IBM Security Access Manager for Mobile
Version 8.0.0.1

Appliance Administration Guide

SC27-6206-01

IBM Security Access Manager for Mobile
Version 8.0.0.1

Appliance Administration Guide

SC27-6206-01

Note
Before using this information and the product it supports, read the information in "Notices" on page 77.

Edition notice

Note: This edition applies to version 8.0.0.1 of IBM Security Access Manager for Mobile (product number 5725-L52) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Tables

About this publication

The *IBM Security Access Manager Appliance Administration Guide* describes how to manage, configure, and deploy an existing IBM Security Access Manager environment.

Access to publications and terminology

This section provides:

- A list of publications in the "IBM Security Access Manager for Mobile library."
- Links to "Online publications."
- A link to the "IBM Terminology website."

IBM Security Access Manager for Mobile library

The following documents are available online in the IBM Security Access Manager for Mobile library:

- *IBM Security Access Manager for Mobile Configuration Guide*, SC27-6205-00
- *IBM Security Access Manager for Mobile Administration Guide*, SC27-6207-00
- *IBM Security Access Manager Appliance Administration Guide*, SC27-6206-00
- *IBM Security Access Manager for Mobile Auditing Guide*, SC27-6208-00
- *IBM Security Access Manager for Mobile Troubleshooting Guide*, GC27-6209-00
- *IBM Security Access Manager for Mobile Error Message Reference*, GC27-6210-00

Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Security IBM Security Access Manager for Mobile library
The product documentation site (http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.ammob.doc_8.0.0/welcome.html) displays the welcome page and navigation for the library.

IBM Security Systems Documentation Central
IBM Security Systems Documentation Central provides an alphabetical list of all IBM Security Systems product libraries and links to the online documentation for specific versions of each product.

IBM Publications Center
The IBM Publications Center site (http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss) offers customized search functions to help you find all the IBM publications you need.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. You can use the keyboard instead of the mouse to operate all features of the graphical user interface.

For additional information, see the IBM Accessibility website at http://www.ibm.com/able/.

Technical training

For technical training information, see the following IBM Education website at http://www.ibm.com/software/tivoli/education.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

IBM Security Access Manager for Mobile Troubleshooting Guide provides details about:

- What information to collect before contacting IBM Support.
- The various methods for contacting IBM Support.
- How to use IBM Support Assistant.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

Note: The **Community and Support** tab on the product information center can provide additional support resources.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Chapter 1. Overview

The IBM® Security Access Manager Appliance is a network appliance-based security solution that provides both access control and protection from web-based threats.

The main features of the appliance include:

- A dashboard for viewing system status such as system notifications and disk usage.
- Analysis and diagnostics tools such as event logs, memory statistics, and CPU utilization.
- Centralized management of settings such as runtime components configuration files, and SSL certificates.
- Control of system settings such as updates, licenses, and network settings.

Most of the features are configurable by using the local management interface (LMI).

Appliance format

The appliance comes in two formats: hardware appliance and virtual appliance.

The hardware appliance consists of the hardware and preinstalled IBM Security Access Manager Appliance firmware. The hardware appliance has the following machine specifications:

- Intel i7 2600 processor
- 32-GB memory
- 100-GB solid-state drive
- 6 network ports

  Note: Two of these ports are dedicated to the management of the appliance.

The virtual appliance is a Security Access Manager component. It can be hosted by the following virtual hypervisors:

- VMware ESXi version 5.0 or later
- VMware ESXi version 5.1 or later

Tips on using the appliance

These tips might be useful during the administration of the appliance.

Backup

It is important to back up your appliance frequently. To back up the appliance, use the snapshot facility that is provided by the appliance.

A *snapshot* is a copy of the state of the appliance at a certain time. By using snapshot files, you can back up your appliance and restore the appliance later. It is a good practice to take snapshots regularly and download them from the appliance

to serve as backups. However, snapshots can consume much disk space and as such it is best to clean up the old snapshots regularly.

For details about working with snapshots, see “Managing snapshots” on page 50.

Session timeouts

Save your configuration updates in the local management interface (LMI) regularly to avoid any data loss in the event of a session timeout.

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, any unsaved data on the current page is lost.

Disk space usage

The disk space in a hardware appliance is limited by the capacity of the installed hard disk. Certain files can use up a significant amount of disk space over time. Such files typically include:

Support files
: *Support files* are used by IBM support personnel to troubleshoot problems with the appliance. The support files contain all log files, temporary and intermediate files, and command output that is needed to diagnose customer support problems. The size of these files can grow large over time. To reduce the disk space that is occupied by these files, download unused support files to an external drive. Then, delete the support files from the appliance. For detailed instructions, see “Managing support files” on page 51.

Snapshot files
: *Snapshot files* record the state that the appliance is in at a certain time. They can be used to restore the appliance to a previous state. The snapshot files are stored on the appliance by default. To reduce the disk space that is used, you can download the snapshot files to an external drive and then delete them from the appliance. For detailed instructions, see “Managing snapshots” on page 50.

The administrator must monitor the remaining free disk space, and take the necessary actions to ensure that there is adequate disk space. The appliance provides a Disk Usage dashboard widget for administrators to monitor the current disk usage. For more information about managing disk space, see “Viewing disk usage” on page 17.

Chapter 2. Getting Started

Complete the following tasks that apply to your appliance format.

Hardware appliance tasks

For the hardware appliance, after you determine where to place the appliance in your network, complete the following tasks.

- Install the network cabling.
- Connect to the local management interface (LMI) or a serial console.
- Configure the initial appliance settings.

Connecting cables and starting the appliance

Connect the appliance to your network after you determine where you want to place it on the network.

Procedure

1. Connect the power cable to the appliance.
2. Connect Management Interface 1 to the network you want to use to manage the appliance.
3. Connect the network cables to the application interfaces.
4. Turn on the appliance.

Options to configure the hardware appliance

You can use either a serial console device that is connected to the appliance or the LMI to configure the hardware appliance.

The LMI is the preferable option as it offers more advanced configuration options.

To use a serial console device, you must connect the console device to the hardware appliance with a serial cable. For instructions, see "Connecting a serial console to the appliance."

To use the LMI to configure the appliance, you must browse to the IP address of the appliance. If you do not know the IP address of the appliance, follow instructions in "Determining the system IP address" on page 4.

Connecting a serial console to the appliance

You must connect a serial console to the hardware appliance before you can proceed with the configuration tasks through the command-line interface (CLI).

Procedure

1. Connect the console device to the hardware appliance with a serial cable.
2. If you use a computer as the console device, connect to the appliance with Microsoft Hyperterminal or another terminal emulation program by using the following settings:

Option	Description
Communication Port	Typically `COM1`

Option	Description
Emulation	VT100
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

3. Follow the instructions in "Common tasks" on page 6 to configure initial appliance settings.

Determining the system IP address

If you want to use the LMI to configure the appliance, use one of the following methods to determine the assigned appliance IP address so that you can access the LMI.

- **Method 1:** Use the LCD panel to determine the IP address of the appliance.
  1. Press **OK** on the LCD panel to view the main menu.

     Note: The **OK** button is labeled with an arrow.
  2. Use the arrows to select **IP Address**.
  3. Press **OK**.

     The LCD panel displays the IP address of the appliance. Take note of the address.
- **Method 2:** Use zero-configuration networking to discover the appliance on your network.

  Because the appliance uses a set of industry standard IP protocols, it can be discovered automatically when it is physically connected to your network.

Virtual appliance tasks

For the virtual appliance, connect to the local management interface or the virtual console to configure the initial appliance settings.

Setting up the virtual network

A VMWare environment must be correctly configured before the appliance installation is attempted. The administrator who is installing the appliance must be familiar with VMWare networking concepts.

The virtual appliance installation does not support scripts or a silent mode installation. To install multiple virtual appliances, you can install the first appliance manually and then use VMware ESX or vSphere to make copies of the virtual machine.

Installing the virtual appliance using VMware

Use the provided .iso image to install the virtual appliance.

Procedure

1. Create a new virtual machine with your VMware ESX or vSphere.

   Note:

- The instructions for creating a virtual machine might differ depending on your VMware ESX or vSphere version. See the VMware documentation that suits your version for specific instructions.
- Ensure that the virtual machine has enough disk space that is allocated to store the configuration and log file data for the appliance. Allocate at least 100 GB of disk space for the appliance.
- Specify **Virtual Machine Version: 7** as your virtual machine version.
- Specify **Linux** as the guest operating system and **Other 2.6x Linux (64-bit)** as the guest operating system version.
- The memory size has influence over how many WebSEAL instances can be created and how many sessions can be active at a single point in time. The minimum memory size is 4096 MB.
- The appliance needs four to six virtual network adapters. The first two network adapters serve as management interfaces. The rest of the network adapters serve as application interfaces. Four network adapters can be configured using the wizard. Additional network adapters can be added upon completion of the wizard. Each network adapter must be of the type **E1000**.)
- For SCSI controller, select **LSI Logic Parallel**.
- For Virtual Device Node, select **SCSI (0:0)**.

2. Configure the virtual machine to boot from the supplied .iso file and then start the virtual machine. The installer executes automatically.
3. Select the language to be used during the installation by entering the number that corresponds to the desired language.
4. Enter `YES` to proceed with the installation. Alternatively if you do not want to proceed with the installation, enter `NO` to move to the reboot prompt.
5. Examine the installation messages to ensure that the installation was successful. After the installation process has completed, unmount the installation media and then press the **Enter** key to reboot the appliance.
6. When the reboot operation has finished, you can start the console-based appliance setup wizard by logging on as the `admin` user with a password of `admin`. Alternatively, the Appliance Setup wizard can be accessed through the LMI.

Calculating license usage

IBM Security Access Manager for Mobile 8.0 virtual appliance is not detected by IBM License Metric Tool. To calculate license usage, create a Processor Value Unit (PVU) report

About this task

You must manually create the Processor Value Unit (PVU) report. You must determine the number and speed of the central processing units (CPUs) on the virtual machine (VM).

Procedure

1. Open the vSphere Client and connect to the IBM Security Access Manager for Mobile appliance.
   a. Supply the host name and the user name and password.
   b. Select the IBM Security Access Manager for Mobile appliance from the list of VMs.

c. Select the **Summary** tab to view the number of CPUs assigned. In the General section of the tab there is a line similar to the following entry::

```
CPU: 1 vCPU
```

d. Select the **Resource Allocation** tab to view the speed of the processors. The CPU section of the tab displays information similar to the following entry:

```
Host CPU 0 MHz ---> 2800 MHz
Consumed: 52.00 MHz
```

e. Exit the VSphere Client. Retain this information for use in the next steps.

2. Consult the following document for specific instructions on how to calculate the PVUs for the target application (the virtual appliance). See page 8 of the document:

   http://public.dhe.ibm.com/software/passportadvantage/SubCapacity/x86_Scenarios.pdf

3. Use the data that you collect to place entries in the following spreadsheet. See the instructions within the spreadsheet.

   http://public.dhe.ibm.com/software/passportadvantage/SubCapacity/Manual_Calculation_of_Virtualization_Capacity_Apr_2012.xls

4. Retain the spreadsheet and data in the event of a license compliance audit.

Common tasks

These tasks are common for both the hardware appliance and the virtual appliance.

You can choose either of the following methods to configure initial appliance settings.

- Command-line interface (CLI)
- Local management interface (LMI)

The LMI method offers more advanced configuration options.

Command-line interface initial appliance settings wizard

The initial appliance settings wizard runs the first time that an administrator logs in to the command-line interface (CLI) of an unconfigured appliance.

Navigation

You can move between screens in the wizard using the following options:

- `p`: Previous Screen
- `n`: Next Screen

To cancel the setup process at any time, use the exit command.

Modules

You must configure the following modules to set up your appliance:

Module	Description
Welcome	Describes the appliance settings that you can configure using the wizard.
Software License Agreement	Describes the appliance license agreement, IBM terms, and non-IBM terms.

Module	Description
FIPS 140-2 Mode Configuration	Enable this option to turn on compliance for NIST SP800-131a. If you enable this option, the appliance is automatically restarted before it continues on with the rest of the setup. **Note:** Enable this option only if you must comply with the NIST SP800-131a requirements. There is no advantage to enabling this option if your installation does not require it. To disable NIST SP800-131a compliance, you must reinstall the appliance.
Password Configuration	Changes your password.
Host Configuration	Changes the host name.
Management Interface Settings	Configures the management network interfaces. Displays device settings and the current working-set policy for the primary and secondary interfaces.
DNS Configuration	Configures the DNS servers that are used by the appliance.
Time Configuration	Configures the time, date, and time zone on the appliance.

Local management interface Appliance Setup wizard

The Appliance Setup wizard runs the first time that an administrator logs in to the local management interface (LMI) of an unconfigured appliance.

After you log in to the LMI for the first time, follow the Appliance Setup wizard to complete the initial configuration of the appliance. The tasks that you must complete for the initial configuration include:

- Read and accept the License Agreement.
- Download and install the license file. You must install the license to download the firmware for the hardware appliance updates.
- Depending on your requirements, choose whether to enable the FIPS option to turn on compliance for NIST SP800-131a. If you enable this option, the appliance is automatically restarted before it continues on with the rest of the setup.

  Note: Enable this option only if you must comply with the NIST SP800-131a requirements. There is no advantage to enabling this option if your installation does not require it. To disable NIST SP800-131a compliance, you must reinstall the appliance.
- Set the appliance password.
- Configure the networking, which includes the host name, management interface settings, and DNS configuration.
- Configure the application interface settings.
- Configure the date and time settings.

When you complete the basic configuration, a summary screen displays. Review the details on the completion page and click **Complete Setup**.

Chapter 3. Managing the appliance

The appliance provides three mechanisms by which it can be managed: the local management interface (LMI), the command-line interface (CLI), and web services interface.

Local management interface

The appliance offers a browser-based graphical user interface for local, single appliance management.

The following paragraphs are general notes about the usage of the local management interface (LMI). Examples of specific commands using the LMI are provided through the remainder of this document.

To log in to the LMI, type the IP address or host name of your appliance into your web browser. The following web browsers are supported:

- Windows
  - Google Chrome, version 27 or later
  - Microsoft Internet Explorer, version 9 or later
  - Mozilla Firefox, version 17 or later
- Linux/AIX®/Solaris
  - Mozilla Firefox, version 17 or later

Use the default credentials to log in to the local management interface for the first time:

- **User Name:** admin
- **Password:** admin

After you log in for the first time, use the first-time configuration pages to change your password.

To log out of the local management interface, click **Logout**.

Only one user can remain logged in to the appliance at the same time. An error occurs if you try to log in when there is an existing user session. You must displace the existing user session before you can log in with your own user session.

Note: When you close the browser window after having accessed the LMI, a session will remain active on the system. You must select the **Displace any existing sessions** check box when you log in to the LMI next time.

Command-line interface

Access the command-line interface (CLI) of the appliance by using either an ssh session or the console.

The following paragraphs are general notes about the usage of the CLI. Examples of specific commands using the CLI are provided through the remainder of this document.

The following example shows the transcript of using an ssh session to access the appliance:

```
usernameA@example.ibm.com>ssh -l admin webapp.vwasp.gc.au.ibm.com
admin@webapp.vmasp.gc.au.ibm.com's password:
Welcome to the IBM Security Access Manager Appliance
Enter "help" for a list of available commands
webapp.vwasp.gc.au.ibm.com>isam
webapp.vwasp.gc.au.ibm.com:isam> help
Current mode commands:
admin           Start an administration session which can be used to administer
                the ISAM security policy.
dscadmin        Start an administration session which can be used to administer
                the Distributed Session Cache.
logs            Work with the ISAM log files.
mga             Work with the Mobile Gateway settings.
Global commands:
back            Return to the previous command mode.
exit            Log off from the appliance.
help            Display information for using the specified command.
reboot          Reboot the appliance.
shutdown        End system operation and turn off the power.
top             Return to the top level.
```

The following example shows the options available under the **mga** menu.

```
webapp.vwasp.gc.au.ibm.com:isam> mga
webapp.vwasp.gc.au.ibm.com:mga> help
Current mode commands:
config          Start a session which can be used to configure a Web Reverse
                Proxy instance so that it can act as a point of contact for
                ISAM for Mobile.
unconfig        Start a session which can be used to unconfigure a Web Reverse
                Proxy instance so that it can no longer act as a point of
                contact for ISAM for Mobile.
Global commands:
back            Return to the previous command mode.
exit            Log off from the appliance.
help            Display information for using the specified command.
reboot          Reboot the appliance.
shutdown        End system operation and turn off the power.
top             Return to the top level.
webapp.vwasp.gc.au.ibm.com:mga>
```

The method to access the console differs between the hardware appliance and the virtual appliance:

- For the hardware appliance, a serial console device must be used. For more information about attaching a serial console device to the hardware, see "Connecting a serial console to the appliance" on page 3.
- For the virtual appliance, you can access the console by using the appropriate VMWare software.

  For example, VMWare vSphere Client.

Note: The CLI contains only a subset of the functionality available from the local management interface. The following list gives a high-level overview of the functions available from the command-line interface:

- Work with firmware images.
- Work with fix packs.
- Work with hardware settings.
- Work with licenses.
- Work with the local management interface.

- Work with management settings.
- Work with policy snapshot files.
- Work with support information files.
- Work with network diagnostic tools.
- Work with firmware and security updates.

Web service

The appliance can also be managed by sending RESTful web service requests to the appliance.

Only one user can remain logged in to the appliance at the same time. Each web service request automatically displaces any existing sessions.

The following paragraphs are general notes about the usage of the web service interface. The content and format of these web service requests are explained through the remainder of this document.

Required header for calling a web service

All web service requests must include these two headers.

Accept:application/json
The `accept` header must be present and the value must be set to `application/json`. If the header is missing, or set as a different value, the web service request fails.

BA header
Each request must contain a BA header with a valid user name and password. If this header is missing, the request fails.

The following example is the valid request format for retrieving the list of reverse proxy instances by using curl.

```
curl -k -H "Accept:application/json" --user username:password
https://{appliance_hostname}/reverseproxy
```

Note: The previous list contains only two headers that are mandatory for all web service requests. It is not an extensive list of headers that are required for all request actions. The previous example shows a curl GET request on a resource URI. This request requires only the two mandatory headers that are listed. Other HTTP methods, such as POST or PUT, require more headers. The following example is a valid request for starting a reverse proxy instance called `inst1` using curl:

```
curl -k -H "Accept:application/json" -H "Content-type:application/json"
--user username:password --data-binary '{ 'operation':'start' }'
-X PUT https://{appliance_hostname}/reverseproxy/inst1
```

Notice the additional required header **Content-type** for the PUT operation.

Other HTTP clients, such as Java, might require more headers. For required headers for RESTful web services, check the HTTP client documentation.

Web service responses

The response to a web service call is composed of two components: HTTP response code and JSON message.

The response to a successful web service request includes a 200 status code, and JSON data that contains context-specific information about the request processing. The response to an unsuccessful web service request includes an HTTP error response code, and JSON data that contains the error message.

HTTP response codes

Table 1. HTTP error response codes

Code	Description
200	Success.
400	There is a problem with the request. The JSON message describes the problem.
404	The resource that is specified in the request does not exist. The JSON message indicates which resource.
500	An internal error was encountered while the request is processed. The JSON message indicates the problem.

JSON error response format

```
{"message":"The error message"}
```

Configuration changes commit process

The LMI uses a two-stage commit process when you make changes to the appliance.

Stage 1
Changes are made by using the LMI and saved to a staging area.

Stage 2
The user explicitly deploys the changes into production.

Multiple changes can exist in a pending state at the same time. They are committed or rolled back together when a user deploys or rolls back these changes.

Any changes that affect running reverse proxy instances require a restart of the effected instances before the changes can take effect.

When an LMI session times out, any unsaved edits are lost. Save your configuration updates regularly. For more information about setting the LMI session timeout, see “Configuring administrator settings” on page 47.

Certain appliance updates require either the appliance or the web server to be restarted before the changes can take effect. When one or more of these updates are made alongside other reverse proxy updates, an additional step is required to deploy the reverse proxy updates. You must:

1. Deploy all updates.
2. Restart the appliance or the web server.
3. Deploy all remaining updates.

If there are conflicts between the pending changes and the production files, then all pending changes are automatically rolled back and the production files remain unchanged.

Web service

Deploy the pending configuration changes

URL

```
https://{appliance_hostname}/pending_changes/deploy
```

Method

```
GET
```

Parameters

N/A

Response

HTTP response code and JSON error response where applicable.

Note: For descriptions of possible error responses that can be returned from a web service call, see "Web service responses" on page 11.

Example

Request:

```
GET https://{appliance_hostname}/pending_changes/deploy
```

Response:

```
200 ok
```

Roll back the pending configuration changes

URL

```
https://{appliance_hostname}/pending_changes/forget
```

Method

```
GET
```

Parameters

N/A

Response

HTTP response code and JSON error response where applicable.

Note: For descriptions of possible error responses that can be returned from a web service call, see "Web service responses" on page 11.

Example

Request:

```
GET https://{appliance_hostname}/pending_changes/forget
```

Response:

```
200 ok
```

Retrieve the number of outstanding changes

URL

```
https://{appliance_hostname}/pending_changes/count
```

Method

```
GET
```

Parameters

N/A

Response

HTTP response code and JSON data that represents the number of pending changes.

Note: For descriptions of possible error responses that can be returned from a web service call, see "Web service responses" on page 11.

Example

Request:

```
GET https://{appliance_hostname}/pending_changes/count
```

Response:

```
{"count": 3}
```

Retrieve the list of outstanding changes

URL

```
https://{appliance_hostname}/pending_changes
```

Method

```
GET
```

Parameters

N/A

Response

HTTP response code and JSON data that represents the list of pending changes.

Note: For descriptions of possible error responses that can be returned from a web service call, see "Web service responses" on page 11.

Example

Request:

```
GET https://{appliance_hostname}/pending_changes
```

Response:

```
200 ok

[{
"id": 0,
"policy": "SSL Certificates",
"user": "admin",
"date": "2012-11-05T11:22:20+10:00"
}]
```

Note: The web service request must use the format that is described in "Required header for calling a web service" on page 11.

local management interface

When there are pending changes, a warning message is displayed at the top of the main pane. To deploy or roll back the pending changes:

1. Click the **Click here to review the changes or apply them to the system** link within the warning message.
2. In the Deploy Pending Changes page:

- To view the details of changes that are made to a particular module, click the link to that module.
- To deploy the changes, click **Deploy**.
- To abandon the changes, click **Roll Back**.
- To close the pop-up page without any actions against the changes, click **Cancel**.

Chapter 4. Home: Appliance Dashboard

The appliance provides a series of dashboard widgets in its local management interface. You can use these widgets to view commonly used system information.

These widgets are displayed right after you log in. You can also access them by clicking **Home: Appliance Dashboard** on the menu bar.

Viewing system notifications

You can view warning information about potential problems with the Notification dashboard widget.

Procedure

1. From the dashboard, locate the Notification widget. Warning messages about the following potential problems are displayed:
   - Certificates that are due to expire.
   - Reverse proxy instances that are not currently running.
   - The disk space utilization has exceeded the warning threshold.
   - The database size has reached the warning threshold, which is 80% capacity.
   - The CPU utilization has exceeded the warning threshold.
2. Take appropriate actions as required.

Viewing disk usage

You can view the disk space status and remaining disk life information with the Disk Usage dashboard widget.

Procedure

1. From the dashboard, locate the Disk Usage widget.

   Disk Space Pie Chart
   Information about used disk space and free disk space is visualized in the pie chart.

   Consumed Disk Space
   How much space (in GB) is already used.

   Note: Most of the disk space is typically used by log files and trace files. To minimize the disk footprint, set the appliance to store log and trace files on a remote server. It is also a good practice to clear unused log and trace files on a periodic basis.

   Free Disk Space
   How much space (in GB) is free.

   Total Disk Space
   How much space in total (in GB) is available to the appliance.

   Note: The disk space in a hardware appliance is limited by the capacity of the hard disk drive it carries.
2. *Optional:* Click **Refresh** to refresh the data.

Viewing IP addresses

You can view a categorized list of IP addresses that the appliance is listening on with the Interfaces dashboard widget.

Procedure

1. From the dashboard, locate the Interfaces widget. The IP addresses of all enabled and configured interfaces are displayed, along with the virtual IP addresses that are managed by the front-end load balancer.

   Management IPs
   A list of IP addresses of the management interfaces (M.1, M.2) that are enabled and configured.

   Application IPs
   A list of IP addresses of the application interfaces (P.1, P.2, P.3, P.4) that are enabled and configured.

   Load Balancer IPs
   A list of IP addresses of the load balancer services.
2. *Optional:* Click **Refresh** to refresh the data.

Viewing certificate expiry

You can view certificate details with the Certificate Expiry widget.

Procedure

1. From the dashboard, locate the Certificate Expiry widget. Details about the certificates are displayed.

   Certificate Label
   Label of the certificate.

   Expiration
   The date on which the certificate expires.

   Type Type of the certificate.

   Key Database
   Name of the key database that the certificate belongs to.
2. *Optional:* Click **Refresh** to refresh the data.

Viewing partition information

You can view information about the active and backup partitions with the Partition Information widget.

Procedure

1. From the dashboard, locate the Partition Information widget. Details about the active and backup partition are displayed.

   Firmware Version
   Version information of the appliance firmware

   Installation Date
   Date on which the appliance firmware was installed

   Installation Type
   Type of the appliance firmware installation

Last Boot
Time when the appliance was last booted

2. *Optional:* Click **Firmware Settings** to go the page to modify settings of the firmware.

Viewing network traffic

You can view network traffic for the past hour with the Network Traffic widget.

Procedure

1. From the dashboard, locate the Network Traffic widget. The **In** and **Out** traffic details for the past hour are displayed.
2. *Optional:* Click **P.1**, **P.2**, **P.3**, or **P.4** to display the details for a specific interface.

Configuring the dashboard

You can add and arrange widgets on the dashboard to monitor traffic, events, and system health in a summary view.

About this task

The appliance includes a dashboard view for a summary of your network status. You can select and arrange the information displayed on the dashboard to meet your needs.

Procedure

1. Click **Home** > **Appliance Dashboard**.
2. To rearrange the placement of the widgets, click the banner of a widget and drag it to where you want it.

   Note: Widgets snap to a grid layout on the dashboard and are automatically arranged when you move one widget to the location of another.

Chapter 5. Monitoring: Analysis and Diagnostics

You can monitor the health and statistics of the appliance.

Viewing the event log

System events are logged when the system settings are changed and when problems occur with the system. Use the Event Log management page to view system events.

Procedure

1. Click **Monitor Analysis and Diagnostics** > **Logs** > **Event Log**. The system events displayed.
2. Click **Pause Live Streaming** to stop the live updating of the event log.
3. Click **Start Live Streaming** to resume live updating of the event log.

Viewing memory statistics

View the memory graph to see the memory utilization of the appliance.

Procedure

1. Click **Monitor Analysis and Diagnostics** > **System Graphs** > **Memory**.
2. Select a **Date Range**:

Option	Description
1 Day	Displays data points for every minute during the last 24 hours.
3 Days	Displays data points for every 5 minutes during the last three days. Each data point is an average of the activity that occurred in that hour.
7 Days	Displays data points every 20 minutes during the last seven days. Each data point is an average of the activity that occurred in that hour.
30 Days	Displays data points for every hour during the last 30 days. Each data point is an average of the activity that occurred in that hour.

3. In the Legend box, select **Memory Used** to review total memory utilization.

Viewing CPU utilization

View the CPU graph to see the CPU utilization of the appliance.

Procedure

1. Click **Monitor Analysis and Diagnostics** > **System Graphs** > **CPU**.
2. Select a **Date Range**:

Option	Description
1 Day	Displays data points for every minute during the last 24 hours.
3 Days	Displays data points for every 5 minutes during the last three days. Each data point is an average of the activity that occurred in that hour.
7 Days	Displays data points every 20 minutes during the last seven days. Each data point is an average of the activity that occurred in that hour.
30 Days	Displays data points for every hour during the last 30 days. Each data point is an average of the activity that occurred in that hour.

3. In the Legend box, select the CPU utilization data that you want to review:
   - User
   - System
   - Idle

Viewing storage utilization

View the storage graph to see the percentage of disk space that is used by the boot and root partitions of the appliance.

Procedure

1. Click **Monitor Analysis and Diagnostics** > **System Graphs** > **Storage**.
2. Select a **Date Range**:

Option	Description
1 Day	Displays data points for every minute during the last 24 hours.
3 Days	Displays data points for every 5 minutes during the last three days. Each data point is an average of the activity that occurred in that hour.
7 Days	Displays data points every 20 minutes during the last seven days. Each data point is an average of the activity that occurred in that hour.
30 Days	Displays data points for every hour during the last 30 days. Each data point is an average of the activity that occurred in that hour.

3. In the Legend box, select which partitions you want to review:

   Boot The boot partition.

   Root The base file system, where the system user is root.

Viewing application interface statistics

To view the bandwidth and frames that are being used on your application interfaces, use the Application Interface Statistics management page.

Procedure

1. From the top menu, select **Monitor Analysis and Diagnostics** > **Network Graphs** > **Application Interface Statistics**.
2. In the **Date Range** field, select the period to display the statistics for.

Option	Description
1 Day	Displays data for every 20-minute interval in one day.
3 Days	Displays data for every 20-minute interval during the last three days.
7 Days	Displays data for every 20-minute interval during the last seven days.
30 Days	Displays data for every day during the last 30 days.

Viewing application log files

Use the Application Log Files management page to view and download log files that are produced by IBM Security Access Manager.

Procedure

1. From the top menu, select **Monitor Analysis and Diagnostics** > **Application Log Files**. The displayed directories contain the application log files that can be viewed and downloaded:
   - **cluster**: Contains logs files for the cluster manager.
   - **management_ui**: Contains log files for the management interface.
   - **mga**: Contains log files specific to the IBM Security Access Manager for Mobile appliance. It contains subdirectories for different categories of log files, such as **auditing**, **isamcfg**, and **runtime**.
2. Optional: Click **Refresh** to get the most up-to-date data.
3. You can then view or download the displayed log files.

   To view the log file

   a. Select the file of interest.
   b. Click **View**. The content of the log file is displayed. By default, the last 100 lines of a log file are displayed if the file is longer than 100 lines. You can define the number of lines to display by entering the number in the **Number of lines to view** field and then click **Reload**. Alternatively, you can provide a value in the **Starting from line** field to define the start of the lines. If the **Starting from line** field is set, then the **Number of lines to view** field determines how many lines to view forward from the starting line. If the **Starting from line** field is not set, then the **Number of lines to view** field determines how many lines to view from the end of the log file.

Note: The maximum size that can be returned is 214800000 lines. If a size greater than that is specified, then the maximum (214800000 lines) is returned.

c. *Optional:* Click **Export** to download the log file.

To download the log file

a. Select the file of interest.

b. Click **Download** to save the file to your local drive.

c. Confirm the save operation in the browser window that pops up.

Chapter 6. Manage: System Settings

Information about configuring Security, Network, and System settings of your appliance.

Updates and licensing

Information about managing updates and licensing on your appliance.

Viewing the update and licensing overview

The Overview page displays current information about the appliance firmware, intrusion prevention content, IP reputation database, update servers, and licenses.

Procedure

1. Click **Manage System Settings** > **Updates and Licensing** > **Overview**.
2. View the updates and licensing information. Click the links on the page to make a specific update.

Managing IP reputation database

You can set the appliance to update its IP reputation database automatically. To do this, use the Manage Application Databases management page.

About this task

The IBM X-Force team frequently publishes the latest IP reputation data. The appliance provides the function to automatically download such updates to its local IP reputation database.

Procedure

1. From the top menu, select **Manage System Settings** > **Updates and Licensing** > **Application Database Settings**.
2. Under **IP Reputation Database**, select the **Auto Update** check box.
3. *Optional:* Select the **Enable Feedback** check box to submit statistical data to IBM that can make your IP reputation classifications more accurate. This data does not include any personal or confidential information about your network.
4. *Optional:* If you want to use a proxy to access the update server, under **Proxy Settings**:
   a. Select the **Use Proxy** check box if you want to use a proxy to access the update server.
   b. For **Server Address**, enter the address of the central repository that contains the most recent IP reputation data.
   c. For **Port**, enter the port to access the central repository that contains the most recent IP reputation data.
   d. If the central repository requires authentication, select the **Use Authentication** check box and also enter the user name and password for authentication.

   Note: Server Address, **Port**, and **Use Authentication** are only required if **Use Proxy** is selected.

5. Click **Save**.

Installing updates

Install firmware and intrusion prevention updates to improve the appliance and the network protection that is provided by the appliance.

About this task

Important: After you install firmware updates, you must restart the appliance.

Firmware updates contain new program files, fixes or patches, enhancements, and online help.

Intrusion prevention updates contain the most recent security content that is provided by IBM X-Force research and development team.

Procedure

1. Click **Manage System Settings** > **Updates and Licensing** > **Available Updates**.
2. On the Available Updates page, use one or more of the following commands:

Option	Description
Upload	To manually add an update, click **Upload**. In the New Update window, click **Select Update**, browse to the update file, click **Open**, and then click **Submit**. **Note:** You can install the update after you manually add it.
Refresh	To check for updates, click **Refresh**.
Install	To install an update, select the update, and then click **Install**.

Configuring the update schedule

Configure the update schedule to receive X-Force content updates daily, weekly, or according to a specified interval of time.

About this task

A 15-minute buffer is applied to update times so that update servers do not become overburdened. Updates are downloaded up to 15 minutes before or after the time you specify.

Procedure

1. Click **Manage System Settings** > **Updates and Licensing** > **Scheduled Security Updates**.
2. In the Update Schedule pane, select **Auto Update** to receive X-Force content updates.
3. Use one of the following methods to schedule updates:
   - To receive updates on a daily basis, select **Daily or Weekly**, select **Every Day** from the first list, and then select a time from the second list.
   - To receive updates on a weekly basis, select **Daily or Weekly**, select the day of the week you would like to receive updates on, and then select a time from the second list.

- To receive updates on a schedule that ranges from 1 hour to 24 hours, select **Specified Interval**, and then select the update interval in minutes.

  Range: 60 - 1440 minutes

4. Click **Save**.

Configuring update server settings

Configure your appliance to download update files from an update server.

About this task

You can configure multiple, ordered servers for failover.

Note: You cannot delete the IBM ISS Default License and Update Server. You can disable it.

Procedure

1. Click **Manage System Settings** > **Updates and Licensing** > **Update Servers**.
2. In the Update Servers pane, take one of the following actions:
   - To add an update server, click **New**. The Add Server window is displayed.
   - To edit an update server, select the server, and then click **Edit**. The Edit Server window is displayed.
   - To delete an update server, select the server, and then click **Delete**.
3. When you add or edit an update server, configure the following options on the General tab:

Option	Description
Order	Defines the order in which update servers are queried for appliance software updates. The appliance uses the next server on the list when a server takes more than 24 hours to respond.
Enable	Enables the update server so that it can be used by the appliance.
Name	A name that describes the update server.
Server Address	The IP address or DNS name of the update server.
Port	The port number that the appliance uses to communicate with the update server. **Tip:** The port number for the IBM ISS Download Center is 443. The default port for internal update servers is 3994.

Option	Description
Trust Level	Defines how the appliance is authenticated with the update server. **Explicit (user-defined)** The appliance uses the local certificate that is pasted into the Certificate box to authenticate the connection to the update server. The certificate must be Base64 PEM-encoded data. Explicit trust is the most secure trust level. Explicit trust certificates must be Base64 PEM-encoded data. **Explicit (xpu.iss.net)** The appliance uses the local certificate for the IBM ISS update server to authenticate the connection to the update server. The IBM ISS update server certificate is installed on the appliance by default. The certificate is Base64 PEM-encoded data. Explicit trust is the most secure trust level. Explicit trust certificates must be Base64 PEM-encoded data. **First Time Trust** If a certificate is not on the appliance, the appliance downloads a certificate from the server when it connects to the server for the first time. First Time Trust is more secure than Trust All and less secure than Explicit Trust. **Note:** After the appliance downloads the certificate, it reverts to explicit-trust functionality. **Trust All** The appliance trusts the update server, and does not use SSL certificates for authentication. Trust all trust is the least secure trust level. **Attention:** The Trust All trust level presents a security risk because the internal update server can be spoofed and redirected to a fake server.

4. Optional: If you use a proxy server, configure the following settings on the Proxy Settings tab:

Option	Description
Use Proxy	Enables the appliance to use a proxy server for update servers.
Server Address	The IP address or DNS name of the proxy server. **Note:** The **Server Address** field is displayed when you select the Use Proxy check box.
Port	The port number that the proxy server uses to communicate with the update server. **Note:** The **Port** field is displayed when you select the Use Proxy check box.
Use Authentication	Enables the appliance to authenticate to a proxy server.
User Name	User name that is required for authenticating to the proxy server. **Note:** The **User Name** field is displayed when you select the Use Authentication check box.
Password	Password that is required for authenticating to the proxy server. **Note:** The **Password** field is displayed when you select the Use Authentication check box.

5. Click **Submit**.

Viewing update history

View the update history to see which firmware and security content updates are downloaded, installed, and rolled back on the appliance.

About this task

After you install an update, the update package is deleted from the appliance.

Procedure

1. Click **Manage System Settings** > **Updates and Licensing** > **Update History**.
2. To refresh the page, click **Refresh**.

Installing a fix pack

Install a fix pack when IBM Customer Support instructs you to do so.

Before you begin

The appliance does not automatically create a backup copy of a partition when you apply a fix pack to it. If you want to back up your partition before you apply the fix pack, then you must do it manually.

Restriction: You cannot uninstall fix packs.

About this task

Fix packs are applied to the current partition. If a fix pack is installed on your appliance, you can view information about who installed it, comments, patch size, and the installation date.

Procedure

1. Click **Manage**, and then click **Fix Packs**.
2. In the Fix Packs pane, click **New**.
3. In the Add Fix Pack window, click **Browse** to locate the fix pack file, and then click **Open**.
4. Click **Submit** to install the fix pack.

Installing a license

You must install a current license file to receive updates to the appliance.

About this task

Contact your IBM representative to get a license registration number. You can download and register your license from the IBM Security Systems License Key Center at https://ibmss.flexnetoperations.com.

Procedure

1. Optional: If you are not configuring your appliance for the first time, click **Manage System Settings** > **Updates and Licensing** > **Licensing and Activation**.
2. On the Licensing and Activation page, click **Select License** and locate the license file that you want to install.
3. Select the license file that you want to install and then click **Open**.
4. Click **Save Configuration**.

   Note: OCNID stands for Order Confirmation Number and ID.

Managing firmware settings

The appliance has two partitions with separate firmware on each partition. Partitions are swapped during firmware updates, so that you can roll back firmware updates.

About this task

Either partition can be active on the appliance. In the factory-installed state, partition 1 is active and contains the firmware version of the current released product. When you apply a firmware update, the update is installed on partition 2 and your policies and settings are copied from partition 1 to partition 2. The appliance restarts the system using partition 2, which is now the active partition.

Note: The appliance comes with identical firmware versions installed on both of the partitions so that you have a backup of the initial firmware configuration.

Tip: Avoid swapping partitions to restore configuration and policy settings. Use snapshots to back up and restore configuration and policy settings.

Procedure

1. Click **Manage System Settings** > **Updates and Licensing** > **Firmware Settings**.
2. On the Firmware Settings page, perform one or more of the following actions:

Option	Description
Edit	To edit the comment that is associated with a partition, select the partition and click **Edit**.
Create Backup	**Important:** Create a backup of your firmware only when you are installing a fix pack that is provided by IBM Customer Support.Fix packs are installed on the active partition and you might not be able to uninstall the fix pack. **Note:** The backup process can take several minutes to complete.
Set Active	Set a partition active when you want to use the firmware that is installed on that partition. For example, you might want to set a partition active to use firmware that does not contain a recently applied update or fix pack.

3. Click **Yes**. If you set a partition active, the appliance restarts the system using the newly activated partition.

Network Settings

Information about configuring network interfaces and information about your appliance.

Managing application interfaces

To manage application interfaces with the local management interface, use the Application Interfaces management page.

Procedure

1. From the top menu, select **Manage System Settings** > **Network Settings** > **Application Interfaces**. All current application interfaces are displayed in tabs. Each tab contains the current addresses and settings for a particular interface.
2. Select the tab of the interface that you want to work with. You can then add, edit, or delete an address on the corresponding interface tab.
   - **Add an address**
     a. Click **New**.
     b. In the Add Address page, provide details of the address to add.
        – Select the **Enabled** check box if you want this address to be enabled after creation.
        – Select **IPv4** or **IPv6** to indicate the type of address to add.
          - If **IPv4** is selected:
            1) Under **IPv4 Settings**, select either **Static** or **Auto** to indicate whether the IPv4 address is static or DHCP-assigned.

               Note: Only one address per interface can be set to auto. If an existing address is already set to auto, then the **Auto** check box is disabled.

2) *Optional*: If **Static** is selected in the previous step, you must enter the IPv4 address and subnet mask. If **Auto** is selected in the previous step, you can ignore the **Address** and **Subnet Mask** field.

- If **IPv6** is selected, enter the IPv6 **Address** and **Prefix**.

– Click **Save**.

- **Modify an address**
  – *Method 1:*
    a. Select the address to modify from the table.
    b. Click **Edit**.
    c. In the Edit Address page, modify as needed. See the "Add an address " section for descriptions of the fields.
    d. Click **Save** to save your changes.
  – *Method 2:*
    a. In the table, double-click the field to edit.
    b. Make changes inline.

    Note: Only some fields can be edited inline.
    c. Click outside the editing field to save the changes.
- **Delete an address**
  a. Select the address to delete from the table.
  b. Click **Delete**.
  c. In the Delete Address page, click **Yes** to confirm the deletion.
- **Test connection to a server**
  a. Click **Test**.
  b. On the Ping Server page, enter the IP address or name of the server to test the connection with.
  c. Click **Test**. A message is then displayed indicating whether the ping operation was successful.

Configuring management interfaces

Use the Management Interfaces page to view and manage the network security interfaces for the appliance.

About this task

Note: If you change the IP address of the management interfaces, connect your web browser to the new IP address for future sessions.

Procedure

1. Click **Manage System Settings** > **Network Settings** > **Management Interfaces**.
2. On the Management Interfaces page, type a **Host name**.
3. To enable network users to locate the appliance using zero configuration networking, select **Advertise managment interface using multicast DNS**.
4. Select the **Default Interface**.
5. To enable the other management interface, select **Enable** *interface name*.
6. Click the tab for the primary interface, and then click **IPV4** or **IPV6**.
7. Configure the following options:

Option	Description
Auto/Manual	Select **Auto** to acquire an IP address from a DHCP server. Select **Manual** to specify a static IP address, Netmask, and Gateway (IPv4) or Prefix (IPv6).
Address	If you selected **Manual** mode, type the IP address that you want to use for the interface.
Gateway	If you selected **Manual** mode, type the Gateway for the interface.
Netmask (IPv4)	If you selected **Manual** mode for IPv4, type the Subnet Mask for the interface.
Prefix (IPv6)	If you selected **Manual** mode for IPv6, type the prefix length for the interface.

8. Click the DNS tab, and then configure the following options:

Option	Description
Auto/Manual	Select **Auto** to acquire DNS server addresses from a DHCP server. Select **Manual** to specify DNS servers.
Primary DNS	Specifies the primary DNS server IP address.
Secondary DNS	Specifies the secondary DNS server IP address.
Tertiary DNS	Specifies an optional third DNS server IP address.
DNS Search Path	Specifies one or more DNS search paths. Separate each path with a comma.

9. Click the tab for the secondary interface, and then click **IPV4** or **IPV6**.
10. Configure the following options:
    - Auto/Manual
    - Address
    - Gateway
    - Netmask (IPv4)
    - Prefix (IPv6)
11. Click **Save**.

Configuring static routes

Configure static routes to the paired protection interfaces on your appliance to enable network routers to redirect users to block pages or authentication pages.

About this task

This task is only necessary for networks that contain an additional network segment between the user segment and the appliance.

Procedure

1. Click **Manage System Settings** > **Network Settings** > **Static Routes**.
2. On the Static Routes page, take one of the following actions:

- Click **New** to create a route.
- Select an existing route, and then click **Edit**.

3. Define the following information in each field:
   - Destination
   - Gateway
   - Metric
   - Interface or Segment
4. Click **Save**.

Front-end load balancer

The appliance provides front-end load balancing function to automatically assign client requests to the appropriate reverse proxy server based on the scheduling specified algorithm.

In a typical setup, there are two front-end load balancer servers and multiple reverse proxy servers. A front-end load balancer is a server that uses a virtual IP address to accept requests from a client, determines which reverse proxy server is most suitable based on the specified scheduling algorithm, and forwards the requests to the appropriate reverse proxy server. A heartbeat is transmitted between the two front-end load balancers so that the state of each front-end load balancer is known. If the primary front-end load balancer is unavailable and thus no heartbeat can be detected, the backup load balancer assumes the virtual IP address of the primary load balancer and starts accepting requests from the client.

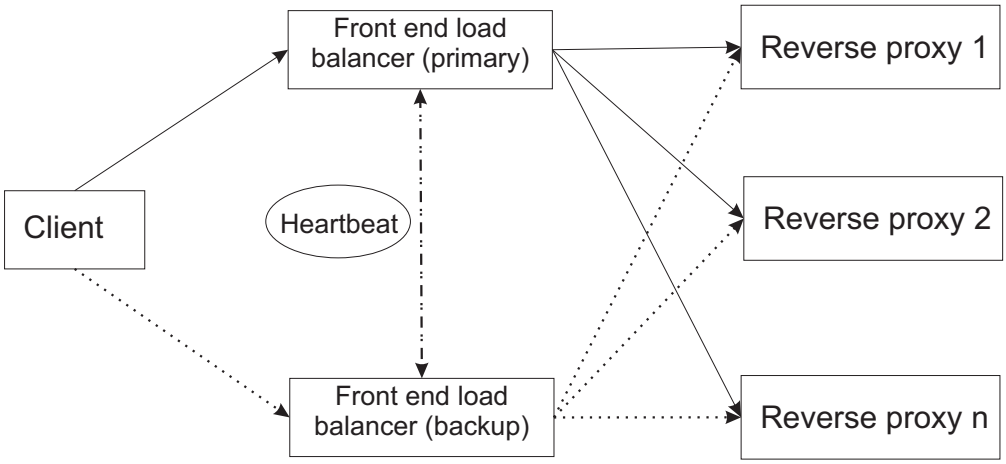

Figure 1. Front-end load balancer

Note: You can have only two front-end load balancers in your environment.

It is possible to configure the reverse proxy functionality on a machine that is also acting as a front-end load balancer. However, this might have a negative impact on the performance of the front-end load balancer. If you decide to use such setting, you must take the resource that is consumed by the reverse proxy into consideration.

Make sure that the front-end load balancer still has enough resources to perform routing effectively. In this configuration, the reverse proxy must be configured to listen on a configured application interface as well as the virtual IP address for the load-balancing environment.

Note: The back-end IP address must be set as the default gateway for load balanced servers. After you enable the front-end load balancer, ensure that each of the back-end servers set their default gateway as the value set in the back-end **Address** field.

Scheduling

The front-end load balancing function of the appliance supports several types of scheduling.

The supported scheduling types are:

lc Least connection

rr Round robin

wlc Weighted least connection

wrr Weighted round robin

lblc Locality-based least connection

dh Destination hashing

sh Source hashing

Persistence

Persistence is a mechanism that ensures a client is connected to the same reverse proxy server during a session.

The persistence functionality acts at the TCP layer (Layer 4). It can be enabled or disabled through configuration.

Persistence is controlled by the client IP address and the destination port number.

Configuring front-end load balancer

To configure the front end load balancer with the local management interface, use the Front End Load Balancer management page.

Procedure

1. From the top menu, select **Manage System Settings** > **Network Settings** > **Front End Load Balancer**.
2. *Optional:* Expand **View Diagram** to see a network diagram that helps associate the various terms that are used within the configuration panels to the corresponding location within the network.
3. On the **General** tab page:
   a. Select **Enabled** if you want to enable this front-end load balancer.
   b. Select **Debug** if you want more debug messages to be sent to the security log.
   c. Under **Gateway**:

      Note: This is the network that the load balancer and the load balanced servers communicate over.

      1) For the **Gateway Address** field, specify the IP address that connects this front-end load balancer to the private network.

         Note: The back-end address must be set as the default gateway for load balanced servers. After enabling the front-end load balancer, ensure that

each of the back-end servers set their default gateway as the value set in the back-end **Address** field that is mentioned previously.

2) For the **Mask** field, specify the network mask for the subnet that connects this front-end load balancer to the private network.

3) Select the back-end interface from the list under **Interface**.

d. *Optional:* Click **Event log** to view system events.

4. On the **Servers** tab page, you can work with virtual servers and real servers. Each virtual server corresponds to an interface (virtual IP address and port) that is load balanced. Each real server corresponds to a load balanced server.

   - **Add a virtual server**

     a. Click **New**.

     b. On the Add Virtual Server page, define settings of the virtual server to be added.

        On the **General** tab page:

Field	Description
Enabled	Specifies whether the new virtual server is active.
Name	Name of the virtual server.
Virtual Address	Specifies the IP address that connects this virtual server to the public network.
Port	Specifies the port on which this virtual server listens.
Mask	Specifies the network mask to be applied to the IP address for the virtual server.
Interface	Specifies the appliance interface on which the new virtual server connects to the public network.

        On the **Scheduler** tab page:

Field	Description
Scheduler	Specifies the scheduling algorithm for distributing jobs to the real servers. Available choices are: • Round-Robin • Weighted Round-Robin • Least-Connection • Weighted Least-Connection • Locality-Based Least-Connection • Destination Hash • Source Hash
Timeout	Specifies the time in seconds that a virtual server must be inactive before it is removed from the routing table.
Re-Entry	Specifies the time in seconds that a virtual server must be inactive before it is added back to the routing table after being previously removed because of failure.
Persistence	Specifies in seconds the time to allow a persistent virtual server connection to remain active. If the value is missing or set to 0, persistence is turned off.

     c. Click **Save**.

   - **Delete a virtual server**

     a. Select the virtual server to delete from the list.

b. Click **Delete**.
c. On the confirmation page, click **Yes**.

- **Edit a virtual server**
  - Method 1:
    a. Select the virtual server to edit from the list.
    b. Click **Edit**.
    c. On the Edit Virtual Server page, modify the settings as needed.
    d. Click **Save**.
  - Method 2:
    a. Double-click the field to edit.

    Note: All fields except **Name** can be edited inline.
    b. Make changes inline.
    c. Click outside the editing field to save the changes.
- **Manage real servers**
  a. From the list of virtual servers, select the virtual server to associate the real servers with.
  b. Click **Real Servers**. The Real Servers page is displayed.
    - To add a real server:
      1) Click **New**.
      2) On the Add Real Server page that pops up, define settings for the reverse proxy server to be added.

Field	Description
Enabled	Specifies whether the new real server is active.
Address	Specifies the IP address for the real server.
Weight	Specifies an integer that represents this processing capacity of the server relative to that of other real servers. For example, a server assigned 2000 has twice the capacity of a sever assigned 1000. The weighted scheduling algorithms adjust this number dynamically based on workload.

      3) Click **Save**.
    - To delete a real server:
      1) Select the real server to delete from the list.
      2) Click **Delete**.
      3) On the confirmation page, click **Yes**.
    - To edit a real server:
      - Method 1:
        1) Select the real server to edit from the list.
        2) Click **Edit**.
        3) On the Edit Real Server page, modify the settings as needed.
        4) Click **Save**.
      - Method 2:
        1) Double-click the field to edit.

        Note: All fields except **Address** can be edited inline.
        2) Make changes inline.

3) Click outside the editing field to save the changes.

c. Click **Close** to return to the Front End Load Balancer main page.

5. On the **High Availability** tab page, you can define the settings that enable high availability of the front-end load balancer function. For example, configure a second front-end load balancer as either a primary or a back-up load balancer for the environment.
   a. Select the **Enable High Availability** check box to enable this feature.
   b. Select **Primary** or **Backup** to designate this system as the primary or backup front-end load balancer.
   c. For the **Local Address - Primary** field, select the local IP address of the front-end load balancer.
   d. For the **Remote Address - Backup** field, specify the IP address that is used by this system to communicate with the other front-end load balancer. This field is required if a backup load balancer is in use.
   e. In the **Health Check Interval** field, specify in seconds the interval of the heartbeat messages that are sent between the primary and backup front-end load balancers.
   f. In the **Health Check Timeout** field, specify in seconds the time to wait before the system declares a non-responsive router unavailable and initiating failover.
6. Click **Save** to save all changes that are made on the Front End Load Balancer management page.

   Note: For the changes to take effect, they must be deployed as described in "Configuration changes commit process" on page 12.

Managing hosts file

To manage hosts file with the local management interface, use the Hosts File management page.

Procedure

1. From the top menu, select **Manage System Settings** > **Network Settings** > **Hosts File**. All current host records with their IP address and host names are displayed.
2. You can then work with host records and host names.
   - **Add a host record**
     a. Select the root level **Host Records** entry or do not select any entries.
     b. Click **New**.
     c. On the Create Host record page, provide IP address and host name of the host record to add.
     d. Click **Save**.
   - **Add a host name to a host record**
     a. Select the host record entry to add the host name to.
     b. Click **New**.
     c. On the Add Hostname to Host Record page, enter the host name to add.
     d. Click **Save**.
   - **Remove a host record**
     a. Select the host record entry to delete.
     b. Click **Delete**.

c. On the confirmation page, click **Yes** to confirm the deletion.

- **Remove a host name from a host record**
  a. Select host name entry to delete.
  b. Click **Delete**.
  c. On the confirmation page, click **Yes** to confirm the deletion.

  Note: If the removed host name is the only associated host name for the IP address, then the entire host record (the IP address and host name) is removed.

Managing packet tracing

To manage packet tracing with the local management interface, use the Packet Tracing management page.

Procedure

1. From the top menu, select **Manage System Settings** > **Network Settings** > **Packet Tracing**. The status of packet tracing is displayed.
2. Manage packet tracing settings.
   - **Start packet tracing**
     a. Click **Start**.
     b. On the Start Packet Tracing page:
        1) Select the interface name in the **Interface** field.

           Note: If no value is selected for the **Interface** field, packet tracing is enabled for all interfaces.
        2) Click the **Filter** field.
        3) On the Set Filter page, select a pre-defined filter in the **Display Filter** field, or enter the filter manually in the **Filter String** field.
        4) Click **Save**.
        5) Define the maximum size of the packet tracing file (PCAP file) in the **Maximum File Size** field. This value is the maximum size that the packet tracing file can grow to before packet tracing is disabled.

           Note: If no value is selected for the **Maximum File Size** field, the maximum file size is set to half the remaining disk size.
     c. Click **Start**.

     Note: Only a single packet tracing operation can be running at the same time. A new packet trace cannot be started until the PCAP file from the previous trace is deleted.
   - **Stop packet tracing**
     a. Click **Stop**.
     b. Click **Yes** to confirm the action.
   - **Export the packet tracing PCAP file**
     a. Click **Export**.

     Note: You must configure the software that blocks pop-up windows in your browser to allow pop-up windows for the appliance before files can be exported.
     b. Confirm the save action in the browser pop-up window.

- **Delete the packet tracing PCAP file**
  a. Click **Delete**.
  b. Click **Yes** to confirm the action.

  Note: If packet tracing is running, the PCAP file cannot be deleted. You must stop the associated packet tracing before you delete the PCAP file.

Managing cluster configuration

Use the Cluster Configuration management page to administer cluster support for the appliance.

About this task

You can configure multiple appliances into a cluster that shares configuration information and runtime information. One of the appliances is designated the primary master, with the option of up to three subordinate masters that are called the secondary, tertiary, and quaternary masters. The cluster services can failover between these masters. The remaining appliances serve as nodes.

By default, every appliance operates as a stand-alone cluster with only a single node. You can optionally configure a group of appliances into a cluster with multiple nodes. To create a cluster with multiple nodes, you must complete the following high-level steps. See Procedure for detailed instructions.

1. Select an appliance to be the primary master. Any appliance can be chosen as the primary master provided that it is not a member of another cluster. If the selected appliance is in another cluster, you must unregister it before you can appoint it as the primary master of a new cluster.
2. Set the value of the **Primary Master** field on the selected appliance to the IP address of the first management interface.

   Note: The default value for this field is set to `127.0.0.1` for a stand-alone cluster with a single node.
3. Save and deploy this update. The chosen appliance is now configured as the primary master of a cluster that can contain multiple nodes.
4. Export the cluster signature file on the primary master. The cluster signature file contains configuration information that cluster members can use to identify and communicate with the primary master.
5. Join appliances to the cluster by importing the cluster signature file on each appliance that you want to become a cluster member. The process of joining an appliance to the cluster is referred to as *registration*.
6. Update the cluster configuration on the primary master. As part of the cluster configuration, you can define more masters from the pool of registered nodes.

   Configuring extra masters provides failover for some of the cluster services. For more information, see “Failover in a cluster” on page 67.
7. Save and deploy the configuration changes.

   Note: As a general rule, try to limit the number of changes that are made to the cluster configuration in a single policy update.

For detailed information about clusters, see Chapter 7, “Cluster support,” on page 63.

Procedure

1. From the top menu of the local management interface (LMI), select **Manage System Settings** > **Cluster Configuration**.
2. A list of the nodes in the cluster is displayed under the **Nodes** section. Use the following operations to manage the cluster configuration.

   Note: Cluster configuration updates do not take effect until you deploy the changes through the LMI.

   Specify an appliance to be the primary master

   a. Select the **General** tab. The current cluster general configuration is displayed.
   b. To make the current node the primary master, select the **Set this appliance as the primary master** option.

      Notes:

      - This option is set on the appliance by default.
      - The corresponding **Primary Master** IP address on the appliance is `127.0.0.1` by default.
      - These initial settings indicate that by default the appliance operates as a stand-alone cluster with a single node.
      - To use this appliance as the primary master of a cluster with multiple nodes, set the **Primary Master** value to the IP address of the first management interface. See Primary Master.
      - If you do not want this appliance to be the primary master, but rather a node in an existing cluster, follow the steps in Join the current appliance to the cluster.

   View and update the current cluster general configuration

   a. Select the **General** tab. The current cluster general configuration is displayed.
   b. Edit the current settings as needed. The update operation can be performed through the primary master LMI only.

      First Port

      The first port in the range of ports that the appliance uses. The appliance uses a range of 30 ports, starting with the assigned **First Port** value.

      This field is mandatory and cannot be empty. The default value is `2020`.

      Primary Master

      The IP address of the first management interface on the primary master. This field is mandatory and cannot be empty.

      If you are configuring the appliance as a stand-alone cluster with only a single node, you can use the local IP address (`127.0.0.1`). However, to configure the appliance as a primary master for a cluster that contains multiple nodes, you must use the IP address of the first management interface.

      Notes:

1) If you change this value to the first management interface, you must save and deploy the changes before you can configure the remaining fields.
2) If you want to configure other masters, you must first join the appliances to the cluster.
3) The entries for **Primary Master**, **Secondary Master**, **Tertiary Master**, and **Quaternary Master** must be added in order. For example, a tertiary cannot be added unless a secondary exists, and a secondary cannot be removed if a tertiary exists.

Secondary Master
The IP address of the secondary master.

Master External Reference Entity
The IP address of an external reference device that the primary and secondary masters can use to check the health of the network.

Note: This field is required if both the **Primary Master** and **Secondary Master** fields are set. Otherwise, it is disabled.

Tertiary Master
The IP address of the tertiary master.

Note: You can set this field only if there is a **Secondary Master** defined. If you specify a **Tertiary Master**, you must also specify a **Quaternary Master**.

Quaternary Master
The IP address of the quaternary master.

Note: This field is mandatory if you specify a **Tertiary Master**.

Replica External Reference Entity
The IP address of an external reference device that the tertiary and quaternary masters can use to check the health of the network.

Note: This field is required if both the **Tertiary Master** and **Quaternary Master** fields are set. Otherwise, it is disabled.

c. Clicking **Save** submits all configuration changes from the General, Session Cache, and Database tabs.
d. Deploy the changes.

View and update the current cluster session cache configuration

The distributed session cache is one of the cluster services. It is used by the IBM Security Access Manager appliance to distribute session data. You must configure the distributed session cache settings for the cluster on the primary master.

a. Select the **Session Cache** tab. The distributed session cache settings for the current cluster are displayed.
b. Edit the current settings as needed. The update operation can be performed through the primary master LMI only.

Worker threads
The number of worker threads that handle the server requests. At a minimum, use a number that is greater than the maximum number of clients.

Maximum session lifetime
The maximum lifetime in seconds for each session. Use a value greater than the maximum lifetime of all clients. That is, use a value greater than the maximum **[session] timeout** value that the WebSEAL clients use.

For more information about the **[session] timeout** configuration entry, see the *IBM Security Access Manager Web Reverse Proxy Stanza Reference*.

Client grace period
The grace period in seconds that a client has available to restart and register an interest in the session again before the session is removed from the session cache. This period gives the client a chance to restart without losing the session from the server.

Use a similar value to the idle timeout value for the session on the client. That is, use a value similar to the **[session] inactive-timeout** value that is set in the client Web Reverse Proxy configuration.

For more information about the **[session] inactive-timeout** configuration entry, see the *IBM Security Access Manager Web Reverse Proxy Stanza Reference*.

Support internal clients only
Indicates that only internal clients can use the distributed session cache.

Notes:

- IBM Security Access Manager for Mobile, version 8.0 supports internal clients only.
- If this option is selected, the remaining fields are disabled.
- Clients can be turned off. For more information about failover events, search for the Options for handling session failover events topic in the *IBM Security Access Manager for Mobile Administration Guide*. For more information about configuration properties, search for the Advanced configuration properties topic in the *IBM Security Access Manager Configuration Guide*.

Support internal and external clients
Indicates that both internal and external clients can use the distributed session cache.

Note: Support for external clients is not available in IBM Security Access Manager for Mobile, version 8.0.

Port The port on which external clients can communicate with the session cache. This field is mandatory if you enable support for internal and external clients.

Enable SSL
If selected, the distributed session cache uses secure communication with its clients.

Note: If you enable SSL, you must also configure the **Keyfile**.

Keyfile
Lists the existing keyfiles on the appliance. These keyfiles are managed from the SSL certificates page. You can click the **SSL Certificates** link on the right to go to that page.

Note: If you want to share the key files across the cluster, you must go to the **SSL Certificates** page and select the **Replicate with Cluster** check box.

Label Lists the certificate labels in the selected keyfile. This field is disabled if a keyfile is not selected.

c. Clicking **Save** submits all configuration changes from the General, Session Cache, and Database tabs.

d. Deploy the changes.

View and update the current runtime database configuration

The runtime database stores runtime data. You can use the embedded runtime database or configure an external database.

a. Select the **Database** tab. The current runtime database configuration is displayed.

b. Edit the current settings as needed. The update operation can be performed through the primary master LMI only.

Note: The following error message returns in the **Database Maintenance** panel after the location of the runtime database is changed from **Local to the cluster** to **Remote to the cluster**:

```
System Error FBTRBA091E The retrieval failed because
   the resource cannot be found.
```

Complete the following steps to restart the local management interface (LMI):

1) Use an ssh session to access the LMI.
2) Log in as the administrator.
3) Type `lmi`, and press Enter.
4) Type `restart`, and press Enter.
5) Type `exit`, and press Enter.

Local to the cluster
Specifies the use of the internal runtime database.

Note: Only the **Maximum Size** field relates to the internal runtime database. If you are using the internal runtime database, all other fields are disabled.

Maximum Size (% of available disk)
The size of the internal runtime database. If you select the **Local to the cluster** option, this field is mandatory. The maximum size is expressed as a percentage of the remaining disk space at the time that the policy is applied.

The valid value range is from 10% to 80%. If a change in this value results in a calculated maximum size, which is smaller that the current size of the database, the database must be re-created. In this case, all existing data from the database will be lost.

To determine the percentage of available disk space to assign to the internal database, consider the following aspects of your environment:

- The current disk usage on the appliance. You can view the **Disk Usage** on the Appliance Dashboard in the LMI.
- Internal disk requirements for other utilities such as logging and snapshots.

Remote to the cluster
Specifies the use of an external runtime database.

Notes:

- All of the remaining fields relate to the external runtime database.
- For more information about using an external runtime database, search for "external runtime database" in the *IBM Security Access Manager for Mobile Administration guide*.

Type The database type, which is either DB2 or Solid DB.

Address
The IP address of the external database server.

Port The port on which the external database server is listening.

Username
The name of the database administrator.

Password
The password for the database administrator.

Secure
Select this check box to create a secure connection with the DB2® server.

Note: Before a secure connection can be established, you must first import the certificate for the appliance to use for communication with the DB2 server. Use the **SSL Certificates** page to import the appropriate certificate.

Database name
The name of the database instance on the external DB2 server.

c. Clicking **Save** submits all configuration changes from the General, Session Cache, and Database tabs.

d. Deploy the changes.

Export the cluster signature file from the cluster master

The signature file contains connection and security information. The file is used by a node to register itself with the cluster master server and participate in the cluster.

You can generate the cluster signature file on the primary master only.

a. On the **Overview** tab, click **Export**.

   Note: If the primary master is set to `127.0.0.1`, the cluster is a stand-alone cluster and the **Export** function is not available. If you want to export the cluster signature file, set the **Primary Master** IP address to the first management interface.

b. In the browser window that pops up, confirm the save operation to export the cluster signature file to your local drive.

   Note: Configure the browser to allow pop-up windows in order to export the files.

c. Deploy the changes.

Join the current appliance to the cluster

This process is referred to as registration. To review the registration rules, see "Cluster registration" on page 74.

This operation must be performed through the LMI of the appliance that is joining the cluster.

a. On the **Overview** tab, click **Import**.

b. In the Join Cluster window, click **Browse** to select the cluster signature file, which you exported from the primary master. See Export the cluster signature file from the cluster master.

c. Click **Join** to add the current appliance to the cluster.

d. Deploy the changes.

View the status of all nodes

On the **Overview** tab, all cluster nodes are displayed under the **Nodes** section. You can view the status of the nodes:

- The **Accessible** column indicates whether the node can be contacted.
- The **Synchronized** column indicates whether the node is running with the current cluster configuration. If this column is empty, it means that the current configuration information cannot be obtained from the primary master.
- The **Master** column indicates whether the node is a cluster master.

Remove a node from the cluster

This process is referred to as *unregistration*. This operation must be performed through the primary master LMI.

a. On the **Overview** tab, under the **Nodes** section, select the node to remove.

b. Click **Delete**.

c. Click **Yes** to confirm the operation.

   Note: To force the removal of the node even if the node cannot be reached, select the **Force** check box before you click **Yes**.

d. Deploy the changes.

Replicate settings across the cluster

You can enable the replication of the IBM Security Access Manager runtime settings and certificate database settings. This operation must be performed through the primary master LMI.

Note: After you enable the replication option, you can no longer update the IBM Security Access Manager runtime and certificate database settings from the non-primary nodes.

- To enable replication of the IBM Security Access Manager runtime settings:
  a. Click the **Runtime component** link on the **Replication** tab.
  b. Select the **Replicate with Cluster** check box.
  c. In the confirmation window, click **Yes** to confirm the operation.
- To enable replication of the certificate database settings:
  a. Click the **Certificate databases** link on the **Replication** tab.
  b. Select the **Replicate with Cluster** check box.

System settings

Information about managing system settings on your appliance.

Configuring date and time settings

Use the Date/Time Configuration page to configure the date, time, time zone, and NTP server information.

Procedure

1. Click **Manage System Settings** > **System Settings** > **Date/Time**
2. Configure the following options:

Option	Description
Time Zone	Specifies the time zone for the appliance.
Date/Time	Specifies the day, month, year, and time for the appliance.
NTP Server address	Lists the NTP (NIST Internet Time Service) servers the appliance uses. You can enter multiple NTP servers, separated by commas.

3. Click **Save**.

Configuring administrator settings

Use administrator settings to change the password you use to access the appliance and the duration of sessions in the local management interface (LMI).

Procedure

1. Click **Manage System Settings** > **System Settings** > **Administrator Settings**.
2. On the Administrator Settings page, type your current password in the **Current Password** field.
3. Type your new password in the **New Password** field.
4. Type your new password in the **New Password Confirmation** field.
5. In the **Session Timeout** field, click the arrows to select the maximum duration, in minutes, for each LMI session. Enter a positive integer value. The session duration begins when you log in. After the specified duration elapses, you are automatically logged out.

   Note: When an LMI session expires, unsaved details on the current screen are lost. Ensure that you save your configuration updates regularly.

6. Click **Save**.

Configuring management authentication

To configure management authentication with the local management interface, use the Management Authentication management page.

Procedure

1. From the top menu, select **Manage System Settings** > **System Settings** > **Management Authentication**. All current management authentication settings are displayed.
2. In the Main tab:
   - Select **Local User Database** if you want to use the local user database for authentication.
   - Select **Remote LDAP User Registry** if you want to use the remote LDAP user registry for authentication.

     Note: If a remote user registry is configured for management authentication, the local administrator user (`admin`) can continue to be referenced with the "`admin@local`" user name. You can use this as a fail safe in the event that the remote user registry is not reachable.

     a. In the LDAP tab:
        1) Specify the name of the LDAP server in the **Host name** field.
        2) Specify the port over which to communicate with the LDAP server in the **Port** field.
        3) Select the **Anonymous Bind** check box if the LDAP user registry supports anonymous bind.
        4) Specify the DN of the user that is used to bind to the registry in the **Bind DN** field.
        5) Specifies the password that is associated with the bind DN in the **Bind Password** field.

     b. In the LDAP General tab:
        1) Specify the name of the LDAP attribute that holds the supplied authentication user name of the user in the **User Attribute** field.
        2) Specify the name of the LDAP attribute that is used to hold the members of a group in the **Group Member Attribute** field.
        3) Specify the base DN that is used to house all administrative users in the **Base DN** field.
        4) Specify the DN of the group to which all administrative users belong in the **Administrative Group DN** field.

           Note: All administrative users must have permission to view the specified `admin_group_dn` group within the user registry.

     c. In the LDAP SSL tab:
        1) Select the **Enable SSL** check box to define whether SSL is used when the system communicates with the LDAP server.
        2) Select the name of the key database file in the **Key File Name** field.
        3) Select the name of the certificate to be used if client authentication is requested by the LDAP server in the **Certificate Label** field.
3. Click **Save** to save your settings.

Note: For the changes to take effect, they must be deployed.

4. *Optional*: Click **Test** to test the authentication.

   Note: If there have been changes made to the management authentication configuration that have not yet been deployed, this test will run using the undeployed configuration.

   a. In the Test Authentication window, enter the user name in the **Username** field.
   b. Enter the password in the **Password** field.
   c. Click **Test**.

   If the authentication is successful, a success message is displayed. If the authentication is not successful, an error message is displayed.

Working with management SSL certificate

In the local management interface, go to **Manage System Settings** > **System Settings** > **Management SSL Certificate**.

Viewing the details of the current management SSL certificate

To view the details of the current management SSL certificate with the local management interface, use the Management SSL Certificate page.

Procedure

1. From the top menu, select **Manage System Settings** > **Secure Settings** > **Management SSL Certificate**.
2. The details of the current management certificate are displayed.

Updating the management SSL certificate

To update the management SSL certificate with the local management interface, use the Management SSL Certificate page.

Procedure

1. From the top menu, select **Manage System Settings** > **System Settings** > **Management SSL Certificate**.
2. Select **Update**.
3. Under **Certificate File**, click **Browse**.
4. Browse to the directory that contains the certificate container file and select the file.

   Note: The certificate container file must be PKCS12 format (.p12 file) and can contain only a single certificate. You can generate this certificate on a server that hosts a certificate utility such as iKeyman. This certificate is used as the management SSL certificate.

5. Click **Open**.
6. Click **Update**. A message that indicates successful update is displayed.

   Note: For the changes to take effect, they must be deployed.

Managing advanced tuning parameters

Change the advanced tuning parameter values only under the supervision of IBM software support.

The default list of **Advanced Tuning Parameters** includes the **nist.sp800-131a.strict** parameter, which is set to false.

CAUTION:
A value of true causes you to lose access to the appliance local management interface (LMI) if your browser does not support TLS 1.2.

Managing snapshots

Use snapshots to restore prior configuration and policy settings to the appliance. Back up the appliance on a frequent basis by downloading snapshot files.

About this task

Snapshots are stored on the appliance. However, you can download snapshots to an external drive in case of system failure.

Procedure

1. Click **Manage System Settings** > **System Settings** > **Snapshots**.
2. In the Snapshots pane, use one or more of the following commands:

Option	Description
New	To create a snapshot, click **New**, type a comment that describes the snapshot, and then click **Save**.
Edit	To edit the comment for a snapshot, select the snapshot, click **Edit**, type a new comment, and then click **Save**.
Delete	To delete snapshots, select one or more snapshots, and then click **Delete**.
Apply	To apply a snapshot, select the snapshot, and then click **Apply**. **Note:** If configuration or policy versions are newer than the firmware version, the settings are rejected. If the configuration and policy versions are older than the firmware version, the settings are migrated to the current firmware version.
Download	To download a snapshot, select the snapshot, click **Download**, browse to the drive where you want to save the snapshot, and then click **Save**. **Note:** If you download multiple snapshots, the snapshots are compressed into a .zip file.
Upload	To upload snapshots, click **Upload**, browse to the snapshots you want to upload and select the snapshots. Wait for the **Comment** field of the Upload Snapshot window to be populated automatically. When the **Comment** field is populated, click **Save Configuration**. **Note:** You can upload only one snapshot at a time.
Refresh	To refresh the list of snapshots, click **Refresh**.

Managing support files

IBM Customer Support uses support files to help you troubleshoot problems with the appliance. Support files contain all log files, temporary and intermediate files, and command output that is needed to diagnose customer support problems.

About this task

Support files might contain customer-identifiable information, such as IP addresses, host names, user names, and policy files. Support files might also contain confidential information, such as passwords, certificates, and keys. The support file contents are stored as a .zip file. All files inside the support file can be inspected and censored by the customer.

Tip: You can create multiple support files to track an issue over time.

Procedure

1. Click **Manage System Settings** > **System Settings** > **Support Files**.
2. In the Support Files pane, use one or more of the following commands:

Option	Description
New	To create a support file, click **New**, type a comment that describes the support file, and then click **Save**. A new support file is created on the appliance.
Edit	To edit the comment for a support file, select the support file, click **Edit**, type a new comment, and then click **Save**.
Delete	To delete a support file, select the support file, and then click **Delete**.
Download	To download support files, select the support files, click **Download**, browse to the drive where you want to save the support files, and then click **Save**. **Note:** If you download multiple support files, the files are compressed into a .zip file.

Configuring system alerts

Configure where you want the system to send notifications about changes to system settings and problems with the system.

About this task

Available alerts include system alerts pre-defined in the system and any alert objects that you created.

Procedure

1. Click **Manage System Settings** > **System Settings** > **System Alerts**.
2. In the System Alerts pane, complete one or more of the following tasks:
   - To receive notifications for problems with the system, select one or more system alert objects from the Available Objects pane, and add them.
   - To create or edit alert objects, see these related topics to configure one or more of the following alert objects:

- "Configuring email alert objects"
- "Configuring remote syslog alert objects" on page 53
- "Configuring SNMP alert objects"

• To delete a system alert, select the alert and then click **Delete**.

Configuring SNMP alert objects

Configure SNMP alert objects to enable the system to send system alerts to an SNMP Manager.

Procedure

1. Click **Manage System Settings** > **System Settings** > **System Alerts**.
2. In the System Alerts page, take one of the following actions:
   • Click **New** > **SNMP**.
   • Select an existing object, and then click **Edit**.
3. Type a name for the alert object.
4. Select a trap version from the list.
5. In the SNMP Manager box, type the IP address, host name, or fully qualified domain name (FQDN) of the SNMP manager.

   Note: The SNMP host must be accessible to the appliance to send SNMP traps.
6. Type the port number that the SNMP manager monitors for notifications.

   Note: The default port number is 162.
7. Type a comment to describe the SNMP alert object.
8. For trap versions V1 or V2c, type the name of the community that is used to authenticate with the SNMP agent.
9. For trap version 3, configure the following options:

Option	Description
Name	Type the user name to be authenticated in the SNMP database.
Notification Type	On the **Notification Type** tab, select **Inform** or **Trap** in the **SNMP Trap Version** field.
Authentication	On the **Authentication and Privacy** tab, select **Enabled** to enable authentication, type the authentication passphrase, and then select an authentication type.
Privacy	Select **Enabled** to enable privacy, type the privacy passphrase, and then select a privacy type.

10. Click **Save**.

Configuring email alert objects

You can create email alert objects to send an email notification to specified users or to administrators when specified events occur on your network. You can also select the event parameters to include in the message so that important information about detected events is provided.

Procedure

1. Click **Manage System Settings** > **System Settings** > **System Alerts**.
2. In System Alerts page, take one of the following actions:
   - Click **New** > **Email**.
   - Select an existing object, and then click **Edit**.
3. Configure the following options:

Option	Description
Name	Specifies a meaningful name for the response. **Note:** This name displays when you select responses for events, so give the response a name that allows users to easily identify what they are selecting.
From	Specifies the email address that displays in the **From** field of the alert email.
To	Specifies the email address or group of addresses to receive the alert. **Note:** Separate individual email addresses with a comma or semicolon.
SMTP Server	Specifies the fully qualified domain name or IP address of the mail server. **Note:** The SMTP server must be accessible to the appliance to send email notifications.
SMTP Port	Specifies the custom port that is used to connect to the SMTP server. The default is 25.
Comment	Type a comment to identify the email alert object.

4. Click **Save**.

Configuring remote syslog alert objects

Configure remote syslog alert objects to enable the system to record system events in a remote log file.

Procedure

1. Click **Manage System Settings** > **System Settings** > **System Alerts**.
2. In the System Alerts page, do one of the following steps:
   - Click **New** > **Remote Syslog**.
   - Select an existing remote syslog alert object, and then click **Edit**.
3. Configure the following options:

Option	Description
Name	Specifies a meaningful name for the response.
Remote Syslog Collector	Specifies the fully qualified domain name or IP address of the host on which you want to save the log. **Note:** The host must be accessible to the appliance.

Option	Description
Remote Syslog Collector Port	Specifies the custom port that is used to connect to the syslog collector. The default is 514.
Comment	Type a comment to identify the remote syslog alert object.

4. Click **Save**.

Restarting or shutting down the appliance

Use the Restart or Shut down page to restart or shut down the appliance.

About this task

Important: When the appliance is restarting or shutting down, traffic is not passed through the appliance and your network might not be protected.

Procedure

1. Click **Manage System Settings** > **System Settings** > **Restart or Shut down**
2. Perform one of the following tasks:

Option	Description
Click Restart to restart the appliance	Restarting the appliance takes it offline for several minutes.
Click Shut down to turn off the appliance	Shutting down the appliance takes it offline and makes it inaccessible over the network until you restart it.

3. Click **Yes**.

Configuring application database settings

Configure auto updating and feedback for application databases. Application databases store classifications for web applications and web sites.

About this task

To receive updates to application and IP reputation databases, you must enable auto updating. You cannot manually update application and IP reputation databases.

Procedure

1. Click **Manage** > **System Settings** > **Updates and Licensing** > **Application Database Settings**.
2. Enable or disable the following options for updating application databases:
   - Auto Update
   - Enable Feedback

     The system classifies a URL as unknown if it is not listed in the application database. Enable the Feedback option to submit unknown URLs and statistics about web application matching to IBM. IBM will classify unknown URLs and include them in a subsequent database update.

IBM uses statistics about matched web applications and actions to continuously improve the classification quality and match ratio for web applications. Feedback data does not include any personal or confidential information about your network.

3. Enable or disable the following options for the IP reputation database:
   - Auto Update
   - Enable Feedback

     Enable the feedback option to submit statistical data to IBM that can make your IP reputation classifications more accurate. This data does not include any personal or confidential information about your network.
   - Include IP reputation info

     Enable inclusion of IP reputation information in the security events. When disabled, the appliance does not perform IP reputation lookup for security events.
4. Optional: If you use a proxy server, configure the following proxy settings:

Option	Description
Use Proxy	Enables the appliance to use a proxy server for application databases.
Server Address	The IP address or DNS name of the proxy server. **Note:** The Server Address field is displayed when you select the Use Proxy check box.
Port	The port number that the proxy server uses to communicate with the update server. **Note:** The Port field is displayed when you select the Use Proxy check box.
Use Authentication	Enables the appliance to authenticate to a proxy server.
User Name	User name required for authenticating to the proxy server. **Note:** The User Name field is displayed when you select the Use Authentication check box.
Password	Password required for authenticating to the proxy server. **Note:** The Password field is displayed when you select the Use Authentication check box.

Setting the locale of application log files

Use the Application Locale management page to set the locale in which the application log files are written.

Procedure

1. From the top menu, select **Manage System Settings** > **System Settings** > **Application Locale**.
2. Select the language that you want the application log files to be written in.
3. Click **Save**.

Secure settings

Information about managing secure settings on your appliance.

Managing SSL certificates

You can use the SSL Certificates management page to manage several types of certificate database files.

In particular, the file types in the following table are supported.

Table 2. Supported certificate file types

File Type	Description
`.kdb`	The key database file. Stores personal certificates, personal certificate requests, and signer certificates.
`.p12`	The PKCS 12 file, where PKCS stands for Public-Key Cryptography Standards. A `.p12` file contains a binary representation of a certificate, including both its public and private keys. A `.p12` file might also include more than one certificate; for example, a certificate chain. Because a `.p12` file contains a private key, it is password protected.

If there are multiple certificates in a database, the appliance uses the first certificate that is found in the supplied database.

Note: If the FIPS 140-2 mode is enabled, all certificates must be at least 2048 bits in length.

Listing current certificate database names

To list all current certificate database names with the local management interface, use the SSL Certificates management page.

Procedure

1. From the top menu, select **Manage System Settings** > **Secure Settings** > **SSL Certificates**.
2. You can view all current certificate database names and their last modified time information.

Adding description to a certificate database

To add a description to a certificate database with the local management interface, use the SSL Certificates management page.

Procedure

1. From the top menu, select **Manage System Settings** > **Secure Settings** > **SSL Certificates**.
2. Select the certificate database that you want to describe.
3. Select **Manage** > **Describe**.
4. In the Describe SSL Certificates Database window, enter the description of the certificate database.
5. Click **Save**.

   Note: For the changes to take effect, they must be deployed as described in "Configuration changes commit process" on page 12.

Creating a certificate database

To create a certificate database with the local management interface, use the SSL Certificates management page.

Procedure

1. From the top menu, select **Manage System Settings** > **Secure Settings** > **SSL Certificates**.
2. From the menu bar, click **New**.
3. On the Create SSL Certificate Database page, enter the name of the certificate database that you want to create. The name of the certificate database name must be unique.
4. Click **Save**.

   Note: For the changes to take effect, they must be deployed as described in "Configuration changes commit process" on page 12.

Importing a certificate database

To import a certificate database with the local management interface, use the SSL Certificates management page.

Procedure

1. From the top menu, select **Manage System Settings** > **Secure Settings** > **SSL Certificates**.
2. Select **Manage** > **Import**.
3. Click **Browse** under **Certificate Database File**.
4. Browse to the directory that contains the file to be imported and select the file. Click **Open**.
5. Click **Browse** under **Stash File**.
6. Browse to the directory that contains the file to be imported and select the file. Click **Open**.
7. Click **Import**. A message that indicates successful import is displayed.

   Note: For the changes to take effect, they must be deployed as described in "Configuration changes commit process" on page 12.

Exporting a certificate database

To export a certificate database with the local management interface, use the SSL Certificates management page.

Procedure

1. From the top menu, select **Manage System Settings** > **Secure Settings** > **SSL Certificates**.
2. Select the certificate database that you want to export.
3. Select **Manage** > **Export**.

   Note: You must configure the software that blocks pop-up windows in your browser to allow pop-up windows for the appliance before files can be exported.
4. Confirm the save operation when the browser prompts you to save the .zip file.

Renaming a certificate database

To rename a certificate database with the local management interface, use the SSL Certificates management page.

Procedure

1. From the top menu, select **Manage System Settings** > **Secure Settings** > **SSL Certificates**.
2. Select the certificate database that you want to rename.
3. Select **Manage** > **Rename**
4. In the Rename SSL Certificates Database window, enter the new name of the certificate database. The new name of the certificate database name must be unique.
5. Click **Save**.

   Note: For the changes to take effect, they must be deployed as described in "Configuration changes commit process" on page 12.

Deleting a certificate database

To delete a certificate database with the local management interface, you can use the SSL Certificates management page.

Procedure

1. From the top menu, select **Manage System Settings** > **Secure Settings** > **SSL Certificates**.
2. Select the certificate database that you want to delete.
3. Select **Delete**
4. In the window that pops up, click **Yes**.

   Note: For the changes to take effect, they must be deployed as described in "Configuration changes commit process" on page 12.

Replicating the certificate databases across the cluster

If your appliance is the primary master of a cluster environment, you can replicate the certificate databases across the cluster with the SSL certificate management page.

Procedure

1. From the top menu, select **Manage System Settings** > **Secure Settings** > **SSL Certificates**.
2. Click **Replicate with Cluster** to have the certificate databases automatically replicated across the cluster.

   Note: This option is available only if the current appliance is the primary master of a cluster. If this option is selected, you cannot modify the certificate databases on any appliance other than the primary master.

Managing signer certificates in a certificate database

To manage signer certificates in a certificate database, you can use the SSL Certificates management page. In particular, you can import, export, or delete signer certificates, and list all signer certificate names.

Procedure

1. From the top menu, select **Manage System Settings** > **Secure Settings** > **SSL Certificates**.
2. Select the certificate database of interest.
3. Select **Manage** > **Edit SSL Certificate Database**.
4. All signer certificate names are displayed on the **Signer Certificates** tab.

   Import a signer certificate

   a. Click **Manage** > **Import**.
   b. Click **Browse**. Then, select the signer certificate to be imported.
   c. In the **Certificate Label** field, enter what you want to label the signer certificate.
   d. Click **Import**.

      Note: For the changes to take effect, they must be deployed as described in "Configuration changes commit process" on page 12.

   View and export a signer certificate

   a. Select the signer certificate that you want to view.
   b. Click **Manage** > **View**. The content of the signer certificate is displayed in the browser.
   c. *Optional:* Click **Export**. Then, confirm the save operation in the window that pops up.

      Note: You must configure the software that blocks pop-up windows in your browser to allow pop-up windows for the appliance before files can be exported.

   Export a signer certificate

   a. Select the signer certificate that you want to export.
   b. Click **Manage** > **Export**.
   c. Confirm the save operation in the browser window that pops up.

   Delete a signer certificate

   a. Select the signer certificate that you want to delete.
   b. Click **Delete**.
   c. In the window that pops up, click **Yes**.

      Note: For the changes to take effect, they must be deployed as described in "Configuration changes commit process" on page 12.

Managing personal certificates in a certificate database

To manage personal certificates in a certificate database with the local management interface, use the SSL Certificates management page. In particular, you can import, view, export, or delete personal certificates, list all personal certificate names, and create self-signed personal certificates.

Procedure

1. From the top menu, select **Manage System Settings** > **Secure Settings** > **SSL Certificates**.
2. Select the certificate database of interest.
3. Select **Manage** > **Edit SSL Certificate Database**.

4. Click the **Personal Certificates** tab. All personal certificate names are displayed on this tab.

Import a personal certificate

a. Click **Manage** > **Import**.
b. Click **Browse**. Then, select the file that contains the personal certificate to import.
c. *Optional:* Specify the password for the file that contains the personal certificate to import.
d. Click **Import**.

Note: For the changes to take effect, they must be deployed as described in "Configuration changes commit process" on page 12.

Receive a personal certificate

Note: A personal certificate can be received only if a corresponding certificate request exists.

a. Click **Manage** > **Recieve**.
b. Click **Browse**. Then, select the personal certificate to be received.
c. Select the **Default** check box if you want to set the personal certificate as default.
d. Click **Receive**.

Note: For the changes to take effect, they must be deployed as described in "Configuration changes commit process" on page 12.

View a personal certificate

a. Select the personal certificate you want to view.
b. Click **Manage** > **View**. The content of the personal certificate is displayed in the browser.
c. *Optional:* Click **Export**. Then, confirm the save operation in the window that pops up.

Note: You must configure the software that blocks pop-up windows in your browser to allow pop-up windows for the appliance before files can be exported.

Export a personal certificate

a. Select the personal certificate that you want to export.
b. Click **Manage** > **Export**.

Note: You must configure the software that blocks pop-up windows in your browser to allow pop-up windows for the appliance before files can be exported.

c. Confirm the save operation in the browser window that pops up.

Delete a personal certificate

a. Select the personal certificate that you want to delete.
b. Click **Delete**.
c. In the window that pops up, click **Yes**.

Note: For the changes to take effect, they must be deployed as described in "Configuration changes commit process" on page 12.

Create a personal certificate (self-signed)

a. Click **New**.
b. Enter **Certificate Label**, **Certificate Distinguished Name**, **Key Size**, and **Expiration Time**. The default value for **Expiration Time** is 365 days.
c. Select the **Default** check box if you want to set this personal certificate as the default certificate.
d. Click **Save**.

Note: For the changes to take effect, they must be deployed as described in "Configuration changes commit process" on page 12.

Set a personal certificate as default

a. Select the personal certificate that you want to edit.
b. Click **Edit**.
c. Select the **Set as the Default Certificate** check box to set the personal certificate as the default certificate.
d. Click **Save**.

Note: For the changes to take effect, they must be deployed as described in "Configuration changes commit process" on page 12.

Managing certificate requests in a certificate database

To manage certificate requests in a certificate database with the local management interface, use the SSL Certificates management page. In particular, you can create, view, export, or delete certificate requests, and list all certificate request names.

Procedure

1. From the top menu, select **Manage System Settings** > **Secure Settings** > **SSL Certificates**.
2. Select the certificate database of interest.
3. Select **Manage** > **Edit SSL Certificate Database**.
4. Click the **Certificate Requests** tab. All certificate request names are displayed on this tab.

Create a certificate request

a. Click **New**.
b. Enter **Certificate Request Label**, **Certificate Request Distinguished Name**, and **Key Size**.
c. Click **Save**.

Note: For the changes to take effect, they must be deployed as described in "Configuration changes commit process" on page 12.

View and export a certificate request

a. Select the certificate request that you want to view.
b. Click **Manage** > **View**. The content of the certificate request is displayed in the browser.
c. *Optional:* Click **Export**. Then, confirm the save operation in the window that pops up.

Export a certificate request

a. Select the certificate request that you want to export.

b. Click **Manage** > **Export**. The content of the certificate request is displayed in the browser.
c. Confirm the save operation in the window that pops up.

Delete a certificate request

a. Select the certificate request that you want to delete.
b. Click **Delete**.
c. In the window that pops up, click **Yes**.

Note: For the changes to take effect, they must be deployed as described in "Configuration changes commit process" on page 12.

Managing file downloads

Use the File Downloads management page in the LMI to access files that are available for download from the appliance.

Procedure

1. From the top menu, select **Manage System Settings** > **Secure Settings** > **File Downloads**. The displayed directories contain the files that can be downloaded. There are three parent directories:
   - **mga** contains files specific to IBM Security Access Manager for Mobile.

     Note: This directory is shown only if the IBM Security Access Manager for Mobile has been activated.
   - **common** contains files that are common across Security Access Manager products.

   These parent directories might contain subdirectories for different categories of files.
2. Optional: Click **Refresh** to get the most up-to-date data.
3. Select the file of interest.
4. Click **Download** to save the file to your local drive.

   Note: You must configure the software that blocks pop-up windows in your browser to allow pop-up windows for the appliance before files can be downloaded.
5. Confirm the save operation in the browser window that pops up.

Chapter 7. Cluster support

The Security Access Manager appliance includes cluster support, which allows multiple appliances to share configuration information and runtime information to work together in a clustered environment.

For information about how to configure and administer a cluster in the LMI, see "Managing cluster configuration" on page 40.

Cluster support overview

To share configuration information between appliances and provide failover for services, you can configure your Security Access Manager appliances into clusters.

Every cluster has a *primary* master and up to three back-up masters, known as the *secondary*, *tertiary* and *quaternary* masters for high availability of cluster services.

By default, an individual appliance is configured as the primary master of a stand-alone cluster. You can configure other appliances to join the cluster as *nodes*. When an appliance is configured as a node, it can access and share the configuration information of the primary master.

Roles and services in a cluster

The nodes in a cluster share the cluster services, which include the distributed session cache, configuration database, geolocation database, and runtime database.

The IBM Security Access Manager appliance provides services that can be shared across the cluster.

You can configure more than one master appliance to provide failover for some of these services as described in "Failover in a cluster" on page 67.

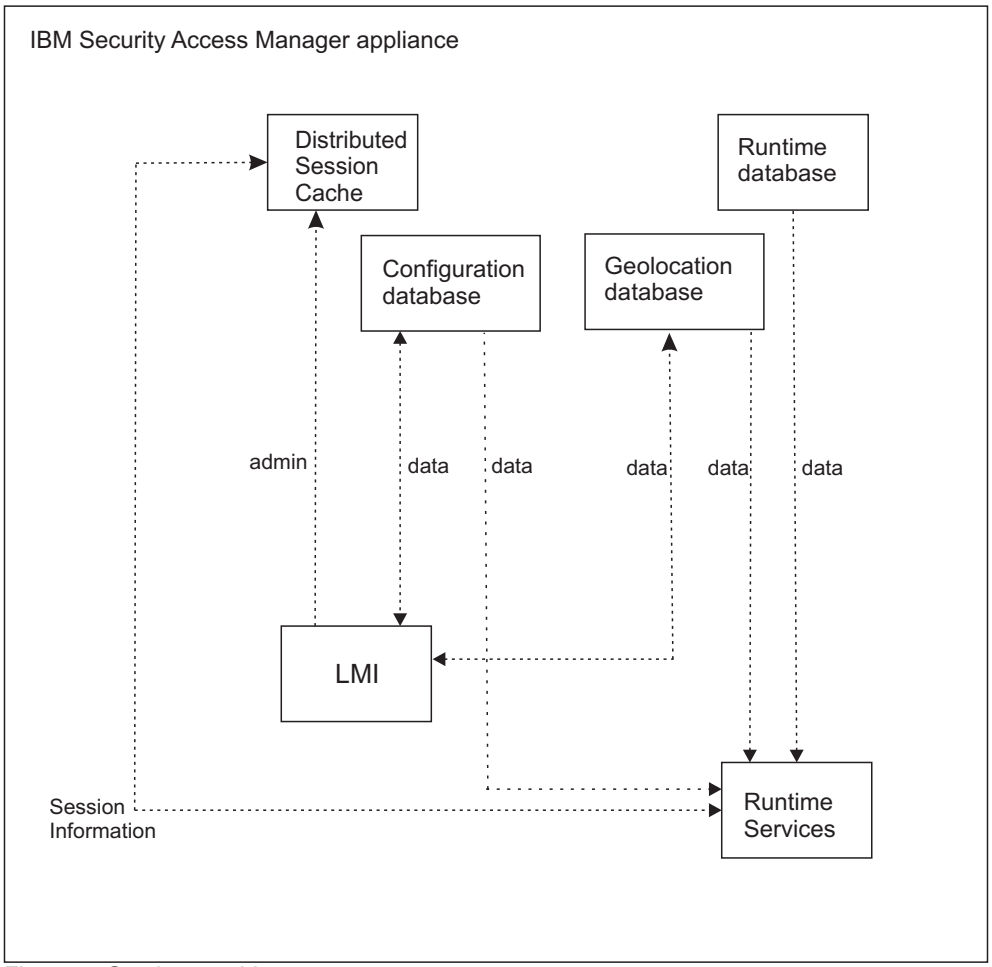

Figure 2. Services architecture

Distributed Session Cache

The distributed session cache is a central cache to hold user session information.

Configuration database

The configuration database stores configuration data that includes policy information, which is shared between the appliances in the cluster.

Note: You can update configuration data on the primary master only.

Geolocation database

The geolocation database provides geographic location information.

Runtime database

The context-based access component populates the high-volume database with runtime data. You can configure this database as an embedded database or an external database.

The embedded database is suitable for small environments only. For large-scale, production environments, configure an external database.

Data replication in a cluster

Cluster members share data that is relevant to the Security Access Manager configuration. You can update the configuration data on the primary master only. The other nodes in the cluster maintain local read-only replicas of the data from the primary master.

Any change to the cluster configuration or runtime parameters policy is automatically synchronized and applied to every node in the cluster. The Cluster Configuration management page in the LMI lists the nodes in the cluster. This list includes a **Status** column to indicate the status of the synchronization of system settings across the cluster.

If the changes to the system settings are not synchronized correctly on a particular node, the cluster administrator must investigate the problem. The administrator can examine the various log files on the node to determine why the change did not deploy successfully. When the problem is fixed, the administrator can either reboot the node, or rejoin the node to the cluster so that it applies the changes again.

Note: The **Status** column indicates whether the system settings on each node are up-to-date. This column does not indicate the status of any other synchronizations.

The data that is replicated across the cluster includes security settings, geolocation data, and system settings.

Security Settings

In an IBM Security Access Manager appliance cluster, the nodes share configuration data and runtime data that is related to the security settings.

Configuration data

- One-time password (OTP) mapping rules.
- Policy information such as risk profiles, attributes, and obligations.
- Configuration information such as user registry data.
- All of the advanced configuration data.

Geolocation data

- Data that maps ranges of IP addresses to geographic locations.

Runtime data

- Session data.
- Non-session data that is relevant to the cluster, such as one-time passwords.
- Template files.

System settings

In an IBM Security Access Manager appliance cluster, the nodes share some system settings.

Cluster configuration
The cluster configuration information is replicated across the nodes of the cluster.

Runtime tuning parameters
The advanced tuning parameters are replicated across the nodes of the cluster.

SSL certificates

By default, the key file that is used by external clients to communicate with the DSC is not automatically distributed to nodes in the cluster. However, you can choose to replicate this data by selecting the 'Replicate with Cluster' check box on the SSL certificates management page.

High availability

When you are planning the architecture of your cluster, consider the services that you use in your environment along with your failover requirements for high availability. Include an External Reference Entity (ERE) for each pair of masters in your architecture to assist in the failover process.

Topic Index:

Cluster service considerations

A cluster requires at least one master, called the primary master, which provides the cluster services. For failover purposes in a cluster with multiple nodes, you can configure up to three more masters in the environment. The required number of masters depends on which services you use and your failover requirements.

The following table depicts the valid master configurations.

Table 3. Possible architectures for clusters that contain multiple nodes

Number of masters	Combination of masters	Considerations
1	Primary master only.	No failover for cluster services.
2	Primary master and secondary master.	This configuration includes a secondary master to provide failover for the cluster services, which include the distributed session cache (DSC), configuration database, geolocation database, and runtime database.
4	Primary master, secondary master, tertiary master, and quaternary master.	You can optionally designate tertiary and quaternary masters to provide extra failover for the distributed session cache. Only the distributed session cache recognizes the tertiary and quaternary master nodes. The configuration, geolocation, and runtime databases consider these nodes as non-master nodes.

For high availability in a cross data center environment, you can consider separating the master appliances between the data centers as depicted in Figure 3 on page 67.

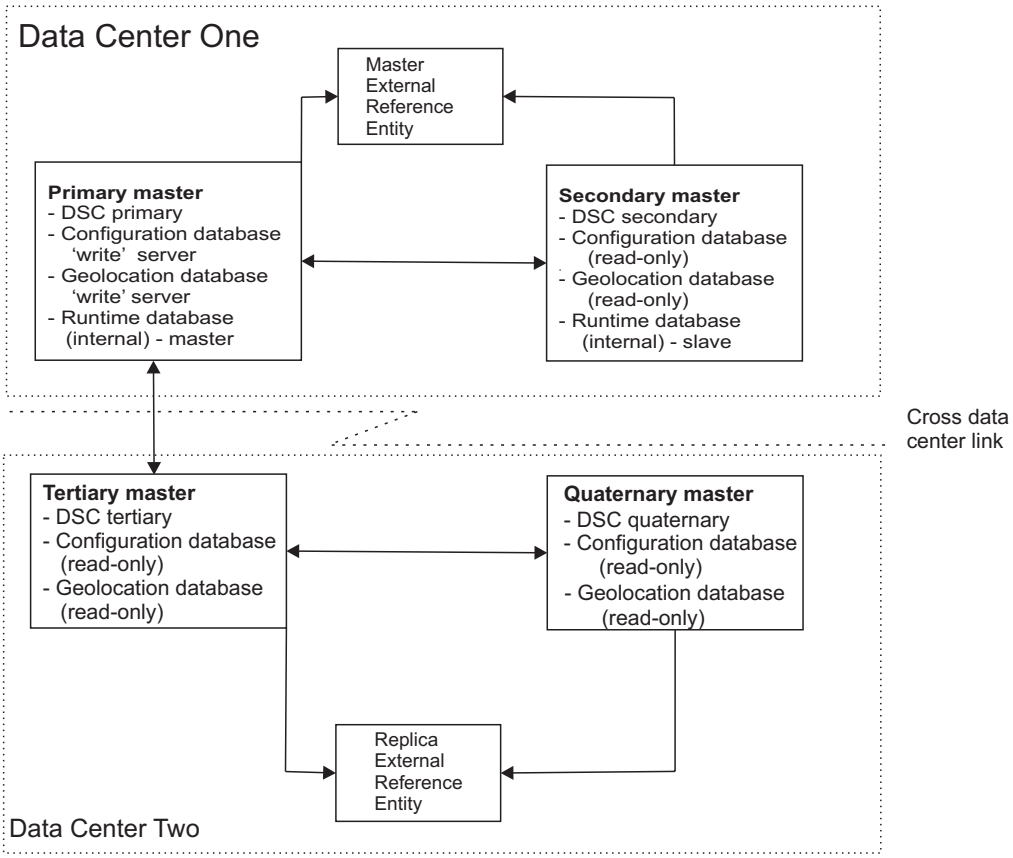

Figure 3. Example cluster architecture

This figure shows the data replication and service availability across the master nodes.

Distributed session cache

The primary master maintains the master copy of the distributed session cache and the other master nodes keep slave copies for failover purposes.

Runtime database

If you are using the internal runtime database, the primary master maintains the master copy of this data, while the secondary master keeps a slave copy for failover purposes.

If you are using an external runtime database, the cluster does not provide failover. In this case, the external database server is responsible for ensuring high availability.

Configuration and geolocation databases

The primary master is the only master on which you can update the configuration and geolocation databases. The other nodes in the cluster, including secondary, tertiary, and quaternary masters, maintain a read-only copy of the information from these databases.

Failover in a cluster

The distributed session cache, internal runtime database, geolocation database, and configuration database have varying failover capabilities in a clustered environment.

If you configure a secondary master and the primary master fails, the distributed session cache and the internal runtime database failover to the secondary master. When the primary master is restored, reconciliation occurs and the primary master resumes control of these services.

You can also configure tertiary and quaternary masters for distributed session cache failover. If the primary and secondary servers are both unavailable, the distributed session cache fails over to the tertiary master. If the tertiary master is also unavailable, the distributed session cache fails over to the quaternary master.

There is no failover between the master servers for the configuration and geolocation databases. If the primary master fails, the other nodes have a local read-only copy of the information that they can use in the interim. However, no configuration or geolocation updates are possible until the primary master is back online or a new primary master is designated.

The primary and secondary master nodes form a high availability pair. Similarly, tertiary and quaternary master nodes form a high availability pair. If one of the nodes in a pair is unavailable, then the other node keeps a record of database transactions until the offline node is restored. When the failed node is restored, it receives a log of the transactions that occurred while it was unavailable and updates its database accordingly.

For the distributed session cache, which is very active, this transaction buffering of all operations can result in considerable disk usage. To avoid consuming too much disk space, or failure if all disk space is consumed, the node must be offline for a short period only.

External Reference Entity

To prepare for failover situations, you must configure an External Reference Entity (ERE) for the paired master nodes.

When the communication link between two master nodes fails, both database servers might mistakenly assume that the other one is down. As a result, a dual primary situation can arise and you might lose transactions when databases are later synchronized. To avoid this situation, you can use a network reference device, such as a network router, as an ERE to check the health of the network.

If you configure a secondary master, you must also configure a master ERE for the primary and secondary masters. If the primary master loses its connection to the secondary master, it can contact ERE to determine whether there is a network fault or the secondary master is down. Similarly, if you are using tertiary and quaternary masters, you must configure a replica ERE for these masters to use.

In a distributed configuration, you can separate the primary and secondary masters into one data center and the tertiary and quaternary masters into another data center. If the data center link fails, the primary and tertiary masters operate in parallel and service requests in their local networks. When the data center link is restored, the tertiary master becomes inactive and reconciles its updates with the primary master.

For more information about the use of an ERE, search for the External Reference Entity topic in the IBM Solid DB Information Center:
http://pic.dhe.ibm.com/infocenter/soliddb/v7r0/topic/com.ibm.swg.im.soliddb.welcome.doc/ic-homepage.html

Cluster failure management

If a cluster member fails, you must take different administrative actions, depending on the role of the node in the cluster.

Failure of the primary master

1. Promote a different node to the primary master. For detailed steps that describe how to promote a different node, see "Promoting a node to master."

   You can promote a non-master node to the primary master so that other master nodes in the environment remain for failover purposes.

   If there is a secondary master in the environment, you can optionally promote it to primary master. The process for this promotion depends on whether there are tertiary and quaternary masters in the environment:

   - If there are tertiary and quaternary masters, you must take either of the following actions at the same time as you promote the secondary master to primary:
     - Promote a non-master node to secondary master, or
     - Demote the tertiary and quaternary nodes to non-master nodes.

     You cannot have a tertiary and quaternary master without a secondary master.
   - If you do not have tertiary and quaternary masters, you can promote the secondary master to primary master and the cluster can operate with a single master. However, for high availability purposes, you might also want to promote a non-master node to secondary master.
2. Remove the failed node from the cluster. For detailed steps, see "Removing an unreachable master node from the cluster" on page 70.

   Note: It is important to remove the failed primary master from the cluster before it is restarted. Otherwise, when it is restored, it tries to act as the primary master, resulting in a dual primary situation.
3. Export the signature file from the new master. You must use this signature file when you are adding new nodes to the cluster.

Failure of a secondary, tertiary, or quaternary master

1. Demote the failed node on the primary master.
2. Promote a non-master node to replace the failed master.

   Note: You might need to complete steps 1 and 2 simultaneously to ensure that you maintain a valid combination of master nodes. For more information about valid architectures, see "Cluster architecture rules" on page 72.
3. Remove the failed node from the cluster.

Failure of a node

1. Unregister the node on the primary master.
2. Optionally, you can add a node to the cluster to replace the failed node.

Promoting a node to master

If a master node fails, you might want to promote a different node to master while you resolve the failure.

About this task

When you are promoting a node to master, ensure that you adhere to the cluster architecture rules. For example, you must specify the supplementary masters in order. You cannot specify tertiary and quaternary masters if there is no secondary master. For a complete list of the cluster configuration rules, see "Cluster configuration rules" on page 72.

Promoting a node to a master falls into two main categories:

- Promoting a node to a supplementary master - secondary master, tertiary master, or quaternary master.
- Promoting a node to primary master.

Promoting a node to a supplementary master

Procedure

You can use the local management interface (LMI) of the primary master to update the cluster configuration and select the supplementary masters. To promote a node to secondary, tertiary, or quaternary master, complete these steps:

1. Open the Cluster Configuration page from the primary master LMI.
2. Go to the **General** tab.
3. Change the values in the master fields. That is, **Secondary master**, **Tertiary master**, **Quaternary master**.
4. Save and deploy the updates.

Promoting a node to primary master

Procedure

Use the LMI of the appliance that you are promoting to primary master to update the configuration. You can promote a non-master node or one of the supplementary masters if available. To promote the selected node to primary master, complete these steps:

1. Access LMI of the node that you want to promote to primary master.
2. Select **Manage System Settings** > **Network Settings** > **Cluster Configuration**.
3. Select the **General** tab.
4. Select **Set this appliance as a Primary Master**.
5. Use the available menu to set the Primary master IP address. Select the first management interface of the appliance.
6. Save and deploy the changes.
7. If the original primary master is unavailable when you complete this change, it is important to remove the failed primary master from the cluster before it is restarted. Otherwise, when it is restored, it tries to act as the primary master, resulting in a dual primary situation.

   For more information, see "Removing an unreachable master node from the cluster."

Removing an unreachable master node from the cluster

If a master node is unreachable, you can demote it from master and then remove it from the cluster to resolve the failure. When the node is restored, you can register it with the cluster again as a non-master node.

About this task

A node can become unavailable for a number of reasons. For example, network outages or hard disk failure. If a master node becomes unavailable, promote a new node to take its place as master. See "Promoting a node to master" on page 69.

Before the failed master can be reinstated in the network and ultimately returned to the cluster, you must then complete the following high-level steps:

- Remove the node that is unreachable from the cluster.
- Change the node to a stand-alone cluster with only a single node and troubleshoot the failure.
- Join the restored node to the cluster as a non-master node.

Procedure

To remove the failed node from the cluster, complete the following steps in the local management interface (LMI) of the new primary master:

1. Go to the **Overview** tab on the Cluster Configuration page.
2. Under the Nodes section, select the node to remove.
3. Click **Delete**.
4. Select the **Force** check box to force the removal of the node even if the node cannot be reached.
5. Click **Yes** to confirm the operation.
6. Deploy the changes.

After you remove the failed node from the cluster, you might want to restart it and ultimately restore it as a cluster member. In this case, you must complete some additional steps. While the node is disconnected from the network, change it to a stand-alone cluster with only a single node, as described in the following steps.

Note: It is important to remove the failed primary master from the cluster before it is restarted. Otherwise, when it is restored, it tries to act as the primary master, resulting in a dual primary situation.

7. Restore the node and use its LMI to access the Cluster Configuration page.
8. Go to **General** tab.
9. Change the **Primary master** IP address to `127.0.0.1`.
10. Save and deploy the change.
11. Troubleshoot the original failure and resolve any problems.

You can now join the restored appliance back in to the original cluster. This process joins the restored node to the cluster as a non-master node:

12. In the LMI of the restored appliance, go to the **Overview** tab on the Cluster Configuration page.
13. Click **Import**.
14. In the Join Cluster window, click **Browse** to select the cluster signature file of the new primary master.

    Note: You can generate the cluster signature file by using the LMI of the new primary master and selecting the **Export** option in the **Overview** tab.
15. Click **Join** to add the current appliance to the cluster.
16. Deploy the changes.

Cluster maintenance

Firmware updates in a cluster

You must apply firmware updates to the masters in order of priority before you install updates on the remaining nodes.

Upgrade the cluster members in the following order as applicable to your environment:

1. Primary master
2. Secondary master
3. Tertiary master
4. Quaternary master
5. Other nodes

Back up procedures

In a clustered environment, you cannot use VMWare snapshots to back up your virtual machines. For reliable backups, use appliance snapshots to back up the cluster.

You can complete an appliance snapshot on each cluster member to effectively back up the cluster. An appliance snapshot of the primary master includes all of the cluster configuration and runtime data. When the primary master is restored from an appliance snapshot, it updates every cluster member with the restored configuration.

An appliance snapshot of a node other than the primary master excludes the runtime database information. When a cluster member is restored from a snapshot, it contacts the primary master to obtain up-to-date configuration and runtime information.

To effectively back up the cluster, complete an appliance snapshot of the primary master after any change to the cluster configuration. For example, take a snapshot after you add or remove a node to ensure that the correct nodes are included in the cluster after a restore.

Cluster configuration rules

When you are configuring a cluster of Security Access Manager appliances, consider the following rules that govern cluster configuration.

General notes:

- Try to limit the number of changes that are made to the cluster configuration in a single policy update.
- After you save the policy changes, you must deploy the updates for the changes to take effect.

Cluster architecture rules

The architecture of a cluster, including the appointment of masters, is governed by numerous rules.

- A node must be a registered member of the cluster before it can be promoted to a master. The only exception is the primary master when there are no other nodes in the cluster.

- At a minimum, you must specify a primary master for the cluster.
- Activate the product on the primary master of the cluster while it is a stand-alone cluster with only a single node. That is, you must activate the product on the primary master before you add any nodes to the cluster.
- Before an appliance joins the cluster, ensure that you activate your products on the selected appliance.

  For more information about registration rules, see "Cluster registration" on page 74.
- You cannot specify a master without first specifying each of the prior masters. For example, you must specify the secondary master before you can specify a tertiary master.
- You cannot specify a tertiary master without also specifying a quaternary master.
- If you specify a secondary master, you must also specify the master external reference entity (ERE).
- If you specify a quaternary master, you must also specify the replica ERE.
- You can modify the cluster policy on the primary master only, unless you are promoting a local node to primary master in a disaster recovery situation.

  Note: If the primary master is unavailable when this policy change is made, it is not aware of the newly appointed primary master.

  When it restarts, the original primary master attempts to resume responsibility as the primary master and reset the cluster configuration to the last known state before it failed. That is, the primary master that was promoted during disaster recovery is demoted back to its original role in the cluster.

  To avoid this situation and retain the new primary master, you can use either of the following approaches:
  - Reinstall and then configure the failed primary master.
  - Reconfigure the failed primary master while it is isolated from the rest of the network.

  After this reconfiguration, the old primary can join the cluster again.

Cluster node availability

If a node is unavailable when you update the cluster configuration, it contacts the primary master to get the updated configuration information when it comes back online. If the primary master is offline at the same time as the secondary master, the primary master comes back online with read-only databases until the secondary master is available.

A node can become unavailable for a number of reasons, including a shutdown request, system failure, or networking failure. If a cluster node is not available during a cluster configuration change, it contacts the primary master for up-to-date information when it restarts. There might be a slight delay where the restored node tries to use the old policy and configuration information before it retrieves the missed updates.

The relationship between the primary and secondary nodes can be temporarily affected if both nodes are shut down simultaneously, and only one is powered back up. Until the other node is up, the databases on the newly powered up node are in read-only mode. When you power up the other node, the databases on the primary node become writable.

You can then shut down the secondary node without affecting the write capability on the primary server. It is only if both master nodes are offline at the same time that the restored primary master becomes read-only until the secondary master is back online.

This situation can be serious if the secondary node fails and the primary node stops for any reason. In this case, the primary node is not writable when it restarts until a secondary node is either started, or removed from the cluster. If the secondary node is removed, the primary master can operate as a single master in the cluster. You must address a failed primary or secondary master as soon as possible to avoid this situation.

Note: Due to a limitation in the underlying database technology, if the primary master fails, the tertiary and quaternary servers are unable to failover to the secondary master. In this situation, the tertiary and quaternary masters operate as if both the primary and the secondary masters are unavailable until the primary master is restored. This limitation affects the distributed session cache only.

First management interface

In a clustered environment, the IP address of the first management interface is used as the node identifier. For this reason, a static IP address must be assigned to the first management interface of the appliance.

When you change the first management interface of a non-master node, the cluster is updated automatically.

You cannot change the IP address of the first management interface on a master. If you want to change the first management interface on a master node, you must first demote the node from master. You can then promote the node to master again and update any external client references in the distributed session cache.

Cluster registration

Before you register or unregister a node in a cluster, consider these registration rules.

- You must activate your products on the primary master before you register any nodes with the cluster.
- Before you join an appliance to the cluster, ensure that you activate your products on the appliance.

  For more information about the activation process, search for 'Activating the product' in the *IBM Security Access Manager for Mobile Configuration guide*. This documentation is available in the product Information Center at http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.ammob.doc_8.0.0/welcome.html.
- A node cannot be registered with a cluster if it is already a member of another cluster. In this situation, the node must first be unregistered from its current cluster.
- Node registration must occur directly through the LMI of the appliance that you want to join the cluster. The appliance that you are registering must be able to communicate with the primary master.
- Node unregistration must occur on the primary master.
- A node cannot be unregistered if it is configured as a master. You must first demote the node from master and promote another node as the master.

Data loss considerations

The cluster services might lose data under certain circumstances.

Distributed session cache

- The policy data, which is used to indicate the first port that is available for use by the cluster, is changed.
- The policy data that defines the masters is changed.
- The external reference entity policy data is changed.

Configuration database

An appliance that is operating as a single node cluster fails. In this situation, you must rely on snapshot information to restore the configuration database.

Internal runtime database

- An appliance that is operating as a single node cluster fails. In this situation, there is no recovery possible.
- The primary master fails, and no secondary master is configured.
- The maximum size of the internal runtime database is adjusted such that the new maximum size is smaller than the existing database.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features contained in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM might have patents or pending patent applications that cover subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it to enable: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

Such information might be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments might vary significantly. Some measurements might have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements might have been estimated through extrapolation. Actual results might vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements, or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding the future direction or intent of IBM are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing, or distributing application programs that conform to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample

programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2004, 2012. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations might not appear.

Privacy Policy Considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both: http://www.ibm.com/legal/copytrade.shtml

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

The Oracle Outside In Technology included herein is subject to a restricted use license and can only be used in conjunction with this application.

Index

W

X

Product Number: 5725-L52

Printed in USA

SC27-6206-01