined for a Virtual Host Junction. (0x38cfc806)

Explanation
Both -K and -B were specified in the virtualhost create command. The two options cannot be used simultaneously on the same Virtual Host Junction.

Administrator response
Read the manual and figure out whether you want to use -K, -B, or neither.

DPWWM2055E

Both -K and -B flag only supported with ssl or sslproxy Virtual Host Junctions. (0x38cfc807)

Explanation
The -K and -B flags can only be used for SSL or SSL proxy Virtual Host Junctions.

Administrator response
Either make this an SSL/SSL Proxy Virtual Host Junction or do not make the Virtual Host Junction mutually authenticated.

DPWWM2056E

-U <username> and -W <password> must be supplied with the -B option. (0x38cfc808)

Explanation
The -B flag was specified without the -U and -W flags.

Administrator response
Specify the username and password for the Virtual Host Junction with the -U and -W flags.

DPWWM2057E

The -b option cannot be specified with the -B option. (0x38cfc809)

Explanation
Both -b and -B were specified in the virtualhost create command. The two options cannot be used simultaneously on the same Virtual Host Junction.

Administrator response
Read the manual and figure out whether you want to use -b, -B, or neither.

DPWWM2058E

Must specify the Virtual Host Junction server hostname using the '-h' flag (0x38cfc80a)

Explanation
No hostname was passed to the virtualhost add or create command.

Administrator response
Include the hostname in the command.

DPWWM2059E

The -H and -P flags are valid only for tcpproxy and sslproxy type Virtual Host Junctions. (0x38cfc80b)

Explanation
The -H and -P parameters are only valid for tcpproxy or sslproxy type Virtual Host Junctions. Either create one of those types of Virtual Host Junctions or remove the -H and -P parameters from this command.

Administrator response
Create a tcpproxy or sslproxy type Virtual Host Junction.

DPWWM2060E

A proxy hostname must be supplied with the -H option (0x38cfc80c)

Explanation
No -H argument was specified to the virtualhost add or create command even though the -P argument was specified.

Administrator response
Include the -H argument in the command.

DPWWM2062E

You can only use the -u flag with a stateful Virtual Host Junction. (0x38cfc80e)

Explanation
The -u flag was passed to the virtualhost add or create command without the -s flag. UUIDs can only be specified for stateful Virtual Host Junctions.

Administrator response
If you wish to specify the UUID of the Virtual Host Junction, then specify the -s flag as well as the -u flag.

DPWWM2063E

-D flag only supported with ssl or sslproxy Virtual Host Junctions. (0x38cfc80f)

Explanation
The -D flag can only be used for SSL or SSL proxy Virtual Host Junctions.

Administrator response
Either make this an SSL/SSL Proxy Virtual Host Junction or do not specify the DN of the Virtual Host Junctioned server.

DPWWM2064E

The UUID specified with the -u flag is in an invalid format. (0x38cfc810)

Explanation
An invalid UUID was specified with the -u flag to the 'virtualhost add' or 'virtualhost create' commands.

Administrator response
Correct the format of the UUID. If you are unsure of the proper format for a UUID, examine the output of the 'virtualhost show' command for a Virtual Host Junction. The 'ID' entry will contain a valid UUID.

DPWWM2065W

NOTE: Ensure the CA root certificate used to sign the Virtual Host Junctioned server certificate is installed in the WebSEAL certificate key database. (0x38cfc811)

Explanation
WebSEAL was unable to communicate with an SSL Virtual Host Junction because the Virtual Host Junction presented a certificate WebSEAL could not validate.

Administrator response
See message.

DPWWM2067E

Must specify a virtual hostname using the '-v' flag (0x38cfc813)

Explanation
No virtual hostname was specified when trying to create a localtcp or localssl Virtual Host Junction.

Administrator response
If you want to create a localtcp or localssl Virtual Host Junction, you must set it's virtual hostname using the -v flag.

DPWWM2068E

Must specify a file system directory using the '-d' flag (0x38cfc814)

Explanation
No directory was specified when trying to create a localtcp or localssl Virtual Host Junction.

Administrator response
If you want to create a localtcp or localssl Virtual Host Junction, pass the full path to the directory to use with the -d flag. If you want to create another type of Virtual Host Junction, pass the correct type using the -t flag.

DPWWM2069E

Must specify a server to remove using the '-i' flag (0x38cfc815)

Explanation
No -i flag was passed to the 'virtualhost remove' command.

Administrator response
If you want to delete the Virtual Host Junction entirely, use the 'virtualhost delete' command. If you want to remove a particular server, use the 'virtualhost show' command to loook up the UUID of the server to remove, and then pass the UUID as the argument to the -i flag.

DPWWM2071E

Could not delete Virtual Host Junction (0x38cfc817)

Explanation
This message is followed by an explanation of why the Virtual Host Junction could not be deleted.

Administrator response
Correct the problem described in the message displayed after this message.

DPWWM2072E

Invalid server ID (0x38cfc818)

Explanation
The argument passed to -i was not a valid UUID.

Administrator response
Obtain the correct UUID by using the 'virtualhost show' command and pass a valid UUID as an argument to the 'virtualhost remove' command.

DPWWM2073E

Virtual Host Junction not found with label *%s*. (0x38cfc819)

Explanation
An attempt was made to add or remove a server from a Virtual Host Junction which does not exist.

Administrator response
Use the 'virtualhost list' and 'virtualhost show' commands to figure out which Virtual Host Junction point you should use.

DPWWM2074E

Could not fetch Virtual Host Junction definition (0x38cfc81a)

Explanation
This message is followed by an explanation of the problem.

Administrator response
Correct the problem described by the following message.

DPWWM2075E

Can only remove servers from a TCP or SSL Virtual Host Junction (0x38cfc81b)

Explanation
It is not possible to remove a server from a local Virtual Host Junction.

Administrator response
Correct the Virtual Host Junction label specified in the remove command. The Virtual Host Junction label should belong to a TCP or SSL Virtual Host Junction.

DPWWM2076E

Server *%s* not found at Virtual Host Junction *%s* (0x38cfc81c)

Explanation
An attempt was made to remove a Virtual Host Junction server based on a UUID which did not match any of the servers on the Virtual Host Junction.

Administrator response
Use the 'virtualhost show' command to find the correct UUID and pass the correct UUID to the 'virtualhost remove' command.

DPWWM2077E

Could not update Virtual Host Junction (0x38cfc81d)

Explanation
This message is followed by an explanation of why the Virtual Host Junction could not be modified.

Administrator response
Correct the problem described in the message displayed after this message.

DPWWM2080E

Cannot list Virtual Host junctions (0x38cfc820)

Explanation
This message is followed by an explanation of why Virtual Host junctions could not be listed. Correct the problem described in that message.

Administrator response
Correct the problem described in the following message.

DPWWM2081E

Cannot show Virtual Host Junction (0x38cfc821)

Explanation
This message is followed by an explanation of the problem. Correct the problem described in that message.

Administrator response
Correct the problem described in the following message.

DPWWM2088E

Must specify a Virtual Host Junction label (0x38cfc828)

Explanation
No Virtual Host Junction label was passed as an argument.

Administrator response
Correct the syntax of the command.

DPWWM2089E

A Virtual Host Junction label cannot contain the '/' character (0x38cfc829)

Explanation
See text.

Administrator response
Correct the syntax of the command and try again.

DPWWM2090E

A junction mount point must begin with '/' (0x38cfc82a)

Explanation
See text.

Administrator response
Correct the syntax of the command and try again.

DPWWM2091E

The existing Virtual Host Junction is in an inconsistent state as it is missing it's virtual host name. (0x38cfc82b)

Explanation
See text.

Administrator response
Contact product support.

DPWWM4023E

Error reading configuration file *%s*: *%s* (0x38cfcfb7)

Explanation
There was an error opening a configuration file.

Administrator response
Make sure the file exists and is readable.

DPWWM4024E

Stanza '*%s*' is missing from configuration file. (0x38cfcfb8)

Explanation
A needed stanza was not found.

Administrator response
The stanza should be added to the configuration file

DPWWM4025E

Unknown configuration item '[*%s*]*%s*' in configuration file. (0x38cfcfb9)

Explanation
Probably a typo of the configuration item in the configuration file.

Administrator response
Correct the configuration item in the configuration file.

DPWWM4041E

Unable to read the stanza [*%s*]. Add the stanza to theWebSEAL configuration file to enable TFIM SSO for the junction '*%s*'. (0x38cfcfc9)

Explanation
See Message.

Administrator response
Add the configuration options to the WebSEAL config file and restart the WebSEAL server.

DPWWM4042E

Unable to enable TFIM junction SSO. (0x38cfcfca)

Explanation
See Message.

Administrator response
Add the configuration options to the WebSEAL config file and restart the WebSEAL server.

DPWWM4045E

The address supplied with the -a option, *%s*, is not a valid local address. (0x38cfcfcd)

Explanation
See Message.

Administrator response
Ensure that the address which is supplied is a valid local address for the WebSEAL server.

HPDAC0153E

Could not build ACL with the supplied ACL entries. (0x1005b099)

Explanation
An ACL entry failed the validity check. The Security Verify Access policy server's error log file will contain an error status message indicating the reason for the failure.

Administrator response
Review the Security Verify Access policy server's error log to determine the reason that the ACL failed the validity check.

HPDAC0178E

Could not obtain local host name. (0x1005b0b2)

Explanation
The system library call to get the local host name failed.

Administrator response
Ensure that the machine has a valid hostname.

HPDAC0179E

Unexpected exception caught. (0x1005b0b3)

Explanation
An unexpected exception was caught while registering an azn administration service with the Security Verify Access policy server.

Administrator response
Ensure that the Security Verify Access policy server is running and that the client and server versions are compatible with each other.

HPDAC0180E

The Security Verify Access authorization server could not be started (0x*%8.8lx*). (0x1005b0b4)

Explanation
The Security Verify Access authorization server encountered an error during initialization.

Administrator response
See the accompanying status code, which gives more information about the failure.

HPDAC0450E

There is no root ACL in the authorization policy database. (0x1005b1c2)

Explanation
See message.

Administrator response
This is a severe error indicating integrity problems with the policy database. If the problem occurs with the Security Verify Access authorization server or with a Security Verify Access resource manager application, then stop the resource manager, remove the resource manager's policy database, and start the resource manager again. If the problem occurs with the Security Verify Access policy server, then stop the policy server, restore a known good version of the master policy database, and then start the Security Verify Access servers again. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC0451E

A protected object should have only one attached ACL (*%s*). (0x1005b1c3)

Explanation
See message.

Administrator response
This is a severe error indicating integrity problems with the policy database. If the problem occurs with the Security Verify Access authorization server or with a Security Verify Access resource manager application, then stop the resource manager, remove the resource manager's policy database, and start the resource manager again. If the problem occurs with the Security Verify Access policy server, then stop the policy server, restore a known good version of the master policy database, and then start the Security Verify Access servers again. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC0452E

An ACL that is attached to a protected object cannot be found in the policy database (*%s*,*%s*). (0x1005b1c4)

Explanation
See message.

Administrator response
This is a severe error indicating integrity problems with the policy database. If the problem occurs with the Security Verify Access authorization server or with a Security Verify Access resource manager application, then stop the resource manager, remove the resource manager's policy database, and start

the resource manager again. If the problem occurs with the Security Verify Access policy server, then stop the policy server, restore a known good version of the master policy database, and then start the Security Verify Access servers again. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC0453E

Authorization policy database version is incompatible with the server version (*%ld*,*%ld*) and will be automatically replaced. (0x1005b1c5)

Explanation
The authorization client application has detected an incompatible version of the policy database. The database is replaced automatically.

Administrator response
No action is required.

HPDAC0454E

Could not initialize the authorization policy database (0x*%8.8lx*). (0x1005b1c6)

Explanation
An error occurred while attempting to access the authorization policy database. The authorization engine client was not initialized correctly.

Administrator response
See the accompanying status code, which gives more information about failure.

HPDAC0455E

The authorization policy database has not been initialized. (0x1005b1c7)

Explanation
An error occurred during application initialization and the authorization policy database was not initialized correctly.

Administrator response
Review the Security Verify Access base error log and look for error messages during initialization that might account for problems with the authorization policy database.

HPDAC0456E

The ACL name specified was not found in the authorization policy database. (0x1005b1c8)

Explanation
See message.

Administrator response
Review the ACL name and ensure that the name is a valid ACL name and that it matches an ACL that exists in the authorization policy database.

HPDAC0457E

The protected object name is invalid. (0x1005b1c9)

Explanation
The protected object name is invalid. The name must begin with the '/' character. The name cannot contain carriage return or line-feed characters and it cannot contain two '/' characters in sequence.

Administrator response
Review the protected object name and ensure that it adheres to the restrictions outlined in the message explanation.

HPDAC0458E

The protected object name specified was not found in the authorization policy database. (0x1005b1ca)

Explanation
See message.

Administrator response
Review the protected object name and ensure that the name is a valid protected object name and that it matches an object that exists in the authorization policy database.

HPDAC0459E

The protected object space specified was not found in the authorization policy database. (0x1005b1cb)

Explanation
See message.

Administrator response
Review the protected object space name and ensure that the name is a valid protected object space name and that it matches an object space that exists in the authorization policy database.

HPDAC0460E

The protected object space specified already exists in the authorization policy database. (0x1005b1cc)

Explanation
See message.

Administrator response
Each protected object space name must be unique so choose a different name for the new protected object space.

HPDAC0461E

The extended attribute specified was not found. (0x1005b1cd)

Explanation
See message.

Administrator response
Review the extended attributes on the target object and ensure that the extended attribute requested actually exists in the extended attribute list for this object.

HPDAC0462E

The extended attribute name specified is invalid. (0x1005b1ce)

Explanation
See message.

Administrator response
Review the extended attribute name to ensure that it is valid.

HPDAC0463E

There are no extended attributes associated with the specified protected object or authorization policy object. (0x1005b1cf)

Explanation
See message.

Administrator response
Define extended attributes for specified object or parent object if you want to perform extended attributes associated with the object.

HPDAC0464E

A POP that is attached to a protected object cannot be found in the policy database (*%s*,*%s*). (0x1005b1d0)

Explanation
See message.

Administrator response
This is a severe error indicating integrity problems with the policy database. If the problem occurs with the Security Verify Access authorization server or with a Security Verify Access resource manager application, then stop the resource manager, remove the resource manager's policy database, and start the resource manager again. If the problem occurs with the Security Verify Access policy server, then stop the policy server, restore a known good version of the master policy database, and then start the Security Verify Access servers again. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC0465E

A new action group could not be created because the count of action groups has reached the maximum permitted. (0x1005b1d1)

Explanation
See message.

Administrator response
If you want to create another action group, then you must first reduce the count of defined action groups. Review the list of defined action groups and remove those that are no longer required.

HPDAC0466E

A new action could not be created because the count of actions has reached the maximum permitted. (0x1005b1d2)

Explanation
See message.

Administrator response
Before creating another action you must first reduce the count of defined actions. Review the list of defined actions and remove those that are no longer required.

HPDAC0467E

Unable to create the new action because the bitmask supplied is invalid. (0x1005b1d3)

Explanation
The bitmask must have only one of bits 0 to 31 set to be a valid action bitmask. Having multiple bits set or no bits at all is invalid.

Administrator response
Review the specified action bitmask to ensure that at least one and only one action bit is set in the mask.

HPDAC0468E

Unable to create new action group because an action group exists with the same name. (0x1005b1d4)

Explanation
See message.

Administrator response
You must choose a unique name for the new action group.

HPDAC0469E

Unable to locate an action group with the name supplied. (0x1005b1d5)

Explanation
See message.

Administrator response
Review the action group name specified and ensure that it is a valid action group name and that the group exists.

HPDAC0470E

Unable to create the new action because an action exists with the same name. (0x1005b1d6)

Explanation
See message.

Administrator response
You must choose a unique action name for the new action.

HPDAC0471E

Action name contains invalid characters or too many characters. (0x1005b1d7)

Explanation
The action name specified is invalid. The name must not be NULL and can contain only one character from the set [a-zA-Z].

Administrator response
Review the action name and ensure that it conforms to the criteria specified in the Security Verify Access Base Administrator's Guide.

HPDAC0472E

Action group name contains invalid characters. (0x1005b1d8)

Explanation
The action group name specified is invalid. The name must not be NULL and can contain only characters from the set [a-zA-Z0-9 +-_:].

Administrator response
Review the action group name and ensure that it conforms to the criteria specified in the Security Verify Access Base Administrator's Guide.

HPDAC0473E

The primary action group cannot be deleted. (0x1005b1d9)

Explanation
See message.

Administrator response
No action is required.

HPDAC0474E

A protected object should have only one rule attached (*%s*). (0x1005b1da)

Explanation
See message.

Administrator response
This is a severe error indicating integrity problems with the policy database. If the problem occurs with the Security Verify Access authorization server or with a Security Verify Access resource manager application, then stop the resource manager, remove the resource manager's policy database, and start the resource manager again. If the problem occurs with the Security Verify Access policy server, then stop the policy server, restore a known good version of the master policy database, and then start the Security Verify Access servers again. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC0475E

A rule that is attached to a protected object cannot be found in the policy database (*%s*,*%s*). (0x1005b1db)

Explanation
See message.

Administrator response
This is a severe error indicating integrity problems with the policy database. If the problem occurs with the Security Verify Access authorization server or with a Security Verify Access resource manager application, then stop the resource manager, remove the resource manager's policy database, and start the resource manager again. If the problem occurs with the Security Verify Access policy server, then stop the policy server, restore a known good version of the master policy database, and then start the Security Verify Access servers again. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC0476E

A protected object should have only one POP attached (*%s*). (0x1005b1dc)

Explanation
See message.

Administrator response
This is a severe error indicating integrity problems with the policy database. If the problem occurs with the Security Verify Access authorization server or with a Security Verify Access resource manager application, then stop the resource manager, remove the policy database of the resource manager, and start the resource manager again. If the problem occurs with the Security Verify Access policy server, then stop the policy server, restore a known good version of the master policy database, and then start the Security Verify Access servers again. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC0750E

Invalid ACL name. (0x1005b2ee)

Explanation
The ACL name received was invalid. The ACL name contained illegal characters or was NULL.

Administrator response
Review the ACL name and ensure that it conforms to the criteria specified in the Security Verify Access Base Administrator's Guide.

HPDAC0751E

Invalid protected object name. (0x1005b2ef)

Explanation
The protected object name received was invalid. The protected object name contained illegal characters or was NULL.

Administrator response
Review the protected object name and ensure that it conforms to the criteria specified in the Security Verify Access Base Administrator's Guide.

HPDAC0752E

The requested object was not found. (0x1005b2f0)

Explanation
See message.

Administrator response
Review the object name and ensure that it is valid and that it actually exists.

HPDAC0753E

The ACL action specified could not be mapped. (0x1005b2f1)

Explanation
There is no mapping for this ACL action in the policy database.

Administrator response
Review the ACL name and ensure that it is valid and refers to an existing ACL action in the policy database.

HPDAC0754E

Privacy or data integrity quality of protection cannot be specified in the unauthenticated entry. (0x1005b2f2)

Explanation
Quality of protection cannot be enforced by the authorization client runtime for unauthenticated users.

Administrator response
No action is required.

HPDAC0755E

The ACL has an unauthenticated entry but there is no any-other entry. The any-other entry must be at least as permissive as unauthenticated. (0x1005b2f3)

Explanation
See message.

Administrator response
Add an any-other entry to the ACL with permissions at least equal to those of the unauthenticated user.

HPDAC0756E

The any-other entry is missing actions from the unauthenticated entry. The any-other entry must be at least as permissive as unauthenticated. (0x1005b2f4)

Explanation
See message.

Administrator response
Ensure that the permissions in the ACL for the any-other entry are at least equal to those of the unauthenticated entry.

HPDAC0757E

An entry in the ACL is missing some actions granted by the unauthenticated entry. Users can bypass an explicit action revocation if allowed by the unauthenticated entry. (0x1005b2f5)

Explanation
See message.

Administrator response
Review the ACL and ensure that the unauthenticated entry does not have the permission to perform actions that other authenticated entries cannot. The permissions of the unauthenticated entry should be the most restrictive in the secure domain.

HPDAC0758E

An entry in the ACL that grants control does not also grant traverse. (0x1005b2f6)

Explanation
To have the control permission the user must also be able to traverse.

Administrator response
Ensure that entries with the control permission also have the traverse permission.

HPDAC0759E

No entry in the ACL grants control permission. (0x1005b2f7)

Explanation
At least one entry in the ACL must have the control permission. Otherwise the ACL cannot be modified or deleted.

Administrator response
Add the control permission to at least one of the ACL entries. An administrative user is the most suitable candidate because control permission will authorize the user to modify and delete the ACL.

HPDAC0760E

The user is revoking the control permission for itself on this ACL. (0x1005b2f8)

Explanation
If the current user removes the control permission from its own ACL entry, that user can no longer modify or delete the object. If the user were the only user with control permission then the ACL can no longer be modified or deleted. To avoid losing control over the ACL, it is more prudent to have another user who has control permission remove the control permission on behalf of the current user.

Administrator response
Login as another user who has the control permission for this ACL and have that user remove the control permission on behalf of the current user.

HPDAC0766E

The ACL cannot be detached from the root protected object. Try replacing the attached ACL instead. (0x1005b2fe)

Explanation
See message.

Administrator response
Modify or even replace the root ACL with an ACL of the desired configuration.

HPDAC0767E

Core ACL actions cannot be deleted. (0x1005b2ff)

Explanation
See message.

Administrator response
No action is required.

HPDAC0768E

The ACL action name already exists. (0x1005b300)

Explanation
See message.

Administrator response
Choose a unique action name for the new action.

HPDAC0769E

Too many ACL actions are already defined. (0x1005b301)

Explanation
Only 32 actions bits can be defined and this limit has been reached.

Administrator response
An ACL action must be deleted before a new action can be created.

HPDAC0771E

The user registry client is unavailable. (0x1005b303)

Explanation
The authorization client was unable to contact the user registry. The user registry client may not be configured correctly.

Administrator response
Refer to the Installation Guide for your chosen platform and ensure that the correct user registry has been specified and that the configuration steps succeeded. Also ensure that the user registry is running and can be contacted from the client machine. The IBM Security Verify Access for Web Troubleshooting Guide contains instructions on how to ensure that the user registry is configured correctly and is operational.

HPDAC0772E

The LDAP user registry client returned an error status for the specified DN. (0x1005b304)

Explanation
The LDAP client returned an error status because the DN was invalid or there are multiples of the same DN.

Administrator response
Ensure that the specified DN exists in the user registry and is valid and that the DN is unique.

HPDAC0773E

The LDAP user registry client returned an unexpected failure status. (0x1005b305)

Explanation
The LDAP user registry client returned an error code that was unexpected or unknown to Security Verify Access.

Administrator response
Ensure that the LDAP registry server and local registry client runtime are correctly installed and operational then try the procedure again. The IBM Security Verify Access for Web Troubleshooting Guide contains instructions on how to ensure that the user registry is configured correctly and is operational. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC0776E

The DN specified was not found in the registry. (0x1005b308)

Explanation
The specified DN was not found in the user registry.

Administrator response
Ensure that the DN specified exists in the user registry and is valid.

HPDAC0777E

LDAP Registry client returned a memory error. (0x1005b309)

Explanation
The LDAP registry client encountered a memory error.

Administrator response
Ensure that the affected process has been configured with sufficient virtual memory for its requirements. The Security Verify Access Performance Tuning Guide contains instructions on how to ensure that the application is configured with the correct amount of virtual memory. Stop and restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC0778E

The specified user's account is set to invalid. (0x1005b30a)

Explanation
When an account is created in the user registry, the user account must also be marked as valid.

Administrator response
Start the administration console or command-line administration tool and set the user account to be valid with the 'user modify' command.

HPDAC0779E

The LDAP registry server is down. (0x1005b30b)

Explanation
The LDAP registry server is not running.

Administrator response
Ensure that the LDAP registry server is running and that the LDAP client has been correctly configured to communicate with the server. The IBM Security Verify Access for Web Troubleshooting Guide contains instructions on how to ensure that the user registry is configured correctly and is operational.

HPDAC0780E

A valid action group is specified, but no action is specified. (0x1005b30c)

Explanation
The permission string contains a valid action group, but no action within this group is specified. Therefore, an authorization check cannot be performed.

Administrator response
Ensure that a valid action for the specified action group was provided.

HPDAC0901E

The Authorization service is already initialized. (0x1005b385)

Explanation
You cannot reinitialize the authorization service once it has been initialized. The azn_shutdown() interface must be called before the aznAPI client can be initialized again.

Administrator response
Review your aznAPI application and ensure that the azn_initialize() interface is called only once during the execution of the program.

HPDAC0902E

There was no authorization client listener port specified. (0x1005b386)

Explanation
The authorization client requires a TCP port to listen for authorization policy updates and azn admin service requests.

Administrator response
Ensure that you have specified a listening port for the authorization client in the aznAPI client configuration file or by using programmatic aznAPI initialization attributes.

HPDAC0906E

An invalid parameter was supplied to the API function. (0x1005b38a)

Explanation
A parameter supplied to the API function was NULL or outside the range of valid values.

Administrator response
Ensure that the API function call parameters supplied meet the criteria defined for the API interface in the Security Verify Access Authorization C API Developer's Reference. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC0909E

An unspecified implementation dependent error has occurred. (0x1005b38d)

Explanation
A minor error could not be mapped to a known message catalog category. The minor error might be returned by an authorization service plug-in without first being encoded using azn_util_errcode(). Another reason this occurs is that an authorization client's message catalogs might not be synchronized with those of the Security Verify Access authorization server.

Administrator response
If you have loaded a custom authorization service plug-in then ensure that the plug-in returns the appropriate azn_status_t error codes from its exported interfaces. If this is not the case, then the authorization client's message catalogs might not be synchronized with those of the server. Upgrade the Security Verify Access Runtime package to the same level as the server.

HPDAC0910E

An invalid policy cache mode value was specified. (0x1005b38e)

Explanation
See message.

Administrator response
Ensure that the specified policy cache mode is a valid mode from the set of modes defined in the Security Verify Access Authorization C API Developer's Reference.

HPDAC0912E

An invalid database file path value was specified. (0x1005b390)

Explanation
See message.

Administrator response
Ensure that the specified database file path is valid.

HPDAC0914E

An invalid policy cache refresh interval value was specified. (0x1005b392)

Explanation
See message.

Administrator response
Ensure that the policy cache refresh interval specified is within the range of valid values specified in the Security Verify Access Authorization C API Developer's Reference.

HPDAC0915E

An invalid listen flags value was specified. (0x1005b393)

Explanation
The listen flags can be set to either 'enable' or 'disable'.

Administrator response
Ensure that the listen flags configuration parameter is set to either 'enable' or 'disable'.

HPDAC0919E

An invalid LDAP host name was specified. (0x1005b397)

Explanation
See message.

Administrator response
Ensure that the LDAP host name specified is valid.

HPDAC0920E

An invalid LDAP host port was specified. (0x1005b398)

Explanation
See message.

Administrator response
Ensure that the LDAP server port specified is valid.

HPDAC0923E

An invalid LDAP server SSL keyfile was specified. (0x1005b39b)

Explanation
The SSL keyfile could not be found, is invalid or has inappropriate access permissions.

Administrator response
Ensure that the path to the LDAP server SSL keyfile is correct that the file exists, is valid and has the appropriate access permissions.

HPDAC0924E

An invalid LDAP server SSL keyfile DN was specified. (0x1005b39c)

Explanation
See message.

Administrator response
Ensure that the specified DN for the LDAP server SSL keyfile is correct.

HPDAC0925E

An invalid LDAP server SSL keyfile password was specified. (0x1005b39d)

Explanation
See message.

Administrator response
Ensure that the specified password for the LDAP server SSL keyfile is correct.

HPDAC0926E

One or more of the LDAP server values was not specified. (0x1005b39e)

Explanation
To configure an LDAP registry server you must at least specify the server host name, the port on which to connect to the server, the DN with which to bind to the server and the password for that DN. One of these values was not specified in the configuration settings.

Administrator response
Ensure that you have specified the LDAP registry server name, request port, bind DN, and bind DN password in the aznAPI client configuration settings.

HPDAC0928E

The attempt to initialize the LDAP registry failed. (0x1005b3a0)

Explanation
This failure can occur when the LDAP registry server configuration settings are incorrect or when the Security Verify Access runtime is incorrectly configured for a registry type other than LDAP.

Administrator response
Ensure that you have correctly configured the Security Verify Access Runtime package to use an LDAP user registry. The current user registry setting can be determined by looking at the 'user-reg-type' entry in the [pdrte] stanza of the 'etc/pd.conf' file in the Security Verify Access install directory. If the runtime is configured incorrectly, you will need to unconfigure all packages and reconfigure the machine again. If the runtime has been correctly configured, then ensure that the configuration parameters specified for the LDAP registry server are correct.

HPDAC0930E

A memory allocation call failed. (0x1005b3a2)

Explanation
In most cases this error due to the aznAPI application program running out of memory.

Administrator response
Ensure that the application has been configured with sufficient virtual memory for its requirements. The Security Verify Access Performance Tuning Guide contains instructions on how to ensure that the application is configured with the correct amount of virtual memory. Stop and restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC0931E

Unable to configure LDAP replica server. (0x1005b3a3)

Explanation
The replica is either misconfigured or there are too many replicas configured.

Administrator response
Ensure that the replica LDAP server configuration settings are valid and refer to an operational replica of the master LDAP server. Also ensure that you have not registered more LDAP replicas than that allowed by the LDAP registry implementation.

HPDAC0932E

An invalid LDAP bind user DN was specified. (0x1005b3a4)

Explanation
See message.

Administrator response
Ensure that the LDAP bind user DN specified is valid.

HPDAC0933E

The password for the LDAP bind user was invalid. (0x1005b3a5)

Explanation
See message.

Administrator response
Ensure that the LDAP bind user password specified is valid.

HPDAC0934E

An invalid configuration file path was specified. (0x1005b3a6)

Explanation
See message.

Administrator response
Ensure that the path to the configuration file that was specified is valid.

HPDAC0935E

An error occurred loading the aznAPI configuration file. (0x1005b3a7)

Explanation
See message.

Administrator response
Review the aznAPI configuration file used to initialize the application and ensure that it is a valid stanza format file and that the entries conform to stanza format syntax.

HPDAC0936E

An error occurred loading the configuration file specified as the parameter to 'ldap-server-config' in the aznAPI config file. (0x1005b3a8)

Explanation
See message.

Administrator response
Review the respective aznAPI configuration file and ensure that it is a valid stanza format file and that the entries conform to stanza format syntax.

HPDAC0937E

An invalid maximum search size was specified. (0x1005b3a9)

Explanation
The specified maximum search size could not be converted to an integer number or is zero.

Administrator response
Ensure that the value specified for maximum search size is a valid integer value in the range specified in the LDAP registry server documentation and is not zero.

HPDAC0940E

An invalid attribute value was specified for the azn_init_set_perminfo_attrs attribute. (0x1005b3ac)

Explanation
See message.

Administrator response
Ensure that the value specified for the azn_init_set_perminfo_attrs initialization attribute is a text string consisting of one or more valid aznAPI attribute names separated by spaces.

HPDAC0941E

Too many permission information attributes were specified with the azn_init_set_perminfo_attrs attribute. (0x1005b3ad)

Explanation
The maximum number of permission info attributes that can be returned from an azn_decision_access_allowed_ext() call is 32.

Administrator response
Review the list of permission information attributes that you have specified in the azn_init_set_perminfo_attrs attribute and ensure that the count of attributes is no greater than 32.

HPDAC0943E

An invalid trace configuration parameter was specified: *%s*. (0x1005b3af)

Explanation
Either the application configuration file contains an invalid 'trace' configuration item in the [aznapi-configuration] stanza or the application is passing an invalid value for the azn_init_trace programmatic initialization attribute. The value considered invalid is shown in the error message.

Administrator response
Correct the value of the trace configuration parameter in the configuration file or the application as appropriate.

HPDAC0944E

An invalid statistics configuration parameter was specified: *%s*. (0x1005b3b0)

Explanation
Either the application configuration file contains an invalid 'stats' configuration item in the [aznapi-configuration] stanza or the application is passing an invalid value for the azn_init_stats azn_initialize parameter. The value considered invalid is shown in the error message.

Administrator response
Correct the value of the 'stats' configuration parameter in the configuration file or the application as appropriate.

HPDAC0945E

The value specified for the 'timeout' parameter in the [ldap] stanza is invalid: *%s*. (0x1005b3b1)

Explanation
Either the application configuration file contains an invalid 'timeout' configuration value in the [ldap] stanza or the application is passing an invalid value for the azn_init_ldap_timeout azn_initialize parameter. The value considered invalid is shown in the error message.

Administrator response
Correct the value of the 'timeout' parameter in the [ldap] stanza. It must be a non-negative integer.

HPDAC0946E

The value specified for the 'authn-timeout' parameter in the [ldap] stanza is invalid: *%s*. (0x1005b3b2)

Explanation
Either the application configuration file contains an invalid 'authn-timeout' configuration value in the [ldap] stanza or the application is passing an invalid value for the azn_init_ldap_authn_timeout azn_initialize parameter. The value considered invalid is shown in the error message.

Administrator response
Correct the value of the 'authn-timeout' parameter in the [ldap] stanza. It must be a non-negative integer.

HPDAC0947E

The value specified for the 'search-timeout' parameter in the [ldap] stanza is invalid: *%s*. (0x1005b3b3)

Explanation
Either the application configuration file contains an invalid 'search-timeout' configuration item in the [ldap] stanza or the application is passing an invalid value for the azn_init_ldap_search_timeout azn_initialize parameter. The value considered invalid is shown in the error message.

Administrator response
Correct the value of the 'search-timeout' parameter in the [ldap] stanza. It must be a non-negative integer.

HPDAC0948E

Validation of the rule text for the rule object failed. Refer to the error log for more information about the failure. (0x1005b3b4)

Explanation
The rule text of the rule policy is not valid.

Administrator response
Review the rule text for the rule policy named in the error log and correct any errors.

HPDAC0949E

Validation of the rule text for rule object *%s* failed. Error code 0x*%x* was returned along with error message *%s*. (0x1005b3b5)

Explanation
The rule text of the rule policy is not valid.

Administrator response
Review the rule text for the rule policy named in the error log and correct any errors.

HPDAC0950E

An ADI container name was found in multiple places in the input from the application. Refer to the error log for more information about the failure. (0x1005b3b6)

Explanation
The same piece of access decision information cannot be provided to the rules evaluator from two different sources as this indicates that one piece of data may not be valid or is incorrectly named. Container names must be unique across data sources.

Administrator response
Review your system configuration to ensure that only one of either the application context or user credentials is the source for the piece of ADI named in the error log.

HPDAC0951E

The ADI container name *%s* was found in multiple places in the input from the application. (0x1005b3b7)

Explanation
The same piece of access decision information cannot be provided to the rules evaluator from two different sources as this indicates that one piece of data may not be valid or is incorrectly named. Container names must be unique across data sources.

Administrator response
Review your system configuration to ensure that only one of either the application context or user credentials is the source for the piece of ADI named in the error log.

HPDAC0952E

The XSL processor failed to evaluate the rule object. Refer to the error log for more information about the failure. (0x1005b3b8)

Explanation
The rule text of the rule policy named in the error log is not valid and caused an error condition in the XSL processor.

Administrator response
Review the rule text for the rule policy object named in the error log and correct any errors.

HPDAC0953E

The XSL processor failed to evaluate the rule object *%s*. Error code 0x*%x* was returned along with error message *%s*. (0x1005b3b9)

Explanation
The rule text of the rule policy named in the error log is not valid and caused an error condition in the XSL processor.

Administrator response
Review the rule text for the rule policy object named in the error log and correct any errors.

HPDAC0954E

The rule object was not evaluated because there was insufficient access decision information provided in the application context and credential attributes. (0x1005b3ba)

Explanation
To evaluate a rule, the authorization engine must have all of the ADI referenced in the rule text available at evaluation time. If any items of data are missing then the rule cannot be evaluated.

Administrator response
Review the rule text for the rule policy object named in the error log and ensure that all of the items of data listed in the error message are provided to the access decision call.

HPDAC0955E

Rule object *%s* was not evaluated because there was insufficient access decision information provided to the access decision call. Missing ADI items include: *%s*. (0x1005b3bb)

Explanation
To evaluate a rule the authorization engine must have all of the ADI referenced in the rule text available at evaluation time. If any items of data are missing then the rule cannot be evaluated.

Administrator response
Review the rule text for the rule policy object named in the error log and ensure that all of the items of data listed in the error message are provided to the access decision call.

HPDAC0956E

The rule text is invalid because the template match statement does not match one of the minimum required paths of /XMLADI or XMLADI. (0x1005b3bc)

Explanation
Input data is supplied to the rules evaluator within a top-level element XMLADI. To match any data item within the XML document the template match statement must match either the XPath /XMLADI or XMLADI. Matching paths above this point in the path is not valid.

Administrator response
Review the rule text for the rule policy object and change the template match statement to include one of /XMLADI or XMLADI.

HPDAC0957E

The rule *%s* is invalid because the template match statement does not match one of the minimum required paths of /XMLADI or XMLADI. (0x1005b3bd)

Explanation

Input data is supplied to the rules evaluator witin a top-level element XMLADI. To match any data item within the XML document the template match statement must match either the XPath /XMLADI or XMLADI. Matching paths above this point in the path is not valid.

Administrator response

Review the rule text for the rule policy object named in the error log and change the template match statement to include one of /XMLADI or XMLADI.

HPDAC0958E

The rule was found to have no identifiable ADI to use when evaluating the rule. (0x1005b3be)

Explanation

The validation of the rule text of the rule policy named in the error log failed because there was no ADI identified in the rule text. ADI consists of the variables used in a rule to make comparisons against. A rule with no variables, for example a rule that is comparing static data, is invalid.

Administrator response

Review the rule text for the rule policy and correct any errors.

HPDAC0959E

Rule *%s* was found to have no identifiable ADI to use when evaluating the rule. (0x1005b3bf)

Explanation

The validation of the rule text of the rule policy named in the error log failed because there was no ADI identified in the rule text. ADI consists of the variables used in a rule to make comparisons against. A rule with no variables, for example a rule that is comparing static data, is invalid.

Administrator response

Review the rule text for the rule policy named in the error log and correct any errors.

HPDAC0960E

The rule has a null entry in the compiled rules cache. (0x1005b3c0)

Explanation

The validation of the rule text of the rule policy named in the error log failed and the rule could not be cached in the local client.

Administrator response

Review the rule text for the rule policy and correct any errors.

HPDAC0961E

Rule *%s* has a null entry in the compiled rules cache. (0x1005b3c1)

Explanation
The validation of the rule text of the rule policy named in the error log failed and the rule could not be cached in the local client.

Administrator response
Review the rule text for the rule policy named in the error log and correct any errors.

HPDAC0962E

The XSL prolog entry specifies an XSL output method other than 'text', which is an invalid processor setting for rules evaluation. (0x1005b3c2)

Explanation
The output of any rule evaluation must be plain text so setting any other output method in the XSL prolog entry for the rules evaluator is invalid.

Administrator response
Review the XSL prolog entry in the application's configuration file and ensure that the output method is 'text'.

HPDAC0963E

The XSL prolog asks the XSL processor to generate an XML declaration in the output from a rule evaluation. This setting is invalid. (0x1005b3c3)

Explanation
The output of any rule evaluation must be minimal plain text so including an XML declaration in the text output is invalid.

Administrator response
This is an invalid processor setting for rules evaluation. Review the XSL prolog entry in the application's configuration file and ensure that the 'omit-xml-declaration' setting in the output method is 'yes'.

HPDAC0964E

The method of output encoding specified for the XSL processor is invalid for the purposes of rule evaluation. (0x1005b3c4)

Explanation
The encoding for XSL output specified in the XSL prolog configuration entry must be UTF-8.

Administrator response
Review the XSL prolog entry in the application's configuration file and ensure that the output encoding is UTF-8.

HPDAC0965E

The parsing of the compiled XSL rule returned an invalid element pointer. (0x1005b3c5)

Explanation
An internal XSL rule parsing error has occurred.

Administrator response
Review the rule text for the rule attached to the target object and ensure that it is valid XSL and conforms to Security Verify Access requirements.

HPDAC0966E

The parsing of the compiled XSL rule returned an invalid template match string pointer. (0x1005b3c6)

Explanation
An internal XSL rule parsing error has occurred.

Administrator response
Review the rule text for the rule attached to the target object and ensure that it is valid XSL and conforms to Security Verify Access 'template match' statement requirements.

HPDAC0967E

An invalid XSL operation was encountered while parsing the compiled XSL rule. (0x1005b3c7)

Explanation
An internal XSL rule parsing error has occurred.

Administrator response
Review the rule text for the rule attached to the target object and ensure that it is valid XSL and conforms to Security Verify Access requirements.

HPDAC0968E

The rule does not return a valid result tag to the authorization engine. (0x1005b3c8)

Explanation
A Security Verify Access authorization rule must return one of the values listed in the message explanation to indicate the success, failure, or indifference of the rule evaluation.

Administrator response
Review the rule text for the rule and ensure that it will return one of the result tags !TRUE!, !FALSE!, or ! INDIFFERENT! in the XSL output document to the authorization engine.

HPDAC0969E

Rule *%s* does not return a valid result tag to the authorization engine. (0x1005b3c9)

Explanation
A Security Verify Access authorization rule must return one of the values listed in the message explanation to indicate the success, failure, or indifference of the rule evaluation.

Administrator response
Review the rule text for the rule named in the error log and ensure that it will return one of the result tags !TRUE!, !FALSE!, or !INDIFFERENT! in the XSL output document to the authorization engine.

HPDAC0970E

The rule contains an absolute XPath that doesn't include the top-level document element /XMLADI. (0x1005b3ca)

Explanation
Security Verify Access authorization rules are restricted to referencing ADI elements within an XML document with the top-level element <XMLADI>. Absolute XPaths that attempt to reference other top-level document elements are invalid.

Administrator response
Review the rule text for the rule and ensure that all absolute XPaths to rule ADI start from the top-level document element /XMLADI.

HPDAC0971E

The XSL prolog contains an XML namespace declaration for the default namespace. The default namespace is reserved for use by Security Verify Access. (0x1005b3cb)

Explanation
The default XML/XSL namespace, which has no prefix, is reserved for use by Security Verify Access.

Administrator response
Review the XSL prolog statement and remove any default namespace declaration.

HPDAC0972E

The XSL prolog contains a namespace declaration that has an invalid URI. (0x1005b3cc)

Explanation
The authorization engine failed to parse a URI from the XSL prolog statement.

Administrator response
Review the XSL prolog statement and ensure that the URIs in the XML namespace declarations have been correctly defined and delimited with quotation marks.

HPDAC0973E

The XSL prolog contains a namespace declaration that has no prefix to URI assignment. (0x1005b3cd)

Explanation
The authorization engine failed to find an '=' sign to denote assignment of a URI to a namespace prefix in the XSL prolog statement.

Administrator response
Review the XSL prolog statement and ensure that a URI has been specified for each namespace prefix declared.

HPDAC0974E

The XSL prolog contains a duplicate namespace prefix or URI declaration. (0x1005b3ce)

Explanation
The authorization engine requires that the mapping of namespace prefix to URI is unique so that target ADI can be properly identified.

Administrator response
Review the XSL prolog statement and ensure that the mapping of namespace prefix to URI is unique.

HPDAC0975E

The XSL prolog contains a namespace declaration for the prefix 'xsl'. This prefix is reserved for the XSLT language namespace. (0x1005b3cf)

Explanation
The authorization engine requires that the mapping of namespace prefix to URI is unique so that target ADI can be properly identified.

Administrator response
Review the XSL prolog statement and remove any namespace declaration for the prefix 'xsl' that is not mapped to the XSLT standard URI.

HPDAC0976E

An unexpected Xalan processor exception was caught during rule processing. Refer to the error log for more information about the exception. (0x1005b3d0)

Explanation
Xalan returned an exception condition to the authorization engine that was not handled and not expected.

Administrator response
Refer to the error log to determine if an error message accompanied the exception.

HPDAC0977E

An unexpected Xalan processor exception was caught during rule processing. Error message *%s* was returned with the exception. (0x1005b3d1)

Explanation
Xalan returned an exception condition to the authorization engine that was not handled and not expected.

Administrator response
Refer to the error log to determine if an error message accompanied the exception.

HPDAC0978E

A predicate expression using the /XMLADI top-level document element cannot be used in an authorization rule. (0x1005b3d2)

Explanation

Security Verify Access authorization rules are restricted to referencing ADI elements within an XML document with the top-level element <XMLADI>. Predicate expressions that use /XMLADI are invalid for use in authorization rules because the target ADI of the predicate expression cannot be determined with certainty before evaluation.

Administrator response

Review the rule text for the rule and remove the predicate expression that uses the top-level document element /XMLADI.

HPDAC0979E

The result string returned from the rule evaluation is greater than the maximum result buffer size of 1023 bytes. (0x1005b3d3)

Explanation

The buffer used to store the text output of a rule evaluation is 1023 bytes in length. The result text string returned by the rule must have a length less than this in order to fit into the result buffer. If the result string token is surrounded by a lot of white space then this error might occur. To determine the result string text that will be returned as output from the rule evaluation, count the number of characters between the last closing '>' character and the first opening '<' character after that in the line containing the result string token.

Administrator response

Review the rule text for the rule and ensure that the rule returns one of the required result string tokens as outlined in the IBM Security Verify Access for Web Administrator's Guide. Also ensure that the white space surrounding the result string token is kept to a minimum so that total count of output characters is less than 1023.

HPDAC0980E

A value added to the azn_cred_groups attribute is not a string value. (0x1005b3d4)

Explanation

The type of all values of the azn_cred_groups attribute must be of type string. Other attribute types are not permitted.

Administrator response

Review the values of the azn_cred_groups attribute returned in the entitlements attribute list and ensure that each attribute value is a string.

HPDAC0981E

The request to add group memberships to the user credential from an entitlement service was denied. (0x1005b3d5)

Explanation

To ensure that the resource manager cannot modify the group memberships of a credential without explicit approval the resource manager must have loaded the credential group modification service

supplied with Security Verify Access. If this service is not loaded or is unavailable then the resource manager cannot modify the group memberships of the credentials with an entitlement service called by azn_id_get_creds().

Administrator response
If the resource manager is permitted to add group memberships to the user credential built by azn_id_get_creds() then the system administrator must also configure the resource manager to load the credential group modification service supplied with Security Verify Access.

HPDAC0982E

The code set parameter specified is not one of the valid code set name constants expected by the aznAPI runtime. (0x1005b3d6)

Explanation
The aznAPI runtime requires that the code set name parameter specified be one of the valid code set name constants. The constants include 'azn_code_set_utf8' and 'azn_code_set_local'.

Administrator response
Review the specified parameter and ensure that the value for the code set name is one of the string constants 'azn_code_set_utf8' or 'azn_code_set_local'.

HPDAC1050E

Operation is not authorized. (0x1005b41a)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDAC1051E

Operation is not authorized. Request permitted by Warning Mode. (0x1005b41b)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDAC1052E

No traverse permission. (0x1005b41c)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDAC1053E

Traverse permission was denied. Request permitted by Warning Mode. (0x1005b41d)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDAC1056E

Delegate principal is unauthorized to perform delegation. (0x1005b420)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDAC1057E

Delegate principal is unauthorized to perform delegation. Request permitted by Warning Mode. (0x1005b421)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDAC1058E

External authorization failed. (0x1005b422)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDAC1059E

ACL evaluation algorithm failure (0x*%8.8lx*). (0x1005b423)

Explanation
The ACL evaluation algorithm failed to obtain the permission set from the effective ACL.

Administrator response
See the accompanying status code, which gives more information about the failure.

HPDAC1060E

Access to the protected object is not allowed during this time of day. (0x1005b424)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDAC1063E

Authentication step up is required to access the protected object. (0x1005b427)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDAC1064E

Access to the protected object is not allowed during this time of day. Request permitted by Warning Mode. (0x1005b428)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDAC1065E

Access to the protected object was permitted by EAS override. (0x1005b429)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDAC1066E

Access to the protected object was denied by EAS. (0x1005b42a)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDAC1067E

Access to the protected object was denied by EAS. Request permitted by Warning Mode. (0x1005b42b)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDAC1068E

Access to the protected object was denied by EAS override. (0x1005b42c)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDAC1069E

Access to the protected object was denied by EAS override. Request permitted by Warning Mode. (0x1005b42d)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDAC1070E

The authorization rule policy attached to the protected object denied access to the object. (0x1005b42e)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDAC1071E

The authorization rule policy attached to the protected object denied access to the object. Request permitted by Warning Mode. (0x1005b42f)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDAC1072E

The step-up authorization policy on the protected object has denied access. (0x1005b430)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDAC1073E

The step-up authorization policy on the protected object has denied access. Request permitted by Warning Mode. (0x1005b431)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDAC1074W

The protected object's effective authorization rule policy has not been enforced. (0x1005b432)

Explanation
Authorization rule policies are not enforced with this version of the product.

Administrator response
No action is required. However if authorization rules are mandatory to enforcing your security policy, you should use a version of the product that supports this feature.

HPDAC1350E

aznAPI -- Internal error: see minor code. (0x1005b546)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1351E

aznAPI -- DCE authentication failed. (0x1005b547)

Explanation
The aznAPI runtime was unable to authenticate to the DCE authentication service. This message is obsolete as DCE is no longer supported by Security Verify Access. The message code must remain to ensure synchronicity between the aznAPI major utility function status codes and the message catalogs.

Administrator response
No action is required.

HPDAC1352E

aznAPI -- LDAP authentication failed. (0x1005b548)

Explanation
The aznAPI runtime was unable to authenticate to the LDAP user registry.

Administrator response
Ensure that the LDAP server is configured correctly, that it is operational and that the authentication parameters supplied are valid.

HPDAC1353E

aznAPI -- Already authenticated (API caller may already be logged in). (0x1005b549)

Explanation
The aznAPI client runtime has attempted to authenticate the server principal again.

Administrator response
If you are calling azn_initialize() twice within the same aznAPI application ensure that the second call is preceded by a call to azn_shutdown().

HPDAC1354E

aznAPI -- User's password has expired. (0x1005b54a)

Explanation
See message.

Administrator response
The user must change the password.

HPDAC1355E

aznAPI -- The user information is invalid. (0x1005b54b)

Explanation
See message.

Administrator response
Ensure that the user specified exists in the user registry and is a valid user.

HPDAC1356E

aznAPI -- The user registry is offline. (0x1005b54c)

Explanation
See message.

Administrator response
Ensure that the user registry is operational.

HPDAC1357E

aznAPI -- Invalid Calling Parameters. (0x1005b54d)

Explanation
The aznAPI function was called with an invalid parameter.

Administrator response
Ensure that the respective parameters are valid.

HPDAC1358E

aznAPI -- Error from pthread call. (0x1005b54e)

Explanation
A thread-related error condition was returned.

Administrator response
Ensure that the applications have enough system resources and worker threads to perform their tasks. The Security Verify Access Performance Tuning Guide contains instructions on how to ensure that the application is configured with the correct amount of system resources and worker threads. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1359E

aznAPI -- Invalid Principal Name. (0x1005b54f)

Explanation
See message.

Administrator response
Specify the name of an existing user in the user registry.

HPDAC1360E

aznAPI -- Invalid Password. (0x1005b550)

Explanation
See message.

Administrator response
The password supplied must match the password in the user registry.

HPDAC1361E

aznAPI -- Invalid Mechanism ID Reference. (0x1005b551)

Explanation
See message.

Administrator response
Ensure that the pointer reference specified references a valid mechanism ID structure.

HPDAC1362E

aznAPI -- Invalid keyfile path. (0x1005b552)

Explanation
See message.

Administrator response
Ensure that the keyfile path is valid.

HPDAC1364E

aznAPI -- Account Login Disabled. (0x1005b554)

Explanation
The account is disabled in the user registry. Logins will not succeed until the account is enabled.

Administrator response
Contact your Security Verify Access network administrator to enable the account.

HPDAC1365E

aznAPI -- Time of Day Access Denied. (0x1005b555)

Explanation
See message.

Administrator response
The caller must perform the desired operation within the time of day constraints set for the protected object. Contact your Security Verify Access network administrator for details on the time of day access restrictions that apply to the resource.

HPDAC1366E

aznAPI -- The user account has been locked out. (0x1005b556)

Explanation
The Security Verify Access network administrator has set a lock out time interval for this account and it has expired causing logins to be disabled for this account.

Administrator response
Contact your Security Verify Access network administrator to unlock and enable login to the account.

HPDAC1367E

aznAPI -- New password is too short. (0x1005b557)

Explanation
See message.

Administrator response
Review the password resitrictions that apply to your account and specify a password that meets the minimum length requirements.

HPDAC1368E

aznAPI -- New password has illegal spaces. (0x1005b558)

Explanation
The password must meet the specified requirements for your account. Spaces within the password are not permitted.

Administrator response
Specify a password that doesn't contain spaces.

HPDAC1369E

aznAPI -- New password has too many repeated characters. (0x1005b559)

Explanation
The password must meet the specified requirements for your account. There is a maximum limit on the number of times a character can be repeated within the password.

Administrator response
Review the password restrictions for your account and specify a password that adheres to the limitations on repeated characters.

HPDAC1370E

aznAPI -- New password has too few alphabetical characters. (0x1005b55a)

Explanation
The password must meet the specified requirements for your account. There is a minimum limit on the number of alphabetical characters within the password.

Administrator response
Review the password restrictions for your account and specify a password that contains the minimum number of alphabetical characters.

HPDAC1371E

aznAPI -- New password has too few non-alphabetical characters. (0x1005b55b)

Explanation
The password must meet the specified requirements for your account. There is a minimum limit on the number of non-alphabetical characters within the password.

Administrator response
Review the password restrictions for your account and specify a password that contains the minimum number of non-alphabetical characters.

HPDAC1372E

aznAPI -- Caller does not have the rights to perform requested operation. (0x1005b55c)

Explanation
See message.

Administrator response
The caller must gain the appropriate privileges before the required operation will be permitted.

HPDAC1373E

aznAPI -- User registry authenticate failed. (0x1005b55d)

Explanation
The aznAPI runtime was unable to authenticate to the user registry.

Administrator response
Ensure that the user registry is configured correctly, that it is operational and that the authentication parameters supplied are valid.

HPDAC1374W

aznAPI -- This account has been disabled due to too many failed login attempts. (0x1005b55e)

Explanation
See message.

Administrator response
Contact your Security Verify Access network administrator to revalidate the account.

HPDAC1375E

aznAPI -- User's account has expired (0x1005b55f)

Explanation
This user account's expiration date has passed and it can no longer be used.

Administrator response
Contact your Security Verify Access network administrator to revalidate the account.

HPDAC1376E

aznAPI -- User registry authentication failed, and user account has been locked out due to too many failed login attempts. (0x1005b560)

Explanation
See message.

Administrator response
Check your password and wait until disable-time-interval has elapsed, or contact your Security Verify Access administrator to unlock and enable login to the account.

HPDAC1377E

aznAPI -- User registry authentication failed, and user account has been disabled due to too many failed login attempts. (0x1005b561)

Explanation
See message.

Administrator response
Check your password and contact your Security Verify Access administrator to enable this account.

HPDAC1501E

aznAPI -- Failure. (0x1005b5dd)

Explanation
The aznAPI failed due to an error.

Administrator response
Review the minor error status and application logs for more details about the failure.

HPDAC1502E

aznAPI -- Authorization Failure. (0x1005b5de)

Explanation
The aznAPI failed because the aznAPI application server principal was not authorized to perform a paticular task.

Administrator response
Review the minor error status and application logs for more details about the failure.

HPDAC1503E

aznAPI -- Invalid Credentials Handle. (0x1005b5df)

Explanation
See message.

Administrator response
Ensure that the credentials handle input parameters passed to the aznAPI interface are valid.

HPDAC1504E

aznAPI -- Invalid New Credentials Handle. (0x1005b5e0)

Explanation
See message.

Administrator response
Ensure that the credentials handle output parameters passed to the aznAPI interface are valid.

HPDAC1505E

aznAPI -- Invalid Entitlements Service. (0x1005b5e1)

Explanation
An entitlement service with the specified service ID was not found in the list of services registered with the aznAPI service dispatcher.

Administrator response
Ensure that the specified entitlement service ID refers to a valid entitlement service that has been loaded into the current aznAPI application.

HPDAC1506E

aznAPI -- Invalid Combined Credentials Handle. (0x1005b5e2)

Explanation
See message.

Administrator response
Ensure that the combined credentials handle output parameter passed to the aznAPI interface is valid.

HPDAC1507E

aznAPI -- Invalid Mechanism Info. (0x1005b5e3)

Explanation
See message.

Administrator response
Ensure that the mechanism info input parameter passed to the aznAPI interface is valid.

HPDAC1508E

aznAPI -- Invalid Mechanism. (0x1005b5e4)

Explanation
The mechanism ID specified does not match a mechanism supported by the Security Verify Access aznAPI runtime.

Administrator response
Ensure that the specified mechanism ID matches one of the IDs supported by Security Verify Access.

HPDAC1509E

aznAPI -- Invalid String Value. (0x1005b5e5)

Explanation
A string value passed to the aznAPI interface is invalid.

Administrator response
Ensure that all strings passed to the interface are not NULL.

HPDAC1510E

aznAPI -- Unknown Label. (0x1005b5e6)

Explanation
The labelling authorization policy model is not implemented in the Security Verify Access authorization model.

Administrator response
No action is required.

HPDAC1511E

aznAPI -- Invalid Added Credentials Handle. (0x1005b5e7)

Explanation
See message.

Administrator response
Ensure that the 'creds to add' credentials handle output parameter passed to the aznAPI interface is valid.

HPDAC1512E

aznAPI -- Invalid Protected Resource. (0x1005b5e8)

Explanation
The specified protected resource is invalid.

Administrator response
Ensure that the protected resource is valid and the resource name meets the criteria set by Security Verify Access.

HPDAC1513E

aznAPI -- Invalid Operation. (0x1005b5e9)

Explanation
The operation string specified is invalid.

Administrator response
Ensure that the operation string supplied meets the criteria set by Security Verify Access.

HPDAC1514E

aznAPI -- Invalid PAC. (0x1005b5ea)

Explanation
The supplied PAC is invalid.

Administrator response
Ensure that the PAC parameter meets the criteria set by Security Verify Access.

HPDAC1515E

aznAPI -- Invalid PAC Service. (0x1005b5eb)

Explanation
A PAC service with the specified service ID was not found in the list of services registered with the aznAPI service dispatcher.

Administrator response
Ensure that the specified PAC service ID refers to a valid PAC service that has been loaded into the current aznAPI application.

HPDAC1516E

aznAPI -- Invalid Permission Information Reference. (0x1005b5ec)

Explanation
See message.

Administrator response
Ensure that the permission info credentials handle output parameter passed to the aznAPI interface is valid.

HPDAC1517E

aznAPI -- Invalid Credentials Modification Function. (0x1005b5ed)

Explanation
A credentials modification service with the specified service ID was not found in the list of services registered with the aznAPI service dispatcher.

Administrator response
Ensure that the specified credentials modification service ID refers to a valid credentials modification service that has been loaded into the current aznAPI application.

HPDAC1518E

aznAPI -- Invalid Subject Index. (0x1005b5ee)

Explanation
The specified index is out of range with respect to the number of subjects in the target credential.

Administrator response
Ensure that the index specified is within range for the target credential.

HPDAC1519E

aznAPI -- Unimplemented Function. (0x1005b5ef)

Explanation
This function is not implemented in the Security Verify Access authorization model.

Administrator response
No action is required.

HPDAC1520E

aznAPI -- Invalid Attribute List Handle. (0x1005b5f0)

Explanation
See message.

Administrator response
Ensure that the attribute list handle parameter is valid.

HPDAC1521E

aznAPI -- Invalid Attribute Name. (0x1005b5f1)

Explanation
An attribute name passed as an input parameter is NULL or does not exist in the target attribute list.

Administrator response
Ensure that the attribute name supplied is non-NULL and exists in the target attribute list.

HPDAC1522E

aznAPI -- Invalid Buffer. (0x1005b5f2)

Explanation
The buffer parameter passed in is NULL.

Administrator response
Ensure that the buffer parameter is valid.

HPDAC1523E

aznAPI -- Invalid Buffer Reference. (0x1005b5f3)

Explanation
The buffer pointer parameter passed in is NULL.

Administrator response
Ensure that the buffer pointer parameter is valid.

HPDAC1524E

aznAPI -- Invalid String Reference. (0x1005b5f4)

Explanation
The string pointer parameter passed in is NULL.

Administrator response
Ensure that the string pointer parameter is valid.

HPDAC1525E

aznAPI -- Attribute Value is not of type string. (0x1005b5f5)

Explanation
The function interface requires a string typed attribute value.

Administrator response
Ensure that the attribute value is of type string.

HPDAC1526E

aznAPI -- Attribute's index value is invalid. (0x1005b5f6)

Explanation
The attribute value index is out of range.

Administrator response
Specify an attribute value index within the range of available values for the attribute.

HPDAC1527E

aznAPI -- Invalid Integer Reference. (0x1005b5f7)

Explanation
The integer pointer parameter passed in is NULL.

Administrator response
Ensure that the integer pointer parameter is valid.

HPDAC1528E

aznAPI -- Invalid Permission Reference. (0x1005b5f8)

Explanation
The permission code pointer parameter passed in is NULL.

Administrator response
Ensure that the permission code pointer parameter is valid.

HPDAC1529E

aznAPI -- Invalid Domain Specified. (0x1005b5f9)

Explanation
The domain specified is not valid.

Administrator response
Specify a valid Security Verify Access domain.

HPDAC1530E

aznAPI -- Invalid Application Context Handle. (0x1005b5fa)

Explanation
See message.

Administrator response
Ensure that the application context attribute list handle parameter is valid.

HPDAC1531E

aznAPI -- Invalid Entitlements Handle. (0x1005b5fb)

Explanation
See message.

Administrator response
Ensure that the entitlements attribute list handle parameter is valid.

HPDAC1532E

aznAPI -- Invalid Labeling Scheme. (0x1005b5fc)

Explanation
The labelling authorization policy model is not implemented in the Security Verify Access authorization model.

Administrator response
No action is required.

HPDAC1533E

aznAPI -- Invalid Init Data Handle. (0x1005b5fd)

Explanation
See message.

Administrator response
Ensure that the initialization data attribute list handle parameter is valid.

HPDAC1534E

aznAPI -- Invalid Init Info Handle. (0x1005b5fe)

Explanation
See message.

Administrator response
Ensure that the initialization information attribute list handle reference is not NULL.

HPDAC1535E

aznAPI -- Attribute's value is not of type buffer. (0x1005b5ff)

Explanation
The function interface requires a buffer typed attribute value.

Administrator response
Ensure that the attribute value is of type buffer.

HPDAC1536E

aznAPI -- API is Uninitialized. (0x1005b600)

Explanation
An aznAPI interface was called before azn_initialize() was called. Only aznAPI attribute list interfaces can be called before azn_initialize().

Administrator response
Ensure that the application calls only aznAPI attribute list interfaces before calling azn_initialize().

HPDAC1537E

aznAPI -- API is Already Initialized. (0x1005b601)

Explanation
azn_initialize() has been called when the authorization runtime has already been initialized. To reinitialize the authorization runtime the application must call azn_shutdown() before calling azn_initialize() again.

Administrator response
Ensure that the application does not attempt to reinitialize the authorization runtime without first calling azn_shutdown().

HPDAC1538E

aznAPI -- Error in plugin service definition. (0x1005b602)

Explanation
See message.

Administrator response
Ensure that the service definition meets the criteria defined in the Authorization C API Developer's Reference.

HPDAC1539E

aznAPI -- Plugin service not found. (0x1005b603)

Explanation
The service ID specified was not found by the service dispatcher.

Administrator response
Ensure that the service ID specified refers to a valid service that has been loaded by the current aznAPI application.

HPDAC1540E

aznAPI -- Error while initializing plugin service. (0x1005b604)

Explanation
See message.

Administrator response
Refer to the application error logs and to the minor status code returned from azn_initialize() for more information about the reason for the service failure. Some services might also return attributes in the intialization information attribute list returned from azn_initialize(). The attributes can contain further information about the failure.

HPDAC1541E

aznAPI -- Error while shutting down plugin service. (0x1005b605)

Explanation
The plugin returned an error while shutting down.

Administrator response
Refer to the application error logs and to the minor status code returned from azn_shutdown() for more information about the the service failure. Some services might also return attributes in the intialization information attribute list returned from azn_shutdown(). The attributes can contain further information about the reason the service shutdown failed.

HPDAC1542E

aznAPI -- Error while authorizing plugin service. (0x1005b606)

Explanation
The plugin was not authorized to perform a task. This might also be due to insufficient privilege of the application server principal. It might also be due to incorrect service configuration.

Administrator response
Ensure that the aznAPI application server principal has the appropriate permissions to enable the aznAPI service to perform the required task. This error might also occur if the parameters supplied to the service plugin were not sufficient and should be reviewed.

HPDAC1543E

aznAPI -- Error while loading plugin service's shared library. (0x1005b607)

Explanation
The service dispatcher encountered an error while loading the aznAPI service plugin shared library.

Administrator response
Refer to the application error logs and to the minor status code returned from azn_initialize() for more information about the failure. The service dispatcher will also return an attribute in the intialization information attribute list returned from azn_initialize() if the information is available. The attribute will contain further information about the failure to load.

HPDAC1544E

aznAPI -- azn_svc_initialize() function not found in the shared library of the plug-in service. (0x1005b608)

Explanation
The shared library of the aznAPI service does not export an azn_svc_initialize() interface.

Administrator response
Review the service source code and build process to ensure that the shared library of the plug-in service exports an azn_svc_initialize() interface to applications.

HPDAC1545E

aznAPI -- azn_svc_shutdown() function not found in the shared library of the plug-in service. (0x1005b609)

Explanation
The shared library of the aznAPI service does not export an azn_svc_shutdown() interface.

Administrator response
Review the service source code and build process to ensure that the shared library of the plug-in service exports an azn_svc_shutdown() interface to applications.

HPDAC1546E

aznAPI -- azn_svc_entitlements_get_entitlements() function not found in the shared library of the plug-in service. (0x1005b60a)

Explanation
The aznAPI service shared library does not export an azn_svc_entitlement_get_entitlements() interface.

Administrator response
Review the service source code and build process to ensure that the shared library of the plug-in service exports an azn_svc_entitlement_get_entitlements() interface to applications.

HPDAC1547E

aznAPI -- PAC function not found in the shared library of the plug-in service. (0x1005b60b)

Explanation
The aznAPI service shared library does not export both an azn_svc_creds_get_pac() and an azn_svc_pac_get_creds() interface.

Administrator response
Review the service source code and build process to ensure that the shared library of the plug-in service exports both the azn_svc_creds_get_pac() and the azn_svc_pac_get_creds() interface to applications.

HPDAC1548E

aznAPI -- EAS function not found in the shared library of the plug-in service. (0x1005b60c)

Explanation
The aznAPI service shared library does not export an azn_svc_decision_access_allowed_ext() interface.

Administrator response
Review the service source code and build process to ensure that the shared library of the plug-in service exports an azn_svc_decision_access_allowed_ext() interface to applications.

HPDAC1549E

aznAPI -- Credentials modification function not found in the shared library of the plug-in service. (0x1005b60d)

Explanation
The aznAPI service shared library does not export an azn_svc_creds_modify() interface.

Administrator response
Review the service source code and build process to ensure that the shared library of the plug-in service exports an azn_svc_creds_modify() interface to applications.

HPDAC1550E

aznAPI -- Another plugin has already been registered with the same service ID. (0x1005b60e)

Explanation
See message.

Administrator response
Ensure that you have a unique service ID for the azn service loaded by the aznAPI application.

HPDAC1551E

aznAPI -- Failure in the aznAPI Service Dispatcher. (0x1005b60f)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1552E

aznAPI -- Message for the minor code is not found. (0x1005b610)

Explanation
A message string for this minor code was not found in the message catalogs.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1553E

aznAPI -- Invalid EAS ACL Action Trigger. (0x1005b611)

Explanation
The ACL actions/operations trigger specified was not valid.

Administrator response
Ensure that the trigger conforms to the criteria outlined in the Authorization C API Developer's Reference.

HPDAC1554E

aznAPI -- Invalid EAS POP Trigger. (0x1005b612)

Explanation
The POP-based EAS trigger attribute specified was not valid.

Administrator response
Ensure that the trigger conforms to the criteria outlined in the Authorization C API Developer's Reference.

HPDAC1555E

aznAPI -- Invalid EAS Weighting. (0x1005b613)

Explanation
The weighting value specified was negative or zero or the string could not be converted to an unsigned integer.

Administrator response
Ensure that the weighting is a positive non-zero integer value that is no greater than MAXULONG.

HPDAC1556E

aznAPI -- Unknown parameter specified in EAS plugin service definition. (0x1005b614)

Explanation
The EAS service definition is incorrectly formatted.

Administrator response
Ensure that the EAS service definitions conform to the criteria outlined in the Authorization C API Developer's Reference.

HPDAC1557E

aznAPI -- One or more protected Object functions not implemented in the Administration Service plugin's shared library. (0x1005b615)

Explanation
The aznAPI administration service shared library does not export both an azn_admin_get_object() and an azn_admin_get_objectlist() interface.

Administrator response
Review the service source code and build process to ensure that the service plugin shared library exports both the azn_admin_get_object() and the azn_admin_get_objectlist() functions to applications.

HPDAC1558E

aznAPI -- Invalid Protected Object. (0x1005b616)

Explanation
The protected object structure passed as a parameter is invalid.

Administrator response
Ensure that the protected object structure parameter is valid.

HPDAC1559E

aznAPI -- Invalid Protected Object Reference. (0x1005b617)

Explanation
The protected object structure reference passed as a parameter is invalid.

Administrator response
Ensure that the protected object structure reference parameter is not NULL.

HPDAC1560E

aznAPI -- Attribute Value is not of type pobj. (0x1005b618)

Explanation
The function interface requires an azn_pobj_t typed attribute value.

Administrator response
Ensure that the attribute value is of type azn_pobj_t.

HPDAC1561E

aznAPI -- Unknown parameter specified in Administration service plugin's definition. (0x1005b619)

Explanation
The Administration Service plugin definition has a parameter that is invalid.

Administrator response
Ensure that you have specified the correct parameter in the AZN Administration Service plugin definition. Refer to the publications for information about supported parameters.

HPDAC1562E

aznAPI -- Protected Object path is not specified in Administration service plugin's definition. (0x1005b61a)

Explanation
The Administration Service plugin definition specifies the -pobj parameter without a protected object hierarchy name following it.

Administrator response
Ensure that you have specified the correct protected object hierarchy name following the -pobj parameter in the Administration Service plugin definition.

HPDAC1563E

aznAPI -- One of the task functions is not found in the Administration service plugin's shared library. (0x1005b61b)

Explanation
The aznAPI administration service shared library does not export both an azn_admin_get_tasklist() and an azn_admin_get_task() interface.

Administrator response
Review the service source code and build process to ensure that the service plugin shared library exports both the azn_admin_get_tasklist() and the azn_admin_get_task() functions to applications.

HPDAC1564E

aznAPI -- Protected Object hierarchy name has already been registered by another Administration service definition. (0x1005b61c)

Explanation
Another Administration Service definition has already registered the protected object hierarchy name being registered by the current Administration Service definition.

Administrator response
Specify another protected object hierarchy name for this Administration Service definition or modify the definition that uses this protected object hierarchy name.

HPDAC1565E

aznAPI -- Invalid Message ID Reference. (0x1005b61d)

Explanation
The message ID pointer parameter is NULL.

Administrator response
Ensure that the message ID pointer parameter is not NULL

HPDAC1566E

aznAPI -- Message for the major code is not found. (0x1005b61e)

Explanation
A message string for this major code was not found in the message catalogs.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1567E

aznAPI -- Attribute Value is not of type unsigned long. (0x1005b61f)

Explanation
The function interface requires an unsigned long attribute value.

Administrator response
Ensure that the attribute value is of type unsigned long.

HPDAC1568E

aznAPI -- Administration Service -- Invalid Service Info Handle passed to plugin's shared library. (0x1005b620)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1569E

aznAPI -- Administration Service -- Invalid Argument Count passed to plugin's shared library. (0x1005b621)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1570E

aznAPI -- Administration Service -- Invalid Argument Array passed to plugin's shared library. (0x1005b622)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1571E

aznAPI -- Administration Service -- Plugin's shared library received an out-of-memory error. (0x1005b623)

Explanation
In most cases this error due to the aznAPI application program running out of memory.

Administrator response
Ensure that the application has been configured with sufficient virtual memory for its requirements. The Security Verify Access Performance Tuning Guide contains instructions on how to ensure that the application is configured with the correct amount of virtual memory. Stop and restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1574E

aznAPI -- Entitlements Service -- Invalid Service Info Handle passed to plugin's shared library. (0x1005b626)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1575E

aznAPI -- Entitlements Service -- Invalid Argument Count passed to plugin's shared library. (0x1005b627)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1576E

aznAPI -- Entitlements Service -- Invalid Argument Array passed to plugin's shared library. (0x1005b628)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1577E

aznAPI -- Entitlements Service -- Plugin's shared library received an out-of-memory error. (0x1005b629)

Explanation
In most cases this error due to the aznAPI application program running out of memory.

Administrator response
Ensure that the application has been configured with sufficient virtual memory for its requirements. The Security Verify Access Performance Tuning Guide contains instructions on how to ensure that the application is configured with the correct amount of virtual memory. Stop and restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1579E

aznAPI -- EAS -- Invalid Service Info Handle passed to plugin's shared library. (0x1005b62b)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1580E

aznAPI -- EAS -- Invalid Argument Count passed to plugin's shared library. (0x1005b62c)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1581E

aznAPI -- EAS -- Invalid Argument Array passed to plugin's shared library. (0x1005b62d)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1582E

aznAPI -- EAS -- Plugin's shared library received an out-of-memory error. (0x1005b62e)

Explanation
In most cases this error due to the aznAPI application program running out of memory.

Administrator response
Ensure that the application has been configured with sufficient virtual memory for its requirements. The Security Verify Access Performance Tuning Guide contains instructions on how to ensure that the application is configured with the correct amount of virtual memory. Stop and restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1584E

aznAPI -- Credential Modification Service -- Invalid Service Info Handle passed to plugin's shared library. (0x1005b630)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1585E

aznAPI -- Credential Modification Service -- Invalid Argument Count passed to plugin's shared library. (0x1005b631)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1586E

aznAPI -- Credential Modification Service -- Invalid Argument Array passed to plugin's shared library. (0x1005b632)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1587E

aznAPI -- Credential Modification Service -- Plugin's shared library received an out-of-memory error. (0x1005b633)

Explanation
In most cases this error due to the aznAPI application program running out of memory.

Administrator response
Ensure that the application has been configured with sufficient virtual memory for its requirements. The Security Verify Access Performance Tuning Guide contains instructions on how to ensure that the application is configured with the correct amount of virtual memory. Stop and restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1589E

aznAPI -- PAC Service -- Invalid Service Info Handle passed to plugin's shared library. (0x1005b635)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1590E

aznAPI -- PAC Service -- Invalid Argument Count passed to plugin's shared library. (0x1005b636)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1591E

aznAPI -- PAC Service -- Invalid Argument Array passed to plugin's shared library. (0x1005b637)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1592E

aznAPI -- PAC Service -- Plugin's shared library received an out-of-memory error. (0x1005b638)

Explanation
In most cases this error due to the aznAPI application program running out of memory.

Administrator response
Ensure that the application has been configured with sufficient virtual memory for its requirements. The Security Verify Access Performance Tuning Guide contains instructions on how to ensure that the application is configured with the correct amount of virtual memory. Stop and restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1594E

aznAPI -- Initialization failed because a non-zero SSL-listening port is not specified. (0x1005b63a)

Explanation
aznAPI could not be initialized because a non-zero SSL-listening port has not been specified. This SSL-listening port is needed either because an AZN Administration Service is registered OR local mode has been configured and listen-flags have been set to enable.

Administrator response
Use svrsslcfg or edit the aznAPI configuration file to specify a non-zero SSL-listening port

HPDAC1595E

aznAPI -- Major code is invalid. (0x1005b63b)

Explanation
The major code portion of the aznAPI status is invalid. So, the error string corresponding to it cannot be retrieved by this API.

Administrator response
Make sure you enter a valid aznAPI major code. Look in the ogauthzn.h header file for valid values for aznAPI major code.

HPDAC1596E

aznAPI -- Modification of the attribute is prohibited. (0x1005b63c)

Explanation
The specified attribute is read-only. Modification of the attribute is prohibited. This is because the attribute is an important attribute for the purposes of authorization that will affect the user's access permissions if it is changed.

Administrator response
Specify the name of an attribute that is not a read-only attribute. If you want to add group memberships to the credential then refer to the Authorization C API Developer's Reference for information about the supplied credentials modification service that can be used to add groups to a credential.

HPDAC1597E

aznAPI -- azn_init_ssl_local_domain cannot override the SSL-local-domain entry in the aznAPI client configuration file. (0x1005b63d)

Explanation
The azn_init_ssl_local_domain initialization attribute cannot override ssl-local-domain entry that is specified in the aznAPI client configuration file. These two entries must always match because a client can be configured to run in only one domain.

Administrator response
The simplest action is to accept the configured default for the authzn_authority parameter by specifying NULL.

HPDAC1598E

aznAPI -- Uninitialized Mechanism Info structure. (0x1005b63e)

Explanation
See message.

Administrator response
Ensure that the mechanism info structure is initialized to 0 for those un-used fields.

HPDAC1599E

The account associated with the DN of the certificate presented to the Policy server does not match the server account owning the values being updated. The Policy server log contains the account names. (0x1005b63f)

Explanation
When the server starts it connects to the Policy server to update it's values for host name, port, version, listening status and administration services. The Policy server extracts the DN of the the certificate of the connection made to make this update. If the Verify Access account associated with the DN does match that of the server information being updated it will fail the request.

Administrator response
Check the server configuration to ensure it is using the correct value for [ssl] ssl-keyfile. Alternatively set [ssl] ssl-enhanced-security = no in the Policy server configuration file.

HPDAC1600E

The account '*%s*' associated with the DN of the certificate presented to the Policy server does not match the server account '*%s*' owning the values being updated. (0x1005b640)

Explanation

When the server starts it connects to the Policy server to update it's values for host name, port, version, listening status and administration services. The Policy server extracts the DN of the the certificate of the connection made to make this update. If the Verify Access account associated with the DN does match that of the server information being updated it will fail the request.

Administrator response

Check the server configuration to ensure it is using the correct value for [ssl] ssl-keyfile. Alternatively set [ssl] ssl-enhanced-security = no in the Policy server configuration file.

HPDAC1650E

AZN Entitlements Extended Attributes Service - app_context does not contain any attribute names. (0x1005b672)

Explanation

No entitlements can be returned by this API because the provided app_context does not specify the object for which attributes are needed.

Administrator response

Ensure that the app_context contains one of the following valid attribute names - OBJ, ACL, or POP.

HPDAC1651E

AZN Entitlements Extended Attributes Service - app_context contains more than one attribute name. (0x1005b673)

Explanation

No entitlements can be returned by this API because the provided app_context contains more than one object name for which attributes are needed.

Administrator response

Ensure that the app_context contains only one of the following valid attribute names - OBJ, ACL, POP

HPDAC1652E

AZN Entitlements Extended Attributes Service - app_context contains an invalid attribute name. (0x1005b674)

Explanation

No entitlements can be returned by this API because the provided app_context contains an invalid object name for which attributes are needed.

Administrator response

Ensure that the app_context contains only one of the following valid attribute names - OBJ, ACL, POP

HPDAC1653E

AZN service plug-in *%s* failed to shutdown (0x*%x*/0x*%x*). (0x1005b675)

Explanation
A plug-in failed to shutdown correctly and returned an error code to the service dispatcher.

Administrator response
Check the returned error status for more detail.

HPDAC1654E

The SOAP client of the AMWebARS entitlement service returned an error. (0x1005b676)

Explanation
The SOAP request failed, and the gSOAP client returned an error code which is printed in the error log.

Administrator response
Consult gSOAP documentation for the meaning of the error code that accompanies this message in the error log.

HPDAC1655E

The SOAP client of the AMWebARS entitlement service returned the error code: *%d*. (0x1005b677)

Explanation
The SOAP request failed, and the gSOAP client returned the error code which is printed in the error log.

Administrator response
Consult gSOAP documentation for the meaning of the error code that accompanies this message in the error log.

HPDAC1656E

The AMWebARS entitlement service returned the internal error: *%s*. (0x1005b678)

Explanation
The SOAP request succeeded, but the AMWebARS Web Service returned an error message which was printed to the error log.

Administrator response
Review the accompanying error message and ensure that the AMWebARS service is configured correctly.

HPDAC1657E

The AMWebARS entitlement service URL is NULL. (0x1005b679)

Explanation
See message.

Administrator response
Review the Security Verify Access authorization client configuration file and ensure that the AMWebARS service URL has been specified correctly.

HPDAC1658E

An error occurred loading the aznAPI configuration file. (0x1005b67a)

Explanation
See message.

Administrator response
Review the aznAPI configuration file used to initialize the AMWebARS service and ensure that it exists and is a valid stanza format file and that the entries conform to stanza format syntax.

HPDAC1659W

No configuration file specified for the credential attributes entitlement service *%s*. (0x1005b67b)

Explanation
This service might not function correctly without proper configuration either from a file or API input.

Administrator response
If a configuration file was intended, check that it is passed to the service either as an attribute or argument to the service library.

HPDAC1660W

No service configuration information was found in the specified file *%s*. (0x1005b67c)

Explanation
Service and attribute configuration was not found in the configuration file. This causes the servce to return withoout any entitlements.

Administrator response
Check that the service and attributes are configured correctly in the configuration file.

HPDAC1661W

The registry operations for source *%s* failed. (0x1005b67d)

Explanation
A registry operation failed for the specified source. This source is skipped.

Administrator response
No action needed.

HPDAC1667E

The AXIS client of the AMWebARS entitlement service returned the error : *%s*. (0x1005b683)

Explanation
The AXIS request failed, and the AXIS C++ client returned the error wh ich is printed in the error log.

Administrator response
Consult AXIS documentation for the meaning of the error.

HPDAC1668E

The AXIS client of the AMWebARS entitlement service returned the unkno wn error. (0x1005b684)

Explanation
See message.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1669E

An unexpected AXIS exception was caught during the call to AMWebArs we b service. Refer to the error log for more information about the exception. (0x1005b685)

Explanation
AXIS C++ client returned an exception condition to AMWebArs entitlemen t service that was not handled and not expected.

Administrator response
Refer to the error log to determine if an error message accompanied th e e xception.

HPDAC1670E

An unexpected AXIS exception was caught during the call to AMWebArs we b service. Error message *%s* was returned with the exception. (0x1005b686)

Explanation
AXIS returned an exception condition to the AMWebARS entitlement servi ce that was not handled and not expected.

Administrator response
Refer to the error log to determine if an error message accompanied th e e xception.

HPDAC1950E

Registry client unavailable. (0x1005b79e)

Explanation
This failure can occur when the registry server configuration settings are incorrect, or when the Security Verify Access runtime is incorrectly configured for a registry type other than that required.

Administrator response
Ensure that you have correctly configured the Security Verify Access Runtime package for the desired user registry. The current user registry setting can be determined by looking at the 'user-reg-type' entry in the [pdrte] stanza of the 'etc/pd.conf' file in the Security Verify Access install directory. If the runtime is configured incorrectly, you will need to unconfigure all packages and reconfigure the machine again. If the runtime has been correctly configured, then ensure that the configuration parameters specified for the user registry server are correct.

HPDAC1951E

Registry client returned a memory error. (0x1005b79f)

Explanation
The registry client encountered a memory error.

Administrator response
Ensure that the affected process has been configured with sufficient virtual memory for its requirements. Stop and restart the process. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1952E

Registry configuration file has invalid contents. (0x1005b7a0)

Explanation
The user registry configuration file is invalid.

Administrator response
Review the registry configuration file in the Security Verify Access 'etc' directory and ensure that the entries are valid. If the problems persists then reconfigure the Security Verify Access runtime package.

HPDAC1953E

Registry failed opening or closing a database file. (0x1005b7a1)

Explanation
See message.

Administrator response
Shutdown and restart the registry server. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1954E

SSL communications with the registry returned an error. (0x1005b7a2)

Explanation
See message.

Administrator response
Shutdown and restart the registry server. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1955E

Non-SSL registry communications returned an error. (0x1005b7a3)

Explanation
See message.

Administrator response
Shutdown and restart the registry server. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1956E

Registry client initialization failed. (0x1005b7a4)

Explanation
A registry API call was made with an invalid parameter, or the registry type could not be determined or the registry is not configured correctly.

Administrator response
Shutdown and restart the registry server. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1957E

Registry server is down or cannot be contacted. (0x1005b7a5)

Explanation
The user registry server is not running.

Administrator response
Ensure that the user registry server is running and that the registry client has been correctly configured to communicate with the server.

HPDAC1958E

Authentication data was incorrectly specified or it is missing. (0x1005b7a6)

Explanation
The aznAPI runtime was unable to authenticate to the user registry.

Administrator response
Ensure that the user registry is configured correctly, that it is operational and that the authentication parameters supplied are valid.

HPDAC1959E

Specified member was not found in the registry group. (0x1005b7a7)

Explanation
The group has no members or the specified member was not found in the group.

Administrator response
Verify that the group name and member name is spelled correctly and that they both exist in the registry database for the domain to which you are logged in.

HPDAC1961E

Multiple registry routing is not supported. (0x1005b7a9)

Explanation
An attempt was made to use multiple registry routing, which is not a supported function.

Administrator response
Disable multiple registry routing in the client and your applications. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1962W

The end of the registry list has been reached. (0x1005b7aa)

Explanation
An internal error has occurred. A program processing a list of registry entries has tried to get an entry beyond the end of the list.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1963E

Unable to locate a group in the registry with the name supplied. (0x1005b7ab)

Explanation
The specified group name was not found in the registry database.

Administrator response
Verify that the group name is spelled correctly and that it exists in the registry database for the domain to which you are logged in.

HPDAC1965E

Invalid user type specified. (0x1005b7ad)

Explanation
An internal error has occurred. When the calling program requested a list of users from the registry it did not specify one of the 3 permitted user types.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1966E

Invalid group type specified. (0x1005b7ae)

Explanation
An internal error has occurred. When the calling program requested a list of groups from the registry it did not specify one of the 3 permitted group types.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1967E

Group name is invalid or not found in the registry. (0x1005b7af)

Explanation
A group operation was attempted for the wrong domain or the group's registry GID value (also known as the DN) was invalid. The DN entered might contain invalid characters or be in an invalid format.

Administrator response
Correct the registry group name (or DN) that you specified and retry the operation.

HPDAC1968E

Policy name is invalid or not found in the registry. (0x1005b7b0)

Explanation
An internal error has occurred. A user specific policy that was expected to be in the registry was not found.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1969E

Resource name is invalid or not found in the registry. (0x1005b7b1)

Explanation
An internal error has occurred. A resource that was expected to be in the registry was not found.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1970E

Resource group name is invalid or not found in the registry. (0x1005b7b2)

Explanation
An internal error has occurred. A resource group that was expected to be in the registry was not found.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1971E

User's Resource Credentials are invalid or not found in the registry. (0x1005b7b3)

Explanation
An internal error has occurred. A resource credential that was expected to be in the registry was not found.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1972E

The specified user is already in the registry. (0x1005b7b4)

Explanation
A user with the specified name is already in the registry.

Administrator response
Select another name or a variation for this user.

HPDAC1973E

The specified group is already in the registry. (0x1005b7b5)

Explanation
A group with the specified name is already in the registry.

Administrator response
Select another name or a variation for this group.

HPDAC1974E

The specified policy is already in the registry. (0x1005b7b6)

Explanation
A policy object already exists for the specified user.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAC1975E

The specified resource is already in the registry. (0x1005b7b7)

Explanation
A resource object already exists with the specified name.

Administrator response
Select another name for the new resource object.

HPDAC1976E

The specified resource group is already in the registry. (0x1005b7b8)

Explanation
A resource group object with the specified name already exists in the registry.

Administrator response
Select another name for the new resource group object.

HPDAC1977E

The specified resource credentials are already in the registry. (0x1005b7b9)

Explanation
A resource credential object with the specified name already exists.

Administrator response
Select another name for which to create a resource credential object.

HPDAC1978E

Multiple users found in the registry using the specified search criteria. (0x1005b7ba)

Explanation
More than one user in the registry shares the specified name.

Administrator response
Select another user name or modify the users to have unique names.

HPDAC1979E

Multiple groups found in the registry using the specified search criteria. (0x1005b7bb)

Explanation
More than one group in the registry shares the specified name.

Administrator response
Select another group name or modify the groups to have unique names.

HPDAC1980E

Registry client returned a failure status. (0x1005b7bc)

Explanation
The user registry client returned an error code that was unexpected or unknown to Security Verify Access.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAU0100E

Invalid config URL (0x30654064)

Explanation
A Non null config URL should be passed for AMAuditServer constructor

Administrator response
Ensure that a non null configURL is passed to the AMAuditServer constructor

HPDAU0101E

Invalid listen port: (0x30654065)

Explanation
Ensure that a non null port is specified, and the AMAuditServer is not already running.

Administrator response
Either the port is not specified or the port is already in use

HPDAU0102E

Socket listen error (0x30654066)

Explanation
Error Listening to the socket

Administrator response
Error listening to the socket

HPDAU0103E

Invalid command line argument list (0x30654067)

Explanation
Invalid arguments, Make sure the command line arguments are correct

Administrator response
Make sure the command line arguments are correct

HPDAU0104E

Config file properties not found *%s* . (0x30654068)

Explanation
Make sure the config file exists and it is valid

Administrator response
A valid config file should be specified.

HPDAU0105E

Properties file *%s* not found. (0x30654069)

Explanation
Make sure the properties file exists and it is valid

Administrator response
Ensure that the properties file exists and is valid.

HPDAU0106E

Properties not found. (0x3065406a)

Explanation
Make sure the properties exists and it is valid

Administrator response
Ensure that the properties exists and is valid.

HPDAU0107E

Acceptor wait failed; no connection was created (0x3065406b)

Explanation
Acceptor wait failed; no connection was created

Administrator response
Acceptor wait failed; no connection was created

HPDAU0108E

AMAudit component is already inited. (0x3065406c)

Explanation
AMAudit component is already inited.

Administrator response
AMAudit component is already inited.

HPDAU0109E

AMAudit component is not inited. (0x3065406d)

Explanation
AMAudit shutdown called before calling AMAudit init.

Administrator response
AMAudit component should be inited before calling shutdown.

HPDAU0110E

AMAudit component is not shutdown. (0x3065406e)

Explanation
AMAudit component is not shutdown.

Administrator response
AMAudit component is not shutdown.

HPDAU0111E

No acceptor class. (0x3065406f)

Explanation
No acceptor class specified.

Administrator response
Specify a valid acceptor

HPDAU0112E

Bad acceptor class : *%s*. (0x30654070)

Explanation
Bad acceptor class specified.

Administrator response
Specify a valid acceptor

HPDAU0113E

Could not initialize acceptor : *%s* on on attempt # *%s* (0x30654071)

Explanation
Bad or no acceptor class.

Administrator response
Specify a valid acceptor

HPDAU0114E

Invalid argument: Null messages. (0x30654072)

Explanation
A nonnull PDMessages object is required to hold any return messages that might be generated during the operation. Typically, this object contains no messages on input.

Administrator response
Ensure that the messages argument is nonnull.

HPDAU0116E

Wild char not in template. (0x30654074)

Explanation
Wild char required in the template.

Administrator response
Ensure that the wild char is in the template.

HPDAU0117E

Invalid Archive file prefix. (0x30654075)

Explanation
Archive file names cannot be a directory.

Administrator response
Ensure that the Archive file name is not a directory.

HPDAU0118E

Archive file create error. (0x30654076)

Explanation
No write permission on the archive directory

Administrator response
Ensure that you have write permission on the directory where the archive file is created.

HPDAU0119E

Unable to execute archive program %s. (0x30654077)

Explanation
Archive cmdFile should exist.

Administrator response
Ensure that executable file exists.

HPDAU0120E

A database error occurred while exporting the table (0x30654078)

Explanation
A database error occurred while exporting the table.

Administrator response
No action required.

HPDAU0121E

Archive program was interrupted by user (0x30654079)

Explanation
Archive program was interrupted by user.

Administrator response
No action required.

HPDAU0122E

Invalid command line option was specified (0x3065407a)

Explanation
Valid command line options are required.

Administrator response
Ensure that the command line options are valid.

HPDAU0123E

Unable to purge audit record. (0x3065407b)

Explanation
Unable to purge audit record.

Administrator response
No action required.

HPDAU0124E

Archive and signing was successful for file *%s*. (0x3065407c)

Explanation
Archive and signing was successful.

Administrator response
No action required.

HPDAU0125E

Archive and signing failed for file *%s*. (0x3065407d)

Explanation
Archive and signing failed.

Administrator response
No action required.

HPDAU0126E

Signing key could not be unlocked (0x3065407e)

Explanation
Signing key should be accessible.

Administrator response
Ensure that the signing key is accesible.

HPDAU0127E

Unable to write to the signature file. (0x3065407f)

Explanation
Unable to write to signature file.

Administrator response
Ensure that you have valid signature file.

HPDAU0128E

Unable to sign data. (0x30654080)

Explanation
Unable to sign data.

Administrator response
Ensure that you can sign the data.

HPDAU0134E

Unable to send audit event to server, *%s* : (0x30654086)

Explanation
AuditServer should be up and running.

Administrator response
Ensure that the AuditServer is running

HPDAU0135E

Unknown host : *%s*, port : *%s* (0x30654087)

Explanation
Valid host and port where AuditServer is running, is required.

Administrator response
Ensure that the host and port are valid

HPDAU0136E

Connection exception, connecting to host : *%s*, port : *%s* (0x30654088)

Explanation
Valid host and port where AuditServer is running, is required.

Administrator response
Ensure that the host and port are valid

HPDAU0137E

IOException connecting to audit server : *%s*, port : *%s* (0x30654089)

Explanation
Valid host and port where AuditServer is running, is required.

Administrator response
Ensure that the host and port are valid

HPDAU0138E

Bad properties file *%s*. (0x3065408a)

Explanation
Make sure the properties file exists and it is valid

Administrator response
A valid properties file should be specified.

HPDAU0139E

Could not check if there are more record from audit_log query (0x3065408b)

Explanation
Make sure that there is no problem, while reading the log.

Administrator response
Ensure that there is no problem while querying the log.

HPDAU0140E

Audit record access failed. (0x3065408c)

Explanation
Make sure that there is no problem accessing the audit records.

Administrator response
Ensure that there is no problem accessing the audit records.

HPDAU0142E

Couldn't get client source (0x3065408e)

Explanation
Client source should be present in the client properties file.

Administrator response
Ensure that the client properties file contains client source.

HPDAU0143E

Couldn't get server port (0x3065408f)

Explanation
Server port should be present in the client properties file.

Administrator response
Ensure that the client properties file contains server port.

HPDAU0144E

Couldn't get server host (0x30654090)

Explanation
Server host should be present in the client properties file.

Administrator response
Ensure that the client properties file contains server host.

HPDAU0145E

Couldn't get doAudit string (0x30654091)

Explanation
doAudit string should be present in the client properties file.

Administrator response
Ensure that the client properties file contains doAudit string.

HPDAU0146E

Couldn't get delivery policy (0x30654092)

Explanation
Delivery policy should be present in the client properties file.

Administrator response
Ensure that the client properties file contains delivery policy.

HPDAU0147E

Error initializing client delivery policy (0x30654093)

Explanation
A valid client properties file required.

Administrator response
Ensure that the client properties file is valid.

HPDAU0148E

AMAuditServer connection is not initialized (0x30654094)

Explanation
AMAuditServer should be running so client can connect to it.

Administrator response
Ensure that the AMAuditServer is running.

HPDAU0149E

Invalid driver manager: *%s* (0x30654095)

Explanation
Driver manager should be valid.

Administrator response
Ensure that the driver manager is valid.

HPDAU0150E

Could not connect to database, url = *%s* (0x30654096)

Explanation
A valid database url is required.

Administrator response
Ensure that the database url is valid.

HPDAU0151E

Failed to Initialize AMAuditLogWriter (0x30654097)

Explanation
Ensure that AMAuditLogWriter can be initialized without any errors.

Administrator response
Ensure that AMAuditLogWriter can be initialized without any errors.

HPDAU0152E

Audit record insertion failed : (0x30654098)

Explanation
Ensure that there is no SQL error.

Administrator response
Ensure that there is no SQL error.

HPDAU0153E

Config file is already specified in command args (0x30654099)

Explanation
Config file is already specified in command args.

Administrator response
Config file is already specified in command args.

HPDAU0158E

Audit database is not initialized (0x3065409e)

Explanation
Audit database should be initialized.

Administrator response
Ensure that the Audit database is initialized.

HPDAU0159E

No Services configured : *%s* (0x3065409f)

Explanation
Services should be configured.

Administrator response
Ensure that at least one service is configured.

HPDAU0208E

Error Reading input stream; abandoning Connection. (0x306540d0)

Explanation
A valid message input stream required.

Administrator response
Ensure that the message InputStream valid

HPDAU0209E

Error Reading input stream end of file ; aborting Connection. (0x306540d1)

Explanation
A valid End of File for input stream required.

Administrator response
Ensure that the input stream has a valid End of File.

HPDAU0210E

Unexpected connection termination. (0x306540d2)

Explanation
A valid connection required.

Administrator response
Ensure that there is no Unexpected connection termination.

HPDAU0211E

Bad configuration file: *%s* (0x306540d3)

Explanation
A valid configuration required.

Administrator response
Ensure that the configuration is valid.

HPDAU0212E

Bad configuration, cannot continue. (0x306540d4)

Explanation
A valid configuration required.

Administrator response
Ensure that the configuration is valid.

HPDAU0213E

Input stream or output stream is null. (0x306540d5)

Explanation
A valid Input and output stream required.

Administrator response
Ensure that the input stream or output stream is not null..

HPDAU0214E

Error reading configuration file (0x306540d6)

Explanation
A valid configuration required.

Administrator response
Ensure that the configuration is valid.

HPDAU0215E

Configuration file not found: *%s* (0x306540d7)

Explanation
A valid configuration required.

Administrator response
Ensure that the configuration exists and is valid.

HPDAU0216E

Configuration file not found: (0x306540d8)

Explanation
A valid configuration required.

Administrator response
Ensure that the configuration exists and is valid.

HPDAU0217E

Event config filename cannot be null (0x306540d9)

Explanation
A Non null config file required.

Administrator response
Ensure that the config file is not null.

HPDAU0218E

Bad event stream format : *%s* (0x306540da)

Explanation
Event stream should contain 'true' or 'false'.

Administrator response
Expecting 'true' or 'false' in event stream.

HPDAU0219E

Bad event stream format : *%s* (0x306540db)

Explanation
Event stream should contain numbers.

Administrator response
Expecting number in event stream.

HPDAU0220E

Bad event stream format, type value = : %s (0x306540dc)

Explanation
Event config stream should contain string.

Administrator response
Expecting string in event config stream.

HPDAU0221E

Bad event stream format, type value = : %s (0x306540dd)

Explanation
Event stream should contain character.

Administrator response
Expecting character in event config stream.

HPDAU0222E

Daemon configuration error, config file = : %s (0x306540de)

Explanation
Error configuring daemon.

Administrator response
Error configuring daemon.

HPDAU0224E

SQL error : Daemon could not access System table (0x306540e0)

Explanation
The system table should be accessible.

Administrator response
Ensure that the system table is accessible.

HPDAU0225E

SQL error : Could not insert event to database (0x306540e1)

Explanation
Could not insert the event into the database.

Administrator response
Ensure that the database is accessible.

HPDAU0226E

SQL error : Could not insert element to database: *%s* (0x306540e2)

Explanation
Could not insert the element into the database.

Administrator response
Ensure that the database is accessible.

HPDAU0227E

SQL error : Could not insert attribute to database: *%s* (0x306540e3)

Explanation
Could not insert the attribute into the database.

Administrator response
Ensure that the database is accessible.

HPDAU0228E

Can't find COM.ibm.db2.jdbc.app.DB2Driver (0x306540e4)

Explanation
COM.ibm.db2.jdbc.app.DB2Driver should be in the classpath.

Administrator response
Ensure that the class COM.ibm.db2.jdbc.app.DB2Driver is in path

HPDAU0300E

Invalid service name (0x3065412c)

Explanation
A Non null eventName is required.

Administrator response
Ensure that a non null eventName is specified

HPDAU0301E

Invalid service count (0x3065412d)

Explanation
A valid service count is required.

Administrator response
Ensure that a valid service count is specified

HPDAU0302E

Invalid event count (0x3065412e)

Explanation
A valid event count is required.

Administrator response
Ensure that a valid event count is specified

HPDAU0303E

Error reading event table (0x3065412f)

Explanation
A valid event table is required.

Administrator response
Ensure that the event table is valid.

HPDAU0304E

Error reading event config table: *%s* (0x30654130)

Explanation
A valid event config table is required.

Administrator response
Ensure that the event config table is valid.

HPDAU0305E

Event could not be found in config table: *%s* (0x30654131)

Explanation
Config table should contain the event.

Administrator response
Ensure that the event exists in the config table.

HPDAU0400E

Could not find msg class name in msg header (0x30654190)

Explanation
A valid message class required in message header.

Administrator response
Ensure that the message header has message class.

HPDAU0401E

Message class could not be found (0x30654191)

Explanation
A valid message class required in input stream.

Administrator response
Ensure that input stream has valid message class.

HPDAU0402E

Message class could not be instantiated (0x30654192)

Explanation
A valid message class that can be instantiated is required.

Administrator response
Ensure that message class can be instantiated.

HPDAU0403E

'End-of-msg' char not found in stream (0x30654193)

Explanation
A valid 'End-of-msg' character required in message input stream.

Administrator response
Ensure that message input strean has 'End-of-msg' character.

HPDAU0404E

Unexpected end of msg stream : *%s* (0x30654194)

Explanation
A valid 'End-of-msg' character required in message input stream.

Administrator response
Ensure that message input strean has 'End-of-msg' character.

HPDAU0405E

Failed closing service : *%s* (0x30654195)

Explanation
Service could not be closed.

Administrator response
Failed closing service.

HPDAU0406E

Control object *%s* has no bound service. (0x30654196)

Explanation
Control object should be bound to a service.

Administrator response
Control object is not bound to a service.

HPDAU0500E

Cannot bind service *%s* to control object (0x306541f4)

Explanation
A valid control service name is required.

Administrator response
Ensure that a valid control service name is specified

HPDAU0501E

Service could not be initialized. Service name = *%s* (0x306541f5)

Explanation
A valid service is required.

Administrator response
Ensure that a valid service name is specified

HPDAU0502E

Deleivery policy initialization failed. Service name = *%s* (0x306541f6)

Explanation
A valid delivery policy service is required.

Administrator response
Ensure that a valid delivery policy is specified

HPDAU0505E

Problem decoding audit event (0x306541f9)

Explanation
Problem decoding audit event

Administrator response
Problem decoding audit event

HPDAZ0100E

Unknown message code: %s. (0x30659064)

Explanation
The text for the message code could not be found in the message catalogs installed on the local system. This typically means that the policy server is at a more recent level than the client and has returned a code undefined in the client runtime. The documentation associated with the policy server installation should include the message code.

Administrator response
Consult the Error Message Reference to obtain the message text, explanation, and suggested actions for the message code.

HPDAZ0101E

The specified configuration or keystore file already exists. (0x30659065)

Explanation
The 'create' configuration action is designed to check for existing files and fail if they are found in order not to overwrite them accidentally.

Administrator response
To preserve existing files, specify new configuration and keystore file names. To overwrite existing files, specify the 'replace' configuration action.

HPDAZ0102E

An unexpected error has occurred. (0x30659066)

Explanation
See message.

Administrator response
See the error log for more information. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport.

HPDAZ0200E

Invalid argument: Null name. (0x306590c8)

Explanation
A nonnull name object is required when adding to a PDAttrs object.

Administrator response
Ensure that the name argument is nonnull.

HPDAZ0201E

Invalid argument: Null collection. (0x306590c9)

Explanation
A nonnull Collection object is required when adding to a PDAttrs object.

Administrator response
Ensure that the collection argument is nonnull.

HPDAZ0202E

Invalid argument: Null value. (0x306590ca)

Explanation
A nonnull value object is required when adding to a PDAttrs object.

Administrator response
Ensure that the value argument is nonnull.

HPDAZ0203E

Invalid argument: Null PDAttrs. (0x306590cb)

Explanation
A nonnull PDAttrs object is required when adding to a PDAttrs object.

Administrator response
Ensure that the PDAttrs argument is nonnull.

HPDAZ0204E

Invalid argument: Null or invalid QOP value. (0x306590cc)

Explanation
A valid, nonnull Quality Of Protection value is required.

Administrator response
Ensure that the QOP argument is nonnull and is one of the QOP_* constants defined in the PDStatics class.

HPDAZ0205E

Server error: No data was returned. (0x306590cd)

Explanation
No data was returned by the server. This usually indicates a server crash. If this reoccurs, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

Administrator response
Ensure that the Authorization server is up and rerun this operation.

HPDAZ0206E

Server error: Unexpected tag in data. (0x306590ce)

Explanation
Unexpected data was returned by the server. This usually indicates a client/server mismatch.

Administrator response
Ensure that the Java client is current with (within two releases of) the Security Verify Access server. If so, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAZ0207E

Invalid argument: Null name. (0x306590cf)

Explanation
A nonnull name object is required when constructing a PDAttr object.

Administrator response
Ensure that the name argument is nonnull.

HPDAZ0208E

Invalid argument: Null value. (0x306590d0)

Explanation
A nonnull value object is required when constructing a PDAttr object.

Administrator response
Ensure that the value argument is nonnull.

HPDAZ0209E

Server error: Unexpected number of values in data: *%d*. (0x306590d1)

Explanation
Unexpected data was returned by the server. This usually indicates a client/server mismatch.

Administrator response
Ensure that the Java client is current with (within two releases of) the Security Verify Access server. If so, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAZ0210E

Server error: Unexpected type of attrlist: *%d*. (0x306590d2)

Explanation
Unexpected data was returned by the server. This usually indicates a client/server mismatch.

Administrator response
Ensure that the Java client is current with (within two releases of) the Security Verify Access server. If so, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAZ0211E

Invalid argument: Collection contains objects other than PDAttrValue. (0x306590d3)

Explanation
The constructor only permits PDAttrValue objects in the Collection.

Administrator response
Ensure that the input Collection only contains PDAttrValue.

HPDAZ0212E

Invalid argument: Only PDAttrValue objects can be in this PDAttrValueList. (0x306590d4)

Explanation
A PDAttrValueList is only for PDAttrValue objects.

Administrator response
Ensure that the input is a PDAttrValue.

HPDAZ0213E

Invalid argument: Null Collection. (0x306590d5)

Explanation
A nonnull Collection object is required when adding to a PDAttrValueList object.

Administrator response
Ensure that the Collection argument is nonnull.

HPDAZ0214E

Invalid argument: Null bytes. (0x306590d6)

Explanation
A nonnull bytes object is required when constructing a PDBufferAttrValue object.

Administrator response
Ensure that the bytes argument is nonnull.

HPDAZ0215E

Invalid argument: Null PDAdmSvcPobj. (0x306590d7)

Explanation
A nonnull PDAdmSvcPobj object is required when constructing a PDPobjAttrValue object.

Administrator response
Ensure that the PDAdmSvcPobj argument is nonnull.

HPDAZ0216E

Invalid argument: Null string. (0x306590d8)

Explanation
A nonnull string object is required when constructing a PDStringAttrValue object.

Administrator response
Ensure that the string argument is nonnull.

HPDAZ0256E

Zero or more than one base entry is configured for the custom repository [*%s*]. Only one base entry is allowed. (0x38638100)

Explanation
This repository only allows one base entry.

Administrator response
Check the base entry that is configured with the custom repository in WebSphere Virtual member manager (VMM). Fix the VMM configuration for this repository and retry.

HPDAZ0257E

The custom configuration property [*%s*] and its value [*%s*] is either invalid or incorrect. (0x38638101)

Explanation
Either the custom configuration property is not supported or its value is incorrect.

Administrator response
Check WebSphere Virtual member manager (VMM) custom repository configuration for the property. Fix the VMM configuration for this repository and retry.

HPDAZ0258E

Cannot modify the entity property [*%s*]. The Security Verify Access custom registry adapter for WebSphere Virtual member manager does not support renaming an entity. (0x38638102)

Explanation
The Security Verify Access custom registry adapter for WebSphere Virtual member manager does not support renaming an entity.

Administrator response

HPDAZ0259E

The specified JRE (*%s*) does not exist. (0x33841103)

Explanation
The path does not contain a valid JRE

Administrator response
Try again with a valid JRE path

HPDAZ0260E

The \'full\' or \'standalone\' are the only options for configuration type. (0x33841104)

Explanation

Administrator response

HPDAZ0261E

'yes' or 'no' are the only acceptable values. (0x33841105)

Explanation
The value supplied was not 'yes' or 'no'.

Administrator response
Try again with an acceptable value of 'yes' or 'no'.

HPDAZ0262E

Unable to query information from pd.conf file. (0x33841106)

Explanation
See message.

Administrator response
Check the file permissions and path. Ensure the file is not locked by another process.

HPDAZ0263E

Unable to query local host name. (0x33841107)

Explanation
See message.

Administrator response
Ensure the machine has a valid host name.

HPDAZ0264E

The *%s* entry for the entity with DN: *%s* in the domain is missing the *%s* attribute. (0x33840108)

Explanation
The secUser or secGroup entry for the user or group in the domain is missing the required attribute that contains the entities ID.

Administrator response
Fix the inconsistency in the registry for the domain.

HPDAZ0265W

The entity with DN: *%s* was not removed as others are still using it. (0x33840109)

Explanation
The secUser or secGroup entry for the user or group has been removed, however, it was also requested that the Native registry entry also be removed, and that was not possible. This is likely due to the entry being used by other applications or is a member of another Security Verify Access domain.

Administrator response
This warning can be ignored if it is acceptable that the Native registry entry was not removed. The entity has been removed from Security Verify Access domain so the entity will no longer be accessable through that domain.

HPDAZ0266E

The Security Verify Access domain *%s* does not exist. (0x3384010a)

Explanation
The Security Verify Access domain name provided was not found in the registry.

Administrator response
Provide a domain name to an existing domain.

HPDAZ0267E

There is no Security Verify Access entity in the domain with ID *%s*. (0x3384010b)

Explanation
The Security Verify Access user or group with the specified ID does not exist in the domain.

Administrator response
Verify the correct user or group ID was provided.

HPDAZ0268E

Unable to modify membership of the group *%s*, it is likely a dynamic group. (0x3384010c)

Explanation
It is likely that the user is a member of the group through a dynamic technique for which this API is not capable of modifying.

Administrator response
Use other methods to exclude or remove the user from the group membership.

HPDAZ0269E

The entity DN *%s* is already a member of the Security Verify Access domain. (0x3384010d)

Explanation
The user/group DN is already a member of the Security Verify Access domain and it is not valid to have more than one Security Verify Access entity for a DN in the domain.

Administrator response
Either delete the existing Security Verify Access entity associated with the DN or do not attempt the import/create.

HPDAZ0270E

The entity ID *%s* is already in use for the Security Verify Access domain. (0x3384010e)

Explanation
The user/group ID is used by another user/group within the domain. The ID must be unique.

Administrator response
Choose another user/group ID that is unique within the domain.

HPDAZ0271E

The entity ID *%s* is missing it's registry entry. (0x3384010f)

Explanation
The user/group ID has Security Verify Access domain information but is missing the underlying registry user/group entry. This situation should not be encountered in normal operation.

Administrator response
Fix the inconsistency in the registry for the domain.

HPDAZ0272E

The supplied DN, *%s*, to create the entity with has characters that are not valid. (0x33840110)

Explanation
Some characters can not be used in DNs.

Administrator response
Ensure the DN has valid characters.

HPDAZ0273E

The supplied entity ID, *%s*, to create the entity with has characters that are not valid. (0x33840111)

Explanation
Some characters can not be used in IDs.

Administrator response
Ensure the ID has valid characters.

HPDAZ0274E

The *%s* attribute value *%s* contains characters that are not valid. (0x33840112)

Explanation
Some or all of the characters in the attribute value are not valid.

Administrator response
Remove the invalid characters from the attribute and retry.

HPDAZ0275E

The *%s* attribute must be provided when creating the entity. (0x33840113)

Explanation
The attribute must be supplied for the creation of the entity.

Administrator response
Include the missing attribute and retry the operation.

HPDAZ0276E

The entity DN *%s* can not be created as it already exists. (0x33840114)

Explanation
The user/group DN already exists, but the API failed as it was asked to create it.

Administrator response
Consider importing the entity rather than attempting to create it.

HPDAZ0277E

Failed to add entity DN *%s* to ADAM registry, the DN is likely invalid. (0x33840115)

Explanation
ADAM returns operations error when the DN provided is not valid. This error has been mapped by the API to a more appropriate exception so that the caller of the API is presented with a more consistent interface.

Administrator response
Ensure the DN is valid for the ADAM registry and retry.

HPDAZ0278E

None of the configured LDAP servers of the appropriate type for the operation can be contacted. (0x33840116)

Explanation
Communication to all LDAP servers that are of the appropriate type, 'readwrite' for modification operation, 'readwrite' or 'readonly' for read operations, have failed, so the operation cannot be completed and has reported this failure.

Administrator response
Examine the log files for additional information about the server connection failures. Ensure at least one LDAP is operational and retry the operation..

HPDAZ0279E

The password must contain at least one character. (0x33840117)

Explanation
The API will not permit empty passwords to be used. This is done to emulate the same behavior of other Security Verify Access components. The use of empty passwords with LDAP can cause authentications to succeed even if the account password is not empty, causing a security issue.

Administrator response
Retry with a longer password.

HPDAZ0280E

There are more matching entries but the limit to return has been exceeded. (0x33840118)

Explanation
Either a supplied limit or an LDAP server configured limit on the number of matching entries to return has been exceeded. There are more matching entries, but they will not be returned.

Administrator response
If the additional entries are required, increase the limites and retry.

HPDAZ0281E

The old password supplied was rejected by the LDAP server. (0x33840119)

Explanation
Some LDAP servers return NoSuchAttribute errors when the old password, in a password change operation, is bad. The error has been remapped to a more appropriate InvalidOldPassword error.

Administrator response
Retry with the correct old password.

HPDAZ0282E

The password contains spaces and the policy does not permit this. (0x3384011a)

Explanation
The password policy for the user does not permit password containing spaces.

Administrator response
Retry with a password that does not contain spaces.

HPDAZ0283E

The password contains the same character repeated consecutively more than is permitted by policy: *%s*. (0x3384011b)

Explanation
The password policy for the user does not permit password containing repetitions of the same characters.

Administrator response
Retry with a password that does not contain repeated characters.

HPDAZ0284E

The password is too short, the policy minimum is *%s*. (0x3384011c)

Explanation
The password policy for the user specifies a minimum length and the password supplied is less that the minimum.

Administrator response
Retry with a longer password that conforms to policy.

HPDAZ0285E

The password does not contain enough alphabetic characters, the policy minimum is *%s*. (0x3384011d)

Explanation
The password policy for the user specifies a minimum number of alphabetic characters that must be present in the password.

Administrator response
Retry with enough alphabetic characters in the password to conform to policy.

HPDAZ0286E

The password does not contain enough non-alphabetic characters, the policy minimum is *%s*. (0x3384011e)

Explanation
The password policy for the user specifies a minimum number of non-alphabetic characters that must be present in the password.

Administrator response
Retry with enough non-alphabetic characters in the password to conform to policy.

HPDAZ0287E

The password must not begin with the *%s* character. (0x3384011f)

Explanation
The LDAP server does not permit password beginning with the specified character.

Administrator response
Retry with a password that begins with a different character.

HPDAZ0288E

A date value, *%s*, fetched from an LDAP value is not of form expected. (0x33840120)

Explanation
This API expects the date value to be of the form 'YYYYMMDDhhmmss.0Z'. The value fetched was not of this form so the operation cannot be completed.

Administrator response
The value must be corrected in the registry, before the operation will succeed.

HPDAZ0289E

The account has been disabled. (0x33840121)

Explanation
The account was previously temporarily locked out due to many authentication attempts which are not valid. However, policy changed to require account disablement instead.

Administrator response
Contact the account administrator to determine what can be done.

HPDAZ0290E

The account has been locked out. (0x33840122)

Explanation
The account was previously disabled due to many authentication attempts which are not valid, however, policy has changed since to only require temporary lockout instead.

Administrator response
Wait for the lockout period and retry. You can also contact the account administrator to determine what can be done.

HPDAZ0291E

The account is disabled. (0x33840123)

Explanation
The account is disabled and can not be used.

Administrator response
Contact the account administrator to determine what can be done.

HPDAZ0292E

The account has been temporarily locked. (0x33840124)

Explanation
The account has been temporarily locked and cannot be used for a preset wait period.

Administrator response
Wait for the lockout period and retry. You can also contact the account administrator to determine what can be done.

HPDAZ0293E

The account cannot be used at this time due to time-of-day policy restrictions. (0x33840125)

Explanation
The account has a Time-Of-Day policy associated with it that restricts access to specific times on specific days.

Administrator response
Retry at a time when account policy permits access.

HPDAZ0294E

The account is set invalid. (0x33840126)

Explanation
The account valid flag on the account is set to false.

Administrator response
The account cannot be used, Contact the account administrator to determine what can be done.

HPDAZ0295E

The account password is flagged as not valid. (0x33840127)

Explanation
The password valid flag on the account is set to false. This can be done by the account administrator to force a password change, or policy can automatically trigger it.

Administrator response
The account password valid flag is false must be changed to true before login can occur. Typically flag can be reset by changing the password on the account.

HPDAZ0296E

The time-of-day policy value, *%s*, fetched from an LDAP value is not of form expected. (0x33840128)

Explanation
This API expects the date value to be of the form 'days:start:end:zone' where: days - is a decimal number representing a bit mask of days of the week. start - is a decimal number representing the start minute of the day of allowed access. end - is a decimal number representing the end minute of the day of allowed access. zone - if set to 1 indicates that GMT time of day should be used, else server local time. The value fetched was not of this form so the operation cannot be completed.

Administrator response
The value must be corrected in the registry, before the operation will succeed.

HPDAZ0297E

The required configuration property *%s* was not found. (0x33840129)

Explanation
The API can not be used without the missing property being provided in the configuration file.

Administrator response
Add the required property to the configuration file.

HPDAZ0298E

The configuration property *%s* has an invalid value *%s*. (0x3384012a)

Explanation
The value assigned to the configuration property is not of the expected form.

Administrator response
Correct the property value in the configuration file.

HPDAZ0299E

The configuration property *%s* value *%s* is not in the range *%s* to *%s*. (0x3384012b)

Explanation
The value assigned to the configuration property is not within the acceptable range for that property.

Administrator response
Correct the property value in the configuration file.

HPDAZ0300E

The configuration property *%s* has an invalid server entry *%s*. (0x3384012c)

Explanation
The server entry is not of the expected form 'host:port:type:rank'.

Administrator response
Correct the server entry in the configuration file.

HPDAZ0301E

The configuration property *%s* has an invalid server entry *%s* port *%s*. (0x3384012d)

Explanation
The server entry port must be a decimal integer in the range 1 to 65535.

Administrator response
Correct the server entry port in the configuration file.

HPDAZ0302E

The configuration property *%s* has a server entry *%s* type *%s* which is not valid. (0x3384012e)

Explanation
The server entry type must be either 'readwrite' or 'readonly'.

Administrator response
Correct the server entry type in the configuration file.

HPDAZ0303E

The configuration property *%s* has a server entry *%s* rank *%s* which is not valid. (0x3384012f)

Explanation
The server entry ranking must be a decimal integer in the range 0 to 10.

Administrator response
Correct the server entry ranking in the configuration file.

HPDAZ0304E

The Relative Distinquished Name, *%s*, is of an unexpected form. (0x33840130)

Explanation
The first RDN of the DN provided is not of the expected form..

Administrator response
Resubmit the request with a valid Distinquished Name.

HPDAZ0305E

The registry reported the password has expired. (0x33840131)

Explanation
The underlying registry reported the password has expired. This is not due to any Security Verify Access policy, rather the policy of the underlying registry.

Administrator response
This condition might be cleared by updating the password.

HPDAZ0306E

The registry reported the account is locked. (0x33840132)

Explanation
The underlying registry reported the account is locked. This is not due to any Security Verify Access policy, rather the policy of the underlying registry.

Administrator response
Contact the underlying registry administrator for a solution.

HPDAZ0307E

The registry reported the password must be changed after reset. (0x33840133)

Explanation
The underlying registry reported the password needs changing as the password was reset and no other other actions can take place for this account until then. This is not due to any Security Verify Access policy, rather the policy of the underlying registry.

Administrator response
This condition might be cleared by updating the password.

HPDAZ0308E

The registry reported the password can not be changed. (0x33840134)

Explanation
The underlying registry reported that the password can not be be changed. This is not due to any Security Verify Access policy, rather the policy of the underlying registry.

Administrator response
Contact the underlying registry administrator for a solution.

HPDAZ0309E

The registry reported the password old password must be supplied during the change. (0x33840135)

Explanation
The underlying registry reported that the password cannot be be changed without supplying the existing password as well as the new password. This is not due to any Security Verify Access policy, rather the policy of the underlying registry.

Administrator response
Contact the underlying registry administrator for a solution.

HPDAZ0310E

The registry reported the new password does not pass its policy syntax rules. (0x33840136)

Explanation
The underlying registry reported that the new password supplied does not have the correct mix of character types in it. This is not due to any Security Verify Access policy, rather the policy of the underlying registry.

Administrator response
Change the content of the password and resubmit.

HPDAZ0311E

The registry reported the new password is too short. (0x33840137)

Explanation
The underlying registry reported that the new password supplied is not long enough. This is not due to any Security Verify Access policy, rather the policy of the underlying registry.

Administrator response
Increase the length of the new password and resubmit

HPDAZ0312E

The registry reported that more time is required before the password can be changed again. (0x33840138)

Explanation
The underlying registry reported that it will not allow changes to the passwod until a preset amount of time has passed since the last change. This is not due to any Security Verify Access policy, rather the policy of the underlying registry.

Administrator response
Resubmit at a later time.

HPDAZ0313E

The registry reported the password has been recently used and can not be reused. (0x33840139)

Explanation
The underlying registry reported that it will not allow changes to the passwod until a preset amount of time has passed since the last change. This is not due to any Security Verify Access policy, rather the policy of the underlying registry.

Administrator response
Create a new password not previously used and resubmit.

HPDAZ0314E

The registry reported an unexpected password policy error *%s*. (0x3384013a)

Explanation
The underlying registry reported a password policy error that was not expected, and as a security precaution the account will be considered locked.

Administrator response
Contact the underlying registry administrator to help determine why.

HPDAZ0315E

Unable to communicate to the registry server. (0x3384013b)

Explanation
The API failed to connect to the LDAP registry server. Additional information may be available in the attached Naming Exception.

Administrator response
Ensure the registry server is operating and a clear communications path exists to it.

HPDAZ0316E

The entry already exists in the registry. (0x3384013c)

Explanation
An attempt to create a new entry in the LDAP registry failed because the entry already exists.

Administrator response
Choose a new DN and retry the operation.

HPDAZ0317E

The registry is too busy and has rejected the operation. (0x3384013d)

Explanation
The LDAP registry server reported that it was too busy to process the request.

Administrator response
Retry when the registry is less busy.

HPDAZ0318E

The operation took longer than the registry time limit and was aborted. (0x3384013e)

Explanation
The LDAP registry server aborted the operation as it was taking too long to process.

Administrator response
Retry with a simpler operation, increase the registry time limit, improve the registry performance, or if the registry is under heavy load, wait for a better time.

HPDAZ0319E

The operation failed due to insufficient access rights. (0x3384013f)

Explanation
Access Controls set in the LDAP registry server do not permit this APIs account to invoke the operation.

Administrator response
Contact the LDAP registry administrator to gain the necessary access rights.

HPDAZ0320E

The Distinguished Name provided has incorrect syntax. (0x33840140)

Explanation
An invalidly formated DN was provided.

Administrator response
Correct the DN provided to adhear to the rules for LDAP DN string representation.

HPDAZ0321E

The Distinguished Name does not map to an existing entry in the registry. (0x33840141)

Explanation
The object was not found in the registry.

Administrator response
Ensure the DN provided is correct.

HPDAZ0322E

An attribute with the given value does not exist for the entry. (0x33840142)

Explanation
The object does not contain the attribute with the specified value so the operation failed.

Administrator response
Ensure the attribute name and value is correct for the operation.

HPDAZ0323E

The operation violates the schema rules for the registry. (0x33840143)

Explanation
The operation requested would violate the schema rules of the registry.

Administrator response
Do not attempt to violate schema rules.

HPDAZ0324E

The attribute type specified is not valid. (0x33840144)

Explanation
The attribute type specified is not valid. This should not occur during normal operation.

Administrator response
Reconsider how this API is being used.

HPDAZ0325E

Partial results were returned due to a referral not being followed. (0x33840145)

Explanation
This error results from LDAP referrals not being followed. If they were followed all the results could be obtained.

Administrator response
This should not occur, as the API is configured to follow referrals.

HPDAZ0326E

The request to the registry included an extension that is not supported by the registry. (0x33840146)

Explanation
The request to the registry included an extension that is not supported by the registry.

Administrator response
Examine the configuration of the registry to ensure the required extension is enabled.

HPDAZ0327E

The value specified for the attribute violates the attributes schema definition. (0x33840147)

Explanation
The value specified for the attribute would violate the attributes schema definition.

Administrator response
Ensure the attribute value and name are correct.

HPDAZ0328E

The non-leaf entry can not be deleted. (0x33840148)

Explanation
Other entries in the registry have been created below this one and the registry will not permit its removal while the other entries exist.

Administrator response
If the entry was specified correctly, remove the entries under it so it becomes a leaf entry and can be removed.

HPDAZ0329E

The credentials provided can not be authenticated by the registry. (0x33840149)

Explanation
The DN provided does not match any existing user in the registry or the password provided is not correct for the user.

Administrator response
Provide correct credentials and retry.

HPDAZ0330E

An attribute type or attribute value specified already exists in the entry. (0x3384014a)

Explanation
An attribute type or attribute value specified already exists in the entry.

Administrator response
Ensure the correct attribute and value was provided.

HPDAZ0331E

An unexpected error was reported by the registry. (0x3384014b)

Explanation
An unexpected error was reported by the registry.

Administrator response
Ensure the registry and this API are configured correctly, and that the registry is an offically supported one.

HPDAZ0332E

Unable to read in the configuration URL: *%s*. (0x3384014c)

Explanation
Opening and reading in the contents of the configuration properties file failed.

Administrator response
Ensure the configuration file specified is correct.

HPDAZ0333E

Unable to determine the registry server type. Error message *%s*. (0x3384014d)

Explanation
The API will attempt to determine the type of LDAP registry it is configured to use. This operation will test some of the essential basic configuration options are correct when the registry instance is provisioned.

Administrator response
Examine the error message take corrective action, and retry.

HPDAZ0334E

Many instances of the registry API are open. The maximum is *%s*. (0x3384014e)

Explanation
There is a maximum number of registry instances that can be instanciated at the same time and this limit has been reached.

Administrator response
Reduce the number of simultaneously open registry instances.

HPDAZ0335E

The cryptographic algorithm *%s* need for SSL to the registry is not available. (0x3384014f)

Explanation
To ensure the SSL certificate recieved from the LDAP server is trusted this algorithm is used and must be available.

Administrator response
Ensure the correct com.ibm.crypto.provider.IBMJCE is in the Java class path.

HPDAZ0336E

The configured trust key store, *%s* does not exist. This is needed for SSL to the registry. (0x33840150)

Explanation
If the trust key store is configured, it must exists.

Administrator response
Ensure trust key store is configured correctly and exists.

HPDAZ0337E

The configured trust key store, *%s* of type *%s* from provider *%s* can not be loaded. This is needed for SSL to the registry. (0x33840151)

Explanation
The configured trust key store cannot be loaded.

Administrator response
Ensure trust key store is configured correctly, exists and if of the correct type.

HPDAZ0338E

The configured trust key store, *%s* cannot be initialized by the trust store factory. This is needed for SSL to the registry. (0x33840152)

Explanation
The configured trust key store could not be initilized by the trust store factory.

Administrator response
Ensure trust key store is configured correctly, and has the correct type.

HPDAZ0339E

Unexpected error using the configured trust key store, *%s*. This is needed for SSL to the registry. (0x33840153)

Explanation
Unexpected error using the configured trust key store.

Administrator response
Ensure trust key store is configured correctly, is of the correct type.

HPDAZ0340E

Unexpected error setting up SSL to the registry. (0x33840154)

Explanation
Unexpected error setting up SSL to the registry.

Administrator response

HPDAZ0341E

The registry returned a generic error that indicates the registries password policy was violated. (0x33840155)

Explanation
An attribute value exception, which is not valid, can be returned by various LDAP registries if the password supplied does not conform to the LDAP registries password policy. This is not caused by Security Verify Access password policy.

Administrator response
Ensure the password complies to the underlying LDAP registries password policy.

HPDAZ0342E

No avaliable method for verifying the password is available. (0x33840156)

Explanation
Two methods of verifying the password are used by the API. Either by binding to the LDAP server using the credentials, or by using the LDAP to directly compare the password to the password attribute of the account. Neither of these two methods are available, possibly due to a combination of the limitations of the LDAP server and the ldap.auth-using-compare setting.

Administrator response
Ensure the ldap.auth-using-compare configuration setting is appropriate.

HPDAZ0343E

The registry reported an error to indicate the account is locked. (0x33840157)

Explanation
The underlying registry reported the account is locked. This is not due to any Security Verify Access policy, rather the policy of the underlying registry.

Administrator response
Contact the underlying registry administrator for a solution.

HPDAZ0344E

The password is not correct. (0x33840158)

Explanation
The password does not match the password of the account.

Administrator response
Retry with the correct password

HPDAZ0345E

The entity is not a Security Verify Access entity, so the attribute, *%s*, is not appropriate. (0x33840159)

Explanation
The attribute being modified is only applicable to Security Verify Access entities, and the entity in this operation is not one.

Administrator response
Ensure the attribute is appropriate for the entity being modified.

HPDAZ0346E

The operation is not valid for attribute, *%s*. (0x3384015a)

Explanation
The operation is not valid for attribute.

Administrator response
Ensure the attribute name is correct.

HPDAZ0347E

GSO enabled user accounts can not be deleted. (0x3384015b)

Explanation
The API does not support deleting user accounts that are GSO enabled.

Administrator response
Remove GSO enablement from the user account before deleting.

HPDAZ0348W

The registry reported the password will expire soon. (0x3384015c)

Explanation
The underlying registry reported the password will expire soon. This is not due to any Security Verify Access policy, rather the policy of the underlying registry.

Administrator response
This condition can be ignored, and might be cleared by updating the password.

HPDAZ0349E

The suffix *%s* configured to be ignored cannot be parsed. (0x3384015d)

Explanation
The suffix string provided is not a correctly formatted DN.

Administrator response
Ensure the suffix syntax is correct.

HPDAZ0350E

The suffix *%s* used internally cannot be parsed. (0x3384015e)

Explanation
The suffix string set internally in the program cannot be parsed by the Java API, which is unexpected.

Administrator response
Internal error, check for updates to this program.

HPDAZ0351W

Authentication failed. The account is not activated. (0x3384015f)

Explanation
The LDAP registry failed the authentication and reported that the account is not activated.

Administrator response
Contact the administrator for the LDAP registry to activate the account.

HPDAZ0352E

An LDAP operations error occurred. (0x33840160)

Explanation
An unexpected error was returned from the LDAP server while attempting the operation. This error can be returned from a search of the suffix: cn=schema.

Administrator response
Make sure that special LDAP suffixes are excluded from searches.

HPDAZ0353E

Unable to setup Audit logger for file pattern *%s* (0x33840161)

Explanation
An error occurred when setting up the Audit Java Logger to output to the specified file.

Administrator response
Ensure the file pattern provided is valid, and that the operating system user running this application has permission to update these audit files. Also examine the cause exception for additional details.

HPDAZ0354E

Failed to convert attribute/value information into PDAdmin PDAttrs in preparation for authorization checks. (0x33840162)

Explanation
An error occurred when creating PDAdmin attribute class instances.

Administrator response
This error is not expected. Examine the cause exception for possible solution.

HPDAZ0355E

Failed to get obtain PDAdmin credentials for user *%s*. (0x33840163)

Explanation
An error occurred when determining the credentials for the user that is to be used in authorization decisions when using the administration methods.

Administrator response
Ensure the administrator user name is valid. Ensure that the Authorization Server is running. Examine the cause exception for addition information.

HPDAZ0356E

Unable to generate PDPermission objects. (0x33840164)

Explanation
An error occurred when creating PDPermission objects used for authorizing administration methods.

Administrator response
Examine the cause exception for addition information.

HPDAZ0357E

Unable to determine if the user is permitted access. (0x33840165)

Explanation
An error occurred when checking if the user has permission to invoke the administration method.

Administrator response
Ensure the Authorization Server is running. Examine the cause exception for addition information.

HPDAZ0358E

The user '*%s*' is not authorized for '*%s*' action on '*%s*'. (0x33840166)

Explanation
The administration user is not permitted access to the method.

Administrator response
Use a different user, or update the ACL on the object to permit the action.

HPDAZ0359E

Domain '*%s*' is not valid, only domain '*%s*' can be used. (0x33840167)

Explanation
The permitted domains is restricted when running the application as it is configured.

Administrator response
Use the correct domain. Note that when authorization is enabled, the only domain permitted is the one configured for the PDAdmin API.

HPDAZ0360E

The user '*%s*' is not permitted to invoke this operation on their own account. (0x33840168)

Explanation
Some operations are not permitted when a user is manipulating their own account.

Administrator response
Use a different user to invoke this operation.

HPDAZ0361E

Unable to create a PDAdmin PDAuthorizationContext for authorization evaluation. (0x33840169)

Explanation
This API attempted to create a PDAdmin PDAuthorizationContext, required when authorization is enabled.

Administrator response
Ensure the configuration is correct. Examine the cause exception for additional details.

HPDAZ0362E

Attribute '*%s*' can only have one value, *%s* values were provided. (0x3384016a)

Explanation
An update was attempted on an attribute which would result in more than one value for the attribute when the attribute only allows one value.

Administrator response
Retry the operation with just one value.

HPDAZ0363E

Attribute '*%s*' must be of String type. (0x3384016b)

Explanation
The attribute only accepts String type values.

Administrator response
Retry the operation with a String value, not a byte[] value.

HPDAZ0364E

The value '*%s*' is not valid for attribute '*%s*'. (0x3384016c)

Explanation
The attribute only accepts String type values.

Administrator response
Retry the operation with a String value, not a byte[] value.

HPDAZ0365E

The condensed resource credential value '*%s*' can not be parsed. (0x3384016d)

Explanation
The value provided was likely not produced from the API and is not formatted correctly.

Administrator response
Correct the value and retry the operation.

HPDAZ0366E

%s resource credential values are required, *%s* was provided. (0x3384016e)

Explanation
A resource credential is made of of four values: the resoure name, type, user and password.

Administrator response
Provide the correct number of values and retry the operation.

HPDAZ0368E

The configured key store, *%s*, does not exist. This key store is required for mutual SSL authentication to the user registry. (0x33840170)

Explanation
If the key store is configured, it must exist.

Administrator response
Ensure the key store is configured correctly and exists.

HPDAZ0369E

The configured key store *%s*, of type *%s*, from the provider *%s* cannot be loaded. This key store is required for mutual SSL authentication to the user registry. (0x33840171)

Explanation
The configured key store cannot be loaded.

Administrator response
Ensure key store is configured correctly, exists and is of the correct type.

HPDAZ0370E

An unexpected error occurred while using the configured key store: *%s*. This key store is required for mutual SSL authentication to the user registry. (0x33840172)

Explanation
An unexpected error occurred while using the configured key store.

Administrator response
Ensure that the key store is configured correctly and is of the correct type.

HPDAZ0400E

Invalid argument: Null PDConfig. (0x30659190)

Explanation
A nonnull PDConfig object is required to construct an AuthNCertCmd.

Administrator response
Ensure that the config argument is nonnull.

HPDAZ0401E

Invalid argument: Null accountName or passphrase or domainName. (0x30659191)

Explanation
A nonnull input is required to construct an AuthNPasswordCmd.

Administrator response
Ensure that the accountName, passphrase and domainName arguments are nonnull.

HPDAZ0402E

Invalid argument: Some nonnull input needs to be provided. (0x30659192)

Explanation
Nonnull input is required to construct an AuthSignCertificateCmd.

Administrator response
Ensure that some input is nonnull.

HPDAZ0403E

Transmission error: Parameters could not be encoded. (0x30659193)

Explanation
I/O error occurred even before the request could be transmitted.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAZ0404E

Invalid argument: Null accountname or passphrase. (0x30659194)

Explanation
Nonnull input is required to construct a ProxyAuthenticateCmd.

Administrator response
Ensure that the input is nonnull.

HPDAZ0405E

Invalid argument: Null userName. (0x30659195)

Explanation
A userName is required to construct a ProxyGetCredsCmd.

Administrator response
Ensure that the userName argument contains meaningful input.

HPDAZ0500E

Configuration error: This application server's account is marked invalid. (0x306591f4)

Explanation
The Security Verify Access server indicates that this server's account is invalid.

Administrator response
Ensure that the correct config file is being used. If it is, ensure that this application server's account has not been marked invalid.

HPDAZ0501E

Configuration error: This application server's account is unknown. (0x306591f5)

Explanation
The Security Verify Access server indicates that this server's account is unknown.

Administrator response
Ensure that the correct config file is being used. If it is, ensure that this application server's account exists. If it does not, re-run SvrSslCfg.

HPDAZ0502E

Transmission error: No response from server at *%s*, port *%d*. (0x306591f6)

Explanation
The Security Verify Access server did not respond to this request.

Administrator response
Ensure that the correct config file is being used, and that the desired server is operational. If all was correct, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAZ0503E

Transmission error: Could not connect to the server, and no alternative servers are configured. (0x306591f7)

Explanation
No communication is possible to this Security Verify Access server.

Administrator response
Ensure that the correct config file is being used, and that the desired server is operational. If all was correct, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAZ0504E

Failover error: cannot contact a configured server. (0x306591f8)

Explanation
No communication could be made to any of the configured servers.

Administrator response
Ensure that network connectivity exists between the client and server machines and verify that the server process is running on the configured port.

HPDAZ0512E

The Security Verify Access custom registry adapter for WebSphere Virtual member manager (VMM) cannot update group membership for group [*%s*] . Security Verify Access does not support nested groups. (0x38638200)

Explanation
The Security Verify Access does not support nested groups; therefore, the Security Verify Access custom registry adapter for WebSphere Virtual member manager does not allow nested group membership update.

Administrator response
Remove the group membership update for nested group.

HPDAZ0513W

Server *%s* has recovered. (0x33840201)

Explanation
An LDAP server that previously failed has been detected as funtioning again. It will be added back into the pool of available servers.

Administrator response
No action required.

HPDAZ0514W

The LDAP server is an IBM Tivoli Directory Server and is running in configuration only mode. Security Verify Access will not be able to operate normally with the LDAP server in this mode. (0x33840202)

Explanation
The LDAP server is an IBM Tivoli Directory Server and the server is currently running in configuration only mode. In this mode, most normal LDAP operations (such as update) cannot be performed. Since many LDAP operations which Security Verify Access performs are not possible, Security Verify Access will not be able to operate normally until the LDAP server is configured properly and restarted in normal mode.

Administrator response
View the IBM Tivoli Directory Server error logs and correct any identified errors which prevent the LDAP server from starting in normal mode. See the IBM Tivoli Directory Server documentation for the location of the error log and information for configuring the server properly. Once the conditions have been corrected, restart the LDAP server in normal mode and restart Security Verify Access.

HPDAZ0600E

Invalid argument: Null URL on constructor. (0x30659258)

Explanation
An internal error occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDAZ0601E

Invalid argument: Could not convert port number to an integer. (0x30659259)

Explanation
The supplied value was not a valid integer.

Administrator response
Supply a valid integer value for the server port number.

HPDAZ0602E

Corrupted file: Insufficient information to contact a Policy Server. (0x3065925a)

Explanation
The configuration file did not correctly specify a Policy Server servername and port.

Administrator response
Re-run SvrSslCfg to generate a valid configuration file.

HPDAZ0603E

Corrupted file: Insufficient information to contact an Authorization Server. (0x3065925b)

Explanation
The configuration file did not correctly specify a Authorization Server servername and port.

Administrator response
Re-run SvrSslCfg to generate a valid configuration file.

HPDAZ0604E

Invalid argument: Duplicate server specified. (0x3065925c)

Explanation
When trying to add a server to the configuration file, it was discoverd that the server was already in the list of servers. Retry without the duplicate entry.

Administrator response
Only supply a server once.

HPDAZ0605E

Corrupted configuration: Cannot use keystore. (0x3065925d)

Explanation
The keystore file supposed to be used in client-server SSL communication could not be opened with the derived password, or the certificate does not have the correct alias, or the encrypted password has been tampered with.

Administrator response
Re-run SvrSslCfg.

HPDAZ0768E

Value '*%s*' is not valid for option '*%s*'. It must be one of 'true' or 'false' (0x33840300)

Explanation
The option can only be set to either 'true' or 'false'. Neither of these values were provided.

Administrator response
Retry the command providing a correct value for the option.

HPDAZ0769E

Invalid value '*%s*' for option '*%s*'. It must be an integer in the range *%s* to *%s* (0x33840301)

Explanation
The option value must be an integer in the range noted in the error text.

Administrator response
Retry the command providing a correct value for the option.

HPDAZ0770E

Invalid value '*%s*' for option '*%s*'. The value must be a non-empty list of values separated by '*%s*' characters. (0x33840302)

Explanation
The option value must be a non-empty list of values separated by the separator characted noted in the error text.

Administrator response
Retry the command providing a correct value for the option.

HPDAZ0771E

The password for '*%s*' can not be zero characters in length. (0x33840303)

Explanation
Password must be at least one character in length.

Administrator response
Retry the command providing a correct value for the option.

HPDAZ0772E

At least one LDAP server must be specified for option '*%s*'. (0x33840304)

Explanation
The option requires at least one LDAP server to be specified.

Administrator response
Retry the command providing a correct value for the option.

HPDAZ0773E

Option '*%s*' has an LDAP server entry '*%s*' which is not valid. It must be of the form 'host:port:type:rank' (0x33840305)

Explanation
The command was not able to find four values separated by ':' characters for the LDAP server entry.

Administrator response
Retry the command providing a correct value for the option.

HPDAZ0774E

Option '*%s*' has entry '*%s*' with a port value '*%s*' that is not valid. It must be an integer in the range 1 to 65535. (0x33840306)

Explanation
The value for the LDAP server port in either not in the range 1 to 65535, or is not an integer.

Administrator response
Retry the command providing a correct value for the option.

HPDAZ0775E

Option '*%s*' has entry '*%s*' with a server type '*%s*' that is not valid. Use one of 'readwrite' or 'readonly' (0x33840307)

Explanation
The server type can only be one of 'readwrite' or 'readonly'.

Administrator response
Retry the command providing a correct value for the option.

HPDAZ0776E

Option '*%s*' has entry '*%s*' with a server rank '*%s*' that is not valid. The rank must be an integer in the range 1 to 10. (0x33840308)

Explanation
The value for rank is in either not in the range 1 to 10, or is not an integer.

Administrator response
Retry the command providing a correct value for the option.

HPDAZ0777E

For option '*%s*' the '*%s*' must be a valid file that exists. (0x33840309)

Explanation
The file must exist and be accessable to the user running this command.

Administrator response
Retry the command providing a correct value for the option.

HPDAZ0779E

The configuration properties file '*%s*' already exists. (0x3384030b)

Explanation
The create command will not overwrite existing files.

Administrator response
Retry the command providing the name of a file that does not exist.

HPDAZ0780E

An unknown configuration property name '*%s*' was provided. Use one of: *%s*. (0x3384030c)

Explanation
An unknown configuration property name was given.

Administrator response
Retry the command providing one of the valid property names.

HPDAZ0781E

The option '*%s*' is required and can not be removed. (0x3384030d)

Explanation
The property can not be removed as it must be present in the configuration properties file.

Administrator response
Do not attempt to remove the option from the configuration properties file.

HPDAZ0782E

Unable to create the configuration property file '*%s*', error '*%s*'. (0x3384030e)

Explanation
The configuration properties file can not be created (either for the first time, or due to an update). If this is an update, the original configuration propertes file is renamed with the extention .bkp, and a new file is written in it's place. If the write fails, the original file is restored.

Administrator response
Ensure there is sufficent disk space. Ensure file system permissions permit the create.

HPDAZ0783E

Unable to write to configuration properties file '*%s*', error '*%s*'. (0x3384030f)

Explanation
The program is unable to write the properties to the configuration properties file.

Administrator response
Ensure there is sufficent disk space and retry.

HPDAZ0784E

Unable to open configuration properties file '*%s*' for reading. Error '*%s*'. (0x33840310)

Explanation
The program is unable to open the the configuration properties file to read the properties.

Administrator response
Ensure permissions on the file allow the action.

HPDAZ0785E

Unable to read propertes from configuration properties file '*%s*'. Error '*%s*' (0x33840311)

Explanation
The program is unable to read the properties from the configuration properties file.

Administrator response
Ensure file is a correctly formated properties file.

HPDAZ0786E

The input properties file is missing the required 'ldap.ssl-truststore' property. (0x33840312)

Explanation
'ldap.ssl-enable' property was set to 'true' which requires 'ldap.ssl-truststore' property.

Administrator response
Either set ldap.ssl-enable to 'false' or add the propery 'ldap.ssl-truststore' in the input properties file.

HPDAZ0787E

The input properties file is missing the required 'ldap.ssl-truststore-pwd' property. (0x33840313)

Explanation
'ldap.ssl-enable' property was set to 'true' which requires 'ldap.ssl-truststore-pwd' property.

Administrator response
Either set ldap.ssl-enable to 'false' or add the propery 'ldap.ssl-truststore-pwd' in the input properties file.

HPDAZ0788E

The input properties file is missing the required '*%s*' property. (0x33840314)

Explanation
The property is required and must be supplied in the input properties file.

Administrator response
Add the missing propery to the input properties file.

HPDAZ0789E

The configured suffix is not of the correct format '*%s*'. (0x33840315)

Explanation
The suffix configured can not be parsed as a valid LDAP Distinguished Name.

Administrator response
Fix the format of the configured Federation suffix.

HPDAZ0790E

The configured suffix '*%s*' has been configured more than once. (0x33840316)

Explanation
The suffix configured has been configured more than once.

Administrator response
Remove the duplicate suffix from the configured Federation servers.

HPDAZ0791E

The configured basic user search suffix *%s* cannot be parsed. (0x33840317)

Explanation
The suffix string provided is not a correctly formatted DN.

Administrator response
Ensure the suffix syntax is correct.

HPDAZ0792E

The configuration properties *%s* and *%s* can not both be set to true. (0x33840318)

Explanation
It is not valid to have both options enabled, only one or none of them can be enabled.

Administrator response
Make one or both options false and retry.

HPDBA0100E

No data accompanied the server response to the request. (0x10652064)

Explanation
See message.

Administrator response
Verify the status of the server.

HPDBA0101E

Memory allocate request failed. (0x10652065)

Explanation
A request to allocate memory failed.

Administrator response
Check the amount of system paging and swap space available as well as the amount of available memory. You might also consider rebooting the system. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0107E

Unable to map file *%s*, error (rc=*%d*). (0x1065206b)

Explanation
An internal error has occurred.

Administrator response
Retry the command. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0108E

Unable to unmap file *%s*, error (rc=*%d*). (0x1065206c)

Explanation
An internal error has occurred.

Administrator response
Retry the command. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0111E

The Tivoli Common Directory configuration file cannot be read. (0x1065206f)

Explanation
Security Verify Access was configured to use the Tivoli Common Directory serviceability scheme; but the Tivoli Common Directory configuration file cannot be read.

Administrator response
Verify that the Tivoli Common Directory configuration file is located in the correct directory and that its has proper file access permissions.

HPDBA0112W

Serviceability messages will not be recorded in the Tivoli Common Directory. (0x10652070)

Explanation
Security Verify Access was configured to use the Tivoli Common Directory serviceability scheme; but the Tivoli Common Directory has been relocated since the configuration was performed.

Administrator response
The location of the Tivoli Common Directory has been relocated since Security Verify Access was configured. Move the Security Verify Access serviceability files into the new location and update the Security Verify Access configuration to use the correct directory.

HPDBA0200E

The server Distinguished Name (DN) specified in the configuration file does not match the DN in the certificate received from the server. (0x106520c8)

Explanation
The DN specified in the "master-dn" attribute of the "manager" stanza of the configuration file does not match the DN in the certificate received from the server.

Administrator response
Verify that the server's hostname, port number, and Distinguished Name are correct and that the correct server certificate is being used.

HPDBA0202E

The keyfile is not configured or it could not be opened or accessed. (0x106520ca)

Explanation
The keyfile does not exist or permissions prevent the application from reading the keyfile.

Administrator response
Ensure that the keyfile specified by the "ssl-keyfile" attribute in the "ssl" stanza of the configuration file exists and that the permissions permit reading. Verify that it can be viewed using a keyfile management program.

HPDBA0203E

The keyfile password is incorrect. (0x106520cb)

Explanation
The password stash file does not exist or its permissions prevent the application from reading it.

Administrator response
Ensure that the file specified by the "ssl-keyfile-stash" attribute in the "ssl" stanza of the configuration file exists and is readable.

HPDBA0204E

The specified certificate could not be used because it does not exist or is otherwise invalid. (0x106520cc)

Explanation
The certificate in the keyfile has expired or the keyfile is invalid.

Administrator response
Ensure that the correct certificate is specified and that it has not expired.

HPDBA0205E

The certificate presented by the SSL partner could not be successfully validated. (0x106520cd)

Explanation
The certificate presented by the application is invalid.

Administrator response
Ensure that the correct configuration file is being used by the application.

HPDBA0206E

The specified SSL V3 session time-out value is invalid. (0x106520ce)

Explanation
The configuration file contains an invalid value.

Administrator response
Specify a valid value (an integer in the range: 10-86400) in the appropriate configuration file for the attribute (ssl-v3-timeout) or initialization parameter (azn_init_ssl_timeout). Security Verify Access components do not operate correctly with small time-out values in some network environments.

HPDBA0207E

A communication error occurred while initializing the SSL connection. (0x106520cf)

Explanation
An internal error has occurred. It might be caused by a TCP/IP connection problem.

Administrator response
Retry the command. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0208E

The requested action cannot be performed because the SSL environment is not initialized. (0x106520d0)

Explanation
An internal error has occurred.

Administrator response
Retry the command. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0209E

The requested action cannot be performed because the SSL environment is already initialized. (0x106520d1)

Explanation
An internal error has occurred.

Administrator response
Retry the command. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0210E

The SSL environment could not be closed. (0x106520d2)

Explanation
An internal error has occurred.

Administrator response
Retry the command. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0211E

The SSL attribute could not be set because the value is invalid. (0x106520d3)

Explanation
An internal error has occurred.

Administrator response
Retry the command. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0212E

The SSL environment could not be initialized. Ensure all required SSL configuration parameters are correct. (0x106520d4)

Explanation
The configuration might be corrupted.

Administrator response
Retry the command. If the problem persists, unconfigure and reconfigure the application.

HPDBA0213E

The WinSock library could not be loaded. (0x106520d5)

Explanation
An internal error has occurred.

Administrator response
Ensure that WinSock support is installed and the library directory is in the PATH then retry the command. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0214E

The SSL socket could not be initialized. Ensure all required SSL configuration parameters are correct. (0x106520d6)

Explanation
The configuration might be corrupted.

Administrator response
Retry the command. If the problem persists, unconfigure and reconfigure the application.

HPDBA0215E

Information about the SSL session could not be determined. (0x106520d7)

Explanation
An internal error has occurred.

Administrator response
Retry the command. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0216E

The SSL session could not be reset. (0x106520d8)

Explanation
An internal error has occurred.

Administrator response
Retry the command. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0217E

The SSL session type cannot be set to client on a server. (0x106520d9)

Explanation
An internal error has occurred.

Administrator response
Retry the command. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0218E

An error occurred writing data to an SSL connection. (0x106520da)

Explanation
An internal error has occurred.

Administrator response
Retry the command. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0219E

An error occurred reading data from an SSL connection. (0x106520db)

Explanation
An internal error has occurred.

Administrator response
Retry the command. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0220E

The partner's SSL certificate information could not be determined. (0x106520dc)

Explanation
An internal error has occurred.

Administrator response
Retry the command. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0221E

The requested action could not be performed because the SSL client is already bound to the server. (0x106520dd)

Explanation
An internal error has occurred.

Administrator response
Retry the command. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0222E

The TCP/IP host information could not be determined from the server hostname. Ensure that the server hostname is correct. (0x106520de)

Explanation
An internal error has occurred.

Administrator response
Retry the command. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0223E

The SSL communication cannot be performed because the socket is invalid. (0x106520df)

Explanation
An internal error has occurred.

Administrator response
Retry the command. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0224E

The specified authentication method is invalid. Ensure that the specified authentication method is a supported value. (0x106520e0)

Explanation
The configuration file contains an invalid value.

Administrator response
Correct the authentication method specified in the configuration file, or unconfigure and reconfigure the application.

HPDBA0225E

A configuration action could not be performed because the SSL server is already initialized and running. (0x106520e1)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0228E

The data could not be sent over SSL because the buffer size was insufficient. (0x106520e4)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0229E

The certificate or keyfile password is expired. (0x106520e5)

Explanation
The certificate or the keyfile password is expired and auto-refresh is not enabled.

Administrator response
Refresh the password or enable auto-refresh in the configuration file.

HPDBA0230E

The certificate label or DN is invalid. (0x106520e6)

Explanation
An internal error has occurred.

Administrator response
Reconfigure the application. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0231E

The date for the partner certificate is invalid. (0x106520e7)

Explanation
An internal error has occurred.

Administrator response
Reconfigure the application. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0232E

The type of the partner certificate is unsupported. (0x106520e8)

Explanation
An internal error has occurred.

Administrator response
Reconfigure the application. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0233E

No certificate was presented by the SSL partner. (0x106520e9)

Explanation
An internal error has occurred.

Administrator response
Reconfigure the application. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0234E

The SSL communications could not be completed. The socket was closed. (0x106520ea)

Explanation
An internal error has occurred.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0236W

The server could not locate the session for the client. (0x106520ec)

Explanation
The client disconnected before the operation completed.

Administrator response
No action is required.

HPDBA0237E

The client is not bound. The client must be bound to perform this operation. (0x106520ed)

Explanation
An internal error has occurred.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0242W

The server could not find a handler for the command: (0x*%x*). (0x106520f2)

Explanation
This might indicate that the client or server should be upgraded.

Administrator response
Ensure that the client and server software are at a compatible level. Update the client or server software if necessary.

HPDBA0245E

GSKKM API failed. *%s* return (*%d*). (0x106520f5)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0263E

Accept failed, errno: (0x%*x*). (0x10652107)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0269E

The session performing the operation lost its credentials. (0x1065210d)

Explanation
This is an internal error.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0272E

The SSL keyfile name is invalid. (0x10652110)

Explanation
The configuration file is corrupted or contains invalid data.

Administrator response
Unconfigure and reconfigure the application.

HPDBA0273E

The SSL version is invalid. The specified version is incorrect or unsupported. (0x10652111)

Explanation
The configuration file is corrupted or contains invalid data.

Administrator response
Unconfigure and reconfigure the application.

HPDBA0274E

The SSL keyfile stash file name are invalid. (0x10652112)

Explanation
The configuration file is corrupted or contains invalid data.

Administrator response
Unconfigure and reconfigure the application.

HPDBA0275E

The client is not configured properly for this call. No replicas have been specified. (0x10652113)

Explanation
The configuration is incomplete.

Administrator response
Use the svrsslcfg -add_replica command to add appropriate replica authorization servers.

HPDBA0276E

The server name is invalid. (0x10652114)

Explanation
The configuration file is corrupted or contains invalid data.

Administrator response
Unconfigure and reconfigure the application.

HPDBA0277E

The server port is invalid. (0x10652115)

Explanation
The configuration file is corrupted or contains invalid data.

Administrator response
Unconfigure and reconfigure the application.

HPDBA0279E

A domain must be specified for authentication. (0x10652117)

Explanation
A domain has not been specified before contacting the server.

Administrator response
Ensure a domain is specified in the configuration file.

HPDBA0280E

An invalid Privilege Attribute Certificate (PAC) was specified. (0x10652118)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0281E

An unexpected exception was caught. (0x10652119)

Explanation
See message.

Administrator response
See the error log for more information. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0282E

An unknown exception was caught. No exception information is available. (0x1065211a)

Explanation
See message.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0285E

Automatic refresh could not be performed because of a GSKKM API error. (0x1065211d)

Explanation
An internal error has occurred.

Administrator response
Verify that there is enough disk space on the machine. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0286W

An invalid data packet was received and discarded. (0x1065211e)

Explanation
Incoming data is unrecognized.

Administrator response
No action is required.

HPDBA0287E

Automatic refresh could not be performed because the certificate has expired. (0x1065211f)

Explanation
The certificate has expired and must be manually refreshed.

Administrator response
Refresh the certificate in the keyfile. For C applications, use the svrsslcfg command with the -chgcert option to attempt a manual refresh of the certificate. For Java applications, use com.tivoli.pd.jcfg.SvrSslCfg -action replcert.

HPDBA0288W

Automatic refresh of the certificate could not be performed because of error (0x*%8.8x*). (0x10652120)

Explanation
An internal error has occurred.

Administrator response
The operation will be automatically retried. No action is required.

HPDBA0289W

Automatic refresh of the certificate could not be performed because of error (0x*%8.8x*). (0x10652121)

Explanation
An internal error has occurred.

Administrator response
The operation will be automatically retried. No action is required.

HPDBA0292E

The certificate has expired or the date is invalid. (0x10652124)

Explanation
The date in the certificate is not valid.

Administrator response
Renew the certificate. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0293E

ICC API failed. *%s* returns *%d*, *%s* (0x10652125)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0294W

Could not get ICC context. (0x10652126)

Explanation
This is an informational message. An error occurred while attempting to get icc context.

Administrator response
No action is required.

HPDBA0295W

Could not get ICC random number (0x10652127)

Explanation
This is an informational message. An error occurred while attempting to get icc random number.

Administrator response
No action is required.

HPDBA0296E

The SSL communications could not be completed. An incorrectly formatted SSL message was received from the partner. (0x10652128)

Explanation
The FIPS setting might not be the same. All machines in a secure Security Verify Access environment must be configured with the same "ssl-enable-fips" value.

Administrator response
Ensure that the value for the "ssl-enable-fips" entry in the "[ssl]" stanza of pd.conf is the same on both the local machine and the machine where communication is attempted. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0297E

Timeout expired. The timeout period elapsed before obtaining a connection from the client to the server. (0x10652129)

Explanation
See Message.

Administrator response
Increase the value of the 'ssl-client-connection-timeout' entry in the [ssl] stanza of the 'etc/ivmgrd.conf' file in the Security Verify Access install directory. And ensure server is running and listening.

HPDBA0298W

Certified FIPS mode is not available on this platform because the underlying FIPS provider is not currently certified. Security Verify Access will run in non-certified FIPS mode. (0x1065212a)

Explanation
See Message. This is a usually a temporary condition, and should be aleviated on this platform in a subsequent version of GSKit.

Administrator response
When available, upgrade to the FIPS certified version of GSKit for this platform.

HPDBA0300E

Invalid protected object policy name. (0x1065212c)

Explanation
The protected object policy (POP) name that was specified is not valid.

Administrator response
Specify a valid POP name. Valid characters are a-z, A-Z, 0-9, underscore (_), hyphen (-), and backslash (\) or any character from a double-byte character set.

HPDBA0301E

The protected object policy specified was not found. (0x1065212d)

Explanation
See message.

Administrator response
Retry the command with a valid protected object policy name.

HPDBA0302E

Policy is attached to one or more protected objects. A policy cannot be deleted while it is still attached. (0x1065212e)

Explanation
See message.

Administrator response
Detach the policy from all protected objects and retry the command.

HPDBA0303E

A protected object policy with this name already exists. (0x1065212f)

Explanation
An attempt was made to create a new protected object policy. A protected object policy by the same name already exists.

Administrator response
Determine if this conflict needs to be resolved and take action accordingly.

HPDBA0305E

The protected object policy cannot be attached to the specified protected object. The protected object has been marked to not accept the protected object policy. (0x10652131)

Explanation
The creator or administrator of the specified protected object has set the attributes of the protected object such that no policy can be attached.

Administrator response
The administator of the specified protected object must change the attributes of the protected object before a policy can be attached.

HPDBA0306E

The ACL cannot be attached to the specified protected object. The protected object has been marked to not accept the ACL policy. (0x10652132)

Explanation
The creator or administrator of the specified protected object has set the attributes of the protected object such that no policy can be attached.

Administrator response
The administator of the specified protected object must change the attributes of the protected object before a policy can be attached.

HPDBA0308E

Invalid authorization rule name. (0x10652134)

Explanation
The rule name that was specified is not valid.

Administrator response
Specify a valid authorization rule name. Valid characters are a-z, A-Z, 0-9, underscore (_), hyphen (-), and backslash (\) or any character from a double-byte character set.

HPDBA0309E

Invalid authorization rule text string. (0x10652135)

Explanation
The rule text string that was specified is not valid.

Administrator response
Specify a valid authorization rule test string. Valid characters are a-z, A-Z, 0-9, underscore (_), hyphen (-), and backslash (\) or any character from a double-byte character set.

HPDBA0310E

The authorization rule specified was not found. (0x10652136)

Explanation
See message.

Administrator response
Specify the correct rule and retry the command.

HPDBA0311E

An authorization rule with this name already exists. (0x10652137)

Explanation
An attempt was made to create a new authorization rule. An authorization rule by the same name already exists.

Administrator response
Determine if this conflict needs to be resolved and take action accordingly.

HPDBA0312E

The authorization rule cannot be attached to the specified protected object. The protected object has been marked to not accept protected object policies. (0x10652138)

Explanation
The creator or administrator of the specified protected object has set the attributes of the protected object so that no authorization rule can be attached.

Administrator response
The administator of the specified protected object must change the attributes of the protected object such that authorization rule will be accepted.

HPDBA0313E

The authorization rule is attached to one or more protected objects. The authorization rule cannot be deleted while it is still attached (0x10652139)

Explanation
See message.

Administrator response
Use the authzrule find command to get a list of the protected objects that are attached to the rule. Detach all protected objects from the authorization rule then retry the command.

HPDBA0401E

ASN.1 encoding error (0x*%8.8lx*). (0x10652191)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0406E

ASN.1 decoding error. The version of ASN.1 encoded data was unexpected.The most likely cause is that the sender is at different version. (0x10652196)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0407E

ASN.1 general error. Unsupported operation. (0x10652197)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0408E

The ASN.1 data stream ended prematurely. (0x10652198)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0409E

An ASN.1 integer value is too large. (0x10652199)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0410E

ASN.1 data length is invalid. The data buffer is invalid. (0x1065219a)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0411E

ASN.1 data invalid encoding. The data buffer contains unexpected data. (0x1065219b)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0412E

ASN.1 data invalid parameter. (0x1065219c)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0413E

ASN.1 indefinite data type is not allowed. The data buffer contains unexpected data. (0x1065219d)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0414E

The ASN.1 data type must be primitive. The data buffer contains unexpected data. (0x1065219e)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0415E

The ASN.1 type must be constructed. The data buffer contains unexpected data. (0x1065219f)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0416E

An ASN.1 data value is not set. The data buffer contains unexpected data. (0x106521a0)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0417E

The ASN.1 indefinite data type is not supported. The data buffer contains unexpected data. (0x106521a1)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0418E

The unused bitcount is invalid for the ASN.1 bitstream type. The data buffer contains unexpected data. (0x106521a2)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0419E

The segmented bitcount is invalid for the ASN.1 bitstream type. The data buffer contains unexpected data. (0x106521a3)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0420E

An unexpected ASN.1 data type was found. The data buffer contains unexpected data. (0x106521a4)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0421E

The ASN.1 data buffer is too long. The data buffer contains unexpected data. (0x106521a5)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0422E

The ASN.1 data stream is missing members of a sorted set. The data buffer contains unexpected data. (0x106521a6)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0423E

The ASN.1 choice index is out of range. (0x106521a7)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0424E

The ASN.1 choice data type is not initialized. (0x106521a8)

Explanation
An internal error has occurred. An attempt was made to set a value to an unselected choice.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0425E

The ASN.1 asn_any data type has specific syntax. (0x106521a9)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0426E

The ASN.1 utc/gmt time type has an invalid value. (0x106521aa)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0427E

The ASN.1 UTF-8 string could not convert the string to or from the local code page. (0x106521ab)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0428E

The specified codeset is not permitted for this ASN.1 data type. (0x106521ac)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0600E

Keyfile password change failed. File: *%s*. Error: *%d* (0x10652258)

Explanation
An unexpected error occurred while changing the password for the specified key file.

Administrator response
Change the password manually using the -chgpwd option. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBA0601E

Keyfile password change failed because GSKit could not resolve the stash file. File: *%s*. Error: *%d* (0x10652259)

Explanation
An error occurred while changing the password for the specified key file. The key stash file is missing.

Administrator response
The stash file may be missing or corrupted. Attempt to locate the stash file for the specified key file.

HPDBA0602E

Keyfile password change failed because permissions on the file are not correct. File: *%s*. (0x1065225a)

Explanation
An error occurred while changing the password for the specified key file. The file permissions are incorrect, or the owner is incorrect.

Administrator response
Ensure that the owner of the file matches the identity of the application. Ensure that the identity has permission to create and write the file. Then change the password manually using the -chgpwd option.

HPDBA0603E

Keyfile password change failed because GSKit could not change the password. File: *%s*. Error: *%d* (0x1065225b)

Explanation
An unexpected error occurred while changing the password for the specified key file. GSKit change key password returned an error.

Administrator response
The key file or stash file may be corrupted.

HPDBA0604E

Keyfile password change rollback failed. GSKit reports an error. File: *%s*. Error: *%d* (0x1065225c)

Explanation
An error occurred while attempting to restore the password for the specified key file.

Administrator response
The key file or stash file may be missing or corrupted.

HPDBA0605W

Warning mode is enabled for this protected object policy (POP). Complete access to the protected object using this POP is permitted regardless of other restrictions in the POP. (0x1065225d)

Explanation
When the warning mode attribute for the POP is set to yes, any user can perform any action on the object where the POP is attached. Any access to the object is permitted even if the security policy attached to the object is set to deny this access. This message is a precautionary warning to safeguard that this is the desired behavior.

Administrator response
If unrestricted access is desired to the object where the POP is attached, no action is required. To enable restrictions in the POP, modify the POP by setting the value of the warning mode attribute to no.

HPDBA0608E

Unable to map interface name '*%s*' to address. getaddrinfo returned error *%d*: *%s*. (0x10652260)

Explanation
The interface name (IP address) provided was not accepted by the operating system.

Administrator response
Change the name of the interface (IP address) and retry.

HPDBA0609E

Unable to auto refresh keystore *%s*. (0x10652261)

Explanation
When attempting to verify that the keystore could be refreshed, an error occurred.

Administrator response
Make sure that the keystore noted can be refreshed. The file system is not full, ACLs on the keystore or it's directory allow for changes.

HPDBF0020E

The specified JRE (*%s*) version (*%s*) does not meet supported JRE version requirement.Consult the manual for a list of supported JREs. (0x30695014)

Explanation
See message.

Administrator response
Install a supported JRE and retry the command.

HPDBF0021E

This Java Runtime Environment (*%s*) has already been configured. Unconfigure first then retry the command. (0x30695015)

Explanation
The specified JRE is already configured and cannot be configured twice.

Administrator response
Unconfigure JRE if you would like to configure again.

HPDBF0022E

This Java Runtime Environment (*%s*) has already been configured. Unconfigure first or specify a different JRE path then retry the command. (0x30695016)

Explanation
The specified JRE is already configured and cannot be configured twice.

Administrator response
Unconfigure JRE if you would like to configure again or specify a different JRE path.

HPDBF0025E

Unable to create the PD.properties file in the specified JRE.Ensure you have the correct permissions to do so. (0x30695019)

Explanation
Unable to create PD.properties file in PolicyDirector directory of the JRE being configured.

Administrator response
Ensure that the user has the necessary permissions to create the PolicyDirector directory and the PD.properties file in the <JRE_HOME>/PolicyDirector directory.

HPDBF0026W

Unable to rename the PD.properties file. (0x3069501a)

Explanation
See message.

Administrator response
Ensure the permissions on the file allow this process to modify it.

HPDBF0027E

An error occurred while creating PD.properties file. (0x3069501b)

Explanation
Unable to create PD.properties file in PolicyDirector directory of the JRE being configured.

Administrator response
Ensure that the user has the necessary permissions to create the PolicyDirector directory and the PD.properties file in the <JRE_HOME>/PolicyDirector directory.

HPDBF0029E

No JRE has been configured. Unable to unconfigure *%s*. (0x3069501d)

Explanation
pdjrte_paths file does not exist. As such, no JREs have been configured already.

Administrator response
Configure a JRE. Or, if a JRE is already configured and this message is still displayed, create the <PDHOME>/etc/pdjrte_paths file w/ the JRE path listed.

HPDBF0030W

The JRE (*%s*) is notconfigured for the Security Verify Access Runtime for Java. (0x3069501e)

Explanation
See message.

Administrator response
Configure the JRE for the Security Verify Access Runtime for Java.

HPDBF0031E

This Java Runtime Environment has already been configured. (0x3069501f)

Explanation
The JRE specified is already listed in the pdjrte_paths file.

Administrator response
Unconfigure this JRE before trying to configure.

HPDBF0032E

There was an internal error during initialization. (0x30695020)

Explanation
See message.

Administrator response
Make sure the CLASSPATH is set correctly.

HPDBF0073W

Unable to stop IBM WebSphere Application Server. (0x30695049)

Explanation
The server could not be stopped. Perhaps it was not running.

Administrator response
No action required.

HPDBF0075W

Unable to Regenerate IBM WebSphere Application Server Plugin Configuration. (0x3069504b)

Explanation
The plugin configuration could not be regenerated. Perhaps the server name is not the default server1

Administrator response
From the command line, run the command GenPluginCfg -server.name <servername> where servername is the name of your IBM WebSphere Application Server.

HPDBF0078W

Unable to start IBM WebSphere Application Server. (0x3069504e)

Explanation
The command to start the server failed. Perhaps it is already running.

Administrator response
No action is required.

HPDBF0080E

Unable to deploy Security Verify Access Web Portal Manager. (0x30695050)

Explanation
An error occurred during the installation of the product.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBF0083E

The Security Verify Access runtime must be configured first. (0x30695053)

Explanation
See message.

Administrator response
Configure the Security Verify Access rutime before configuring Web Portal Manager.

HPDBF0084E

Unable to perform SvrSslCfg configuration forSecurity Verify Access Web Portal Manager. (0x30695054)

Explanation
See message.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBF0085E

Unable to find the iscwpm.war directory. Make sure that the WPM application is deployed in the WebSphere systemApps directory. (0x30695055)

Explanation
See message.

Administrator response
See message

HPDBF0086E

The WebSphere server installation full path is not valid.Possible causes are: Make sure you have installed a supported version of WebSphere. Make sure you have configured Security Verify Access Runtime for Java to this WebSphere Java path. (0x30695056)

Explanation
The path specified for WebSphere is not valid.

Administrator response
Install a supported version of WebSphere.

HPDBF0087E

The Security Verify Access Web Portal Manager has already been configured. (0x30695057)

Explanation
See message.

Administrator response
Unconfigure the Security Verify Access Web Portal Manager first, then retry the command.

HPDBF0088E

The Security Verify Access Web Portal Manager has already been unconfigured. (0x30695058)

Explanation
See message.

Administrator response
No action required.

HPDBF0089E

Unable to configure Security Verify Access Runtime for Java into the IBM WebSphere Application Server. (0x30695059)

Explanation
An internal error has occurred.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBF0091E

Security Verify Access Web Portal Manager could not be removedfrom WebSphere. Continuing with the unconfig operation. (0x3069505b)

Explanation
An internal error occurred during the uninstall process.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command. Use the WebSphere Admin Console to remove the Security Verify Access Web Portal Manager.

HPDBF0094E

Unable to unconfigure Security Verify Access Runtime for Javafrom IBM WebSphere Application Server. (0x3069505e)

Explanation
See message.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBF0095E

The SvrSslCfg unconfiguration command cannot be performedfor Security Verify Access Web Portal Manager. (0x3069505f)

Explanation
See message.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBF0097E

IBM WebSphere Application Server plug-in configuration could not be regenerated. (0x30695061)

Explanation
An internal error occurred.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBF0098E

The Windows registry could not be opened. (0x30695062)

Explanation
The API that is used to manipulate the registry failed.

Administrator response
Ensure you are using a supported operating system. Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBF0099E

The registry key value could not be set. (0x30695063)

Explanation
The API that is used to manipulate the registry failed.

Administrator response
Ensure you are using a supported operating system. Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBF0100E

The IBM HTTP server installation path could not be obtained. (0x30695064)

Explanation
See message.

Administrator response
Ensure that IBM HTTP server is properly installed.

HPDBF0101E

The httpd.conf file could not be modified. SSL is not available for connecting toSecurity Verify Access Web Portal Manager. (0x30695065)

Explanation
Unable to access the configuration file for the IBM HTTP server. SSL will not function properly.

Administrator response
Check the file permissions and path. Ensure the file is not locked by another process.

HPDBF0102E

The pdwpm.conf file could not be modified. (0x30695066)

Explanation
Unable to access the configuration file for Security Verify Access Web Portal Manager.

Administrator response
Check the file permissions and path. Ensure the file is not locked by another process.

HPDBF0116E

The port number is not valid. The port must be an integer greater than or equal to zero. (0x30695074)

Explanation
See message.

Administrator response
Retry the command with a valid port number.

HPDBF0119E

The local host name cannot be obtained. Specify the host name using the - policysvr option. (0x30695077)

Explanation
See message.

Administrator response
Specify a value for -policysvr option, and retry the command.

HPDBF0120E

Could not contact the Security Verify Access policy server. Possible causes are:The Policy server is not running.The Policy server host name or port number is incorrect. (0x30695078)

Explanation
See message.

Administrator response
Make sure the policy server is running and specify a correct value for host name and port number, and retry the command.

HPDBF0122E

The value specified for -action option (*%s*) was not valid. The value must be one of the following: config|unconfig|status|name (0x3069507a)

Explanation
See message.

Administrator response
Specify a correct value for the -action option. Retry the command.

HPDBF0153E

An error occurred backing up the data. (0x30695099)

Explanation
See message.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBF0154E

An error occurred restoring the archive. (0x3069509a)

Explanation
An error occurred during the restoration process.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBF0155E

Could not resolve path for Security Verify Access runtime. (0x3069509b)

Explanation
The Security Verify Access runtime path could not be obtained from the registry.

Administrator response
Ensure Security Verify Access runtime is installed on the system.

HPDBF0156E

Could not parse the line: *%s*. (0x3069509c)

Explanation
The line in the backup list is misformed.

Administrator response
Correct the line and retry the command.

HPDBF0157E

Could not backup the registry subkey: *%s*. (0x3069509d)

Explanation
The registry subkey could not be saved.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBF0158E

Could not restore the registry subkey: *%s*. (0x3069509e)

Explanation
The registry subkey could not be restored.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBF0159E

Could not copy *%s* to *%s*. (0x3069509f)

Explanation
An error occurred copying the file.

Administrator response
Check the paths and permissions of the directories.

HPDBF0160E

Could not open file: *%s* (0x306950a0)

Explanation
The specified file could not be opened.

Administrator response
Check the path, name, and permissions of the file and retry the command.

HPDBF0161E

Could not access list: *%s* (0x306950a1)

Explanation
The backup list could not be accessed.

Administrator response
Check the path, name, and permissions of the file and retry the command.

HPDBF0162E

The drive *%s* is not a fixed drive. (0x306950a2)

Explanation
The drive specified must be a fixed drive for the restore to occur.

Administrator response
Specify the correct drive letter and retry the command.

HPDBF0163E

Could not access the path: *%s* (0x306950a3)

Explanation
The path specified does not exist.

Administrator response
Check the path and retry the command.

HPDBF0169E

Could not open file: *%s* (0x306950a9)

Explanation
The specified file could not be opened.

Administrator response
Check the path, name, and permissions of the file and retry the command.

HPDBF0171E

Could not resolve path for Security Verify Access runtime. (0x306950ab)

Explanation
The Security Verify Access runtime path could not be obtained from the registry.

Administrator response
Ensure Security Verify Access runtime is installed on the system.

HPDBF0172E

The file, *%s*, could not be read. (0x306950ac)

Explanation
See message.

Administrator response
Check the file's permissions and path and retry the command.

HPDBF0178E

Error opening or reading the response file *%s*. Ensure the file exists and that it contains the correct stanza name, *%s*. (0x306950b2)

Explanation
The response file could not be accessed or the stanza name is invalid.

Administrator response
Check the path and permissions of the file, make sure it has a valid stanza name, then retry the command.

HPDBF0229E

The configuration action is invalid. Valid actions are 'create' or 'replace'. (0x306950e5)

Explanation
See message.

Administrator response
Retry the command with a valid configuration action.

HPDBF0230E

The port number is invalid. The port must be an integer greater than or equal to zero. (0x306950e6)

Explanation
See message.

Administrator response
Retry the command with a valid port number.

HPDBF0231E

The rank is invalid. The rank must be an integer. (0x306950e7)

Explanation
See message.

Administrator response
Retry the command with a valid rank.

HPDBF0232E

The format of the servers option is host1:port1:rank1,host2:port2:rank2,... (0x306950e8)

Explanation
An invalid servers format was entered.

Administrator response
Rerun the command with a valid servers format.

HPDBF0233E

An invalid server option was entered. The format of the server option is host:port:rank. (0x306950e9)

Explanation
See message.

Administrator response
Rerun the command with a valid server option.

HPDBF0234E

Unable to load pd.properties. (0x306950ea)

Explanation
Not able to load pd.properties files.

Administrator response
Make sure pdjrte is configured.

HPDBF0235E

Invalid key file or configuration file name. (0x306950eb)

Explanation
See message.

Administrator response
Retry the command with valid key file or configuration file name.

HPDBF0236E

The directory does not exist. (0x306950ec)

Explanation
See message.

Administrator response
Ensure the specified directory exist and has appropriate permissions.

HPDBF0237E

The mode value is invalid. The value must be 'remote' or 'local'. (0x306950ed)

Explanation
See message.

Administrator response
Retry the command with valid mode value.

HPDBF0238E

The server option is invalid. Specify one policy server or authorization server parameter. (0x306950ee)

Explanation
See message.

Administrator response
Retry the command with valid server parameter.

HPDBF0239E

The listening option is invalid. The value must be 'true' or 'false'. (0x306950ef)

Explanation
See message.

Administrator response
Retry the command with valid listening value.

HPDBF0240E

The refresh interval is invalid. The value must be an integer greater than or equal to zero. (0x306950f0)

Explanation
See message.

Administrator response
Retry the command with a valid refresh value.

HPDBF0247E

The local host name cannot be obtained. Specify the host name using the -host option. (0x306950f7)

Explanation
See message.

Administrator response
Specify a value for -host option. and retry the command.

HPDBF0248W

The following options are ignored when configuring a remote-mode server: *%s* (0x306950f8)

Explanation
The -dblisten, -dbrefresh and -dbdir options are valid only for local-mode servers. Remote mode was specified.

Administrator response
No action required, but be aware that the values for the listed options are not included in the application server's configuration. If the application server is required to use the options, it must be unconfigured and reconfigured as a local-mode server.

HPDBF0250E

The certificate refresh is invalid. The value must be true or false. (0x306950fa)

Explanation
See message.

Administrator response
Retry the command with a valid appsvr-certrefresh setting.

HPDBF0275E

Invalid LDAP SSL information was entered. (0x30695113)

Explanation
See message.

Administrator response
Provide the correct key file, key label, password and ssl port number, then retry the command.

HPDBF0281E

Incorrect Security Verify Access administrator name or password. (0x30695119)

Explanation
An incorrected administrator name or password was given.

Administrator response
Correct the information and retry the command.

HPDBF0284E

The port number is invalid. The value must be greater than 0.: (0x3069511c)

Explanation
See message.

Administrator response
Enter a port number that is greater than zero.

HPDBF0287E

An error occurred while copying the template file. (0x3069511f)

Explanation
The template file could not be copied.

Administrator response
Make sure the file exists and has permissions appropriate for copying.

HPDBF0290E

Security Verify Access runtime must be configured first. (0x30695122)

Explanation
See message.

Administrator response
Configure Security Verify Access runtime, then retry the command.

HPDBF0291E

Security Verify Access policy server has already been unconfigured. (0x30695123)

Explanation
The policy server is already unconfigured.

Administrator response
This process only works if the policy server is currently configured. Configure the server and retry the command.

HPDBF0292E

The PDMgrProxyd service could not be deleted. (0x30695124)

Explanation
See message.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBF0293E

The PDMgrProxyd service could not be registered. (0x30695125)

Explanation
See message.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBF0294E

An error occurred opening configuration file. (0x30695126)

Explanation
See message.

Administrator response
Check the permissions of the file and make sure it is not in use by another process, then retry the command.

HPDBF0295E

An error occurred while unconfiguring the Security Verify Access proxy server. (0x30695127)

Explanation
See message.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBF0296E

A memory allocation error resulted in the termination of the program. Check the maximum allowable memory and the amount of system paging space as these may both need to be increased. (0x30695128)

Explanation
See message.

Administrator response
Increase the maximum allowable memory and the system paging space or shut down one or more applications.

HPDBF0297E

An error occurred while starting the Security Verify Access policy proxy server. (0x30695129)

Explanation
See message.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBF0340W

An error occurred while checking the properties of the target Java Runtime Environment (*%s*). The JRE might need post-configuration modification. (0x30695154)

Explanation
During Security Verify Access Runtime for Java configuration, the version and vendor of the target JRE are examined. Since the version and vendor could not be determined, the configuration continues as if the JRE needs no modification.

Administrator response
After Security Verify Access Runtime for Java configuration, determine the target Java runtime version and vendor manually. This can be done by executing 'java -version', where the java invoked is in the target runtime. The output should indicate the version and vendor. If the version is JRE 1.4 or later and the vendor is Sun Microsystems, the JRE can then be modified manually: The jsse.jar file present in the JRE's lib directory must be moved to a backup location outside of the lib directory. Note that when the Security Verify Access Runtime for Java is unconfigured for that JRE, the jsse.jar file must be manually restored from its backup location to the lib directory.

HPDBF0341E

The Java Runtime Environment (*%s*) cannot be configured. Configure by using the pdjrtecfg command in non-interactive mode. (0x30695155)

Explanation

During Security Verify Access Runtime for Java configuration, it was determined that the target JRE must be modified. The currently running JRE is the target JRE and cannot be modified as required.

Administrator response

Configure the Security Verify Access Runtime for Java by executing the pdjrtecfg command found in the Security Verify Access sbin directory. The pdjrtecfg command must be executed in non-interactive mode. Also, do not use a response file when executing pdjrtecfg.

HPDBF0342E

The Java Runtime Environment (*%s*) cannot be configured. (0x30695156)

Explanation

The target Java Runtime Environment must be modified in order to be configured. The configuration program was unable to make the modifications, possibly due to file system access problems.

Administrator response

Ensure that the lib directory in the target Java Runtime Environment is writable by the user running the configuration program. Also ensure that the jsse.jar file found in the lib directory can be moved by that same user. Finally, ensure the target JRE is not actively running during configuration. Alternatively, manually move the jsse.jar file to a backup location outside of the lib directory and then re-run the configuration program. In this case, note that when the Security Verify Access Runtime for Java is unconfigured for that JRE, the jsse.jar file must be manually restored from its backup location to the lib directory.

HPDBF0343W

An error occurred while restoring the original state of the target Java Runtime Environment (*%s*). The JRE might need post-unconfiguration modification. (0x30695157)

Explanation

During Security Verify Access Runtime for Java configuration, the target JRE was modified so that the jsse.jar file in its lib directory was moved to a jarbackup directory created under lib. The unconfiguration program is unable to move the jsse.jar file back to its original location and remove the jarbackup directory, possibly due to file system access problems.

Administrator response

Manually restore the state of the Java Runtime Environment by moving the jsse.jar file in JRE lib/jarbackup directory to its original location in the lib directory. Then remove the jarbackup directory.

HPDBF0344W

The temporary file *%s* cannot be deleted. Manually delete the file. (0x30695158)

Explanation

During Security Verify Access Runtime for Java configuration, a temporary file was created, but cannot be deleted, possibly due to file system access problems.

Administrator response
Manually delete the named file.

HPDBF0350E

Unable to start Security Verify Access Web Portal Manager. (0x3069515e)

Explanation
An error occurred while starting Security Verify Access Web Portal Manager.

Administrator response
Stop and restart the IBM WebSphere Application Server.

HPDBF0358E

Could not contact the Security Verify Access authorization server. Possible causes are:The Authorization server is not running.The Authorization server host name or port number is incorrect. (0x30695166)

Explanation
See message.

Administrator response
Make sure the authorization server is running and specify a correct value for host name and port number, and retry the command.

HPDBF0359E

Could not contact the WebSphere server. Possible causes are:The WebSphere server is not running.The WebSphere server host name or port number is incorrect. (0x30695167)

Explanation
See message.

Administrator response
Make sure the IBM WebSphere Application Server or Deployment Manager is running and specify a correct value for host name and port number, and retry the command.

HPDBF0360E

Could not find a IBM WebSphere Application Server or Cluster. Possible causes are:The WebSphere server host name or port number is incorrect. The specified cluster or application server is invalid. (0x30695168)

Explanation
See message.

Administrator response
Specify a correct value for host name and port number, and retry the command.

HPDBF0361E

Invalid hostname for the Security Verify Access policy server. Possible causes are:The Policy server host name is incorrect. (0x30695169)

Explanation
See message.

Administrator response
Specify a correct value for the host name and retry the command.

HPDBF0362E

Invalid hostname for the Security Verify Access authorization server. Possible causes are:The Authorization server host name is incorrect. (0x3069516a)

Explanation
See message.

Administrator response
Specify a correct value for the host name and retry the command.

HPDBF0363E

Invalid hostname for the WebSphere server. Possible causes are:The WebSphere host name is incorrect. (0x3069516b)

Explanation
See message.

Administrator response
Specify a correct value for the host name and retry the command.

HPDBF0364E

The required option (*%s*) was not specified. (0x3069516c)

Explanation
See message.

Administrator response
Specify all of the required options. Retry the command.

HPDBF0380E

Unable to create the PDJLog.properties file in the specified JRE.Ensure you have the correct permissions to do so. (0x3069517c)

Explanation
Unable to create PDJLog.properties file in PolicyDirector directory of the JRE being configured.

Administrator response
Ensure that the user has the necessary permissions to create the PolicyDirector directory and the PDJLog.properties file in the <JRE_HOME>/PolicyDirector directory.

HPDBF0391E

The Security Verify Access Runtime for Java cannot run with the FIPS mode set. (0x30695187)

Explanation
The Security Verify Access Runtime for Java has configured FIPS mode that is different from the WebSphere FIPS mode.

Administrator response
Make sure that the WebSphere and Security Verify Access Runtime for Java are configured with the same FIPS setting.

HPDBF0405E

The Security Verify Access Runtime for Java installed within the JRE (*%s*) version (*%s*) is outdated.Upgrade the Security Verify Access Runtime for Java. (0x30695195)

Explanation
Security Verify Access Runtime for Java needs to be upgraded.

Administrator response
Upgrade the Security Verify Access Runtime for Java configured to the JRE.

HPDBF0432E

A memory allocation error resulted in the termination of the program. Check the maximum allowable memory and the amount of system paging space as these may both need to be increased. (0x306951b0)

Explanation
See message.

Administrator response
Increase the maximum allowable memory and the system paging space or shut down one or more applications.

HPDBF0435E

An error occurred while copying the template file. (0x306951b3)

Explanation
The template file could not be copied.

Administrator response
Make sure the file exists and has permissions appropriate for copying.

HPDBF0436E

Security Verify Access server has already been unconfigured. from common and audit reporting services. (0x306951b4)

Explanation
The server is already unconfigured from common audit and reporting services.

Administrator response
No action required.

HPDBF0437E

Option *%s* is required. (0x306951b5)

Explanation
Required option is not specified.

Administrator response
Reissue the command specifying the missing option.

HPDBF0438E

The server configuration file *%s* is invalid. (0x306951b6)

Explanation
The file does not contain an azn server name and is not the policy server configuration file.

Administrator response
Reissue the command specifying a valid server configuration file.

HPDBF0439E

Invalid value specified for -action. Valid values are \'config\' and \'unconfig\'. (0x306951b7)

Explanation
Invalid value specified for -action. Valid values are \'config\' and \'unconfig\'.

Administrator response
Reissue the command specifying an action of \'config\' or \'unconfig\'.

HPDBF0440E

The file *%s* could not be accessed. (0x306951b8)

Explanation
The file does not exist or does not have the correct permissions.

Administrator response
Reissue the command specifying a valid file.

HPDBF0442E

Option *%s* is required with option *%s*. (0x306951ba)

Explanation
Required option is not specified.

Administrator response
Reissue the command specifying the missing option.

HPDBF0443E

The server audit configuration file *%s* could not be created. (0x306951bb)

Explanation
The server audit configuration file could not be created.

Administrator response
Ensure that there is enough space and that the directory has the correct permissions Then, reissue the command.

HPDBF0444E

Configuration data could not be written to *%s*. (0x306951bc)

Explanation
The server audit configuration file could not be created.

Administrator response
Ensure that there is enough space and that the directory has the correct permissions Then, reissue the command.

HPDBF0445E

Invalid value specified for -disk_cache_mode. Valid values are \'auto\', \'always\', and \'never\'. (0x306951bd)

Explanation
Invalid value specified for -disk_cache_mode. Valid values are \'auto\', '\always'\, and \'never\'.

Administrator response
Reissue the command specifying a valid value for -disk_cache_mode.

HPDBF0446E

Invalid value specified for -enable_ssl. Valid values are \'yes\' and \'no\'. (0x306951be)

Explanation
Invalid value specified for -enable_ssl. Valid values are \'yes' and \'no\'.

Administrator response
Reissue the command specifying a valid value for -enable_ssl.

HPDBF0447E

Invalid value specified for -enable_pwd_auth. Valid values are \'yes\' and \'no\'. (0x306951bf)

Explanation
Invalid value specified for -enable_pwd_auth. Valid values are \'yes' and \'no\'.

Administrator response
Reissue the command specifying a valid value for -enable_pwd_auth.

HPDBF0448E

The audit server could not be contacted. (0x306951c0)

Explanation
The audit server is down or the information provided for the audit server is incorrect.

Administrator response
After verifying the audit server is running and the information provided for the audit server is correct, reissue the command.

HPDBF0470E

The audit key file is invalid. (0x306951d6)

Explanation
The audit key file is invalid.

Administrator response
Specify a valid key file.

HPDBF0471E

The audit stash file is invalid. (0x306951d7)

Explanation
The audit stash file is invalid.

Administrator response
Specify a valid stash file.

HPDBF0472E

The audit ID is invalid. (0x306951d8)

Explanation
The audit ID is invalid.

Administrator response
Specify a valid audit ID.

HPDBF0473E

The audit ID password is invalid. (0x306951d9)

Explanation
The audit ID password is invalid.

Administrator response
Specify a valid audit ID password.

HPDBF0474E

The audit server URL is invalid. (0x306951da)

Explanation
The audit server URL is invalid.

Administrator response
Specify a valid audit server URL.

HPDBF0475E

The audit cache file is invalid. (0x306951db)

Explanation
The audit cache file is invalid.

Administrator response
Specify a valid audit cache file.

HPDBF0476E

Incorrect Security Verify Access value for policysvr. The value should contain host:port:rank. (0x306951dc)

Explanation
An incorrect entry was given for policysvr. It should have host:port:rank.

Administrator response
Correct the information and retry the command.

HPDBF0479E

Invalid value specified for -temp_storage_full_timeout. Valid values are \'-1\', \'0\', and any positive integer. (0x306951df)

Explanation
Invalid value specified for -temp_storage_full_timeout. Valid values are \'-1\', '\0'\, and any positive integer.

Administrator response
Reissue the command specifying a valid value for -temp_storage_full_timeout.

HPDBF0480E

The option -temp_storage_full_timeout is only valid when -disk_cache_mode is set to \'auto\' or \'always \'. (0x306951e0)

Explanation
The option -temp_storage_full_timeout is only valid when -disk_cache_mode is set to \'auto\' or '\always \'.

Administrator response
Reissue the command specifying a proper value for -disk_cache_mode.

HPDBF0495E

The -ldap_mgmt option must be either 'true' or 'false'. (0x306951ef)

Explanation
See message.

Administrator response
Retry the command with valid -ldap_mgmt value.

HPDBF0496E

The -ldap_mgmt option must be set to 'true' to use the -ldap_svrs option. (0x306951f0)

Explanation
See message.

Administrator response
Retry the command with valid -ldap_mgmt value.

HPDBF0497E

The -ldap_svrs opton must be set when -ldap_mgmt option is set to 'true'. (0x306951f1)

Explanation
See message.

Administrator response
Retry the command adding -ldap_svrs option.

HPDBF0498E

The LDAP server option entered was not valid.The format of the LDAP server option is host:port:type:rank[,host1:port1:rank1[,...]] where type is one of 'readwrite' or 'readonly'. (0x306951f2)

Explanation
See message.

Administrator response
Rerun the command with a valid LDAP server option.

HPDBF0499E

The LDAP server port number is not valid.The port must be an integer greater than 0 and less than 65536. (0x306951f3)

Explanation
See message.

Administrator response
Retry the command with a valid port number.

HPDBF0500E

The LDAP server type is not valid.The type must be one of 'readwrite' or 'readonly'. (0x306951f4)

Explanation
See message.

Administrator response
Retry the command with a valid LDAP server type.

HPDBF0501E

The LDAP server rank is not valid.The rank must be an integer from 0 to 10. (0x306951f5)

Explanation
See message.

Administrator response
Retry the command with a valid rank value.

HPDBF0502E

The -ldap_mgmt option must be set to 'true' to use the -ldap_ssl_enable option. (0x306951f6)

Explanation
See message.

Administrator response
Retry the command with valid -ldap_mgmt value.

HPDBF0503E

The -ldap_ssl_enable option must be either 'true' or 'false'. (0x306951f7)

Explanation
See message.

Administrator response
Retry the command with valid -ldap_ssl_enable value.

HPDBF0504E

The -ldap_mgmt option must be set to 'true' to use the -ldap_ssl_truststore option. (0x306951f8)

Explanation
See message.

Administrator response
Retry the command with valid -ldap_mgmt value.

HPDBF0505E

The file specified by the -ldap_ssl_truststore is not accessible. (0x306951f9)

Explanation
See message.

Administrator response
Ensure that the specified file exists and that it has appropriate permissions.

HPDBF0506E

The -ldap_ssl_truststore option must be set to use the -ldap_ssl_truststore_pwd option. (0x306951fa)

Explanation
See message.

Administrator response
Retry the command with -ldap_ssl_truststore set.

HPDBF0507E

The -ldap_ssl_truststore_pwd option must be set to use the -ldap_ssl_truststore option. (0x306951fb)

Explanation
See message.

Administrator response
Retry the command with -ldap_ssl_truststore_pwd set.

HPDBF0526E

The Security Verify Access Runtime for Java cannot run as the WebSphere security standard does not match the configured compliance. (0x3069520e)

Explanation
The Security Verify Access Runtime for Java has configured a compliance mode that is different from the WebSphere security standard compliance.

Administrator response
Make sure that the WebSphere and Security Verify Access Runtime for Java are configured with the same setting.

HPDBF0528E

The response file *%s* could not be deleted. (0x30695210)

Explanation
The response file could not be deleted.

Administrator response
Check the path and permissions of the file, then delete the file.

HPDBF0531E

The SSL V3 protocol enable flag is invalid. The value must be true or false. (0x30695213)

Explanation
See message.

Administrator response
Retry the command with a valid ssl_v3_enable setting.

HPDBF0533E

The TLS V1.0 protocol enable flag is invalid. The value must be true or false. (0x30695215)

Explanation
See message.

Administrator response
Retry the command with a valid tls_v10_enable setting.

HPDBF0535E

The TLS V1.1 protocol enable flag is invalid. The value must be true or false. (0x30695217)

Explanation
See message.

Administrator response
Retry the command with a valid tls_v11_enable setting.

HPDBF0537E

The TLS V1.2 protocol enable flag is invalid. The value must be true or false. (0x30695219)

Explanation
See message.

Administrator response
Retry the command with a valid tls_v12_enable setting.

HPDBG0001E

Unsupported operating system type: *%s*. (0x30696001)

Explanation
The command is not supported on this operating system.

Administrator response
Change to a supported operating system and retry the command.

HPDBG0003E

Login to the server failed. (0x30696003)

Explanation
An attempt to login to the server was unsuccessful.

Administrator response
Ensure the server is running, that all ports, user IDs and passowrds are correct, then retry the command.

HPDBG0005E

This script must be executed by 'root' (uid = 0). (0x30696005)

Explanation
Invalid credentials detected running this process.

Administrator response
Login as the root user and retry the command.

HPDBG0017E

The policy server must first be installed in the secure domain.Install the Security Verify Access policy server on one of the systemsin your secure domain and retry the command. (0x30696011)

Explanation
Same as text.

Administrator response
Same as text.

HPDBG0019W

The policy server is not running in this secure domain.Start the policy server and retry the command. (0x30696013)

Explanation
The policy server cannot be contacted.

Administrator response
Start the policy server and retry the command.

HPDBG0028W

The parent directory does not exist.Cannot create the document root directory. (0x3069601c)

Explanation
The directory cannot be created.

Administrator response
Check the file permissions and ensure there is enough disk space.

HPDBG0043W

Could not restart the server. (0x3069602b)

Explanation
The server could not be restarted.

Administrator response
Check the error logs, correct the problem, then retry the command.

HPDBG0062W

The post-configuration phase of the package failed. (0x3069603e)

Explanation
A problem has occurred that prevented the package from configuring successfully.

Administrator response
Review the log files, correct the problem, then retry the command.

HPDBG0063W

The pre-configuration phase of the package failed. (0x3069603f)

Explanation
A problem has occurred that prevented the package from configuring successfully.

Administrator response
Review the log files, correct the problem, then retry the command.

HPDBG0064W

The package is already configured. (0x30696040)

Explanation
The package cannot be configured because it is already configured.

Administrator response
Unconfigure the package first, then retry the command.

HPDBG0066W

The pre-removal of the package has failed. (0x30696042)

Explanation
An error occurred during the pre-remove phase of the process.

Administrator response
Review log files, correct the problem, then retry the command.

HPDBG0087W

Could not contact the LDAP server. (0x30696057)

Explanation
Same as text.

Administrator response
Ensure the port, administrator id, and password are correct, and ensure the server is running on the specified host name.

HPDBG0106W

SBS configuration error. (0x3069606a)

Explanation
An error occurred during the configuration.

Administrator response
Review the log files, correct the problem, then retry the command.

HPDBG0107W

SBS unconfiguration error. (0x3069606b)

Explanation
An error occurred during the unconfiguration.

Administrator response
Review the log files, correct the problem, then retry the command.

HPDBG0108W

Cannot connect to the LDAP server. (0x3069606c)

Explanation
Same as text.

Administrator response
Ensure the administrator id, password, and port are correct and that the server is running on the specified machine.

HPDBG0109W

Invalid LDAP authentication. (0x3069606d)

Explanation
A password, administrator id, keyfile password, etc. was invalid.

Administrator response
Ensure the correct passwords and ids have been specified, then retry the command.

HPDBG0110W

The LDAP server is not available. (0x3069606e)

Explanation
The LDAP server is not responding.

Administrator response
Ensure the server name and port have been speified correctly then retry the command.

HPDBG0111W

Not authorized to perform the LDAP operation. (0x3069606f)

Explanation
The LDAP server denied the requested operation.

Administrator response
Ensure the user has appropriate access then retry the command.

HPDBG0112W

Cannot connect to the LDAP server using SSL. (0x30696070)

Explanation
Same as text.

Administrator response
Ensure the SSL key file is valid, the password and port is correct, and that the server is running. Also check the date on the machines and validate that the key file has not expired.

HPDBG0113W

An unexpected LDAP error has occurred. (0x30696071)

Explanation
Same as text.

Administrator response
Check the log files on this machine and on the LDAP server, correct the problem, then retry the command.

HPDBG0114W

Unable to disable the Security Verify Access WebSEAL server. (0x30696072)

Explanation
Same as text.

Administrator response
Review the log files, correct the problem, then retry the command.

HPDBG0115W

Unable to disable the NetSEAL server. (0x30696073)

Explanation
Same as text.

Administrator response
Review the log files, correct the problem, then retry the command.

HPDBG0117W

LDAP client version *%s* does not appear to be installed.The LDAP client must be installed and configured in order to use the LDAP user registry. (0x30696075)

Explanation
Same as text.

Administrator response
Same as text.

HPDBG0119W

Configure the net package before the trap package. The configuration failed. (0x30696077)

Explanation
A configuration was attempted out of sequence.

Administrator response
Configure the packages in order.

HPDBG0123W

Unconfigure the authorization server package before the base package. The unconfiguration failed. (0x3069607b)

Explanation
The unconfiguration was attempted out of sequence.

Administrator response
Same as text.

HPDBG0131W

This package is partially configured.Unconfigure this package before configuring it. To unconfigure,return to the Security Verify Access Configuration Menu and select Exit. (0x30696083)

Explanation
Same as text.

Administrator response
Same as text.

HPDBG0147W

Configure the Security Verify Access Runtime package before this package. The configuration failed. (0x30696093)

Explanation
A configuration was attempted out of sequence.

Administrator response
Configure the packages in order.

HPDBG0148W

Configure the Security Verify Access Runtime package before the Net package. The configuration has failed. (0x30696094)

Explanation
A configuration was attempted out of sequence.

Administrator response
Configure the packages in order.

HPDBG0149W

Configure the runtime package before the authorization server package. The configuration failed. (0x30696095)

Explanation
A configuration was attempted out of sequence.

Administrator response
Configure the packages in order.

HPDBG0150W

Unconfigure the policy server package before the runtime package. The unconfiguration failed. (0x30696096)

Explanation
The unconfiguration was attempted out of sequence.

Administrator response
Same as text.

HPDBG0151W

Unconfigure the authorization server package before the runtime package. The unconfiguration failed. (0x30696097)

Explanation
The unconfiguration was attempted out of sequence.

Administrator response
Same as text.

HPDBG0152W

Unconfigure the Net package before the runtime package. The unconfiguration failed. (0x30696098)

Explanation
The unconfiguration was attempted out of sequence.

Administrator response
Same as text.

HPDBG0153W

Could not initialize the SSL configuration. (0x30696099)

Explanation
Same as text.

Administrator response
Ensure the key file, password, and port are correct and that the server is running in SSL mode.

HPDBG0154W

Could not initialize the Base SSL configuration. (0x3069609a)

Explanation
Same as text.

Administrator response
Ensure the key file, password, and port are correct and that the server is running in SSL mode.

HPDBG0163W

Install all required Security Verify Access packageson the system before running pdconfig. (0x306960a3)

Explanation
Same as text.

Administrator response
Same as text.

HPDBG0164W

Configure the runtime package before the application developer kit. The configuration failed. (0x306960a4)

Explanation
A configuration was attempted out of sequence.

Administrator response
Same as text.

HPDBG0165W

Configure the runtime package before the console package. The configuration failed. (0x306960a5)

Explanation
A configuration was attempted out of sequence.

Administrator response
Same as text.

HPDBG0166W

Unconfigure the application developer kit before the runtime package. (0x306960a6)

Explanation
The unconfiguration was attempted out of sequence.

Administrator response
Same as text.

HPDBG0167W

Unconfigure the console package before the runtime package. (0x306960a7)

Explanation
The unconfiguration was attempted out of sequence.

Administrator response
Same as text.

HPDBG0192W

Unconfigure the Web package before the policy server package. The unconfiguration failed. (0x306960c0)

Explanation
An unconfiguration was attempted out of sequence.

Administrator response
Same as text.

HPDBG0193W

Unconfigure the Web package before the runtime package. The unconfiguration failed. (0x306960c1)

Explanation
The unconfiguration was attempted out of sequence.

Administrator response
Same as text.

HPDBG0205W

Some packages have not been upgraded yet.Upgrade the remaining packages and retry the command. (0x306960cd)

Explanation
Same as text.

Administrator response
Same as text.

HPDBG0207W

The upgrade failed. (0x306960cf)

Explanation
The upgrade did not complete successfully.

Administrator response
Review log files or other previous messages, correct the problem, then retry the command.

HPDBG0210W

%s was not found. (0x306960d2)

Explanation
A file could not be found.

Administrator response
Ensure the file exists and can be accessed, then retry the command.

HPDBG0211W

Configure the policy server before the authorization server. The configuration failed. (0x306960d3)

Explanation
A configuration was attempted out of sequence.

Administrator response
Same as text.

HPDBG0212W

Configure the policy server before the net package. The configuration failed. (0x306960d4)

Explanation
A configuration was attempted out of sequence.

Administrator response
Same as text.

HPDBG0213W

Configure the policy server before the Web package. The configuration failed. (0x306960d5)

Explanation
A configuration was attempted out of sequence.

Administrator response
Same as text.

HPDBG0214W

The version of the installed LDAP client must be *%s* or higher. (0x306960d6)

Explanation
Same as text.

Administrator response
Install the LDAP client and retry the command.

HPDBG0215W

Security Verify Access policy server must be upgraded on the system. (0x306960d7)

Explanation
Same as text.

Administrator response
Same as text.

HPDBG0217W

The LDAP server host name does not exist. (0x306960d9)

Explanation
Same as text.

Administrator response
Ensure the LDAP server host name was entered correctly, that the server is running, and that the port was specified correctly.

HPDBG0232E

Load the Security Verify Access schema entries. (0x306960e8)

Explanation
The schema for secAuthority=Default has not been set up on the LDAP server.

Administrator response
Apply the schema then retry the command.

HPDBG0275W

The necessary LiveCONTENT directory components have not been installed.They must be installed before configuration can continue. (0x30696113)

Explanation
Same as text.

Administrator response
Same as text.

HPDBG0277W

Security Verify Access policy server (*%s*,*%s*) cannot be contacted. (0x30696115)

Explanation
The specified host and port cannot be accessed.

Administrator response
Ensure the port and host name are correct, then retry the command.

HPDBG0278E

Login to the Security Verify Access policy server failed.Ensure that the password is correct and the policy server is running, then retry the command. (0x30696116)

Explanation
Same as text.

Administrator response
Same as text.

HPDBG0284E

Unable to read necessary files. Ensure read permission is set forthe current user on the following files located in the directory specifiedabove: ivmgrd.conf, ivmgrd.kdb, ivmgrd.sth, pdcacert.b64 (0x3069611c)

Explanation
Same as text.

Administrator response
Same as text.

HPDBG0297W

Unconfigure the policy proxy server before the policy server. The unconfiguration failed. (0x30696129)

Explanation
The unconfiguration was attempted out of sequence.

Administrator response
Same as text.

HPDBG0298W

Unconfigure the policy proxy server before the runtime package. The unconfiguration failed. (0x3069612a)

Explanation
The unconfiguration was attempted out of sequence.

Administrator response
Same as text.

HPDBG0322E

The specified administrator ID is not authorized to configurethe server. Check the ID, password, and port and be sure the policy serveris configured and running. (0x30696142)

Explanation
Same as text.

Administrator response
Log in as an administrative user and retry the command.

HPDBG0323E

The specified administrator ID is not authorized to configurethe server. Check the ID, password, and port and be sure the policy serveris configured and running. (0x30696143)

Explanation
Same as text.

Administrator response
Ensure the correct user name, password, and port are specified.

HPDBG0327E

LDAP client version *%s* does not appear to be installed.The LDAP client must be installed to use the Active Directory user registry. (0x30696147)

Explanation
Same as text.

Administrator response
Same as text.

HPDBG0331E

The version of the installed *%s* must be *%s* or higher. (0x3069614b)

Explanation
Same as text.

Administrator response
Same as text.

HPDBG0348E

The environment variable JAVA_HOME must be set to an existing valid JRE before executing this command. (0x3069615c)

Explanation
JAVA_HOME is necessary to determine what JRE to use for the process.

Administrator response
Set the JAVA_HOME variable then retry the command.

HPDBG0349E

The LDAP client package *%s*, version *%s* does not appear to be installed. (0x3069615d)

Explanation
Same as text.

Administrator response
Install the package and try the command again.

HPDBG0350E

The Tivoli Common Logging directory cannot be a relative directory. (0x3069615e)

Explanation
The path is invalid. It must be an absolute path.

Administrator response
Re-enter the directory.

HPDBG0351E

The Tivoli Common Logging directory cannot be created. (0x3069615f)

Explanation
The path is invalid. It must be an absolute path and must allow creation.

Administrator response
Re-enter the directory.

HPDBG0358E

The management domain name, *%s*,already exists within LDAP. (0x30696166)

Explanation
The domain name must not already exist within LDAP.

Administrator response
Retry the command specifying a different domain name or remove the existing one from LDAP.

HPDBG0367E

Instance '*%s*' is already configured ('*%s*'). (0x3069616f)

Explanation
A configuration file for the instance specified already exists.

Administrator response
Use a different name or remove the existing configuration file and its associated key files.

HPDBG0812E

An Administrative account must be used to run this program. (0x3069632c)

Explanation
The user is not qualified to run the program.

Administrator response
Log in as an administrative user and retry the command.

HPDBG0813E

Security Verify Access registry entries could not be created. (0x3069632d)

Explanation
A problem was detected while trying to create entries in the system registry.

Administrator response
Be sure another process is not accessing the registry and retry the command.

HPDBG0826E

The *%s* service failed to start. (0x3069633a)

Explanation
The service could not be started.

Administrator response
Review log files, the Event Viewer, or other messages, then retry the command.

HPDBG0827E

The directory *%s* could not be created. (0x3069633b)

Explanation
The specified directory could not be created.

Administrator response
Check the permissions of the parent directory and disk space, then retry the command.

HPDBG0828E

The unconfiguration of the *%s* server failed. (0x3069633c)

Explanation
Same as text.

Administrator response
Review log files, the Event Viewer, or other messages, correct the problem, then retry the command.

HPDBG0829W

The *%s* service could not be deleted. (0x3069633d)

Explanation
Same as text.

Administrator response
Review log files, the Event Viewer, or other messages, correct the problem, then retry the command.

HPDBG0830E

The *%s* server could not be configured. (0x3069633e)

Explanation
Same as text.

Administrator response
Review log files, the Event Viewer, or other messages, correct the problem, then retry the command.

HPDBG0832E

The directory *%s* could not be created. (0x30696340)

Explanation
Same as text.

Administrator response
Check permissions on the parent directory and disk space, then retry the command.

HPDBG0836E

Could not create keytab directory: *%s* (0x30696344)

Explanation
The directory could not be created.

Administrator response
Check permissions of the parent directory and disk space, then retry the command.

HPDBG0837E

Startup of Security Verify Access Policy Server failed. (0x30696345)

Explanation
Same as text.

Administrator response
Review the logs, Event Viewer, or other messages, correct the problem, then retry the command.

HPDBG0838E

Startup of Security Verify Access Security Server failed. (0x30696346)

Explanation
Same as text.

Administrator response
Review the logs, Event Viewer, or other messages, correct the problem, then retry the command.

HPDBG0839E

Startup of Security Verify Access Authorization Server failed. (0x30696347)

Explanation
Same as text.

Administrator response
Review the logs, Event Viewer, or other messages, correct the problem, then retry the command.

HPDBG0840E

An error occurred configuring the *%s* service. (0x30696348)

Explanation
Same as text.

Administrator response
Review the logs, Event Viewer, or other messages, correct the problem, then retry the command.

HPDBG0841E

Could not get configuration information from the Security Verify Access registry. (0x30696349)

Explanation
The process could not access the system registry properly.

Administrator response
The package may need to be reinstalled or the registry may be corrupt.

HPDBG0843E

Could not stop the *%s* service. (0x3069634b)

Explanation
Same as text.

Administrator response
Review the logs, Event Viewer, or other messages, correct the problem, then retry the command.

HPDBG0844E

The *%s* package must be removed first. (0x3069634c)

Explanation
Same as text.

Administrator response
Remove the specified package, then retry the command.

HPDBG0857W

The Security Verify Access Policy Server is already configured in this secure domain.The Security Verify Access Policy Server must be removed completely before installing. (0x30696359)

Explanation
Same as text.

Administrator response
Same as text.

HPDBG0858W

The Security Verify Access Policy Server appears to be configured on another machine in the secure domain. The local Security Verify Access Policy Server cannot be unconfigured. (0x3069635a)

Explanation
Same as text.

Administrator response
Same as text.

HPDBG0860E

GsoInit error 1: Invalid Parameters (0x3069635c)

Explanation
An invalid parameter was specified.

Administrator response
Correct the parameter and retry the command.

HPDBG0861W

GsoInit error 2: No LDAP Connection (0x3069635d)

Explanation
The LDAP host could not be reached.

Administrator response
Ensure the information is correct, then retry the command.

HPDBG0862W

GsoInit error 3: Not Authorized (0x3069635e)

Explanation
The user is not authroized to perform the task.

Administrator response
Increase the user's authority or try the command again as a different user.

HPDBG0863W

GsoInit error 4: Object Exists (0x3069635f)

Explanation
The object that is trying to be created already exists.

Administrator response
Delete the object then retry the command.

HPDBG0864W

GsoInit error 5: Object Not Found (0x30696360)

Explanation
The object could not be found.

Administrator response
Ensure the configuration was successful, then retry the command.

HPDBG0865W

GsoInit error 6: No GSO Database (0x30696361)

Explanation
The GSO database does not exist.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBG0866W

GsoInit error 7: No Suffix (0x30696362)

Explanation
The suffix does not exist.

Administrator response
Ensure the configuration was successful, then retry the command.

HPDBG0867W

GsoInit error 8: GSO Database Exists (0x30696363)

Explanation
The database could not be created because it already exists.

Administrator response
The database could not be created because it already exists. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBG0868W

GsoInit error 9: GSO Unrecoverable Error (0x30696364)

Explanation
An unknown error occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBG0869W

GsoInit error 10: Can't get LDAP Connection (0x30696365)

Explanation
The LDAP server could not be reached.

Administrator response
Ensure the server is running and that the information is correct, then retry the command.

HPDBG0870W

GsoInit error 11: Not GSO User (0x30696366)

Explanation
The user is not a valid GSO user.

Administrator response
Retry the command as a valid GSO user.

HPDBG0905E

SBS Unconfiguration Error (0x30696389)

Explanation
An error occurred unconfiguring SBS.

Administrator response
Review log files or other messages, then retry the command.

HPDBG0906W

Cannot connect to the LDAP server. (0x3069638a)

Explanation
The LDAP server could not be reached.

Administrator response
Ensure the server is running and that the information is correct, then retry the command.

HPDBG0907W

Invalid LDAP authentication (0x3069638b)

Explanation
The LDAP server denied the request.

Administrator response
Ensure the LDAP administrator id and password are correct.

HPDBG0908W

LDAP server not available (0x3069638c)

Explanation
Same as text.

Administrator response
Ensure the LDAP server is running and the ports are correct, then retry the command.

HPDBG0909W

Not authorized to perform LDAP operation (0x3069638d)

Explanation
The LDAP server denied the request.

Administrator response
Ensure the LDAP administrator id and password are correct.

HPDBG0910W

Cannot connect to registry server using SSL. (0x3069638e)

Explanation
SSL could not be used to communicate to the registry server.

Administrator response
Ensure the ports, key file, passowrd, and ids are correct, and that the registry server can use SSL, then retry the command.

HPDBG0938E

Configuration failed.\r (0x306963aa)

Explanation
The configuration process failed.

Administrator response
Review logs, correct the problem, then retry the command.

HPDBG0957E

Error attempting to shutdown the system. (0x306963bd)

Explanation
The system could not be shut down.

Administrator response
Shut down and restart the system manually.

HPDBG0964E

ERROR: SecAuthority=Default suffix not found on LDAP server. Load secschema.def before configuring Security Verify Access (0x306963c4)

Explanation
The LDAP server configuration may not be completely finished.

Administrator response
Apply the schema as directed, then retry the command.

HPDBG0972W

Security Verify Access Policy Server must first be upgraded on this system. (0x306963cc)

Explanation
The policy server must be upgraded before this package.

Administrator response
Upgrade the policy server, then retry the command.

HPDBG0973E

SecAuthority=Default suffix not found on LDAP server, Security Verify Access initialization of LDAP failed (0x306963cd)

Explanation
The LDAP server configuration was not completed before running this process.

Administrator response
Apply the schema on the LDAP server, then retry this command.

HPDBG0991E

URAFCFG environment variable not set. (0x306963df)

Explanation
Same as text.

Administrator response
Set the variable, then retry the command.

HPDBG0992E

Notes_ExecDirectory environment variable not set. (0x306963e0)

Explanation
Same as text.

Administrator response
Set the variable, then retry the command.

HPDBG0993E

The Notes install directory is not in the PATH (0x306963e1)

Explanation
Same as text.

Administrator response
Set the PATH to include the Notes install directory, then retry the command.

HPDBG0994E

The EXTMGR_ADDINS parameter is not set in notes.ini. (0x306963e2)

Explanation
Same as text.

Administrator response
Set the parameter in the notes.ini file, then retry the command.

HPDBG0997W

The notes.ini file does not exist in the Windows directory. (0x306963e5)

Explanation
Same as text.

Administrator response
Ensure the product was installed correctly, then retry the command.

HPDBG1005E

Could not contact the LDAP server. Possible causes are:The LDAP server is not running.The LDAP server host name or port is incorrect.There is an SSL configuration mismatch between Security Verify Access and the registry server. (0x306963ed)

Explanation
Same as text.

Administrator response
Same as text - correct the problem, then retry the command.

HPDBG1006E

Could not contact the Security Verify Access Policy Server.Ensure that you have specified a valid host name and port number and that Security Verify Access Policy Server is started before retrying this operation. (0x306963ee)

Explanation
Same as text.

Administrator response
Same as text.

HPDBG1007W

Could not get the TCP/IP host name of local machine. (0x306963ef)

Explanation
Same as text.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBG1032W

You are not authorized to update the schema! (0x30696408)

Explanation
Same as text.

Administrator response
Log in as a different user and retry the command.

HPDBG1049W

Unable to read necessary files. Make sure that the readpermission is set for the current user on the following files located inthe directory specified: ivmgrd.conf, ivmgrd.kdb, ivmgrd.sth, pdcacert.b64 (0x30696419)

Explanation
Same as text.

Administrator response
Same as text.

HPDBG1054W

Cannot contact the host server.Possible causes are:The host server is not running.The host server name is incorrect. (0x3069641e)

Explanation
Same as text.

Administrator response
Ensure the server is running and that the information is correct, then retry the command.

HPDBG1056W

Could not contact the Domino server. Possible causes are:The Domino server is not running.The Domino server host name is incorrect.The Notes client password is incorrect for the active Notes ID file.Verify that information and then unconfigure and reconfigure the Runtime component with the correct values. (0x30696420)

Explanation
Same as text.

Administrator response
Same as text.

HPDBG1080E

Could not contact the Security Verify Access Policy Server.Ensure that you have specified a valid ID, password and domain name and that Security Verify Access Policy Server is started before retrying this operation. (0x30696438)

Explanation
Same as text.

Administrator response
Same as text.

HPDBG1083E

Error: Command *%s* failed (0x*%x*). Make sure java is in the path. (0x3069643b)

Explanation
See text.

Administrator response
See text, review logs, correct the problem, then retry the command.

HPDBG1096E

The environment variable JAVA_HOME must be set to an existing valid JRE before executing this command. (0x30696448)

Explanation
JAVA_HOME is necessary to determine what JRE to use for the process.

Administrator response
Set the JAVA_HOME variable then retry the command.

HPDBG1097E

The Security Verify Access License registry key is missing. (0x30696449)

Explanation
The current version of Security Verify Access License must be installed to configure other Security Verify Access components.

Administrator response
Install Security Verify Access License from the Security Verify Access CDs then retry this command.

HPDBG1098E

Security Verify Access License is not installed. (0x3069644a)

Explanation
The current version of Security Verify Access License must be reinstalled to configure other Security Verify Access components. The registry key may contain an incorrect 'Path' or the path doesn't match the path returned by the pd_get_path command.

Administrator response
Install Security Verify Access License from the Security Verify Access CDs to the same path as the other Security Verify Access components then retry this command.

HPDBG1099E

Security Verify Access License is not at the required version level. (0x3069644b)

Explanation
Security Verify Access License must be at the current level to configure other Security Verify Access components.

Administrator response
Reinstall the Security Verify Access License from the current Security Verify Access CDs then retry this command.

HPDBG1100E

Security Verify Access Policy Server must be unconfigured before it is removed. (0x3069644c)

Explanation
The policy server must be unconfigured before removal.

Administrator response
Unconfigure the policy server and then retry the removal.

HPDBG1101E

Security Verify Access policy proxy server must be unconfigured before it is removed. (0x3069644d)

Explanation
The policy proxy server must be unconfigured before removal.

Administrator response
Unconfigure the policy proxy server and then retry the removal.

HPDBG1102E

Security Verify Access Authorization Server must be unconfigured before it is removed. (0x3069644e)

Explanation
The authorization server must be unconfigured before removal.

Administrator response
Unconfigure the authorization server and then retry the removal.

HPDBG1104E

Could not contact the Active Directory server. Possible causes are:The Active Directory server is not running.The Active Directory Global Catalog server is not running.The Active Directory server host name or domain is incorrect. (0x30696450)

Explanation
Same as text

Administrator response
Make sure that the Active Directory server or Active Directory Global Catalog server is running and that the host name specified is the fully qualified host name.

HPDBG1105E

The domain name is different from the local domain and Security Verify Access Policy Server is installed on this machine.If the Policy Server is to be configured on this machine, make sure the domain is correct.If Security Verify Access is configured with the Active Directory multiple domains option, make sure this domain is the root of the Active Directory forest. Policy Server must be installed and configured on the root domain of the forest.When using an LDAP client to communicate with the Active Directory server for a Security Verify Access blade server or user application it's necessary to remove the Security Verify Access Policy Server package then retry the configuration. (0x30696451)

Explanation
Same as text

Administrator response
If the Policy Server will be configured on this machine and it is a client of an Active Directory server, make sure the machine is logged in to the correct domain. Also note that in order for Security Verify Access to be configured with Active Directory multiple domain, the Policy Server must be installed and configured on the root of the Active Directory forest or a client machine of that root domain. Correct the problem and retry.

HPDBG1106E

Invalid authentication information. Either the Active Directory admin ID doesn't exist or the admin password is incorrect. (0x30696452)

Explanation
Same as text

Administrator response
Correct the user ID and password and retry.

HPDBG1107E

Unable to locate the Active Directory data location information. Make sure the Active Directory domain is up and running or check to make sure the distinguished name for the data location exists on the Active Directory server before using it. (0x30696453)

Explanation
The Active Directory data location may not exist or is not yet created in the Active Directory server.

Administrator response
Correct the the Active Directory data location information and retry.

HPDBG1120E

The pdcacert.b64 file could not be downloaded from the policy server. (0x30696460)

Explanation
The certificate automatic download failed.

Administrator response
Make sure the policy server is running.

HPDBG1133W

The management domain location DN, *%s*, was not found in the LDAP server. Create the location DN on the LDAP server or specify a different one. (0x3069646d)

Explanation
The user specified a location DN for private policy server data but the DN does not already exist on the LDAP server.

Administrator response
Create the location DN on the LDAP server first, or specify an existing one.

HPDBG1137E

The windows socket library could not be loaded. (0x30696471)

Explanation
An internal error has occurred.

Administrator response
Ensure that windows socket support is installed and the library directory is in the PATH then retry the command. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBG1156E

The file *%s* could not be deleted. Errno *%d* (0x30696484)

Explanation
The specified file could not be deleted.

Administrator response
Check the permissions of the file, then retry the command.

HPDBG1167E

The parameter supplied for the -C paramter is not valid. (0x3069648f)

Explanation
The user has supplied a value that is not one of: none, fips, sp800-131-transition, sp800-131-strict, suite-b-128, suite-b-192.

Administrator response
Retry the command with a correct -C paramter value

HPDBG1168E

The compliance type is not valid. It must be one of: 'none', 'fips', 'sp800-131-transition', 'sp800-131-strict', 'suite-b-128', 'suite-b-192'. (0x30696490)

Explanation
The user has configured a value that is not one of: none, fips, sp800-131-transition, sp800-131-strict, suite-b-128, suite-b-192.

Administrator response
Retry the command with a correct compliance value

HPDBG1169E

The compliance type is not valid. It must be one of: 'none', 'fips', 'sp800-131-transition', 'sp800-131-strict', 'suite-b-128', 'suite-b-192'. (0x30696491)

Explanation
Same as text.

Administrator response
Same as text.

HPDBG1170E

The compliance value '*%s*' is not valid for ssl-compliance in pd.conf. It must be one of the following values: 'none', 'fips', 'sp800-131-transition', 'sp800-131-strict', 'suite-b-128', 'suite-b-192'. (0x30696492)

Explanation
The pd.conf [ssl] ssl-compliance value is not a valid value.

Administrator response
Correct the value in pd.conf and retry the command.

HPDBG1171E

A second policy server may be configured for standby purposes for AIX ONLY. (0x30696493)

Explanation
A second policy server may be configured for standby purposes for AIX ONLY.

Administrator response
Do not configure a standby policy server on this platform.

HPDBG1172W

Invalid SSL information. (0x30696494)

Explanation
The specified SSL information is invalid.

Administrator response
Ensure the correct SSL information has been provided.

HPDBI0026E

An error occurred configuring *%s*. (0x3078d01a)

Explanation
Configuration failed for the component.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBI0027E

An error occurred while installing *%s*. (0x3078d01b)

Explanation
The installation of the component failed.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBI0036E

Could not change to directory: *%s*. (0x3078d024)

Explanation
The directory does not exist or the permissions are not correct.

Administrator response
Check the permissions and path of the directory.

HPDBI0084E

%s completed with errors. The exit code was *%s*. (0x3078d054)

Explanation
Indicates that the process finished unsucsessfully.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBI0133W

The file, *%s*, did not exist during GSKit configuration. (0x3078d085)

Explanation
Message indicating that a non-critical file was not available on the CD during configuration of GSKIT.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBI0134E

The ldapdb2 user did not get created. Aborting the configuration. (0x3078d086)

Explanation
The creation of the ldapdb2 user failed and configuration cannot continue.

Administrator response
Remove the installed LDAP server components, reboot, and retry the command.

HPDBI0136E

This script only works on: *%s*. (0x3078d088)

Explanation
These are the only platforms on which this process works.

Administrator response
Use this process on one of the listed platforms only.

HPDBI0140E

Unable to determine the machine type. (0x3078d08c)

Explanation
See message.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBI0141E

The response file, *%s*, could not be read. (0x3078d08d)

Explanation
The specified response file could not be read.

Administrator response
Verify the path and permissions of the response file and retry the command.

HPDBI0146E

You must be the root user to run this process. (0x3078d092)

Explanation
See message.

Administrator response
Log in as root and retry the command.

HPDBI0159E

Could not load *%s*. (0x3078d09f)

Explanation
An expected installation file could not be loaded.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDBI0162E

Ezinstall failed to complete successfully. (0x3078d0a2)

Explanation
An error occurred durnig the ezinstall process.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBI0163E

The file, *%s*, could not be read. (0x3078d0a3)

Explanation
See message.

Administrator response
Check the existence and permissions of the file and retry the command.

HPDBI0170E

You must have administrator authority to run this program. (0x3078d0aa)

Explanation
The user does not have authority to run this program.

Administrator response
Log in as the administrative user and retry the command.

HPDBI0175E

The file, *%s*, could not be created. (0x3078d0af)

Explanation
The file could not be created.

Administrator response
Check the permissions of the directory and available disk space, then retry the command.

HPDBI0196E

The current *%s* version is *%s*. *%s* or higher is required. (0x3078d0c4)

Explanation
The process cannot migrate components that are too old.

Administrator response
Use the supported version and retry the command.

HPDBI0215E

The backup or restore of the information failed. (0x3078d0d7)

Explanation
The migration process could not be completed.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBI0217W

Start the *%s* and policy servers if they are not already started. (0x3078d0d9)

Explanation
The servers must be running before continuing.

Administrator response
Start the servers at this time, then continue.

HPDBI0222E

Ezinstall is not supported on this platform. (0x3078d0de)

Explanation
See message.

Administrator response
Move to a supported platform and retry the command.

HPDBI0232E

Solaris version 2.7 or later is required to run the LDAP server. (0x3078d0e8)

Explanation
See message.

Administrator response
Upgrade the operating system and retry the command.

HPDBI0237E

%s could not be removed from the registry. (0x3078d0ed)

Explanation
See message.

Administrator response
Remove the key manually, reboot, and retry the command.

HPDBI0263E

Cannot upgrade the LDAP client. A previous version of the server exists. (0x3078d107)

Explanation
A previous version of the LDAP server exists on this machine.

Administrator response
Upgrade the LDAP server on this machine before continuing.

HPDBI0264E

Upgrade the server first, then retry the command. (0x3078d108)

Explanation
A previous version of the server exists on this machine.

Administrator response
Upgrade the LDAP server on this machine before continuing.

HPDBI0266E

Cannot upgrade Security Verify Access runtime because a previous version of the policy server exists. (0x3078d10a)

Explanation
See message.

Administrator response
Upgrade the policy server then retry the command.

HPDBI0276E

Check that the server is configured properly and running. (0x3078d114)

Explanation
Inform the user that the host name specified was invalid.

Administrator response
Check the host name entered and make sure it is running the software.

HPDBI0283E

The *%s* server did not start properly. (0x3078d11b)

Explanation
A problem prevented the server from starting.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDBI0285E

An error occurred while installing *%s* patches. (0x3078d11d)

Explanation
The patch could not be installed due to an error.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDCF0002E

A memory allocation error resulted in the termination of the program. Check the maximum allowable memory and the amount of system paging space as these may both need to be increased. (0x15e3a002)

Explanation
See message.

Administrator response
Increase the maximum allowable memory and the system paging space or shut down one or more applications.

HPDCF0003E

The file, *%s*, could not be opened. Ensure that file exists and that the file permissions allow access. (0x15e3a003)

Explanation
See message.

Administrator response
Make sure the file exists and that the permissions are set so this process can access it.

HPDCF0004E

The file, *%s*, could not be read. Ensure that file exists and that the file permissions allow read access. (0x15e3a004)

Explanation
See message.

Administrator response
Make sure the file exists and that the permissions are set so this process can access it.

HPDCF0005E

The current time could not be obtained. (0x15e3a005)

Explanation
See message.

Administrator response
Retry the command and if the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDCF0006E

The file, *%s*, could not be modified. Ensure that file exists and that the file permissions allow write access. (0x15e3a006)

Explanation
See message.

Administrator response
Make sure the file exists and that the permissions are set so this process can access it.

HPDCF0009E

The installation directory could not be determined. Ensure that the product is installed correctly. (0x15e3a009)

Explanation
See message.

Administrator response
Reinstall the product.

HPDCF0033E

The file, *%s*, is in use.You must stop the server or application before using this command. (0x15e3a021)

Explanation
An attempt was made to modify the configuration of an active server application.

Administrator response
Stop the server and retry the command.

HPDCF0051E

The file, *%s*, was not found. (0x15e3a033)

Explanation
See message.

Administrator response
Check the path to the file, its permissions, fix the problem then retry the command.

HPDCF0052E

The request to change the key file password failed. (0x15e3a034)

Explanation
An internal error has occurred or access to perform the operation was denied.

Administrator response
Ensure that the administrator ID being used to permorm this cmmand has authority.

HPDCF0053E

The request to renew the server certificate failed. (0x15e3a035)

Explanation
An internal error has occurred or access to perform the operation was denied.

Administrator response
Ensure that the administrator ID being used to permorm this cmmand has authority.

HPDCF0054E

An operating system function for obtaining the local TCP/IP host name has failed. The error code is *%d*. (0x15e3a036)

Explanation
See message text.

Administrator response
Ensure that the TCP/IP host name of the system is properly configured and retry the command.

HPDCF0055E

Socket initialization failed. The error code is *%d*. (0x15e3a037)

Explanation
Unable to initialize a necessary socket communication.

Administrator response
Retry the operation and if the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDCF0057E

A replica entry for the specified host name already exists in the configuration file. (0x15e3a039)

Explanation
An attempt was made to add an authorization server replica that already exists in the specified configuration file.

Administrator response
If the replica name was incorrectly specified, retry the command specifying the correct name.

HPDCF0058E

A replica entry for the specified host name was not found in the configuration file. (0x15e3a03a)

Explanation
An attempt was made to change an authorization server replica that does not exist in the specified configuration file.

Administrator response
Retry the command specifying the correct parameters.

HPDCF0059E

A replica entry in the configuration file is corrupted. (0x15e3a03b)

Explanation
The configuration file contains invalid data.

Administrator response
First unconfigure then reconfigure the server application and then retry the command.

HPDCF0060E

The user registry type cannot be determined. Ensure that Security Verify Access runtime is properly installed and configured. (0x15e3a03c)

Explanation
Unable to determine the registry type.

Administrator response
Reconfigure Security Verify Access runtime.

HPDCF0061E

The function, *%s*, returned the error code: 0x*%8.8lx*. (0x15e3a03d)

Explanation
An internal error has occurred.

Administrator response
Retry the command and if the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDCF0062E

Could not connect to the Security Verify Access policy server. Error code is 0x*%8.8lx*.Ensure that the policy server host name, port and local domain name are correct. (0x15e3a03e)

Explanation
The policy server may not be properly configured or is not started.

Administrator response
Ensure that the policy server is properly configured and started and retry the command.

HPDCF0074E

The keyring database files already exist. This indicates that the server might already be configured or partially configured. (0x15e3a04a)

Explanation
See message.

Administrator response
The server must first be unconfigured before retrying this command.

HPDCF0079E

SSL configuration failed. The error code is 0x*%8.8lx*. (0x15e3a04f)

Explanation
The command failed. This message is preceded by other messages that more fully describe the cause of the failure.

Administrator response
Refer to previous messages that have appeared on the screen for more details. Fix the problem and then retry the command.

HPDCF0084E

File *%s* is missing essential information.You must first use the -config action to create the initial configuration file. (0x15e3a054)

Explanation
See message.

Administrator response
Specify a valid configuration file or use the -config action to create one.

HPDCF0085E

The configuration file *%s* is not valid.Ensure that Security Verify Access runtime is properly configured. (0x15e3a055)

Explanation
See message.

Administrator response
Ensure that the Security Verify Access runtime is properly configured.

HPDCF0086E

The configured user registry type is not supported. (0x15e3a056)

Explanation
See message.

Administrator response
Ensure that the Security Verify Access runtime is properly configured.

HPDCF0101E

Configuration cannot be performed for server *%s*.File *%s* already exists. The server might already be configured. (0x15e3a065)

Explanation
See message.

Administrator response
The server must first be unconfigured before it can be reconfigured.

HPDCF0104W

This usage is deprecated. Refer to the help for the correct usage of this command. (0x15e3a068)

Explanation
A usage error has occurred.

Administrator response
Type the command and action to see the command help.

HPDCF0116E

The keyring database or file, *%s*, could not be modified. Ensure that file exists and that the file permissions allow write access. (0x15e3a074)

Explanation
See message.

Administrator response
Make sure the file exists and that the permissions are set so this process can access it.

HPDCF0117E

An error occurred in the IKeyMan API. Configuration failed. (0x15e3a075)

Explanation
An internal error has occurred.

Administrator response
Retry the command and if the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDCF0118E

Configuration failed. The specified configuration file does not exist or you do not have the proper permissions to access the configuration file. (0x15e3a076)

Explanation
The specified configuration file is invalid.

Administrator response
Ensure that the configuration file exists and that you have the required permissions to write to the file.

HPDCF0120E

An application server with the specified name is already configured. You must use a different name or unconfigure the existing application (0x15e3a078)

Explanation
See message.

Administrator response
The server must first be unconfigured before retrying the command.

HPDCF0122E

If listen mode is enabled, the listening port must be specified with the -r parameter. (0x15e3a07a)

Explanation
A port parameter is required when listening mode is enabled.

Administrator response
Specify the missing port parameter.

HPDCF0123E

The currently configured SSL listening port number cannot be zero if listening mode is enabled. (0x15e3a07b)

Explanation
See message.

Administrator response
Configure a listening port before enabling listening mode or disable listening mode.

HPDCF0126W

The Security Verify Access policy server has been configured to disallow downloading of its CA certificate. A root CA certificate base64 file must be available on the local machine in order to configure. (0x15e3a07e)

Explanation
See message.

Administrator response
Contact your Security Verify Access administrator to obtain the secure domain's root CA certificate. This file was saved as "pdcacert.b64" when the policy server was configured. Retry the command specifying the location of the "pdcacert.b64" file on your local machine.

HPDCF0127E

Download of the root CA certificate failed. Ensure that the Security Verify Access policy server host and port are specified correctly and that the correct version of the policy server is configured and running properly. (0x15e3a07f)

Explanation
Unable to download the root CA certificate file.

Administrator response
Be sure the policy server is configured to allow automatic download of this file and that the specified host and ports are correct.

HPDCF0129W

The value *%s* of ca-cert-download-enabled keyword in ivmgrd.conf file is incorrect. Acceptable values are yes or no. Downloading of the secure domain's root CA certificate is disabled. (0x15e3a081)

Explanation
See message.

Administrator response
If the root CA certifcate downloading is desired, edit the ivmgrd.conf file and correct the ca-cert-download-enabled parameter to "yes" or "no", then restart the policy server.

HPDCF0133E

The Security Verify Access policy server is not responding. Verify the host name and port, and verify that the server is started. (0x15e3a085)

Explanation
See message.

Administrator response
Start the policy server then retry the command, and ensure that the port and host name was entered correctly.

HPDCF0134E

A listening port number of zero is allowed only if the [aznapi-admin-services] stanza in the configuration file is empty. (0x15e3a086)

Explanation
An invalid value was detected in the configuration files.

Administrator response
Either specify a non-zero port number or edit the configuration file to remove the "[aznapi-admin-services]" stanza before retrying the command.

HPDCF0140E

The keyring database could not be located using the specified configuration file. (0x15e3a08c)

Explanation
Either the wrong configuration file was specified, it contains invalid data or the keyring database does not exist.

Administrator response
Ensure that the specified configuration file is correct or unconfigure and reconfigure the application.

HPDCF0157E

The specified configuration file does not exist or you do not have the proper permissions to access the file. (0x15e3a09d)

Explanation
The specified configuration file cannot be opened.

Administrator response
Ensure that the configuration file exists and that you have the required permissions to write to the file.

HPDCF0158E

The specified stanza/key pair does not exist in the specified configuration file. (0x15e3a09e)

Explanation
The specified stanza/key pair is invalid. They do not exist in the given configuration file.

Administrator response
Ensure that the specified stanza/key pair are valid values.

HPDCF0159E

The specified configuration file may be corrupted. (0x15e3a09f)

Explanation
The specified configuration file is invalid.

Administrator response
Ensure that the configuration file is a valid stanza-based file.

HPDCF0160E

Unknown error occurred while reading and writing to the configuration file. (0x15e3a0a0)

Explanation
The specified configuration file is invalid.

Administrator response
Ensure that the configuration file is a valid stanza-based file.

HPDCF0161E

The configuration file is missing essential information. (0x15e3a0a1)

Explanation
The configuration file does not contain information required to perform the command. The configuration file is not valid or the application must be configured.

Administrator response
Specify a valid configuration file or use the -config action to create one.

HPDCF0164E

Configuration failed. An error occurred creating the specified DN, accessing a configuration file, or setting up the keyfile. (0x15e3a0a4)

Explanation
An error occurred in relation to creating the DN.

Administrator response
Ensure that the configuration file exists, that you have the required permissions to write to the file, and that the DN does not already exist.

HPDCF0165E

Cannot display configuration file information from the obfuscated version of the file. (0x15e3a0a5)

Explanation
The specified stanza/key pair cannot be displayed because the pair is in the obfuscated version of the configuration file.

Administrator response
None

HPDCF0166E

Cannot modify information in the specified version of the configuration file because it exists in the alternate version. (0x15e3a0a6)

Explanation
If a stanza/key/value exists in the obfuscated config file then trying to modify it in the non-obfuscated config file is not allowed. The same restriction applies to modifying a stanza/key/value in the non-obfuscated config file, that already exists in the obfuscated config file

Administrator response
Remove the stanza/key/value from the appropriate config file before setting a new value to the alternate config file

HPDCF0170E

Instance '*%s*' is already configured ('*%s*'). (0x15e3a0aa)

Explanation
A configuration file for the instance specified already exists.

Administrator response
Use a different name or remove the existing configuration file and its associated key files.

HPDCF0178E

The compliance entry, ssl-compliance in the ssl stanza, is not set in the Security Verify Access Runtime configuration file pd.conf. (0x15e3a0b2)

Explanation
Under typical configuration conditions, this value is always set in pd.conf. If the value is unset, then ssl-compliance has a default value of 'none'.

Administrator response
Make sure that the ssl-compliance entry is set in pd.conf or reconfigure the Security Verify Access Runtime.

HPDCF0179E

The compliance value '*%s*' is not valid for ssl-compliance in pd.conf. It must be one of the following values: 'none', 'fips', 'sp800-131-transition', 'sp800-131-strict', 'suite-b-128', 'suite-b-192'. (0x15e3a0b3)

Explanation
The pd.conf [ssl] ssl-compliance value is not a valid value.

Administrator response
Correct the value in pd.conf and retry the command.

HPDCF0180E

The -C compliance value '*%s*' is not valid and must be one of the following values: 'none', 'fips', 'sp800-131-transition', 'sp800-131-strict', 'suite-b-128', 'suite-b-192'. (0x15e3a0b4)

Explanation
The -C value is not a valid value.

Administrator response
Retry the command with a valid value.

HPDDB0150E

Not implemented (0x13279096)

Explanation
This message is obsolete.

Administrator response
No action is required.

HPDDB0450W

Could not bind to server (*%s*, 0x*%8.8lx*). (0x132791c2)

Explanation
The application is unable to contact the policy server.

Administrator response
Verify that the policy server host name and port number are configured correctly and that the remote host can be contected directly through the network.

HPDDB0451E

CDS entry for database server does not exist (*%s*). (0x132791c3)

Explanation
Message is obsolete.

Administrator response
No action required.

HPDDB0601E

Could not close backing database (0x*%8.8lx*). (0x13279259)

Explanation
The policy database could not be closed during replication or server shutdown.

Administrator response
Restart the application.

HPDDB0602E

Could not create backing database (*%s*, 0x*%8.8lx*). (0x1327925a)

Explanation
The primary policy database could not be created or initialized.

Administrator response
Verify the policy database pathname configuration and file permissions. Ensure that sufficent disk space is available in the file system.

HPDDB0603E

Could not fetch object from backing database (*%s*, 0x*%8.8lx*). (0x1327925b)

Explanation
The policy server is unable to retrieve an item from the policy database.

Administrator response
No action is required.

HPDDB0604E

Could not write object to backing database (*%s*, 0x*%8.8lx*). (0x1327925c)

Explanation
The policy server is unable to update the policy database.

Administrator response
Ensure that sufficient disk space is available in the file system. If a server restart does not resolve the problem, use the pdacld_dump utility to verify the policy database. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDDB0605E

Could not delete object from backing database (*%s*, 0x*%8.8lx*). (0x1327925d)

Explanation
The policy server is unable to update the policy database.

Administrator response
Ensure that sufficient disk space is available in the file system. If a server restart does not resolve the problem, use the pdacld_dump utility to verify the policy database. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDDB0606E

Could not initialize database iterator (0x*%8.8lx*). (0x1327925e)

Explanation
The policy server is unable to retrieve an item from the policy database.

Administrator response
Use the pdacld_dump utility to verify that the policy database can be read. Compare the number of objects read with the expected number of objects. If these numbers differ, use the pdacld_dump utility to rebuild the policy database. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDDB0607E

Could not fetch next database element (0x*%8.8lx*). (0x1327925f)

Explanation
The policy server is unable to retrieve an item from the policy database.

Administrator response
Use the pdacld_dump utility to verify that the policy database can be read. Compare the number of objects read with the expected number of objects. If these numbers differ, use the pdacld_dump utility to rebuild the policy database. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDDB0608E

Could not build initial database replica (*%s*, 0x*%8.8lx*). (0x13279260)

Explanation
A policy database replication operation has failed and a replica policy database is unavailable.

Administrator response
If a policy replica exists, move it to a temporary location. Try an application restart. If the problem persists, check Electronic Support for additional information - https://www.ibm.com/mysupport

HPDDB0609E

Could not rebuild database replica (*%s*, 0x*%8.8lx*). (0x13279261)

Explanation
A policy database replication operation has failed.

Administrator response
If a policy replica exists, move it to a temporary location. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDDB0611E

Invalid database specified for replication. (0x13279263)

Explanation
The policy server is unable to provide replication services.

Administrator response
Restart the policy server. If this problem persists, check Electronic Support for additional information - https://www.ibm.com/mysupport

HPDDB0612E

Replica database version is incompatible and will be replaced. (0x13279264)

Explanation
The application has detected an incompatible version of the policy database. The database is replaced automatically.

Administrator response
No action is required.

HPDDB0750E

Invalid object name (*%s*). (0x132792ee)

Explanation
Message is obsolete.

Administrator response
No action is required.

HPDDB0751E

Could not decode object (*%ld*, 0x*%8.8x*). (0x132792ef)

Explanation
An error occurred interpreting an item from the policy database.

Administrator response
Run the pdacld_dump utility to verify the database integrity and if necessary, rebuild the policy database.

HPDDB0752E

Could not encode object (*%ld*, 0x*%8.8x*). (0x132792f0)

Explanation
An error occurred while storing an item to the policy database.

Administrator response
Restart the policy server and run the pdacld_dump utility to verify the database integrity.

HPDDB0753E

Could not find object (*%s*). (0x132792f1)

Explanation
The policy server is unable to retrieve an item from the policy database.

Administrator response
No action is required.

HPDDB0754E

Object type is unknown. (0x132792f2)

Explanation
Message is obsolete.

Administrator response
No action is required.

HPDDB0755E

Unexpected object type. (0x132792f3)

Explanation
Message is obsolete.

Administrator response
No action is required.

HPDDB0756E

The policy database is not ready for use. (0x132792f4)

Explanation
An internal error has occurred which prevents the application from retrieving records from security policy database.

Administrator response
If a server restart does not resolve the problem, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDDB0901E

Could not bind to client for notification (*%s*, 0x*%8.8lx*). (0x13279385)

Explanation
The policy server was unable to contact the client for a policy database update notification.

Administrator response
Ensure that the application is available to receive notifications.

HPDDB0906E

Client not found. (0x1327938a)

Explanation
An attempt was made to retrieve information about an unknown client.

Administrator response
No action is required.

HPDDB0907E

Client already exists. (0x1327938b)

Explanation
An attempt was made to add a client which already exists.

Administrator response
No action is required.

HPDDB1050E

Could not download object (*%s*, 0x*%8.8lx*). (0x1327941a)

Explanation
Message is obsolete.

Administrator response
No action is required.

HPDDB1051E

Remote update detected - aborting download. (0x1327941b)

Explanation
The application received multiple policy update notifications. The secondary notifications are discarded.

Administrator response
No action is required.

HPDDB1052E

Could not read database header (0x*%8.8lx*). (0x1327941c)

Explanation
The policy database could not be opened and initialized.

Administrator response
The database file might have incorrect permissions br truncated or corrupted. Verify that policy database file permissions are valid. Also, ensure that sufficient disk space is available in the file system and restart the application. For local-mode applications, if the problem persists, recreate the replica by moving the database to a temporary location and restarting the application. For the policy server, restore a backup database or use the pdacld_dump utility to salvage the existing database.

HPDDB1053E

Could not write database header (0x*%8.8lx*). (0x1327941d)

Explanation
The primary policy database could not be created or initialized.

Administrator response
Verify the policy database pathname configuration and file permissions. Ensure that sufficent disk space is available in the file system.

HPDDB1054W

Master database server is unavailable (0x*%8.8lx*). (0x1327941e)

Explanation
The application is unable to contact the policy server.

Administrator response
Verify that the policy server host name and port number are configured correctly and that the remote host can be contected directly through the network.

HPDDB1060W

Could not check synchronization with master database server - using local replica instead. (0x13279424)

Explanation
A new policy database could not be downloaded. The existing database is used.

Administrator response
No action is required.

HPDDB1061E

Critical failure during DB replication - aborting (0x*%8.8lx*). (0x13279425)

Explanation
The application is unable to create a policy database replica. The application aborts.

Administrator response
If a policy replica exists, move it to a temporary location. Ensure that the files system has sufficent disk space and that file and directory permissions are correct. Try an application restart. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDDB1062W

Could not rebuild local replica - continuing to use existing replica (0x*%8.8lx*). (0x13279426)

Explanation
The application is not able to update the existing policy database. The existing database is used.

Administrator response
Ensure that the file system has sufficent disk space. If this problem persists, restart the policy server.

HPDDL0001E

Database not open. (0x14601001)

Explanation
The database was not opened before this database call.

Administrator response
Call pd_db_open before this database procedure.

HPDDL0002E

Database filename missing. (0x14601002)

Explanation
The database filename was not supplied when trying to open the database with pd_db_open.

Administrator response
Call pd_db_open with a valid database filename.

HPDDL0004E

The data type is not known or is incorrectly specified. (0x14601004)

Explanation
An attempt was made to create a database without specifying an index type or to open an existing database with an incorrect type.

Administrator response
When creating a new database, the data_type (pd_db_type_t) parameter must be either pd_db_type_ivobj or pd_db_type_encoded. When opening an existing database, the data type must match the type used when the database was first created.

HPDDL0005E

The data type (pd_db_type_t) in the flags parameter does not match the type in the database. (0x14601005)

Explanation
The data type parameter to pd_db_open did not match the type stored in the database.

Administrator response
Call pd_db_open with the data type that matches the database data type.

HPDDL0009E

Database create failure - data file already exists. (0x14601009)

Explanation
When attempting to open a database with the PD_DB_CREATE flag the specified database file was found to already exist.

Administrator response
Do not open an existing database with the PD_DB_CREATE flag, Or, you can remove the database file if a new (and empty) database is desired.

HPDDL0011E

Database open failure - permission denied (0x1460100b)

Explanation
The server does not have permission to open the database file. The open call returned EACCES.

Administrator response
Run the process as the operating system user who has permission to access the database, or change the permission of the database file itself or the path to it.

HPDDL0012E

Database open failure. (0x1460100c)

Explanation
The database-open procedure has failed.

Administrator response
Examine the global variable, errno, for further information. Database open failures can also occur if codepage conversion tables are not accessible or could not be initialized.

HPDDL0013E

Database store failure. (0x1460100d)

Explanation
The database-store procedure has failed.

Administrator response
Examine the global variable, errno, for further information.

HPDDL0014E

Database fetch failure. (0x1460100e)

Explanation
The database-fetch procedure has failed.

Administrator response
Examine the global variable, errno, for further information.

HPDDL0015E

Database delete operation failure. (0x1460100f)

Explanation
The database-delete procedure has failed.

Administrator response
Examine the global variable, errno, for further information.

HPDDL0017E

This database does not contain a valid header. (0x14601011)

Explanation
An attempt to fetch the database header failed. The database might be truncated or otherwise corrupted.

Administrator response
Use the pdacld_dump utility to validate and if necessary, repair the database.

HPDDL0023E

The operation is not allowed while iterating. (0x14601017)

Explanation
A call to either a function that alters a backing store (a store or delete operation) or one that starts another iteration was attempted while iterating. This is not allowed.

Administrator response
Do not call routines that alter the backing store or nest iterations while in an iteration loop.

HPDED0100E

Invalid argument: Null context. (0x306e3064)

Explanation
A nonnull PDContext object is required to communicate with the Security Verify Access policy server.

Administrator response
Ensure that the context argument is nonnull.

HPDED0101E

Unknown message code: *%s*. (0x306e3065)

Explanation
The text for the message code could not be found in the message catalogs installed on the local system. This typically means that the policy server is at a more recent level than the client and has returned a code undefined in the client runtime. The documentation associated with the policy server installation should include the message code.

Administrator response
Consult the Error Message Reference to obtain the message text, explanation, and suggested actions for the message code.

HPDED0102E

The specified configuration or keystore file already exists. (0x306e3066)

Explanation
The 'create' configuration action is designed to check for existing files and fail if they are found in order not to overwrite them accidentally.

Administrator response
To preserve existing files, specify new configuration and keystore file names. To overwrite existing files, specify the 'replace' configuration action.

HPDED0200E

Invalid argument: Null context. (0x306e30c8)

Explanation
A nonnull PDContext object is required to communicate with the Security Verify Access policy server.

Administrator response
Ensure that the context argument is nonnull.

HPDED0201E

The AmIdentity does not contain a valid name. (0x306e30c9)

Explanation
The AmIdentity does not contain a valid name.

Administrator response
Refer to the Security Verify Access error log for more information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDED0202E

The AmObject cannot be created from the encoded object. (0x306e30ca)

Explanation
The AmObject cannot be created from the encoded object.

Administrator response
Refer to the Security Verify Access error log for more information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDED0203E

The object type requested is unexpected. (0x306e30cb)

Explanation
The object type requested is unexpected. The object cannot be decoded.

Administrator response
Refer to the Security Verify Access error log for more information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDED0204E

The configuration information cannot be stored to file. (0x306e30cc)

Explanation
The configuration information cannot be stored to file.

Administrator response
Ensure that the configuration file is writable.

HPDED0205E

The temporary database file *%s* cannot be written. (0x306e30cd)

Explanation
The temporary database file cannot be written.

Administrator response
Refer to the Security Verify Access error log for more information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDED0206E

Could not get socket input stream. (0x306e30ce)

Explanation
Could not get socket input stream.

Administrator response
Refer to the Security Verify Access error log for more information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDED0207E

Could not read data from data input stream or socket. (0x306e30cf)

Explanation
Could not read data from data input stream or socket.

Administrator response
Refer to the Security Verify Access error log for more information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDED0208E

Could not write data to data output stream or socket. (0x306e30d0)

Explanation
Could not write data to data output stream or socket.

Administrator response
Refer to the Security Verify Access error log for more information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDED0209E

An error occurred while creating database sequence property file. (0x306e30d1)

Explanation
Unable to create database sequence property file in PolicyDirector/db directory of the AM_INSTALL_DIR.

Administrator response
Ensure that the user has the necessary permissions to create file in the <AM_INSTALL_DIR>/PolicyDirector/db directory.

HPDED0210E

An error occurred while loading database sequence property file. (0x306e30d2)

Explanation
Unable to load database sequence property file in PolicyDirector/db directory of the AM_INSTALL_DIR.

Administrator response
Ensure that the user has the necessary permissions to read/write database sequence property file in the <AM_INSTALL_DIR>/PolicyDirector /db directory.

HPDED0211E

The database sequence information cannot be stored to file. (0x306e30d3)

Explanation
The database sequence information cannot be stored to file.

Administrator response
Ensure that the user has the necessary permissions to read/write database sequence property file in the <AM_INSTALL_DIR>/PolicyDirector /db directory.

HPDED0300E

Invalid argument: Null context. (0x306e312c)

Explanation
A nonnull PDContext object is required to communicate with the Security Verify Access policy server.

Administrator response
Ensure that the context argument is nonnull.

HPDED0400E

Invalid argument: Too many properties. (0x306e3190)

Explanation
The database filename configured for the application is not specified correctly in the configuration file.

Administrator response
Ensure that the keyword/value for 'filename=<db pathname>' is correctly specified in the configuration file.

HPDED0401E

Invalid argument: Filename property not found. (0x306e3191)

Explanation
The database filename configured for the application is not specified correctly in the configuration file.

Administrator response
Ensure that the keyword/value for 'filename=<db pathname>' is correctly specified in the configuration file.

HPDED0402E

Invalid argument: Filename not supplied. (0x306e3192)

Explanation
The database filename configured for the application is not specified correctly in the configuration file.

Administrator response
Ensure that the keyword/value for 'filename=<db pathname>' is correctly specified in the configuration file.

HPDED0403E

Invalid state: Could not open database. (0x306e3193)

Explanation
The database file specified in the configuration file could not be opened.

Administrator response
Ensure that the keyword/value for 'filename=<db pathname>' is correctly specified in the configuration file.

HPDED0404E

Invalid state: Expected *%d*, but got *%d* from database. (0x306e3194)

Explanation
An internal error occurred. The database may have been corrupted.

Administrator response
Refer to the Security Verify Access error log for more information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDED0405E

The version of the local replicated database is downlevel and not supported. (0x306e3195)

Explanation
See text.

Administrator response
Ensure the versions of the local Security Verify Access runtime environment and policy server are supported. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDED0406E

A database object cache store operation failed. (0x306e3196)

Explanation
An error occurred while attempting to retrieve an entry from the database object cache.

Administrator response
Refer to the Security Verify Access error log for more information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDED0407E

A database object cache retrieve operation failed. (0x306e3197)

Explanation
An error occurred while attempting to write an entry to the database object cache.

Administrator response
Refer to the Security Verify Access error log for more information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDED0408E

A database file read operation failed. (0x306e3198)

Explanation
An error occurred while attempting to read the database file. The database could be corrupted.

Administrator response
Refer to the Security Verify Access error log for more information. Ensure the Security Verify Access is up and running and the application is properly configured. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDED0409E

The database file was not found. (0x306e3199)

Explanation
The database file was not found in the location specified by the configuration file.

Administrator response
Ensure the Security Verify Access is up and running and the application is properly configured.

HPDED0410E

Could not read policy database header. (0x306e319a)

Explanation
The policy database header information could not be read. The database could be corrupted or have incorrect permissions.

Administrator response
Verify that the policy database file permissions are valid. Also, ensure that sufficient disk space is available in the file system and restart the application. For local-mode applications, if the problem persists, recreate the replica by moving the database to a temporary location and restarting the application.

HPDED0411E

Invalid state: Policy retrieval error. (0x306e319b)

Explanation
An unexpected error occurred while retrieving policy data from the database. The database could be currupted.

Administrator response
Ensure the Security Verify Access is up and running and the application is properly configured. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDED0412E

Startup failure: Local policy database unavailable. (0x306e319c)

Explanation
An error occurred while attempting to retrieve the policy database from the Security Verify Access policy server at application statup. A subsequent attempt to start the application with a valid local copy of the database also failed.

Administrator response
Ensure both the Security Verify Access and the user registry server are up and running, and the application is properly configured.

HPDIA0100E

An internal error has occurred. (0x13212064)

Explanation
The authentication switch encountered an unexpected internal error.

Administrator response
Retry the operation. If the problem persists contact your IBM service representative.

HPDIA0101E

An unexpected error code was encountered. (0x13212065)

Explanation
The authentication switch encountered an unexpected error code.

Administrator response
Retry the failing operation. If the problem persists, contact your IBM service representative.

HPDIA0102E

Unable to open shared library. (0x13212066)

Explanation
An attempt to open a shared library failed.

Administrator response
Make sure that the path to the shared library is correct, or if the full path is not specified make sure that the library is present in /usr/lib on UNIX systems or is in the path on Windows systems.

HPDIA0103E

Unable to locate symbol in shared library. (0x13212067)

Explanation
An attempt to retrieve a symbol from a shared library failed. The most probable reason for the error is that the library was built incorrectly.

Administrator response
If the failing library is supplied as part of Security Verify Access, retry the operation. If the problem persists, contact your IBM service representative.

HPDIA0104E

The authentication mechanism is incorrectly specified. (0x13212068)

Explanation
The authentication mechanism is not specified or invalid in the .conf configuration file.

Administrator response
Make sure the correct authentication mechanism is specified in the [authentication-mechanisms] stanza of the .conf configuration file.

HPDIA0105W

Invalid authentication method. (0x13212069)

Explanation
The specified authentication method is either invalid or unsupported in the current product configuration.

Administrator response
Verify the validity of the specified authentication method.

HPDIA0110E

An authentication mechanism module specific error occurred. (0x1321206e)

Explanation
A configured authentication mechanism module generated an unexpected error.

Administrator response
If the failing authentication mechanism module is supplied as part of Security Verify Access, retry the operation. If the problem persists, contact your IBM service representative.

HPDIA0111E

A memory allocation call failed. (0x1321206f)

Explanation
In most cases this error due to the application program running out of memory.

Administrator response
Ensure that the application has been configured with sufficient virtual memory for its requirements. The Security Verify Access Performance Tuning Guide contains instructions on how to ensure that the application is configured with the correct a mount of virtual memory. Stop and restart the process. If the problem persists then contact your IBM service representative.

HPDIA0112E

The current authentication module operation terminated due to an exception. (0x13212070)

Explanation
See message.

Administrator response
Retry the failing operation. If the problem persists, contact your IBM service representative.

HPDIA0113E

Could not acquire a client credential. Major status = 0x*%8.8lx*, minor status = 0x*%8.8lx* (0x13212071)

Explanation
A request to create a client credential was denied by the Security Verify Access Authorization API.

Administrator response
Retry the failing operation. If the problem persists, contact your IBM service representative.

HPDIA0114E

Could not acquire a client credential. (0x13212072)

Explanation
A request to create a client credential was denied by the Security Verify Access Authorization API.

Administrator response
Retry the failing operation. If the problem persists, contact your IBM service representative.

HPDIA0115E

Unknown identity type. (0x13212073)

Explanation
Unrecognized identity information returned from an authentication mechanism module.

Administrator response
Check the identity information returned from the module and, if the failing authentication mechanism module is supplied as part of Security Verify Access, retry the failing operation. If the problem persists, contact your IBM service representative.

HPDIA0116E

Can't load extended attributes into the client credential. (0x13212074)

Explanation
Security Verify Access was unable to annotate the client credentials with extended attributes returned from an authentication mechanism module.

Administrator response
Retry the failing operation. If the problem persists, contact your IBM service representative.

HPDIA0117E

Can't select authentication mechanism. (0x13212075)

Explanation
Security Verify Access was unable to authenticate a client because no suitable authentication mechanisms are configured.

Administrator response
Make sure the correct authentication mechanism is configured in the [authentication-mechanisms] stanza of the .conf configuration file.

HPDIA0118W

Authentication method is not supported. (0x13212076)

Explanation
Security Verify Access was unable to authenticate a client because the authentication method employed is not supported.

Administrator response
Use a different authentication method.

HPDIA0119W

Authentication mechanism is not available. (0x13212077)

Explanation
Security Verify Access was unable to authenticate a client because the authentication mechanism is currently out of service.

Administrator response
Make sure the registry server (LDAP server,or DOMINO server, or other type of registry server) is up running.

HPDIA0120W

Not authorized to perform the current operation. (0x13212078)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDIA0121W

The requested operation is not valid. (0x13212079)

Explanation
Security Verify Access was unable to perform a requested operation because it is not valid. An example would be a token authentication user attempting to change their password

Administrator response
Consult documentation for operation.

HPDIA0122E

Unable to open shared library *%s*: *%s*. (0x1321207a)

Explanation
An attempt to open a shared library failed.

Administrator response
Examine the reason given in the error message, and attempt to correct the problem. Make sure that the path to the shared library is correct, or if the full path is not specified make sure that the library is present in /usr/lib on UNIX systems or is in the path on Windows systems.

HPDIA0123E

Unable to locate symbol *%s* in shared library *%s*: *%s*. (0x1321207b)

Explanation
An attempt to retrieve a symbol from a shared library failed, probably because the symbol was not found. The most probable reason for the error is that the library was built incorrectly.

Administrator response
If the failing library is supplied as part of Security Verify Access, retry the operation. If the problem persists, contact your IBM service representative.

HPDIA0125W

Authentication method (*%s*) is not supported. (0x1321207d)

Explanation
Security Verify Access was unable to authenticate a client because the authentication method employed is not supported.

Administrator response
Use a different authentication method.

HPDIA0126W

Authentication method (*%s*) is not configured. (0x1321207e)

Explanation
Security Verify Access was unable to authenticate a client because the authentication method employed is not configured.

Administrator response
Make sure the employed authentication method is configured in the [authentication-mechanisms] stanza of the .conf configuration file.

HPDIA0127W

User *%s* is not authorized to perform the current operation. (0x1321207f)

Explanation
See message.

Administrator response
An authorization decision result. No action is required.

HPDIA0128W

The requested operation by user *%s* is not valid. (0x13212080)

Explanation
Security Verify Access was unable to perform a requested operation because it is not valid. An example would be a token authentication user attempting to change their password

Administrator response
Consult documentation for operation.

HPDIA0129E

An error occurred processing the EAI external user list of groups. (0x13212081)

Explanation
This error is returned when processing the group or list of groups for an EAI external user.

Administrator response
Examine log files for additional information. Make sure the group or list of groups returned by the EAI are valid Verify Access groups.

HPDIA0200W

Authentication failed. You have used an invalid user name, password or client certificate. (0x132120c8)

Explanation
See message.

Administrator response
Check your authentication information and try again.

HPDIA0201W

The client supplied invalid authentication information. (0x132120c9)

Explanation
Invalid authentication information was presented to Security Verify Access.

Administrator response
Check the format of the authentication information and try again.

HPDIA0202W

An unknown user name was presented to Security Verify Access. (0x132120ca)

Explanation
Security Verify Access could not locate the supplied user name in the authentication registry.

Administrator response
Check the supplied user name information and try again.

HPDIA0203W

Authentication retry limit reached. (0x132120cb)

Explanation
The user has performed too many consecutive invalid authentication attempts.

Administrator response
Contact your Security Verify Access administrator.

HPDIA0204W

The user's password has expired. (0x132120cc)

Explanation
See message.

Administrator response
Contact your Security Verify Access administrator, and change your password.

HPDIA0205W

The user's account has expired. (0x132120cd)

Explanation
See message.

Administrator response
Contact your Security Verify Access administrator.

HPDIA0206W

Login rejected due to policy violation. (0x132120ce)

Explanation
Login rejected due to policy enforced for the account.

Administrator response
Contact your Security Verify Access network administrator.

HPDIA0207W

A PIN must be assigned to enable account (0x132120cf)

Explanation
A PIN must be assigned to enable account

Administrator response
Contact system administrator to assign new PIN

HPDIA0208W

User's account has been disabled. (0x132120d0)

Explanation
See message.

Administrator response
Contact your Security Verify Access administrator.

HPDIA0209W

Next token required for authentication (0x132120d1)

Explanation
Next token required for authentication

Administrator response
Enter next token

HPDIA0210W

The login data entered could not be mapped to an Security Verify Access user (0x132120d2)

Explanation
A mapping function, such as that in a library or CDAS, failed to map the login information to a Security Verify Access user.

Administrator response
Check the login data, registry, or mapping function.

HPDIA0211W

A client certificate could not be authenticated. (0x132120d3)

Explanation
A client certificate could not be authenticated.

Administrator response
Check the client certificate

HPDIA0212W

The data contained in the HTTP header *%s* failed authentication. (0x132120d4)

Explanation
The request an HTTP header that Security Verify Access was configured to use as authentication data. This data failed authentication.

Administrator response
Check the request, the proxy server (if one is used), and the mapping library

HPDIA0214W

IP address based authentication failed (0x132120d6)

Explanation
Security Verify Access is configured to authenticate using the client IP address, which was either unavailable or invalid

Administrator response
Check Security Verify Access configuration and/or authentication library

HPDIA0215E

The supplied username does not exist in the registry. (0x132120d7)

Explanation
The administrator attempting to SU entered a username which does not exist in the registry.

Administrator response
Verify that username exists in user registry.

HPDIA0216E

Administrator does not have permission to su to this account. (0x132120d8)

Explanation
The administrator attempted to SU to a privileged user, and the authentication mechanism did not allow them to do so.

Administrator response
Make sure that the administrator has the permissions needed to switch username to the desired account.

HPDIA0217W

Authentication by user *%s* denied at this time of day. (0x132120d9)

Explanation
A user attempted to authenticate during a time of day when his/her account is restricted.

Administrator response
Contact your Security Verify Access administrator to validate or change the time of day for which this user is allowed to authenticate.

HPDIA0218W

Authentication by user denied at this time of day. (0x132120da)

Explanation
A user attempted to authenticate during a time of day when his/her account is restricted.

Administrator response
Contact your Security Verify Access administrator to validate or change the time of day for which this user is allowed to authenticate.

HPDIA0219W

An unknown user, *%s*, was presented to Security Verify Access. (0x132120db)

Explanation
Security Verify Access could not locate the user name in the authentication registry.

Administrator response
Check the supplied user name information and try again.

HPDIA0221W

Authentication for user *%s* failed. You have used an invalid user name, password or client certificate. (0x132120dd)

Explanation
See message.

Administrator response
Check your authentication information and try again.

HPDIA0222W

The client, *%s*, supplied invalid authentication information. (0x132120de)

Explanation
Invalid authentication information was presented to Security Verify Access.

Administrator response
Check the format of the authentication information and try again.

HPDIA0223W

The authentication retry limit for user *%s* was reached. (0x132120df)

Explanation
The user has performed too many consecutive invalid authentication attempts.

Administrator response
Contact your Security Verify Access administrator.

HPDIA0224W

The password for user *%s* has expired. (0x132120e0)

Explanation
See message.

Administrator response
Contact your Security Verify Access administrator, and change your password.

HPDIA0225W

The account for user *%s* has expired. (0x132120e1)

Explanation
See message.

Administrator response
Contact your Security Verify Access administrator.

HPDIA0226W

The login for user *%s* was rejected due to a policy violation. (0x132120e2)

Explanation
Login rejected due to policy enforced for the account.

Administrator response
Contact your Security Verify Access network administrator.

HPDIA0227W

The account for user *%s* has been disabled. (0x132120e3)

Explanation
See message.

Administrator response
Contact your Security Verify Access administrator.

HPDIA0228W

A client certificate for user %s could not be authenticated. (0x132120e4)

Explanation
See message.

Administrator response
Check the client certificate

HPDIA0229W

IP address authentication failed for address %s. (0x132120e5)

Explanation
Security Verify Access is configured to authenticate using the client IP address, which was either unavailable or invalid

Administrator response
Check Security Verify Access configuration, or authentication library

HPDIA0230E

The supplied username %s does not exist in the registry. (0x132120e6)

Explanation
The administrator attempting to use the switch username command and entered a username that does not exist in the registry.

Administrator response
Verify that username exists in user registry.

HPDIA0231E

Administrator %s does not have permission to use switch username on this account. (0x132120e7)

Explanation
The administrator attempted to SU to a privileged user, and the authentication mechanism did not allow them to do so.

Administrator response
Make sure that the administrator has the permissions needed to switch username to the desired account.

HPDIA0232W

The data contained in the HTTP header failed authentication. (0x132120e8)

Explanation
The request an HTTP header that Security Verify Access was configured to use as authentication data. This data failed authentication.

Administrator response
Check the request, the proxy server (if one is used), and the mapping library

HPDIA0233W

Authentication failed. You have used an invalid password. This account has been temporarily locked due to too many failed login attempts. (0x132120e9)

Explanation

The Security Verify Access administrator has set a disable-time-interval to lock this account when the maximum number of login failures is exceeded.

Administrator response

Check your password and wait until disable-time-interval has elapsed, or contact your Security Verify Access administrator to unlock and enable login to the account.

HPDIA0234W

Authentication failed. You have used an invalid password. This account has been disabled due to too many failed login attempts. (0x132120ea)

Explanation

The Security Verify Access administrator has set a disable-time-interval to disable this account when the maximum number of login failures is exceeded.

Administrator response

Check your password and contact your Security Verify Access administrator to enable this account.

HPDIA0235W

Authentication for user *%s* failed. You have used an invalid password. This account has been temporarily locked due to too many failed login attempts. (0x132120eb)

Explanation

The Security Verify Access administrator has set a disable-time-interval to lock this account when the maximum number of login failures is exceeded.

Administrator response

Check your password and wait until disable-time-interval has elapsed, or contact your Security Verify Access administrator to unlock and enable login to the account.

HPDIA0236W

Authentication for user *%s* failed. You have used an invalid password. This account has been disabled due to too many failed login attempts. (0x132120ec)

Explanation

The Security Verify Access administrator has set a disable-time-interval to disable this account when the maximum number of login failures is exceeded.

Administrator response

Check your password and contact your Security Verify Access administrator to enable this account.

HPDIA0237W

Authentication failed. The account could not be logged into as the password has expired. (0x132120ed)

Explanation
The LDAP registry failed the authentication and reported that the password has expired.

Administrator response
Contact the administrator for the LDAP registry to reset the password.

HPDIA0238W

Authentication for user *%s* failed. The account could not be logged into as the password has expired. (0x132120ee)

Explanation
The LDAP registry failed the authentication and reported that the password has expired.

Administrator response
Contact the administrator for the LDAP registry to reset the password.

HPDIA0239W

Authentication failed. The account is locked. (0x132120ef)

Explanation
The LDAP registry failed the authentication and reported that the account is locked.

Administrator response
Contact the administrator for the LDAP registry to reset the account.

HPDIA0240W

Authentication for user *%s* failed. The account is locked. (0x132120f0)

Explanation
The LDAP registry failed the authentication and reported that the account is locked.

Administrator response
Contact the administrator for the LDAP registry to reset the account.

HPDIA0241W

Authentication failed. The account is deactivated. (0x132120f1)

Explanation
The LDAP registry failed the authentication and reported that the account is deactivated.

Administrator response
Contact the administrator for the LDAP registry to activate the account.

HPDIA0242W

Authentication for user %s failed. The account is deactivated. (0x132120f2)

Explanation
The LDAP registry failed the authentication and reported that the account is deactivated.

Administrator response
Contact the administrator for the LDAP registry to activate the account.

HPDIA0300W

Password rejected due to policy violation. (0x1321212c)

Explanation
A password violates the rules for valid passwords set in a policy for the account.

Administrator response
Contact your Security Verify Access administrator for a list of password policies.

HPDIA0301W

Password rejected due to minimum length policy. (0x1321212d)

Explanation
A password does not meet the minimum length requirement set in a policy for the account.

Administrator response
Contact your Security Verify Access administrator for a list of password policies.

HPDIA0302W

Password rejected due to the spaces policy. (0x1321212e)

Explanation
A password does not meet the spaces requirement set in a policy for the account.

Administrator response
Contact your Security Verify Access administrator for a list of password policies.

HPDIA0303W

Password rejected due to the maximum repeated characters policy. (0x1321212f)

Explanation
A password does not meet the maximum repeated characters requirement set in a policy for the account.

Administrator response
Contact your Security Verify Access administrator for a list of password policies.

HPDIA0304W

Password rejected due to the minimum alphabetic characters policy. (0x13212130)

Explanation
A password does not meet the minimum alphabetic characters requirement set in a policy for the account.

Administrator response
Contact your Security Verify Access administrator for a list of password policies.

HPDIA0305W

Password rejected due to the minimum non-alphabetic characters policy. (0x13212131)

Explanation
A password does not meet the minimum non-alphabetic characters requirement set in a policy for the account.

Administrator response
Contact your Security Verify Access administrator for a list of password policies.

HPDIA0306W

This account has been temporarily locked out due to too many failed login attempts. (0x13212132)

Explanation
The Security Verify Access administrator has set a disable-time-interval to disable this account when the maximum number of login failures is exceeded.

Administrator response
Wait until disable-time-interval has elapsed, or contact your Security Verify Access administrator to unlock and enable login to the account.

HPDIA0307W

Post password change processing for user *%s* failed. (0x13212133)

Explanation
A configured post password change processing module returned a failure status.

Administrator response
Check the post password change processing module's log file.

HPDIA0309W

This account is disabled. (0x13212135)

Explanation
This account is disabled in the user registry. Logins will not succeed until the account is enabled.

Administrator response
Contact your Security Verify Access administrator to enable this account.

HPDIA0310W

The password for user *%s* was rejected due to policy violation. (0x13212136)

Explanation
A password violates the rules for valid passwords set in a policy for the account.

Administrator response
Contact your Security Verify Access administrator for a list of password policies.

HPDIA0311W

The password for user *%s* was rejected due to minimum length policy. (0x13212137)

Explanation
A password does not meet the minimum length requirement set in a policy for the account.

Administrator response
Contact your Security Verify Access administrator for a list of password policies.

HPDIA0312W

The password for user *%s* was rejected due to the spaces policy. (0x13212138)

Explanation
The password does not meet the spaces requirement set in a policy for the account.

Administrator response
Contact your Security Verify Access administrator for a list of password policies.

HPDIA0313W

The password for user *%s* was rejected due to the maximum repeated characters policy. (0x13212139)

Explanation
A password does not meet the maximum repeated characters requirement set in a policy for the account.

Administrator response
Contact your Security Verify Access administrator for a list of password policies.

HPDIA0314W

The password for user *%s* was rejected due to the minimum alphabetic characters policy. (0x1321213a)

Explanation
A password does not meet the minimum alphabetic characters requirement set in a policy for the account.

Administrator response
Contact your Security Verify Access administrator for a list of password policies.

HPDIA0315W

The password for user *%s* was rejected due to the minimum non-alphabetic characters policy. (0x1321213b)

Explanation
A password does not meet the minimum non-alphabetic characters requirement set in a policy for the account.

Administrator response
Contact your Security Verify Access administrator for a list of password policies.

HPDIA0316W

The account for user *%s* has been temporarily locked due to too many failed login attempts. (0x1321213c)

Explanation
The Security Verify Access administrator has set a disable-time-interval to disable this account when the maximum number of login failures is exceeded.

Administrator response
Wait until disable-time-interval has elapsed, or contact your Security Verify Access administrator to unlock and enable login to the account.

HPDIA0317W

The account for user *%s* is disabled. (0x1321213d)

Explanation
This account is disabled in the user registry. Logins will not succeed until the account is enabled.

Administrator response
Contact your Security Verify Access administrator to enable this account.

HPDIA0318W

The user does not have permission to modify their password. (0x1321213e)

Explanation
The LDAP registry rejected the password change as the user does not have permission.

Administrator response
Contact the administrator for the LDAP registry to gain access.

HPDIA0319W

The user *%s* does not have permission to modify their password. (0x1321213f)

Explanation
The LDAP registry rejected the password change as the user does not have permission.

Administrator response
Contact the administrator for the LDAP registry to gain access.

HPDIA0320W

The user is not permitted to change their password this early after the prior change. (0x13212140)

Explanation
The LDAP registry rejected the password change as it reported that the password can not be changed this early after a prior change.

Administrator response
Avoid changing the password, or contact the administrator for the LDAP registry to reset the password.

HPDIA0321W

The user *%s* is not permitted to change their password this early after the prior change. (0x13212141)

Explanation
The LDAP registry rejected the password change as it reported that the password can not be changed this early after a prior change.

Administrator response
Avoid changing the password, or contact the administrator for the LDAP registry to reset the password.

HPDIA0322W

The user is not permitted to use the new password as it has already been used recently. (0x13212142)

Explanation
The LDAP registry rejected the password change as it reported that the password has already been used by the user and cannot be reused.

Administrator response
Choose a new password that has not been used with the account before.

HPDIA0323W

The user *%s* is not permitted to use the new password as it has already been used recently. (0x13212143)

Explanation
The LDAP registry rejected the password change as it reported that the password has already been used by the user and cannot be reused.

Administrator response
Choose a new password that has not been used with the account before.

HPDIA0500W

Authentication failure (error status 0x%x). (0x132121f4)

Explanation
An error occurred that was outside the bounds of expected authentication errors.

Administrator response
Contact your IBM service representative with the given error status.

HPDIA0501E

Authentication failed for user %s (error status 0x%x). (0x132121f5)

Explanation
An error occurred that was outside the bounds of expected authentication errors.

Administrator response
Contact your IBM service representative with the given error status.

HPDIA0502E

Password change failed for user %s (error status 0x%x). (0x132121f6)

Explanation
An error occurred that was outside the bounds of expected authentication errors.

Administrator response
Contact your IBM service representative with the given error status.

HPDJA0100E

Invalid argument: Null context. (0x307a8064)

Explanation
A nonnull context object is required to communicate with the Security Verify Access policy server and define values for message and trace logging.

Administrator response
Ensure that the context argument is nonnull.

HPDJA0101E

Invalid argument: Null messages. (0x307a8065)

Explanation
A nonnull PDMessages object is required to hold any return messages that might be generated during the operation. Typically, this object contains no messages on input.

Administrator response
Ensure that the messages argument is nonnull.

HPDJA0102E

Invalid argument: Null or zero-length user or group name. (0x307a8066)

Explanation
A valid, nonnull name is required.

Administrator response
Ensure that the user or group name argument is nonnull and has a positive length.

HPDJA0103E

Invalid argument: Null or zero-length registry name. (0x307a8067)

Explanation
A valid, nonnull registry name is required.

Administrator response
Ensure that the registry name argument is nonnull and that the name returned by its getRgyName() method is nonnull and has a positive length.

HPDJA0104E

Invalid argument: Null or zero-length password. (0x307a8068)

Explanation
A valid, nonnull password is required.

Administrator response
Ensure that the password argument is nonnull and has a positive length.

HPDJA0105E

Invalid argument: Null or zero-length pattern. (0x307a8069)

Explanation
A valid, nonnull pattern is required.

Administrator response
Ensure that the pattern argument is nonnull and has a positive length.

HPDJA0106E

Invalid argument: Negative maximum return number. (0x307a806a)

Explanation
The number of returned items must be nonnegative.

Administrator response
Ensure that the maximum return argument is greater than or equal to 0.

HPDJA0107E

Invalid argument: Null locale. (0x307a806b)

Explanation
A valid, nonnull locale is required. To use the default locale, use the method that does not take a locale argument.

Administrator response
Ensure that the locale argument is nonnull.

HPDJA0108E

Invalid argument: Null configuration URL. (0x307a806c)

Explanation
A valid, nonnull URL is required. In addition, the caller must have adequate permission to access and read the URL. The configuration data in the URL must be in the proper format and must contain all the data necessary to locate and communicate with a Security Verify Access policy server.

Administrator response
Ensure that the configuration URL argument is nonnull.

HPDJA0109W

A nonnull value is being passed to an unsupported argument. (0x307a806d)

Explanation
The method being invoked has one or more unsupported arguments. A nonnull value is being passed for an unsupported argument.

Administrator response
Ensure that a value of null is passed for unsupported arguments. Refer to product documentation to find out what arguments are unsupported for the method being invoked.

HPDJA0110E

Invalid data received from the Security Verify Access policy server. (0x307a806e)

Explanation
The data received from the Security Verify Access policy server is invalid. Required values might be missing or the values might have been corrupted during transmission. Data values might be missing because the policy server is incompatible with the client.

Administrator response
Ensure the Security Verify Access policy server supports the release level of the client. If the policy server is compatible with the client, try the operation again.

HPDJA0111W

The component has not been initialized or has already been shut down. (0x307a806f)

Explanation
The shutdown() method was called on a component that has already been shut down or was never initialized.

Administrator response
No action is required.

HPDJA0112W

The component has already been initialized. (0x307a8070)

Explanation
The initialize() method of a component initialization class might be called more than once, but only the first caller sets the program name for the component log output.

Administrator response
No action is required, but the program name might differ from what is expected. Use the getProgramName() method to determine the program name that appears in the component message and trace log output.

HPDJA0113W

The component was not shut down. There might be other users. (0x307a8071)

Explanation
Several calls might have been made to initialize a component using the initialize() method. The component is shut down only after the same number of calls have been made to the shutdown() method. Each program that calls the initialize() method should also call the shutdown() method.

Administrator response
No action is required.

HPDJA0114E

Invalid argument: Null or zero-length attribute name. (0x307a8072)

Explanation
A valid, nonnull attribute name is required.

Administrator response
Ensure that the attribute name argument is nonnull and has a positive length.

HPDJA0115E

Invalid argument: Null attribute value. (0x307a8073)

Explanation
A nonnull attribute value is required.

Administrator response
Ensure that the attribute value argument is nonnull.

HPDJA0116E

Cannot contact server. (0x307a8074)

Explanation
The client cannot connect to the server. This can mean that the server process is not running or that network connectivity does not exist between the client and server machines due to network partitioning caused by an intervening firewall or a nonfunctional intermediate router. The server address and port can be found in the trace log file.

Administrator response
Ensure that network connectivity exists between the client and server machines (issue a ping, for example) and verify that the server process is running on the expected port.

HPDJA0117E

Invalid argument: Null description text. (0x307a8075)

Explanation
A nonnull description value is required.

Administrator response
Ensure that the description argument is nonnull.

HPDJA0118E

Invalid argument: Port number is less than or equal to 0. (0x307a8076)

Explanation
Only port numbers greater than 0 are valid. It is usually good practice to assign port numbers greater than 1024 to user applications because many systems reserve port numbers below that value for special purposes.

Administrator response
Ensure that the input port number is greater than 0.

HPDJA0119E

Invalid argument: Null or zero-length server host name. (0x307a8077)

Explanation
A valid, nonnull host name is required.

Administrator response
Ensure that the server host name argument is nonnull and has a positive length.

HPDJA0120W

The outData information received from the policy server was not returned because the input outData parameter is null. (0x307a8078)

Explanation
A nonnull outData argument is required to return outData information received from the policy server.

Administrator response
Ensure the outData argument is nonnull.

HPDJA0122E

Unknown message code: *%s*. (0x307a807a)

Explanation
The text for the message code could not be found in the message catalogs installed on the local system. This typically means that the policy server is at a more recent level than the client and has returned a code undefined in the client runtime. The documentation associated with the policy server installation should include the message code.

Administrator response
Consult the Error Message Reference to obtain the message text, explanation, and suggested actions for the message code.

HPDJA0123E

Invalid argument: Null properties. (0x307a807b)

Explanation
A valid, nonnull properties object is required.

Administrator response
Ensure that the properties argument is nonnull.

HPDJA0124E

Invalid argument: Null or zero-length credentials. (0x307a807c)

Explanation
A valid, nonnull credentials array is required.

Administrator response
Ensure that the delegated credentials argument is nonnull and has a positive length.

HPDJA0125E

The data for *%s* that was received from the Security Verify Access policy server is not valid. (0x307a807d)

Explanation
The data received from the Security Verify Access policy server is not valid. Required values might be missing or the values might have been garbled during transmission. Data values might be missing because the policy server is incompatible with the client.

Administrator response
Ensure that the Security Verify Access policy server supports the release level of the client. If the policy server is compatible with the client, try the operation again.

HPDJA0126E

Connection pool closed. (0x307a807e)

Explanation
Attempting to acquire a connection from a connection pool when in the process of closing or is closed. This is usually due to resuing a PDContext after calling its close() method. Create a new PDContext or defer calling PDContext.close() method.

Administrator response
Do not re-use a PDContext after calling its close() method.

HPDJA0127E

No PDContext available. (0x307a807f)

Explanation
There is no more free PDContext in the PDContextPool to service the getPDContext() call.

Administrator response
Increase the PDContextPool size and ensure application calls PDContext.close() to return the PDContext back into the pool it's no longer needed.

HPDJA0200E

Invalid operation: The current object does not represent a Security Verify Access user. (0x307a80c8)

Explanation
An operation was attempted on a PDUser object that represents a user that exists in the user registry but is undefined in Security Verify Access. Therefore, certain Security Verify Access operations are invalid.

Administrator response
Ensure that the user this object represents is defined in Security Verify Access. That is, there must be a user defined to the Security Verify Access policy server with the registry name used to instantiate this object.

HPDJA0201E

Invalid argument: The user name object is not a valid type or is zero-length. (0x307a80c9)

Explanation
The input user name argument can be a String object representing a Security Verify Access user name or an instance of the PDRgyUserName class if the name being specified is a registry name. No other object types are allowed. If the input name argument is a String, it must have a positive length. If the input name is a PDRgyUserName object, the String returned from its getRgyName() method must be nonnull and have a positive length.

Administrator response
Ensure that the user name argument is an instance of the String class for Security Verify Access user names or an instance of the PDRgyUserName class for registry names. Ensure the input String or the name returned from the PDRgyUserName object getRgyName() method is nonnull and has a positive length.

HPDJA0300E

Invalid operation: The current object does not represent a Security Verify Access group. (0x307a812c)

Explanation
An operation was attempted on a PDGroup object that represents a group that exists in the user registry but is undefined in Security Verify Access. Therefore, certain Security Verify Access operations are invalid.

Administrator response
Ensure that the group this object represents is defined in Security Verify Access. That is, there must be a group defined to the Security Verify Access policy server with the registry name used to instantiate this object.

HPDJA0301E

Invalid argument: The group name object is not a valid type or is zero-length. (0x307a812d)

Explanation
The input group name argument can be a String object representing a Security Verify Access group name or an instance of the PDRgyGroupName class if the name being specified is a registry name. No other object types are allowed. If the input name argument is a String, it must have a positive length. If the input name is a PDRgyGroupName object, the String returned from its getRgyName() method must be nonnull and have a positive length.

Administrator response
Ensure that the group name argument is an instance of the String class for Security Verify Access group names or an instance of the PDRgyGroupName class for registry names. Ensure the input String or the name returned from the PDRgyGroupName object getRgyName() method is nonnull and has a positive length.

HPDJA0302E

Invalid argument: Null or empty member name list. (0x307a812e)

Explanation
At least one valid, nonnull member name is required.

Administrator response
Ensure that the member name list argument is nonnull and has at least one member.

HPDJA0400E

Invalid argument: The maximum number of login failures is outside of the allowed range. (0x307a8190)

Explanation
The maximum number of login failures is enforced to be a nonnegative integer.

Administrator response
Ensure that the maximum number of login failures argument is greater than or equal to 0.

HPDJA0401E

Invalid argument: The account-disable time interval argument is outside of the allowed range. (0x307a8191)

Explanation
The account-disable time interval is enforced to be an integer greater than or equal to 0 (where 0 indicates an unlimited time interval).

Administrator response
Ensure that the account disable time interval argument is greater than or equal to 0.

HPDJA0402E

Invalid argument: The account expiration date argument is outside of the allowed range. (0x307a8192)

Explanation
The account expiration date is enforced by the API logic. The maximum value is consistent with existing Security Verify Access installations that impose this limitation.

Administrator response
Ensure that the account expiration date argument falls within the acceptable range, current time - 2035-12-31-23:59:59.

HPDJA0403E

Invalid argument: The maximum password age argument is outside of the allowed range. (0x307a8193)

Explanation
The maximum password age must be a nonnegative integer.

Administrator response
Ensure that the maximum password age argument is greater than or equal to 0.

HPDJA0404E

Invalid argument: The maximum repeated characters argument is outside of the allowed range. (0x307a8194)

Explanation
The range of the maximum repeated characters value is enforced to be a nonnegative integer.

Administrator response
Ensure that the maximum repeated characters argument is greater than or equal to 0.

HPDJA0405E

Invalid argument: The minimum alphabetic characters argument is outside of the allowed range. (0x307a8195)

Explanation
The minimum alphabetic characters value is enforced to be a nonnegative integer.

Administrator response
Ensure that the minimum alphabetic characters argument is greater than or equal to 0.

HPDJA0406E

Invalid argument: The minimum nonalphabetic characters argument is outside of the allowed range. (0x307a8196)

Explanation
The minimum nonalphabetic characters value is enforced to be a nonnegative integer.

Administrator response
Ensure that the minimum nonalphabetic characters argument is greater than or equal to 0.

HPDJA0407E

Invalid argument: The minimum password length argument is outside of the allowed range. (0x307a8197)

Explanation
The minimum password length value is enforced to be a nonnegative integer.

Administrator response
Ensure that the minimum password length argument is greater than 0.

HPDJA0408E

Invalid argument: The time-of-day access days specification argument does not correspond to any predefined value. (0x307a8198)

Explanation
The bitmaps defined in the PDPolicy class represent the days of the week positionally within an 8-bit structure.

Administrator response
Ensure that the access days are specified using the predefined bitmaps. These bitmaps can be used individually. A logical OR operation can be performed on two or more of the bitmaps to generate the desired bitmap.

HPDJA0409E

Invalid argument: The time-of-day start time is either less than 0 or greater than the maximum allowable time. (0x307a8199)

Explanation
The time-of-day start time must fall within 0 through 1439.

Administrator response
Ensure that the time-of-day start time falls within the acceptable range, 0 through 1439.

HPDJA0410E

Invalid argument: The time-of-day end time is either less than 0 or greater than the maximum allowable time. (0x307a819a)

Explanation
The maximum value is the number of minutes in 24 hours, less 1 minute.

Administrator response
Ensure that the time-of-day end time falls within the acceptable range, 0 through 1439.

HPDJA0411E

Invalid argument: The time-of-day time zone is not UTC or local. (0x307a819b)

Explanation
Only two time zone values are supported: UTC or local. These values are represented by constants in the PDPolicy class.

Administrator response
Ensure that the time zone is one of the predefined constants, PDPOLICY_TIME_UTC or PDPOLICY_TIME_LOCAL, found in the PDPolicy class.

HPDJA0412E

Invalid argument: The maximum number of concurrent web sessions is outside of the allowed range. (0x307a819c)

Explanation
The maximum number of concurrent web sessions is enforced to be a nonnegative integer and greater than zero.

Administrator response
When specifying a number for the maximum number of concurrent web sessions, ensure that it is an integer greater than 0.

HPDJA0500E

Invalid argument: Null or zero-length ACL name. (0x307a81f4)

Explanation
An ACL name is required.

Administrator response
Ensure that the ACL name argument is nonnull.

HPDJA0502E

Invalid argument: Null PDAclEntryUser object. (0x307a81f6)

Explanation
A nonnull PDAclEntryUser argument is required.

Administrator response
Ensure that the PDAclEntryUser argument is nonnull.

HPDJA0503E

Invalid argument: Null PDAclEntryGroup object. (0x307a81f7)

Explanation
A nonnull PDAclEntryGroup argument is required.

Administrator response
Ensure that the PDAclEntryGroup argument is nonnull.

HPDJA0504E

Invalid argument: Null PDAclEntryAnyOther object. (0x307a81f8)

Explanation
A nonnull PDAclEntryAnyOther argument is required.

Administrator response
Ensure that the PDAclEntryAnyOther argument is nonnull.

HPDJA0505E

Invalid argument: Null PDAclEntryUnAuth object. (0x307a81f9)

Explanation
A nonnull PDAclEntryUnAuth argument is required.

Administrator response
Ensure that the PDAclEntryUnAuth argument is nonnull.

HPDJA0506E

Invalid argument: Null or zero-length user name field for the ACL entry. (0x307a81fa)

Explanation
A user name is required to create an ACL entry.

Administrator response
Ensure that the user name for the ACL entry is nonnull.

HPDJA0507E

Invalid argument: Null or zero-length group name field for the ACL entry. (0x307a81fb)

Explanation
A group name is required to create an ACL entry.

Administrator response
Ensure that the group name for the ACL entry is nonnull.

HPDJA0508E

Invalid argument: Null permissions field for the ACL entry. (0x307a81fc)

Explanation
A nonnull permissions field is required to create an ACL entry.

Administrator response
Ensure that the permissions field for the ACL entry is nonnull.

HPDJA0509E

An ACL entry present in the UserAclEntries HashMap is not a PDAclEntryUser object. (0x307a81fd)

Explanation
Only PDAclEntryUser objects can be present in the UserAclEntries HashMap. Use the GroupAclEntries HashMap for passing in the PDAclEntryGroup objects.

Administrator response
Ensure that the UserAclEntries HashMap contains only PDAclEntryUser objects.

HPDJA0510E

An ACL entry present in the GroupAclEntries HashMap is not a PDAclEntryGroup object. (0x307a81fe)

Explanation
Only PDAclEntryGroup objects can be present in the GroupAclEntries HashMap. Use the UserAclEntries HashMap for passing in the PDAclEntryUser objects.

Administrator response
Ensure that the GroupAclEntries HashMap contains only PDAclEntryGroup objects.

HPDJA0600E

Invalid argument: Null or zero-length protected object name. (0x307a8258)

Explanation
A nonnull protected object name is required.

Administrator response
Ensure that the protected object name argument is nonnull.

HPDJA0601E

Invalid argument: Null or zero-length permission string (0x307a8259)

Explanation
A nonnull permission string is required.

Administrator response
Ensure that the permission string is nonnull.

HPDJA0602E

Invalid argument: Length of input arrays do not match. (0x307a825a)

Explanation
Matching Input array lengths required.

Administrator response
Ensure that the size of all input arrays match.

HPDJA0700E

Invalid argument: Null or zero-length protected objectspace name. (0x307a82bc)

Explanation
A nonnull protected objectspace name is required.

Administrator response
Ensure the protected objectspace name argument is nonnull.

HPDJA0800E

Invalid argument: Null or zero-length application server name. (0x307a8320)

Explanation
A valid, nonnull name is required.

Administrator response
Ensure that the application server name argument is nonnull and has a positive length.

HPDJA0801E

Invalid argument: Null group list. (0x307a8321)

Explanation
A valid, nonnull group list is required.

Administrator response
Ensure that the application server group list argument is nonnull. An empty list may be used to clear an existing group list.

HPDJA0802E

Invalid argument: Null URL or invalid protocol. (0x307a8322)

Explanation
A valid, nonnull URL is required. In addition, only the 'file' protocol is currently supported.

Administrator response
Ensure that the URL argument is nonnull and that the URL uses the 'file' protocol.

HPDJA0803E

Database URL does not specify a directory. (0x307a8323)

Explanation
The operation requires an existing directory in which to locate the local policy database.

Administrator response
Ensure that the database URL argument specifies an existing directory on the local system.

HPDJA0804E

Invalid argument: Null or empty Security Verify Access server list. (0x307a8324)

Explanation
Configuration and use of Java application servers require communication with the Security Verify Access policy server and an authorization server.

Administrator response
Ensure that there is at least one server in the server list argument.

HPDJA0805E

Invalid argument: Preference rank must be greater than 0. (0x307a8325)

Explanation
Internal logic requires that all Security Verify Access servers specified in an application configuration have a rank greater than 0.

Administrator response
Ensure that the rank argument is greater than 0.

HPDJA0806E

Invalid argument: Unsupported configuration action. (0x307a8326)

Explanation
The configureAppSvr() method verifies that a known action is specified and executes different logic based on that action.

Administrator response
Ensure that one of the configuration action constants defined in the PDAppSvrConfig class is used.

HPDJA0807E

Invalid argument: Null application server specification. (0x307a8327)

Explanation
The nonnull application server specification is required.

Administrator response
Ensure that the application server specification argument is nonnull.

HPDJA0808E

The specified configuration or keystore file already exists. (0x307a8328)

Explanation
The 'create' configuration action is designed to check for existing files and fail if they are found in order not to overwrite them accidentally.

Administrator response
To preserve existing files, specify new configuration and keystore file names. To overwrite existing files, specify the 'replace' configuration action.

HPDJA0809E

Cannot create the specified configuration or keystore file. (0x307a8329)

Explanation
Failure to create the configuration or keystore file might be caused by a variety of reasons such as access restrictions or limited resources (file descriptors or disk space).

Administrator response
Try another file name or another directory. Ensure that the process has permission to create and write to the file.

HPDJA0810E

The signature needed to sign a certificate request is not supported. (0x307a832a)

Explanation
Only RSA is used to create application server certificate requests. If the Security Verify Access policy server's certificate has not been signed using RSA, then information required to complete the application server certificate request is not available.

Administrator response
Ensure that the keystore used by the Security Verify Access policy server has not been corrupted and that the signature algorithm for the server certificate is RSA. Other signature algorithms, such as DSA, are not supported.

HPDJA0811W

Some aspect of local unconfiguration failed. (0x307a832b)

Explanation
When unconfiguring a Java application server, a number of operations are performed locally. These steps include removing configuration data from the configuration URL and deleting the keystore file. One or more of these steps failed, so the files must be manually cleaned up.

Administrator response
Manually remove the configuration or keystore file, or both, if desired. Alternatively, information in the files can be overwritten by configuring another Java application server using the 'replace' action.

HPDJA0812E

Invalid argument: Unrecognized server type. (0x307a832c)

Explanation
A recognized server type is required.

Administrator response
Ensure the server type argument is one of the server type constants defined in the PDAppSvrConfig class.

HPDJA0813E

Invalid argument: Null server object. (0x307a832d)

Explanation
A nonnull server object is required.

Administrator response
Ensure the server argument is nonnull.

HPDJA0814E

The specified server already exists in the configuration. (0x307a832e)

Explanation
A server cannot be added to the configuration if it already exists.

Administrator response
Check that the input server has been specified properly. Ensure that the host, port and server type are correct. The configuration information can be examined using the getAppSvrInfo() method for further information.

HPDJA0815E

The specified server does not exist in the configuration. (0x307a832f)

Explanation
A server of the specified type with the given host and port cannot be found the configuration.

Administrator response
Check that the input server has been specified properly. Ensure that the host, port, and server type are correct. The configuration information can be examined using the getAppSvrInfo() method.

HPDJA0816E

Cannot remove last server. (0x307a8330)

Explanation
At least one policy server and one authorization server must be specified in a Java application server configuration. The last policy server and authorization server cannot be removed.

Administrator response
Add another server of the specified type before trying to remove this one.

HPDJA0817E

The specified server is ambiguous. It matches more than one server in the configuration. (0x307a8331)

Explanation
When searching for a match to the input server, first both host and port are examined. If a server in the configuration matches both host and port, the search is done. If no server in the configuration matches both host and port, a match is made on host alone. If more than one server matches on host, the results are ambiguous.

Administrator response
Change the port specification of the server so that the combination of host and port matches one and only one server of its type in the configuration. The configuration information can be examined using the getAppSvrInfo() method.

HPDJA0818E

Cannot set value for remote mode application server. (0x307a8332)

Explanation
The configuration data that is being set is used only by local mode Java application servers, and the specified configuration URL indicates a remote mode server.

Administrator response
Verify that the application server was configured correctly. If it is supposed to operate in local mode, the server must be unconfigured and configured again. If it is not supposed to operate in local mode, the attempted operation is not applicable and no further action is necessary.

HPDJA0819W

Failure restoring original configuration or keystore information. (0x307a8333)

Explanation
The configuration operation failed but the original contents of the configuration or keystore file, or both, could not be restored, possibly due to a system-dependent file I/O error. The information contained in the files is lost, but this is significant only if there was application-specific data in the configuration file. If that was the case, the only recovery is to reconfigure the application server and supply any extra information to the new configuration.

Administrator response
The Java application server should be unconfigured and then reconfigured.

HPDJA0820W

Local unconfiguration ignored; specified application server name or host does not match data in configuration file. (0x307a8334)

Explanation
Before performing local unconfiguration operations, a check is made to verify that the user specified the same server and host data that is present in the configuration file. This check prevents a user from inadvertently removing local configuration for the wrong application server. Since this check is made after calling the policy server to unconfigure the application server, it has no effect on remote unconfiguration operations.

Administrator response
Ensure that the application server name and host specified to the unconfiguration operation matches the application server name and host present in the configuration file.

HPDJA0821E

Cannot create temporary configuration file. (0x307a8335)

Explanation
Failure to create the configuration file might be caused by a variety of reasons such as access restrictions or limited resources (file descriptors or disk space).

Administrator response
Try another file name or another directory. Ensure that the process has permission to create and write to the file.

HPDJA0822E

Cannot store information in temporary configuration file. (0x307a8336)

Explanation
Failure to create the configuration file might be caused by a variety of reasons such as access restrictions or limited resources (file descriptors or disk space).

Administrator response
Try another file name or another directory. Ensure that the process has permission to create and write to the file.

HPDJA0823E

Cannot set Local LDAP Management value as it is not enabled. (0x307a8337)

Explanation
The configuration data that is being set is used only by the Local LDAP Management API, and the specified configuration URL indicates a it is not enabled.

Administrator response
Verify that Local LDAP Management was configured correctly. If it is supposed to be enabled, the server must be unconfigured and configured again. If it is not supposed to have Local LDAP Management, the attempted operation is not applicable and no further action is necessary.

HPDJA0900E

Invalid argument: Null or zero-length SSO resource name. (0x307a8384)

Explanation
A valid, nonnull SSO resource name is required.

Administrator response
Ensure the SSO resource name argument is nonnull and has a positive length.

HPDJA1000E

Invalid argument: Null or zero-length SSO resource group name. (0x307a83e8)

Explanation
A valid, nonnull SSO resource group name is required.

Administrator response
Ensure the SSO resource group name argument is nonnull and has a positive length.

HPDJA1100E

Invalid argument: SSO resource type. (0x307a844c)

Explanation
The SSO resource type must be either PDSSOCRED_SSORESOURCE or PDSSOCRED_SSORESOURCEGROUP, defined in the PDSSOCred class.

Administrator response
Ensure the SSO resource type is one of the supported types.

HPDJA1101E

Invalid argument: SSO resource user name. (0x307a844d)

Explanation
A nonnull SSO resource user name is required.

Administrator response
Ensure the SSO resource user name argument is nonnull.

HPDJA1102E

Invalid argument: SSO resource password. (0x307a844e)

Explanation
A nonnull SSO resource password is required.

Administrator response
Ensure the SSO resource password argument is nonnull.

HPDJA1200E

Invalid argument: Null or zero-length action name. (0x307a84b0)

Explanation
A valid, nonnull action name is required.

Administrator response
Ensure that the action name argument is nonnull and has a positive length.

HPDJA1201E

Invalid argument: Null action type. (0x307a84b1)

Explanation
A valid, nonnull action type is required.

Administrator response
Ensure that the action type argument is nonnull.

HPDJA1202E

Invalid argument: Null or zero-length action group name. (0x307a84b2)

Explanation
A valid, nonnull action group name is required.

Administrator response
Ensure that the action group name argument is nonnull and has a positive length.

HPDJA1300E

Invalid argument: Null or zero-length server name. (0x307a8514)

Explanation
A valid, nonnull server name is required.

Administrator response
Ensure that the server name argument is nonnull and has a positive length.

HPDJA1301E

Invalid argument: Null task name. (0x307a8515)

Explanation
A valid, nonnull task name is required.

Administrator response
Ensure that the task name argument is nonnull and has a positive length.

HPDJA1400E

Invalid argument: Null or zero-length POP name. (0x307a8578)

Explanation
A valid, nonnull POP name is required.

Administrator response
Ensure that the POP name argument is nonnull and has a positive length.

HPDJA1401E

Invalid argument: Null or invalid QOP value. (0x307a8579)

Explanation
A valid, nonnull QOP value is required.

Administrator response
Ensure that the QOP argument is nonnull and is one of the PDPOP_QOP_* constants defined in the PDPop class.

HPDJA1402E

Invalid argument: Invalid audit level value. (0x307a857a)

Explanation
A valid, nonnull value for the audit level is required.

Administrator response
Ensure that the audit level argument is set to one of the PDPOP_AUDIT_LEVEL_* constants defined in the PDPop class or a logical OR operation on these constants.

HPDJA1403E

Invalid argument: Null todAccessInfo argument. (0x307a857b)

Explanation
A nonnull todAccessInfo argument is required.

Administrator response
Ensure that the todAccessInfo argument is nonnull. Use the PDTodAccessInfo constructor to create a valid PDTodAccessInfo object.

HPDJA1404E

Invalid argument: Null or empty IPAuthInfo argument. (0x307a857c)

Explanation
A nonnull and nonempty IPAuthInfo argument is required.

Administrator response
Ensure that the IPAuthInfo argument is nonnull and nonempty. Use the PDPop.IPAuthInfo constructor to create IPAuthInfo objects and pass them as elements of the IPAuthInfo ArrayList argument.

HPDJA1405W

IPAuthInfo specified at index *%s* already exists for this POP. (0x307a857d)

Explanation
New IPAuthInfo cannot be specified if IPAuthInfo already exists for a given IP address and netmask.

Administrator response
Ensure that the existing IPAuthInfo for the specified IP address and netmask is removed before specifying a new one for the same IP address and netmask.

HPDJA1406W

IPAuthInfo specified at index *%s* not found for this POP. (0x307a857e)

Explanation
Only IPAuthInfo entries that exist can be removed.

Administrator response
Ensure that the IPAuthInfo entry exists. If the entry does not exist, remove it from the input list.

HPDJA1407E

Specified IP address is not valid. (0x307a857f)

Explanation
A valid IP address is required.

Administrator response
Ensure that the IP address is specified in dotted decimal format with valid numeric characters.

HPDJA1408E

Specified netmask is not valid. (0x307a8580)

Explanation
A valid netmask is required.

Administrator response
Ensure that the netmask is specified in dotted decimal format with valid numeric characters.

HPDJA1500E

Invalid argument: Null or zero-length domain name. (0x307a85dc)

Explanation
A valid, nonnull domain name is required.

Administrator response
Ensure that the domain name argument is nonnull and has a positive length.

HPDJA1600E

Invalid argument: Null or zero-length rule name. (0x307a8640)

Explanation
A valid, nonnull rule name is required.

Administrator response
Ensure that the rule name argument is nonnull and has a positive length.

HPDJA1601E

Invalid argument: Null or zero-length rule text. (0x307a8641)

Explanation
A valid, nonnull rule text is required.

Administrator response
Ensure that the rule text argument is nonnull and has a positive length.

HPDJA1602E

Invalid argument: Null fail reason. (0x307a8642)

Explanation
A nonnull fail reason is required.

Administrator response
Ensure that the fail reason argument is nonnull.

HPDJA1700E

Command does not pass validation check. (0x307a86a4)

Explanation
The command syntax was incorrect. This can occur when an argument of the wrong type is specified.

Administrator response
Verify the correct syntax for the command and try again.

HPDJA1708E

The server did not start. (0x307a86ac)

Explanation
A problem occurred when the command line program tried to start the server.

Administrator response
Try to start the server independently of the command line administration tool; it might start successfully under those circumstances. If the server fails to start, any errors that are written to the terminal or to the server's trace logs can be used to help determine the problem.

HPDJA1710E

The server did not stop. Check the host and port number. (0x307a86ae)

Explanation
A problem occurred when the command line program tried to stop the server.

Administrator response
Ensure that the host and port specify a valid audit server. If the host and port specify a different type of server, the stop command will not work. If the host and port do specify a valid audit server, try to stop the server independently of the command line administration tool; it might stop successfully using that method. If the server fails to stop, any errors that are written to the terminal or to the server's trace logs can be used to help determine the problem.

HPDJA1711E

Invalid argument: Port number must be greater than 0. (0x307a86af)

Explanation
A valid, positive port number is required in order to try to connect to the server.

Administrator response
Ensure that the specified port number is greater than 0.

HPDJA1712E

Could not detect a server running on host *%s*, port *%s*. (0x307a86b0)

Explanation
The command line program cannot stop a server if it cannot connect to it using the specified host and port.

Administrator response
Ensure that the specified host and port number are correct. Also, test connectivity from the system on which the command line program is running to the target system.

HPDMG0150E

Invalid object name. (0x14c01096)

Explanation
The Security Verify Access policy server received a request containing an invalid object name.

Administrator response
Ensure that the object has been specified properly.

HPDMG0155E

Too many subjects found within the client credential. (0x14c0109b)

Explanation
The Security Verify Access policy server encountered a client credential that contained more than one subject.

Administrator response
Ensure that the request or operation deals with a single identity.

HPDMG0156E

Unable to sign a certificate. Unexpected error from *%s* (0x*%8.8lx*). (0x14c0109c)

Explanation
An unexpected error was encountered while attempting to issue a certificate.

Administrator response
Ensure that the keystore used by the Security Verify Access policy server has not been corrupted.

HPDMG0157E

The policy server failed to sign a certificate. (0x14c0109d)

Explanation
The Security Verify Access policy server encountered an unexpected error while attempting to sign a certificate.

Administrator response
Ensure that there is enough disk space on the policy server machine. See ivmgrd.log for more information.

HPDMG0158E

Could not open *%s* because the password stash file does not exist or is corrupted. (0x14c0109e)

Explanation
The server's configuration has possibly been corrupted.

Administrator response
Ensure that the keystore has not been corrupted. If the failure persists, reconfigure the failed server.

HPDMG0160E

SSL database (ivmgrd.kdb) could not be opened. (0x14c010a0)

Explanation
The Security Verify Access policy server keystore file, ivmgrd.kdb, could not be opened.

Administrator response
Ensure that the keystore used by the Security Verify Access policy server exists and has not been corrupted. Should the failure persist, stop the policy server, and run mgrsslcfg to re-configure the policy server.

HPDMG0162E

ASN1 decode error *%d* occurred. The certificate buffer received is invalid and cannot be decoded. (0x14c010a2)

Explanation
The Security Verify Access policy server has received a corrupted or invalid request.

Administrator response
Retry the operation. If the problems persists, unconfigure and reconfigure the client application or remote server.

HPDMG0164E

The Policy Server could not be started (0x*%8.8lx*). (0x14c010a4)

Explanation
The Security Verify Access policy server encountered an error during initialization. Probably the password or login DN is incorrect or the password has expired. This error should not occur if the program is correctly configured, but if [ldap] admin-dn or admin-pwd values in .conf files have been modified then it is possible.

Administrator response
Check ivmgrd.log for additional information.

HPDMG0165W

The application has received a database update notification however the version of the command is incorrect. The policy database will not be updated. (0x14c010a5)

Explanation
The policy server has sent a database update notification however the policy server is unaware that this system has been upgraded.

Administrator response
This is typically a self-correcting problem and no action is normally required. If the problem persists beyond a restart of the application, check the application logs and policy server logs for additional information.

HPDMG0166W

Memory allocation failure. Attempted to allocate *%d* bytes of memory. (0x14c010a6)

Explanation
The Security Verify Access policy server attempted to allocate memory, and an error occurred.

Administrator response
This error might be a temporary condition. Attempt to free up memory by closing other running applications. If the problem persists, increase the system memory in the machine.

HPDMG0167E

Domain in the certificate to be signed does not match the local domain. (0x14c010a7)

Explanation
PDMgr received a certificate to be signed but the domain in the certificate distinguished name is different from the local domain contained in the authenticated credentials for the session.

Administrator response
Log in to the correct domain for the certificate.

HPDMG0169E

Database migration failed! (0x14c010a9)

Explanation
The Security Verify Access policy server has opened a down-level version of the policy database, and encountered an error in the process of migrating the database to the current level.

Administrator response
Ensure that system resources are available and retry. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG0170E

The policy server is unable to sign certificates. The policy server's CA certificate has expired. (0x14c010aa)

Explanation
The policy server's CA certificate lifetime of 20 years has expired.

Administrator response
Unconfigure and re-configure the policy server, then unconfigure and re-configure all clients and applications in the secure domain.

HPDMG0301E

No command handler is installed for the command. (0x14c0112d)

Explanation
The Security Verify Access policy server received an unsupported request. This can occur when Security Verify Access is running in an unsupported configuration.

Administrator response
Ensure that the client application version is supported by Security Verify Access.

HPDMG0451E

Invalid server name. (0x14c011c3)

Explanation
The Security Verify Access policy server has received a server request containing an invalid server name. This error is likely due to a syntax error in the name.

Administrator response
Ensure that the server name argument is nonnull.

HPDMG0452E

Server not found. (0x14c011c4)

Explanation
The Security Verify Access policy server has received a server request containing a server name that cannot be found in the policy database.

Administrator response
Ensure that the server name appears in the list of configured servers.

HPDMG0453E

A server with the same name already exists. (0x14c011c5)

Explanation
The Security Verify Access policy server has received a configure server request containing a server name of an already configured server.

Administrator response
Ensure that the server name is not in the list of configured servers.

HPDMG0455W

The API function is not supported by this registry type. (0x14c011c7)

Explanation
An attempt was made to use a registry API function that is not supported by the installed registry type.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG0462E

The AZN application returned an error. (0x14c011ce)

Explanation
The admin service plugin has returned an error.

Administrator response
Refer to the admin service plugin documentation.

HPDMG0463E

A protected object *%s* was requested from the *%s* application. The application returned the following error: (0x*%8.8lx*). (0x14c011cf)

Explanation
The Security Verify Access policy server will request protected object information from applications at various times. This information is used to facilitate management of the protected object space. An error has occurred while attempting to retrieve this information.

Administrator response
The application might not be configured correctly. Check the returned error code, make any necessary corrections, and retry the operation.

HPDMG0464E

A list of child protected objects under the parent protected object *%s* was requested from the *%s* application. The application returned the following error: (0x*%8.8lx*). (0x14c011d0)

Explanation

The Security Verify Access policy server will request protected object information from applications at various times. This information is used to facilitate management of the protected object space. An error has occurred while attempting to retrieve this information.

Administrator response

The application might not be configured correctly. Check the returned error code, make any necessary corrections, and retry the operation.

HPDMG0465E

An administration task was forwarded to the *%s* application. The application returned the following error: (0x*%8.8lx*). (0x14c011d1)

Explanation

The Security Verify Access policy server attempted to forward the requested administration task to the application. The application returned an error indicating the task could not be performed.

Administrator response

The application might not be configured correctly. Check the returned error code, make any necessary corrections, and retry the operation.

HPDMG0466E

A list of supported administration tasks was forwarded to the *%s* application. The application returned the following error: (0x*%8.8lx*). (0x14c011d2)

Explanation

The Security Verify Access policy server requested the list of supported administration tasks from the application. The application returned an error indicating that the list could not be provided.

Administrator response

The application may not be configured correctly. Check the returned error code, make any necessary corrections, and retry the operation.

HPDMG0467E

A policy database update notification was sent to the *%s* application. The application returned the following error: (0x*%8.8lx*). (0x14c011d3)

Explanation

The Security Verify Access policy server sent a database update notification to the application. This notification informs the application that a change has been made to the policy database.

Administrator response

The application may not be configured correctly. Check the returned error code and make any necessary corrections. You can force a database update notification to be sent by using the "server replicate" administration command.

HPDMG0600E

Object not found. (0x14c01258)

Explanation
The Security Verify Access policy server received a request that referenced an object which was not found in the policy database.

Administrator response
Ensure that the requested object exists and is referenced correctly.

HPDMG0601E

Object already exists. (0x14c01259)

Explanation
The Security Verify Access policy server received a create protected object request for an object name that already exists in the policy database.

Administrator response
Ensure that the requested protected object name does not already exist.

HPDMG0609E

The specified group container cannot be used as it corresponds to an existing group name. (0x14c01261)

Explanation
The Security Verify Access policy server received a request to create a group container specifying a container name that already exists as a group name.

Administrator response
Ensure that the group name does not already exist.

HPDMG0611E

This operation is not supported for the objects in this object space. (0x14c01263)

Explanation
A Security Verify Access admin service plugin has received a request that is not supported.

Administrator response
Refer to the admin service plugin documentation to determine the capabilities of the plugin.

HPDMG0612E

The operation requested cannot be performed on the root object. (0x14c01264)

Explanation
The Security Verify Access policy server received a request to create, delete, or modify the root object. These operations are not permitted.

Administrator response
No action is required.

HPDMG0613E

One or more of the child object names was invalid. (0x14c01265)

Explanation
The Security Verify Access policy server received a request with a protected object as an argument. The object string contained at least one child object that was not present in the policy database.

Administrator response
Ensure that the protected object is specified correctly.

HPDMG0614W

One or more ACL entries contain both the Add (A) and Password (W) capabilities. These capabilities potentially create a security vulnerability if they are granted to an administrator of a group. The administrator may then add any user to the group and then change the user's password. (0x14c01266)

Explanation
With both capabilities, the administrator of a group of users may add any user to the group and then change the user's password.

Administrator response
Only grant both of these capabilities to the same administrator under special controlled circumstances or to a highly trusted user.

HPDMG0615W

One or more ACL entries contain both the Add (A) and Modify (m) capabilities. These capabilities potentially create a security vulnerability if they are granted to an administrator of a group. The administrator may then add any user to the group and then change the user's data. (0x14c01267)

Explanation
With both capabilities, the administrator of a group of users may add any user to the group and then change the user's data.

Administrator response
Only grant both of these capabilities to the same administrator under special controlled circumstances or to a highly trusted user.

HPDMG0616W

One or more ACL entries contain both the Add (A) and Delete (d) capabilities. These capabilities potentially create a security vulnerability if they are granted to an administrator of a group. The administrator may then add any user to the group and then delete the user. (0x14c01268)

Explanation
With both capabilities, the administrator of a group of users may add any user to the group and then delete user.

Administrator response
Only grant both of these capabilities to the same administrator under special controlled circumstances or to a highly trusted user.

HPDMG0619E

The user is not authorized to view attached ACL information. (0x14c0126b)

Explanation
Attached ACL information is available at the specified protected object location, however, the user is not authorized to view ACLs.

Administrator response
No action is required.

HPDMG0620E

The user is not authorized to view attached POP information. (0x14c0126c)

Explanation
Attached POP information is available at the specified protected object location, however, the user is not authorized to view POPs.

Administrator response
No action is required.

HPDMG0621E

The user is not authorized to view attached Rule information. (0x14c0126d)

Explanation
Attached Rule information is available at the specified protected object location, however, the user is not authorized to view Rules.

Administrator response
No action is required.

HPDMG0622E

The user is not authorized to view effective ACL information. (0x14c0126e)

Explanation
Effective ACL information is available at the specified protected object location, however, the user is not authorized to view ACLs.

Administrator response
No action is required.

HPDMG0623E

The user is not authorized to view effective POP information. (0x14c0126f)

Explanation
Effective POP information is available at the specified protected object location, however, the user is not authorized to view POPs.

Administrator response
No action is required.

HPDMG0624E

The user is not authorized to view effective Rule information. (0x14c01270)

Explanation
Effective Rule information is available at the specified protected object location, however, the user is not authorized to view Rules.

Administrator response
No action is required.

HPDMG0625E

The user is not authorized to view one or more protected objects where the requested ACL is attached. (0x14c01271)

Explanation
See text.

Administrator response
No action is required.

HPDMG0626E

The user is not authorized to view one or more protected objects where the requested POP is attached. (0x14c01272)

Explanation
See text.

Administrator response
No action is required.

HPDMG0627E

The user is not authorized to view one or more protected objects where the requested authzrule is attached. (0x14c01273)

Explanation
See text.

Administrator response
No action is required.

HPDMG0628E

The specified network addresses cannot be processed by the Security Verify Access policy server. (0x14c01274)

Explanation
This error may occurr if the network addresses are invalid, or the addresses are in IPv6 format and the Security Verify Access policy server is running on an operating system that does not support IPv6.

Administrator response
No action is required.

HPDMG0632E

An error occurred while attempting to copy the project object, *%s*, to *%s* (0x*%x*). (0x14c01278)

Explanation
See message.

Administrator response
Examine the log file for additional information on this error.

HPDMG0752E

More than one matching Distinguished Name (DN) was found. (0x14c012f0)

Explanation
Multiple entries have been found in the LDAP registry when only one was expected.

Administrator response
Ensure that the LDAP registry has not been modified using external tools.

HPDMG0753E

An invalid format of the authorization mechanism attribute was found in the user entry. (0x14c012f1)

Explanation
The correct format is <AppName>:<mechanism>[,<mechanism>....]. The default is Default:LDAP. This information is stored in the secUser object's secLoginType attribute.

Administrator response
Ensure that the LDAP registry has not been modified using external tools.

HPDMG0754W

The entry was not found. If a user or group is being created, ensure that the Distinguished Name (DN) specified has the correct syntax and is valid. (0x14c012f2)

Explanation
A search of the LDAP registry did not locate the entry.

Administrator response
Ensure that the name specified is correct. If a user or group is being created or imported, ensure that the Distinguished Name (DN) specified has the correct syntax and is valid.

HPDMG0755W

The specified Distinguished Name (DN) does not exist. (0x14c012f3)

Explanation
See message.

Administrator response
Make sure the specified DN is a valid LDAP entry.

HPDMG0756W

Incorrect current password. (0x14c012f4)

Explanation
The correct current password must be provided to be able to change the password.

Administrator response
Retry the change password operation specifying the correct current password.

HPDMG0757W

The Distinguished Name (DN) is already configured as a user. (0x14c012f5)

Explanation
This error can occur when creating or importing a user. It is generated because the DN provided has been successfully created or imported before.

Administrator response
Ensure that the DN specified is correct.

HPDMG0758W

The Distinguished Name (DN) is already configured as a group. (0x14c012f6)

Explanation
This error can occur when creating or importing a group. It is generated because the DN provided has been successfully created or imported before.

Administrator response
Ensure that the DN specified is correct.

HPDMG0759W

The user name already exists in the registry. (0x14c012f7)

Explanation
A user already exists with the user name chosen. If Microsoft Active Directory registry is used, the error may apply to the sAMAccountName, userPrincipalName or the CN attributes of the registry user object.

Administrator response
Specify a different user name.

HPDMG0760W

The group name already exists in the registry. (0x14c012f8)

Explanation
A group already exists with the group name chosen.

Administrator response
Specify a different group name.

HPDMG0761W

The entry referred to by the Distinguished Name (DN) must be a person entry. (0x14c012f9)

Explanation
Security Verify Access validates that the Distinguished Name (DN) provided is the DN of a person entry.

Administrator response
Ensure that the DN specified refers to a person type entry.

HPDMG0762W

The entry referred to by the Distinguished Name (DN) must be a group entry. (0x14c012fa)

Explanation
Security Verify Access validates that the Distinguished Name (DN) provided is the DN of a group (accessGroup, groupOfNames, or groupOfUniqueNames).

Administrator response
Ensure that the DN specified refers to a group type entry.

HPDMG0763E

LDAP is not configured as a registry of users and groups. (0x14c012fb)

Explanation
During configuration of Security Verify Access, LDAP was not chosen as the registry type to store user and group information.

Administrator response
Reconfigure Security Verify Access if the LDAP registry should have been selected.

HPDMG0764E

An internal error has occurred. (0x14c012fc)

Explanation
This error indicates an unexpected condition has occurred. For example, this may be generated if a return code is received from the LDAP server that was unexpected.

Administrator response
Retry the operation. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG0765W

The request made to the LDAP server exceeded the server's configured time limit. (0x14c012fd)

Explanation
The LDAP server can be configured for the maximum amount of time allowed to process a request. If it takes too long to fulfill a particular request, then this error is returned.

Administrator response
Ensure that the LDAP server is configured to allow adequate time to process requests. This time might have to be extended if the server is busy.

HPDMG0766W

The search request exceeded the maximum number of entries the LDAP server is allowed to return. (0x14c012fe)

Explanation
This limit is imposed from two sources. First, the LDAP server has a configurable size limit setting. Second, Security Verify Access has a default size limit of 2048. The effective size limit will be the smaller of the two.

Administrator response
Ensure that the LDAP server is configured to allow the number of entries required to be returned. The Security Verify Access limit can be set using the max-search-size parameter in the [ldap] stanza of the .conf configuration file.

HPDMG0767E

The Distinguished Name (DN) has an invalid syntax. (0x14c012ff)

Explanation
A Distinguished Name (DN) consists of a set of attribute value assertions (for example, o=ibm) separated by commas. Either the DN specified is invalid or a value input when used to construct the DN caused an invalid DN to be constructed.

Administrator response
Ensure the DN syntax is correct.

HPDMG0768E

Unable to login. (0x14c01300)

Explanation
The password or login Distinguished Name (DN) is incorrect.

Administrator response
Ensure that the admin-dn or admin-pwd in the [ldap] stanza of the .conf configuration files have not been modified. If the configuration has been modified or corrupted, restore the configuration from a backup copy or reconfigure.

HPDMG0769E

There were insufficient LDAP access privileges to allow Security Verify Access to create and delete entries in the registry. (0x14c01301)

Explanation
The portion of the LDAP namespace where users and groups are created or maintained must have access contol lists (ACLs) set to permit the Security Verify Access Security Group proper authority. This access is normally set when the policy server is configured.

Administrator response
Ensure that the LDAP server access controls allow the Security Verify Access Security Group to create and delete entries in the namespace.

HPDMG0770E

The settings defined for the entry are invalid (object class violation). (0x14c01302)

Explanation
An attempt to create or update an entry in the LDAP registry failed because it did not agree with the LDAP schema definition. For example, an attribute was given a value larger than the maximum size allowed by the attribute's LDAP schema definition.

Administrator response
Ensure that the Security Verify Access schema is correctly applied. This is normally automatically done when the policy server is configured.

HPDMG0771E

Cannot delete the entry completely because it has unexpected subentries in the LDAP registry. This is usually because the user or group being deleted is a member of another domain. (0x14c01303)

Explanation
An attempt was made to delete an entry in the LDAP namespace. However, the entry contains subentries that cannot be deleted. If a user or group is being deleted, ensure the user or group Distinguished Name (DN) is not a member of another domain.

Administrator response
Security Verify Access is unable to delete the entry. If a user or group is being deleted with the -registry option, check to ensure that the user or group is not a member of another domain and retry the operation.

HPDMG0772W

The entry already exists. (0x14c01304)

Explanation
See message.

Administrator response
Choose a different name or accept the existing entry.

HPDMG0773E

The request failed because the LDAP server is down. (0x14c01305)

Explanation
See message.

Administrator response
Activate the LDAP server, restart Security Verify Access, and retry the operation.

HPDMG0774E

Illegal characters were specified in the LDAP search filter. (0x14c01306)

Explanation
When Security Verify Access attempted a search request, the resulting filter was unacceptable to LDAP.

Administrator response
If a pattern is being specified, ensure that it is syntactically correct. If a user or group name is being specified, ensure that it does not contain special characters that could cause the filter to be invalid.

HPDMG0775E

Not enough memory was available to perform the operation. (0x14c01307)

Explanation
See message.

Administrator response
Restart Security Verify Access and retry the operation.

HPDMG0776E

An error connecting to the LDAP server has occurred. (0x14c01308)

Explanation
A connection could not be established with the configured LDAP server.

Administrator response
Ensure that the LDAP server has the correct configured host name and port number and that the server is active.

HPDMG0777W

The LDAP referral limit was exceeded. (0x14c01309)

Explanation
The LDAP servers can be configured with referrals from one server to another to split the namespace. There is a maximum number of referrals that is followed to locate the final server. This default is 10.

Administrator response
Ensure that the network of LDAP servers using referrals does not exceed the limit.

HPDMG0778E

The SSL initialization failed for connection to the LDAP server. (0x14c0130a)

Explanation
Security Verify Access attempted to create an SSL connection with the LDAP server but the SSL session could not be established.

Administrator response
Ensure that the server's SSL certificate is correct and that the Security Verify Access key file contains a certificate of the Certificate Authority (signer) that can validate the certificate.

HPDMG0779E

An SSL parameter error occurred when connecting to the LDAP server. (0x14c0130b)

Explanation
Security Verify Access attempted to create an SSL connection with the LDAP server but the SSL session could not be established.

Administrator response
Ensure that the server's SSL certificate is correct and that the Security Verify Access key file contains a certificate of the Certificate Authority (signer) which can validate that certificate.

HPDMG0780E

The SSL handshake failed when connecting to the LDAP server. (0x14c0130c)

Explanation
Security Verify Access attempted to create an SSL connection with the LDAP server but the SSL session could not be established.

Administrator response
Ensure that the server's SSL certificate is correct and that the Security Verify Access key file contains a certificate of the Certificate Authority (signer) which can validate that certificate.

HPDMG0781E

SSL failed to establish the requested encryption cipher level when connecting to the LDAP server. (0x14c0130d)

Explanation
Security Verify Access attempted to establish an SSL connection with the LDAP server but was unable to acquire the required cipher.

Administrator response
Configure the LDAP server SSL settings for a lower encryption cipher level and retry the operation.

HPDMG0782E

SSL was not available for connection to the LDAP server. (0x14c0130e)

Explanation
Security Verify Access was configured to use SSL for connection with the LDAP server but the SSL support is not available.

Administrator response
Ensure that the GSKit is properly installed. See the Security Verify Access Base Installation Guide for information to install GSKit.

HPDMG0783E

The SSL Key Database File was not found for connection to the LDAP server. (0x14c0130f)

Explanation
Security Verify Access attempted to open an SSL connection with the LDAP server but could not locate the specified key database file.

Administrator response
Ensure that the configured Key Database File has the correct name and that the permissions allow Security Verify Access to read the file.

HPDMG0784E

The SSL password was not specified for connection to the LDAP server. (0x14c01310)

Explanation
Security Verify Access attempted to open an SSL connection with the LDAP server but no password for the key database file was specified.

Administrator response
Ensure that the correct password is configured for the Security Verify Access key database file.

HPDMG0786E

Unable to sign certificate because of missing attribute definitions in the LDAP schema. (0x14c01312)

Explanation
The LDAP schema for the secCertDN and secCertSerialNumber attributes is missing.

Administrator response
Ensure that LDAP is properly configured and that the Security Verify Access schema has been correctly applied. This is normally automatically done when the policy server is configured.

HPDMG0787E

Unable to sign certificate due to unexpected error (0x*%8.8lx*). (0x14c01313)

Explanation
An unexpected internal processing error has occurred while trying to create an SSL certificate.

Administrator response
Refer to the Security Verify Access error log for more information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG0788E

Unable to sign certificate due to an unexpected error. (0x14c01314)

Explanation
An unexpected internal processing error has occurred while trying to create an SSL certificate.

Administrator response
Refer to the Security Verify Access error log for more information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG0789W

The user Distinguished Name (DN) cannot be created because it already exists. (0x14c01315)

Explanation
This error can occur when creating a user. It is generated because the DN provided already exists in the registry.

Administrator response
You can either choose to delete this DN and retry the operation or use the import command to make the DN specified a Security Verify Access user.

HPDMG0790W

The group Distinguished Name (DN) cannot be created because it already exists. (0x14c01316)

Explanation
This error can occur when creating a group. It is generated because the DN provided already exists in the registry.

Administrator response
You can either choose to delete this DN and retry the operation or use the import command to make the DN specified a Security Verify Access group.

HPDMG0793E

Duplicate member assignment was attempted. No members have been added. (0x14c01319)

Explanation
All members to be added to a group must be new members.

Administrator response
Remove users from the list that are already members of the group.

HPDMG0900E

The Distinguished Name (DN) cannot be determined. (0x14c01384)

Explanation
The specified entry cannot be found on the LDAP server, or more than one exists when only one was expected.

Administrator response
Ensure the resource or resource group name is correct.

HPDMG0901E

Cannot determine the exported suffixes on the LDAP Server. (0x14c01385)

Explanation
The LDAP server encountered an error while performing a suffix search.

Administrator response
Refer to the Security Verify Access error log for more information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG0902E

LDAP server SSL initialization failed. (0x14c01386)

Explanation
Security Verify Access cannot initialize an SSL session with the LDAP server.

Administrator response
Ensure the LDAP server is properly configured and is up and running.

HPDMG0903E

The LDAP server cannot be located. (0x14c01387)

Explanation
Security Verify Access cannot initialize an SSL session with the LDAP server.

Administrator response
Ensure the LDAP server is properly configured and is up and running.

HPDMG0904E

LDAP server bind options cannot be initialized. (0x14c01388)

Explanation
Security Verify Access has encountered bind option errors while attempting to contact the LDAP server.

Administrator response
Refer to the Security Verify Access error log for more information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG0905E

Invalid parameters passed to GSO Management API. (0x14c01389)

Explanation
Invalid parameter data has been provided to the Global Sign-On (GSO) Management API.

Administrator response
Refer to the Security Verify Access error log for more information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG0906E

The configured LDAP server is not correct version. (0x14c0138a)

Explanation
A downlevel version of The LDAP server is configured into Security Verify Access. This can result from upgrading Verify Access without upgrading the LDAP server.

Administrator response
Ensure the supported version of LDAP server is configured into the Security Verify Access environment.

HPDMG0907E

A memory allocation error in the GSO Management API. (0x14c0138b)

Explanation
A error occurredThe Global Sign-On (GSO) Management API attempted to allocate memory.

Administrator response
This is potentially a temporary condition. Attempt to free up memory by closing other running applications. If the problem persists, increase the system memory in the machine

HPDMG0908E

Cannot perform remove operation, because subdirectories exist. (0x14c0138c)

Explanation
An attempt was made to remove Security Verify Access Global Sign-On (GSO) resource object without first removing its subobjects.

Administrator response
Remove the GSO subobjects then retry the operation.

HPDMG0909E

GSO Management API reports that invalid data was specified. (0x14c0138d)

Explanation
Invalid parameter data has been provided to the Global Sign-On (GSO) Management API.

Administrator response
Refer to the Security Verify Access error log for more information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG0910E

Cannot find the member resource. (0x14c0138e)

Explanation
An attempt was made to remove a Global Sign-On (GSO) resource from a resource group, but the resource was not a member.

Administrator response
Ensure that the name of the resource to be removed exists and is a member of the resource group.

HPDMG0911E

Cannot access GSO database. Invalid user name or password. (0x14c0138f)

Explanation
The Security Verify Access policy server attempted to access the Global Sign-On (GSO) database but the identity was not authorized

Administrator response
Ensure that the directory server access control settings have not been altered. The policy server identity, specified in the ivmgrd.conf file, must have the authority to search and make updates to the Global Sign-On (GSO) data.

HPDMG0912E

User not authorized to perform operation. (0x14c01390)

Explanation
The portion of the LDAP namespace where users and groups are created or maintained must have access contol lists (ACLs) set to permit the Security Verify Access Security Group proper authority. This access is normally set when the policy server is configured.

Administrator response
Ensure that the LDAP server access controls allow the Security Verify Access Security Group to access entries in the namespace.

HPDMG0913E

Cannot connect to GSO database LDAP Server. Either the LDAP Server is inactive or busy. (0x14c01391)

Explanation
See text.

Administrator response
Retry this operation when the LDAP Server is available.

HPDMG0914E

GSO database not found on LDAP server. (0x14c01392)

Explanation
The Security Verify Access is unable to locate the Global Sign-On (GSO) objects in the user registry.

Administrator response
Ensure the Security Verify Access Global Sign-On (GSO) definition is properly defined in the user registry. Also, verify the Verify Access is configured properly.

HPDMG0915E

No SSL connection exists between Security Verify Access and the LDAP server. (0x14c01393)

Explanation
Security Verify Access attempted to create an SSL connection with the LDAP server but the SSL session could not be established.

Administrator response
Ensure that the server's SSL certificate is correct and that the Security Verify Access key file contains a certificate of the Certificate Authority (signer) that can validate the certificate.

HPDMG0916E

No account information for GSO resource credential found. (0x14c01394)

Explanation
A request was made to retrieve the account information from a Global Sign-On (GSO) resource credential but none was found.

Administrator response
Either create or modify the resource credential for the specified user to specify the account information (user id and password).

HPDMG0917E

The specified GSO resource credential was not found. (0x14c01395)

Explanation
The Global Sign-On (GSO) resource credential was not found at the LDAP server.

Administrator response
Ensure that the Global Sign-On (GSO) resource credential is specified correctly for the user indicated and that the resource credential type (web or group) is specified correctly. The pdadmin rsrccred list user command can be used to determine the set of defined credentials for the user.

HPDMG0918E

The requested GSO resource was not found. (0x14c01396)

Explanation
The Global Sign-On (GSO) resource was not found at the LDAP server.

Administrator response
Ensure that the Global Sign-On (GSO) resource is specified correctly. The pdadmin rsrc list command can be used to determine the current set of defined resources.

HPDMG0919E

The GSO resource type could not be determined. (0x14c01397)

Explanation
The Global Sign-On (GSO) resource type could not be retrieved from the LDAP server.

Administrator response
Refer to the Security Verify Access error log for more information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG0920E

Resource group not found. (0x14c01398)

Explanation
The specified Global Sign-On (GSO) resource group was not found at the LDAP server.

Administrator response
Ensure that the resource group was specified correctly. The pdadmin rsrcgroup list command can be used to determine the current set of defined resource groups.

HPDMG0921E

The specified user identity was not found. (0x14c01399)

Explanation
The specified user is not known to Security Verify Access.

Administrator response
Specify a user that is defined to Security Verify Access.

HPDMG0922E

The specified user is not a GSO user. (0x14c0139a)

Explanation
The specified user is not configured as a Global Sign-On (GSO) user.

Administrator response
Use pdadmin to configure the user as a Global Sign-On (GSO) user.

HPDMG0923E

Object already exists. (0x14c0139b)

Explanation
The Global Sign-On (GSO) resource, resource group or resource credential already exists.

Administrator response
Either choose a different name for the object being created or delete the existing object and re-create it.

HPDMG0924E

Object not found. (0x14c0139c)

Explanation
The specified Global Sign-On (GSO) resource, resource group or resource credential could not be found.

Administrator response
Ensure that the name of the resource, resource group or resource credential is specified correctly.

HPDMG0925E

An unexpected exception occurred in the GSO Management API. (0x14c0139d)

Explanation
Security Verify Access encountered an unexpected error while processing Global Sign-On (GSO) data.

Administrator response
Check the Security Verify Access error log for additional information. If after re-trying the operation, the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG0931E

The specified user is inactive. (0x14c013a3)

Explanation
The specified user is a defined Security Verify Access user, but is not active.

Administrator response
Ensure the desired user is both an active Security Verify Access user, and a Global Sign-On (GSO) user.

HPDMG0932E

The GSO Management Function is not implemented. (0x14c013a4)

Explanation
Security Verify Access attempted to perform a Global Sign-On (GSO) function which is not supported.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG0937E

LDAP is not enabled in the ivmgrd configuration file. (0x14c013a9)

Explanation
LDAP is not enabled in the ldap stanza of the iv.conf file.

Administrator response
Modify the configuration file to enable LDAP.

HPDMG0942E

The GSO management function returns unknown error. (0x14c013ae)

Explanation
An unknown error has been returned by the Global Sign-On (GSO) Management API

Administrator response
Refer to the Security Verify Access error log for more information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG0943E

Invalid name. (0x14c013af)

Explanation
Security Verify Access invoked the Global Sign-On (GSO) interface with an invalid name.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG0957E

Resource Type (0x14c013bd)

Explanation
none needed

Administrator response
none needed

HPDMG0960E

An LDAP limit (timelimit or sizelimit) was exceeded. (0x14c013c0)

Explanation
See text.

Administrator response
Ensure the LDAP server is correctly configured.

HPDMG0961E

An unrecoverable LDAP error has occurred. (0x14c013c1)

Explanation
See text.

Administrator response
Refer to the Security Verify Access error log for more information. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG1052E

A registry memory allocation failed. (0x14c0141c)

Explanation
An attempt to allocate memory using the registry adapter API returned a NULL pointer.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG1053E

The configuration file is invalid. (0x14c0141d)

Explanation
One of the configuration files (for example, domino.conf) could not be opened or was missing some required information.

Administrator response
Repair or replace the server and/or registry .conf files in the etc subdirectory. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG1054E

A registry input/output error has occurred. (0x14c0141e)

Explanation
The registry server had an error while processing a request.

Administrator response
Verify that the registry server is functioning normally before retrying the operation.

HPDMG1055E

A registry SSL error has occurred. (0x14c0141f)

Explanation
An error occurred during Secure Sockets Layer (SSL) communications with the registry server.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG1056E

A registry initialization error has occurred. (0x14c01420)

Explanation
A registry API call was made with an invalid parameter, or the registry type could not be determined or is not configured correctly.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG1057E

A registry data error has occurred. (0x14c01421)

Explanation
One of several basic registry functions has failed.

Administrator response
Verify that the registry server is functioning normally before retrying the operation.

HPDMG1058E

The user is not defined in the registry. (0x14c01422)

Explanation
The specified user ID was not found in the registry database.

Administrator response
Verify that the user ID is spelled correctly and that it exists in the registry database for the domain to which you are logged in.

HPDMG1059E

Group is not defined in the Registry. (0x14c01423)

Explanation
The specified group ID was not found in the registry database.

Administrator response
Verify that the group ID is spelled correctly and that it exists in the registry database for the domain to which you are logged in.

HPDMG1064E

The group member was not found. (0x14c01428)

Explanation
The group has no members or the specified member was not found in the group.

Administrator response
Verify that the group name and member ID is spelled correctly and that they both exist in the registry database for the domain to which you are logged in.

HPDMG1065E

An invalid user type was specified. (0x14c01429)

Explanation
When the calling program requested a list of users it did not specifiy one of the 3 allowed types.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG1066E

An invalid group type was specified. (0x14c0142a)

Explanation
When the calling program requested a list of groups it did not specifiy one of the 3 allowed types.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG1067E

The Universal Unique Identifier (UUID) was not specified. (0x14c0142b)

Explanation
The UUID used to find a user in the registry was missing from the lookup operation.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG1068E

An invalid group identification or Distinguished Name (DN) was specified. (0x14c0142c)

Explanation
A group operation was attempted for the wrong domain or the group's registryGID value (also known as the DN) was invalid. The DN entered may contain invalid characters or be in an invalid format.

Administrator response
Correct the registry group ID (or DN) that you specified and retry the operation.

HPDMG1069E

An invalid policy identification was specified. (0x14c0142d)

Explanation
A user specific policy that was expected to be in the registry was not found.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG1070E

An invalid resource identification was specified. (0x14c0142e)

Explanation
A resource that was expected to be in the registry was not found.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG1071E

An invalid resource group identification was specified. (0x14c0142f)

Explanation
A resource group that was expected to be in the registry was not found.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG1072E

Invalid resource credentials identification was specified. (0x14c01430)

Explanation
A resource credential that was expected to be in the registry was not found.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG1073E

The user is already defined in the registry. (0x14c01431)

Explanation
A user with the name you chose is already in the registry.

Administrator response
Select another name or a variation for this user.

HPDMG1074E

The group is already defined in the registry. (0x14c01432)

Explanation
A group with the name you chose is already in the registry.

Administrator response
Select another name or a variation for this group.

HPDMG1075E

The policy is already defined in the registry. (0x14c01433)

Explanation
A policy object already exists for the chosen user.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG1076E

The resource is already defined in the registry. (0x14c01434)

Explanation
A resource object already exists with the specified name.

Administrator response
Select another name for the new resource object.

HPDMG1077E

The resource group is already defined in the registry. (0x14c01435)

Explanation
A resource group object with the specified name already exists in the registry.

Administrator response
Select another name for the new resource group object.

HPDMG1078E

The resource credentials are already defined in the registry. (0x14c01436)

Explanation
A resource credential object with the specified name already exists.

Administrator response
Select another name for which to create a resource credential object.

HPDMG1079E

The user registry identification is not unique in the registry. (0x14c01437)

Explanation
More than one user in the registry shares the specified registryID.

Administrator response
Select another user registryID or modify the users to have unique registry IDs.

HPDMG1080E

The group registry identification is not unique in the registry. (0x14c01438)

Explanation
More than one group in the registry shares the specified registryID.

Administrator response
Select another group registryID or modify the groups to have unique registry IDs.

HPDMG1081W

Not all requested users were assigned to group (*%s*). (0x14c01439)

Explanation
There was a problem assigning one or more users to a group.

Administrator response
Make sure the users in the user list are specified correctly.

HPDMG1082W

Not all requested users were removed from group (*%s*). (0x14c0143a)

Explanation
There was a problem removing one or more users from a group.

Administrator response
Make sure the users in the user list are specified correctly.

HPDMG1083W

The domain name already exists. (0x14c0143b)

Explanation
The name that you specified for the new domain already exists in the registry.

Administrator response
Choose another name for the new domain.

HPDMG1084W

The domain name is unknown. (0x14c0143c)

Explanation
The domain name that you specified could not be found in the registry.

Administrator response
Verify the spelling of the name of the domain and retry the command.

HPDMG1085E

The location specified in which to create the management domain does not exist. (0x14c0143d)

Explanation
The location in which to create the management domain that you specified could not be found in the registry.

Administrator response
Verify the location to be used to create the management domain and retry the command.

HPDMG1086W

The domain has been re-created successfully. (0x14c0143e)

Explanation
The domain being created had previously existed and had not been removed from the registry.

Administrator response
Ensure that the administrator intended to re-create a previously deleted domain.

HPDMG1087E

The domain name specified is invalid. (0x14c0143f)

Explanation
The domain name specified is not allowed. Either the name is too long, contains invalid characters, or does not match the Active Directory domain name.

Administrator response
Ensure that the domain name is not too long and that for Active Directory it matches the Active Directory domain name.

HPDMG1088W

The registry client is not available. (0x14c01440)

Explanation
An attempt was made to access a registry type that is not installed.

Administrator response
Make sure the same registry type is configured for all servers.

HPDMG1089W

Multiple registry routing is not supported. (0x14c01441)

Explanation
An attempt was made to use multiple registry routing, which is not a supported function.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG1090W

The registry server is down or cannot be contacted. (0x14c01442)

Explanation
An attempt to contact the registry server failed. Either the server is not up or the communications path to it has been disrupted.

Administrator response
Verify that the registry server is up and functioning normally and that this client can communicate with it. If Active Directory is used as a user registry, an incorrect distinguished name (DN) input (if applicable) also results in this error.

HPDMG1091W

The user does not have the rights to perform requested operation. (0x14c01443)

Explanation
The server has indicated the user does not have the right to perform the requested operation.

Administrator response
Verify that the user whose credentials are being used has the authority to perform the requested operation.

HPDMG1092W

The registry client received a non-SSL communications error when communicating with the registry server. (0x14c01444)

Explanation
A non-SSL communication error occurred between this server and the server that provides the registry service.

Administrator response
Verify that this server and its registry server are configured correctly for non-SSL communications.

HPDMG1093W

No more entries are in the list. (0x14c01445)

Explanation
A program processing a list of registry entries has tried to get an entry beyond the end of the list.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG1094W

The required list parameter is missing from the API call. (0x14c01446)

Explanation
A program failed to provide a list parameter that is required for the API call it made.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDMG1950E

The user is already a member of the group. (0x14c0179e)

Explanation
The Security Verify Access policy server received a request to add a user to a group in which the user was already a member.

Administrator response
No action is required.

HPDMG1951E

The management domain is empty. (0x14c0179f)

Explanation
The Security Verify Access policy server returned an empty value for the domain name.

Administrator response
Ensure that the policy server is configured correctly and is reachable.

HPDMG1952E

The requested command is no longer supported. (0x14c017a0)

Explanation
An attempt was made to use a command that is no longer supported in the installed version of Security Verify Access.

Administrator response
Upgrade your application or revert to the previously installed version of Security Verify Access.

HPDMG1953E

The admin command input data that is required is missing or invalid. (0x14c017a1)

Explanation
The Security Verify Access policy server received a request that contained incomplete or missing input data.

Administrator response
Ensure that all input data required for the admin command is provided.

HPDMG1954E

The requested command is not supported for the registry specified. (0x14c017a2)

Explanation
The Security Verify Access policy server received an administration command that is not supported using the currently configured registry.

Administrator response
Ensure that the administration command is supported by the registry configured for Security Verify Access.

HPDMG2100E

The policy proxy server could not be started (0x*%8.8lx*). (0x14c01834)

Explanation
The policy proxy server encountered an error during initialization.

Administrator response
Check pdmgrproxyd.log for additional information.

HPDMS0406E

Could not read from rule file *%s* (0x14c52196)

Explanation
The specified rule file could not be opened or read.

Administrator response
Ensure that the specified rule file exists on the system and that the user who invoked pdadmin has read permission on the file.

HPDMS0412E

Invalid argument (0x14c5219c)

Explanation
An invalid argument was passed to a library routine that accesses a non-LDAP registry.

Administrator response
Ensure that all arguments supplied to the command line or programming interface are valid.

HPDMS0416E

Unknown internal exception (0x14c521a0)

Explanation
This typically means that there is inter- or intra-process contention for access to the policy database.

Administrator response
Stop and restart all of the Security Verify Access servers running on the system that exhibits the error. If the problem persists, increase the per-process limits of system resources (available threads, available open file handles, and so forth), reboot the system, and restart the Security Verify Access servers.

HPDMS0429E

Invalid command (0x14c521ad)

Explanation
The Security Verify Access policy server has received a command it does not recognize. This may mean that the server is incompatible with the client.

Administrator response
Ensure the Security Verify Access policy server supports the release level of the clients.

HPDMS0461E

Extract of entry *%s* from stanza *%s* in configuration file *%s* failed (0x14c521cd)

Explanation
The specified entry could not be found in the specified stanza in the configuration file.

Administrator response
Ensure that the entry, stanza, and configuration file have been specified correctly.

HPDMS0462E

Entry does not exist (0x14c521ce)

Explanation
The specified entry could not be found in the specified stanza in the configuration file.

Administrator response
Ensure that the entry, stanza, and configuration file have been specified correctly.

HPDMS0463E

Extract of stanza *%s* from configuration file *%s* failed (0x14c521cf)

Explanation
The specified stanza could not be found in the configuration file.

Administrator response
Ensure that the stanza and configuration file have been specified correctly.

HPDMS0465E

The write operation to the configuration file *%s* failed with error code *%d*. (0x14c521d1)

Explanation
The specified configuration file could not be written to.

Administrator response
Ensure that the user who invoked pdconf has write permission on the configuration file.

HPDMS0466E

Can not retrieve information from the ldap.conf configuration file. (0x14c521d2)

Explanation
Required information could not be read from the %PD_HOME%\etc\ldap.conf file.

Administrator response
Ensure that the ldap.conf configuration file exists and is not corrupted. If the file is missing or corrupted, then unconfigure the Security Verify Access Runtime component and reconfigure.

HPDMS4047E

Non-local authentication (login) is required to perform this operation (0x14c52fcf)

Explanation
For security reasons, most Security Verify Access administration operations require an authenticated session with the Security Verify Access policy server.

Administrator response
Login using the 'login' subcommand and retry the operation. Do not use the login -l option.

HPDMS4061E

Local authentication (local login) is required to perform this operation (0x14c52fdd)

Explanation
For security reasons, most Security Verify Access administration operations require an authenticated session to perform local tasks.

Administrator response
Login using the 'login -l' subcommand and retry the operation.

HPDMS4068E

The specified network IP address is not in a valid IPv4 address format. (0x14c52fe4)

Explanation
The network IP address specified is not in one of the industry standard formats permitted for IPv4 addresses. See the Security Verify Access documentation for further information regarding IPv4 formats.

Administrator response
Specify the address in a valid IPv4 format

HPDMS4069E

The specified netmask IP address is not in a valid IPv4 address format. (0x14c52fe5)

Explanation
The netmask IP address specified is not in one of the industry standard formats permitted for IPv4 addresses. See the Security Verify Access documentation for further information regarding IPv4 formats.

Administrator response
Specify the address in a valid IPv4 format

HPDMS4070E

The specified network IP address is not in a valid IPv6 address format. (0x14c52fe6)

Explanation
The network IP address specified is not in one of the industry standard formats permitted for IPv6 addresses. Alternatively, on Win2k clients, IPv6 addresses cannot be specified since IPv6 addresses are not supported by this platform. See the Security Verify Access documentation for further information regarding IPv6 formats.

Administrator response
Specify the IP address in a valid IPv6 format. For Win2k clients, specify an IPv4 address or use an alternative client platform to specify the IPv6 address.

HPDMS4071E

The specified netmask IP address is not in a valid IPv6 address format. (0x14c52fe7)

Explanation
The netmask IP address specified is not in one of the industry standard formats permitted for IPv6 addresses. Alternatively, on Win2k clients, IPv6 addresses cannot be specified since IPv6 addresses are not supported by this platform. See the Security Verify Access documentation for further information regarding IPv6 formats.

Administrator response
Specify the IP address in a valid IPv6 format. For Win2k clients, specify an IPv4 address or use an alternative client platform to specify the IPv6 address.

HPDMS4072E

The specified network and netmask IP addresses must both be in IPv4 or IPv6 address formats. (0x14c52fe8)

Explanation
The network IP address was specified in IPv4 or IPv6 format and the netmask address was not specified in the same format. Both IP addresses must be specified in the same industry standard format for either IPv4 or IPv6 addresses. See the Security Verify Access documentation for further information regarding IPv4 and IPv6 formats.

Administrator response
Specify the network and netmask addresses using the same IP address format.

HPDMS4073E

The network or netmask IP address was specified as zero. (0x14c52fe9)

Explanation
The network IP address or netmask IP address was specified using zeros. See the Security Verify Access documentation for further information regarding IPv4 and IPv6 formats.

Administrator response
Specify the network and netmask addresses as valid, non-zero addresses.

HPDMS4074E

The binary AND of network and netmask addresses must be non-zero. (0x14c52fea)

Explanation
The network IP address and netmask IP address are combined using a bitwise AND. The resulting masked network address cannot be zero. See the Security Verify Access documentation for further information regarding IPv4 and IPv6 formats.

Administrator response
Specify the network and netmask addresses that do not result in a zero masked network when combined.

HPDMS4075E

Incorrect account-expiry-date. Acceptable dates are between the current date and 2035-12-31-23:59:59. (0x14c52feb)

Explanation
The date specified was earlier than the current date or greater than 2035-12-31-23:59:59.

Administrator response
Specify an valid account-expiry-date for the policy. Acceptable values can be the current date or later but not greater than 2035-12-31-23:59:59

HPDMS4076E

Incorrect max-return value specified. Use a value that is greater than or equal to zero. Use zero to return all found. (0x14c52fec)

Explanation
The max-return value that was specified was not an integer equal to or greater than 0.

Administrator response
Specify a valid integer value for the max-return argument. Use a value that is greater than or equal to 0. Use zero to return all entries that are found.

HPDMS4077E

Name cannot begin with a space character. (0x14c52fed)

Explanation
The first character of the name was a space character.

Administrator response
Specify a valid name without leading space characters. For string names, ensure there are no space characters after the opening quotation mark.

HPDMS4078E

User specified does not have an entry in the ACL specified. (0x14c52fee)

Explanation
The user specified does not exist for the ACL specified.

Administrator response
No action required. If desired, specify a different user or a different ACL.

HPDMS4079E

Group specified does not have an entry in the ACL specified. (0x14c52fef)

Explanation
The group specified does not exist for the ACL specified.

Administrator response
Specify a different group or a different ACL.

HPDMS4080W

The any-other entry does not exist for the ACL specified. (0x14c52ff0)

Explanation
See message.

Administrator response
No action required.

HPDMS4081W

The unauthenticated entry does not exist for the ACL specified. (0x14c52ff1)

Explanation
See message.

Administrator response
No action required.

HPDMS4082E

ACL name contains characters that are not allowed. (0x14c52ff2)

Explanation
The ACL name specified contains one or more characters that are not allowed in ACL names.

Administrator response
Specify an ACL name that contains valid characters. For information about characters that are valid in ACL names, see the " IBM Security Verify Access for Web Administration Guide".

HPDMS4083E

Value for the 'type' option is not an integer greater than or equal to zero. (0x14c52ff3)

Explanation
See message.

Administrator response
Specify an integer value that greater than or equal to zero.

HPDMS4084E

Value for the 'ispolicyattachable' option is not a valid Boolean value. (0x14c52ff4)

Explanation
See message.

Administrator response
Specify a valid Boolean value. Acceptable values are 'yes','no','true','false','1','0', 'on', or 'off'.

HPDMS4085E

Value is not an integer greater than or equal to zero. (0x14c52ff5)

Explanation
See message.

Administrator response
Specify an integer value greater than or equal to zero.

HPDMS4086E

Value specified for option 'rsrctype' is not 'web' or 'group'. (0x14c52ff6)

Explanation
See message.

Administrator response
Specify a valid value for the rsrctype parameter. Valid values include 'web' and 'group'.

HPDPZ0001E

Exception: *%s* File: *%s %d* Error: *%d*No text has been defined for this exception. (0x35e51001)

Explanation
An exception was caught that has no appropriate text to display. This is an internal error.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0002E

Memory allocation failure. (0x35e51002)

Explanation
A request to allocate memory failed.

Administrator response
Ensure that sufficient disk space and memory are available in the system. If restarting the server does not resolve the problem, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0003E

Unexpected error opening XPG4 converter for codepage *%s* to *%s* conversion. The iconv_open error code is *%d*. (0x35e51003)

Explanation
The required codepage tables could not be located.

Administrator response
On the Windows platforms, ensure that LOCPATH and LANG environment variables are set correctly.

HPDPZ0004E

Unexpected error from pthread_mutex_init(). The error code is *%d*. (0x35e51004)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0005E

Unexpected error from pthread_mutex_destroy(). The error code is *%d*. (0x35e51005)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0006E

Unexpected error from pthread_mutex_lock(). The error code is *%d*. (0x35e51006)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0007E

Unexpected error from pthread_mutex_unlock(). The error code is *%d*. (0x35e51007)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0008E

Unexpected error from pthread_cond_init(). The error code is *%d*. (0x35e51008)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0009E

Unexpected error from pthread_cond_destroy(). The error code is *%d*. (0x35e51009)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0010E

Unexpected error from pthread_cond_wait(). The error code is *%d*. (0x35e5100a)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0011E

Unexpected error from pthread_cond_signal(). The error code is *%d*. (0x35e5100b)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0012E

This function is not supported on this platform. (0x35e5100c)

Explanation
An attempt was made to use an API that is not supported on the current operating system.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0013E

Unexpected error from Windows RegOpenKeyEx(). Opening of the registry key *%s* failed with error *%s*. (0x35e5100d)

Explanation
An attempt to open a Windows registry key has failed.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0014E

Unexpected error from Windows RegQueryValueEx(). Reading of the value *%s* failed with error *%s*. (0x35e5100e)

Explanation
An attempt to read a value from a Windows registry key has failed.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0015E

Object is not cloneable. (0x35e5100f)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0016E

Unexpected error from pthread_attr_init(). The error code is *%d*. (0x35e51010)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0017E

Unexpected error from pthread_attr_setdetachstate(). The error code is *%d*. (0x35e51011)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0018E

Unexpected error from pthread_create(). The error code is *%d*. (0x35e51012)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0019E

Unexpected error from pthread_attr_destroy(). The error code is *%d*. (0x35e51013)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0020E

An unknown exception was caught. No exception information is available. (0x35e51014)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0021E

Unexpected error from pthread_join(). The error code is *%d*. (0x35e51015)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0022E

Unexpected error from pthread_cond_timedwait(). The error code is *%d*. (0x35e51016)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0023E

A function or method was called with an invalid parameter. (0x35e51017)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0024E

Unexpected error from WSAStartup(). The error code is *%d*. (0x35e51018)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0025E

Unexpected error from gethostname(). The error code is *%d*. (0x35e51019)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0026E

Unexpected error from gethostbyname(). The error code is *%d*. (0x35e5101a)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0027E

Unexpected error from pthread_cond_broadcast(). The error code is *%d*. (0x35e5101b)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0028E

The configuration file *%s* is missing the required attribute *%s* in stanza *%s*. (0x35e5101c)

Explanation
A required attribute is missing probably because the configuration file is damaged or was modified incorrectly.

Administrator response
Provide a valid value for the attribute or reconfigure the application.

HPDPZ0029E

Unexpected error from pthread_key_create(). The error code is *%d*. (0x35e5101d)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0030E

Unexpected error from pthread_setspecific(). The error code is *%d*. (0x35e5101e)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0031E

The requested function is not implemented. (0x35e5101f)

Explanation
An attempt was made to use an API that is not implemented.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0032E

An unexpected lock state was detected. The current lock state is *%s*. (0x35e51020)

Explanation
An internal coding error has occurred. The current state of the resource lock is not valid for the requested operation.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0033E

An unexpected error was received when trying to obtain a process lock. The error code is *%d*. (0x35e51021)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0034E

An unexpected error was received when trying to release a process lock. The error code is *%d*. (0x35e51022)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0035E

A read operation failed for a process lock. The error code is *%d*. (0x35e51023)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0036E

A write operation failed for a process lock. The error code is *%d*. (0x35e51024)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0037E

A create operation failed for a process lock. The error code is *%d* and the lock file name is *%s*. (0x35e51025)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0038E

A close operation failed for a process lock. The error code is *%d* and the lock file name is *%s*. (0x35e51026)

Explanation
An internal coding error has occurred.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0039E

The configuration file *%s* has an invalid value *%s* for key *%s* in stanza *%s*. (0x35e51027)

Explanation
An attribute value is incorrect.

Administrator response
Provide a valid value or reconfigure the application.

HPDPZ0040E

The configuration file *%s* has an invalid numeric value *%s* for key *%s* in stanza *%s*. (0x35e51028)

Explanation
A numeric attribute has a non-numeric value. The configuration file might be damaged or was modified incorrectly.

Administrator response
Provide a valid value or reconfigure the application.

HPDPZ0041E

The configuration file *%s* has an invalid boolean value *%s* for key *%s* in stanza *%s*. (0x35e51029)

Explanation
A boolean attribute has an invalid value. The configuration file might be damaged or was modified incorrectly.

Administrator response
Provide a valid value or reconfigure the application.

HPDPZ0042E

The iterator for configuration file *%s* is in an invalid state for the operation. (0x35e5102a)

Explanation
The current state of the iterator does not permit the attempted access.

Administrator response
This is an internal error. Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0043E

An access function failed for configuration file *%s*. The access function was *%s* and return code was *%d*. (0x35e5102b)

Explanation
An Input/Output operation could not be performed on a configuration file. The daemon process might not have proper permissions to access the file.

Administrator response
Ensure that the file and directory permissions permit program access to the file.

HPDPZ0044E

The configuration file *%s* contains invalid data at line *%d*.Data: *%s*. (0x35e5102c)

Explanation
The specified configuration file contains valid data. This might be caused by a duplicate stanza name in the file.

Administrator response
Correct the invalid data or reconfigure the application.

HPDPZ0045E

The AMTISDIR environment variable is not set. (0x35e5102d)

Explanation
The AMTISDIR environment variable was not available to the application.

Administrator response
Ensure that application is properly configured.

HPDPZ0046E

The tis_mblen() function failed. Probable cause is an invalid multi-byte character. (0x35e5102e)

Explanation
The function returned -1 if it could not determine the length of the multibyte character.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0047E

The handle for codeset *%s* could not be created.The AMTISDIR environment variable is *%s*. (0x35e5102f)

Explanation
The function failed. The AMTISDIR, LC_CODE or LANG might not be correct.

Administrator response
Verify that the product is properly installed and configured.

HPDPZ0048E

The function or operation is not supported. (0x35e51030)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0049E

A string could not be converted from the local codeset *%s* to UTF-8. (0x35e51031)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0050E

A string could not be converted from UTF-8 to the local codeset *%s*. (0x35e51032)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0051E

Shared Library error (*%s*) *%d*. *%s* (0x35e51033)

Explanation
An error occurred loading or unloading a shared library. Verify installation, permissions and path settings to ensure that the library can be located.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0052E

Shared Library resolve error (*%s*:*%s*) *%d*. *%s* (0x35e51034)

Explanation
An error occurred resolving a symbol in a shared library. Verify installation to determine that the correct library is being loaded.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0053E

Unexpected end of file encounted while reading *%s*. (0x35e51035)

Explanation
An end of file character was unexpectedly encountered while reading a file. Verify that the file is valid.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0054E

Internal error encountered while loading Java property file *%s*. (0x35e51036)

Explanation
An internal state error was encountered while loading a Java property file. The file was not loaded.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDPZ0055E

The configuration file *%s* contains a duplicate stanza entry at line *%d*.Stanza: *%s*. (0x35e51037)

Explanation
The specified configuration file contains a duplicate stanza entry.

Administrator response
Remove the duplicate stanza entry.

HPDRA0001E

Trace is not initialized. (0x308fa001)

Explanation
An internal error occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDRA0002E

Trace initialization failed. (0x308fa002)

Explanation
An internal error occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDRA0004E

Component already exists. (0x308fa004)

Explanation
An internal error occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDRA0005E

Component not found. (0x308fa005)

Explanation
The specified trace component is not a known component.

Administrator response
Retry the operation specifying a valid component.

HPDRA0006E

Component handle is invalid. (0x308fa006)

Explanation
An internal error occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDRA0007E

Trace level is invalid. (0x308fa007)

Explanation
An invalid trace level has been specified.

Administrator response
Specify a valid trace level and retry the operation.

HPDRA0008E

Component name is invalid. (0x308fa008)

Explanation
The specified component name does not conform to the rules for a valid component name.

Administrator response
Specify a valid component name. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDRA0010E

The specified destination is invalid. (0x308fa00a)

Explanation
The log agent specified is invalid.

Administrator response
Specify a valid log agent and retry the operation.

HPDRA0011W

Serviceability component *%s* could not be registered for dynamic trace: 0x*%x*: *%s* (0x308fa00b)

Explanation
A serviceability component could not be registered for dynamic trace for the reason indicated. This condition is benign and does not stop operation of the product however trace points for the identified component can not be activated dynamically.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDRA0064E

Unable to perform requested task: 0x*%x*: *%s* (0x308fa040)

Explanation
The task could not be performed for the indicated reason.

Administrator response
Correct the problem indicated and retry the operation.

HPDRA0065E

The requested task is incomplete or malformed. (0x308fa041)

Explanation
The task command is badly formed.

Administrator response
Specify a valid task command and retry the operation.

HPDRA0066E

The requested task does not exist. (0x308fa042)

Explanation
A task name was specified that is not handled by this server.

Administrator response
Specify a valid task name and retry the operation.

HPDRA0068E

The specified destination (*%s*) is invalid. (0x308fa044)

Explanation
The log agent specified is invalid.

Administrator response
Correct the log agent specification and retry the operation.

HPDRA0192E

Statistics gathering is already registered for this component. (0x308fa0c0)

Explanation
An internal error occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDRA0193E

Statistics gathering is not registered for this component. (0x308fa0c1)

Explanation
No statistics gathering capability is available for the specified component.

Administrator response
Only specify components with statistics capabilities with statistics tasks.

HPDRA0194E

Statistics gathering for this component is already on. (0x308fa0c2)

Explanation
An internal error occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDRA0195E

Statistics gathering for this component is always on. (0x308fa0c3)

Explanation
An internal error occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDRA0196E

Statistics gathering for this component is not on. (0x308fa0c4)

Explanation
An internal error occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDRA0197E

The structure containing statistics gathering functions is invalid. (0x308fa0c5)

Explanation
An internal error occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDRA1091E

The specified component has not been registered with the framework. (0x308fa443)

Explanation
A command has been received for which there is no registered component.

Administrator response
Re-issue the command with a valid component.

HPDRA1093E

The component is already writing transactional information to a file. (0x308fa445)

Explanation
An attempt was made to start the transaction logging while it was already running.

Administrator response
Stop the component transaction logging before issuing the start command.

HPDRA1094E

A supplied transaction record is larger than the specified maximum file size: *%d* (0x308fa446)

Explanation
A transaction record was received which exceeded the specified maximum file size.

Administrator response
Increase the maximum size of the transaction log file.

HPDRA1095E

The filename must not contain any path information. (0x308fa447)

Explanation
A base path for the transaction log files has been statically configured and as such the supplied file name should not contain any path information.

Administrator response
Specify the file name with no path information.

HPDRG0100E

The operation in the Active Directory registry for *%s* failed with return error *%lx*. (0x16b48064)

Explanation
An unknown Active Directory user registry error has occurred.

Administrator response
Retry the failing operation. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDRG0101E

The user password violates the Active Directory user password policies. (0x16b48065)

Explanation
Make sure that the specified password conforms to the password policies and/or complexity requirements of the Active Directory domain controller. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

Administrator response
This password may violate one of the Active Directory general password policies or the password complexity requirements.

HPDRG0102E

An invalid user name or distinguished name (DN) was presented to Security Verify Access. The user name or DN may contain incorrect information, invalid characters or violates a registry user name limitation. (0x16b48066)

Explanation
If Security Verify Access is configured using Active Directory multiple domains, the username or distinguished name may belong to different domains or the domain suffix doesn't exist or is unreachable.

Administrator response
Check the user name and DN information and try again. For Active Directory user registry, note that a "." as the 20th character of the user name is not allowed.

HPDRG0103E

The specified group is a dynamic group and dynamic group membership cannot be modified. (0x16b48067)

Explanation
Use the tools or utilities provided with the Microsoft Active Directory server product to manage a dynamic group.

Administrator response
The specified group is a dynamic group in which its membership is determined by its LDAP query filter . Security Verify Access can use dynamic groups but cannot create or manage them. Use the tools or utilities provided with the directory server product to manage the group.

HPDRG0104E

The specified group is a registry dynamic group and Security Verify Access dynamic group support is not enabled. (0x16b48068)

Explanation
Must enable dynamic group support in Security Verify Access in order to use registry dynamic group.

Administrator response
Use the padmin command to modify the configuration file to enable dyanmic group support. Restart server service and retry.

HPDRG0105W

Unable to remove Security Verify Access meta data from Active Directory domain *%s*. Either the data doesn't exist in the Active Directory domain or this domain can not be contacted. (0x16b48069)

Explanation
Either the Active Directory domain is no longer existed or is unreachable or the data doesn't exist in the specified Active Directory domain.

Administrator response
To ensure that no Security Verify Access data is left behind after it is unconfigured, manually delete the Security Verify Access data from the domain once it's available. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDRG0107E

The value of the userPrincipalName in the Active Directory registry is not unique. Duplicate userPrincipalName values are not allowed to be used for the Security Verify Access user or policy ID. (0x16b4806b)

Explanation
There may exist more than one user in the registry with the same userPrincipalName. Security Verify Access requires the userPrincipalName attribute of the registry user object to be unique, otherwise it can cause unexpected results for Security Verify Access operations.

Administrator response
Duplication of the userPrincipalName must be resolved before using it as an object ID in Security Verify Access or choose a different object ID.

HPDRG0108E

The Active Directory Global Catalog server may be down or unreachable. The Global Catalog is required to be up and reachable from the Security Verify Access configured Active Directory domain. (0x16b4806c)

Explanation

The Global Catalog server may be down or unreachable by the Security Verify Access configured Active Directory Domain.

Administrator response

Ensure the Global Catalog server is up and/or check the firewall to ensure connections between the Global Catalog server and the Active Directory domain/client are allowed.

HPDRG0109W

Unable to migrate user *%s* to the alternate userPrincipalName/e-mail format. Microsoft Active Directory Registry error: 0x*%x*. (0x16b4806d)

Explanation

Unable to modify registry data for the user. Security Verify Access blade server identity might not have the privilege to modify registry user data.

Administrator response

Make sure the Security Verify Access blade server identity has the administrative privilege to modify user if it's desired and the Microsoft returned error is access denial. Otherwise, migration is done at a later time.

HPDRG0150E

The registry object could not be found. (0x16b48096)

Explanation

See message.

Administrator response

Change the supplied DN to that of an existing registry object.

HPDRG0151E

Unable to load the IBM Directory client library. (0x16b48097)

Explanation

Security Verify Access could not be able to locate and dynamically load the IBM Directory client library in order to use the LDAP client to communicate with the Microsoft Active Directory server.

Administrator response

Ensure that the IBM Directory client is installed and has the correct permissions to allow Security Verify Access to load the library.

HPDRG0152W

Unable to contact the Policy Server to create the registry handle. The Policy Server may be down. (0x16b48098)

Explanation

Blade Servers that use a LDAP client to communicate with Active Directory servers require the Policy Server to be up in order to perform the registry write operation. The Policy Server may currently be down.

Administrator response

Make sure that the Policy Server is up and running. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDRG0153E

Either Secure Socket Layer (SSL) support is not enabled or the SSL key file or key file password are missing or incorrect. If the 'change user password using LDAP APIs' option is enabled, SSL is required to be enabled with a valid key file and key file password. (0x16b48099)

Explanation

Either Secure Socket Layer (SSL) is not enabled or SSL key file and/or key file password are missing. Change user passwords using LDAP APIs requires SSL to be enabled with a valid key file and key file password.

Administrator response

Check to see if SSL is enabled and ensure the key file and key file password are valid.

HPDRG0154E

The Active Directory Global Catalog server hostname(s) is either missing or incorrect. The hostname(s) must be specified and reachable when the e-mail/UPN support is enabled. (0x16b4809a)

Explanation

The Global Catalog server hostname is required and must be available when the e-mail/UPN format ID support is enabled.

Administrator response

Mofify the registry configuration file and try again.

HPDRG0200E

The specified group is a dynamic group and cannot be modified. (0x16b480c8)

Explanation

The specified group is a dynamic group in which its membership is specified as a filter. Security Verify Access can use dynamic groups but cannot create or manage them. Use the tools or utilities provided with the directory server product to manage the group.

Administrator response

Use the tools or utilities provided with the directory server product to manage a dynamic group.

HPDRG0201E

Error code 0x*%x* was received from the LDAP server. Error text: *%s*. (0x16b480c9)

Explanation
Security Verify Access attempted to perform a request to the LDAP server and received an unexpected error code. The error code returned to Security Verify Access from the LDAP server is displayed in hexadecimal and error text describing the code is displayed.

Administrator response
Use the tools or utilities provided with the directory server product to examine the error logs of the LDAP server for possible additional information. The documentation included with the LDAP server being used, should have additional information for possible causes for error codes. If the error code and error text indicate a problem with Secure Socket Layer (SSL) initialization, be sure that the correct SSL Key Database (sometimes referred to as a "keyring" or "keyfile"), password and label are configured. Also ensure that the SSL Key Database file has read and write permission for the process attempting to establish an SSL connection to the LDAP server. If, after retrying the operation, the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDRG0202E

Unable to load the IBM Directory client library. The LDAP registry cannot be initialized. (0x16b480ca)

Explanation
To use the LDAP registry, Security Verify Access must locate and dynamically load the IBM Directory client and it could not.

Administrator response
Ensure that the IBM Directory client is installed and has the correct permissions to allow Security Verify Access to load the library.

HPDRG0203E

Unable to load the Access Control Information dynamic library. The LDAP registry cannot be initialized. (0x16b480cb)

Explanation
The Generic LDAP Access Control Information dynamic library has been configured in the ldap.conf configuration file and therefore Security Verify Access must dynamically load the library and it could not.

Administrator response
Ensure that the Access Control Information dynamic library is configured properly, installed and has the correct permissions to allow Security Verify Access to load the library. If the Access Control Information dynamic library is not required, unconfigure it by modifying the ldap.conf configuration file and comment out the external-aci-libpath parameter.

HPDRG0204E

The LDAP server is an IBM Tivoli Directory Server proxy and the required cn=itamproxy container is missing. The Policy Server cannot be configured. (0x16b480cc)

Explanation

Security Verify Access attempted to configure the Policy Server but the LDAP server being used is an IBM Tivoli Directory Server proxy. When the proxy server is used, a container called cn=itamproxy is required to exist on the proxy. This required container was not found.

Administrator response

Use the tools provided with the directory server proxy to create a partition called cn=itamproxy and instantiate the container object on the back-end server. See the Security Verify Access documentation for information about setting up and configuring the proxy server for use with Security Verify Access. Also ensure that the LDAP administration DN identity being used has sufficient authority to create LDAP objects on the back-end server(s) being used. The LDAP administration DN identity should usually be a member of the global administration group (ex. cn=manager,cn=ibmpolicies). If, after retrying the operation, the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDRG0205E

The LDAP server is an IBM Tivoli Directory Server proxy. The requested action cannot be performed with a proxy server. (0x16b480cd)

Explanation

Security Verify Access attempted to perform an action but the LDAP server being used is an IBM Tivoli Directory Server proxy. The proxy server has some restrictions about the set of LDAP actions which can be performed. For example, schema cannot be applied, Access Control Lists (ACLs) cannot be set and the partition object cannot be modified through the proxy.

Administrator response

See the Security Verify Access documentation for information about setting up and configuring the proxy server for use with Security Verify Access. Also ensure that the LDAP administration DN identity being used has sufficient authority to create LDAP objects on the back-end server(s) being used. The LDAP administration DN identity should usually be a member of the global administration group (ex. cn=manager,cn=ibmpolicies). If, after retrying the operation, the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDRG0206E

The secAuthority=Default suffix is required but was not found on the LDAP server. The requested operation cannot be performed. (0x16b480ce)

Explanation

Security Verify Access attempted to create the management domain but the required LDAP suffix (secAuthority=Default) was not found.

Administrator response

See the Security Verify Access documentation for information about setting up and configuring the LDAP server for use with Security Verify Access. Ensure that the secAuthority=Default suffix has been created and that the LDAP server has been restarted to allow the suffix to be used.

HPDRG0207W

The LDAP server is an IBM Tivoli Directory Server and is running in configuration only mode. Security Verify Access will not be able to operate normally with the LDAP server in this mode. (0x16b480cf)

Explanation

The LDAP server is an IBM Tivoli Directory Server and the server is currently running in configuration only mode. In this mode, most normal LDAP operations (such as update) cannot be performed. Since many LDAP operations which Security Verify Access performs are not possible, Security Verify Access will not be able to operate normally until the LDAP server is configured properly and restarted in normal mode.

Administrator response

View the IBM Tivoli Directory Server error logs and correct any identified errors which prevent the LDAP server from starting in normal mode. See the IBM Tivoli Directory Server documentation for the location of the error log and information for configuring the server properly. Once the conditions have been corrected, restart the LDAP server in normal mode and restart Security Verify Access.

HPDRG0208E

The *%s* suffix is required but was not found on the LDAP server. The requested operation cannot be performed. (0x16b480d0)

Explanation

Security Verify Access attempted to create the management domain but the required LDAP suffix was not found.

Administrator response

See the Security Verify Access documentation for information about setting up and configuring the LDAP server for use with Security Verify Access. Ensure that the suffix has been created and that the LDAP server has been restarted to allow the suffix to be used.

HPDRG0209E

Ensure the LDAP administrator is a member of the CN=Administrators group of the partition. (0x16b480d1)

Explanation

Security Verify Access attempted to create the management domain but the required LDAP suffix was not found.

Administrator response

See the Security Verify Access documentation for information about setting up and configuring the ADAM server for use with Security Verify Access. Ensure that the suffix has been created and that the LDAP administrator has the authority to manage the partition.

HPDRG0210E

The requested operation cannot be performed. Ensure SSL has been configured with the ADAM instance or the ADAM SSL requirement for password operations has been disabled. (0x16b480d2)

Explanation

Security Verify Access could not perform a password operation with the ADAM registry. By default, ADAM requires an SSL connection for any password operation or the SSL requirement to be disabled on the ADAM instance.

Administrator response
See the Security Verify Access documentation for information about setting up and configuring the ADAM server for use with Security Verify Access.

HPDRG0211E

The LDAP server reports a naming violation. Ensure the distinguished name (DN): *%s* is allowed by the LDAP server schema. (0x16b480d3)

Explanation
Security Verify Access could not perform the requested operation because the LDAP server did not allow the DN used in the operation. The DN may not be allowed because the LDAP server schema is not configured to allow the DN containment or the RDN values are not defined.

Administrator response
See the Security Verify Access documentation for information about setting up and configuring the LDAP server for use with Security Verify Access.

HPDRG0212E

The IBM Tivoli Directory Server LDAP client does not provide the required function to support the ssl-compliance setting. (0x16b480d4)

Explanation
Security Verify Access could not enable secure connection compliance options within the LDAP client because the LDAP client does not support them. These options were introduced in IBM Tivoli Directory Server 6.3 Feature Pack 2.

Administrator response
Ensure the prerequisite version of the IBM Tivoli Directory Server client is installed on the Security Verify Access system.

HPDRG0213E

The ldap.conf file contains duplicate 'server' entries under the '[backend-servers]' stanza. (0x16b480d5)

Explanation
The values for the 'server' entries under the '[backend-servers]' stanza must be unique.

Administrator response
Remove the duplicate 'server' entry and restart the server.

HPDRG0214E

The ldap.conf file contains a 'suffix' value of '*%s*' under the '[*%s*]' stanza that is not unique. (0x16b480d6)

Explanation
The values for the 'suffix' entries under the '[server:<id>]' stanzas must be unique for all servers including the primary LDAP server.

Administrator response
Remove the duplicate 'suffix' value and restart the server.

HPDRG0215E

The ldap.conf file stanza '[*%s*]' must contain at least one 'suffix' value. (0x16b480d7)

Explanation
At least one 'suffix' value must be provided under the '[server:<id>]' stanzas.

Administrator response
Add at least one 'suffix' value to the [server:<id>] stanza and restart the server.

HPDRG0250E

A user that you tried to add to a group is already a member of that group (0x16b480fa)

Explanation
Users that are already members of a group cannot be added a second time.

Administrator response
Use the pdadmin 'group show-members' command to see the current group membership. Avoid attempts to add those members a second time.

HPDRG0251E

A user registry request to the Domino database failed with return code *%lx*. (0x16b480fb)

Explanation
The Domino server may be down, the Domino server may be stopped, or the server is unreachable over the network.

Administrator response
Verify that the Domino server is functioning normally. This can be accomplished by temporarily starting the Notes client application and verifying that the Notes name and address book is accessible.

HPDRG0252E

The Domino error message is: *%s* (0x16b480fc)

Explanation
The Domino server may be down, the Domino server may be stopped, or the server is unreachable over the network.

Administrator response
Refer to the Lotus Notes or Domino documentation for more information.

HPDRG0300E

Memory allocation failure. (0x16b4812c)

Explanation
A memory allocation request issued by the amldif2v6 program failed.

Administrator response
Ensure that sufficient disk space and memory are available in the system. If rerunning the amldif2v6 program does not resolve the problem, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDRG0301E

The amldif2v6 program has experienced an internal error caused by the failure of a system call. (*%s*, rc=*%d*) (0x16b4812d)

Explanation
The amldif2v6 program experienced an internal error caused by the failure of a system call.

Administrator response
Ensure that sufficient disk space and memory are available in the system. If rerunning the amldif2v6 program does not resolve the problem, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDRG0302E

The amldif2v6 program has experienced an internal error caused by an unusable input LDIF file. (0x16b4812e)

Explanation
While processing the input LDIF file, the amldif2v6 program experienced an internal processing error caused by an unusable input LDIF file.

Administrator response
Ensure that the input LDIF file was generated using one of the LDAP tools specified by the Security Verify Access documentation.

HPDRG0303E

The input LDIF file contains more than one object with the distinguished name *%s*. (0x16b4812f)

Explanation
While processing the input LDIF file, the amldif2v6 program detected more than one object with the same distinguished name.

Administrator response
Ensure that the input LDIF file was generated using one of the LDAP tools specified by the Security Verify Access documentation.

HPDRG0304E

A failure occurred while trying to open file *%s*. (0x16b48130)

Explanation
A failure occurred while amldif2v6 was trying to open the specified file.

Administrator response
Check the permissions on the directory that contains the specified file.

HPDRG0305E

A failure occurred while trying to make a temporary copy of the input LDIF file (*%s*.tmp). (0x16b48131)

Explanation
A failure occurred while amldif2v6 was trying to make a temporary copy of the input LDIF file.

Administrator response
Ensure that directory permissions allow this file to be created.

HPDRG0306E

A failure occurred while trying to write to the file *%s*. (0x16b48132)

Explanation
A failure occurred while trying to write to the specified file.

Administrator response
Ensure that directory permissions allow this file to be written.

HPDRG0307E

A failure occurred while trying to read file *%s*. (0x16b48133)

Explanation
A failure occurred while trying to read the specified file.

Administrator response
Ensure that directory permissions allow this file to be read.

HPDRG0351E

Failed to initialize the registry. (0x16b4815f)

Explanation
When attempting to bind to the registry, an error occurred.

Administrator response
Unable to bind to the registry. Make sure all parameter values are correct to allow a connection to the registry.

HPDRG0352E

Failed to bind to the registry. (0x16b48160)

Explanation
When attempting to bind to the registry, an error occurred.

Administrator response
Unable to bind to the registry. Make sure all parameter values are correct to allow a connection to the registry.

HPDRG0355E

Must provide -K keyfile parameter if -N keyfile_label is provided. (0x16b48163)

Explanation
The -N keyfile_label parameter was provided but the -K keyfile parameter was not provided. The -N keyfile_label is appropriate only if the -K keyfile parameter is present.

Administrator response
Rerun the amuvu executable and either provide the -K keyfile parameter, or remove the -N keyfile_label parameter.

HPDRG0356E

Syntax error. (0x16b48164)

Explanation
One or more parameters you provided to the amuvu executable are incorrect.

Administrator response
Ensure that you have provided the appropriate parameters to amuvu.

HPDRG0358E

Registry search failed. Error[*%d*][*%s*]. (0x16b48166)

Explanation
One or more parameters you provided to the amuvu executable are incorrect.

Administrator response
Ensure that you have provided the appropriate parameters to amuvu.

HPDRG0359E

Failed to retrieve the list of Registry suffixes. The amuvu tool can't continue. (0x16b48167)

Explanation
When attempting to query the list of registry suffixes, an error occurred.

Administrator response
No action is required.

HPDRG0360E

Can only run with an LDAP registry. (0x16b48168)

Explanation
This tool was run on a system configured for a URAF registry. It can be run only on a system configured for an LDAP registry.

Administrator response
Run this tool only on a system configured for an LDAP registry.

HPDRG0361E

Error creating ILMT tag file [%s]. (0x16b48169)

Explanation
When attempting to create the file noted, a failure occurred.

Administrator response
Make sure the subdirectory provided for the -dilmt parameter is writeable and there is space available on that drive. Choose another subdirectory and attempt to run the tool again.

HPDRG0362E

Error writing to ILMT tag file [%s]. (0x16b4816a)

Explanation
When attempting to write to the previously created tag file noted, a failure occurred.

Administrator response
Make sure the subdirectory provided for the -dilmt parameter is writeable and there is space available on that drive. Choose another subdirectory and attempt to run the tool again.

HPDST0102W

The security translation layer is not initialized. (0x30923066)

Explanation
See message.

Administrator response
Initialize the security translation layer by calling the security translation layer initialization interface.

HPDST0104E

A memory address that is not valid was supplied to the security translation layer. (0x30923068)

Explanation
See message.

Administrator response
Retry the failing operation. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDST0105E

A credential that is not valid was supplied to the security translation layer. (0x30923069)

Explanation
The credential supplied to the security translation layer is not valid.

Administrator response
Retry the failing operation after obtaining a valid credential. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDST0106E

The context input token supplied to the security translation layer is not valid. (0x3092306a)

Explanation
The security translation layer was presented a security token which could not be validated for security context negotiation.

Administrator response
Retry the failing operation with a valid security token. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDST0118E

The security context presented to the security translation layer was not valid. (0x30923076)

Explanation
The security context presented to the security translation layer was not valid. Either it has expired, has been destroyed, or the reference presented was to a security context that has not been initialized.

Administrator response
Establish a valid security context and retry the failing operation. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDST0120E

The security translation layer was unable to perform the memory operation because memory is full. (0x30923078)

Explanation
Memory has been exhausted and there is no available memory to perform the memory operation.

Administrator response
Check the memory status of the system and retry the failing operation. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDST0121E

The security translation layer could not load the security library. (0x30923079)

Explanation
The security library required by the security translation layer could not be found on the system, or could not be loaded.

Administrator response
Check that the security library is installed. Retry the failing operation. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDST0122E

The security translation layer could not find the initializer function for the security system. (0x3092307a)

Explanation
The security library that was loaded does not have the required initializer function.

Administrator response
Ensure that the correct security library is installed on the system. Retry the failing operation. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDST0123E

The security translation layer could not initialize the security function table. (0x3092307b)

Explanation
The security translation layer initialization using the security library initialization function failed.

Administrator response
Check the system security configuration and system event log for details. Retry the failing operation. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDST0126E

The buffer type encountered by the security translation layer is unknown. (0x3092307e)

Explanation
An unknown buffer type was encountered by the security translation layer.

Administrator response
Retry the failing operation. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDST0127E

An undiagnosed error was detected by the security translation layer. The security system specific error code was: *%08x*. (0x3092307f)

Explanation
An undiagnosed error was detected by the security translation layer. The security system specific error is provided to assist with debugging.

Administrator response
Check system event logs and system documentation for further details of the problem. Retry the failing operation. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDST0128E

A routine was called with one or more parameter values that were not correct. (0x30923080)

Explanation

The parameter values supplied to the security translation layer are very important. If the values supplied by a caller are incorrect the routines cannot continue to process the parameters. This typically occurs when required length parameters have a value of less than or equal to zero.

Administrator response

Retry the failing operation. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDST0129E

The security service function *%s* returned major error code *%d* and minor error code *%d*. (0x30923081)

Explanation

A security service function failed and provided a minor error code.

Administrator response

Look in the IBM Security Verify Access for Web Troubleshooting Guide section dealing with common Web security SPNEGO problems. If no documentation describing the solution is available, consult the OS specific documentation for the security service (Kerberos or SSPI). If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDST0130E

The security service function *%s* returned the error '*%s*' (code 0x*%08x*/*%d*). (0x30923082)

Explanation

A security service function failed. The error string and error code provide a more detailed reason for the failure.

Administrator response

Look in the IBM Security Verify Access for Web Troubleshooting Guide section dealing with common Web security SPNEGO problems. If no documentation describing the solution is available, consult the OS specific documentation for the security service (Kerberos or SSPI). If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

HPDST0131E

A general error was detected by the security translation layer. (0x30923083)

Explanation

A general error was detected by the security translation layer. The security system specific error is provided to assist with debugging.

Administrator response

Check system event logs and system documentation for further details of the problem. Retry the failing operation. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

WGAWA0002E

Error accessing the database file: *%s* (*%s*:0x*%x*) (0x38a70002)

Explanation
An attempt to access a database file failed.

Administrator response
Check that the database file exists and that the file permissions allow access.

WGAWA0004E

The data which was passed into the program is not valid: *%s* (0x38a70004)

Explanation
The supplied data is not valid.

Administrator response
Check the provided data to ensure that it is being used in the correct context.

WGAWA0007E

The file, *%s*, contains data which is not valid. (0x38a70007)

Explanation
The specified file contains unexpected content.

Administrator response
Examine the file for the data which is not valid, or specify a different file.

WGAWA0008E

The file, *%s*, already exists. (0x38a70008)

Explanation
The supplied file name matches a file which already exists on the file system.

Administrator response
Either remove the specified file or select a different file name.

WGAWA0009E

The file, *%s*, does not exist. (0x38a70009)

Explanation
The supplied file name does not match a file which exists on the file system.

Administrator response
Check the supplied file name to ensure that it is correct.

WGAWA0010E

An internal error has occurred (*%s*:*%d*). (0x38a7000a)

Explanation
An internal error has occurred.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

WGAWA0011E

The configuration entry, '*%s*', in the [*%s*] stanza does not exist. (0x38a7000b)

Explanation
The requested configuration entry does not exist in the configuration file.

Administrator response
Check the supplied information to ensure that it is correct.

WGAWA0012E

Failed to establish a secure connection to the policy server (0x38a7000c)

Explanation
An attempt to establish a secure connection to the policy server failed.

Administrator response
Check the TAM policy server to ensure that it is running.

WGAWA0013E

The administration command, *%s*, failed (0x38a7000d)

Explanation
An attempt to execute an administration command failed.

Administrator response
Check the TAM servers to ensure that they are running.

WGAWA0014E

The file, *%s*, cannot be removed as it is still in use. (0x38a7000e)

Explanation
An attempt to delete a file failed as it is currently in use by another process.

Administrator response
Determine what is using the file and take the appropriate action before attempting to delete the file again.

WGAWA0015E

An unsupported configuration entry was supplied. (0x38a7000f)

Explanation
An attempt to supply an unsupported configuration entry was encountered.

Administrator response
Ensure that the correct configuration data is supplied.

WGAWA0016E

The [*%s*] stanza is an unsupported configuration stanza. (0x38a70010)

Explanation
An attempt to supply an unsupported configuration entry was encountered.

Administrator response
Ensure that the correct configuration data is supplied.

WGAWA0017E

The '*%s*' configuration entry, in the [*%s*] stanza, is an unsupported configuration entry. (0x38a70011)

Explanation
An attempt to supply an unsupported configuration entry was encountered.

Administrator response
Ensure that the correct configuration data is supplied.

WGAWA0018E

A value which is not valid, '*%s*', was supplied for the configuration entry, '*%s*', in the [*%s*] stanza. (0x38a70012)

Explanation
An attempt was made to supply data which is not valid for a configuration entry.

Administrator response
Ensure that the correct configuration data is supplied.

WGAWA0019E

A prior configuration does not exist for this resource. (0x38a70013)

Explanation
An attempt to revert the configuration was made when there were no changes to revert.

Administrator response
Ensure that the correct resource has been specified.

WGAWA0020E

An instance name is required when referencing the ftype: *%s*. (0x38a70014)

Explanation
The supplied ftype is instance specific and an instance name was not specified.

Administrator response
Retry the command, specifying an instance name.

WGAWA0021E

An instance name should not be supplied when referencing the ftype: *%s*. (0x38a70015)

Explanation
The supplied ftype is not instance specific and an instance name was specified.

Administrator response
Retry the command, without specifying an instance name.

WGAWA0022E

The supplied instance name, *%s*, is not a configured instance. (0x38a70016)

Explanation
The supplied instance name does not match a configured instance on this appliance.

Administrator response
Retry the command, specifying the correct instance name.

WGAWA0023E

The supplied ftype, *%s*, was not recognized. (0x38a70017)

Explanation
The supplied ftype was not recognized and the command cannot be completed.

Administrator response
Retry the command, ensuring that the ftype given is correct.

WGAWA0024E

The [*%s*] stanza was not found in the configuration file. (0x38a70018)

Explanation
An attempt was made to delete a stanza which does not exist.

Administrator response
Ensure that the correct stanza name is supplied.

WGAWA0025E

Cannot allocate memory (0x38a70019)

Explanation
Memory allocation operation failed.

Administrator response
Check memory limits on your machine, and increase available memory if possible.

WGAWA0026E

The file, *%s*, contains data which is not valid at line *%d*. (0x38a7001a)

Explanation
The specified file contains unexpected content.

Administrator response
Examine the file for the data which is not valid, or specify a different file.

WGAWA0027E

An error occurred in the *%s* system function: 0x*%x* (0x38a7001b)

Explanation
An error occurred while attempting to execute a system function.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

WGAWA0028E

An error occurred while executing the system call: *%s* (0x*%x*) (0x38a7001c)

Explanation
An attempt to execute a system call failed.

Administrator response
Check the system log for further information.

WGAWA0029E

The file, *%s*, cannot be opened (0x*%x*) (0x38a7001d)

Explanation
An attempt to access a file failed.

Administrator response
Check that the file permissions allow access.

WGAWA0031E

The '*%s*' configuration entry, in the [*%s*] stanza, is a read only configuration entry and should not be modified. (0x38a7001f)

Explanation
An attempt was made to change a configuration entry which is not allowed to be modified.

Administrator response
Ensure that the configuration entry has not been modified.

WGAWA0032E

A read only configuration entry was supplied. (0x38a70020)

Explanation
An attempt to supply a read only configuration entry was encountered.

Administrator response
Ensure that the correct configuration data is supplied.

WGAWA0034E

The process, *%s*, was terminated by the signal, *%d*. The process will be automatically restarted. (0x38a70022)

Explanation
A process terminated unexpectedly. The process will be automatically restarted by the system.

Administrator response
Check the system log for further information.

WGAWA0035E

Failed to stop the *%s* process (pid: *%d*). (0x38a70023)

Explanation
An attempt to stop a running process failed.

Administrator response
Check the system log for further information. If the problem persists reboot the system.

WGAWA0036E

The *%s* operation for the ldap server, *%s*:*%d*, failed: (*%s*). (0x38a70024)

Explanation
An attempt to perform an operation on the LDAP server failed.

Administrator response
Ensure that the LDAP server information has been supplied correctly and that the LDAP server is currently contactable.

WGAWA0037E

Cannot obtain a unique DN for the user: *%s*. (0x38a70025)

Explanation
An attempt to locate the DN for a user has failed.

Administrator response
Ensure that the correct user information has been supplied, and that the LDAP server information has been supplied correctly.

WGAWA0038E

An error occurred while executing the command: *%s* (0x*%x*) *%s* (0x38a70026)

Explanation
An attempt to execute a system command failed.

Administrator response
Check the system log for further information.

WGAWA0039E

The directory, *%s*, does not exist. (0x38a70027)

Explanation
The supplied directory name does not match a directory which exists on the file system.

Administrator response
Check the supplied directory name to ensure that it is correct.

WGAWA0040E

A file or directory which is not valid was encountered: *%s* (0x38a70028)

Explanation
The specified file is not valid.

Administrator response
Check the provided data to ensure that it is being used in the correct context.

WGAWA0041E

The following files already exist: *%s* (0x38a70029)

Explanation
The specified files already exist on the system.

Administrator response
Check the system log for further information.

WGAWA0042E

An error occurred in the *%s* system function: *%s* (0x38a7002a)

Explanation
An error occurred while attempting to execute a system function.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

WGAWA0043W

High CPU utilization: *%s* (0x38a7002b)

Explanation
This message is generated when the CPU usage exceeds the warning threshold.

Administrator response
Examine the appliance to determine if any action should be taken.

WGAWA0044W

High disk usage: *%s* (0x38a7002c)

Explanation
This message is generated when the disk usage exceeds the warning threshold.

Administrator response
Review the disk usage of the appliance. Consider removing old log files to free up space.

WGAWA0045W

Certificate expires in *%d* days: *%s* (0x38a7002d)

Explanation
This message is generated when a certificate will expire within the warning threshold.

Administrator response
No action is required

WGAWA0046W

Certificate expired: *%s* (0x38a7002e)

Explanation
This message is generated when a certificate has expired. The message includes the certificate label of the expired certificate.

Administrator response
Update or replace the expired certificate.

WGAWA0047W

Reverse Proxy is not running: *%s* (0x38a7002f)

Explanation
This message is generated when a reverse proxy instance is configured but not running. The message includes the name of the reverse proxy instance.

Administrator response
If the reverse proxy instance is stopped unexpectedly, examine the reverse proxy log files to determine why the instance is no longer running.

WGAWA0048E

Invalid configuration for the *%s* notifications module. Reverting to default values. (0x38a70030)

Explanation
The configured advanced tuning parameters for the notifications module are invalid. The default values will be used until this is corrected.

Administrator response
No action is required

WGAWA0049E

An error occurred while executing an SQL statement at *%s*:*%d*. (*%d*:*%s*) (0x38a70031)

Explanation
There was an error writing the FlowData information to disk. If the problem persists, see the IBM Electronic Support for additional information - https://www.ibm.com/mysupport

Administrator response
No action is required

WGAWA0050E

The requested configuration data was not found. (0x38a70032)

Explanation
A request for specific configuration data failed as the configuration data does not exist.

Administrator response
Ensure that the correct data has been specified, and that the configuration file contains this data.

WGAWA0051E

An ICC toolkit failure occurred while calling *%s*. Error: *%s*. (0x38a70033)

Explanation
An internal ICC error occurred.

Administrator response
The action to correct this problem depends on details in the error message. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

WGAWA0052E

An ICC toolkit failure occurred while calling *%s*. No further details are known. (0x38a70034)

Explanation
An internal ICC error occurred. However, no details about the error were able to be determined beyond the name of the ICC function which failed.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

WGAWA0053E

The library, *%s*, cannot be opened: *%s* (0x38a70035)

Explanation
An attempt to load a library file failed.

Administrator response
If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

WGAWA0054E

An error occurred while executing the system call: *%s* (0x*%x*) *%s* (0x38a70036)

Explanation
An attempt to execute a system call failed.

Administrator response
Check the system log for further information.

WGAWA0055W

High disk usage for the runtime database: *%s* (0x38a70037)

Explanation
When the runtime database is local to the cluster, the disk usage of the runtime database is monitored. This message is generated when the disk usage reaches the warning threshold. These percentages are based on the size limit that can be set on the Database tab of the Cluster Configuration page in the LMI. (The default value for the maximum size of the runtime database is 40% of the current active partition)

Administrator response
Examine the runtime database and consider increasing the maximum allowed size.

WGAWA0056E

Failed to write to the file, *%s* (0x*%x*) (0x38a70038)

Explanation
An attempt to write to a file failed.

Administrator response
Check that the file permissions allow access and that the disk is not full.

WGAWA0057E

The database is not yet available. (0x38a70039)

Explanation
The database is in the process of being updated and is not yet available for use.

Administrator response
Wait a period of time and then retry the operation.

WGAWA0061E

The command, '*%s*', did not complete within the allotted time. (0x38a7003d)

Explanation
A command which was executed did not complete in the allotted time.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

WGAWA0062E

The supplied authorization server name, *%s*, is not a known server. (0x38a7003e)

Explanation
The supplied authorization server name does not match a configured authorization server.

Administrator response
Retry the command, specifying a valid server name.

WGAWA0063E

The specified authorization server, *%s*, could not be deleted. (0x38a7003f)

Explanation
An attempt to delete an authorization server has failed.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

WGAWA0067E

No image was found on the installation media. (0x38a70043)

Explanation
The firmware package was not found on the installation media.

Administrator response
Check that the installation media is not corrupt.

WGAWA0068E

More than one image was found on the installation media. (0x38a70044)

Explanation
More than one firmware package was found on the installation media.

Administrator response
Check that the installation media is not corrupt.

WGAWA0069E

The current root partition could not be determined. (0x38a70045)

Explanation
The installer could not determine the partition on which to install the firmware image.

Administrator response
Check that the installation media is not corrupt and that the virtual machine settings are correct.

WGAWA0070E

An invalid destination partition has been specified. (0x38a70046)

Explanation
The installer is attempting to install the firmware on an unsupported partition.

Administrator response
Check that the installation media is not corrupt.

WGAWA0071E

Failed to verify the signature of the install image. (0x38a70047)

Explanation
The installer failed to verify the install image.

Administrator response
Check that the installation media is not corrupt and has not expired.

WGAWA0072E

Failed to remove the temporary files which were created during the installation. (0x38a70048)

Explanation
The installer failed to remove the temporary files which were created during the installation.

Administrator response
Reboot the system and verify that the installation completed successfully.

WGAWA0073E

Failed to initialize the loopback device. (0x38a70049)

Explanation
The installer could not mount the installation package.

Administrator response
Check that the installation media is not corrupt and that the virtual image has been configured correctly.

WGAWA0074E

Failed to extract the firmware archive. (0x38a7004a)

Explanation
The installer could not extract the firmware archive which was provided on the installation media.

Administrator response
Check that the installation media is not corrupt and that the virtual image has been configured correctly.

WGAWA0075E

Failed to locate the files which are used to correctly determine the running hardware. (0x38a7004b)

Explanation
The installer could not determine the running hardware.

Administrator response
Check that the installation media is not corrupt and that the virtual image has been configured correctly.

WGAWA0076E

Failed to detect the running hardware. (0x38a7004c)

Explanation
The installer could not determine the running hardware.

Administrator response
Check that the installation media is not corrupt and that the installer is running under a supported hypervisor.

WGAWA0077E

The firmware image could not be installed. (0x38a7004d)

Explanation
The firmware image could not be installed.

Administrator response
Check that the installation media is not corrupt and that the installer is running under a supported hypervisor.

WGAWA0078E

Untranslated message: *%s* (0x38a7004e)

Explanation
A message was returned from the installer program for which there is no translation.

Administrator response
Check the console for further information.

WGAWA0192E

The runtime environment must be configured before invoking this command. (0x38a700c0)

Explanation
The runtime environment is not currently configured. It must be configured to execute the requested operation.

Administrator response
Configure the runtime environment and then retry the operation.

WGAWA0193E

The tool is not supported on this system. (0x38a700c1)

Explanation
The requested tool is not supported on the system. This error will usually occur if the system is running as a virtual appliance and the tool requires direct access to hardware.

Administrator response
No action is required.

WGAWA0194E

The file system on the USB drive could not be mounted. Please check the USB drive and then retry the command. (0x38a700c2)

Explanation
An attempt was made to mount a USB drive, but the operation failed.

Administrator response
Ensure that the USB drive is inserted and is formatted with a FAT file system.

WGAWA0195E

The log files could not be archived to the USB drive. (0x38a700c3)

Explanation
The log files could not be archived to the USB drive.

Administrator response
Check to ensure that the USB drive has sufficient space for all of the log files.

WGAWA0198E

No log files are available for this selection. (0x38a700c6)

Explanation
A request was made to display a log file which doesn't exist.

Administrator response
No action is required.

WGAWA0199E

The specified option is not supported. (0x38a700c7)

Explanation
A request to the system was made using an unsupported option.

Administrator response
Re-issue the request, using a supported option.

WGAWA0256E

Incorrect usage for the mesa_config *%s* command. (0x38a70100)

Explanation
The command line options which were supplied to the mesa_config program were not valid.

Administrator response
Retry the command, supplying the correct command line options.

WGAWA0257E

A path which is not valid has been specified. (0x38a70101)

Explanation
The command is only authorized to perform an action on specific file paths. The supplied path does not match one of these supported paths.

Administrator response
Retry the command, supplying a supported path.

WGAWA0258E

Failed to copy the file, *%s*, to *%s*: *%d* (0x38a70102)

Explanation
An attempt to copy a file failed.

Administrator response
Check the supplied file names for accuracy and then retry the command.

WGAWA0259E

Authorization for the requested command has been denied. (0x38a70103)

Explanation
A command request has been denied.

Administrator response
Examine the requested command and ensure that the necessary rules have been met.

WGAWA0260E

The IBM Security Verify Access runtime environment is not configured. (0x38a70104)

Explanation
The IBM Security Verify Access runtime is not currently configured. It must be configured to execute the requested operation.

Administrator response
Configure the IBM Security Verify Access runtime environment and then retry the operation.

WGAWA0261E

A web reverse proxy instance with the name *%s* has already been configured. (0x38a70105)

Explanation
An attempt to configure a new web reverse proxy instance has failed because the supplied instance name matches the name of a pre-existing instance.

Administrator response
Either unconfigure the existing existence or select a new instance name.

WGAWA0262E

The runtime environment has already been configured. (0x38a70106)

Explanation
An attempt to configure the runtime environment has been made while the environment is still configured.

Administrator response
Unconfigure the runtime environment before attempting to reconfigured it.

WGAWA0263E

The supplied file name, *%s*, must have a file extension of '*%s*'. (0x38a70107)

Explanation
A file name was supplied with an unexpected extensions.

Administrator response
Specify a file name with the correct extension.

WGAWA0264E

The key database, *%s*, does not exist. (0x38a70108)

Explanation
The supplied database does not match one which exists on the file system.

Administrator response
Check the supplied database name to ensure that it is correct.

WGAWA0265E

An IP address which is not valid was located in the supplied entry: *%s* (0x38a70109)

Explanation
The supplied IP address does not match one of the IP addresses of the protected interfaces.

Administrator response
Check the supplied IP address to ensure that it is correct.

WGAWA0266E

A matching interface was not found. (0x38a7010a)

Explanation
The supplied IP address does not match one of the IP addresses of the protected interfaces.

Administrator response
Check the supplied IP address to ensure that it is correct.

WGAWA0267E

The *%s* parameter is required. (0x38a7010b)

Explanation
A required parameter was missing from the supplied information.

Administrator response
Check the supplied information and ensure that the missing data is supplied.

WGAWA0268E

The supplied starting value of *%ld* is larger than the number of lines contained in the file (*%ld*) (0x38a7010c)

Explanation
The starting line number is greater than the current number of lines in the file.

Administrator response
Check the supplied information and ensure that a start value which is less than the number of lines in the file is supplied.

WGAWA0269E

An incorrect range was specified. The starting value (*%ld*) must be less than the ending value (*%ld*) (0x38a7010d)

Explanation
The start value is greater than the end value.

Administrator response
Check the supplied information and ensure that a start value which is less than the end value is supplied.

WGAWA0270E

The pending changes cannot be committed as conflicts have been discovered between the staged and production files. (0x38a7010e)

Explanation
Conflicts have been discovered between the pending changes and production files. This will only occur if the production file has been modified by a source outside of the appliance.

Administrator response
Manually apply the changes again.

WGAWA0271E

The IP address, *%s*, is already in use. (0x38a7010f)

Explanation
The supplied IP address is already in use by the system.

Administrator response
Choose an IP address which is not already in use by the system.

WGAWA0272E

The *%s* interface is not a configured interface. (0x38a70110)

Explanation
The supplied interface name does not match one of the configured interfaces.

Administrator response
Check the supplied interface name to ensure that it is correct.

WGAWA0273E

One or more instances of the Web reverse proxy is still configured. These instances must be unconfigured first. (0x38a70111)

Explanation
An attempt to unconfigure the runtime environment has been made while Web reverse proxy instances remain configured.

Administrator response
Unconfigure the Web reverse proxy instances and then retry the operation.

WGAWA0279E

An incorrect user name or password has been supplied. (0x38a70117)

Explanation
An authentication attempt has failed. Either an incorrect user name or password was supplied.

Administrator response
Ensure that the correct user name and password have been used.

WGAWA0280E

Examine the log of the Web Reverse Proxy instance for further information on the failure. (0x38a70118)

Explanation
A request to start or stop the Web Reverse Proxy has failed. The log for the instance should contain more information on this failure.

Administrator response
Examine the log of the Web Reverse Proxy instance for further information on the failure.

WGAWA0282E

The key database, *%s*, already exists. (0x38a7011a)

Explanation
The supplied database name already matches one which exists on the file system.

Administrator response
Check the supplied database name to ensure that it is correct.

WGAWA0283E

The requested operation cannot proceed as there are pending changes which first need to be committed. (0x38a7011b)

Explanation
The requested operation cannot be performed while there are pending changes. These changes need to be deployed, or rolled back, before the operation can be processed.

Administrator response
Either deploy or rollback the changes and then attempt the operation again.

WGAWA0284E

The configuration file for the *%s* instance is missing from the migration zip file. (0x38a7011c)

Explanation
The migration functionality only supports the migration to an instance of the same name. The supplied migration zip file does not contain the configuration file for the specified instance.

Administrator response
Check the migration zip file to ensure that the configuration file for the specified instance is present.

WGAWA0285E

An invalid filter rule was specified (*%s*) (0x38a7011d)

Explanation
An attempt to capture packet data failed as an invalid filter rule was provided.

Administrator response
Check the filter rule and ensure that it is a valid rule.

WGAWA0286E

The specified maximum file size exceeds the available space of *%ld* MB. (0x38a7011e)

Explanation
The specified maximum file size will exceed the amount of available disk space.

Administrator response
Ensure that the maximum file size is less than the remaining available disk space.

WGAWA0287E

The system is already capturing network packets. The current capture operation must be stopped before the requested operation can be completed. (0x38a7011f)

Explanation
The system can only perform a single capture operation at a time.

Administrator response
Stop the current capture operation and then attempt the request again.

WGAWA0301E

A packet capture file already exists on the system. The current file must be deleted before a new capture operation can be started. (0x38a7012d)

Explanation
A capture file already exists and it must be deleted before a new capture operation can be started.

Administrator response
Delete the current capture file and then retry the operation.

WGAWA0302E

The maximum capture file size has been reached. (0x38a7012e)

Explanation
The maximum file size for the capture file has been reached. This file size was specified when the capture operation was started.

Administrator response
Ensure that the specified maximum file size is adequate for the packets which are being captured.

WGAWA0303W

The log file, *%s*, has been automatically purged from the system. (0x38a7012f)

Explanation
The disk utilisation has reached the maximum threshold and as such the system has deleted the specified log file.

Administrator response
Check the system to ensure that all unnecessary files are deleted.

WGAWA0304E

A management interface has already been configured with the same IP address: *%s*. (0x38a70130)

Explanation
An attempt was made to configure an application interface with the same address as a management interface. This configuration is not supported.

Administrator response
Either change the corresponding management interface address, or change the configured application interface address.

WGAWA0305E

An invalid activation code has been supplied. (0x38a70131)

Explanation
The supplied activation code is not valid.

Administrator response
Check the provided activation code to ensure that it has been entered correctly.

WGAWA0307E

The server failed to start correctly. (0x38a70133)

Explanation
The attempt to start the server failed.

Administrator response
Check the system log for further information.

WGAWA0309E

The server could not be stopped. (0x38a70135)

Explanation
The attempt to stop the server failed.

Administrator response
Check the system log for further information.

WGAWA0310E

The command is not supported with the current configuration. (0x38a70136)

Explanation
An invalid command was attempted.

Administrator response
Check the configuration of the system to see if the specified command should be supported.

WGAWA0313E

The supplied database name, *%s*, does not match any known databases. (0x38a70139)

Explanation
The supplied database name does not match a configured database on this appliance.

Administrator response
Retry the command, specifying the correct database name.

WGAWA0314E

The user identity for the local database cannot be modified after the database has been created. (0x38a7013a)

Explanation
The new configuration data could not be applied because the user identity for a local database has been modified.

Administrator response
Ensure that the user identity which is associated with the local databases have not been changed.

WGAWA0315E

The database, *%s*, is not currently enabled. (0x38a7013b)

Explanation
The specified database is not currently enabled.

Administrator response
Enable the database or select a different database and then retry the command.

WGAWA0316E

Failed to obtain the state of the specified database: *%s*. (0x38a7013c)

Explanation
The program could not obtain the state of the specified database.

Administrator response
Check the system log for further information.

WGAWA0317E

The server has already been started. (0x38a7013d)

Explanation
An attempt was made to start a server when it was already running.

Administrator response
Ensure that the server is not running before attempting the operation again.

WGAWA0318E

The cluster signature file could not be created. (0x38a7013e)

Explanation
An attempt to create the cluster signature file failed.

Administrator response
Check the system log for further information.

WGAWA0319E

The cluster signature file could not be validated. (0x38a7013f)

Explanation
An attempt to validate the cluster signature file failed.

Administrator response
Ensure that a valid signature file is used.

WGAWA0384E

The cluster master cannot currently be reached, and must be reachable in order to complete the operation. (0x38a70180)

Explanation
The operation failed because the cluster master cannot currently be reached.

Administrator response
Ensure that the cluster master is running and can be reached.

WGAWA0385W

The specified node cannot currently be reached. (0x38a70181)

Explanation
The operation could not be fully completed because the cluster node cannot currently be reached.

Administrator response
Ensure that the node is running and can be reached.

WGAWA0386E

The database server failed to start within the allocated time. (0x38a70182)

Explanation
The database server did not start within the allocated time.

Administrator response
Check the system log for further information.

WGAWA0387W

The specified node, *%s*, is not a member of the cluster. (0x38a70183)

Explanation
The operation could not be fully completed because the specified node is not a member of the cluster.

Administrator response
Ensure that the specified node is a recognised member of the cluster.

WGAWA0388E

A cluster master cannot be deregistered from the cluster. (0x38a70184)

Explanation
A cluster master cannot be deleted from the cluster.

Administrator response
Change the cluster policy so that the local appliance is not a master and then delete the appliance from the cluster.

WGAWA0389E

A cluster must be defined before this request can be processed. To define a cluster the primary master must be set to something other than 127.0.0.1. (0x38a70185)

Explanation
A cluster must be defined before the request can be processed.

Administrator response
Configure a primary master and then retry the operation.

WGAWA0390E

The port which has been specified for the cluster cannot be used because another service is already using one of the range of required ports. (0x38a70186)

Explanation
The cluster utilises a range of network ports, starting at a port which is specified as a part of the cluster configuration. One or more ports within this range is currently being used by a different service of the appliance.

Administrator response
Select another range of ports which can be used by the cluster.

WGAWA0391E

The signature file could not be created. (0x38a70187)

Explanation
An attempt to create the signature file failed.

Administrator response
Check the system log for further information.

WGAWA0392E

The signature file could not be validated. (0x38a70188)

Explanation
An attempt to validate the signature file failed.

Administrator response
Ensure that a valid signature file is used.

WGAWA0393E

The supplied signature file is not compatible with the local server. (0x38a70189)

Explanation
An attempt to apply the configuration data from the supplied signature file failed.

Administrator response
Ensure that the signature file was generated from a server which has a compatible configuration with the local server.

WGAWA0394E

One or more Authorization server instances are still configured. These instances must be unconfigured first. (0x38a7018a)

Explanation
An attempt to unconfigure the runtime environment has been made while Authorization server instances remain configured.

Administrator response
Unconfigure the Authorization server instances and then retry the operation.

WGAWA0395W

Failed to attach the ACL which is used to allow unauthenticated access to the favicon.ico resource. (0x38a7018b)

Explanation
An attempt to attach an ACL to an object on the new Web Reverse Proxy instance failed. This usually occurs when the policy server cannot connect to the Web Reverse Proxy instance.

Administrator response
Check the environment to ensure that the policy server can communicate with the new Web Reverse Proxy instance.

WGAWA0396E

The operation is not permitted on this key database. (0x38a7018c)

Explanation
The attempted operation on the key database is not permitted.

Administrator response
No action is required. The requested operation is not allowed.

WGAWA0397E

The suffix, '*%s*', already exists. (0x38a7018d)

Explanation
The supplied suffix name matches a suffix which already exists in the embedded LDAP server.

Administrator response
Either remove the specified suffix or select a different suffix name.

WGAWA0398E

The suffix, '*%s*', does not exist. (0x38a7018e)

Explanation
The supplied suffix name does not match a suffix which exists in the embedded LDAP server.

Administrator response
Check the supplied suffix name to ensure that it is correct.

WGAWA0399E

The suffix, '*%s*', is not valid. (0x38a7018f)

Explanation
The supplied suffix name is not a valid suffix name.

Administrator response
Check the supplied suffix name to ensure that it is a valid suffix.

WGAWA0400E

The debug level, '*%s*', is not valid. (0x38a70190)

Explanation
The supplied debug level is not a valid level.

Administrator response
Check the supplied debug level to ensure that it is a valid level.

WGAWA0403E

Failed to export the configuration of the Web Reverse Proxy instance. (0x38a70193)

Explanation
An attempt to export the configuration information for a Web Reverse Proxy instance failed.

Administrator response
Examine additional messages to determine the cause of the error and correct the problem. If the problem persists, check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

WGAWA0404E

The LMI account, *%s*, has been temporarily locked due to an excessive number of failed authentication attempts. (0x38a70194)

Explanation
To help protect against brute force attacks a user account will be temporarily locked after a certain number of consecutive failed authentication attempts.

Administrator response
Ensure that you have the correct user name and password. The account will be automatically unlocked after a period of time and then the authentication can be attempted again.

WGAWA0406E

The offering could not be activated because of a conflict with a currently activated offering. (0x38a70196)

Explanation
An attempt to activate an offering has failed because one of the currently activated offerings conflicts with the new offering.

Administrator response
Check the activated offerings to ensure that there are no conflicting offerings.

WGAWA0407E

The key file could not be created because an existing key file already references a different Thales network HSM device. (0x38a70197)

Explanation
An attempt has been made to create a key file which references a new Thales network HSM device. The system can only support a single Thales network HSM device configuration.

Administrator response
Examine the other key files on the system and ensure that only a single Thales network HSM device is being referenced.

WGAWA0408E

A connection could not be established to the device. Please ensure that the device is contactable, and that all of the supplied information is correct. (0x38a70198)

Explanation
An attempt to communicate with a HSM device has failed. This could be caused by a network connectivity issue, or if incorrect connection information has been supplied.

Administrator response
Ensure that the device can be reached and that all of the supplied information is correct.

WGAWA0418E

The embedded LDAP server failed to start within the allocated time. (0x38a701a2)

Explanation
The embedded LDAP server did not start within the allocated time.

Administrator response
Check the system log for further information.

WGAWA0419E

The key file could not be created because an existing key file already references a Thales network HSM device. (0x38a701a3)

Explanation
An attempt has been made to create a key file which references a new Thales network HSM device. The system can only support a single Thales network HSM device configuration.

Administrator response
Examine the other key files on the system and ensure that only a single Thales network HSM device is being referenced.

WGAWA0420E

The environment variable '*%s*' is not a supported variable and cannot be modified. (0x38a701a4)

Explanation
An attempt has been made to modify an environment variable which is not supported and is not allowed to be modified.

Administrator response
Remove the specified environment variable and attempt the request again.

WGAWA0421E

The supplied certificate has a key length of *%d* which is less than the minimum key length of *%d*. (0x38a701a5)

Explanation
A certificate was supplied which has a key length less than the minimum supported key length.

Administrator response
Supply a certificate which has a key length which is greater than or equal to the minimum supported key length.

WGAWA0422E

The federation, *%s*, is not configured for this instance. (0x38a701a6)

Explanation
The federation identifier was not found in the instance configuration file

Administrator response
Ensure that the federation identifier provided is correct

WGAWA0423E

The junction *%s* was used for the runtime host *%s*. The same junction cannot be used for the runtime host in this request. (0x38a701a7)

Explanation
The requested junction is in use by another runtime host. A junction cannot be used by more than one runtime server.

Administrator response
Update the federation configuration on the supplied runtime server so that it uses a different junction name.

WGAWA0429E

The activation policy for the offering, *%s*, failed. The runtime database must be configured prior to activating this offering. (0x38a701ad)

Explanation
The runtime database has not yet been configured and must be configured prior to the activation of this offering.

Administrator response
Configure the runtime database prior to activating this offering.

WGAWA0430E

Clustering is not supported in a Docker environment. (0x38a701ae)

Explanation
An attempt was made to import a snapshot with clustering configured.

Administrator response
Disable clustering and regenerate the snapshot.

WGAWA0431E

Local mode Runtime Database is not supported in a Docker environment. (0x38a701af)

Explanation
An attempt was made to import a snapshot which uses the Local mode Runtime Database.

Administrator response
Configure an external Runtime Database and regenerate the snapshot.

WGAWA0432E

An external configuration database has been configured, or the snapshot has been taken from a firmware version prior to 9.0.2.0, and this is not supported in a Docker environment. (0x38a701b0)

Explanation
An attempt was made to import a snapshot which has been configured to use an external configuration database or taken from an appliance which is running a firmware version prior 9.0.2.0.

Administrator response
Use a snapshot that has been configured with an embedded configuration database and has been taken from an appliance which is running firmware version 9.0.2.0 or later.

WGAWA0433E

Network keystores are not supported in a Docker environment. (0x38a701b1)

Explanation
An attempt was made to import a snapshot which contains configured network keystores.

Administrator response
Remove all Network keystores and regenerate the snapshot.

WGAWA0434E

The snapshot version is not compatible with the current operating environment. (0x38a701b2)

Explanation
An attempt was made to import a snapshot which was generated on a version that is not compatible with the current operating environment.

Administrator response
Regenerate the snapshot in a compatible environment. Verify Access does not support importing snapshots from versions earlier than 9.0.0.0 or from versions at a later level than the current operating environment.

WGAWA0435E

Authorization Server instances are not supported in a Docker environment. (0x38a701b3)

Explanation
An attempt was made to import a snapshot which contains configured Authorization Server instances.

Administrator response
Remove all Authorization Server instances and regenerate the snapshot.

WGAWA0436E

The local user registry is only supported for snapshots generated on Verify Access 9.0.4.0 or later. (0x38a701b4)

Explanation
An attempt was made to import a snapshot containing local user registry data. This is not supported.

Administrator response
Regenerate the snapshot in a compatible environment. Verify Access does not support importing snapshots from versions earlier than 9.0.0.0 or from versions at a later level than the current operating environment.

WGAWA0437E

The local user registry is only available for snapshots which embed the local user registry data. (0x38a701b5)

Explanation
An attempt was made to import a snapshot which does not contain the required local user registry data.

Administrator response
Regenerate the snapshot in a compatible environment. Ensure that the advanced tuning parameter wga_rte.embedded.ldap.include.in.snapshot is enabled when generating the snapshot.

WGAWA0439E

An invalid DSC instance was specified: *%s* (0x38a701b7)

Explanation
The supplied DSC instance is not valid.

Administrator response
Check the supplied instance environment variable to ensure that it corresponds to a valid and defined DSC node identifier. The identifier should be in the range of 1 to 4.

WGAWA0440E

Failed to write to the configuration file. (0x38a701b8)

Explanation
An attempt to write to a file failed.

Administrator response
Check that the file permissions allow access and that the disk is not full.

WGAWA0441E

Failed to read the configuration file. (0x38a701b9)

Explanation
An attempt to read a file failed.

Administrator response
Check that the file permissions allow access.

WGAWA0442E

The advanced tuning parameter, *%s*, contains an invalid value: *%s* (0x38a701ba)

Explanation
An invalid value was supplied as an advanced tuning parameter.

Administrator response
Correct the value of the advanced tuning parameter.

WGAWA0444E

The environment variable, *%s*, has not been defined. (0x38a701bc)

Explanation
A required environment variable is missing.

Administrator response
Define the missing environment variable and then retry the operation.

WGAWA0452E

The IP address which is being used as the cluster identifier cannot be changed while the appliance is acting as a master in the cluster. (0x38a701c4)

Explanation
The appliance is currently acting as a master in the cluster, and you are not permitted to change the IP address it is using as an identifier while it is acting as a master.

Administrator response
Change the cluster policy so that the appliance is not acting as a master before attempting to reconfigure this IP address.

WGAWA0453E

The operation can only be performed on the primary master. (0x38a701c5)

Explanation
An attempt was made to modify the cluster. This change can only be made on the primary master of the cluster.

Administrator response
Try again on the primary master.

WGAWA0454E

A required cluster master definition is missing from the cluster policy. (0x38a701c6)

Explanation
An attempt was made to update the cluster policy, but the definition is missing at least one master. When adding a new master to the cluster policy all prior masters must first be defined. In addition to this you are not allowed to define the tertiary master without also defining a quaternary master.

Administrator response
Check the definition of the cluster policy to ensure that it is valid.

WGAWA0455E

A required cluster definition is missing from the cluster policy. (0x38a701c7)

Explanation
An attempt was made to update the cluster policy, but the definition is missing for at least one piece of data.

Administrator response
Check the definition of the cluster policy to ensure that it is valid.

WGAWA0456E

The appliance is already a member of a cluster. (0x38a701c8)

Explanation
An attempt was made to join the appliance to a new cluster whilst it was registered to an existing cluster.

Administrator response
Remove the appliance from the cluster and then try again.

WGAWA0457E

The first management interface must be enabled and configured with a static IP address in order to operate within a cluster. (0x38a701c9)

Explanation
In order to operate within a cluster the appliance must have a statically configured IP address assigned to the first management interface.

Administrator response
Ensure that the first management interface has been configured correctly.

WGAWA0458E

The cluster node '*%s*' is currently engaged in data replication and can not be interrupted. (0x38a701ca)

Explanation
A cluster node database servers must be stopped to change configuration settings. This can not be done while a node is actively engaged in replication.

Administrator response
Wait for the cluster node replication to become idle and retry the operation.

WGAWA0459E

The Security Verify Access Runtime configuration mode '*%s*' is not valid. (0x38a701cb)

Explanation
Either the mode configuration parameter was not a valid string or is not a permitted next mode to change to from the current mode.

Administrator response
Correct the mode to a valid one and rerun the operation.

WGAWA0460E

The Security Verify Access Runtime is configured for non-clustered operation. (0x38a701cc)

Explanation
It is not valid to configure the Security Verify Access Runtime for a cluster if it is already configured for non-clustered use.

Administrator response
Unconfigure the non-clustered Security Verify Access Runtime before configuring it for the cluster.

WGAWA0461E

The Security Verify Access Runtime is configured for clustered operation. (0x38a701cd)

Explanation
It is not valid to configure the Security Verify Access Runtime for non-clustered use if it is already configured for clustered use.

Administrator response
Unconfigure the clustered Security Verify Access Runtime before configuring it for the non-cluster.

WGAWA0462E

An error occurred when attempting to validate the activation level of the remote server: *%s* (0x38a701ce)

Explanation
We need to validate the activation level of the server before we can accept the data changes. This validation failed because we could not contact the server.

Administrator response
Validate that the correct data has been entered and that the primary master can contact the specified server.

WGAWA0463E

The server, *%s*, does not have all of the necessary offerings activated. (0x38a701cf)

Explanation
The primary and secondary masters must be activated with all of the offerings which are used by nodes in the cluster.

Administrator response
Ensure that the required offerings on the specified server have been activated.

WGAWA0464E

The server does not have all of the necessary offerings activated. (0x38a701d0)

Explanation
The primary and secondary masters must be activated with all of the offerings which are used by nodes in the cluster.

Administrator response
Ensure that the required offerings on the server have been activated.

WGAWA0465E

The server, *%s*, is a restricted node which cannot be promoted to a master role. (0x38a701d1)

Explanation
The restricted flag prevents nodes from being promoted to a master role. One of the cluster nodes being promoted to a master role is flagged as restricted.

Administrator response
From the primary master, ensure that the restricted flag is removed from all nodes to be promoted to master roles.

WGAWA0466E

You cannot manage the IBM Security Verify Access security policy from this node as it is currently a restricted member of the cluster. (0x38a701d2)

Explanation
The restricted flag prevents nodes from managing IBM Security Verify Access security policy, and as such this node cannot be used to manage the Verify Access security policy.

Administrator response
Update the cluster configuration on the primary master to remove the restricted property from the node, or use a non-restricted node to manage the security policy.

WGAWA0467E

The property hvdb_driver_type is required when using an Oracle database. Valid values are 'thin' or 'oci'. (0x38a701d3)

Explanation
When using an Oracle database for an external runtime database a valid driver type must be specified. Valid values are 'thin' or 'oci'.

Administrator response
Resend the request with the hvdb_driver_type property with either the value of 'thin' or 'oci'.

WGAWA0468W

Using the runtime database which is located on the primary master. (0x38a701d4)

Explanation
The local server has been set to use the runtime database located on the primary master.

Administrator response
No action is required.

WGAWA0469W

Using the runtime database which is located on the secondary master. (0x38a701d5)

Explanation
The local server has been set to use the runtime database located on the secondary master.

Administrator response
No action is required.

WGAWA0470E

The IP address which is being used as the cluster identifier cannot be deleted while the appliance is in a cluster. (0x38a701d6)

Explanation
The appliance is currently configured in a cluster, and you are not permitted to delete the IP address which the appliance is using to identify itself to other nodes.

Administrator response
Remove this appliance from the cluster before attempting to remove the IP address.

WGAWA0603E

Failed to create the temporary file, '*%s*', for the database '*%s*': error '*%s*'. (0x38a7025b)

Explanation
A temporary file could not be created.

Administrator response
No action is required

WGAWA0604E

Failed to obtain a list of SQL tables from the '*%s*' database. (0x38a7025c)

Explanation
To remove the SolidDB replica metadata a list of tables in the database must be obtained. The request to obtain this list of tables failed.

Administrator response
No action is required

WGAWA0605E

Failed to open the temporary file, '*%s*', for the database '*%s*': error '*%s*'. (0x38a7025d)

Explanation
A temporary file which was created earlier could not be opened for reading.

Administrator response
No action is required

WGAWA0606E

Failed to obtain a list of SQL tables from the '*%s*' database. (0x38a7025e)

Explanation
A list of tables must be obtained in order to be able to add the SolidDB master metadata. The request to obtain the list of tables failed.

Administrator response
No action is required

WGAWA0607E

Failed to obtain the definitions of the SQL tables from the master '*%s*' database. (0x38a7025f)

Explanation
A list of tables must be obtained in order to be able to create the SolidDB replica database. The request to obtain the list of tables failed.

Administrator response
Ensure the primary master is running.

WGAWA0640W

There are pending changes waiting to be deployed. (0x38a70280)

Explanation
This message is generated when there are changes made using the LMI/Web services which are not active because they have not yet been deployed.

Administrator response
This is an informational message. No action is required.

WGAWA0641W

(*%s*) *%s* (0x38a70281)

Explanation
This is an informational message from a system server. It includes an informational message and the name of the server which generated the message.

Administrator response
This is an informational message. No action is required.

WGAWA0642W

The pending changes failed to deploy within the allotted time. (0x38a70282)

Explanation
The pending changes did not complete deploying within the command timeout.

Administrator response
Adjust the command timeout as required.

WGAWA0643E

High CPU utilization: *%s* (0x38a70283)

Explanation
This message is generated when the CPU usage exceeds the alert threshold.

Administrator response
Examine the appliance to determine if any action should be taken.

WGAWA0644E

High disk usage: *%s* (0x38a70284)

Explanation
This message is generated when the disk usage exceeds the alert threshold.

Administrator response
Review the disk usage of the appliance. Consider removing old log files to free up space.

WGAWA0645E

Certificate expires in *%d* days: *%s* (0x38a70285)

Explanation
This message is generated when a certificate will expire within the alert threshold.

Administrator response
No action is required

WGAWA0646E

High disk usage for the runtime database: *%s* (0x38a70286)

Explanation
When the runtime database is local to the cluster, the disk usage of the runtime database is monitored. This message is generated when the disk usage reaches the alert threshold. These percentages are based on the size limit that can be set on the Database tab of the Cluster Configuration page in the LMI. (The default value for the maximum size of the runtime database is 40% of the current active partition)

Administrator response
Examine the runtime database and consider increasing the maximum allowed size.

WGAWA0647W

Local clock is not synchronized. (0x38a70287)

Explanation
The clock on the appliance is not currently synchronized. This condition can arise if a NTP server is not currently configured, or if there is a problem in reaching the configured NTP server.

Administrator response
Examine and correct the configuration of the NTP server.

WGAWA0654E

The server, *%s*, could not be contacted. (0x38a7028e)

Explanation
An attempt to connect to a specific server has failed.

Administrator response
Ensure that the specified server is running and can be reached by the local server.

WGAWA0655E

The supplied file is not valid. (0x38a7028f)

Explanation
The specified file contains unexpected content.

Administrator response
Ensure that the correct file has been supplied.

WGAWA0656E

An error occurred while sending a request to the LMI: *%s*. (0x38a70290)

Explanation
An attempt to make a Web service request against the LMI failed.

Administrator response
Check IBM Electronic Support for additional information - https://www.ibm.com/mysupport

WGAWA0658W

There are pending changes made by *%s* waiting to be deployed. (0x38a70292)

Explanation
This message is generated when there are changes made by the user using the LMI/Web services which are not active because they have not yet been deployed.

Administrator response
This is an informational message. No action is required.

WGAWA0660E

The network service, *%s* (*%s*:*%d*), is not accessible. (0x38a70294)

Explanation
This message is generated when the notification daemon detects that an external network service is not accessible.

Administrator response
Check to ensure that the correct host and port has been specified, and that the service is currently running.

WGAWA0662E

An invalid response code was returned from the request to *%s*: *%d* (0x38a70296)

Explanation
The responses from a Web request returned an unexpected response code.

Administrator response
Check the log file on the server for additional information.

WGAWA0663E

A failure occurred when attempting to retrieve the file. (0x38a70297)

Explanation
An attempt was made to retrieve a file, but for some reason the file was not retrieved correctly.

Administrator response
Check the log file on the server for additional information.

WGAWA0664E

No published snapshots are available. (0x38a70298)

Explanation
An attempt was made to apply a published snapshot but no published snapshots are available.

Administrator response
Publish a snapshot and then retry the operation.

Chapter 22. Security Access Manager configuration messages

These messages are provided by the Security Access Manager configuration component.

FBTTAC003E

An error occurred when reading or writing the file *file name*:\n*error text*\n

Explanation
An error occurred when either reading or writing a file. The error text contains additional information about the error.

System action
If the file is a non-critical file, the tool will attempt to proceed. If the file is critical to the operation being performed, the tool will exit.

Administrator response
Attempt to resolve the problem described by the error text. Verify that the file exists. If the error occurs because the tool does not have permission to modify the file, verify the file is writable.

FBTTAC004E

Unable to understand file *file name*, line *line number*.\n The text *invalid line from stanza file* is not valid.\n

Explanation
An error occurred when interpreting a stanza file. The file format does not appear to be correct.

System action
The file will not be read. The tool will exit.

Administrator response
The most likely cause of this error is that the file specified is not a Security Verify Access stanza file. Verify that the file specified is the correct file to use. If necessary, refer to the documentation for examples of how to use the autoconfiguration tool.

FBTTAC005E

Unable to connect to host *host name or IP address*, port *TCP port number*:\n*error text*\n

Explanation
The isamcfg tool tried to create a TCP connection to the server and port specified. The connection failed.

System action
The action taken depends on what connection failed. In some cases, the connection will be retried or the configuration will continue even though the connection failed. In other cases, the configuration will stop. Subsequent messages will explain what action is being taken.

Administrator response
The administrative response depends on which TCP connection failed and for what reasons. As a general rule, the administrator should verify connectivity to the machine to which the connection failed. Administrators should also verify that they entered the correct hostname and port information if they were prompted to do so.

FBTTAC006W

Please verify the WebSEAL server is running.\n

Explanation
The WebSEAL server does not appear to be running, so the autoconfiguration cannot proceed.

System action
The autoconfiguration tool will exit without modifying any configuration.

Administrator response
Start the WebSEAL server. If the WebSEAL server is already running, verify that the configuration file specified is correct.

FBTTAC007E

The file *file name* indicates that\n PDJrte has not been fully configured for your Java runtime. Please configure\n the PDJrte in 'full' mode before running the Security Verify Access autoconfiguration tool.\n

Explanation
The Security Verify Access autoconfiguration tool requires that the PDJrte package be fully configured before the tool is run.

System action
The autoconfiguration tool will exit without modifying any configuration.

Administrator response
Use the pdconfig program to configure the PDJrte in 'full' mode, and then rerun the Security Verify Access autoconfiguration tool.

FBTTAC008W

The stanza entry [*stanza name*]*entry name* was not found.\n

Explanation
The Security Verify Access autoconfiguration tool checked for but did not find the configuration file entry described in the message.

System action
If it is possible to proceed without that configuration entry, the autoconfiguration tool will do so. Otherwise the tool will exit.

Administrator response
Verify that the configuration file specified to the autoconfiguration tool belongs to a configured WebSEAL server.

FBTTAC011W

The value *property name* was not specified in the response file.\n

Explanation
The Security Verify Access autoconfiguration tool checked for but did not find the response file entry described in the message.

System action
If it is possible to proceed without the response file entry, the autoconfiguration tool will do so. Otherwise the tool will exit.

Administrator response
If the configuration proceeds, no action is necessary. If the configuration fails, attempt an interactive configuration by omitting the '-rspfile' option.

FBTTAC015E

An unexpected error occurred:\n*exception text*:\n*exception stack trace*\n

Explanation
Most error conditions are handled automatically by the autoconfiguration tool. This messages means an unexpected error occurred, and could not be handled automatically.

System action
The autoconfiguration tool will give the administrator an opportunity to make different selections for the configuration.

Administrator response
Attempt to diagnose the cause of the error based on the exception text. If possible, choose different configuration options.

FBTTAC019E

None of the endpoints for this federation are handled by this WebSEAL server. Configuration cannot continue. Federation endpoint URLs:

Explanation
The tool examined the URLs hosted by this WebSEAL server and the URLs used by the federation specified. None of the URLs for the federation are intended for this WebSEAL server. The message is followed by a list of endpoints for the federation.

System action
The autoconfiguration tool will give the administrator an opportunity to choose a different federation to configure.

Administrator response
Make sure that you have configured your WebSEAL server to specify on the appropriate hostnames and port number for the federation you are configuring.

FBTTAC022E

No capabilities are configured on this WebSEAL server.\n

Explanation
The tool checked for federations or capabilities that had been configured on this WebSEAL server, and there were none.

System action
The autoconfiguration tool will do nothing.

Administrator response
No administrative response is necessary unless the administrator wishes to configure federation information that was not detected by the autoconfiguration tool. In that case, the unconfiguration should be performed manually.

FBTTAC034E

The group *group name* exists in the registry but has not been imported into Security Verify Access.\n

Explanation
The group specified exists in the user registry, but has not been imported into Security Verify Access.

System action
The autoconfiguration tool will prompt the administrator to select a different group.

Administrator response
The administrator should either use a different group, or else use pdadmin or WPM to import the user into Security Verify Access.

FBTTAC035E

Unable to determine junction point for endpoint URL *URL*\n You may need to manually create a junction for that endpoint.\n

Explanation
The federation uses an endpoint that would require a junction / on the WebSEAL server. The autoconfiguration tool cannot create that junction.

System action
The autoconfiguration tool will skip creating that junction.

Administrator response
The administrator should either reconfigure their federation to use a different endpoint, or else manually create the / junction.

FBTTAC045E

Error creating ACL *acl name* and attaching it\n to *object name*: *exception message*\n

Explanation
An error occurred in the process of creating and attaching an ACL.

System action
The autoconfiguration tool will continue with the configuration.

Administrator response
The administrator may attempt to diagnose the error condition and fix the problem, or they may create the ACL manually.

FBTTAC046E

Junction creation failed with error code *error code*.\n

Explanation
An error occurred in the process of creating a junction. Other messages may have more information on the root cause of the problem.

System action
The autoconfiguration tool will continue with the configuration.

Administrator response
The administrator may attempt to diagnose the error condition and fix the problem, or they may create the junction manually.

FBTTAC047E

Junction creation failed.\n

Explanation
An error occurred in the process of creating a junction. Other messages may have more information on the root cause of the problem.

System action
The autoconfiguration tool will continue with the configuration.

Administrator response
The administrator may attempt to diagnose the error condition and fix the problem, or they may create the junction manually.

FBTTAC048W

Unable to locate the *library name* library.\n Using default library *library name*.\n

Explanation
The autoconfiguration tool could not find a library.

System action
The autoconfiguration tool will continue with the configuration, inserting a standard library path for the library location. The WebSEAL server may fail to start properly after the configuration is done.

Administrator response
If WebSEAL does not start after the configuration is complete, the administrator should check the WebSEAL log file to verify the problem is the library name, and then specify the correct name in the WebSEAL configuration file.

FBTTAC049W

Error interpreting federation endpoint '*endpoint type*', URL *url*:\n *exception text*\n

Explanation
The autoconfiguration tool could not interpret a URL associated with the federation.

System action
The autoconfiguration tool will continue with the configuration, ignoring the malformed URL.

Administrator response
The administrator may need to perform manual configuration for the endpoint.

FBTTAC054E

Error connecting to *url*:\n*exception text*\n

Explanation
The autoconfiguration tool could not connect to a URL.

System action
The autoconfiguration tool will prompt the administrator to correct the URL.

Administrator response
The administrator should correct the URL.

FBTTAC055E

The URL *url* does not appear to connect to a Web server.\n

Explanation
The autoconfiguration tool could not connect to a URL.

System action
The autoconfiguration tool will prompt the administrator to correct the URL.

Administrator response
The administrator should correct the URL.

FBTTAC056E

The request to the Web server failed. Response: *http error code http status message*:\n Response text:\n \n *text from web server*:\n \n \n

Explanation
The Web server returned an error for an HTTP request.

System action
The autoconfiguration tool will prompt the administrator to correct the URL.

Administrator response
The administrator may need to update the Web server configuration to fix the problem.

FBTTAC057W

Warning: the URL *url* appears to connect directly to WebSphere. For better performance and stability, connecting to a Web server running the WebSphere Web server plug-in is recommended.

Explanation
The administrator specified a URL that connects directly to WebSphere, which is not a recommended configuration.

System action
The autoconfiguration tool will prompt the administrator to correct the URL.

Administrator response
The administrator may need to update the Web server configuration to fix the problem.

FBTTAC059E

No federations were returned from the Security Verify Access InfoService.\n Response body:\n\n *response text* \n

Explanation
The Federated Identity Manager InfoService did not return any federations.

System action
The autoconfiguration tool will prompt the administrator to correct the URL for the InfoService.

Administrator response
The administrator should make sure that federations have been configured on the Federated Identity Manager server. It may be necessary to restart the WebSphere server if the configuration has been changed recently.

FBTTAC081E

Unable to create Security Verify Access administration context.\n

Explanation
An error occurred creating the Security Verify Access administration context. Other error messages with more detail may be displayed.

System action
The autoconfiguration tool will give the administrator an opportunity to specify a different Security Verify Access user-id ans password.

Administrator response
Attempt to diagnose the cause of the error based on the other error messages. Verify the administrator user-id and password are correct.

FBTTAC087E

ACL deletion failed:\n*error messages*\n.

Explanation
An error occurred in the process of deleting an ACL. Other messages may have more information on the root cause of the problem.

System action
The autoconfiguration tool will continue with the unconfiguration.

Administrator response
The administrator should delete the junction manually.

FBTTAC088E

Attribute deletion failed:\n*error messages*\n.

Explanation
An error occurred in the process of deleting extended attributes from an object. Other messages may have more information on the root cause of the problem.

System action
The autoconfiguration tool will continue with the unconfiguration.

Administrator response
The administrator should delete the attributes manually.

FBTTAC098E

An error occurred when restarting the WebSEAL server. Please check\n the log file *log file* to diagnose and fix the problem.\n

Explanation
The configuration tool tried to restart WebSEAL, but the server did not start.

System action
The autoconfiguration tool will not proceed until the WebSEAL server is operational.

Administrator response
The administrator should check the WebSEAL log file and correct the problem.

FBTTAC101W

An error occurred when executing the command *command*:\n *exception text*\n

Explanation
Executing a command failed.

System action
The action taken depends on which command failed, and for what reasons.

Administrator response
No response is necessary unless other problems occur.

FBTTAC102E

The Security Verify Access policy server was unable to modify an\n entry in the user registry because of insufficient access rights. You may\n need to update the ACLs applied to your user registry to grant the policy\n server access. The error message from the policy server was:\n *Security Verify Access error messages*\n

Explanation
An attempt to create a user or group failed, and the error message from the Security Verify Access policy server indicates that the problem is due to insufficient LDAP access rights.

System action
The user or group will not be created. If the user or group is not critical, the remainder of the configuration will proceed.

Administrator response
Refer to the Security Verify Access documentation on applying Security Verify Access ACLs to new LDAP suffixes for additional information on how to correct the LDAP ACLs.

FBTTAC111W

The Web server did not provide a CA certificate for the SSL handshake. You will need to contact the Web server administrator to obtain the CA certificate. Once you have obtained the CA certificate, add it to the WebSEAL key database manually.

Explanation
The fimtamcfg tool attempts to download the CA certificate from the Web server, since many Web servers include the CA certificate as part of the SSL handshake. The CA certificate was not included in the SSL handshake, so the administrator will need to obtain the certificate through other means.

System action
The configuration will continue without the CA certificate, but the junction from WebSEAL to the application server will not function correctly until WebSEAL has the CA certificate.

Administrator response
Refer to the message for instructions on how to resolve this problem. For assistance with adding the CA certificate to the WebSEAL key database, refer to the WebSEAL administration guide chapters discussing SSL and GSKit.

FBTTAC113E

Unable to convert key database *file name* from .kdb format to .jks format. The gsk7cmd program returned error code *numeric error code.log data*

Explanation
The fimtamcfg tool attempts to convert the WebSEAL key database from .kdb format to .jks (Java Key Store) format. This conversion failed with the specified error code and error text.

System action
The administrator will be prompted to either correct the problem or else cancel the configuration.

Administrator response
Read the messages printed to the screen to diagnose the root cause of the problem. Correct the problem, and then repeat the configuration.

FBTTAC114E

Unable to add the certificate *cert file* to the key database *file name*. The gsk7cmd program returned error code *numeric error code.log data*

Explanation
The fimtamcfg tool attempts to add a Web server's CA certificate to the WebSEAL key database. This process failed with the specified error code and error text.

System action
The administrator will be prompted to either correct the problem or else cancel the configuration.

Administrator response
Read the messages printed to the screen to diagnose the root cause of the problem. Correct the problem, and then repeat the configuration.

FBTTAC117E

The values provided in the response file for the SSL certificate did not match the values presented by the SSL server. Invalid value: *Certificate DN or fingerprint* Configuration cannot continue.

Explanation
The fimtamcfg tool checks the certificate presented by an SSL partner against the expected values recorded in a response file from previous configurations. The certificates did not match.

System action
The fimtamcfg tool will not continue configuration until the partner's certificate can be validated.

Administrator response
The administrator should make sure that the values they have provided for the Security Verify Access hostname and port are correct. If those values are correct, the administrator should verify the SSL certificate presented by the Web server is the correct certificate. If the hostname, port, and certificate are all correct, the administrator should run the configuration in interactive mode, without the -rspfile flag, to complete the task.

FBTTAC122E

The option *command line option* must be specified.

Explanation
The isamcfg tool was passed invalid command line options.

System action
The isamcfg tool will exit.

Administrator response
Review the isamcfg usage message and documentation and correct the command line options.

FBTTAC123E

The argument to the option *command line option* must be specified.

Explanation
The isamcfg tool was passed invalid command line options.

System action
The isamcfg tool will exit.

Administrator response
Review the isamcfg usage message and documentation and correct the command line options.

FBTTAC124E

The configuration option *command line option* is not valid.

Explanation
The isamcfg tool was passed invalid command line options.

System action
The isamcfg tool will exit.

Administrator response
Review the isamcfg usage message and documentation and correct the command line options.

FBTTAC125E

The file *file name* does not appear to belong to a WebSEAL server.

Explanation
The isamcfg tool examined the configuration file specified and determined it did not belong to a WebSEAL server.

System action
The tool will exit without changing any configuration.

Administrator response
The most likely cause of this error is that the file specified is not a Security Verify Access for Web stanza file that belongs to a WebSEAL server. Verify that the file specified is the correct file to use. If necessary, refer to the documentation for examples of how to use the autoconfiguration tool.

FBTTAC140W

LDAP server type '*ldap server type*' unknown. You should manually update the ACLs for the LDAP suffixes.

Explanation
The isamcfg tool tries to set appropriate ACLs on LDAP suffixes, but does not support all LDAP server types. The ACLs could not be updated because the LDAP server was not recognized.

System action
The configuration will continue without updating the ACLs.

Administrator response
The administrator should manually update the ACLs on the LDAP suffixes.

FBTTAC145W

Object already exists. Reusing existing object.

Explanation
The isamcfg tool tries to create LDAP objects as needed. An object already exists.

System action
The configuration will reuse the object.

Administrator response
No response necessary.

FBTTAC146W

Missing required property *property name*.

Explanation
A required property was not specified in the response file.

System action
The configuration will stop.

Administrator response
Correct the response file.

FBTTAC147W

Suffix already exists. Reusing existing suffix.

Explanation
The isamcfg tool tries to create LDAP suffixes as needed. A suffix already exists.

System action
The configuration will reuse the suffix.

Administrator response
No response necessary.

FBTTAC148W

LDAP server type '*ldap server type*' unknown. You should manually add LDAP suffixes.

Explanation
The isamcfg tool tries to automatically create suffixes, but does not support all LDAP server types. The suffixes could not be created because the LDAP server was not recognized.

System action
The configuration will continue without creating the suffixes.

Administrator response
The administrator should manually create the LDAP suffixes.

FBTTAC150E

Unable to connect to LDAP server:*exception*.

Explanation
The isamcfg tool was unable to make a connection to the LDAP server.

System action
The configuration will halt.

Administrator response
Verify that the hostname and port number specified for the connection are correct and that the LDAP server can be contacted.

FBTTAC151E

Unable to authenticate to LDAP server:*exception*. Verify that the user-id and password are correct.

Explanation
The isamcfg tool was unable to make a connection to the LDAP server.

System action
The configuration will halt.

Administrator response
Verify that the user-id and password specified for the connection are correct.

FBTTAC152E

Permission denied by LDAP server:*exception*. Verify that you are binding to LDAP as an administrative user with sufficient permissions to complete the configuration tasks.

Explanation
The isamcfg tool was unable to access the LDAP server because of insufficient access rights.

System action
The configuration will halt.

Administrator response
Verify that the user you are using to bind to LDAP has sufficient access rights to perform the failing configuration task.

FBTTAC153E

Object not found:*exception*. You may have specified an incorrect object DN, or you may need to create an LDAP suffix manually.

Explanation
The isamcfg tool was unable to create an object in the LDAP server because the parent object was not found.

System action
The configuration will halt.

Administrator response
Verify that you have specified the object DN correctly. You may need to create the suffix for the object manually.

FBTTAC154W

Configuration of authenticated SOAP endpoints with the IVT application is not recommended. Authentication for the IVT application can conflict with authentication for the SOAP endpoints.

Explanation
The IVT application requires forms authentication, while SOAP endpoints require certificate or BA authentication. Attempting to use both those authentication types simultaneously can cause one or both to stop functioning.

System action
The configuration will continue.

Administrator response
The administrator should use a separate WebSEAL server for SOAP endpoints.

FBTTAC166E

Unable to convert key database *file name* from .kdb format to .jks format. The *program name* program returned error code *numeric error code.log data*

Explanation
The isamcfg tool attempts to convert the WebSEAL key database from .kdb format to .jks (Java Key Store) format. This conversion failed with the specified error code and error text.

System action
The administrator will be prompted to either correct the problem or else cancel the configuration.

Administrator response
Read the messages printed to the screen to diagnose the root cause of the problem. Correct the problem, and then repeat the configuration.

FBTTAC167E

Unable to add the certificate *cert file* to the key database *file name*. The *program name* program returned error code *numeric error code*.*log data*

Explanation
The isamcfg tool attempts to add a Web server's CA certificate to the WebSEAL key database. This process failed with the specified error code and error text.

System action
The administrator will be prompted to either correct the problem or else cancel the configuration.

Administrator response
Read the messages printed to the screen to diagnose the root cause of the problem. Correct the problem, and then repeat the configuration.

FBTTAC172W

Unable to find running reverse proxy instances when connecting to host *host URL*. *error text*

Explanation
The isamcfg tool tried to query the number of running reverse proxy instances on a Security Verify Access Appliance. No running instances were found.

System action
The isamcfg utility will not proceed until a running reverse proxy instance is found on a Security Verify Access Appliance.

Administrator response
The administrative response should be to check that the URL of the Web Appliance Gateway that needs to be configured is valid and correct. The administrator should also ensure that there are running reverse proxy instances on the target Security Verify Access Appliance.

FBTTAC173E

Error interpreting configuration URL *url*:\n *exception text*\n

Explanation
The isamcfg tool could not interpret the Security Verify Access Appliance configuration URL.

System action
The isamcfg utility will not proceed until a valid Security Verify Access Appliance configuration URL is specified.

Administrator response
The administrator may need to specify a valid Security Verify Access Appliance configuration URL.

FBTTAC174E

An error occurred when restarting the reverse proxy instance '*instance name*' on the Security Verify Access Appliance. Please check\n the log file of the reverse proxy instance on the Security Verify Access Appliance to diagnose and fix the problem.\n

Explanation
The configuration tool tried to restart a reverse proxy instance on a Security Verify Access Appliance, but the server did not start.

System action
The autoconfiguration tool will not proceed until the reverse proxy instance is operational.

Administrator response
The administrator should check the Security Verify Access Appliance's reverse proxy instance log file and correct the problem.

FBTTAC176E

An error occurred during an attempt to connect to the Security Verify Access Appliance. The response code was *response code*:\n*error text*\n

Explanation
An error occurred during an attempt to connect to the Security Verify Access Appliance. The response code and error text contains additional information about the error.

System action
If the change being made is non-critical file, the tool will attempt to proceed. If the change is critical to the operation being performed, the tool will exit.

Administrator response
Attempt to resolve the problem described by the error text. Ensure that the tool has access to the network where the Security Verify Access Appliance is running.

FBTTAC187E

POP creation failed:\n*error messages*\n.

Explanation
An error occurred in the process of creating a POP. Other messages may have more information on the root cause of the problem.

System action
The autoconfiguration tool will continue with the configuration.

Administrator response
Attempt to diagnose the error condition and fix the problem, or create the POP manually.

FBTTAC188E

An invalid URL value was entered.

Explanation
The value entered was not a valid URL.

System action
The autoconfiguration tool will show the URL entry prompt again.

Administrator response
Enter a valid URL.

FBTTAC189E

No OAuth federations were returned from the Security Verify Access InfoService.\n

Explanation
The Federated Identity Manager InfoService did not return any OAuth federations.

System action
The autoconfiguration tool will do nothing.

Administrator response
The administrator should make sure that OAuth federations were configured on the Federated Identity Manager server. It may be necessary to restart the WebSphere server if the configuration was recently changed.

FBTTAC190E

The file *file name* does not exist in the file system.\n

Explanation
The file does not exist on the file system.

System action
The autoconfiguration tool will do nothing.

Administrator response
Verify that the file exists.

FBTTAC228E

The Security Verify Access autoconfiguration tool requires *tool name* on the system PATH.

Explanation
A tool required by the Security Verify Access autoconfiguration tool was not available on the system PATH.

System action
The autoconfiguration tool will exit without modifying any configuration.

Administrator response
Add the appropriate tool (gsk7ikm or ikeycmd) to the system PATH and then rerun the Security Verify Access autoconfiguration tool.

FBTTAC240E

Unable to delete the certificate *cert file* from the key database *file name*. The *program name* program returned error code *numeric error code.log data*

Explanation
The isamcfg tool attempted to delete a CA certificate from the WebSEAL key database. This process failed with the specified error code and error text.

System action
Correct the problem or cancel the configuration.

Administrator response
Read the messages printed to the screen to diagnose the root cause of the problem. Correct the problem, and repeat the configuration.

FBTTAC241E

Error occurred while trying to find *cert file* in the key database *file name*. The *program name* program returned error code *numeric error code.log data*

Explanation
The isamcfg tool attempted to find a CA certificate in the WebSEAL key database. This process failed with the specified error code and error text.

System action
Correct the problem or cancel the configuration.

Administrator response
Read the messages printed to the screen to diagnose the root cause of the problem. Correct the problem, and repeat the configuration.

Chapter 23. Security token service module messages

These messages are provided by the security token service module component.

FBTSTM006E

The given TokenType or AppliesTo (*TokenType/AppliesTo*) in the request is not supported by this server's configuration for *RequestType* RequestType.

Explanation
The request requested a TokenType or AppliesTo that is not supported by the server's configuration. This error can occur because the request data did not map to any processing chains or because the expected processing chain that the request maps to did not start correctly.

System action
The request has been halted.

Administrator response
Ensure that the request has all the required data.

FBTSTM007E

STSModule *module_name* not found.

Explanation
The server attempted to load the STSModule but could not because an error occurred.

System action
The module has not been loaded possibly because the chains that the module is in have not been loaded.

Administrator response
Check the server logs for errors and exceptions to identify the problem.

FBTSTM008E

The QName namespace prefix (*QName*) does not match any defined namespaces.

Explanation
The given namespace prefix does not match any defined namespaces.

System action
The request has been halted.

Administrator response
Ensure that the request uses supported XML namespaces.

FBTSTM009E

The server did not start correctly.

Explanation
The trust server did not start correctly because of internal errors.

System action
The server will not accept requests.

Administrator response
Inspect logs and configuration files and ensure that data in the configuration file is correct.

FBTSTM010E

A TokenType or AppliesTo must be specified in the request.

Explanation
According to the specification, at least one of TokenType or AppliesTo must be specified in the request.

System action
The request has been halted.

Administrator response
Ensure that the required request data is given.

FBTSTM011E

The date and time are not in the expected UTC format.

Explanation
The date and time given in the request was not in the expected UTC time format.

System action
The request has been halted.

Administrator response
Ensure that the correct time format is used for the request.

FBTSTM013E

A RequestType must be specified in the request.

Explanation
According to the specification, a RequestType must be specified in the request.

System action
The request has been halted.

Administrator response
Ensure that the required request data is given.

FBTSTM014E

The given RequestType (*RequestType*) is not supported by this server's configuration.

Explanation
The RequestType does not apply to any of the STSChainMappingDefinitions located in the server's configuration.

System action
The request has been halted.

Administrator response
Ensure that the required request data is given.

FBTSTM015E

Either no configured XPath selected a node from the request, or the given TokenType or AppliesTo (*TokenType/AppliesTo*) in the request is not supported by this server's configuration for *RequestType* RequestType and Issuer (*Issuer*).

Explanation
Either no XPath in the configuration selected a node from the request, or the request requested a TokenType or AppliesTo that is not supported by the server's configuration.

System action
The request has been halted.

Administrator response
Ensure that the required request data is given.

FBTSTM016E

The given Issuer (*Issuer*) is not supported by this server's configuration.

Explanation
The Issuer does not apply to any of the STSChainMappingDefinitions located in the server's configuration.

System action
The request has been halted.

Administrator response
Ensure that the required request data is given.

FBTSTM017E

The server could not find the expected token included in the request.

Explanation
The given request did not include the expected token based on the server's configuration.

System action
The request has been halted.

Administrator response
Ensure that the required request data is given.

FBTSTM018E

An incorrect namespace was encountered and received *QName*, but expected *QName*.

Explanation
The client sent a request that used a namespace that was not expected. This error is typically caused by an old namespace being used.

System action
The request has been halted.

Administrator response
Ensure that the supported XML namespaces are used.

FBTSTM019E

The expected namespace *URI* for the WS-Trust schema was not found in the request.

Explanation
The client did not specify a valid WS-Trust schema in the request.

System action
The request has been halted.

Administrator response
Ensure that the required request data is given.

FBTSTM020E

An error was encountered when attempting to open file *filename*.

Explanation
The server attempted to open the specified file and encountered an error.

System action
The operation did not complete.

Administrator response
Ensure that the file exists and has the correct file permissions.

FBTSTM021E

Either the properties file (*filename*) was not found in the classpath or the key (*key*) returned no data.

Explanation
The given properties file could not be found in the classpath or the key to look up data in the properties file did not return the expected data.

System action
The operation did not complete.

Administrator response
Ensure that the given properties file is located in the classpath, or that the key given has data associated with it, or both.

FBTSTM022E

The message passed to the service from the webservices runtime was not complete or did not exist.

Explanation
A possible cause of this problem is that the Trust Service System Handler was not installed correctly or was removed from the system.

System action
The request was halted.

Administrator response
Ensure that the Trust Service System Handler is installed and located in the WebSphere Application Server classpath.

FBTSTM023E

The trust service did not start successfully because it could not locate the local or distributed configuration data.

Explanation
The trust service could not locate the configuration data.

System action
The service did not start.

Administrator response
If the service is the only service for the domain, ensure that the configuration file exists. If the service is in a cluster, ensure that the cluster is operating correctly.

FBTSTM030E

The trust service did not fully stop.

Explanation
See message.

System action
No action taken.

Administrator response
No response required.

FBTSTM031E

The trust service did not fully start.

Explanation
See message.

System action
No action taken.

Administrator response
No response required.

FBTSTM032E

The trust service did not fully start, stop, or both.

Explanation
See message.

System action
No action taken.

Administrator response
No response required.

FBTSTM033E

The trust service failed to write configuration to persistent storage.

Explanation
See message.

System action
No action taken.

Administrator response
No response required.

FBTSTM034E

The context was not found.

Explanation
See message.

System action
No action taken.

Administrator response
No response required.

FBTSTM035E

The management method requested is not implemented.

Explanation
See message.

System action
No action taken.

Administrator response
No response required.

FBTSTM036E

An error occurred while retrieving the server's configuration for the management operation.

Explanation
The server encountered an error when it attempted to retrieve its configuration.

System action
The operation was halted.

Administrator response
Check logging messages for errors related to retrieving the server's configuration and ensure that the correct file permissions are set on the server's configuration file.

FBTSTM038E

A classname must be provided.

Explanation
The caller-requested operation requires a classname but did not provide a classname.

System action
The operation was halted.

Administrator response
Ensure that a classname is given.

FBTSTM039E

The classname provided (*classname*) was not found in the server's classpath.

Explanation
A classname was provided that does not exist in the server's classpath.

System action
The operation was halted.

Administrator response
Ensure that the given class exists in the server's classpath.

FBTSTM041E

The classname provided (*classname*) does not implement the required interface for modules.

Explanation
The classname provided exists but does not implement the required interface for modules.

System action
The operation was halted.

Administrator response
Ensure that the classname provided implements the required interface for modules.

FBTSTM042E

The classname provided (*classname*) does not implement the expected model.

Explanation
The classname provided does not have a no-argument public constructor.

System action
The operation was halted.

Administrator response
Ensure that the classname provided includes a no-argument public constructor.

FBTSTM043E

The given unique identifier (*identifier*) does not exist in the configuration.

Explanation
The given unique identifier does not exist.

System action
The operation was halted.

Administrator response
Ensure that the provided identifier exists in the current configuration.

FBTSTM044E

The remove request could not be completed. There must be no references to the object being removed in order for the request to complete.

Explanation
There must be no references to the configuration data being removed.

System action
The operation was halted.

Administrator response
Ensure that the configuration data being removed does not have any references to it.

FBTSTM046E

The unique identifier did not match the expected type.

Explanation
The given unique identifier did not match the expected type in the configuration. This error might also mean that the unique identifier did not exist in the configuration.

System action
The operation was halted.

Administrator response
Ensure that the entire unique identifier is for the correct data.

FBTSTM047E

A unique identifier must be provided.

Explanation
A unique identifier was not provided.

System action
The operation was halted.

Administrator response
Ensure that a unique identifier is provided.

FBTSTM048E

The request type is already in the configuration.

Explanation
The management request to add a new request type was denied because there cannot be duplicate request types in the configuration.

System action
The operation was halted.

Administrator response
Ensure that the request type is not already in the configuration.

FBTSTM049E

To add a request type, a request type URI must be provided.

Explanation
A request type URI was not provided and is required.

System action
The operation was halted.

Administrator response
Ensure that a unique request type URI is provided.

FBTSTM050E

The mapping type given is not a supported mapping type.

Explanation
Either the mapping type was not given or it did not match one of the supported mapping types.

System action
The operation was halted.

Administrator response
Ensure that the mapping type is one of the supported mapping types.

FBTSTM051E

The request-type mapping requested to be modified does not exist.

Explanation
The request-type mapping requested to be modified does not exist in the server's configuration.

System action
The operation was halted.

Administrator response
Ensure that the request type mapping that is being modified exists in the server's configuration.

FBTSTM058E

The chain (*chain identifier*) could not be initialized due to errors.

Explanation
The given chain could not be started without errors being returned.

System action
The operation was halted.

Administrator response
Check the trace logs for a more specific error for the given chain.

FBTSTM059E

The request failed to process successfully.

Explanation
The given request failed to process successfully. See the server logs for a specific cause of the failure.

System action
The request was halted.

Administrator response
Check the trace logs for a more specific error for the given chain.

FBTSTM060E

The module reference ID used in the configuration of module chain ID '*chainId*', (*chainReference*) is not valid. The module reference does not exist.

Explanation
The referenced identifier does not exist.

System action
The module chain will not be available at runtime.

Administrator response
Validate the STS configuration.

FBTSTM061E

The module reference used in the configuration of module chain ID '*chainId*', (*referenceId*) is not valid. The module does not exist.

Explanation
The referenced module does not exist.

System action
The module chain will not be available at runtime.

Administrator response
Validate the STS configuration and installed STS plug-ins.

FBTSTM062E

The class '*className*' referenced in module chain ID '*chainId*' could not be initialized. The init method did not successfully complete.

Explanation
The module implementation did not successfully initialize.

System action
The module chain will not be available at runtime.

Administrator response
Validate the STS configuration and installed STS plug-ins.

FBTSTM063E

The module chain with ID '*id*' could not be created because of an earlier error.

Explanation
The module chain could not be successfully created.

System action
The module chain will not be available at runtime.

Administrator response
Validate the STS configuration and installed STS plug-ins.

FBTSTM064E

The module chain with ID '*id*' does not exist.

Explanation
The module chain could not be located in the configuration.

System action
The module chain will not be available at runtime.

Administrator response
Validate the STS configuration and installed STS plug-ins.

FBTSTM065E

The input request did not contain any data and cannot be processed.

Explanation
The input request was null or was not provided.

System action
The request cannot be processed.

Administrator response
Validate the configuration of the caller and the input message.

FBTSTM067E

The module chain mapping with ID '*id*' references a group that does not exist.

Explanation
The group membership was either not specified or does not exist in the configuration. Modules with the module chain may need information from this group to operate.

System action
The module chain mapping will not be available at runtime.

Administrator response
Validate the STS configuration and installed STS plug-ins.

FBTSTM068W

The server encountered an exception while processing a request in validate mode. If the environment has trace enabled, the exception will appear in the trace log.

Explanation
The STS encountered an exception while processing a request in the validate mode. According to specifications, the server must return a status code similar to the following: http://schemas.xmlsoap.org/ws/2005/02/trust/status/invalid. The exception was caught and logged, allowing the server to return the correct message.

System action
The request failed. The server returned an http://schemas.xmlsoap.org/ws/2005/02/trust/status/invalid status message.

Administrator response
Validate the request parameters and retry the operation.

FBTSTM069E

The security token service could not create a logger in the given directory (*directory name*) because it is not a directory.

Explanation
The Security Token Service was not able to create a logger in the given directory because it is not a directory.

System action
The logger will not log messages.

Administrator response
Ensure the given directory is a valid directory.

FBTSTM070E

The security token service message logger encountered an error and could not log the message.

Explanation
The security token service message logger encountered an error that is preventing it from logging messages.

System action
The logger will not log messages.

Administrator response
Confirm that the system is allocated enough resources and there are no initialization errors.

FBTSTM071E

The security token service message logger encountered an error while creating the log file. The error text is: *file name*.

Explanation
The Security Token Service was not able to create a log file because an error occurred.

System action
The logger will not log messages.

Administrator response
Correct the logger name.

FBTSTM072E

The security token service message for chain mapping (*Mapping*) failed signature validation.

Explanation
The Security Token Service was not able to validate the signature on the trust message. This may be caused by an incorrect key alias configured for this chain mapping or the SOAP request was modified along the way or the message was not signed by a trusted signer.

System action
The message is rejected.

Administrator response
Verify that the correct key alias is configured and the SOAP message was not modified en route.

FBTSTM073E

The security token service is configured to validate signatures for chain mapping (*Mapping*) but the request received was not signed.

Explanation
The Security Token Service was not able to validate the signature on the trust message. Threceived request was not signed.

System action
The message is rejected.

Administrator response
Ensure that the message came from a trusted source and that the message must be signed.

FBTSTS021E

The Keystore service is not available for signing or validating assertions.

Explanation
The Keystore service was not started or has encountered an error.

System action
The request has been halted.

Administrator response
Validate the configuration and restart the server.

FBTSTS310E

The contents of the JWT could not be parsed as valid JSON.

Explanation
An parsing error occured when parsing the JWT.

System action
The request is halted.

Administrator response
Check the contents of the JWT.

FBTSTS311E

An error occured when performing an operation on the JWT.

Explanation
The JWT could not be validated.

System action
The request is halted.

Administrator response
Check the logs to determine the cause of the failure.

FBTSTS312E

The signature of the JWT was not valid.

Explanation
Signature verification of the JWT failed.

System action
The request is halted.

Administrator response
Check the JWT and the method of signature validation.

FBTSTS313E

The payload of the JWT could not be decrypted.

Explanation
The JWT could not be de-encrypted.

System action
The request is halted.

Administrator response
Check the JWT keys configured for use when performing decryption.

FBTSTS314E

The JWT algorithm provided was unknown or invalid.

Explanation
An unsupported JWT algorithm was provided.

System action
The request is halted.

Administrator response
Check the JWT or the chain configuration.

FBTSTS315E

The header portion of the JWT was not valid.

Explanation
The JWT headers could not be parsed

System action
The request is halted.

Administrator response
Check the JWT.

FBTSTS316E

A 'none' signed JWT was provided, when there was a signature or information to perform signature validation present.

Explanation
JWTs signed with 'none' will be rejected if there was any data present by which to perform signature validation. This is to prevent attacks by moifying a JWT header, and dropping the signature.

System action
The request is halted.

Administrator response
Ensure there is nothing configured which would be used to perform signature validation (Hmac key, or keystore and lable.

FBTSTS317E

The JWT was empty.

Explanation
The token element of the message was empty.

System action
The request is halted.

Administrator response
Check the request.

FBTSTS318E

The token payload contained the wrong type. The type [*attributeName*] was provided, when [*attributeName*] was expected.

Explanation
The token presented must have the correct type attribute

System action
The request is halted.

Administrator response
Check the request

FBTSTS319E

The request did not contain a JWT token.

Explanation
There was no token element present in the request.

System action
The request is halted.

Administrator response
Check the request.

FBTSTS320E

The claim [*attributeName*] did not match the configured value.

Explanation
The value provided did not match the pattern or value configured for that claim.

System action
The requiest is halted.

Administrator response
Check the request and the chain configuration.

FBTSTS321E

The JWT presented has expired.

Explanation
The 'exp' claim is in the past.

System action
The request is halted.

Administrator response
Check the JWT and the system clock. Optionally adjust the validation skew value.

FBTSTS322E

The JWT presented is not yet considered valid.

Explanation
The 'nbf' claim is in the future.

System action
The request is halted.

Administrator response
Check the JWT and the system clock. Optionally adjust the validation skew value.

FBTSTS323E

A JWT could not be formed.

Explanation
A JWT could not be formed from the provided values

System action
The request is halted.

Administrator response
Check the request, or the chain configuration.

Chapter 24. Single sign-on protocol service messages

These messages are provided by the single sign-on protocol service component.

FBTSPS002E

The requester cannot be prompted for an identity provider. No defined federations are valid for the request.

Explanation
The current request and delegate protocol do not match any known defined federation.

System action
The request will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service.

FBTSPS003E

The template *identifier* cannot be located.

Explanation
The current request action cannot be processed.

System action
The request will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service.

FBTSPS004E

The template document used to request a requester's identity provider is not valid.

Explanation
The template document is missing the required tokens or is not a valid XML document.

System action
The request will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service.

FBTSPS006E

The request message could not be understood by the adapter.

Explanation
The request adapter was unable to adapt the input message.

System action
The request will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service and the input message.

FBTSPS007E

The single sign-on protocol service is in a state such that the status cannot be displayed with a template page.

Explanation
This error can be caused by an input request before the single sign-on protocol service is fully bootstrapped or it is caused by a configuration that is not valid.

System action
The request will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service and the input message.

FBTSPS008E

Requests cannot be accepted.

Explanation
This error can be caused by an input request before the single sign-on protocol service is fully bootstrapped or it can be caused by a configuration that is not valid.

System action
The request will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service and the input message.

FBTSPS010E

The request to address *address* cannot be accepted.

Explanation
This error might be caused by misconfiguration or by a request that is not valid.

System action
The request will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service and the input message.

FBTSPS011E

The protocol for address *address* could not be determined.

Explanation
This error typically occurs because the configuration is not valid or because a configuration has not been received.

System action
The request will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service and replication latency.

FBTSPS012E

The single-sign on protocol service has not started.

Explanation
This error typically occurs because the configuration is not valid or because a configuration has not been received.

System action
The request will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service and replication latency.

FBTSPS014E

An instance of a distributed map cannot be retrieved.

Explanation
Without the distributed map, the single sign-on protocol service cannot be configured.

System action
The request will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service and environment.

FBTSPS015E

An error occurred while moving to a new configuration.

Explanation
The newly set or retrieved configuration could not be used.

System action
The request will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service and environment.

FBTSPS017E

An error occurred while bootstrapping the single sign-on protocol service.

Explanation
The configuration could not be found or contains items that are not valid.

System action
The startup will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service. A detailed message can be found in the trace.

FBTSPS018E

The version of the configuration *inputVersion* is not valid for the single sign-on protocol service.

Explanation
The configuration version is not valid.

System action
The startup will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service and the configuration versions.

FBTSPS020E

The configured component *className* cannot be loaded.

Explanation
The configuration component is not valid.

System action
The startup will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service and the configuration versions.

FBTSPS021E

The configured endpoint *endpoint* is not valid.

Explanation
The configuration component is not valid.

System action
The startup will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service and the configuration versions.

FBTSPS025E

Unable to register a management bean.

Explanation
The configuration component is not valid.

System action
The startup will be halted.

Administrator response
Check the log file for errors.

FBTSPS027E

The configured delegate protocol *delegate* is not valid.

Explanation
The configuration component is not valid.

System action
The startup will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service and valid configuration versions

FBTSPS029E

The configured delegate protocol *delegate* has a configuration entry that is not valid for the configuration file location.

Explanation
The configuration component is not valid.

System action
The startup will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service and valid configuration versions.

FBTSPS037E

The single sign-on protocol service configuration file cannot be located. This result might be expected.

Explanation
The configuration component is not valid.

System action
The startup will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service and the configuration versions.

FBTSPS038E

The configuration file at *confLocation* cannot be read. This file is specified in the configuration and is required for the single sign-on protocol service to start.

Explanation
The configuration file is not valid. This result might be due to access violations or an XML validation error.

System action
The startup will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service and the configuration versions.

FBTSPS039E

The component *component* cannot be created.

Explanation
The configuration file is not valid, or a specified class could not be loaded.

System action
The startup will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service and the configuration versions.

FBTSPS040E

The component *component* cannot be created. The provided configuration is not valid.

Explanation
The configuration file is not valid.

System action
The startup will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service and the configuration versions.

FBTSPS041E

No input was received with the management operation.

Explanation
The management operation is not valid.

System action
The operation will be halted.

Administrator response
Validate the management operation.

FBTSPS042E

The property, *property*, is required for this operation.

Explanation
The management operation is not valid.

System action
The operation will be halted.

Administrator response
Validate the management operation.

FBTSPS043E

The page factory root, *root*, does not exist.

Explanation
The management operation is not valid.

System action
The operation will be halted.

Administrator response
Validate the management operation.

FBTSPS044E

The page factory default language, *root*, does not exist.

Explanation
The management operation is not valid.

System action
The operation will be halted.

Administrator response
Validate the management operation.

FBTSPS045E

The given reference ID, *id*, is not valid.

Explanation
The management operation is not valid.

System action
The operation will be halted.

Administrator response
Validate the management operation.

FBTSPS046E

The given classname ,*classname*, could not be loaded.

Explanation
The management operation is not valid.

System action
The operation will be halted.

Administrator response
Validate the management operation.

FBTSPS047E

The given entity, *entity*, does not exist.

Explanation
The management operation is not valid.

System action
The operation will be halted.

Administrator response
Validate the management operation.

FBTSPS048E

The given value, *value*, is not valid for configuration item *item*.

Explanation
The management operation is not valid.

System action
The operation will be halted.

Administrator response
Validate the management operation.

FBTSPS051E

The WebSEAL authentication service client cannot be initialized.

Explanation
The management operation is not valid.

System action
The operation will be halted.

Administrator response
Validate the management operation.

FBTSPS052E

The WebSEAL authentication service client is not in a valid state because the configuration is not valid and cannot be used.

Explanation
The sign in or sign out operation cannot be performed.

System action
The operation will be halted.

Administrator response
Validate the configuration of the authentication service and policy server configuration files.

FBTSPS053E

The credential included with the request, *cred*, is not valid.

Explanation
The credential format is not understandable.

System action
The operation will be halted.

Administrator response
Validate the configuration of the authentication service and WebSEAL.

FBTSPS054E

The entity ID, *id*, is not valid.

Explanation
The configuration component is not valid.

System action
The startup will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service and the configuration versions.

FBTSPS055E

The configured class, *classN*, does not implement or extend the required class or interface, *intf*.

Explanation
The configuration file is not valid.

System action
The startup will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service and the configuration versions.

FBTSPS056E

The token included with the sign in request, *cred*, is not valid.

Explanation
The token type and format is not understandable.

System action
The operation will be halted.

Administrator response
Validate the configuration of the authentication service and caller.

FBTSPS057E

The required WebSEAL header, *cred*, is missing.

Explanation
The header is required for proper operation.

System action
The operation will be halted.

Administrator response
Validate the WebSEAL configuration.

FBTSPS058E

The sign out operation has failed.

Explanation
Sign out failed.

System action
The operation will be halted.

Administrator response
Check the trace log for detailed output from the policy server.

FBTSPS059E

The configured default page factory selector, *selector*, is not valid.

Explanation
The specified default selector is not valid.

System action
The management operation will be halted.

Administrator response
Check the configured default against the available selectors.

FBTSPS060E

Page factory operation requires at least one page selector.

Explanation
The specified page factory configuration does not specify any selectors.

System action
The management operation will be halted.

Administrator response
Check the configuration of the page factory.

FBTSPS061E

An unexpected error has occurred with a protocol module *module*.

Explanation
This error might be caused by misconfiguration or by a request that is not valid.

System action
The request will be halted.

Administrator response
Validate the configuration of the single sign-on protocol service, protocol module, and the input message.

FBTSPS062E

The Point of Contact protocol module is missing the required action, specified by parameter *parameter*.

Explanation
This error is typically caused by a request that is not valid. The action parameter is necessary to determine the behavior of the module.

System action
The request will be halted.

Administrator response
Validate the request message.

FBTSPS063E

The Point of Contact protocol module is missing the required token for the chosen action.

Explanation
This error is typically caused by a request that is not valid. The token is necessary to perform the specified action.

System action
The request will be halted.

Administrator response
Validate the request message.

FBTSPS064E

The configured module with ID *id* and version *version* was not found when searching for modules.

Explanation
The module with the specified ID and version was not found while attempting to load modules. This can occur if the Federated Identity Manager modules have not been configured correctly or the module does not exist.

System action
The request to load the module will be halted.

Administrator response
Validate the Federated Identity Manager configuration.

FBTSPS065E

The configured module with ID *id* does not expose a class with ID *id*.

Explanation
The module with the given ID and exposed class ID was not found while attempting to load modules. This can occur if the Federated Identity Manager modules have not been configured correctly or the module does not exist.

System action
The request to load the module will be halted.

Administrator response
Validate the Federated Identity Manager configuration.

FBTSPS066E

The configured module with ID *id* referencing a module with ID *moduleId* with java class *className* cannot be instantiated.

Explanation
When attempting to load a module with the given ID and class name, an error occurred. This can occur if the if the Federated Identity Manager modules have not been configured correctly or the module does not exist.

System action
The request to load the module will be halted.

Administrator response
Validate the Federated Identity Manager configuration.

FBTSPS067E

The configured module reference, *referenceId*, could not be located in the configuration.

Explanation
In order to load a module, a valid reference ID is required.

System action
The request to load the module will be halted.

Administrator response
Validate the Federated Identity Manager configuration.

FBTSPS068E

An attempt was made to retrieve a component with identifier '*id*' which does not exist.

Explanation
In order to load a component, a valid reference ID is required.

System action
The request to load the component will be halted.

Administrator response
Validate the Federated Identity Manager configuration.

FBTSPS069E

The delegate protocol instance *delegateId* requires a protocol action *actionClassName* which could not be created.

Explanation
The actions for the delegate protocol need to be located and created in order to be invoked.

System action
The request to load the component will be halted.

Administrator response
Validate the Federated Identity Manager configuration.

FBTSPS073E

The group membership *group* specified for delegate *id* is not valid and will be ignored.

Explanation
The specified group ID does not exist or could not be found.

System action
The protocol module will not have access to that group's properties.

Administrator response
Validate the Federated Identity Manager configuration.

FBTSPS074E

The delegate protocol *id* will not be available at runtime because the properties provided in the groups that it is a member of are not valid.

Explanation
The properties for the delegate group memberships are not correct. This typically indicates that federation configuration is not valid.

System action
The protocol module will not be available at runtime.

Administrator response
Validate the Federated Identity Manager configuration. Additional messages in the error and trace logs by the protocol implementation will display the exact error condition.

FBTSPS075E

The delegate protocol *id* will not be available at runtime because the protocol action *className* could not be created.

Explanation
A protocol action used by this delegate could not be created.

System action
The protocol module will not be available at runtime.

Administrator response
Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS076E

An error occurred reading page templates. The SPS will continue startup, but no pages will be available at runtime.

Explanation
An error occurred reading the pages directory. The directory may not exist or the service may not have the required permissions to read the files.

System action
Startup will continue, but pages will not be available at runtime.

Administrator response
Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS077E

An error occurred creating the service factory *id*. This service factory will not be available to protocols at runtime.

Explanation
An error occurred creating the service factory.

System action
Startup will continue, but the service will not be available at runtime.

Administrator response
Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS078E

An error occurred creating the point of contact client *id*. The service will not be available to protocols at runtime.

Explanation
An error occurred creating the point of contact client.

System action
Startup will continue, but the service will not be available at runtime.

Administrator response
Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS079E

An error occurred creating the global handler *id*. The service will not be available at runtime.

Explanation
An error occurred creating the global handler.

System action
Startup will continue, but the service will not be available at runtime.

Administrator response
Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS080E

An error occurred creating the protocol determination module *id*. The service will not be available at runtime.

Explanation
An error occurred creating the protocol determination module.

System action
Startup will continue, but the service will not be available at runtime.

Administrator response
Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS081E

Unable to retrieve an instance of the IdServiceClientFactory.

Explanation
An error occurred retrieving an instance of the alias service client factory.

System action
Startup will continue, but the service will not be available at runtime.

Administrator response
Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS082E

Unable to retrieve an instance of the Token Command Factory with endpoint *endpoint*.

Explanation
An error occurred retrieving an instance of the token service client factory.

System action
Startup will continue, but the service will not be available at runtime.

Administrator response
Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS083E

The single sign-on protocol service was unable to locate a directory where template pages are stored.

Explanation
The Federated Identity Manager application does not contain the directory containing template page directories.

System action
No template pages can be used.

Administrator response
Validate the Federated Identity Manager configuration.

FBTSPS084E

An internal error has occurred within the SPS.

Explanation
The current request could not be processed because of an internal error.

System action
Processing of the current request will be halted.

Administrator response
Validate the Federated Identity Manager configuration.

FBTSPS085E

The current request cannot be accepted because the component that is required to process it is missing.

Explanation
The current request could not be processed because of an internal error.

System action
Processing of the current request will be halted.

Administrator response
Validate the Federated Identity Manager configuration.

FBTSPS087E

Unable to retrieve an instance of the Name Identifier Generator with key *id*.

Explanation
An error occurred retrieving an instance of the specified NameId generator from the alias service.

System action
The request is stopped.

Administrator response
Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS088W

The time zone identifier given, [*id*], is not valid.

Explanation
The given time zone identifier is not a supported time zone.

System action
The default UTC time zone will be used.

Administrator response
Ensure that the time zone identifier in the configuration is correct. Check the returned exception for more details.

FBTSPS089W

The time display pattern [*id*] is not supported.

Explanation
The given time display pattern is not supported.

System action
The default ISO8601 time format will be used.

Administrator response
Ensure that the time format in the configuration is correct. Check the returned exception for more details.

FBTSPS090W

The callback [*id*] could not be initialized.

Explanation
An error was encountered during the initialization of the given callback.

System action
The given callback will be removed from the list of running callbacks.

Administrator response
Check the logs for a related exception and correct the problem. The error is most likely caused by a configuration error.

FBTSPS092E

Access denied.

Explanation
The user does not have permission to access the Web page.

System action
The user will be shown a Web page indicating that access is not allowed.

Administrator response
If the user should be permitted to access the Web page, the administrator should grant the user permission. The administrator may need to add a user to the group being used for SOAP endpoint access control, for instance.

FBTSPS096E

The point of contact implementation failed to perform programmatic login.

Explanation
An error occurred performing JAAS login.

System action
The request is stopped.

Administrator response
Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS097E

The point of contact implementation failed to authenticate the user performing the request.

Explanation
An error occurred performing JAAS login.

System action
The request is stopped.

Administrator response
Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS098E

The point of contact implementation failed to obtain the initial request URL.

Explanation
An error occurred obtaining the initial request URL from the user session.

System action
The request is stopped.

Administrator response
Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS106E

ITFIM Form Login Error

Explanation
See message.

System action
No action taken.

Administrator response
Check the trace and message logs for further details.

FBTSPS107E

Form Login Error

Explanation
See message.

System action
No action taken.

Administrator response
Check the trace and message logs for further details.

FBTSPS109E

Form authentication failed.

Explanation
See message.

System action
No action taken.

Administrator response
Check the trace and message logs for further details.

FBTSPS110E

Check the user ID and password, and try again.

Explanation
See message.

System action
No action taken.

Administrator response
Check the trace and message logs for further details.

FBTSPS111E

The point of contact endpoint requires the user to be authenticated. Please validate the point of contact settings.

Explanation
Unable to obtain user information from the request.

System action
The request is stopped.

Administrator response
Validate that the security roles are mapped properly to users and the point of contact settings.

FBTSPS112E

Access to the URL '*url*' by the user '*user name*' was denied because the user was not assigned the role '*role name*'.

Explanation
A user attempted to access the specified URL, but was denied access.

System action
The request is stopped.

Administrator response
Validate that the security roles are mapped properly to users. If the request was a SOAP request, verify that the partner has a valid password or certificate. Verify that the SOAP Endpoint Security Settings have been configured properly. If you are using groups to control access to the SOAP endpoint, verify that the partner's user ID is in the correct group.

FBTSPS113E

The query service factory was configured with a class name that cannot be loaded. The class name is: '*class*'

Explanation
This is an internal error in the configuration of the query service factory in the sps.xml configuration file.

System action
The query service factory cannot be configured.

Administrator response
Report this error to IBM Software Support; this error should not happen.

FBTSPS114E

The query service was unable to complete the request with the trust service.

Explanation
An exception was thrown when communicating with the trust service.

System action
The request is stopped.

Administrator response
Examine the exception reported in the log file.

FBTSPS115E

The claims object passed to the query service for update was of type: '*class*' and did not support the required interface: '*interface*'.

Explanation
An internal programming error has been detected.

System action
The request is stopped.

Administrator response
Report this error to IBM Software Support; this error should not happen.

FBTSPS116W

Cannot locate the domain mapping file. Will not try to initialize ITFIMRuntime components.

Explanation
The Tivoli Federated Identity Manager domain mapping properties file could not be located in the WebSphere configuration repository. This could be that the Tivoli Federated Identity Manager runtime has not yet been deployed.

System action
The Tivoli Federated Identity Manager runtime components will not be initialized.

Administrator response
Deploy the Tivoli Federated Identity Manager runtime.

FBTSPS120E

The Tivoli Federated Identity Manager runtime components cannot be initialized because the runtime cannot connect to a remote configuration repository.

Explanation
If the Tivoli Federated Identity Manager runtime components are deployed in a WebSphere cluster, then the runtime components need to acquire a handler to a remote deployment manager's configuration repository. This connection may fail if the deployment manager was not started, or that the managed nodes were started before launching the deployment manager.

System action
The runtime components are left in an uninitialized state.

Administrator response
Restart the WebSphere cluster by first starting the deployment manager, then starting the node agents, and finally starting the managed node servers.

FBTSPS121W

The credential attribute '*attribute*' with value '*attribute value*' could not be added to the SSO token because the attributes size limit has been reached.

Explanation
The Tivoli Federated Identity Manager PoC implementation was not able to add the attribute to the SSO token.

System action
The SSO token will not include the attribute.

Administrator response
Increase the attributes size limit.

FBTSPS122E

The Tivoli Federated Identity Manager runtime components are not initialized.

Explanation
The Tivoli Federated Identity Manager runtime components are not initialized. The runtime node is probably not configured. The following components will not be operational: Security Token Service, Single Sign-on Protocol Service, Info Service, and Audit Service.

System action
No action taken.

Administrator response
Configure the runtime nodes.

FBTSPS123E

The point of contact client callback mapping rule is invalid.

Explanation
The point of contact client callback mapping rule is invalid.

System action
The point of contact client callback mapping fails.

Administrator response
Verify that the point of contact client callback is configured correctly.

FBTSPS124E

The point of contact client callback could not determine mapping rule type.

Explanation
The point of contact client callback cannot determine the rule type based on the configuration.

System action
The point of contact client callback mapping fails.

Administrator response
Verify that the point of contact client callback is configured correctly.

FBTSPS125E

The point of contact client callback failed to execute the mapping rule.

Explanation
The point of contact client callback could not execute the mapping rule.

System action
The point of contact client callback mapping fails.

Administrator response
Verify that the point of contact client callback is configured correctly.

FBTSPS127E

The point of contact client callback attribute {0} in the universal user is invalid.

Explanation
The point of contact client callback attribute value in the universal user is invalid.

System action
The request is stopped.

Administrator response
Verify that the authentication policy callback is configured correctly.

FBTSPS128E

The point of contact client callback failed to create the authentication policies.

Explanation
The point of contact client callback failed to create the authentication policies.

System action
he request is stopped.

Administrator response
Verify that the authentication policy callback is configured correctly.

FBTSPS129E

The point of contact implementation failed to obtain the authentication target URL or transaction id from the supplied query string parameters.

Explanation
An error occurred obtaining the target URL or transaction id from the query string.

System action
The request is stopped.

Administrator response
Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS130E

The point of contact multi phase authentication callback implementation failed to obtain the authentication target URL.

Explanation
An error occurred obtaining the target URL.

System action
The request is stopped.

Administrator response
Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS131W

The point of contact callback query string parameters {0} value {1} is not valid.

Explanation
An error occurred obtaining the query string parameter value.

System action
The request will continue using a default value.

Administrator response
Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS132W

The point of contact callback mapping rule context attribute {0} value {1} is not valid.

Explanation
An error occurred obtaining the mapping rule context attribute value.

System action
The request will continue using a default value.

Administrator response
Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS133E

The system cannot read the 'dscclient.properties' file

Explanation
The client configuration containing information on available DSCs is missing.

System action
The in memory HttpSession will be used.

Administrator response
Ensure the file named dscclient.properties exists with the correct values present.

FBTSPS134E

No DSC can be reached at this time.

Explanation
All configured DSCs in the dscclient.conf are not responding.

System action
The in memory HttpSessions will be used.

Administrator response
Check that the dscclient.properties contains valid DSC information, and check that the DSCs are responsive.

FBTSML001E

The received request is missing the required parameter: *parameter*

Explanation
The current request is not valid.

System action
The request will be halted.

Administrator response
Validate the incoming message.

FBTSML002E

The value *value* for attribute *attr* is not valid.

Explanation
The current request is not valid.

System action
The request will be halted.

Administrator response
Validate the incoming message.

FBTSML003E

The requested target, *target* is unknown or disabled.

Explanation
The current request is not valid.

System action
The request will be halted.

Administrator response
Validate the incoming message, and that the identity provider has configured and enabled service provider partners for this target.

FBTSML004E

The request received an artifact with succinct ID: *succinctId*, which did not match a known partner identity provider.

Explanation
The current request is not valid.

System action
The request will be halted.

Administrator response
Validate the incoming message and the configuration of the partner identity providers.

FBTSML005E

The current user making the request is not authenticated.

Explanation
The current request is not valid.

System action
The request will be halted.

Administrator response
Validate the incoming message.

FBTSML006E

The token cannot be exchanged for the service provider.

Explanation
The current request could not be completed because the token exchange failed.

System action
The request will be halted.

Administrator response
Validate the incoming message and the trust service configuration.

FBTSML007E

No configured post page is available to use to return the token to the service provider.

Explanation
The current request could not be completed because the token exchange succeeded but no configured post page was available.

System action
The request will be halted.

Administrator response
This is a configuration error. Ensure that the post page exists in the template directory.

FBTSML008E

No token was available to return to the service provider.

Explanation
The current request could not be completed because the token exchange failed.

System action
The request will be halted.

Administrator response
Validate the incoming message and the trust service configuration.

FBTSML009E

The SAML response object received is not valid.

Explanation
The current request could not be completed because the SAML response object is not valid.

System action
The request will be halted.

Administrator response
Validate the incoming message and the trust service configuration.

FBTSML010E

The sign-on message at the service provider contained parameters that are not valid.

Explanation
The current request could not be completed because the sign-on request is not valid.

System action
The request will be halted.

Administrator response
Validate the incoming message from the identity provider.

FBTSML011E

The response from the identity provider could not be understood or did not contain an assertion: *samlresponse*.

Explanation
The current request could not be completed because the identity provider response was not understandable or did not contain a SAML assertion for sign on.

System action
The request will be halted.

Administrator response
Ensure that the identity provider is configured to send the correct XML element response and that the request to the identity provider was valid.

FBTSML012E

The identity provider token cannot be exchanged for one that is valid for the resource.

Explanation
The current request could not be completed because the identity provider response was not understandable.

System action
The request will be halted.

Administrator response
Validate that the identity provider is configured to send the correct XML element response.

FBTSML013E

The SAML artifact: *artifact* is not valid.

Explanation
The current request could not be completed as the provided SAML artifact is not valid.

System action
The request will be halted.

Administrator response
Validate that the service provider is configured correctly.

FBTSML014E

The SAML assertion cannot be retrieved.

Explanation
The current request could not be completed because a SAML assertion could not be retrieved.

System action
The request will be halted.

Administrator response
Validate that the service provider is configured correctly and that the identity provider is configured to store the assertions for a sufficient time.

FBTSML015E

While processing action: *action* the internal context was missing attribute: *action*.

Explanation
The current request could not be completed because of an internal processing error.

System action
The request will be halted.

Administrator response
Contact IBM software support with this log file.

FBTSML016E

While processing action: *action* the following configuration parameter was determined to be missing or incorrect: *action*.

Explanation
The current request could not be completed because the configuration is not valid.

System action
The request will be halted.

Administrator response
Validate that the system is configured correctly.

FBTSML017E

The assertion could not be retrieved from the identity provider at: *ip* using artifact: *artifact*.

Explanation
The service provider could not retrieve the assertion from the identity provider.

System action
The request will be halted.

Administrator response
Ensure that the identity provider is available.

FBTSML018E

The user cannot be authenticated.

Explanation
The current request could not be completed because the trust service response could not authenticate the user.

System action
The request will be halted.

Administrator response
Validate that the trust service and Point of Contact are properly configured.

FBTSML019E

The SAML request is not valid.

Explanation
The current request could not be completed because the request received is not valid.

System action
The request will be halted.

Administrator response
Validate that the request is valid.

FBTSML020E

The where-are-you-from process received a request for the identity provider: *ipURL*, which did not match a known partner identity provider.

Explanation
The current request received a where-are-you-from cookie which did not match an enabled partner identity provider.

System action
The request will be halted.

Administrator response
Validate that the incoming message contains a WAYF cookie that matches one of the provider IDs for an enabled partner identity provider. One workaround is to delete all persistent cookies on the browser and have the user perform the WAYF process again.

FBTSML021E

The sign-on request at the service provider did not contain valid sign-on parameters. Either a SAML Response or a SAML Artifact should be included in the initial sign-on request.

Explanation
The current request could not be completed because the sign-on request is not valid.

System action
The request will be halted.

Administrator response
Validate the incoming message from the browser to ensure that the identity provider has sent either a valid browser-artifact sign-on (redirect containing a SAMLart parameter), or a valid browser-post sign-on (POST containing a SAMLResponse parameter).

FBTSML200E

Unexpected exception: *exception*

Explanation
The SAML 2.0 plug-in caught an unexpected exception.

System action
The operation will be halted.

Administrator response
Examine the trace logs for more information.

FBTSML201E

Cannot determine the message issuer.

Explanation
The Issuer attribute is required for this message and cannot be determined.

System action
The operation will be halted.

Administrator response
Verify that configuration is correct. The message issuer is the self provider ID.

FBTSML202W

The provider is passive and cannot display the following page on the browser: *page*

Explanation
The provider is passive cannot take control of the user interface, including displaying pages.

System action
The page will not be displayed on the browser.

Administrator response
This might or might not be a problem. If it is a problem, determine why the provider is passive by examining trace logs and configuration. A provider can be directed to be passive by the IsPassive attribute in an authentication request.

FBTSML203E

The provider cannot find the page to display.

Explanation
The provider cannot find a page to display in the browser.

System action
The page will not be displayed on the browser.

Administrator response
Examine the trace logs to determine which page was supposed to have been displayed. It might have been an error status page or a success status page. Check the system installation to determine if the pages have been properly installed.

FBTSML205E

The provider is passive and cannot force a user authentication.

Explanation
The provider is passive and cannot take control of the user interface, including authenticating the user.

System action
The operation will halt.

Administrator response
Reconfigure the requesting provider to send authentication requests that do not require forced authentication, or that do not require the identity provider to be passive, or both.

FBTSML206E

The provider is passive and cannot query the user for consent to federate.

Explanation
The provider is passive and cannot take control of the user interface, including querying the user for consent-to-federate accounts.

System action
The operation will halt.

Administrator response
Reconfigure the requesting provider to send authentication requests that do not require the identity provider to be passive.

FBTSML207E

Cannot determine the SAML status.

Explanation
The SAML status attribute is required for this message and cannot be determined.

System action
The operation will be halted.

Administrator response
Examine the trace logs to see why the SAML status was not set.

FBTSML208E

Cannot create account linkage between the providers.

Explanation
The accounts are not linked and the SAML request forbids creating account information required for linkage.

System action
The operation will be halted.

Administrator response
Reconfigure the requesting provider to send authentication requests that allow the identity provider to create account linkage. This is done by setting the AllowCreate attribute in the NameIDPolicy element to true.

FBTSML209E

Cannot create account linkage between the providers because the user denied consent to federate.

Explanation
The accounts are not linked (federated) and the user denied permission to link them.

System action
The operation will be halted.

Administrator response
Instruct end users to consent to account linkage (federation).

FBTSML210E

The timestamp in the SAML message is out of range. The message timestamp, *msgTime*, is not within *tolerance* seconds of *compareTime*.

Explanation
The SAML message has a timestamp that is not valid.

System action
The message will be ignored.

Administrator response
There are several reasons that a SAML message timestamp might be out of range: The clocks on the service and identity providers systems are skewed beyond the acceptable tolerance, network delays are hampering message flow, or the acceptable tolerance for message timestamp is set too low. The administrator should check these points and make any necessary adjustments.

FBTSML211E

The destination URL in the SAML message (*msgDest*) does not match the current provider location (*here*).

Explanation
The SAML message has a destination URL that is not valid.

System action
The message will be ignored.

Administrator response
The most likely problem is that the SAML message is being created with an incorrect destination. Verify that configuration on the sending provider specifies the correct URL for the receiving provider.

FBTSML212E

No authentication assertions were found.

Explanation
No assertions could be found at the identity provider.

System action
No assertions will be included in the authentication response message.

Administrator response
Examine the trace logs to see why no authentication assertion was set.

FBTSML213E

Cannot determine the message destination.

Explanation
The Destination attribute is required for this message and cannot be determined.

System action
The operation will be halted.

Administrator response
Verify that configuration is correct. The message destination is the URI to which the message is sent.

FBTSML214E

Cannot determine the *endpoint* endpoint for provider *provider*.

Explanation
The required target endpoint for the SAML message cannot be determined.

System action
The operation will be halted.

Administrator response
Verify that configuration is correct.

FBTSML215E

The name identifier policy in the authentication request could not be met by this identity provider.

Explanation
The identity provider could not create a name identifier that adhered to the policy in the authentication request. Usually, this means that the policy specified an unsupported format or not did specify that a persistent identifier could be created.

System action
The operation will be halted.

Administrator response
Verify that authentication requests specify supported name identifier policies, or do not specify a policy at all.

FBTSML216E

The user account could not be federated.

Explanation
The identity provider could not federate the user account. Usually, this means that there is something wrong with the identity service.

System action
The operation will be halted.

Administrator response
Verify that the identity service is configured properly and that the registry server is available.

FBTSML217E

This provider cannot accept an unsolicited authentication response.

Explanation
The authentication response being processed does not have a corresponding authentication request. This provider is not configured to accept unsolicited authentication responses.

System action
The operation will be halted.

Administrator response
Verify that the service provider is configured properly regarding acceptance of unsolicited authentication responses.

FBTSML218E

The specifications for the *endpoint* endpoint are not valid.

Explanation
The endpoint specified by the SAML message cannot be validated.

System action
The operation will be halted.

Administrator response
Verify that configuration is correct and that endpoint specifications such as index, URL and binding in the message are correct.

FBTSML219E

Cannot determine the name identifier for the logout request.

Explanation
The NameID attribute is required for this message and cannot be determined.

System action
The operation will be halted.

Administrator response
Examine the trace logs to see why no name identifier information was set.

FBTSML220E

Cannot determine the session index for the logout request.

Explanation
The SessionIndex attribute is required for this message and cannot be determined.

System action
The operation will be halted.

Administrator response
Examine the trace logs to see why no session index was set.

FBTSML221E

The logout requester is not a valid partner.

Explanation
The issuer of the logout request message cannot be determined as a valid partner to this provider. On an identity provider, the request issuer must be a provider to which this provider has issued an assertion. On a service provider, the request issuer must be a provider that has issued an assertion to this provider.

System action
The operation will be halted.

Administrator response
If the request is legitimate, examine the trace logs to see why the request issuer was not found in the list of known logout partners.

FBTSML222E

The response message does not correlate to the pending request.

Explanation
The response message contains an InResponseTo attribute that does not match the ID attribute of the pending request. It is possible that the response was received in error.

System action
The operation will be halted.

Administrator response
If the response is legitimate, examine the trace logs to see why the InResponseTo attribute does not match the ID attribute of the currently pending request.

FBTSML223E

Logout failed.

Explanation
The locally authenticated user was not logged out successfully.

System action
The operation will be halted.

Administrator response
Examine the trace logs to see why logout failed.

FBTSML224E

Cannot find partner configuration for provider *partner*.

Explanation
The required configuration for the partner provider cannot be found.

System action
The operation will be halted.

Administrator response
Ensure that the partner provider's metadata has been imported into this federation and that the configuration file is not corrupted.

FBTSML225E

Token exchange failed.

Explanation
The current request could not be completed because the token exchange failed.

System action
The request will be halted.

Administrator response
Validate the incoming message and the trust service configuration. In addition, examine the trace logs to see why the token exchange failed.

FBTSML226E

The message has an Issuer attribute that is not valid.

Explanation
The SAML message is required by the specification to have an Issuer attribute. The Issuer format, if specified, must be urn:oasis:names:tc:SAML:2.0:nameid-format:entity. The message is either missing the Issuer attribute or has the wrong format specified.

System action
The message will be ignored.

Administrator response
Examine the trace logs on the provider that issued the message to see why the message was constructed without the Issuer attribute or with the incorrect Issuer format.

FBTSML227E

The issuer of the ArtifactResolve message, *issuer*, does not match the intended recipient of the artifact message, *recipient*.

Explanation
An ArtifactResolve message was received from a provider which is not the intended recipient of the message associated with the artifact.

System action
The artifact in the ArtifactResolve message will not be exchanged for a SAML protocol message. An empty ArtifactResponse message will be returned.

Administrator response
The system is behaving correctly by disregarding potential attacks.

FBTSML228E

Cannot initialize the SOAP client for the *endpoint* endpoint.

Explanation
Unable to initialize the SOAP client.

System action
The request will be halted.

Administrator response
Validate the SOAP client configuration. In addition, examine the trace logs for additional information.

FBTSML229E

The artifact exchange failed. The message could not be retrieved using artifact: *artifact*.

Explanation
This provider attempted to exchange an artifact for a SAML protocol message but no message was returned.

System action
The operation will be halted.

Administrator response
Examine the artifact issuer to see why the artifact was not exchanged. The artifact may have expired and its associated message purged from the system, for example.

FBTSML230E

A SAML response message was received that is not valid.

Explanation
A SAML response message was received, but a corresponding SAML request message could not be found. The response is considered invalid.

System action
The operation will be halted.

Administrator response
If the SAML response is expected, examine the trace logs to see why the corresponding SAML request was not found. Otherwise, no action is needed.

FBTSML231E

A SAML response message was received that is not valid.

Explanation
A SAML response message was received, but it did not contain any AuthnStatements. The response is considered invalid for purposes of authentication.

System action
The operation will be halted.

Administrator response
Examine the issuer of the SAML message to see why it issued a SAML assertion with no AuthnStatement.

FBTSML232E

No alias was found for user *User* and provider *PartnerProvider*.

Explanation
There was no alias found for the currently authenticated user for the specified partner provider.

Administrator response
Enable trace for detailed messages about the error.

FBTSML233E

The identity service request to remove an alias for *userId* and provider *providerId* failed.

Explanation
The identity service operation was not successful.

Administrator response
Ensure that the identity and provider are valid and check the log for messages returned from the identity service.

FBTSML234E

No principal was found for alias *aliasId* and partner provider *providerId*.

Explanation
The identity service operation was not successful.

Administrator response
Validate that the alias and provider are valid and check the log for messages returned from the identity service.

FBTSML235E

The identity service request to update an alias for *userId* and provider *providerId* failed.

Explanation
The identity service operation was not successful.

Administrator response
Validate that the identity and provider are valid and check the log for messages returned from the identity service.

FBTSML236E

The assertion issued by *partnerProvider* could not be validated or decrypted.

Explanation
The assertion could not be validated or decrypted.

Administrator response
Make sure that the validation keys, decryption keys and decryption parameters are configured properly for the provider that issued the assertion. The trace log will indicate which operation failed, validation or decryption.

FBTSML237E

The SAML message could not be decrypted.

Explanation
The SAML message could not be decrypted.

Administrator response
Make sure that the decryption keys and decryption parameters are configured properly for the provider that sent the message.

FBTSML238E

The SAML message signature could not be validated.

Explanation
The SAML message signature could not be validated.

Administrator response
Make sure that the validation key is configured properly for the provider that sent the message.

FBTSML239E

The SAML message could not be parsed.

Explanation
The SAML message could not be parsed.

Administrator response
Make sure that incoming message is properly formatted.

FBTSML240E

The SAML artifact could not be parsed.

Explanation
The SAML artifact could not be parsed.

Administrator response
Make sure that incoming artifact is properly formatted.

FBTSML241E

The incoming HTTP message is not valid.

Explanation
The incoming HTTP message is not valid.

Administrator response
Make sure that incoming HTTP message is properly formatted.

FBTSML242E

Authentication failed at the identity provider.

Explanation
The SAML status included in the authentication response message indicates that authentication failed at the identity provider.

System action
The operation will be halted.

Administrator response
Examine the trace logs on the identity provider that issued the response message to see why the authentication operation failed.

FBTSML243E

The name identifier in the request is not valid.

Explanation
The name identifier in the request does not match the information that was stored for that provider during login. If the service provider was acting as a member of an affiliation group during login, the name identifier in the request must reflect that fact.

System action
The operation will be halted.

Administrator response
If the request is legitimate, examine the trace logs to see why information in the request name identifier does not match the information stored for that provider.

FBTSML244E

Cannot perform the name ID management operation on a name identifier with format *Format*.

Explanation
The name identifier established during authentication in the current session is not persistent. Name ID update and termination management operations can be performed only on persistent name identifiers.

System action
The operation will be halted.

Administrator response
The user should authenticate using a means that establishes a persistent name identifier and then retry the operation.

FBTSML245E

The request was missing the TARGET parameter.

Explanation
The initial request to the service provider must contain a TARGET parameter.

System action
The operation will be halted.

Administrator response
Modify the initial request to the service provider to contain a TARGET parameter, which should point to the desired SSO target URL.

FBTSML246E

The request failed due to an internal error on the identity provider.

Explanation
The identity provider encountered an internal error preparing the samlp:Response for the service provider.

System action
The operation will be halted.

Administrator response
Check the identity provider log to determine the root cause of this error. The identity provider configuration for this partner might not be correct.

FBTSML247E

The SAML request for artifact *Artifact* could not be created using signing key *KeyIdentifier*.

Explanation
The service provider was unable to generate a signed samlp:Rquest message.

System action
The operation will be halted.

Administrator response
Check that the service provider signing key identifier is correctly configured.

FBTSML248E

The SAML artifact *Artifact* has already been presented to the identity provider.

Explanation
The identity provider has detected that this artifact has already been presented for exchange.

System action
The operation will be halted.

Administrator response
This could be a replay attack, or the browser user may have simply reloaded the page containing the redirect to the service provider with the artifact.

FBTSML249E

The federation group type specified in the configuration is not supported. Group ID: '*id*', Group display name: '*id*', federation group type '*type*'.

Explanation
The federation group defined is not a supported type.

System action
The SAML module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify a supported group type in the configuration.

FBTSML250E

The *partnerEndpointType* endpoint for partner '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is not valid. Endpoint value is '*displayName*'.

Explanation
The specified partner endpoint is not valid.

System action
The SAML Module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify a valid endpoint value in the configuration.

FBTSML251E

The *partnerEndpointType* endpoint for self '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is not valid. Endpoint value is '*displayName*'.

Explanation
The specified self endpoint is not valid.

System action
The SAML module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify a valid endpoint value in the configuration.

FBTSML252E

The *partnerEndpointType* endpoint is missing from the provider [*id*] and display name [*displayName*] configuration for federation group with ID [*id*] and display name [*displayName*].

Explanation
A required endpoint is missing from the provider's configuration.

System action
The SAML module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify the required endpoint in the provider's configuration.

FBTSML253E

The *propertyName* property is missing from the provider [*id*] and display name [*displayName*] configuration for federation group with ID [*id*] and display name [*displayName*].

Explanation
A required property is missing from the provider's configuration.

System action
The SAML Module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify the required property in the provider's configuration.

FBTSML254E

The property value '*propertyValue*' for property '*propertyName*' specified for provider '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is not valid.

Explanation
The specified property value is not valid.

System action
The SAML Module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify a valid property value in the configuration.

FBTSML255E

The boolean property value '*propertyValue*' for property '*propertyName*' specified for provider '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is not valid. For Boolean properties the permitted values are 'true' or 'false'.

Explanation
The specified Boolean property value is not valid.

System action
The SAML module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify a valid Boolean property value in the configuration.

FBTSML256E

The numeric property value [*propertyValue*] for property [*propertyName*] specified for provider [*id*] and display name [*displayName*] for federation group with ID [*id*] and display name [*displayName*] is not valid. The minimum value for this property is [*displayName*].

Explanation
The specified numeric property value is not valid.

System action
The SAML Module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify a valid numeric property value in the configuration.

FBTSML257E

The Identity provider succinct id value '*propertyValue*' specified under property '*propertyName*' for provider '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is not valid. The identity provider succinct ID is a required property.

Explanation
The specified numeric property value is not valid.

System action
The SAML module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify a valid identity provider succinct ID value in the configuration.

FBTSML258E

The common domain service host value '*commonDomainServiceHost*' specified using property '*propertyName*' for partner '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is not valid. The common domain service host must start with http:// or https:// and end with the common domain value '*displayName*'.

Explanation
The specified common domain service host is not valid.

System action
The SAML module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify a valid common domain service host in the configuration.

FBTSML259E

The provider source id value [*propertyValue*] specified under property [*propertyName*] for provider [*id*] and display name [*displayName*] for federation group with ID [*id*] and display name [*displayName*] does not match the message digest of the provider ID.

Explanation
The specified provider source ID value is not valid.

System action
The SAML module could not be initialized.

Administrator response
Verify that configuration files are present and have not been corrupted. Specify a valid provider source ID value in the configuration.

FBTSML260E

The binding value *value* for attribute *attr* is not valid for profile *profile*.

Explanation
The specified binding is not valid for the profile being executed.

System action
The request will be halted.

Administrator response
Validate the incoming message.

FBTSML261E

Unobfuscation of the basic authentication password for SOAP client authentication failed.

Explanation
Unobfuscation of the basic authentication password for SOAP client authentication failed.

System action
The request will be halted.

Administrator response
Check the logs for a runtime exception.

FBTSML262E

The ECP profile is not enabled for the provider.

Explanation
The ECP profile is not enabled.

System action
The request will be halted.

Administrator response
Validate the incoming message.

FBTSML263E

The name identifier policy in the request is not valid.

Explanation
The name identifier policy in the request is not valid. The format is not a supported format or the SPNameQualifier is not known to the provider.

System action
The operation will be halted.

Administrator response
If the request is legitimate, examine the trace logs to see why the name identifier policy is considered invalid.

FBTSML264E

The SAML assertion contains a session index value that has been invalidated by a previously received logout request.

Explanation
The current request could not be completed because a SAML assertion is not considered valid.

System action
The request will be halted.

Administrator response
If the response is legitimate, examine the trace logs to see why the session index attribute was included on a logout request.

FBTSML265E

The SAML assertion with the specified assertion ID *value* was not found.

Explanation
The current request could not be completed because a SAML assertion was not stored or the assertion ID is not valid.

System action
The request will be halted.

Administrator response
Please submit the request with a valid assertion ID.

FBTSML266E

The index '*value*' for endpoint type '*value*' specified using query string parameter '*value*' does not exist.

Explanation
The current request could not be completed because a the endpoint index is not valid.

System action
The request will be halted.

Administrator response
Please submit the request with a valid endpoint index.

FBTSML267E

The value '*value*' specified using query string parameter '*value*' is not valid integer value.

Explanation
The current request could not be completed because a query string parameter is not valid.

System action
The request will be halted.

Administrator response
Please submit the request with a valid integer value.

FBTSML268E

Logout from one or more partners failed.

Explanation
A failed status was returned from one or more partner logout attempts.

System action
The request did not complete successfully.

Administrator response
Check the logs for failure reason.

FBTSML269E

The users account was not successfully deferated from the partner.

Explanation
The users account was not successfully deferated from the partner

System action
The request did not complete successfully.

Administrator response
Check the logs for failure reason.

FBTSML270E

The user provided to the administrative command does not have an active session.

Explanation
The users could not be logged out because they do not currently have a valid session.

System action
The request did not complete successfully.

FBTSML271E

The SAML assertion cannot be retrieved using artifact: *artifact*

Explanation
The current request could not be completed because a SAML assertion could not be retrieved.

System action
The request is halted.

Administrator response
Validate that the service provider is configured correctly and that the identity provider is configured to store the assertions for a sufficient time.

FBTSML272E

The SAML module was unable to query the user attributes.

Explanation
The current request could not be completed because the SAML module was unable to create a attribute query service claims object.

System action
The request will be halted.

Administrator response
Check the logs for failure reason.

FBTSML273E

The SAML module was unable to obtain the subject name id from the attribute query request.

Explanation
The current request could not be completed because the subject name id is not valid.

System action
The request will be halted.

Administrator response
Please submit a valid attribute query request.

FBTSML274E

The SAML module was unable to obtain the subject principal name using the name id included with the attribute query request.

Explanation
The current request could not be completed because the subject principal name can not be obtained.

System action
The request will be halted.

Administrator response
Please submit a valid attribute query request.

FBTSML275E

The SAML message could not be retrieved using artifact: *artifact*.

Explanation
The provider could not retrieve the SAML message using the supplied artifact.

System action
The request will be halted.

Administrator response
Ensure that the artifact is valid and the provider is properly configured.

FBTSML276E

The SAML artifact: *artifact* is expired.

Explanation
The artifact received is no longer valid.

System action
The request will be halted.

Administrator response
Ensure that the artifact is valid and the provider is properly configured.

FBTSML278E

The SAML request is expired.

Explanation
The request received is no longer valid.

System action
The request will be halted.

Administrator response
Ensure that the request is valid and the provider is properly configured.

FBTSML279E

Cannot find partner configuration for SourceID *partner*.

Explanation
The required configuration for the partner with the SourceID cannot be found.

System action
The operation will be halted.

Administrator response
Ensure that the metadata of the partner with the SourceID has been imported into this federation and that the configuration file is not corrupted.

FBTSML280E

The target or relay state URL *targetURL* is not whitelisted.

Explanation
The target or relay state URL received by the system is rejected because it is not whitelisted.

System action
The flow is stopped.

Administrator response
Check if the target or relay state URL should be whitelisted.

Chapter 25. SOAP client messages

These messages are provided by the SOAP client component.

FBTSOC001E

The SOAP endpoint passed in the SOAP client is not valid. The passed-in value was *parameter*.

Explanation
The current request is not valid.

System action
The request will be halted.

Administrator response
Make sure that the correct SOAP endpoint URL is configured.

FBTSOC002E

An error occurred in initializing SSL with the SOAP endpoint.

Explanation
The server might not be enabled for SSL. The SSL parameters passed in might not be valid.

System action
The request will be halted.

Administrator response
Validate the partner's SSL configuration for the SOAP back channel.

FBTSOC003E

The TrustStore identifier passed in SOAPClientImpl is null. The SSL connection with the endpoint *parameter* cannot be initialized.

Explanation
The current request is not valid.

System action
The request will be halted.

Administrator response
Validate the partner's SSL configuration for the SOAP back channel.

FBTSOC004E

The KeyStore name *parameter* cannot be obtained from KessService.

Explanation
The specified keystore cannot be obtained from KessService.

System action
The request will be halted.

Administrator response
Validate the partner's SSL configuration for the SOAP back channel.

FBTSOC005E

The TrustStore cannot be initialized from the passed in identifier *parameter*.

Explanation
The truststore parameter passed in is not valid.

System action
The request will be halted.

Administrator response
Validate the partner's SSL configuration for the SOAP back channel.

FBTSOC006E

The SOAP client is unable to parse the response SOAP message.

Explanation
The SOAP client was unable to parse the incoming response SOAP message.

System action
The request will be halted.

Administrator response
Validate the Access Control List configuration in the destination endpoint.

FBTSOC007E

The Client Keystore cannot be initialized from the passed in identifier *parameter*.

Explanation
The client keystore parameter passed in is not valid.

System action
The request will be halted.

Administrator response
Validate the partner's SSL configuration for the SOAP back channel.

FBTSOC008E

The SOAP client is unable to send the request SOAP message.

Explanation
The SOAP client was unable to send the outgoing request SOAP message.

System action
The request will be halted.

Administrator response
Validate the Access Control List configuration in the destination endpoint.

FBTSOC009E

Unobfuscation of the basic authentication password for SOAP client authentication failed.

Explanation
Unobfuscation of the basic authentication password for SOAP client authentication failed.

System action
The request will be halted.

Administrator response
Check the logs for a runtime exception.

FBTSOC010E

Unable to construct a SOAP fault because the compulsory parameter *parameter* was null.

Explanation
A constructor of a SOAP fault attempted to build it without the required parameter.

System action
The SOAP fault will not be build.

Administrator response
Contact support.

FBTSOC011E

The AccessApproval module: *module* has denied access to the endpoint: *url*

Explanation
A custom AccessApproval module has denied access to the endpoint.

System action
The connection is rejected.

Administrator response
If the URL is supposed to be accessible, modify the custom access approval module to permit access to it.

FBTSOC012E

Unable to load an AccessApproval module with the extension ID: *module*

Explanation
The extension manager could not load an AccessApproval module.

System action
The request is not processed.

Administrator response
Verify that an extension with the specified ID is included in the published plug-ins.

Chapter 26. Software development kit messages

These messages are provided by the software development kit component.

FBTSDK003E

An error occurred loading or starting extension bundle [*filename*]. The error was [*error message*].

Explanation
An error occurred loading or starting an extension bundle.

System action
The extension bundle will not be available to the runtime.

Administrator response
Check the server logs for more details to trace the cause of the error and fix the error in the extension bundle.

FBTSDK006E

An error occurred stopping extension bundle [*symbolic name*]. The error was [*error message*].

Explanation
An error occurred stopping an extension bundle.

System action
The extension bundle will not be shutdown cleanly.

Administrator response
Check the server logs for more details to trace the cause of the error and fix the error in the extension bundle.

Chapter 27. Username password messages

These messages are provided by the username password component.

FBTUPD000E

Internal Error. Contact the System Administrator.

Explanation
An internal error occurred.

System action
The application encountered an error. The process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTUPD100E

The configuration for the username password authentication mechanism is missing or not valid.

Explanation
The username password mechanism requires configuration to connect to the user repository.

System action
The authentication process encountered an error. The process has been halted.

Administrator response
Check the configuration data for the username password authentication mechanism.

FBTUPD101E

The username or password that you entered is incorrect.

Explanation
The username or password that you entered is incorrect.

System action
None

Administrator response
None

FBTUPD102E

The account has been disabled.

Explanation
Too many invalid password authentication attempts have triggered the policy to disable the account.

System action
The authentication process encountered an error. The process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTUPD103E

The account has been locked out.

Explanation
Too many invalid password authentication attempts have triggered the policy to temporarily lock out the account.

System action
The authentication process encountered an error. The process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTUPD104E

The account cannot be used at this time due to time-of-day policy restrictions.

Explanation
The Time-of-Day policy does not allow a login at this time.

System action
The authentication process encountered an error. The process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTUPD105E

An internal error occurred. Contact the System Administrator or try again later.

Explanation
None of the configured LDAP servers of the appropriate type for the operation can be contacted.

System action
The authentication process encountered an error. The process has been halted.

Administrator response
Check the LDAP configuration data for the username password authentication mechanism and verify that the LDAP server is running.

FBTUPD106E

An internal error occurred. Contact the System Administrator or try again later.

Explanation
An error occurred in the registry when authenticating the user.

System action
The authentication process encountered an error. The process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTUPD107E

Change password failed. Make sure both new password fields contain the same data.

Explanation
New password verification failed. Make sure both new password fields contain the same data.

System action
None

Administrator response
None

FBTUPD108E

Change password failed. The old password you entered is incorrect.

Explanation
The credentials supplied are invalid.

System action
None

Administrator response
None

FBTUPD109E

Change password failed. The old password was not supplied.

Explanation
The old password supplied for the user is missing.

System action
None

Administrator response
None

FBTUPD110E

New password verification failed. The password contains control characters or characters that are not accepted by the particular LDAP server type being used.

Explanation
The password contains control characters or characters that are not accepted by the particular LDAP server type being used.

System action
None

Administrator response
None

FBTUPD111E

New password verification failed. The password has space characters in it, but the password policy does not allow spaces.

Explanation
The password has space characters in it, but the password policy does not allow space characters.

System action
None

Administrator response
None

FBTUPD112E

New password verification failed. The password has a character repeated consecutively too many times to comply with password policy.

Explanation
The password has a character repeated consecutively too many times to comply with password policy.

System action
None

Administrator response
None

FBTUPD113E

New password verification failed. The password does not have enough characters in it to comply with password policy.

Explanation
The password does not have enough characters in it to comply with password policy.

System action
None

Administrator response
None

FBTUPD114E

New password verification failed. There are not enough alphabetic characters in the password for it to comply with password policy.

Explanation
There are not enough alphabetic characters in the password for it to comply with password policy.

System action
None

Administrator response
None

FBTUPD115E

New password verification failed. There are not enough non-alphabetic characters in the password for it to comply with password policy.

Explanation
There are not enough non-alphabetic characters in the password for it to comply with password policy.

System action
None

Administrator response
None

FBTUPD116E

An internal registry error occurred. Contact the System Administrator or try again later.

Explanation
Failed to change the password.

System action
The authentication process encountered an error. The process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTUPD117E

The password has expired. You need to change your password.

Explanation
The registry indicated the password was expired.

System action
None

Administrator response
None

FBTUPD118E

An internal registry error occurred. Contact the System Administrator or try again later.

Explanation
An error occurred in the registry getting a user attribute.

System action
The authentication process encountered an error. The process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTUPD119E

The account is set invalid.

Explanation
The account valid flag on the account is set to false.

System action
The authentication process encountered an error. The process has been halted.

Administrator response
The account cannot be used. Contact the account administrator to determine what can be done.

FBTUPD120E

An internal configuration error occurred. Contact the System Administrator or try again later.

Explanation
Unable to determine the registry server type.

System action
The authentication process encountered an error. The process has been halted.

Administrator response
Check the log file for more information about the cause of the problem.

FBTUPD121E

An internal registry error occurred. The error is *message*.

Explanation

An error occurred when authenticating a user

System action

The authentication process encountered an error. The process has been halted.

Administrator response

Check the log file for more information about the cause of the problem.

Chapter 28. Utility messages

These messages are provided by the utility component.

FBTUTI001E

The required parameter [code] is missing.

Explanation
The parameter [code] is required.

System action
The request is rejected.

Administrator response
Ensure that the parameter [code] is sent in the request.

FBTUTI002E

The parameter [code] contains invalid characters.

Explanation
The parameter [code] can only contain alphanumeric characters.

System action
The request is rejected.

Administrator response
Ensure that the parameter [code] only contains alphanumeric characters.

FBTUTI003E

The parameter [code] exceeds the permitted length.

Explanation
The parameter [code] must be less than 4296 characters

System action
The request is rejected.

Administrator response
Ensure that the parameter [code] does not exceed the permitted length