WebSphere Application Server (WSAS): Secure Sockets Layer (SSL)

Ajay Bhalodia

IBM Certified WebSphere Application Server System Administrator

Introduction to SSL

- Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols were designed to help protect the privacy and integrity of data while it is transferred across a network

- As data traveling across networks is UNSECURED it may be intercepted by someone who is not the intended recipient – not a desired situation!

- Personal data such as credit card information and passwords which travel across networks MUST be protected

Security components in the Java 2 platform

- JCA
  - Java Cryptography Architecture (JCA)
- JCE
  - Java Cryptography Extension (JCE)
- JSSE
  - Java Secure Socket Extension (JSSE)
- JAAS
  - Java Authentication and Authorization Service (JAAS)

What is JCA?

- Java Cryptography Architecture (JCA)
  - A framework for accessing and developing cryptographic functionality for the Java platform

What is JCE?

- Java Cryptography Extension (JCE)
  - Provides a framework and implementations for encryption, key generation, and key agreement, as well as Message Authentication Code (MAC) algorithms

What is JSSE?

- Java Secure Socket Extension (JSSE)
  - Provides the same functionality as JCE however exists at the socket layer
  - Classes for secure socket are part of javax.net.ssl package
  - The security services provided by JSSE consist of
    - the transport-level message integrity and confidentiality (encryption)
    - server authentication
  - Optional client authentication
  - Is integrated into JDK 1.4

What is JAAS?

- Java Authentication and Authorization Service (JAAS)
  - A package that enables services to authenticate and enforce access controls upon users

Vocabulary

- Certificate
  - A “code” that is used to authenticate users and data on a network
- Signer Certificate (CA certificate)
  - A certificate that contains a public key
- User Certificate (Personal certificate)
  - A certificate that contains a private key and corresponding public key

Vocabulary *(cont.)*

- Private key
  - A “code” which is not shared with anyone in the network.
  - Used to decrypt information that was encrypted with its corresponding public key
  - Used to encrypt information that can be decrypted with its corresponding public key

Vocabulary *(cont.)*

- Public key
  - A “code” that is given to other applications and users on the network
  - Used to decrypt information that was encrypted with its corresponding private key
  - Used to encrypt information that can only be decrypted with its corresponding private key

Vocabulary *(cont.)*

- Key repository
  - A file/location where certificates are stored
  - It is also known as trust stores and key stores

SSL handshake protocol

- Before data can be sent across an SSL connection, the two ends must negotiate and exchange key information
- This is called the *handshake protocol*
  - Client initiates communication with a server. The server sends its public certificate to the client and the client verifies the server certificate. Why is this important?
  - The client sends its certificate to the server and the server verifies the client certificate. Client authentication is an optional step.
  - The client encrypts the password information with the server's public key then sends it to the server. The password information is used by both ends of the connection to generate identical secret keys, which are then used to transmit data.

WSAS components that use SSL

- SSL is used by multiple components with in WebSphere Application Server (WSAS)
  - HTTP Transport
  - Object Request Broker (ORB)
  - LDAP client
  - SOAP port

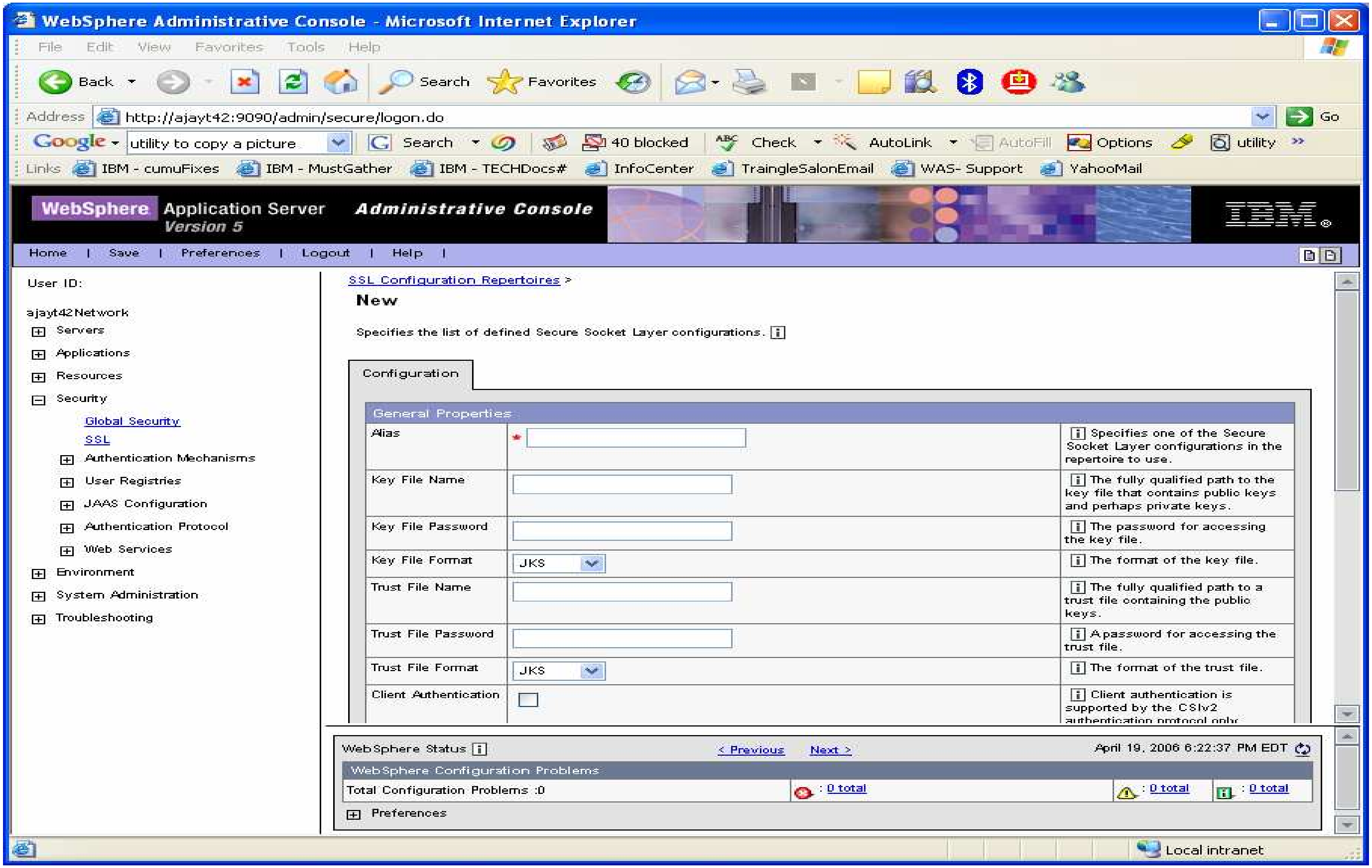
SSL Configuration with in WSAS

1. Define a SSL repertoire
2. Associate the repertoire to the component that needs to use SSL
3. Import the necessary signer certificates in the truststore (truststore is defined in the repertoire – step #1 above)

Define SSL Repertoire

1. Open WSAS Admin console
2. Navigate in the left pane
3. Expand Security and click on SSL
4. Open an existing repertoire or create your own

- Note: WSAS ships with DefaultSSLSettings repertoire with dummy keyfiles and trustfiles. It is recommended that you define your own for production use.


WebSphere Administrative Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://ajayt42:9090/admin/secure/logon.do
Go
Google utility to copy a picture Search 40 blocked Check AutoLink AutoFill Options utility
Links IBM - cumuFixes IBM - MustGather IBM - TECHDocs# InfoCenter TraingleSalonEmail WAS- Support YahooMail
WebSphere Application Server Version 5 Administrative Console
Home | Save | Preferences | Logout | Help |
User ID:
ajayt42Network
Servers
Applications
Resources
Security
Global Security
SSL
Authentication Mechanisms
User Registries
JAAS Configuration
Authentication Protocol
Web Services
Environment
System Administration
Troubleshooting
Local intranet

SSL Configuration Repertoires >

New

Specifies the list of defined Secure Socket Layer configurations.

Configuration

General Properties

Alias	*	Specifies one of the Secure Socket Layer configurations in the repertoire to use.
Key File Name		The fully qualified path to the key file that contains public keys and perhaps private keys.
Key File Password		The password for accessing the key file.
Key File Format	JKS	The format of the key file.
Trust File Name		The fully qualified path to a trust file containing the public keys.
Trust File Password		A password for accessing the trust file.
Trust File Format	JKS	The format of the trust file.
Client Authentication	☐	Client authentication is supported by the CSIv2 authentication protocol only

WebSphere Status < Previous Next > April 19, 2006 6:22:37 PM EDT

WebSphere Configuration Problems

Total Configuration Problems :0 : 0 total : 0 total : 0 total

Preferences

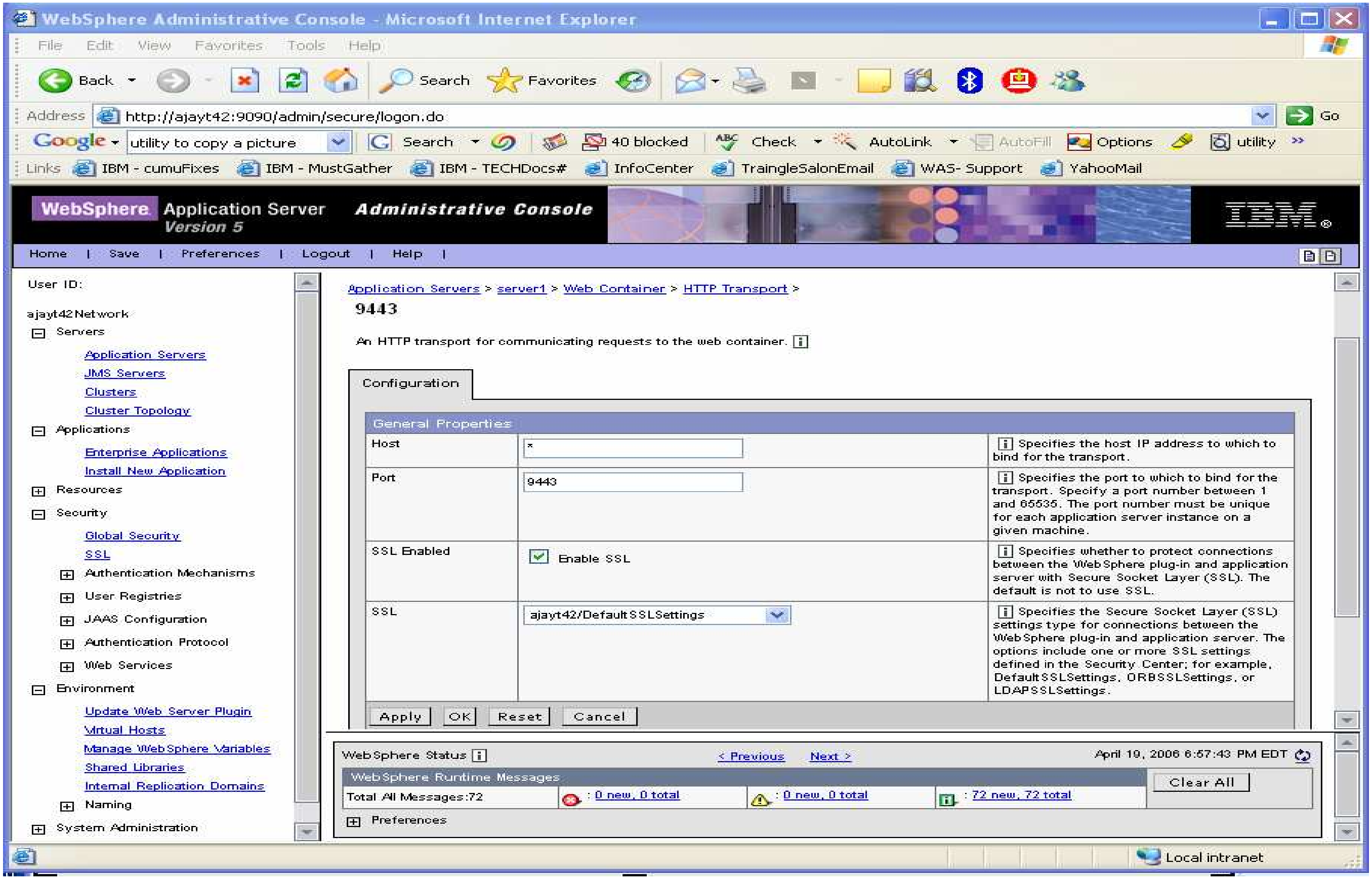
Associating the repertoire

- As stated previously you now need to associate the repertoire to the component in WSAS that needs to use SSL

- WSAS Components that use SSL
  - HTTP Transport
  - Object Request Broker (ORB)
  - LDAP client
  - SOAP Port

Associating repertoire to HTTP Transport

1. Open WSAS Admin console
2. Navigate in the left pane
3. Expand Servers and click on “Application Servers”
4. Click on your server
5. Under additional properties click on “Web Container”
6. Under additional properties click on “HTTP Transports”
7. Click on SSL enabled port


WebSphere Administrative Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://ajayt42:9090/admin/secure/logon.do Go
utility to copy a picture Search 40 blocked Check AutoLink AutoFill Options utility
Links IBM - cumuFixes IBM - MustGather IBM - TECHDocs# InfoCenter TraingleSalonEmail WAS- Support YahooMail
WebSphere Application Server Version 5 Administrative Console
Home | Save | Preferences | Logout | Help |
User ID:
ajayt42Network
Servers
Application Servers
JMS Servers
Clusters
Cluster Topology
Applications
Enterprise Applications
Install New Application
Resources
Security
Global Security
SSL
Authentication Mechanisms
User Registries
JAAS Configuration
Authentication Protocol
Web Services
Environment
Update Web Server Plugin
Virtual Hosts
Manage WebSphere Variables
Shared Libraries
Internal Replication Domains
Naming
System Administration
Local intranet

Application Servers > server1 > Web Container > HTTP Transport >

9443

An HTTP transport for communicating requests to the web container.

Configuration

General Properties

Host	*	Specifies the host IP address to which to bind for the transport.
Port	9443	Specifies the port to which to bind for the transport. Specify a port number between 1 and 65535. The port number must be unique for each application server instance on a given machine.
SSL Enabled	☑ Enable SSL	Specifies whether to protect connections between the WebSphere plug-in and application server with Secure Socket Layer (SSL). The default is not to use SSL.
SSL	ajayt42/DefaultSSLSettings	Specifies the Secure Socket Layer (SSL) settings type for connections between the WebSphere plug-in and application server. The options include one or more SSL settings defined in the Security Center; for example, DefaultSSLSettings, ORBSSLSettings, or LDAPSSLSettings.

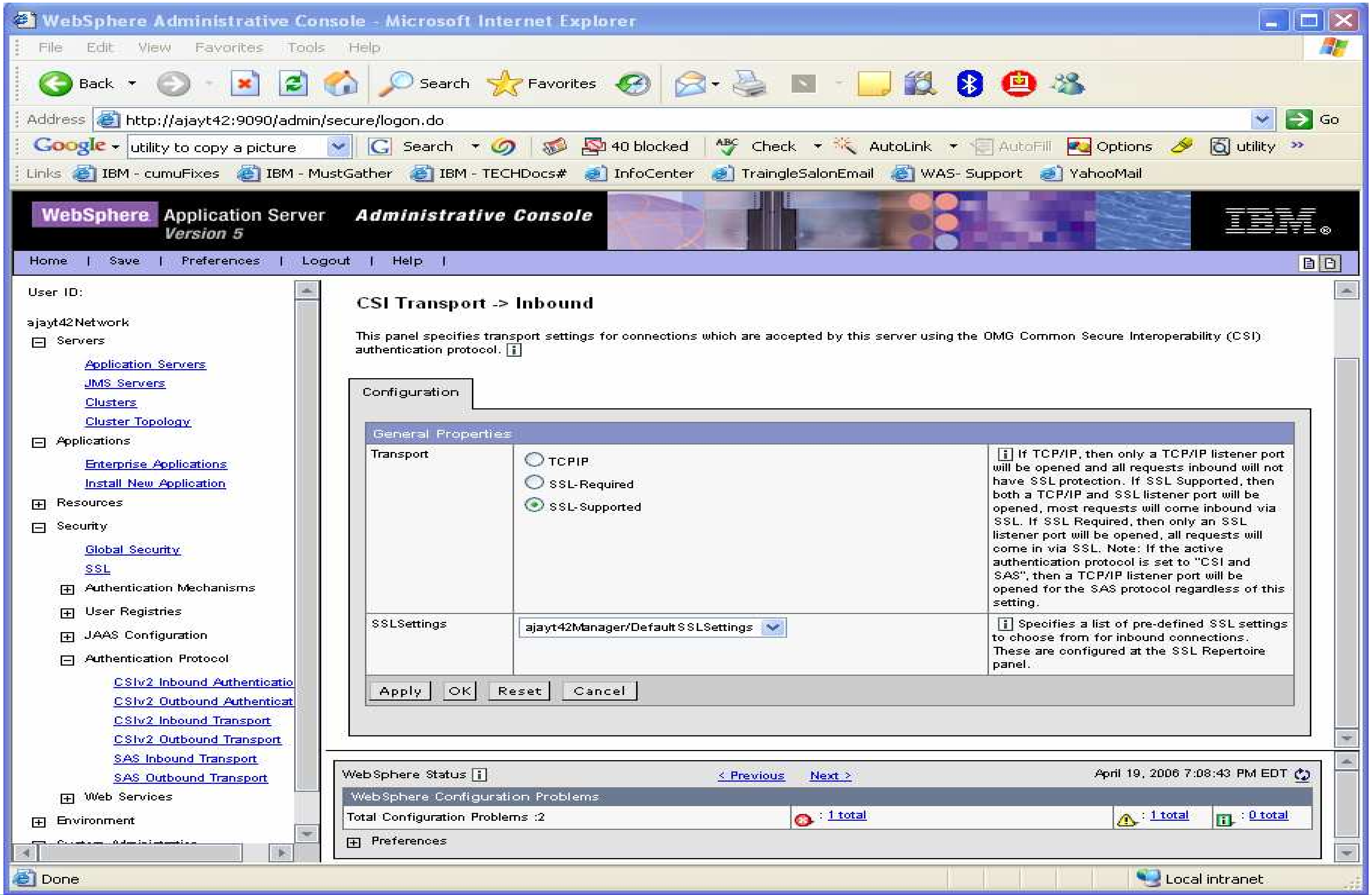
WebSphere Status < Previous Next > April 19, 2006 6:57:43 PM EDT

WebSphere Runtime Messages

Total All Messages:72 : 0 new, 0 total : 0 new, 0 total : 72 new, 72 total

Associating repertoire to ORB

1. Open WSAS Admin console
2. Navigate in the left pane
3. Expand Security and click on “Authentication Protocol”
4. Click on CSIv2 Inbound Transport or CSIv2 Outbound Transport


WebSphere Administrative Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://ajayt42:9090/admin/secure/logon.do Go
Google utility to copy a picture Search 40 blocked Check AutoLink AutoFill Options utility
Links IBM - cumuFixes IBM - MustGather IBM - TECHDocs# InfoCenter TraingleSalonEmail WAS- Support YahooMail
WebSphere Application Server Version 5 Administrative Console
Home | Save | Preferences | Logout | Help |
User ID:
ajayt42Network
Servers
Application Servers
JMS Servers
Clusters
Cluster Topology
Applications
Enterprise Applications
Install New Application
Resources
Security
Global Security
SSL
Authentication Mechanisms
User Registries
JAAS Configuration
Authentication Protocol
CSIv2 Inbound Authenticatio
CSIv2 Outbound Authenticat
CSIv2 Inbound Transport
CSIv2 Outbound Transport
SAS Inbound Transport
SAS Outbound Transport
Web Services
Environment
Done
Local intranet

CSI Transport -> Inbound

This panel specifies transport settings for connections which are accepted by this server using the OMG Common Secure Interoperability (CSI) authentication protocol.

Configuration

General Properties

Transport	○ TCPIP ○ SSL-Required ● SSL-Supported	If TCP/IP, then only a TCP/IP listener port will be opened and all requests inbound will not have SSL protection. If SSL Supported, then both a TCP/IP and SSL listener port will be opened, most requests will come inbound via SSL. If SSL Required, then only an SSL listener port will be opened, all requests will come in via SSL. Note: If the active authentication protocol is set to "CSI and SAS", then a TCP/IP listener port will be opened for the SAS protocol regardless of this setting.
SSLSettings	ajayt42Manager/DefaultSSLSettings	Specifies a list of pre-defined SSL settings to choose from for inbound connections. These are configured at the SSL Repertoire panel.

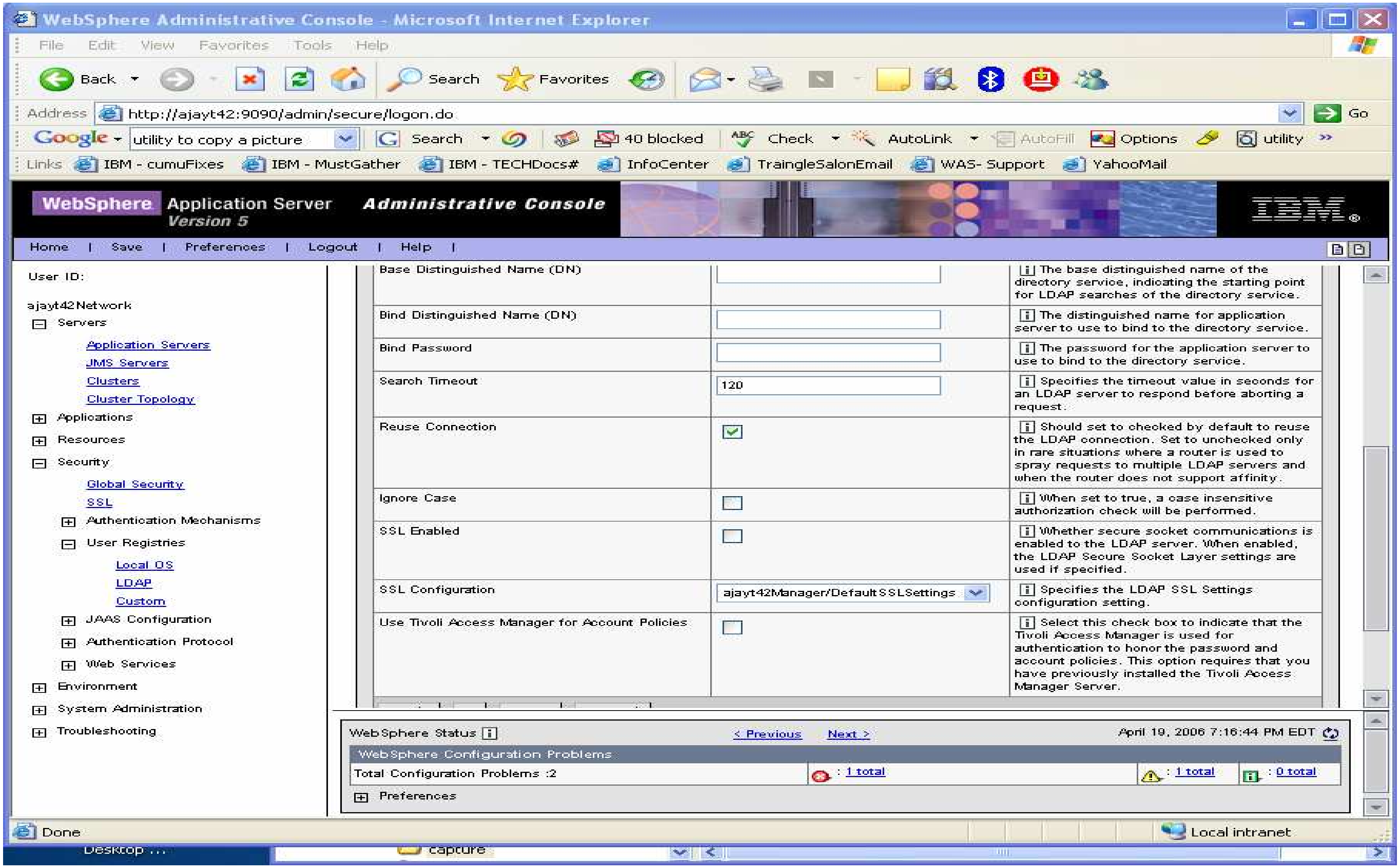
WebSphere Status < Previous Next > April 19, 2006 7:08:43 PM EDT

WebSphere Configuration Problems

Total Configuration Problems :2 : 1 total : 1 total : 0 total

Associating repertoire to LDAP

1. Open WSAS Admin console
2. Navigate in the left pane
3. Expand Security click on “User Registries”
4. Click on LDAP


WebSphere Administrative Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://ajayt42:9090/admin/secure/logon.do Go
Google utility to copy a picture Search 40 blocked Check AutoLink AutoFill Options utility
Links IBM - cumuFixes IBM - MustGather IBM - TECHDocs# InfoCenter TraingleSalonEmail WAS- Support YahooMail
WebSphere Application Server Version 5 Administrative Console
Home | Save | Preferences | Logout | Help |
User ID:
ajayt42Network
Servers
Application Servers
JMS Servers
Clusters
Cluster Topology
Applications
Resources
Security
Global Security
SSL
Authentication Mechanisms
User Registries
Local OS
LDAP
Custom
JAAS Configuration
Authentication Protocol
Web Services
Environment
System Administration
Troubleshooting
Done
Local intranet

Base Distinguished Name (DN)		The base distinguished name of the directory service, indicating the starting point for LDAP searches of the directory service.
Bind Distinguished Name (DN)		The distinguished name for application server to use to bind to the directory service.
Bind Password		The password for the application server to use to bind to the directory service.
Search Timeout	120	Specifies the timeout value in seconds for an LDAP server to respond before aborting a request.
Reuse Connection	☑	Should set to checked by default to reuse the LDAP connection. Set to unchecked only in rare situations where a router is used to spray requests to multiple LDAP servers and when the router does not support affinity.
Ignore Case	☐	When set to true, a case insensitive authorization check will be performed.
SSL Enabled	☐	Whether secure socket communications is enabled to the LDAP server. When enabled, the LDAP Secure Socket Layer settings are used if specified.
SSL Configuration	ajayt42Manager/DefaultSSLSettings	Specifies the LDAP SSL Settings configuration setting.
Use Tivoli Access Manager for Account Policies	☐	Select this check box to indicate that the Tivoli Access Manager is used for authentication to honor the password and account policies. This option requires that you have previously installed the Tivoli Access Manager Server.

WebSphere Status < Previous Next > April 19, 2006 7:16:44 PM EDT

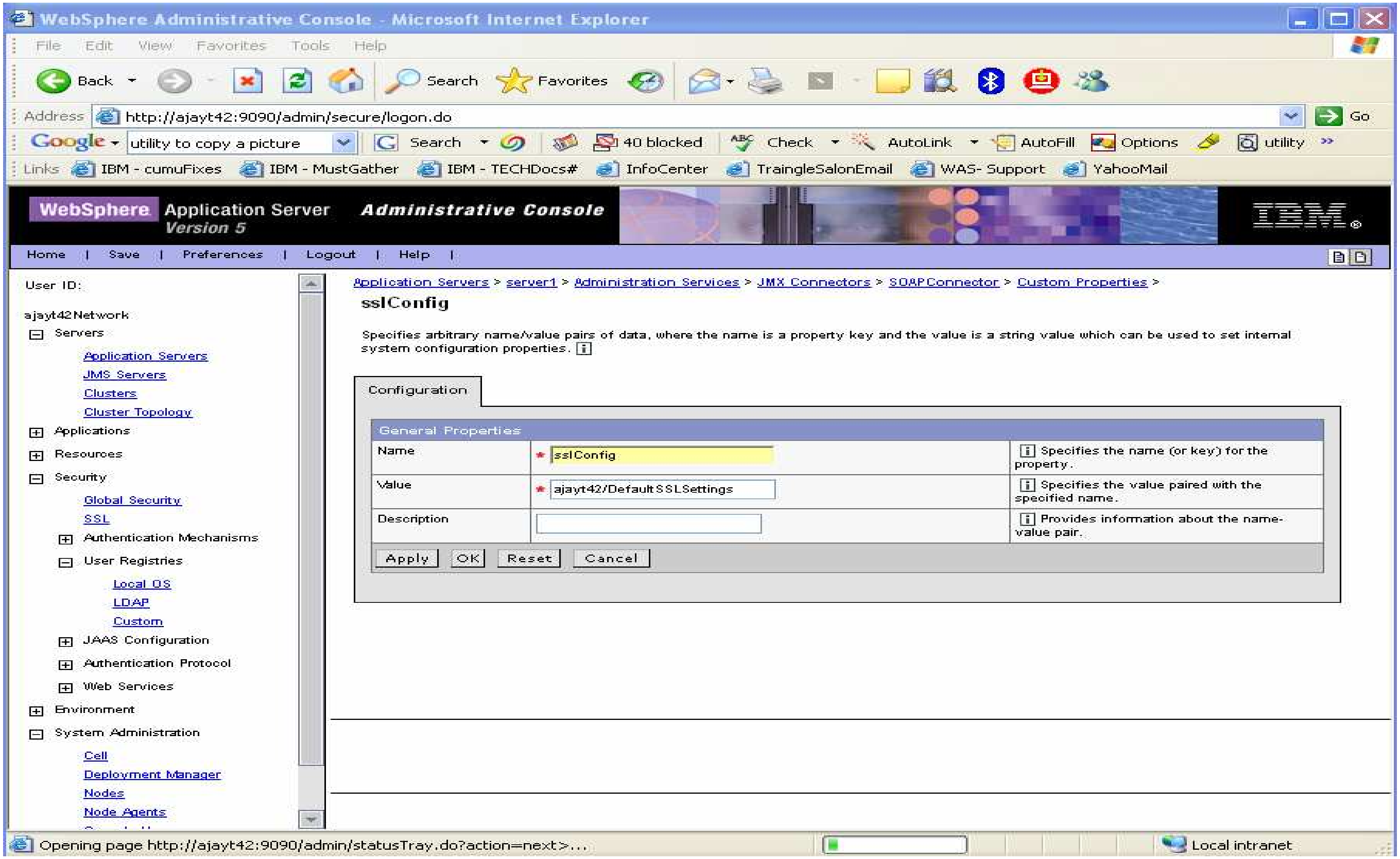
WebSphere Configuration Problems

Total Configuration Problems :2 : 1 total : 1 total : 0 total

Preferences

Associating repertoire to SOAP port

1. Open WSAS Admin console
2. Navigate in the left pane
3. Expand Servers and click on “Application Servers”
4. Click on your server
5. Under additional properties click on “Administration Services”
6. Under additional properties click on “JMX Connectors”
7. Click on “SOAPConnector”
8. Click on “sslConfig”



http://ajayt42:9090/admin/secure/logon.do

Application Servers > server1 > Administration Services > JMX Connectors > SOAPConnector > Custom Properties >

sslConfig

Specifies arbitrary name/value pairs of data, where the name is a property key and the value is a string value which can be used to set internal system configuration properties.

Name	* sslConfig	Specifies the name (or key) for the property.
Value	* ajayt42/DefaultSSLSettings	Specifies the value paired with the specified name.
Description		Provides information about the name-value pair.

Opening page http://ajayt42:9090/admin/statusTray.do?action=next>...

Common Problems - 1

- Able to connect to LDAP over non SSL but cannot connect via SSL port
    1. Find the SSL repertoire associated with LDAP configuration with in WSAS
    2. Make sure the signer certificate of the server(LDAP) is present in the truststore file defined in the repertoire

Common Problems - 2

- Deploy of a portlet fails – the error is SSL [10/14/05 9:28:09:599 CDT] 63daf428 SystemOut O Alert: fatal, unknown certificate
    - Portal server uses SOAP communication to connect to deployment manager and when SSL is enabled the signer certificate configured in the SOAP port is sent to the client (portal server). If the signer cert is not present in the client (CACERTS by default in portal server) then unknown certificate error will occur.

Helpful URLs

- WSAS Support Site:
  http://www-306.ibm.com/software/webservers/appserv/was/support/
- WSAS Information Centers:
  http://www-306.ibm.com/software/webservers/appserv/was/library/
- Custom SSL for advanced JSSE developers:
  http://www-128.ibm.com/developerworks/java/library/j-customssl/
- MustGather document for JSSE/SSL issues:
  http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQTP&uid=swg21162961

Additional WebSphere Product Resources

- Discover the latest trends in WebSphere Technology and implementation, participate in technically-focused briefings, webcasts and podcasts at: www.ibm.com/developerworks/websphere/community/

- Learn about other upcoming webcasts, conferences and events: www.ibm.com/software/websphere/events_1.html

- Join the Global WebSphere User Group Community: http//www.websphere.org

- Access key product show-me demos and tutorials by visiting IBM Education Assistant: www.ibm.com/software/info/education/assistant

- Learn about the Electronic Service Request (ESR) tool for submitting problems electronically: www.ibm.com/software/support/viewlet/probsub/ESR_Overview_viewlet_swf.html

- Sign up to receive weekly technical My Support emails: www.ibm.com/software/support/einfo.html

Questions and Answers