

IBM Security Verify Access
Version 10.0.2
June 2021

Product overview



Contents

- Accessibility features for Security Verify Access..... v**
- Chapter 1. Documentation for getting started..... 1**
- Chapter 2. What's new in this release.....3**
- Chapter 3. Product requirements..... 9**
- Chapter 4. Documentation for an activation level.....11**
- Chapter 5. Secure deployment considerations..... 13**
- Chapter 6. Upgrading to the current version..... 15**
- Chapter 7. APARs fixed in this version..... 19**
- Chapter 8. Compatibility with earlier versions of the product..... 21**
- Chapter 9. Known limitations..... 23**
- Chapter 10. Security Verify Access appliance FRU/CRU documentation.....27**
 - Disk Drive Assembly Replacement Instructions 27
 - Replacing a storage drive assembly..... 27
 - Fan Assembly Replacement Instructions..... 28
 - Replacing a fan assembly.....29
 - Network Interface Module Replacement Instructions 30
 - Replacing a failed network interface module.....30
 - Power Supply Replacement Instructions 32
 - Identifying a failed power supply..... 32
 - Replacing a failed power supply 34
- Chapter 11. Supporting content..... 37**
- Chapter 12. Language support overview.....39**
- Index..... 41**

Accessibility features for Security Verify Access

Accessibility features assist users who have a disability, such as restricted mobility or limited vision, to use information technology content successfully.

Accessibility features

Security Verify Access includes the following major accessibility features:

Accessibility features
Supports interfaces commonly used by screen readers. This feature applies to applications on Windows operating systems only.
Can be operated by using only the keyboard.
Allows the user to request more time to complete timed responses.
Supports customization of display attributes such as color, contrast, and font size.
Communicates all information independently of color.
Supports interfaces commonly used by screen magnifiers. This feature applies to applications on Windows operating systems only.
Allows the user to access the interfaces without inducing seizures due to photosensitivity.

Security Verify Access uses the latest W3C Standard, [WAI-ARIA 1.0](http://www.w3.org/TR/wai-aria/) (<http://www.w3.org/TR/wai-aria/>), to ensure compliance to [US Section 508](http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) (<http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards>), and [Web Content Accessibility Guidelines \(WCAG\) 2.0](http://www.w3.org/TR/WCAG20/) (<http://www.w3.org/TR/WCAG20/>). To take advantage of accessibility features, use the latest release of your screen reader in combination with the latest web browser that is supported by this product.

The Security Verify Access online product documentation in IBM® Knowledge Center is enabled for accessibility. The accessibility features of IBM Knowledge Center are described at <https://www.ibm.com/support/knowledgecenter/help?view=kc#accessibility>.

Keyboard navigation

This product uses standard navigation keys.

Interface information

The Security Verify Access user interfaces do not have content that flashes 2 - 55 times per second.

The Security Verify Access web user interfaces and the IBM Knowledge Center rely on cascading style sheets to render content properly and to provide a usable experience. The application provides an equivalent way for low-vision users to use a user's system display settings, including high-contrast mode. You can control font size by using the device or web browser settings.

The Security Verify Access web user interface includes WAI-ARIA navigational landmarks that you can use to quickly navigate to functional areas in the application.

Related accessibility information

In addition to standard IBM help desk and support websites, IBM has established a TTY telephone service for use by deaf or hard of hearing customers to access sales and support services:

TTY service 800-IBM-3383 (800-426-3383) (within North America)

IBM and accessibility

For more information about the commitment that IBM has to accessibility, see [IBM Accessibility \(www.ibm.com/able\)](http://www.ibm.com/able).

Chapter 1. Documentation for getting started

The IBM Knowledge Center provides documentation that can help you get started with the IBM Security Verify Access product.

IBM Security Verify Access is available from Passport Advantage. You can use this distribution to either configure a new deployment or upgrade a previous version of the product.

1. If you are upgrading from a previous version of IBM Security Verify Access for Web 8.*, IBM Security Verify Access for Mobile 8.*, or IBM Security Verify Access 9.0 be sure to review [Chapter 6, “Upgrading to the current version,”](#) on page 15. If applicable, you must complete these steps before you configure the product.
2. See [Product activations overview](#) to review the features you can use when you activate the Security Verify Access Platform, the Advanced Access Control Module, or the Federation Module.
3. Configure the appliance by using the instructions in [Getting Started](#).
4. Complete the initial setup of your Security Verify Access appliance deployment by following the instructions in [Initial configuration](#).
5. (Advanced Access Control Module only) Complete the initial setup of this module by following the instructions in [Getting Started with Advanced Access Control](#).

Security Verify Access Platform includes an optional Java ADK, available for download. To install the Java ADK, see [Intalling IBM Security Verify Access Runtime for Java](#).

See [Administering Web Reverse Proxy](#) for instructions on how to use the local management interface on the appliance to configure and administer Security Verify Access Platform.

Chapter 2. What's new in this release

IBM Security Verify Access provides new features and extended functions for Version 10.0.2.

Verify Access Platform

- Proxy Protocol Support

The Web reverse proxy now supports the 'proxy protocol' for the receipt of connection information from a proxy which sits in front of the Web reverse proxy. See [Proxy Protocol Support](#).

- Client IP Rules

The Web reverse proxy now provides the ability to define rules to permit or deny connections based on the client IP address. See [Client IP Rules](#).

- Reverse Proxy Persistent Sessions

A change has been made to the format of the tokens which are used for persistent sessions which means that tokens which have been created by an earlier version of Verify Access will no longer work. Users will be prompted to re-authenticate if an older token is provided to the Reverse Proxy. For more information on persistent sessions, see [Persistent Sessions](#).

- LMI Message Timeout

A new administrator setting has been added to allow a timeout to be set for LMI notification messages. The default timeout is set as 5 seconds. Setting a value of 0 removes the timeout and messages will remain until manually closed. To update this entry, see [Configuring administrator settings](#).

- License Auditing for Containerized Deployments

The IBM License Metric Tool (ILMT) container now supports IBM Security Verify Access. By using the ILMT container, administrators are able to automate license usage and auditing for deployments which use Kubernetes infrastructure and are based on a processor based licensing model. To deploy the ILMT container with Verify Access, see [License usage with IBM Security Verify Access deployed on Kubernetes](#).

- nCipher Hardserver and watchdog log forwarding

Remote Syslog forwarding capabilities has been added for the nCipher watchdog and hardserverlog files. These log files can now be collected by a remote logging server where they can be centrally managed. To set up a remote syslog server for IBM Security Verify Access, see [Forwarding logs to a remote syslog server](#).

- Junctioned Servers Priority

It is now possible, when configuring a junctioned server in the Web Reverse Proxy, to specify a priority value for the server. See [Adding multiple back-end servers to the same junction](#).

- Adding HTTP Headers to requests

It is now possible to generate a HTTP header, from a credential attribute, which is inserted into requests sent to any junction. See [Adding a HTTP header for all junctions](#).

- Container Enhancements

To help improve the start-up time of Docker containers the verification of files on the file system is now controlled by the VERIFY_FILES environment variable. See [Docker Image for Security Verify Access](#).

A new container image has been created which embeds the AAC and Federation runtime. See [Docker Image for Verify Access Runtime](#).

A new container image has been created which provides the Web Reverse Proxy capabilities. See [Docker Image for Verify Access Web Reverse Proxy](#).

Note: The capability of running the verify-access image as anything other than a configuration container is being deprecated and will not be available in verify-access images released after 2021. The new runtime, Web reverse proxy and DSC images should be used instead.

The management of Web Reverse Proxy instances, including junction management and object space management, from the configuration container is now more efficient and performant.

Support for a Kubernetes start-up probe has been added to the embedded health check script. See [Kubernetes support](#).

A new container image has been created which provides the Distributed Session Cache capabilities. See [Docker image for Verify Access Distributed Session Cache](#).

- Reverse Proxy Auditing

It is now possible to configure the Web reverse proxy to send audit records in JSON format. See [audit-json](#).

- Reverse Proxy JWT Support

A configuration option is now available which controls, when the Web Reverse proxy generates a JWT to be sent to a junctioned application:

- The lifetime of the generated JWT. See [lifetime](#).
- The format of the HTTP header which is added to the request. See [hdr-format](#).

- Junction Cookie

The junction cookie can now be returned to clients as a standard HTTP cookie. See [Inserting the junction cookie as a standard HTTP cookie](#).

- Enable Junction Protocols

It is now possible to enable and disable SSL/TLS protocols on a per junction basis. See [\[junction:<jct-id>\] stanza](#)

- Web Reverse Proxy Tracing

The snoop tracing for the Web Reverse proxy can now be activated on a per junction basis. See [junction-specific-snoop](#).

- Management Authentication

When a remote LDAP user registry is configured for management authentication the DN of a client certificate can now be mapped to a new format using a Javascript function. See [Configuring management authentication](#).

- Web Reverse Proxy TFIM Junction Configuration

It is now possible to set global configuration entries for TFIM SSO style junctions. See [Single sign-on Security Token Service](#).

- Access Logging for Administrator Interface

Support has been added to log administrator requests to the Local Management Interface (LMI). The output format of this log can be customized using an administrator setting. See [Configuring administrator settings](#).

- Reverse Proxy OAuth Introspection

You can now configure additional HTTP headers which will be sent to the OAuth introspection endpoint. See [http-header](#).

- Runtime FIPS file integrity check

A new command has been added to the FIPS Command Line Interface (CLI) menu on FIPS enabled appliances. This command scans the appliance file system and validates that the firmware has not been modified. To learn more about FIPS Compliance, see [FIPS 140-2](#).

- New Management Authorization Roles

Two new management authorization roles have been added: **Full Read** which permits read access to all Local Management Interface (LMI) URLs and **Full Write** which permits write access to all LMI URLs. Unlike existing authorization roles, Full Read and Full Write do not use a feature list and do not need to be updated when an appliance is upgraded. See [Managing roles of users and groups](#).

- Statistics Monitoring

The memory, storage, CPU and interface monitoring statistics can now be returned for shorter ranges. See [Monitoring](#).

- Amazon CloudWatch Support

The virtual appliance now supports the unified CloudWatch agent which can be used to report on metrics from the virtual appliance in a Amazon Web Services (AWS) environment. See [Configuring Amazon CloudWatch support](#).

- AAC Configuration Wizards

The AAC configuration wizards, which are used to configure the Web reverse proxy as a point of contact, have been modified so that the automatic retrieval of the server certificate from the runtime profile is now optional. This allows the configuration to successfully complete even when the AAC runtime server is not available. This impacts the MMFA Configuration, OAuth and OpenID Connect Provider Configuration, Authentication and Context Based Access Configuration, and IBM Verify Gateway Configuration wizards.

- Web Reverse Proxy Certificate Validation

It is now possible to perform CN and Subject Alternative Name validation on certificates which are provided by Junctioned servers. See [Matching the common name \(CN\) and subject alternative name \(SAN\)](#).

- Reverse Proxy HTTP Header Sessions

It is now possible to restrict the creation of HTTP Header indexed sessions to include only those HTTP headers which have been used in the authentication process. See [require-auth-session-http-hdrs](#).

- Remote Syslog Forwarding

It is now possible to forward messages to a remote syslog server using the syslog format defined in RFC5424. See [Forwarding logs to a remote syslog server](#).

- RSA SecurID configuration

In the RSA SecurID configuration the ability to provide a `sdopts.rec` file has been added. This allows the specification of the IP address that the SecurID authentication method should use. See [Managing RSA SecurID configuration](#).

- Deprecated Reverse Proxy SSO functionality

For new installations of IBM Security Verify Access the legacy cross-domain single-sign-on (CDSSO) and e-community single-sign-on (eCSSO) authentication mechanisms have been deprecated. In these environments a more modern federated single-sign-on protocol should be used. These authentication mechanisms will however continue to work in an environment which has been upgraded from an older version of Verify Access.

The query contents capability of the Web Reverse Proxy has been deprecated. This legacy capability allowed the Web Reverse Proxy to send a Web request to a junctioned server to determine the composition of the policy object space for the junction. This has no impact on the ability to attached ACLs and POPs to any location under a junction.

Advanced Access Control (AAC)

- Managing LDAP password attributes

Support is now added for updating LDAP User Registry attributes when you are performing password authentication using AAC AuthSvc. Administrators can now update LDAP attributes which record the number of failed password attempts and the last successful login time. This capability is available from

either the Username/Password authentication mechanism, or using the `UserLookupHelper` in an InfoMap authentication rule. See [Configuring username and password authentication](#).

- Apple Push Notification Service Updates

The Apple Push Notification Provider has been updated to use the new HTTP/2 Apple Push Notification service API. The previous implementation was based on the Binary Provider API, which has been decommissioned by Apple and is no longer available. Migration of configuration data relating to Apple Push Notification Service will be done automatically on upgrade. See [Push notification registration](#).

- New Request Context Attributes and Macros

Multiple new request context attributes have been added for use in AAC Mapping Rules. See [Authentication policy parameters and credentials](#). The Target URL is also now available as a default macro, `@TARGET@`.

- AuthSvcClient helper for InfoMap policy execution

A new helper has been added which allows administrators to complete other authentication service policies within an InfoMap step without having to use HTTP requests to the authentication service. For more details and a simple example, see [Execute authentication service policies in an Info Map](#)

- Sample geo-location database

The appliance firmware no longer embeds a sample geo-location database. A free database which can be used is available from the MaxMind site (<https://www.maxmind.com>). See [Updating location attributes](#).

- Local FIDO2 Client Custom Challenge

The LocalFIDOClient helper has been updated to allow a custom challenge to be specified in both the assertion and attestation options requests. See [Local FIDO Client](#).

- Redis Support

Support has been added for storing Authentication Service user sessions in Redis via the Distributed Map (DMap) when cookie-less is enabled. See [Configuring the authentication and access module for cookieless operation](#) and [Server connection properties](#).

The HVDB value for `authsvc.stateMgmt.store` has been removed. The HVDB can still be used as the cookie-less store, configured instead via the new DMap implementation, which supports HVDB as a store.

FIDO2 short-lived data is stored in the DMap and will be impacted by the new DMap store configuration. See [Advanced configuration properties](#).

- RSA One-Time Password has been deprecated

The RSA SecurID Authentication agent used by the RSA One-Time Password mechanism has been deprecated and is no longer supported. See [RSA SecurID Authentication API](#).

Instead use the RSA SecurID mechanism which utilizes the REST-based Authentication API. See [Configuring an RSA one-time password mechanism](#). To enable the Authentication API on the Authentication Manager, see [How to set up the REST RSA SecurID Authentication API for Authentication Manager 8.2 SP1](#).

- New Local FIDO Client configuration ID discovery function

The LocalFIDOClient helper has been updated to include a new function that can be used to exchange a rpId for the Relying Party configuration ID. See [Local FIDO Client](#).

- IBM Security Verify Gateway Integration

An InfoMap based integration with IBM Security Verify Gateway has been added. Two Verify Gateway wizards have been created in the LMI to ensure all the required configuration is performed, located under the Reverse Proxy Manage menu, and a new AAC menu item **IBM Security Verify Gateway**. See [IBM Security Verify Gateway](#).

Federation

- Support for JSON Web Token (JWT) PS signing algorithm

The IBM Security Verify Access Federation component now supports the PS signing algorithm. See [JWT Support](#).

- OAuth2 Token Exchange

Token Exchange can now be enabled as OAuth2 grant type on IBM Security Verify Access. See [OAuth 2.0 and OIDC workflows](#).

- Redis Support

IBM Security Verify Access now supports storing HTTP sessions and Protocol specific sessions into Redis. See [Server connection properties](#).

- Federation Connection Templates

The appliance firmware no longer embeds a copy of the Federation connector templates. The template package is available for download from [IBM Security App exchange](#). See [Managing federation partner templates](#).

- Support for regular expression based signature validation

SAML 2.0 service provider partners now supports regular expression based signature validation for assertion during Single Sign On flows. See [SAML 2.0 Service Provider Partner Worksheet](#).

- Session Persistence

Support has been added to the Local Management Interface (LMI) to allow the Advanced Access Control and Federation session persistence stores and consumers to be configured through their own UI page. See [Managing Session Persistence](#).

Chapter 3. Product requirements

You can view Software Product Compatibility Reports that list the system requirements and appliance specifications for the product.

The reports provide current information about hardware and software support and requirements for IBM Security Verify Access.

- System requirements for hardware appliance:
 - Prerequisite software, including supported databases, user registries, and browsers
 - Appliance specifications such as disk size, memory, network ports, physical characteristics, and electrical and environmental parameters
- System requirements for the virtual appliance:
 - Supported hypervisors, databases, user registries, and browsers
 - Disk space and memory requirements for virtual images

To view the reports, see [Software Product Compatibility Reports](#).

You can also view the specifications of the hardware and virtual appliance in the following Technotes:

- [Hardware appliance specifications](#)
- [Virtual appliance specifications](#)

WebSEAL client support

When acting as a reverse proxy, WebSEAL generally supports clients that conform to the HTTP 1.1 standard as defined by RFC 2616 and the HTTP/2 standard as defined by RFC 7540. The preceding statement is not a comprehensive statement of support. WebSEAL relies on a number of client characteristics that are either not defined or are loosely defined by RFC 2616 and RFC 7540. Examples of such characteristics include, but are not limited to:

- Cookie management
- SSL support
- Concurrency of multiple connections

Widely used browsers such as Firefox, Chrome, Safari, and Internet Explorer support such characteristics during typical use.

The extension of browser capabilities that modify these characteristics can, however, introduce compatibility problems with WebSEAL. The same is true of other client types, such as mobile applications or rich clients. Compatibility complications that cannot be resolved through modification of the environment or configuration of the WebSEAL product are not supported.

Chapter 4. Documentation for an activation level

IBM Security Verify Access uses the listed activation levels, depending on the modules you purchase. Use the information in the tables to determine which topics to start with in the documentation.

Security Verify Access Supporting Components

No activation key is required for these functions.

Table 1. Security Verify Access Supporting Components functions and topic links

Function	Topic
Appliance Management: Local Management Interface	Appliance Management
Appliance Management: REST APIs	REST API documentation
Policy Server	Policy server administration tasks
Embedded LDAP server	Embedded LDAP server management
Authorization Server	Authorization servers

Security Verify Access Platform

An activation key is required for these functions.

Table 2. Security Verify Access Platform functions and topic links

Function	Topic
Web Reverse Proxy	Web Reverse Proxy configuration and Web Reverse Proxy administration
Load Balancer	Front-end load balancer
X-Force threat protection	Configuring web application firewall
Distributed Session Cache	Distributed session cache

Advanced Access Control Module

This module is an add-on feature that requires an activation key.

Table 3. Advanced Access Control functions and topic links

Function	Topic
Authentication	Authentication
OAuth 2.0 API protection	Configuring API protection
Context-based access	Overview of context-based access
Device fingerprinting	Device fingerprints
Device registration	Consent-based device registration
HOTP and TOTP Key Manager	Managing OTP secret keys
Fine-grained authorization/XACML 2.0	Access control policies
Runtime security services	Runtime security services external authorization service

Table 3. Advanced Access Control functions and topic links (continued)

Function	Topic
Policy distribution (Policy administration point)	Risk management overview

Federation Module

This module is an add-on feature that requires an activation key.

Table 4. Federation functions and topic links

Function	Topic
SAML 2.0 Federations	SAML 2.0 federations
Open ID Connect Federations	OpenID Connect Federations
Module chains	Manage module chains and Configuring STS modules

Related information

[Product activations overview](#)

Chapter 5. Secure deployment considerations

When you deploy the IBM Security Verify Access appliance, consider the following points.

- The Security Verify Access embedded user registry should only be used in the following scenarios:
 - Proof of Technology deployments
 - Deployments with a low number of Security Verify Access users (< 5000)
 - When using federated directories with the Security Verify Access basic user feature
- Choose the suitable Security Verify Access user authentication mode for your environment.
 - Use basic user for all scenarios unless GSO lock-box, user based ACLs, or account-valid/password-valid features are required.
 - Only use the full user model if basic user is not suitable. Basic user only supports minimal mode.
- The appliance has management and application interfaces. Network separation between the management and application interfaces must be maintained.
- Any Security Verify Access web reverse proxies that are hosted in the corporate DMZ network zone should be configured as restricted nodes.
- The Security Verify Access appliance that hosts the Policy Server component should be hosted in a secure network zone and not exposed to the internet.
- If the embedded user registry is used, it should be hosted on the same appliance as the Security Verify Access Policy Server in a secure network zone. The embedded user registry port (636) should not be routable from the internet.
- Security Verify Access clustering is recommended to provide a highly available solution. Two Security Verify Access appliances performing the primary and secondary roles respectively should be used. These should be hosted in the secure network zone with Security Verify Access runtime replication enabled.
- If advanced authentication/authorization is required, the Security Verify Access authentication service in the Advanced Access Control (AAC) component should be used. This should be hosted on the Security Verify Access primary and secondary appliances in the secure network zone. This service should not be routable from the internet.
- Second factor or multi-factor authentication should be considered to increase assurance of user identity.
- Enable Network Time Protocol (NTP) on all appliances to synchronize the time correctly. This is to ensure that the appliance works correctly with distributed components.
- Do not use self-signed certificates for any public facing services. Always obtain certificates issued by an appropriate certificate authority.
- All non-TLS communication should be disabled:
 - Only use port 636 for LDAP communication.
 - Only use HTTPS 443 application interfaces.
 - Only use TLS for junction communication.
- Enable the Security Verify Access Web Application Firewall (WAF) feature on all appliances hosting the Security Verify Access reverse proxy.
- Session affinity should be enabled between all Security Verify Access components for performance and scalability reasons.
- The Security Verify Access Distributed Session Cache (DSC) or failover cookie should be used to provide a highly available solution across multiple reverse proxy instances.
- If the DSC is deployed, it should be hosted in the secure network zone.

- Configure the reverse proxy cookie jar feature to prevent application cookies from being returned to clients unnecessarily.
- Connection pooling for junctions should be enabled to optimize performance of the solution. This capability is disabled by default.
- FIPS should be enabled if appropriate.
- Enable these security headers in the reverse proxy configuration:
 - **strict-transport-security**
 - **content-security-policy**
- Minimize access to unauthenticated resources using standard Security Verify Access ACL policy.
- Host the Security Verify Access runtime database on an external Database. This database is used for federation and/or AAC features. The runtime database should be hosted in a secure network zone and should not be routable from the internet.
- Use a highly available solution for the external Security Verify Access runtime database. This service is critical to Security Verify Access operation.
- Best practice is to use the Security Verify Access REST APIs for automated deployment to allow:
 - Rapid recovery
 - Consistent and repeatable deployment configuration
- Don't use Basic Authentication (BA) for authentication to Security Verify Access REST APIs when automating deployment and management of the Security Verify Access appliance. Certificate authentication should be used.
- Standard network security guidelines should be applied. Network access and administrative credentials to the appliance should only be available to authorized administrators on appropriate networks.
- Minimize on-board storage of logs by configuring remote syslog to store log and audit archives in a protected network zone. A separate logging server/service should be used to store logs.
- An appropriate patch process should be implemented to:
 - Subscribe to, and monitor IBM support site for Security Verify Access appliance patches
 - Apply all patches promptly when released
- Set the **sps.setCookiesAsSecure** parameter to Secure to flag the cookies set by Security Verify Access.

Chapter 6. Upgrading to the current version

Complete this task if you are upgrading an existing Security Verify Access for Web, Security Verify Access for Mobile, or Security Verify Access installation to the current version.

Before you begin

Important:

See [IBM Security Verify Access Upgrade Paths](#).

When you upgrade a cluster, upgrade the primary master first and do not upgrade the remaining cluster nodes until the primary master finishes upgrading and is operational.

In the case where one of the non-primary nodes is upgraded when the primary master is not available, upon upgrade completion the node will be in a non-operational state. To rectify this problem, remove the non-operational node from the cluster and then re-add it. This approach will ensure that the configuration and database replication returns to a working state.

If you are installing the virtual appliance for the first time, download the .iso image and follow the installation instructions in the [IBM Security Verify Access Virtual Appliance](#).

Review the following tasks and complete the tasks that are appropriate to your environment:

Clear the browser cache

As part of the upgrade process, clear your browser cache to reduce the likelihood of encountering issues with cached items.

USB drive for an update

If you use a USB drive for an update, it must be formatted with a FAT file system.

Risk engine reports

Any risk engine reports that you generated before you begin the upgrade task are not preserved. Export copies of the risk reports and save them locally by completing the following steps:

1. Log in to the local management interface.
2. Click **Monitor > Application Log Files**.
3. Expand **access_control** and select the risk reports to export.
4. Click **Export** and save the files.

Database failover in a cluster

For information about how the upgrade affects database failover in a cluster, see the [Database failover capabilities vary during a cluster upgrade](#) section in [Advanced Access Control known issues and solutions](#).

Procedure

Choose one of the following upgrade methods and complete the steps:

Use the online update server.

- a. Meet the following conditions:
 - A valid license is installed on the appliance.
 - The appliance has network connectivity to the online update server.
- b. Log in to the local management interface. If you are upgrading a cluster, log in to the local management interface of the primary master first.
- c. Select **System > Updates and Licensing > Available Updates**.
- d. Click **Refresh**.
- e. Select the firmware update.

- f. Click **Install**. The firmware update might take a long time to complete, depending on the bandwidth that is available to the appliance. After the update is successfully applied, the appliance automatically restarts.
- g. If you use any external databases, download the **dbupdate9.zip** file from **File Downloads** area of the appliance and upgrade the external databases.
- h. If you are upgrading a cluster, complete the following steps:
 - i) Repeat steps “1.b” on page 15 through “1.f” on page 16 on each node in the cluster starting with the secondary master.

Note: If you use internal databases, do not subsequently reboot the primary master until the secondary master has been upgraded.
 - ii) Wait for the cluster to synchronize. The firmware for each appliance in the cluster is now upgraded and the cluster is operational.

Note: Although the secondary master remains present and the embedded runtime database fails over to the secondary master when the primary master is down during the migration, you cannot avoid down time by leveraging this failover mechanism. This is due to the fact that the database changes made to the secondary master while the primary master is being migrated will likely be discarded and replaced by the upgraded databases from the primary master after it begins operating again after the migration.

Use the local management interface for a single appliance *not* in a cluster.

- a. Download the .pkg file.
- b. Log in to the local management interface.
- c. Select **System > Updates and Licensing > Available Updates**.
- d. Click **Upload**. The **New Update** window opens.
- e. Click **Select Update**.
- f. Browse to the .pkg file.
- g. Click **Open**.
- h. Click **Save Configuration**. The upload process might take several minutes.
- i. Select the new firmware and click **Install**. The installation of the new firmware takes a few minutes. After the update is successfully applied, the appliance restarts automatically.

Use the local management interface for a cluster of appliances.

- a. Download the .pkg file.
- b. Log in to the local management interface of the primary master.
- c. Upload and install the firmware .pkg file on the primary master. This step includes the automatic restart of the appliance. If you use internal databases, do not subsequently reboot the primary master until the secondary master has been upgraded.
- d. If you use any external databases, download the dbupdate9.zip file from **File Downloads** area of the primary master and upgrade the external databases.
- e. Upload and install the firmware .pkg file on each node in the cluster starting with the secondary master if present.
- f. Wait for the cluster to synchronize. The firmware for each node in the cluster is now upgraded and the cluster is operational.

Note: Although the secondary master remains present and the embedded runtime database fails over to the secondary master when the primary master is down during the migration, you cannot avoid down time by leveraging this failover mechanism. This is due to the fact that the database changes made to the secondary master while the primary master is being migrated will likely be discarded and replaced by the upgraded databases from the primary master after it begins operating again after the migration.

Use a USB drive. (Only for upgrading a hardware appliance.)

- a. Download the .pkg file.
- b. Copy the firmware update from the .pkg file to a USB flash drive.
- c. Insert the USB flash drive into the hardware appliance.
- d. Log in to the appliance console as admin or use Secure Shell.
- e. Type updates and press Enter.
- f. Type install and press Enter.
- g. Select the following options:
 - i) Type 1 for a firmware update.
 - ii) Type 1 to install the update from a USB drive.
 - iii) Type YES to confirm that the USB drive is plugged into the appliance.
 - iv) Type the index number to select the appliance firmware from the list.
 - v) Type YES to confirm the update and start the update process.

Note: The firmware update takes a few minutes to complete and the appliance automatically restarts.

What to do next

- If you are using an external database to store the runtime or configuration data, you also need to update the database schema. This can be achieved by downloading the database update utility from the appliance and running this utility against the external database. For more details, see [Upgrading external databases with the dbupdate tool \(for appliance at version 9.0.0.0 and later\)](#).
- If you are upgrading an existing appliance, your Security Verify Access Platform is ready to use.
- If you are upgrading an existing Security Verify Access for Mobile appliance or Advanced Access Control module to the current version, continue with the [Upgrading configuration](#) instructions.
- If you are upgrading an existing Federation module to the current version, continue with the [Upgrading configuration](#) instructions.

Chapter 7. APARs fixed in this version

Several APARs were fixed with this version of the product.

For the latest list, see [APARs fixed by IBM Security Verify Access version 10.0.2](#).

Chapter 8. Compatibility with earlier versions of the product

IBM Security Verify Access V10.0.* is compatible with previous versions of Security Verify Access for Web, Tivoli Access Manager for e-business, Security Access Manager for Web, Security Access Manager for Mobile, and Security Verify Access for Mobile.

The Version 10.0.* policy server can communicate with some previous versions of Security Access Manager for Web, Tivoli Access Manager for e-business, and Security Verify Access for Mobile. The following compatibility with earlier versions is supported:

- Policy server compatibility with servers in prior versions
- Compatibility with single sign-on targets
- Limited compatibility with earlier versions for session management

Compatibility with single sign-on targets

IBM Security Verify Access maintains compatibility with earlier versions for all single sign-on information that is sent over HTTP to applications behind WebSEAL junctions. Applications that are written to use single sign-on information that is supplied by previous versions of the product can use the same information that is provided by Version 10.0.*.

This compatibility applies to both custom applications and IBM applications such as the Trust Association Interceptor. The Trust Association interface is a service provider API that enables the integration of third-party security service (for example, a reverse proxy) with WebSphere Application Server. Security Verify Access, version 10.0.*, is compatible with all versions of the Trust Association Interceptor.

Chapter 9. Documentation updates for known limitations

You can view the known software limitations, problems, and workarounds on the IBM® Security Verify Access Support site.

The Support site describes not only the limitations and problems that exist when the product is released, but also any additional items that are found after product release. As limitations and problems are discovered and resolved, the IBM Software Support team updates the online knowledge base. By searching the knowledge base, you can find workarounds or solutions to problems that you experience.

Also, check the [Troubleshooting](#) topics.

Known limitations for Security Verify Access

A system error is displayed briefly when the Mozilla Firefox browser is refreshed.

When you use the Mozilla Firefox browser to access the local management interface, sometimes a system error is displayed briefly during a browser refresh.

This error is displayed because the browser refresh causes an XMLHttpRequest (XHR) request to be canceled before the request finishes. The error does not indicate impact to normal operations and can be ignored.

Unable to remove local users or groups from authorization roles with Mozilla Firefox on Mac OS X.

When you use the local management interface through a Mozilla Firefox browser version on a Mac OS X system, you might not be able to remove a user or group from an authorization role.

On the **Management Authorization** page of the local management interface, when you click **Edit**, the **Edit Local Members** window is displayed. To remove a user or group, normally you uncheck the check box for that user or group and then click **OK** to save the changes. However, if you use Firefox on Mac OS X to complete such operation, the browser does not properly recognize the change and does not display any error messages. The user or group list remains unchanged after you click **OK**.

To avoid such issue on Mac OS X, you have two options:

- Use a different browser to access the local management interface.
- Use the REST API. See the [REST API documentation](#) and browse to **Manage: System Settings > System Settings > Management Authorization > Updating an authorization role**.

Lower throughput observed with certificate revocation list enabled

Enabling certificate revocation list (CRL) validation might result in a lower throughput from the system. If your certificate does not have a CRL, you might want to disable CRL checking by using the advanced configuration parameter **kess.crlEnabled**. Alternatively, you might want to reduce the frequency of CRL checking by using the advanced configuration parameter **kess.crlInterval**.

Client certificate authentication for federated directories is not supported for UsernameTokenSTSModule

When you configure a federated directory, do not select a client certificate.

In rare circumstances, an OAuth access token validation might fail.

These instances have been observed very shortly after a restart of the Advanced Access Control runtime server. The symptoms and conditions include:

1. Restart the Advanced Access Control runtime server.
2. Execute an OAuth flow, such as the Resource Owner Password Credential flow, to obtain a valid access and refresh token pair.
3. Attempt to use the access token to access a resource that is protected by the API Definition associated with the OAuth client that has been granted the access token.

Step 3 has been observed to fail on some rare occasions. The cause is due to delayed restart initialization of some internal Advanced Access Control runtime components. Normal successful processing has been observed when the request for the protected resource in step 3 is resubmitted.

Junction type for Security Verify Access Oracle PeopleSoft PeopleTools integration

When you access the PeopleSoft Workcenter Dashboard via WebSEAL using a standard junction type, the dashboard is not displayed correctly. The browser issues a message "Only secure content is displayed" with a button "Show all content". When this button is clicked, an Oracle authentication login panel is displayed.

Note that the full URI of the server is used instead of just the junction name. Because the content contains an absolute address that WebSEAL cannot filter when a standard junction type is used, for example:

```
<DIV id="ptasjs1"> http://hostaddress/cs/path/cache  
/PT_PORTAL_UTIL_JS_MIN_1.js</DIV>
```

In this case, a virtual host junction type must be adopted to negate the limitations associated with the use of standard junction script filtering.

Tooltips display issue

Tooltips might not display if you use the keyboard (for example, the Tab key) to navigate to a field. Tooltips are displayed properly when you use a mouse to navigate to the field.

Creating PIP resource when the server connection for database and LDAP is not available returns the wrong response.

For example, when you use the following command:

```
curl -k -b whatigtot -s -S --ciphers "DES-CBC3-SHA" -X "POST" -H  
"Accept:application/json" -H "Content-Type: application/json" --data-binary  
"{\"name\": \"tldap1234\", \"description\": \"\", \"attributes\": [{\"name  
\": \"trusteer.pinpoint.csid\", \"selector\": \"wrongtestLdap\"}]\"type  
\": \"LDAP\", \"predefined\": false, \"properties\": [{\"datatype\": \"String  
\", \"readOnly\": false, \"sensitive\": false, \"value\": \"objectclass=abc  
\", \"key\": \"searchBaseDN\"}, {\"datatype\": \"String\", \"readOnly  
\": false, \"sensitive\": false, \"value\": \"cn=*\", \"key\": \"searchFilter\"},  
{\"datatype\": \"String\", \"readOnly\": false, \"sensitive\": false, \"value  
\": \"0cdebb0c-49d9-4179-a47a-52f759a4ff57\", \"key\": \"dataSource\"}]}" --  
user admin:admin -D whatigtot "https://{appliance_host}/iam/access/v8/pips/"
```

The expected response is as follows:

```
HTTP/1.1 400 Bad Request
```

But the actual response is as follows:

```
HTTP/1.1 201 Created
```

The error message "illegal character" when you modify an SSO rule is always displayed in English.

The error message "illegal character" is always displayed in English no matter which locale your browser uses.

Audit events cannot be sent to the remote syslog server if certain information is not provided.

If you choose to send the audit events to a remote machine, you must specify the correct details on the Audit Configuration page for host, port, protocol, and certificates. Otherwise, the audit events cannot be sent to the remote machine.

Attribute sources that are being used by a federation or partner is deletable.

Users can accidentally delete attribute sources that are in use by a federation or partner. Such operation causes errors to the federation. You must ensure that an attribute source is not in use before you delete it.

Federation Module: The email address name ID format requires a mapping rule

If you use an email address name ID format in a SAML 2.0 federation, you must set the type of STS Universal User attribute, whose name is "name", to:

```
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
```

You can accomplish this by using a mapping rule. Following is an example:

```
// Get the current principal name.
var principalName = stsuu.getPrincipalName();
// Set the type of principal name attribute "name" to
// "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress".
stsuu.addPrincipalAttribute(new Attribute("name",
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress", principalName));
```

Personal certificates are not included in the list of selections when you choose certificates to use for encryption or signature validation with the SAML 2.0 partner management GUI

If you use the local management interface to choose certificates to be used for encryption or signature validation, only signer certificates are available for selection. Personal certificates are not included in the list of selections. A work-around is to use the REST API for such operations.

Federation module: The RSA-OAEP key encryption algorithm is not supported with HSM keys

IBM Security Verify Access does not support decryption of SAML 2.0 messages using the RSA Optional Asymmetric Encryption Padding (RSA-OAEP) key transport algorithm with Hardware Security Module (HSM) keys. The RSA-OAEP algorithm is supported with software (non-HSM) keys. For more information on RSA-OAEP, see <http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p>.

The upgrade from Security Access Manager 8.0, 8.0.0.1, and 8.0.0.2 does not correctly migrate the authentication module policies for Security Verify Access for Mobile.

The work-around is to create the default set of authentication policies with the local management interface or REST API.

The following link creates a customized query of the live Support knowledge base for items specific to IBM® Security Verify Access, Version 10.0, and its fix packs.

[IBM Security Access Manager technical documents](#)

You can also create your own search query on the IBM Support Portal. For example:

1. Go to the IBM Support Portal:<http://www.ibm.com/support/entry/portal/support>
2. In the **Search** field, enter: Verify Access.

Identity Provider and Service Provider is not recommended to be configured as partners on the same appliance or on the same external HVDB

Identity Provider and Service Provider is not recommended to be configured as partners on the same appliance or on the same external HVDB. This might lead to several features not functioning correctly. The following problems (but not limited to) might be encountered:

- HTTP Artifact binding SAML single sign flows does not work due to key conflict in storing the messages in runtime database.
- The STS chain mapping created internally for Identity Provider and Service Provider will have identical 'issuer' and 'applies to' which can lead to unexpected behavior during runtime flow.
- Leads to database contention as the DMAP entries could be inserted or modified simultaneously by Identity provider and Service provider.

It is recommended that the Identity Provider and Service Provider that are partners reside in separate appliances configured with separate external HVDB.

Synchronization of WebSEAL data is unable to handle deleted junctions

The current WebSEAL sync functionality is designed to pick up new entries or junctions and modifications to existing entries or junctions. However, it is currently unable to detect a deleted junction or entry. This limitation applies to both configuration entries and junctions.

Local management interface (LMI) session timeouts

LMI sessions expire after the duration of time that is specified by the **Session Timeout** field on the **Administrator Settings** page. When a session timeout occurs, you are automatically logged out and any unsaved data on the current page is lost.

Save your configuration updates in the LMI regularly to avoid data loss in the event of a session timeout.

PAM Support

The Web Application Firewall capability will reach end of service on 31st December, 2022. After this date, no further updates will be made available. Customers can continue to use the capability on an as-is basis, and support will be available for general information and existing functionality only. There will be no defect support available.

Chapter 10. Security Verify Access appliance FRU/CRU documentation

Read the IBM Security Verify Access Field Replacement Unit (FRU) parts and Customer Replacement Unit (CRU) parts documentation before you replace the relevant parts.

Disk Drive Assembly Replacement Instructions

This document helps you to complete the following tasks:

- Remove a failed disk drive and replace it with a new disk drive
- Verify that the new disk drive is working correctly

Important: Before you proceed with these instructions, review the *IBM Systems Safety Notices* provided in the *IBM Media Terms and Conditions CD* that is included with your appliance model.

Note: The illustrations in this document might differ slightly from your appliance model.

Supported appliances

The instructions in this document support IBM Security Verify Access (IBM Part Number: 01LK905).

Replacing a storage drive assembly

Before you begin

You must have a replacement storage drive assembly before you remove and replace the failed assembly.

About this task

Identifying the storage drive assembly

The front panel of the appliance contains the storage drive assembly, as highlighted in yellow in the following figure:

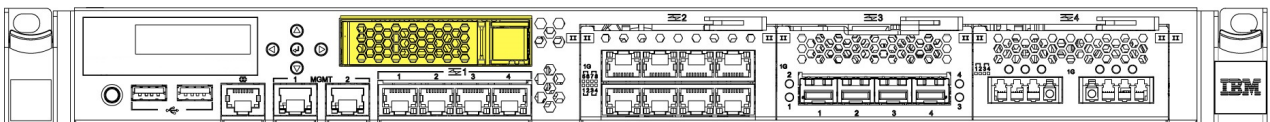


Figure 1. Location of the storage drive assembly on the front of the appliance

Procedure

1. Shut down the appliance by using the local management interface (LMI) or the command-line interface (CLI).
2. Unplug all of the power cords that are attached to the appliance.
3. Press the release button on the right side of the storage drive assembly to release the assembly lock.
4. Pull the drive handle lever to the left to pull the storage drive assembly from the drive bay, as shown in the following figure:

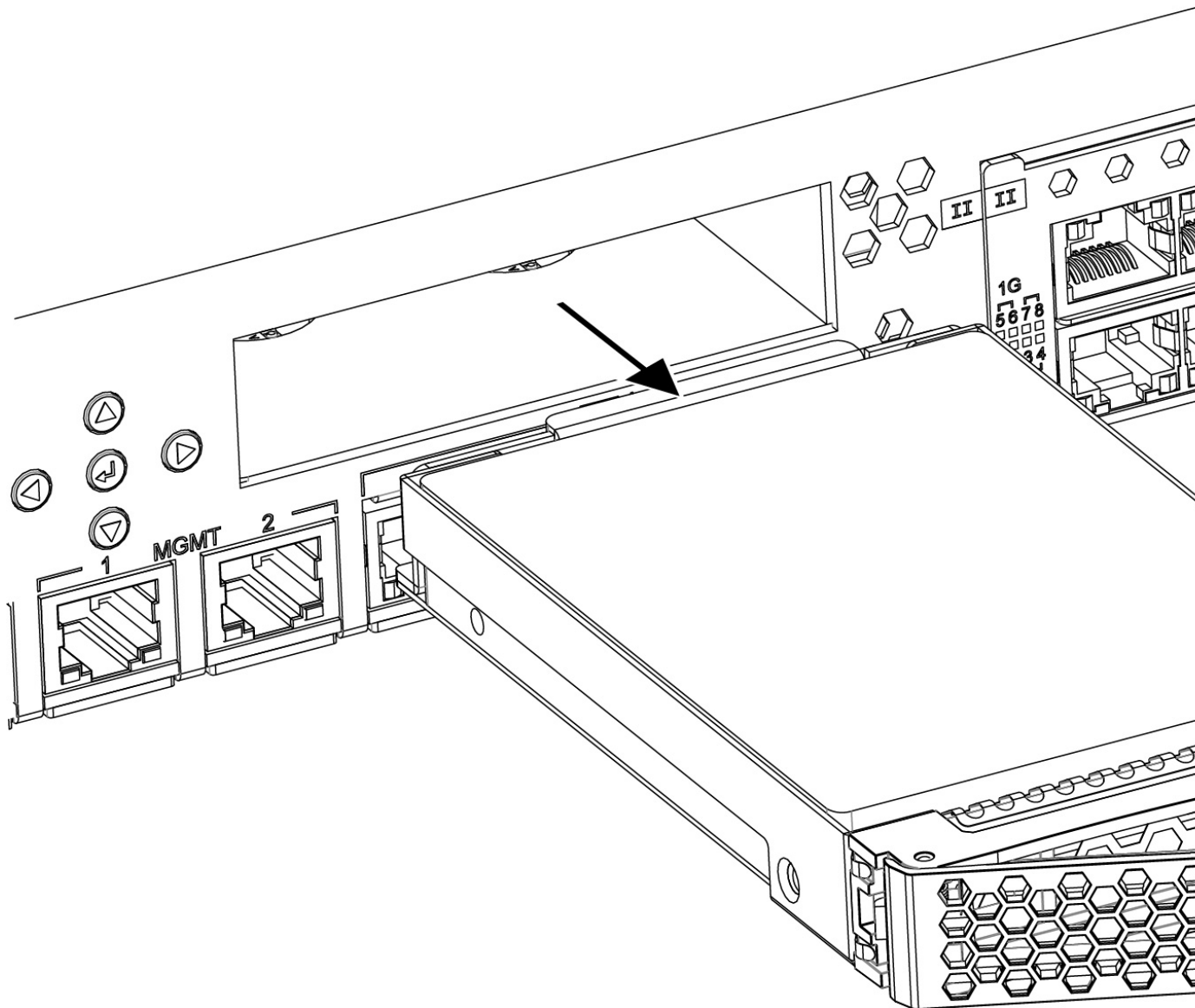


Figure 2. Removing the storage drive assembly from the drive bay

5. Place the new storage drive assembly in the drive bay.
6. Push the storage drive assembly into the drive bay until the lever locks into place.

What to do next

Turn on the appliance, and then reimage it.

Important: You must reimage the appliance after you replace the storage drive. If you do not reimage the appliance, the appliance can become inoperable.

Fan Assembly Replacement Instructions

Use these instructions to complete the following tasks:

- Remove a failed fan module from the appliance and replace it with a new one

- Verify that the new fan module is working correctly

Important: Before you proceed with these instructions, review the *IBM Systems Safety Notices* provided in the *IBM Media Terms and Conditions CD* that is included with your appliance model.

Note: The illustrations in this document might differ slightly from your appliance model.

Supported appliances

The instructions in this document support IBM Security Verify Access (IBM Part Number: 01LK905).

Replacing a fan assembly

Before you begin

You must have the applicable replacement fan assembly before you can remove and replace the failed fan assembly.

About this task

Identifying a failed fan assembly

The back panel of the appliance contains four user-accessible fan modules, as highlighted in yellow in the following figure:

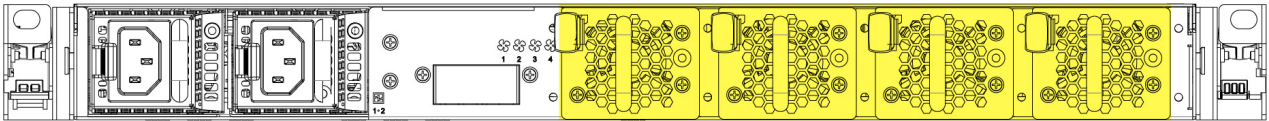


Figure 3. Location of the fan modules on the back of the appliance

During normal operation, the LED for the fan module is not illuminated. If one of the fan modules experiences a failure, the LED for the failed fan module is illuminated in amber.

Procedure

1. Pinch the orange retention clip on the fan module to release the fan assembly from the chassis.
2. Pull the fan assembly out of the chassis, as shown in the following figure:

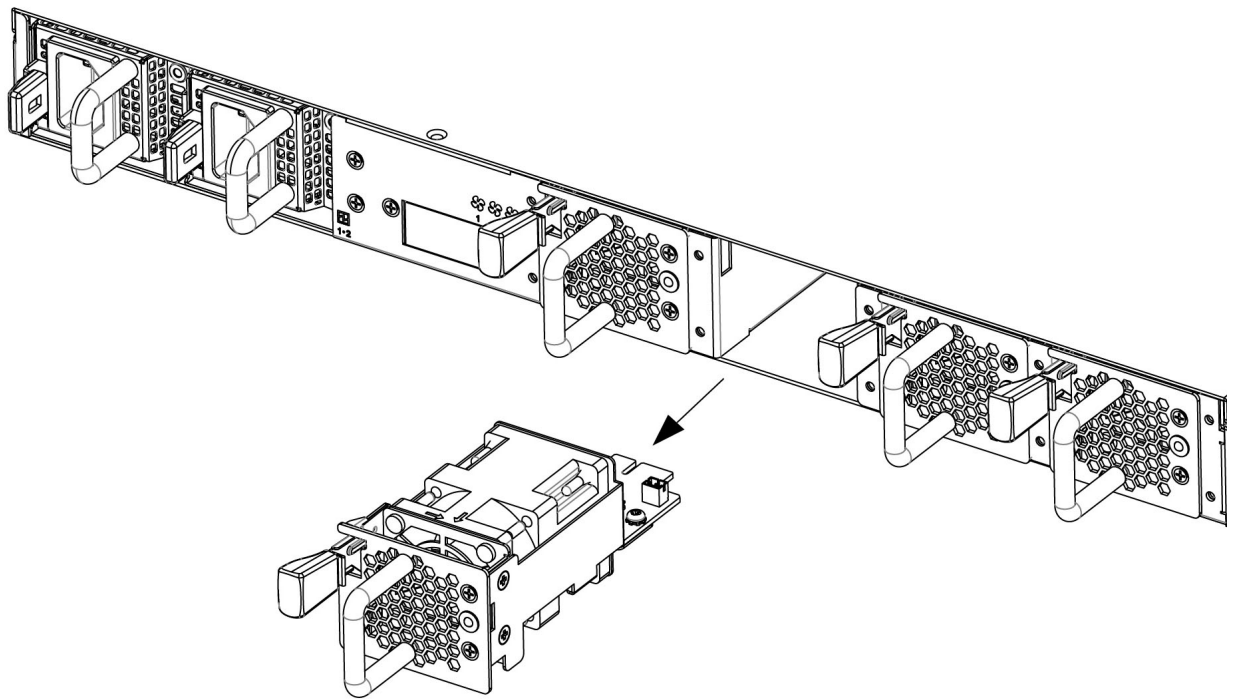


Figure 4. Removing a fan assembly from the back of the appliance

3. Slide the replacement fan assembly into the fan assembly bay. Make sure the fan assembly is secured in the chassis.

Results

The fan module LED is not illuminated in amber and the fan starts to circulate air.

Network Interface Module Replacement Instructions

This document helps you to complete the following tasks:

- Remove a failed network interface module and replace it with a new network interface module
- Verify that the replacement network interface module is working correctly

Best practice: Replace a failed network interface module as soon as possible.

Important: Before you proceed with these instructions, review the *IBM Systems Safety Notices* provided in the *IBM Media Terms and Conditions CD* that is included with your appliance model.

Note: The illustrations in this document might differ slightly from your appliance model.

Supported appliances

The instructions in this document support IBM Security Verify Access (IBM Part Number: 01LK905).

Replacing a failed network interface module

About this task

Identifying the network interface module

The front panel of the appliance contains the network interface modules, as highlighted in yellow in the following figure:

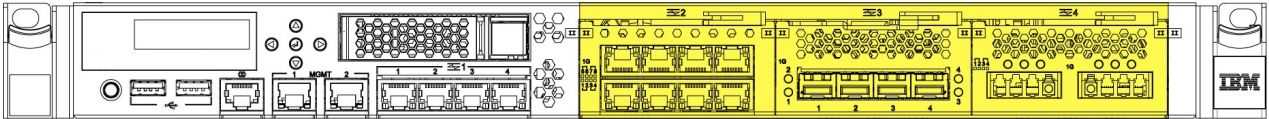


Figure 5. Location of the network interface modules on the front of the appliance

Procedure

1. Turn off the appliance by using the local management interface (LMI) or the command-line interface (CLI).
2. Unplug all of the power cords that are attached to the appliance.
3. Grasp the blue latch on the front of the appliance and pull it toward you.
4. Pull the lever on the failed module toward you, and then pull module from the chassis, as shown in the following figure:

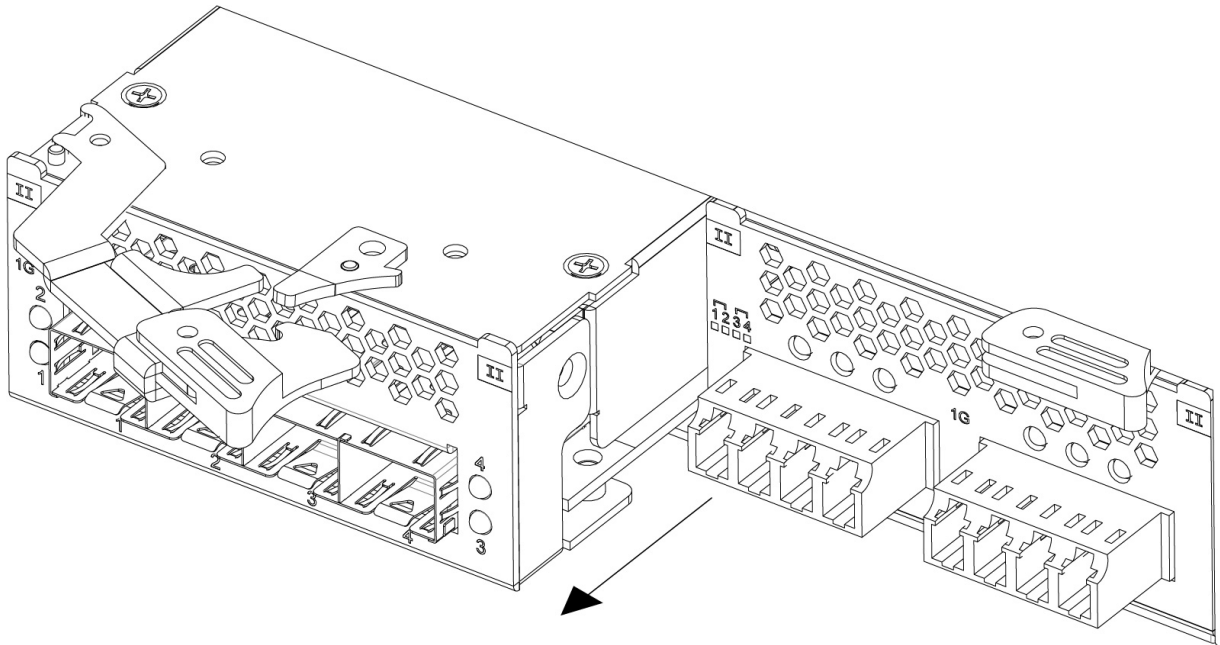


Figure 6. Removing a network interface module from the front of the appliance

5. Set aside the failed module.



Attention: As you unpack the replacement module, make sure that you do not touch the gold connectors on the back of the module, and do not let the gold connectors come in contact with the packing material. In addition, do not let these gold connectors touch the appliance while you are inserting the replacement module into the chassis. The gold connectors are extremely fragile and can be damaged if they touch anything.

6. Unpack the replacement module.
7. Carefully align the replacement module with the chassis, and then push the module into the chassis until the module is in place.
8. Push the blue latch on the front of appliance into place.
9. Plug in all of the power cords that are attached to the appliance.
10. Turn on the appliance by pressing the power button on the front.
11. Verify that the LCD panel on the front of the appliance is illuminated.

What to do next

Check whether the new module is working correctly by logging in to the appliance LMI and verifying that the new module was recognized by the appliance.

Power Supply Replacement Instructions

This document helps you to complete the following tasks:

- Identify a failed power supply
- Remove the failed power supply and replace it with a new power supply
- Verify that the replacement power supply is working correctly

Best practice: Replace a failed power supply as soon as possible.


Important: Before you proceed with these instructions, review the *IBM Systems Safety Notices* provided in the *IBM Media Terms and Conditions CD* that is included with your appliance model.

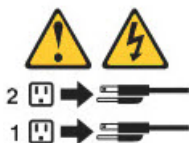
Note: The illustrations in this document might differ slightly from your appliance model.


Supported appliances

The instructions in this document support IBM Security Verify Access (IBM Part Number: 01LK905).



 **CAUTION:** The power control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all current from the device, ensure that all power cords are disconnected from the power source.



 **CAUTION:** Never remove the cover on a power supply or any part that has the following label attached.



Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

Identifying a failed power supply

The power supply unit uses an LED that indicates whether the unit is working as expected. The location of the LED is shown in the following figure:

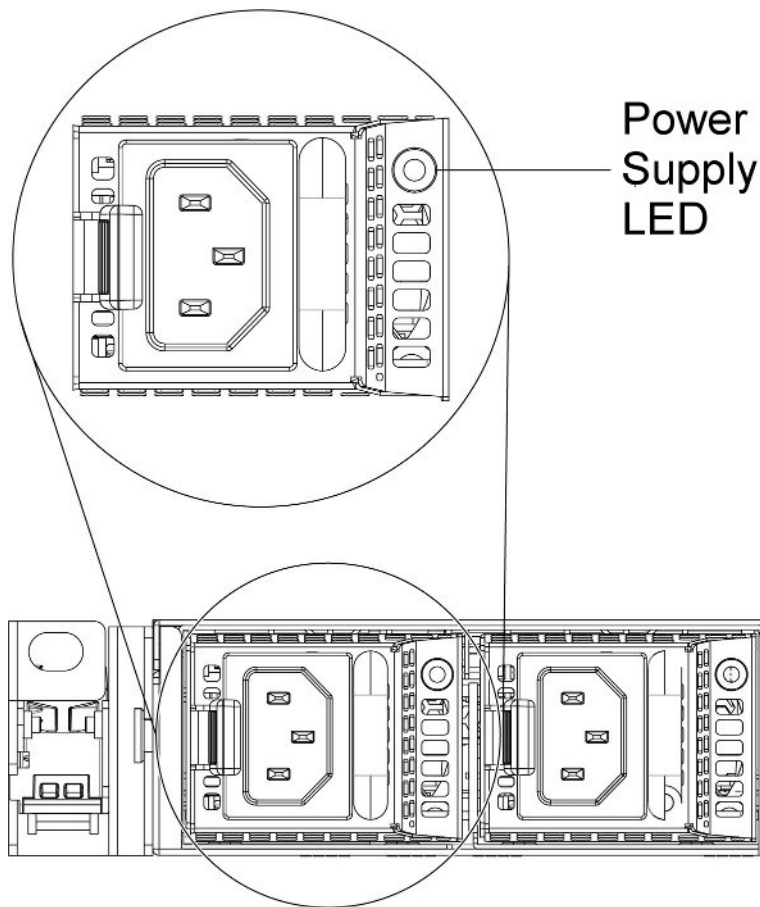


Figure 7. Power supply LED

The following table indicates the potential problems that can occur with the power supply:

<i>Table 5. Power supply LED combinations for detecting potential problems</i>	
Power supply condition	LED state
Normal work	Green
No AC power to all the power supplies	Off
AC present / Only 12VSB on (PS off) or PS in CR state	1 Hz Blink Green
AC cord unplugged with a second power supply in parallel still with AC input power	0.5 Hz Blink Green
Power supply warning events where power supply continues to operate: high temp, high power, high current, slow fan	1 Hz Blink Red
Power supply critical event causing a shutdown, failure, OCP, OVP, Fan Fail	Red

Replacing a failed power supply

Before you begin

When you replace a failed power supply, do not unplug the power supply unit that is working. This action disrupts service to the appliance.

Procedure

1. Remove the failed power supply from the power supply bay by pinching the side clip and pulling the failed power supply from the bay, as shown in Figure 2.

Important:

During normal operation, each power supply bay must contain either a power supply or a power supply blank for proper cooling.

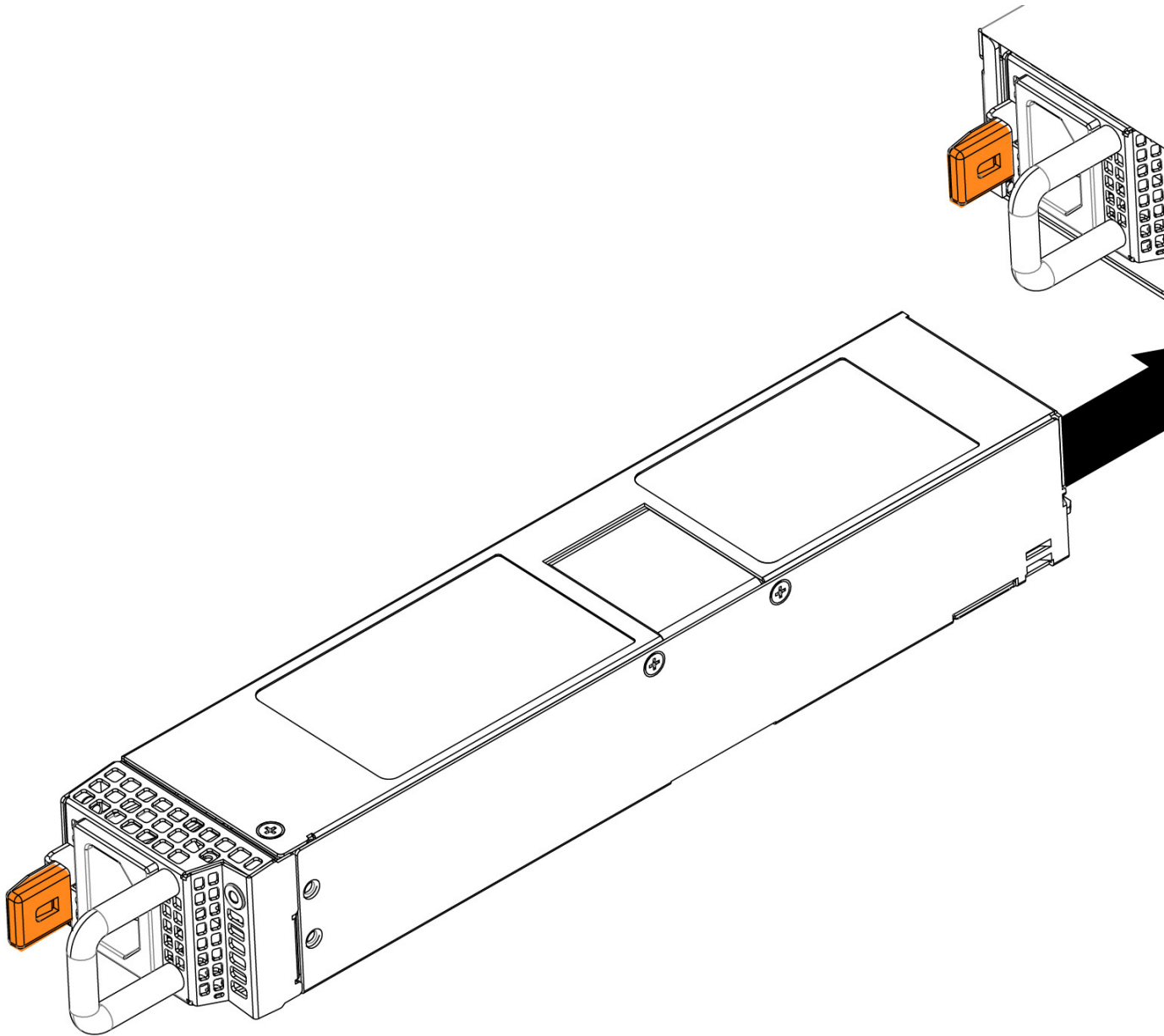
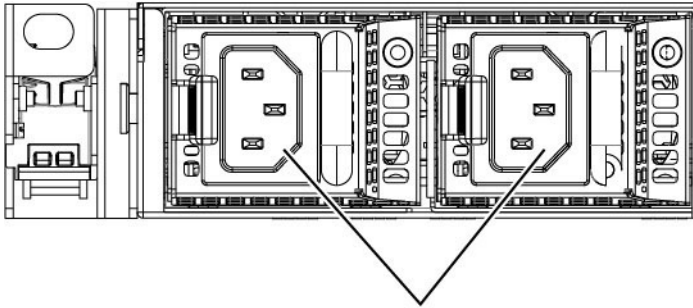


Figure 8. Removing the power supply from the back of the appliance

2. Slide the AC power supply into the bay until the retention latch clicks into place. Make sure that the power supply connects firmly to the power supply connector.
3. Connect the power cord for the new AC power supply to the power cord connector on the power supply. The AC power supply connectors on the back of the appliance are shown in the following figure:



Power cord connectors

Figure 9. Identifying the power cord connectors

4. Route the power cord through the power supply handle and through any cable clamps on the back of the appliance to prevent the power cord from being accidentally pulled out when you slide the appliance into and out of the rack.
5. Connect the power cord to a properly grounded electrical outlet.

What to do next

Make sure that the AC power LED and the DC power LED on the AC power supply are illuminated, which indicates that the power supply is operating correctly. The two power LEDs are to the left of the power cord connector.

Chapter 11. Supporting content

Use these resources to better understand the product.

IBM Security Verify Access product page

<https://www.ibm.com/products/verify-access>

IBM Security Learning Academy

<https://www.securitylearningacademy.com/local/navigator/index.php?level=iaam01>

The IBM Security YouTube Channel

<https://www.youtube.com/user/IBMSecuritySolutions>

The IBM Security Support YouTube Channel

<https://www.youtube.com/channel/UCIYjTUJjvRaolva6tiYU4Cg>

IBM Support Community Forums

<https://www.ibm.com/mysupport/s/forumshome>

IBM Security Community for Identity and Access Management (IAM)

<https://community.ibm.com/community/user/security/communities/community-home?CommunityKey=e7c36119-46d7-42f2-97a9-b44f0cc89c6d>

Chapter 12. Language support overview

IBM Security Verify Access software is translated into the following languages:

- Brazilian Portuguese
- Czech
- Chinese (Simplified)
- Chinese (Traditional)
- French
- German
- Hungarian
- Italian
- Japanese
- Korean
- Polish
- Spanish
- Russian

Note: The translations for these languages are pre-installed on the IBM Security Verify Access appliance. A language can be selected by using the **Language** drop-down list in the appliance dashboard LMI menu.

Index

A

accessibility features for this product [v](#)
APARs fixed [19](#)

D

documentation updates [23](#)

F

fixes
APARs [19](#)

G

getting started [1](#)

K

known limitations [23](#)

N

new features [3](#)

S

Security Verify Access
features [3](#)

V

Verify Access
features [3](#)

W

what's new [3](#)

