

IBM® Security Privileged Identity Manager  
Version 1.0.1.1

*Virtual Appliance Deployment Guide*





IBM® Security Privileged Identity Manager  
Version 1.0.1.1

*Virtual Appliance Deployment Guide*



**Note**

Before using this information and the product it supports, read the information in Notices.

**Edition notice**

**Note:** This edition applies to Version 1.0.1.1 of *IBM Security Privileged Identity Manager* (product number 5725-H30) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2012, 2014.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

**Figures . . . . . v**

**Tables . . . . . vii**

**About this publication . . . . . ix**

Access to publications and terminology . . . . . ix  
Accessibility . . . . . x  
Technical training. . . . . x  
Support information. . . . . x  
Statement of Good Security Practices . . . . . x

**Chapter 1. Virtual appliance overview . . . . . 1**

Language support overview . . . . . 1  
Hardware and software requirements . . . . . 2  
Appliance format. . . . . 3  
Roadmap to the IBM Security Privileged Identity Manager Virtual Appliance setup . . . . . 3

**Chapter 2. Getting started . . . . . 5**

Personas and use cases . . . . . 5  
Installation of prerequisite software . . . . . 12  
    Installing and configuring the database server. . . . . 12  
    Installing and configuring the directory server. . . . . 14  
    Setting up the directory server for SSL connection 15  
Setting up the virtual machine . . . . . 18  
    Installing the IBM Security Privileged Identity Manager Virtual Appliance . . . . . 19  
    Setting up the initial IBM Security Privileged Identity Manager Virtual Appliance . . . . . 19  
    Managing the Mode Selection page . . . . . 22  
    Configuring the IBM Security Privileged Identity Manager by using the Initial Configuration wizard . . . . . 23  
    Setting up an IBM Security Privileged Identity Manager Member node from the Initial Configuration wizard . . . . . 25  
Logging on to the consoles from the Appliance Dashboard. . . . . 26

**Chapter 3. Appliance Dashboard . . . . . 29**

Viewing notifications . . . . . 29  
Viewing the cluster status . . . . . 29  
Viewing and using server controls. . . . . 31  
Viewing deployment statistics . . . . . 31  
Viewing the middleware and server monitor widget 31  
Viewing and using quick links . . . . . 31  
Viewing disk usage. . . . . 32  
Viewing IP addresses . . . . . 32  
Viewing partition information . . . . . 33  
Viewing the update history . . . . . 33  
Viewing the licensing . . . . . 33  
Managing the firmware settings . . . . . 34  
Installing a fix pack. . . . . 34  
Viewing the About page information . . . . . 35

Viewing the memory utilization . . . . . 36  
Viewing the CPU utilization. . . . . 36  
Viewing the storage utilization . . . . . 37  
Configuring the date and time settings . . . . . 38  
Configuring the administrator settings . . . . . 38  
Managing the snapshots . . . . . 39  
Managing the support files . . . . . 39  
Restarting or shutting down. . . . . 40

**Chapter 4. IBM Security Privileged Identity Manager Virtual Appliance command line interface . . . . . 41**

IBM Security Privileged Identity Manager Virtual Appliance command line interface commands for IBM Security Privileged Identity Manager . . . . . 41  
Cleaning core dump files. . . . . 43  
IBM Security Privileged Identity Manager Virtual Appliance command line interface commands. . . . . 46  
Enabling trace for the virtual appliance services . . . . . 48

**Chapter 5. Managing the virtual appliance . . . . . 51**

Enabling the Session Recording feature in the virtual appliance . . . . . 51  
Managing the Database Server configuration . . . . . 51  
Managing the Directory Server configuration . . . . . 53  
Configuring the Load Balancer . . . . . 54  
Managing mail configuration . . . . . 55  
Managing the server properties. . . . . 55  
Managing feed files. . . . . 57  
Changing a Member node to a Primary node . . . . . 57  
Changing a Primary node to a Member node . . . . . 58  
Removing a node from the cluster. . . . . 58  
Reconnecting a node into the cluster . . . . . 59  
Synchronizing a Member node with a Primary node 60  
Managing log configuration . . . . . 61  
    Retrieving logs . . . . . 62  
    Configuring logs . . . . . 63  
Reconfiguring the data store connection . . . . . 63  
Reconfiguring the directory server connection . . . . . 65

**Chapter 6. Configuration . . . . . 67**

IBM Security Access Manager for Enterprise Single Sign-On configuration . . . . . 67  
Shared access configuration . . . . . 67  
Session recording configuration. . . . . 68  
Optional configuration tasks. . . . . 70  
Load Balancer settings and requirements . . . . . 71

**Chapter 7. Shared credential check-out and check-in . . . . . 73**

Automatic check-out and check-in with client application logon . . . . . 73  
Logging on with PuTTY . . . . . 73

Logging on with the Microsoft Remote Desktop Connection (RDP) client . . . . .	73
Logging on with IBM Personal Communications	74
Logging on with the VMware vSphere Client . . . . .	75
Manual check-out and check-in of shared credentials	76
Checking out a credential or credential pool . . . . .	76
Checking in credentials in a credential pool . . . . .	77
Checking in credentials from a credential vault	79

**Chapter 8. Setting up a secondary virtual appliance for active-passive configuration . . . . . 81**

Setting up a primary virtual appliance . . . . .	81
Backing up the primary virtual appliance . . . . .	81
Reverting the virtual appliance to its backup . . . . .	82
Creating a snapshot of the primary virtual appliance	82
Setting up a secondary virtual appliance. . . . .	83
Enhance availability by using monitoring URLs . . . . .	84

**Chapter 9. Upgrading the IBM Security Privileged Identity Manager Virtual Appliance . . . . . 85**

**Chapter 10. Troubleshooting and support . . . . . 89**

Restrict operations for a Member node . . . . .	89
Handling password synchronization issues . . . . .	89
Cluster bootstrap process . . . . .	90
Cluster monitor service . . . . .	91
Checking logs . . . . .	92
Common issues . . . . .	92
Limitations . . . . .	95
Known issues and workarounds . . . . .	96
Troubleshooting dashboard panel widget display issues on Microsoft Internet Explorer 10 . . . . .	97

Troubleshooting Logon to Session Reply Console	97
Value for a property is not retained if update_syslog command is executed without any value for other properties. . . . .	97
Startup problems with the IBM Security Privileged Identity Manager Virtual Appliance Dashboard. . . . .	98
IBM Security Privileged Identity Manager Virtual Appliance Dashboard displays notifications about snapshots . . . . .	98
LDAP Server must run when IBM Security Privileged Identity Manager Virtual Appliance servers are restarted after LDAP configuration. . . . .	99
Bulkload command errors . . . . .	99

**Chapter 11. Sample configuration response file. . . . . 101**

**Notices . . . . . 103**

**Glossary . . . . . 107**

A . . . . .	107
C . . . . .	107
D . . . . .	107
E . . . . .	107
F . . . . .	108
I. . . . .	108
M . . . . .	108
P . . . . .	108
R . . . . .	108
S . . . . .	108
W . . . . .	108

**Index . . . . . 109**

---

## Figures

1. Deployment diagram of a typical Load Balancer in a customer environment . . . . 71





---

## Tables

1. Supported language per product . . . . .	1	10. Privileged Session Recordings . . . . .	12
2. Server installation by using a virtual appliance roadmap . . . . .	3	11. Files in the /certs directory . . . . .	17
3. Main stages or tasks that are involved in using the IBM Security Privileged Identity Manager Virtual Appliance . . . . .	5	12. Synchronization states table . . . . .	30
4. Virtual Appliance Administrator tasks . . . . .	6	13. Data stores configuration options . . . . .	52
5. Privileged Identity Manager Administrator tasks . . . . .	7	14. Directory or LDAP server configuration details	54
6. Privileged Administrator tasks . . . . .	10	15. Available IBM Security Identity Manager properties in the IBM Security Privileged Identity Manager Virtual Appliance . . . . .	56
7. Privileged User tasks in the IBM Security Identity Manager self-service UI. . . . .	11	16. Synchronization state table . . . . .	61
8. Privileged User task with AccessAgent . . . . .	11	17. Available logs to help you diagnose or troubleshoot . . . . .	62
9. Privileged User Manager task in the IBM Security Identity Manager self-service UI. . . . .	11	18. Single Sign-On configuration tasks . . . . .	67
		19. Shared access configuration tasks . . . . .	67
		20. Session recording configuration tasks . . . . .	69
		21. Optional configuration tasks . . . . .	70



---

## About this publication

*IBM Security Privileged Identity Manager Virtual Appliance Deployment Guide* describes the process of setting up, administering, and configuring the IBM® Security Privileged Identity Manager virtual appliance.

---

## Access to publications and terminology

This section provides:

- A list of publications in the “IBM Security Privileged Identity Manager library.”
- Links to “Online publications.”
- A link to the “IBM Terminology website” on page x.

### IBM Security Privileged Identity Manager library

The following documents are available online in the IBM Security Privileged Identity Manager library:

- *IBM Security Privileged Identity Manager Deployment Overview Guide*, SC27-4382-03
- *IBM Security Privileged Identity Manager Administrator Guide*, SC27-5619-02
- *IBM Security Privileged Identity Manager Virtual Appliance Deployment Guide*, SC27-5625-01

### Online publications

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

#### IBM Security Privileged Identity Manager library

The product documentation site ([http://www.ibm.com/support/knowledgecenter/SSRQBP\\_1.0.1.1/com.ibm.ispim.doc\\_1.0.1.1/kc-homepage.html](http://www.ibm.com/support/knowledgecenter/SSRQBP_1.0.1.1/com.ibm.ispim.doc_1.0.1.1/kc-homepage.html)) displays the welcome page and navigation for the library.

#### IBM Security Identity Manager library

The product documentation site ([https://www.ibm.com/support/knowledgecenter/SSRMWJ\\_6.0.0.2/com.ibm.isim.doc\\_6.0.0.2/kc-homepage.htm](https://www.ibm.com/support/knowledgecenter/SSRMWJ_6.0.0.2/com.ibm.isim.doc_6.0.0.2/kc-homepage.htm)) displays the welcome page and navigation for the IBM Security Identity Manager product.

#### IBM Security Access Manager for Enterprise Single Sign-On library

The product documentation site ([https://www.ibm.com/support/knowledgecenter/SS9JLE\\_8.2.1/com.ibm.itamesso.doc\\_8.2.1/kc-homepage.html](https://www.ibm.com/support/knowledgecenter/SS9JLE_8.2.1/com.ibm.itamesso.doc_8.2.1/kc-homepage.html)) displays the welcome page and navigation for the IBM Security Access Manager for Enterprise Single Sign-On product.

#### 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 <http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss> site 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. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

For additional information, see the *IBM Security Privileged Identity Manager Deployment Overview Guide*.

---

## 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>.

The *IBM Security Identity Manager Troubleshooting Guide* and *IBM Security Access Manager for Enterprise Single Sign-On 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.

See *IBM Security Privileged Identity Manager Deployment Overview Guide* for instructions and problem-determination resources for IBM Security Privileged Identity Manager.

**Note:** The **Community and Support** tab on the product documentation 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. Virtual appliance overview

The IBM Security Privileged Identity Manager is a network appliance-based identity management solution that provides privileged identity management and session recording.

IBM Security Privileged Identity Manager Virtual Appliance features:

- A configuration wizard for the first time configuration of the IBM Security Privileged Identity Manager solution in a stand-alone or a cluster mode.
- A dashboard for viewing system status such as system notifications, cluster status, component and application status, deployment statistics, and disk usage.
- Analysis and diagnostics tools such as memory statistics, and CPU utilization.
- Centralized management of IBM Security Privileged Identity Manager settings such as data tier components or external entities, and log files.
- Control of system settings such as host name, date or time, and network settings.
- Most of the features are configurable by using the graphical management interface.

---

## Language support overview

The IBM Security Privileged Identity Manager virtual appliance and its integrated products, are translated into the following languages:

*Table 1. Supported language per product*

Language	IBM Security Access Manager for Enterprise Single Sign-On	IBM Security Identity Manager	IBM Security Privileged Identity Manager Virtual Appliance
Arabic	Yes	Yes	No
Chinese (Simplified)	Yes	Yes	Yes
Chinese (Traditional)	Yes	Yes	Yes
Czech	Yes	Yes	No
Danish	Yes	No	No
Dutch	Yes	No	No
English (United States)	Yes	Yes	Yes
Finnish	Yes	No	No
French (Standard)	Yes	Yes	Yes
German	Yes	Yes	Yes
Greek	No	Yes	No
Hebrew	Yes	Yes	No
Hungarian	Yes	Yes	No
Italian	Yes	Yes	Yes
Japanese	Yes	Yes	Yes
Korean	Yes	Yes	Yes

Table 1. Supported language per product (continued)

Language	IBM Security Access Manager for Enterprise Single Sign-On	IBM Security Identity Manager	IBM Security Privileged Identity Manager Virtual Appliance
Polish	Yes	Yes	No
Portuguese (Brazilian)	Yes	Yes	Yes
Russian	Yes	Yes	Yes
Spanish	Yes	Yes	Yes

**Note:** To change the language for IBM Security Privileged Identity Manager virtual appliance console, select the required language from the **Language** drop-down menu at the top right corner of the console. For languages with right-to-left text orientation, for example, Hebrew or Arabic, the **Language** drop-down menu is on the upper left corner of the console.

---

## Hardware and software requirements

The IBM Security Privileged Identity Manager has specific hardware and software requirements.

### IBM Security Privileged Identity Manager, Version 1.0.1.1 Virtual Appliance Server

- VMware ESXi 5.0 and 5.1.
- CPU: Minimum 4 GHz, four cores (64-bit).
- Minimum 16 GB system memory.
- Disk space: At least 100 GB free hard disk space.

### Data tier

Components: IBM DB2®, IBM Security Directory Server

- CPU: Minimum 4 GHz, four cores.
- At least 8 GB of RAM is required. However, use 16 GB of RAM for the three databases and one directory server instance.
- Minimum 16 to 24 GB<sup>1</sup> system memory.
- Disk space: At least 40 GB<sup>2</sup> free hard disk space per user and per year, depending on the typical screen size, recorded applications, and user activity.

### Database and Directory Server support

- IBM DB2 Enterprise Server Version 10.1 Fix Pack 2
- IBM Security Directory Server Version 6.3 Fix Pack 21

### Notes:

<sup>1</sup> System Memory (RAM) to allocate for IBM Security Privileged Identity Manager Session Recorder WebSphere Application Server, and database.

<sup>2</sup> Allocate at least 40 GB to consider the indexing activity in the virtual appliance for data retention. By default, the IBM Security Privileged Identity Manager Session Recorder periodical index update action happens every 15 minutes. It is during that time that the Privileged Session Recorder indexer component detects that the index is outdated and must be updated.



---

## Appliance format

The IBM Security Privileged Identity Manager comes in a virtual appliance format.

The IBM Security Privileged Identity Manager Virtual Appliance can be hosted on the following virtual hypervisors:

- VMware ESXi 5.0
- VMware ESXi 5.1

---

## Roadmap to the IBM Security Privileged Identity Manager Virtual Appliance setup

Use the roadmap as a reference for a server deployment, IBM Security Privileged Identity Manager installation in the virtual appliance, and initial configuration settings.

*Table 2. Server installation by using a virtual appliance roadmap*

<b>Procedure</b>	<b>Reference</b>
Prepare the database server	"Installing and configuring the database server" on page 12
Prepare the directory server	"Installing and configuring the directory server" on page 14
Set up the virtual appliance on VMware ESXi	"Setting up the virtual machine" on page 18
Install IBM Security Privileged Identity Manager in the virtual appliance	"Installing the IBM Security Privileged Identity Manager Virtual Appliance" on page 19
Configure the virtual appliance	"Setting up the initial IBM Security Privileged Identity Manager Virtual Appliance" on page 19
Configure the virtual appliance in a stand-alone or a clustered mode.	"Managing the Mode Selection page" on page 22



---

## Chapter 2. Getting started

An overview about how to get started with the IBM Security Privileged Identity Manager Virtual Appliance is described here.

The following table describes the main stages or tasks that are involved in using the IBM Security Privileged Identity Manager Virtual Appliance.

*Table 3. Main stages or tasks that are involved in using the IBM Security Privileged Identity Manager Virtual Appliance*

	Tasks	Action by
1.	Deploy and configure the Privileged Identity Management System.	IBM Security Privileged Identity Manager Virtual Appliance Administrator
2.	Configure system-wide organizational structure and roles, and policies for password, single sign-on and session recording.	IBM Security Privileged Identity Manager Administrator
3.	Create roles. <b>Note:</b> Skip this task if the role exists.	IBM Security Privileged Identity Manager Administrator or Privileged Administrator
4.	On-board Privileged Administrators.	IBM Security Privileged Identity Manager Administrator
5.	On-board Privileged Users.	IBM Security Privileged Identity Manager Administrator
If you want to connect the credentials to the accounts on the managed systems, complete tasks 6, 7, and 8.		
If you do not want to connect the credentials to the accounts on the managed systems, complete tasks 7, and 8 only.		
6.	On-board service types, service instances, and accounts.	IBM Security Privileged Identity Manager Administrator
7.	On-board credentials.	IBM Security Privileged Identity Manager Administrator or Privileged Administrator
8.	Assign users to role.	IBM Security Privileged Identity Manager Administrator or Privileged Administrator

---

## Personas and use cases

There are different personas that are involved with the setup and usage of the virtual appliance. Each persona is responsible for a set of tasks or is privileged to do specific workflows.

## Persona: Virtual Appliance Administrator

The Virtual Appliance Administrator is responsible for the following tasks.

Table 4. Virtual Appliance Administrator tasks

Tasks	Subtasks and references
Deploy and configure the Privileged Identity Management System.	<ol style="list-style-type: none"> <li>1. "Installing and configuring the database server" on page 12</li> <li>2. "Installing and configuring the directory server" on page 14</li> <li>3. "Setting up the virtual machine" on page 18</li> <li>4. "Installing the IBM Security Privileged Identity Manager Virtual Appliance" on page 19</li> <li>5. "Setting up the initial IBM Security Privileged Identity Manager Virtual Appliance" on page 19</li> <li>6. "Configuring the IBM Security Privileged Identity Manager by using the Initial Configuration wizard" on page 23               <ol style="list-style-type: none"> <li>a. "Enabling the Session Recording feature in the virtual appliance" on page 51</li> <li>b. "Managing the Database Server configuration" on page 51</li> <li>c. "Managing the Directory Server configuration" on page 53</li> <li>d. "Managing mail configuration" on page 55</li> </ol> </li> <li>7. "Setting up an IBM Security Privileged Identity Manager Member node from the Initial Configuration wizard" on page 25</li> <li>8. Deploy AccessAgent. See the <i>IBM Security Access Manager for Enterprise Single Sign-On Installation Guide</i>.</li> </ol>
Back up and restore the virtual appliance by using snapshots	"Creating a snapshot of the primary virtual appliance" on page 82
Set up and enact disaster recovery for the virtual appliance	<ol style="list-style-type: none"> <li>1. "Setting up a primary virtual appliance" on page 81</li> <li>2. "Setting up a secondary virtual appliance" on page 83</li> </ol>
Applying Fix Pack	Use the <code>fixpack</code> command in the "IBM Security Privileged Identity Manager Virtual Appliance command line interface commands for IBM Security Privileged Identity Manager" on page 41.
Upgrade Firmware	Use the <code>firmware_update</code> command in the "IBM Security Privileged Identity Manager Virtual Appliance command line interface commands for IBM Security Privileged Identity Manager" on page 41.

Table 4. Virtual Appliance Administrator tasks (continued)

Tasks	Subtasks and references
Reconfigure the virtual appliance	<ul style="list-style-type: none"> <li>• “Reconfiguring the data store connection” on page 63</li> <li>• “Reconfiguring the directory server connection” on page 65</li> </ul>

## Persona: Privileged Identity Manager Administrator

The Privileged Identity Manager Administrator is responsible for the following tasks.

Table 5. Privileged Identity Manager Administrator tasks

Tasks	Subtasks and reference
Configure system-wide organizational structure and roles, and policies for password, single sign-on and session recording.	<ol style="list-style-type: none"> <li>1. Create a node in an organization tree. See "Creating a node in an organization tree" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> <li>2. Create account ownership type ("shared"). <b>Note:</b> This step is required for subsequent on-boarding of connected credentials. See "Creating ownership types" in the <i>IBM Security Identity Manager Configuration Guide</i>.</li> <li>3. Define password policies for the Privileged account. For example, Set password expiry. See "Enabling password expiration" in the <i>IBM Security Identity Manager Administration Guide</i>. For other policies, see "Password administration" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> <li>4. Review the IBM Security Access Manager for Enterprise Single Sign-On and IBM Security Privileged Identity Manager session recording policies. See "Configure additional IMS Server policies for session recording" in "Session recording configuration" on page 68.</li> </ol>
Create roles. <b>Note:</b> Skip this task if the role exists.	See "Creating roles" in the <i>IBM Security Identity Manager Administration Guide</i> .

Table 5. Privileged Identity Manager Administrator tasks (continued)

Tasks	Subtasks and reference
On-board Privileged Administrators.	<ol style="list-style-type: none"> <li>1. Create a Privileged Administrator profile. See "Creating user profiles" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> <li>2. (Optional) Assign the user to a Privileged Administrator role if the role is already defined. See "Adding users to membership of a role" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> <li>3. Add user to the pre-defined Privileged Administrator group. See "Adding members to groups" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> <li>4. (Optional) Add an Administrator domain and make the Privileged Administrator user as Administrator to the Admin domain. See "Creating a node in an organization tree" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> </ol>
On-board Privileged Users.	<ol style="list-style-type: none"> <li>1. Create a Privileged User profile. See "Creating user profiles" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> <li>2. (Optional) Assign the user to a Privileged User role if needed or if the role is already defined. See "Adding users to membership of a role" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> </ol>
<p>On-board service types, service instances, and accounts.</p> <p>If the service type is not yet pre-configured</p>	<ol style="list-style-type: none"> <li>1. Create a Service Type by importing a service type profile.</li> <li>2. Update the Service Type form with the erURI property.  <b>Note:</b> This step is not required for pre-configured service type profiles such as POSIX, Windows Local, and Windows Active Directory.</li> </ol> <p>See "Creating service types" and "Customizing the service form template to include the unique identifier (eruri)" in the <i>IBM Security Identity Manager Configuration Guide</i>.</p>

Table 5. Privileged Identity Manager Administrator tasks (continued)

Tasks	Subtasks and reference
<p>On-board service types, service instances, and accounts.</p> <p>If the service type is already pre-configured</p>	<ol style="list-style-type: none"> <li>1. Create a specific Privileged Administrator Role. See "Creating roles" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> <li>2. Create a provisioning policy for the appropriate Privileged Administrator role, which covers present Service Type or more, with type value "shared". See "Creating a provisioning policy" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> <li>3. Create a Service instance. See "Creating services" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> <li>4. Reconcile the accounts for the Service by using filters like <b>erposixsecondgroup</b> (for Linux) and <b>erntlocalgroups</b> (for Windows) where appropriate; See "Reconciling accounts immediately on a service" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> <li>5. Adopt and assign accounts, as shared type to be owned by Privileged Identity Manager Administrator or Privileged Administrator. See "Assigning an account to a user" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> </ol>
<p>On-board credentials.</p>	<ol style="list-style-type: none"> <li>1. Add credential to vault. See "Adding credentials to the vault" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> <li>2. (Optional) Set up the Credential Pool for the Connected Credentials. See "Creating credential pools" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> <li>3. Set up the shared access policy. See "Creating shared access policies" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> </ol> <p>Alternatively, you can add credential to the vault and set up the Credential Pool by using Batch Upload. See "Uploading a CSV file with the administrative console" in the <i>IBM Security Identity Manager Administration Guide</i>.</p>
<p>Assign users to role.</p>	<p>See "Adding users to membership of a role" in the <i>IBM Security Identity Manager Administration Guide</i>.</p>

Table 5. Privileged Identity Manager Administrator tasks (continued)

Tasks	Subtasks and reference
On-board Privileged Session Recorder Auditor <b>Note:</b> Do this task only if Session Recording is enabled.	<ol style="list-style-type: none"> <li>1. Create a Privileged User profile. See "Creating user profiles" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> <li>2. Assign the user to a Privileged Session Recorder Auditor role if needed or if the role is already defined. See "Adding users to membership of a role" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> </ol>
(Optional) Update user roles	See "Modifying roles" in the <i>IBM Security Identity Manager Administration Guide</i> .
(Optional) Update user group	See "Modifying groups" in the <i>IBM Security Identity Manager Administration Guide</i> .
(Optional) Update shared access policies	See "Modifying shared access policies" in the <i>IBM Security Identity Manager Administration Guide</i> .

## Persona: Privileged Administrator

The Privileged Administrator is responsible for the following tasks.

Table 6. Privileged Administrator tasks

Tasks	Subtasks and reference
On-board unconnected credentials	<ol style="list-style-type: none"> <li>1. Add credential to the vault. See "Adding credentials to the vault" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> <li>2. Create a shared access policy and assign the policy to an existing role. See "Creating shared access policies" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> </ol>
On-board connected credentials	<ol style="list-style-type: none"> <li>1. Add credentials by connecting the credentials to "vendor" accounts. See "Creating user profiles" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> <li>2. Create credential pool for added credentials.</li> <li>3. Create Privileged User role for the credential pool.</li> <li>4. Create a shared access policy. See "Creating shared access policies" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> </ol>
Assign users to role.	See "Adding users to membership of a role" in the <i>IBM Security Identity Manager Administration Guide</i> .
(Optional) Update user roles	See "Modifying roles" in the <i>IBM Security Identity Manager Administration Guide</i> .



Table 6. Privileged Administrator tasks (continued)

Tasks	Subtasks and reference
(Optional) Update user group	See "Modifying groups" in the <i>IBM Security Identity Manager Administration Guide</i> .
(Optional) Update shared access policies	See "Modifying shared access policies" in the <i>IBM Security Identity Manager Administration Guide</i> .

## Persona: Privileged User

The Privileged User uses the IBM Security Identity Manager self-service UI for the following tasks

Table 7. Privileged User tasks in the IBM Security Identity Manager self-service UI

Tasks	Subtasks and reference
Change password	See "Changing user passwords" in the <i>IBM Security Identity Manager Administration Guide</i> .
Reset password	See "Resetting user passwords" in the <i>IBM Security Identity Manager Administration Guide</i> .
Manually check out and check in shared credentials	"Manual check-out and check-in of shared credentials" on page 76
Request role for access to some shared ID	See "Request access" in the <i>IBM Security Identity Manager Scenarios Guide</i> .

The Privileged User also logs on to AccessAgent for automatic check-out and check-in of shared credentials.

**Note:** The Privileged User cannot sign up, change passwords and reset passwords in AccessAgent.

Table 8. Privileged User task with AccessAgent

Tasks	Subtasks and reference
Access systems and applications with shared credentials	"Automatic check-out and check-in with client application logon" on page 73

## Persona: User Manager

The User Manager uses the IBM Security Identity Manager self-service UI for the following task.

Table 9. Privileged User Manager task in the IBM Security Identity Manager self-service UI

Tasks	Subtasks and reference
Approve role requests	See "Approving user requests" in the <i>IBM Security Identity Manager Administration Guide</i> .

## Persona: Privileged Session Recorder Auditor

A Privileged Session Recorder Auditor uses the Privileged Session Recording console to search and review recordings to verify compliance to audit requirements.

Table 10. Privileged Session Recordings

Tasks	Subtasks and reference
Search recordings	See "Searching for recordings" in the <i>IBM Security Privileged Identity Manager Administration Guide</i> .
Replay recordings	See "Playing back recordings" in the <i>IBM Security Privileged Identity Manager Administration Guide</i> .

---

## Installation of prerequisite software

Install and configure the prerequisite components before you install the IBM Security Privileged Identity Manager Virtual Appliance.

### Installing and configuring the database server

You must install and configure the database server before you can install and configure the directory server.

#### Procedure

1. Follow the DB2 instance creation instructions.
  - a. Access [http://www.ibm.com/support/knowledgecenter/SSEPGG\\_10.1.0/com.ibm.db2.luw.kc.doc/welcome.html](http://www.ibm.com/support/knowledgecenter/SSEPGG_10.1.0/com.ibm.db2.luw.kc.doc/welcome.html).
  - b. Search for **Creating an instance using db2icrt**.
2. Configure the database server for the IBM Security Privileged Identity Manager Virtual Appliance.
  - a. Create the database instance.
    - 1) Create an operating system user. For example, piminst.
    - 2) Run the following command to create a database instance:

#### For Windows:

```
DB2_Install_Location\bin\db2icrt -u piminst piminst
```

*DB2\_Install\_Location* is the DB2 installation directory.

The created user piminst must be a member of these groups:

- DB2ADMNS
- DB2USERS

#### For Linux:

```
DB2_Install_Location/instance/db2icrt -u piminst piminst
```

- 3) Start the DB2 instance.

#### For Windows:

- Run **set DB2INSTANCE=piminst**, where piminst is the database instance.
- Run **db2cmd** to start the DB2 command line.
- Run **db2start**.

**For Linux:**

- Run **su - pminst**
  - Run **db2start**.
- 4) Run the following commands to set up the DB2 instance:
- **db2 update dbm cfg using SVCENAME 50050**, where 50050 is the port on which you want your database server to listen.
  - **db2set DB2COMM=tcPIP**
  - **db2set -a11 DB2COMM**
  - **db2stop**
  - **db2start**

b. Create the database.

When you work with the IBM Security Privileged Identity Manager, use three separate databases for the three data stores: Identity, Sign-On, and Session Recording.

To create a database, take the following actions:

1) Start the DB2 instance.

**For Windows:**

- In the command line, run **set DB2INSTANCE=pminst**, where pminst is the database instance and owner of the database that you want to create.
- Run **db2cmd** to start the DB2 command line.
- Run **db2start**.

**For Linux:**

- Run **su - pminst**, where pminst is the database instance and owner of the database that you want to create.
  - Run **db2start**.
- 2) In the DB2 command line, type the following example commands as the instance owner.

**For the Identity data stores**

```
db2 create db idmdb using codeset utf-8 territory us
pagesize 32 K
```

**For the Single Sign-On data stores**

```
db2 create db essodb using codeset utf-8 territory us
pagesize 8 K
```

**For the Session Recording data stores**

```
db2 create db psrdb using codeset utf-8 territory us
pagesize 8 K
```

- 3) On Windows, run the following commands to grant certain accesses to the instance owner on the Identity data store.
- **db2 connect to idmdb**
  - **db2 GRANT DBADM, SECADM ON DATABASE TO USER pminst**
  - **db2 disconnect current**
  - **db2stop**
  - **db2start**
- 4) Use the database administrator privileges for the Session Recording data store to meet the following requirements.

- Create a temporary table space with the following command, if necessary.

**Note:** The database administrator for the IBM Privileged Session Recorder must have access to a temporary table space.

- **db2 connect to psrdb**
- **db2 create user temporary tablespace systoolstmpspace  
pagesize 8 k managed by automatic storage bufferpool  
ibmdefaultbp**
- Grant the following permissions to the IBM Privileged Session Recorder database owner.
  - **db2 grant execute on module sysibmadm.utl\_file to user db2admin with grant option**
  - **db2 grant execute on module sysibmadm.utl\_dir to user db2admin with grant option**

db2admin is the database owner.

**Note:** The IBM Privileged Session Recorder database Administrator cannot grant these permissions. This permission can be granted only by another Administrator or a SYSADMIN account.

## Installing and configuring the directory server

You must install and configure the directory server before you can install the virtual appliance.

### Before you begin

You must have the database server installed.

### Procedure

1. For information about installing the directory server, see documentation that the directory server product provides. For example, access the documentation at <http://www.ibm.com/support/knowledgecenter/SSVJJU/welcome?lang=en> and search for **Installing and Configuring**.
2. Configure the directory server for IBM Security Privileged Identity Manager Virtual Appliance by creating and configuring the directory server instance.

- a. Create a user.

- Windows

In the command line, enter:

```
LDAP_Install_Location\sbin\idsadduser -u ldapinst -w ldapinstpwd
```

where ldapinst is the user name, and ldapinstpwd is the password.

- UNIX and Linux

In the command line, enter:

```
LDAP_Install_Location/sbin/idsadduser -u ldapinst -w ldapinstpwd -g  
idsldap
```

where ldapinst is the LDAP instance name, ldapinstpwd is the password, and idsldap is the default LDAP group.

- b. Create a directory server instance.

In the command line, enter:

```
LDAP_Install_Location/sbin/idsicrt -I ldapinst -e encryptionseed -l /home/ldapinst
```

where *ldapinst* is an LDAP instance name, *encryptionseed* is the encryption seed, and */home/ldapinst* is the instance home.

- c. Create a database for the newly created LDAP instance.

In the command line, enter:

```
LDAP_Install_Location/sbin/idscfgdb -I ldapinst -a dbadmin -w dbadminpwd -t dbname -l /home/ldapinst/
```

where *ldapinst* is an LDAP instance name, *dbadmin* is the Database Administrator, *dbadminpwd* is the Database Administrator password, *dbname* is the database name, and */home/ldapinst* is the instance home.

- d. Set the password for directory server instance Principal DN.

In the command line, enter:

```
LDAP_Install_Location/sbin/idsdnpw -I ldapinst -u cn=root -p root
```

where *ldapinst* is the LDAP instance name, *cn=root* is the Principal DN, and *root* is the Principal DN password.

- e. Add the suffix (*dc=com*) in the directory server instance.

In the command line, enter:

```
LDAP_Install_Location/sbin/idscfgsuf -I ldapinst -s dc=com
```

where *ldapinst* is an LDAP instance name, and *dc=com* is the suffix.

- f. Start the directory server instance.

- Windows

In the command line, enter:

```
LDAP_Install_Location/sbin/ibmslapd -I ldapinst -n
```

where *ldapinst* is the LDAP instance name.

- UNIX and Linux

In the command line, enter:

```
LDAP_Install_Location/sbin/ibmslapd -I ldapinst -n -t
```

where *ldapinst* is an LDAP instance name.

- g. Prepare a *ldif* file. For example, *dccom.ldif* with the following content.

```
dn:dc=com
objectclass:domain
```

Run the command:

```
LDAP_Install_Location/bin/idsldapadd -h ldap_server_host
-p ldap_server_port -D bind_root_dn -w bind_root_password
-f dccom.ldif
```

For example:

```
/opt/IBM/ldap/V6.3/bin/idsldapadd -D cn=root -w password -p port
-f dccom.ldif
```

## Setting up the directory server for SSL connection

To set up an IBM Security Privileged Identity Manager Virtual Appliance, you must first set up the directory server for an SSL connection.

### Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

## About this task

The iKeyman utility is in the IBM Security Directory Server.

### Procedure

1. Create a certificate. Use the iKeyman utility to create a self-signed certificate and extract the certificate to make it available for secure communication.
  - a. Start the iKeyman utility. For example, type the `gsk7ikm` command in the `/usr/local/ibm/gsk7/bin` directory.
  - b. If the iKeyman utility cannot locate Java™, run this command: **export JAVA\_HOME=opt/IBM/1dapv6.3/java/jre**
  - c. On the IBM Key Management page, select **Key Database File > Open > New**.
  - d. Select a default database type of CMS.
  - e. In the **File Name** field, type a name for the CMS key database file. For example, type: `LDAPSERVER_TEST1234.kbd`.

For example, the value specifies *application\_serverhostname* where *application* is the directory server, and *serverhostname* is the computer that has the directory server.
  - f. In the **Location** field, specify a location to store the key database file. For example, type `/certs`.
  - g. Click **OK**.
  - h. On the **Password** menu:
    - 1) Type and then confirm a password, such as `Pa$$word1`.
    - 2) Specify the highest password strength possible.
    - 3) Specify **Stash the password to a file?**
    - 4) Click **OK**.
  - i. Select **Create > New Self Signed Certificate** and specify a label that matches the CMS key database file name, such as `LDAPSERVER_TEST1234`.

This example uses the same name (`LDAPSERVER_TEST1234`) for both the certificate name and the key database file that contains the certificate.
  - j. Type `IBM` in the **Organization** field, accept the remaining field default values, and click **OK**. A self-signed certificate, including public and private keys, now exists.
  - k. For subsequent use with clients, extract the contents of the certificate into an ASCII Base-64 Encoded file. Complete these steps:
    - 1) Select **Extract Certificate**.
    - 2) Specify a data type of Binary DER Data.

A file with an extension of `.der` contains binary data. This format can be used only for a single certificate. Specify this format to extract a self-signed certificate.
    - 3) Specify the name of the certificate file name you created, such as `LDAPSERVER_TEST1234.der`.
    - 4) Specify a location, such as `/certs`, in which you previously stored the key database file.
    - 5) Click **OK**.
  - l. Verify that the `/certs` directory contains the following files:

Table 11. Files in the /certs directory

File	Description
LDAPSERVER_TEST1234.cr1	Not used in this example.
LDAPSERVER_TEST1234.der	The certificate.
LDAPSERVER_TEST1234.kdb	Key database file that has the certificate.
LDAPSERVER_TEST1234.rdb	Not used in this example.
LDAPSERVER_TEST1234.sth	Stash file that has the password

**Note:** If you use an existing or newly acquired certificate from a CA, copy it to the /certs directory on root file system of the directory server.

Alternatively, you can use the WebSphere® Application Server Administrative Console to create a self-signed certificate:

- 1) Select **Security > SSL certificate and key management > Manage endpoint security configurations > {Inbound | Outbound} > ssl\_configuration > Key stores and certificates > [keystore ]**. From Additional Properties, click **Personal certificates**.
- 2) Click **Create a self-signed certificate**.

For more information, see:

- Topics on securing directory communications in the *IBM Security Directory Server Administration Guide* at [http://www.ibm.com/support/knowledgecenter/SSVJJU\\_6.3.1/com.ibm.IBMDS.doc\\_6.3.1/welcome.htm](http://www.ibm.com/support/knowledgecenter/SSVJJU_6.3.1/com.ibm.IBMDS.doc_6.3.1/welcome.htm)
  - *IBM Global Security Kit Secure Sockets Layer Introduction and iKeyman User's Guide* at <http://www.ibm.com/support/docview.wss?uid=pub1sc23651000>
2. Enable the directory server for an SSL connection. Use an LDIF file to configure SSL on the directory server and to specify a secure port.
    - a. If the directory server is not running, start the server. For example, on UNIX, type this command:
 

```
/opt/IBM/ldap/V6.3/sbin/ibmslapd -I itimldap
```

 Where *-I* specifies the instance.
    - b. Create an LDIF file, such as `ssl.ldif`, with the following data:
 

```
dn: cn=SSL,cn=Configuration
changetype: modify
replace: ibm-slapdSecurity
ibm-slapdSecurity: sslonly
-
replace: ibm-slapdSslKeyDatabase
ibm-slapdSslKeyDatabase: /certs/LDAPSERVER_TEST1234.kdb
-
add: ibm-slapdSslKeyDatabasePW
ibm-slapdSslKeyDatabasePW: server
```
    - c. Place the LDIF file in the following directory:

**Note:** The empty lines that contain only the - (hyphen) character are expected for LDIF file formatting.

To change the secured port from the default port number 636, add these additional lines:

```
replace: ibm-slapdSecurePort
ibm-slapdSecurePort: 637
```

```
/opt/IBM/ldap/V6.3/bin
```

- d. Run the **idsldapmodify** command, which modifies the password policy by adding the LDIF file to the process.

```
idsldapmodify -D cn=root -w passwd -i ssl.ldif
```

- D** Binds to the LDAP directory, which is `cn=root` in this example.
- w** Uses the *passwd* value, which is the directory server administrator password, as the password for authentication.
- i** Reads the entry modification information from an LDIF file instead of from standard input. In this example, the file is named `ssl.ldif`.

A successful result produces a message similar to the following one:

```
Operation 0 modifying entry cn=SSL,cn=Configuration
```

- e. Test the directory server to confirm that it is listening on the default secure port 636. Follow these steps:

- 1) Stop the directory server. Type `/opt/IBM/ldap/V6.3/sbin/ibmslapd -k -I itimldap`.

- 2) Start the directory server. Type `/opt/IBM/ldap/V6.3/sbin/ibmslapd -I itimldap`.

Where **-I** specifies the instance.

- 3) Determine whether the directory server is listening on port 636.

For example, display statistics for the network interface with the directory server by typing `netstat -an |grep 636`.

A return message that indicates the port is listening might be this example:

```
tcp    0    0 9.42.62.72:636 0.0.0.0:*    LISTEN
```

---

## Setting up the virtual machine

Set up the virtual machine that you must use to host the IBM Security Privileged Identity Manager.

### Procedure

1. Download the `ispim_*.iso` build.
2. Create a virtual machine on ESXi 5.x with the following configuration.
  - a. Select **Custom**.
  - b. Provide a name for the virtual machine.
  - c. Choose the destination storage for this virtual machine.
  - d. Set virtual machine version to 8.
  - e. For the IBM Security Privileged Identity Manager Virtual Appliance, the required guest operating system is Linux with version 2.6.x 64 bit.
  - f. Enter the number of virtual sockets and cores per virtual sockets for the virtual machine. For example: 4 cores.
  - g. Enter the memory size. For example: 16 GB.
  - h. Enter the network configuration. Set E1000 for the IBM Security Privileged Identity Manager Virtual Appliance network adapter.
  - i. Set the SCSI controller type to **LSI Logic Parallel**.
  - j. Select the **Create a new virtual disk** option as the type of disk to use.
  - k. Enter the disk size for virtual machine. For example: 60 GB.
  - l. Accept the default settings in the Advanced Options page.



3. Check summary for the configuration accuracy.
4. Click **Finish**.
5. Mount the IBM Security Privileged Identity Manager media.
  - a. List the options. Right-click on virtual machine, and then select **Edit Settings**.
  - b. Choose **CD/DVD drive 1**.
  - c. Browse for the location of the `.iso` file that is uploaded in the data store.
  - d. Select **Connect at power on**.
  - e. Click **Power on the virtual machine** to proceed with the IBM Security Privileged Identity Manager Virtual Appliance installation.

## Installing the IBM Security Privileged Identity Manager Virtual Appliance

You can install IBM Security Privileged Identity Manager Virtual Appliance after you set up the virtual machine.

### Procedure

1. When you start the virtual machine for the first time, a list of available languages is displayed. Select the required language and then enter **Yes** to start the installation process.
2. When the installation process completes, press **Enter** to restart the system.

## Setting up the initial IBM Security Privileged Identity Manager Virtual Appliance

For the virtual appliance, the Appliance Setup wizard runs the first time that you connect to the virtual console of an unconfigured virtual appliance.

### Procedure

1. Provide the following user credentials when the system restarts after the IBM Security Privileged Identity Manager Virtual Appliance installation:
  - **Unconfigured login:** admin
  - **Password:** admin
2. Press 1 to choose the language.  
Press 2 to view the IBM terms.  
Press 3 to view the non-IBM terms.  
Press 4 to accept the license terms.

```

Software License Agreement
Currently selected language: English
1: Select language for license display
2: Read IBM terms
3: Read non-IBM terms
4: Proceed to acceptance

Select option: 4

By choosing 'I agree,' you agree that (1) you have had the opportunity to
review the terms of both the IBM and non-IBM licenses presented above and (2)
such terms govern this transaction. If you do not agree, choose 'I do not
agree'.
1: I agree
2: I do not agree

Select option: 1

```

3. Change the virtual appliance password. After you change the virtual appliance password, continue to the next screen.

```

Appliance Password
Password changes are applied immediately.
Password has not been modified.
1: Change password
x: Exit
p: Previous screen
n: Next screen

Change Password
Enter old password:
Enter new password:
Confirm new password:
Password changed successfully.

Appliance Password
Password changes are applied immediately.
Password has been modified.
1: Change password
x: Exit
p: Previous screen
n: Next screen

Select option: n

```

4. Change the host name.

```

Change the Host Name
Enter the new host name: ispimva.us.example.com

Host Name Configuration
Host name: ispimva.us.example.com
1: Change the host name
x: Exit
p: Previous screen
n: Next screen

Select option: n

```

**Note:** The host name is cited in the SSL certificate for the virtual appliance. In a non-cluster setup, you must use the value that is provided as the server location during AccessAgent configuration on the client system.

5. Configure network interface M1 with the IP address, subnet mask, and default gateway.

```
Management Interface Settings
1: Display device settings
2: Display policy
3: Configure M.1
4: Configure M.2
x: Exit
p: Previous screen
n: Next screen

Select option: 3

Configure M.1
Select an IPv4 configuration mode:
1: Automatic
2: Manual
Enter index: 2
Enter the IPv4 address: 192.0.2.21
Enter the IPv4 subnet mask: 255.255.254.0
Enter the IPv4 default gateway: 192.0.2.12
Select an IPv6 configuration mode:
1: Automatic
2: Manual
Enter index: 1
```

## 6. Configure the DNS for the virtual appliance.

```
DNS Configuration
No DNS servers configured.
1: Set DNS server 1
2: Set DNS server 2
3: Set DNS server 3
x: Exit
p: Previous screen
n: Next screen

Select option: 1

Set DNS Server 1
Enter the DNS Server IP address: 198.51.100.0

DNS Configuration
DNS server 1: 198.51.100.0
1: Set DNS server 1
2: Set DNS server 2
3: Set DNS server 3
x: Exit
p: Previous screen
n: Next screen

Select option: n
```

## 7. Configure the time settings for the virtual appliance.

```
Time Configuration
Time configuration changes are applied immediately.
Time: 08:28:58
Date: 09/09/2013
Time Zone: Asia/Kolkata
1: Change the time
2: Change the date
3: Change the time zone
x: Exit
p: Previous screen
n: Next screen

Select option: n
Command cancelled
1: Change the time
2: Change the date
3: Change the time zone
x: Exit
p: Previous screen
n: Next screen

Select option: n
```

8. Review the summary of configuration details.

**Note:** If necessary, record the details of the assigned IP address, DNS, and host name of the virtual appliance.

9. Press 1 to accept the configuration.

## Managing the Mode Selection page

In the Mode Selection page, you can set up IBM Security Privileged Identity Manager Virtual Appliance as a stand-alone server or Primary node, or a Member node. Select an option that is based on your deployment preference.

### Before you begin

Depending on how your system was customized, you might not have authorization to complete this task. To obtain authorization to this task or to have someone complete it for you, contact your system administrator.

### About this task

IBM Security Privileged Identity Manager Virtual Appliance supports high availability deployment mode. A high availability deployment is a cluster of multiple servers that are active and can process requests. The IBM Security Privileged Identity Manager Virtual Appliance consists of one Primary node and other nodes that are called as Member node.

### Procedure

1. In a web browser, type the host name of the IBM Security Privileged Identity Manager Virtual Appliance in the following format.

*https://host name of the IBM Security Privileged Identity Manager*

For example: `https://pim1.jk.example.com`

2. Log on to the IBM Security Privileged Identity Manager Virtual Appliance with the administrator credentials.
  - **Configured login:** admin
  - **Password:** admin

3. Select one of the mode options that are based on your requirement and click **Next**.

**Set up a stand-alone node for IBM Security Privileged Identity Manager Virtual Appliance or**

**Set up a Primary node for the IBM Security Privileged Identity Manager Virtual Appliance cluster**

Sets up a stand-alone node or a Primary node for the IBM Security Privileged Identity Manager Virtual Appliance cluster.

**Set up a Member node for the IBM Security Privileged Identity Manager Virtual Appliance cluster**

Sets up a Member node for the IBM Security Privileged Identity Manager Virtual Appliance cluster.

## Configuring the IBM Security Privileged Identity Manager by using the Initial Configuration wizard

In a web browser, log on to the Initial Configuration wizard from the web user interface after you complete the virtual appliance logon configuration. Complete the Appliance first steps virtual appliance setup tasks from either the command line or the IBM Security Privileged Identity Manager Virtual Appliance management user interface. The initial configuration tasks for IBM Security Privileged Identity Manager are done in the Initial Configuration wizard, by using the web user interface, to get the virtual appliance working.

### Before you begin

- Configure the initial virtual appliance settings.
- Collect the following information that is associated with the tasks you are about to do:
  1. Setup mode selection  
Choose **Guided** or **Advanced**. If **Advanced**, then supply a file with all configuration details in the required format.
  2. Session recording activation code
  3. Root CA or signer certificate configuration
  4. Mail server configuration
  5. Database server configuration
  6. Directory server configuration

### Procedure

1. In a web browser, type the host name of the configured virtual appliance in the following format.  
*https://host name of the virtual appliance*  
  
For example: `https://pimval.jk.example.com`
2. Log on to the IBM Security Privileged Identity Manager Virtual Appliance with the administrator credentials.
  - **Configured login:** admin
  - **Password:** admin
3. Choose a configuration mode and then click **Next page**.

Option	Description
<b>Guided Configuration</b>	Define the configuration details a step at a time with the wizard.  To continue, go to step 4.
<b>Advanced Configuration</b>	Define the configuration by using a properties response file that contains the necessary predefined values for the configuration parameters.  After you upload the response file, continue to step 9 on page 25.

4. In the **Session Recording Configuration** page, take one of the following actions, and then click **Next page**:
  - If you want to enable the session recording feature, enter the activation key.

**Note:** If you do not enter the activation key at this stage, you can enter the activation key afterward. The session recording feature is not enabled until you enter the activation key.

- If you do not plan to use the session recording feature or do not have a session recording activation key, skip to the next page.
5. Optional: In the **Root CA Configuration** page, take one of the following actions, and click **Next page**.

**Note:** You might want to use this step to create and use a stand-alone virtual appliance and want to change the own signer certificate. If you plan to set up a cluster of virtual appliances, you can upload the correct Root CA certificate on the Load Balancer.

- To use the default SSL certificate, review the default details that are generated by the virtual appliance.
- To define your own signer certificate, click **Update**.

**Common Name**

(Mandatory) Specify the common name or domain name of the certificate owner. This field is a mandatory attribute. For example: jk.example.com

**Organization**

(Mandatory) Organization of the certificate owner.

**Organizational Unit**

(Optional) Organization Unit of the certificate owner.

**Locality**

(Optional) Locality name of the certificate owner.

**State/Province**

(Optional) State or province of the certificate owner.

**Zipcode**

(Optional) Postal code for the locality of the certificate owner.

**Country or region**

(Mandatory) Country or region of the certificate owner.

6. Configure the mail server and click **Next page**.
7. Configure the database settings for the following data stores and click **Next page**.

- Identity
- Single Sign-On
- Session Recording

For more information about the database settings, see Table 13 on page 52.

8. Configure the directory server and click **Next page**.
9. On the **Completion Setup** page, complete the following tasks that depend on the configuration mode you selected.
  - **Guided Configuration:** Review the instructions and click **Complete Setup** to complete the configuration process.

**Important:** When the configuration process begins, do not refresh the page or close the browser session.

- **Advanced Configuration:** Review the instructions and click **Start Configuration** to begin the configuration process.

After the configuration completes, a link to restart the virtual appliance is displayed. If the mail server configuration setup is correct, an email notification is sent when the virtual appliance configuration is complete.

10. Click the restart link to restart the IBM Security Privileged Identity Manager Virtual Appliance.

**Note:** Check the restart status in the VMware client console.

## Setting up an IBM Security Privileged Identity Manager Member node from the Initial Configuration wizard

The initial configuration tasks for IBM Security Privileged Identity Manager are done in the Initial Configuration wizard by using the web user interface to get the virtual appliance working. The Initial Configuration wizard configures the virtual appliance.

### Before you begin

Configure the initial virtual appliance settings.

### About this task

In a web browser, log on to the Initial Configuration wizard from the web user interface after you complete the virtual appliance logon configuration. Complete the virtual appliance setup tasks from either the command line or the IBM Security Privileged Identity Manager Virtual Appliance management user interface.

Use the **Set up a Member node for the IBM Security Privileged Identity Manager cluster** option to set up a Member node.

### Procedure

1. In the **Connect to Primary** tab of the Setup Progress page, provide the details of the Primary node.
  - a. Type the host name in the **Primary node host name** field. For example, pimval.jk.example.com.

The Primary node host name must be same that was used to create the Primary virtual appliance host name. That is, the value in the **Issued To** field of the Primary node host name must match with the value that you entered in the **Primary node host name** field of the **Connect to Primary** tab.

- b. Type the user ID in the **Primary node administrator** field. The user ID must be the same ID that you used to log on to the IBM Security Privileged Identity Manager Virtual Appliance. For example, admin.
  - c. Type the password in the **Primary node administrator password** field. For example, admin.
2. Click **Test Connection** to validate the details and to verify this connection of the Member node with the Primary node. The system notifies that the connection to the Primary node was successful.
3. Click **Next page**.

**Note:** The **Next page** button is activated only when the connection to the Primary node is successful.

The **Completion** tab is displayed.

4. Click **Fetch Configuration** to obtain configuration details from the Primary node. A progress bar indicates about fetching the configuration details from the Primary node. The **Start Configuration** button is activated only when the **Fetch Configuration** operation is completed successfully.
5. Optional: To review or edit the data in the **Connect to Primary** tab, click **Previous page**.
6. Click **Start Configuration** to start the initial configuration for the IBM Security Privileged Identity Manager Virtual Appliance. The Completion page opens to indicate the data synchronization process. Do one of these actions:
  - If the configuration is successful, a message indicates to restart the IBM Security Privileged Identity Manager Virtual Appliance. See “Restarting or shutting down” on page 40.
  - If the configuration is not complete or not successful, a message indicates the reason. Do one of the following actions:
    - Click the **log files** link to open the Log Retrieval and Configuration page and check for any messages and errors in the log files.
    - Click the **Click here** link to restart the configuration process in case of failures.

---

## Logging on to the consoles from the Appliance Dashboard

You can log on to the administrative consoles from the **Appliance Dashboard** and only from a stand-alone node. The administrative console links that you can view in the **Appliance Dashboard** are **Identity and Credential Vault Administration**, **Single Sign-On** and **Session Recorder Administration**, and **Session Replay Console**.

### Procedure

1. Log on to the **Appliance Dashboard**. In a web browser, type `https://pimva_hostname`. For example: `https://ispimva.example.com`.
2. In the Quick Links panel, go to the consoles for an application.

**Note:**

- The default user ID is pim manager and password is secret. Log on to **Identity and Credential Vault Administration** console and change the password before you start any operations.



- To allow a new user to access the IBM Privileged Session Recorder console, add the user into the **Session Recorder Auditor** group in the IBM Security Identity Manager. Click the **Identity and Credential Vault Administration** link.



---

## Chapter 3. Appliance Dashboard

The **Appliance Dashboard** provides important status information, statistics, and quick links to the administrative consoles.

---

### Viewing notifications

You can view warning information about potential problems and required actions with the **Notification** dashboard widget.

#### Procedure

1. From the **Appliance Dashboard**, locate the **Notifications** widget. Warning messages about potential problems and expected actions are displayed as follows:

Identity service restart required  
SingleSignOn service restart required  
SessionRecorder service restart required  
Appliance restart required  
Middleware components not configured  
The disk space utilization has exceeded the warning threshold.  
Synchronize the current Member node with the Primary node.  
Reconnect the current Member node with the Primary node.

2. Take appropriate actions as required. For example:

If the following warning messages are displayed, restart the identity service by using the option that is provided in the **Server Control** widget.

Identity service restart required  
SingleSignOn service restart required  
SessionRecorder service restart required

If a message for the **Appliance Dashboard** restart is displayed, restart the virtual machine from the vSphere console. This condition occurs only if you did not restart after your first configuration.

---

### Viewing the cluster status

You can view a list of all the nodes in the cluster on the Cluster Status widget of the **Appliance Dashboard**.

#### About this task

You can view the Cluster Status widget only on a cluster node.

The Cluster Status widget is displayed only when you are in a cluster setup. In a stand-alone environment, the widget is not displayed.

#### Procedure

1. On the **Appliance Dashboard**, locate the **Cluster Status** widget.

If the Cluster Status widget is not displayed on the **Appliance Dashboard**, select **Dashboard > Cluster Status** and click **Save**.

The Cluster Status widget displays the following table columns:

##### Host Name

Displays the host name of a node in the cluster. Click the host name of

a node to open the **Appliance Dashboard** in a separate web browser. A node with no link indicates that it is the same node that you are working from.

**Role** Displays the role of the node in the cluster.

**Primary**

Indicates that the node is Primary.

**Member** Indicates that the node is Member.

**Status** Displays the status of the node in the cluster.

**Available**

It indicates that the node is available for your business requirement.

**Not Available**

It indicates that the node is not available for your business requirement.

**Note:** If the status of a node is displayed as Not Available, you can still click the host name link to start the **Appliance Dashboard**.

**Undetermined**

It indicates that the status of the node cannot be determined.

**Synchronization State**

Displays the synchronization state of the node in the cluster. For more information, see the following table.

Table 12. Synchronization states table.

State	Description	Action
Not Connected	Displays when a Member node cannot connect to a Primary node or when a Primary node cannot connect to the Member node.	Connect the Member node with the Primary node.  For a node with the Not Connected status, click <b>Reconnect Node</b> to connect that node into the cluster.  See “Reconnecting a node into the cluster” on page 59.
Not Synchronized	Displays when the Member node is not synchronized with the Primary node.	Synchronize the Member node with the Primary node. See “Synchronizing a Member node with a Primary node” on page 60.
Synchronized	Displays when the Member node is synchronized with the Primary node.	No action is required.
Synchronizing	Displays when the Member node is synchronizing with the Primary node.	Wait until the synchronization is complete. Click the <b>Refresh</b> icon to get the most recent status.
Not Applicable	Displays if the cluster node is a Primary node because the Primary node does not require any synchronization.	No action is required.

Table 12. Synchronization states table. (continued)

State	Description	Action
Error	Displays when the action fails to retrieve synchronization details for the node.	Check log files for more information.

- Optional: Click the **Refresh** icon to display the updated data again.

---

## Viewing and using server controls

You can view the status and control different components in the system by using the **Server Control** widget.

### Procedure

- From the **Appliance Dashboard**, locate the **Server Control** widget.
- Do one of the following actions:
  - Stop** Stops all the server components.
  - Start** Starts all the server components.
  - Restart** Restarts the server as per the requirement.
- Optional: Click **Refresh** to display the data again.

---

## Viewing deployment statistics

You can view information about number of users, groups, services, credentials, and credential pools in the system by using the **Deployment Statistics** widget.

### Procedure

- From the **Appliance Dashboard**, locate the **Deployment Statistics** widget. The first row displays the type of entity. The second row displays the number of entities that exist in the system.
- Optional: Click **Refresh** to display the data again.

---

## Viewing the middleware and server monitor widget

The health status of a server is determined by the state of the middleware and services. You can view the health status information with the **Middleware and Server Monitor** dashboard widget.

### Procedure

- From the **Appliance Dashboard**, locate the **Middleware and Server Monitor** widget.
- Optional: Click **Refresh** to display the data again.

---

## Viewing and using quick links

You can view the links for accessing the administration console application. This option is provided mainly for an appliance Administrator to validate the success of IBM Security Privileged Identity Manager configuration.

## About this task

You can view the **Quick Links** widget only on a stand-alone node.

### Procedure

1. From the **Appliance Dashboard**, locate the **Quick Links** widget. The various links are as follows:
  - Identity and Credential Vault Administration
  - Single Sign-On and Session Recorder Administration
  - Session Replay Console
2. Click a quick link to view and use for your requirement.

---

## 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 **Appliance Dashboard**, locate the **Disk Usage** widget. The disk usage statistics are displayed.

#### Disk Space Pie Chart

Information about used disk space and free disk space is visualized in the pie chart.

#### Consumed Disk Space

Displays 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 virtual appliance to store log and trace files on a remote server. You can also clear unused log and trace files on a periodic basis.

#### Free Disk Space

Displays how much space (in GB) is available.

#### Total Disk Space

How much space in total (in GB) is available to the virtual appliance.

**Note:** The disk space in a hardware appliance is limited by the capacity of the hard disk drive it holds.

2. Optional: Click **Refresh** to display the data again.

---

## Viewing IP addresses

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

### Procedure

1. From the **Appliance Dashboard**, locate the **Interfaces** widget. The IP address is displayed.
2. Optional: Click **Refresh** to display the data again.

---

## Viewing partition information

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

### Procedure

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

#### Firmware version

Displays the version information about the virtual appliance firmware. For example, 1.0.1.1.

#### Installation date

Displays the date on which the virtual appliance firmware was installed. For example, Oct 16, 2013 8:15:51 PM.

#### Installation type

Displays the type of the virtual appliance firmware installation. For example, ISO.

#### Last boot

Displays the time when the virtual appliance was last booted. For example, Oct 16, 2013 8:19:40 PM.

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

---

## Viewing the update history

View the update history to see a which firmware and security content updates are downloaded, installed, and rolled back on the IBM Security Privileged Identity Manager Virtual Appliance.

### About this task

After you install an update, the update package is deleted from the IBM Security Privileged Identity Manager Virtual Appliance.

### Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > Updates and Licensing > Update History**. The Update History page is displayed.
2. Optional: Click **Refresh** to display the data again.

---

## Viewing the licensing

View the licensing to see the service agreement that you accepted when you installed the IBM Security Privileged Identity Manager Virtual Appliance.

### About this task

A service agreement defines the agreement and formal commitments about the IBM Security Privileged Identity Manager Virtual Appliance.

### Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > Updates and Licensing > Licensing**. The Licensing page is displayed.

2. Click **Service Agreement** to view the service agreement in the Software License Agreement page.

---

## Managing the firmware settings

The IBM Security Privileged Identity Manager Virtual Appliance has two partitions with separate firmware on each partition. Partitions are swapped during firmware updates so that you can roll back the firmware updates.

### About this task

Either partition can be active on the IBM Security Privileged Identity Manager Virtual 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 IBM Security Privileged Identity Manager Virtual Appliance restarts the system by using partition 2, which is now the active partition.

**Note:** The IBM Security Privileged Identity Manager Virtual 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. From the top-level menu of the **Appliance Dashboard**, click **Manage > Updates and Licensing > Firmware Settings**. The Firmware Settings page is displayed.
2. On the Firmware Settings page, do one or more of the following actions.

Option	Description
<b>Edit</b>	Select the partition and click <b>Edit</b> to revise the partition comment.
<b>Create Backup</b>	<p><b>Important:</b> Create a backup of your firmware only when you are installing a fix pack that is provided by IBM Customer Support.</p> <p>Fix packs are installed on the active partition and you might not be able to uninstall the fix pack.</p> <p><b>Note:</b> The backup process can take several minutes to complete.</p>
<b>Set Active</b>	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 to active, the IBM Security Privileged Identity Manager Virtual Appliance restarts the system by using the newly activated partition.

---

## Installing a fix pack

Install a fix pack on the IBM Security Privileged Identity Manager Virtual Appliance to address software maintenance updates for reliability and performance enhancements.



## Before you begin

**Restriction:** You cannot uninstall a fix pack by using the local management interface. You must use the command-line interface to uninstall a fix pack.

Fix packs are applied to your active partition. You can manually create a backup of your active partition before you apply a fix pack so that you can roll back your changes.

## About this task

If a fix pack is installed on your IBM Security Privileged Identity Manager Virtual Appliance, you can view information about who installed the fix pack, comments, patch size, and the installation date.

## Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > Updates and Licensing > Fix Packs**. The Fix Packs page is displayed.
2. On the Fix Packs page, click **New**.
3. In the Add Fix Pack window, click **Browse for fix pack** to locate the fix pack file.
4. Select the fix pack file, and click **Open**. The Browse for fix pack table displays the fix pack details.
5. Click **Save Configuration** to install the fix pack.

---

## Viewing the About page information

View the About page to learn more about IBM Security Privileged Identity Manager Virtual Appliance and its content.

## Procedure

1. From the **Appliance Dashboard** top-level menu, click **Manage > Maintenance > About**.
2. View the product-specific information for the IBM Security Privileged Identity Manager Virtual Appliance.

## Results

The following information is displayed in the About page:

```
Product Name: IBM Security Privileged Identity Manager
Product Version: 1.0.1.1
Server Name: fitval.in.ibm.com
Installed Fix Packs: None
Build number: 20140224-1328
Build Date and Time: Feb 25, 2014 1:32:57 AM
```

The About page items are described as follows.

### Product Name

Displays the name of product that you are using.

### Product Version

Displays the version of product that you are using.

### Server Name

Displays the server name.

**Installed Fix Packs**

Displays the last fix pack level that was installed for the version of the product that you are using.

**Build number**

Displays the current build number for the version of the product that you are using.

**Build Date and Time**

Displays the date and the exact time and the time zone on which the last build occurred.

**What to do next**

Read the IBM Security Privileged Identity Manager Virtual Appliance product information to determine how it can be useful in your work.

## Viewing the memory utilization

View the memory graph to see the memory that is used by the IBM Security Privileged Identity Manager Virtual Appliance.

**Procedure**

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > System Graphs > Memory**. The System Memory Statistics page is displayed.
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 area, select **Memory Used** to review the total used memory.

## Viewing the CPU utilization

View the CPU graph to see the CPU that is used by the IBM Security Privileged Identity Manager Virtual Appliance.

**Procedure**

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > System Graphs > CPU**. The System CPU Statistics page is displayed.
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.

- In the Legend area, select the following options to review the CPU data.

**User CPU**

Indicates the CPU use by the user.

**System CPU**

Indicates the CPU use by the system.

**Idle CPU**

Indicates the idle use of the CPU.

---

## Viewing the storage utilization

View the storage graph to see the percentage of disk space that is used by the boot and root partitions of the IBM Security Privileged Identity Manager Virtual Appliance.

### Procedure

- From the top-level menu of the **Appliance Dashboard**, click **Manage > System Graphs > Storage**. The Storage Statistics page is displayed.
- 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.

- In the Legend area, select which partitions that you want to review.

**Boot** Indicates the boot partition.

**Root** Indicates the base file system, where the system user is root.

---

## Configuring the date and time settings

Use the Date/Time page to configure the date, time, time zone, and NTP server information of the IBM Security Privileged Identity Manager Virtual Appliance.

### Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > System Settings > Date/Time**. The Date/Time page is displayed.
2. Configure the following options on the Date/Time page.

Option	Description
<b>Date</b>	Specifies the day, month, and year for the IBM Security Privileged Identity Manager Virtual Appliance.
<b>Time</b>	Specifies the time for the IBM Security Privileged Identity Manager Virtual Appliance.
<b>Time Zone</b>	Specifies the time zone for the IBM Security Privileged Identity Manager Virtual Appliance.
<b>NTP Server address</b>	Select <b>Enable NTP</b> to list the NTP (NIST Internet Time Service) servers that the IBM Security Privileged Identity Manager Virtual Appliance uses. You can enter multiple NTP servers, which are separated by commas.

**Note:** You cannot set the **Time Zone** or **Date/Time** by using the SiteProtector™ System console. You can specify only NTP server addresses.

3. Click **Save Configuration**.
4. Optional: Click **Reset** to set the configuration again or differently.

---

## Configuring the administrator settings

Use the administrator settings to change the password that you use to access your IBM Security Privileged Identity Manager Virtual Appliance. Use the settings to also access the length of idle time that is granted to pass before your session times out.

### Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > System Settings > Administrator Settings**. The Administrator Settings page is displayed.
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 amount of time that you are allowed to be idle before you are automatically logged out.
6. Click **Save Configuration**.

---

## Managing the snapshots

Use snapshots to restore prior configuration and policy settings to the IBM Security Privileged Identity Manager Virtual Appliance.

### About this task

Snapshots are stored on the IBM Security Privileged Identity Manager Virtual Appliance. However, you can download the snapshots to an external drive in case of system failure.

### Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > System Settings > Snapshots**. The Snapshots page is displayed.
2. On the Snapshots page, do one or more of the following actions.

Option	Description
<b>New</b>	To create a snapshot, click <b>New</b> , type a comment to describe the snapshot, and then click <b>Submit</b> .
<b>Edit</b>	To edit the comment for a snapshot, select the snapshot, click <b>Edit</b> , type a new comment, and then click <b>Submit</b> .
<b>Delete</b>	To delete snapshots, select one or more snapshots, and then click <b>Delete</b> .
<b>Apply</b>	To apply a snapshot, select the snapshot, and then click <b>Apply</b> . <b>Note:</b> 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.
<b>Download</b>	To download a snapshot, select the snapshot, click <b>Download</b> , browse to the drive where you want to save the snapshot, and then click <b>Save</b> . <b>Note:</b> If you download multiple snapshots, the snapshots are compressed into a .zip file.
<b>Upload</b>	To upload snapshots, click <b>Upload</b> , browse to the snapshots you want to upload, select the snapshots, and then click <b>OK</b> . <b>Note:</b> You can upload only one snapshot at a time.
<b>Refresh</b>	To refresh the list of snapshots, click <b>Refresh</b> .

---

## Managing the support files

IBM Customer Support uses support files to help you troubleshoot problems with the IBM Security Privileged Identity Manager Virtual 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 do not contain confidential information, such as passwords, certificates, and keys. All files inside a support file contain text that can be inspected and censored by the customer.

The support file contents are stored in a .zip file.

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

## Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > System Settings > Support Files**. The Support Files page is displayed.
2. On the Support Files page, do one or more of the following actions.

Option	Description
<b>New</b>	To create a support file, click <b>New</b> , type a comment to describe the support file, and then click <b>Submit</b> . A new support file is created on the IBM Security Privileged Identity Manager Virtual Appliance.
<b>Edit</b>	To edit the comment for a support file, select the support file, click <b>Edit</b> , type a new comment, and then click <b>Submit</b> .
<b>Delete</b>	To delete a support file, select the support file, and then click <b>Delete</b> .
<b>Download</b>	To download support files, select the support files, click <b>Download</b> , browse to the drive where you want to save the support files, and then click <b>Save</b> . <b>Note:</b> If you download multiple support files, the files are compressed into a .zip file.

---

## Restarting or shutting down

Use the Restart or Shutdown page to restart or shut down the IBM Security Privileged Identity Manager Virtual Appliance.

### Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > System Settings > Restart or Shut down**. The Restart or Shutdown page is displayed.
2. Do one of the following tasks.

Option	Description
<b>Restart</b>	Restarting the IBM Security Privileged Identity Manager Virtual Appliance takes it offline for several minutes.
<b>Shut Down</b>	Shutting down the IBM Security Privileged Identity Manager Virtual Appliance takes it offline and makes it inaccessible over the network until you restart it.

---

## Chapter 4. IBM Security Privileged Identity Manager Virtual Appliance command line interface

Access the command line interface (CLI) of the virtual 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 by 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 virtual appliance.

```
usernameA@example.com> ssh -l admin pimva.example.com
admin@pimva.example.com's password:
Welcome to the IBM Security Privileged Identity Manager appliance
Enter "help" for a list of available commands
pimva.example.com> ispm
pimva.example.com:ispm> help
Current mode commands:
firmware_update    Work with the ISPIM firmware settings.
service_properties Work with the ISPIM properties settings.
service_trace      Work with the ISPIM trace 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.
pimva.example.com:ispm>
```

You can also access the console by using the appropriate VMware software. For example, VMware vSphere Client.

**Note:** The CLI contains only a subset of the function available from the graphical user interface.

---

### IBM Security Privileged Identity Manager Virtual Appliance command line interface commands for IBM Security Privileged Identity Manager

The initial virtual appliance settings wizard runs the first time that an Administrator logs on to the command line interface (CLI) of an unconfigured IBM Security Privileged Identity Manager Virtual Appliance. The topic provides information about the sub sections of the IBM Security Privileged Identity Manager Virtual Appliance CLI command that is specific to IBM Security Privileged Identity Manager.

The IBM Security Privileged Identity Manager Virtual Appliance CLI commands are broadly divided into the following main sections:

- Current mode commands
- Global commands

In the current mode commands, the **ispim** command is used to work with the IBM Security Privileged Identity Manager settings. When an Administrator or a user enters the **ispim** command, the following sub sections are listed.

## **firmware\_update**

The sub section provides options to work with IBM Security Privileged Identity Manager firmware updates.

### **delete\_firmware**

Deletes firmware updates from the system.

### **install\_firmware**

Installs the available firmware update to the system.

### **list\_firmware**

Lists firmware updates from a USB device.

### **transfer\_firmware**

Transfers firmware update from a USB device to the system.

## **service\_properties**

The sub section provides options to change the properties of the services.

You can see the list of modifiable properties at [http://www.ibm.com/support/knowledgecenter/SSRMWJ\\_6.0.0.2/com.ibm.isim.doc\\_6.0.0.2/reference/ref\\_ic\\_props\\_supp\\_table.htm](http://www.ibm.com/support/knowledgecenter/SSRMWJ_6.0.0.2/com.ibm.isim.doc_6.0.0.2/reference/ref_ic_props_supp_table.htm). Use the IBM Security Privileged Identity Manager Virtual Appliance CLI for the properties that are not available in the graphical user interface.

### **list\_properties**

Lists all the properties added through CLI.

### **add\_property**

Adds a property that is managed through CLI.

### **update\_property**

Updates an existing property added through CLI.

### **list\_syslog**

Lists all the values of syslog properties.

### **update\_syslog**

Updates the values of syslog properties.

## **service\_trace**

The sub section provides options to manage the log levels for the services. This sub section is provided for the troubleshooting.

### **add\_trace**

Adds a service trace level that is managed through CLI.

### **list\_trace**

Lists all the service trace level added through CLI.

### **update\_trace**

Updates a service trace level added through CLI.



## coredump

The sub section provides options to manage the core dump files. This sub section is provided for the troubleshooting.

### delete\_coredump

Deletes the core dump files.

### list\_coredump

Lists all the core dump files.

---

## Cleaning core dump files

You can clean core dump files through the command-line interface in the IBM Security Privileged Identity Manager Virtual Appliance.

### About this task

To see a list of available commands, enter the `help` command at the command-line prompt. The `help` command provides detailed information about each command from the list.

### Procedure

1. From the command-line interface, log on to the IBM Security Privileged Identity Manager Virtual Appliance.

For example:

```
usernameA@example.com> ssh -l admin pimvasrv
admin@pimvasrv's password: admin
```

The following message is displayed:

```
Welcome to the IBM Security Privileged Identity Manager appliance
Enter "help" for a list of available commands
```

2. Enter the `help` command at the `pimvasrv` prompt for a list of available commands. The following result is displayed:

```
Current mode commands:
firmware          Work with firmware images.
fixpacks          Work with fix packs.
ispim             Work with the ISPIM settings.
license           Work with licenses.
management        Work with management settings.
snapshots         Work with policy snapshot files.
support           Work with support information files.
tools             Work with network diagnostic tools.
updates           Work with firmware and security updates.
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.
```

3. Enter the `ispim` command at the `pimvasrv` prompt.
4. Enter the `help` command at the `pimvasrv:ispim` prompt for a list of available commands. The following result is displayed:

```
Current mode commands:
coredumps        Work with the ISPIM service coredump files.
firmware_update  Work with the ISPIM firmware settings.
service_properties Work with the ISPIM properties settings.
service_trace    Work with the ISPIM trace 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.

```

5. Enter the `coredumps` command at the `pimvasrv:ispim` prompt.
6. Enter the `help` command at the `pimvasrv:coredumps` prompt for a list of available commands. The following result is displayed:

```

Current mode commands:
delete_coredump  Delete coredump files.
list_coredump    List coredump files.
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.

```

7. For a detailed help on `list_coredump`, enter the `help list_coredump` command at the `pimvasrv:coredumps` prompt. The following result is displayed:

```

List of coredump files.
Usage: list_coredump

```

8. Enter the `list_coredump` command at the `pimvasrv:coredumps` prompt. The following result is displayed:

```

List of core dump files:
1: 4.0K /opt/IBM/TDI/core.2333.23442.22334.00004.dmp
2: 4.0K /opt/IBM/ispim/core.2333.23442.22334.00007.dmp
3: 4.0K /opt/IBM/wlp/lib/core.2333.23442.22334.00002.dmp
4: 4.0K /opt/IBM/wlp/core.2333.23442.22334.00009.dmp
5: 4.0K /opt/IBM/isamesso82/core.2333.23442.22334.00006.dmp
6: 4.0K /opt/IBM/WebSphere85/core.2333.23442.22334.00005.dmp
7: 4.0K /opt/IBM/HTTPServer/core.2333.23442.22334.00003.dmp

```

9. To get a detailed help on `delete_coredump`, enter the `help delete_coredump` command at the `pimvasrv:coredumps` prompt. The following result is displayed:

```

Delete coredump files.
Usage: delete_coredump

```

10. Enter the `delete_coredump` command at the `pimvasrv:coredumps` prompt. The following result is displayed:

```

1: /opt/IBM/TDI/core.2333.23442.22334.00004.dmp
2: /opt/IBM/ispim/core.2333.23442.22334.00007.dmp
3: /opt/IBM/wlp/lib/core.2333.23442.22334.00002.dmp
4: /opt/IBM/wlp/core.2333.23442.22334.00009.dmp
5: /opt/IBM/isamesso82/core.2333.23442.22334.00006.dmp
6: /opt/IBM/WebSphere85/core.2333.23442.22334.00005.dmp
7: /opt/IBM/HTTPServer/core.2333.23442.22334.00003.dmp
8: Delete All

```

11. Do one of the following actions.

- Enter the index number for the core dump file that you want delete. For example, specify 1 at **Enter index**.

The following message is displayed:

```
Are you sure you want to delete this core dump file?
```

- Type the input as **YES** to confirm and delete the core dump file that you want to delete. The following message is displayed:

```
The core dump file '/opt/IBM/TDI/core.2333.23442.22334.00004.dmp' is deleted.
```

- Enter the index number for the **Delete All** option to delete all the core dump files. For example, specify 8 at **Enter index**.

- Type the input as **YES** to confirm and delete one or all the core dump files. The following message is displayed:

```
The core dump files were deleted.
```

## Example

The following example shows the entire transcript to delete one or all the core dump files.

```
usernameA@example.com> ssh -l admin pimvasrv
admin@pimvasrv's password:admin
Welcome to the IBM Security Privileged Identity Manager appliance
Enter "help" for a list of available commands
pimvasrv> help
Current mode commands:
firmware          Work with firmware images.
fixpacks          Work with fix packs.
ispim             Work with the ISPIM settings.
license           Work with licenses.
management        Work with management settings.
snapshots         Work with policy snapshot files.
support           Work with support information files.
tools             Work with network diagnostic tools.
updates           Work with firmware and security updates.
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.
pimvasrv> ispim
pimvasrv:ispim> help
Current mode commands:
coredumps        Work with the ISPIM service coredump files.
firmware_update Work with the ISPIM firmware settings.
service_properties Work with the ISPIM properties settings.
service_trace    Work with the ISPIM trace 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.
pimvasrv:ispim> coredumps
pimvasrv:coredumps> help
Current mode commands:
delete_coredump  Delete coredump files.
list_coredump    List coredump files.
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.
pimvasrv:coredumps> help list_coredump
List coredump files.
Usage: list_coredump
pimvasrv:coredumps> list_coredump
List of core dump files:
1: 4.0K /opt/IBM/TDI/core.2333.23442.22334.00004.dmp
2: 4.0K /opt/IBM/ispim/core.2333.23442.22334.00007.dmp
3: 4.0K /opt/IBM/wlp/lib/core.2333.23442.22334.00002.dmp
4: 4.0K /opt/IBM/wlp/core.2333.23442.22334.00009.dmp
5: 4.0K /opt/IBM/isamesso82/core.2333.23442.22334.00006.dmp
6: 4.0K /opt/IBM/WebSphere85/core.2333.23442.22334.00005.dmp
7: 4.0K /opt/IBM/HTTPServer/core.2333.23442.22334.00003.dmp
pimvasrv:coredumps> help delete_coredump
Delete coredump files.
Usage: delete_coredump
pimvasrv:coredumps> delete_coredump
1: /opt/IBM/TDI/core.2333.23442.22334.00004.dmp
2: /opt/IBM/ispim/core.2333.23442.22334.00007.dmp
3: /opt/IBM/wlp/lib/core.2333.23442.22334.00002.dmp
4: /opt/IBM/wlp/core.2333.23442.22334.00009.dmp
5: /opt/IBM/isamesso82/core.2333.23442.22334.00006.dmp
6: /opt/IBM/WebSphere85/core.2333.23442.22334.00005.dmp
7: /opt/IBM/HTTPServer/core.2333.23442.22334.00003.dmp
8: Delete All
Enter index: 1
Are you sure you want to delete all the core dump files from the system?
```

```

Enter 'YES' to confirm: YES
The core dump file '/opt/IBM/TDI/core.2333.23442.22334.00004.dmp' is deleted
pimvasrv:coredumps> delete_coredump
1: /opt/IBM/ispim/core.2333.23442.22334.00007.dmp
2: /opt/IBM/wlp/lib/core.2333.23442.22334.00002.dmp
3: /opt/IBM/wlp/core.2333.23442.22334.00009.dmp
4: /opt/IBM/isamesso82/core.2333.23442.22334.00006.dmp
5: /opt/IBM/WebSphere85/core.2333.23442.22334.00005.dmp
6: /opt/IBM/HTTPServer/core.2333.23442.22334.00003.dmp
7: Delete All
Enter index: 7
Are you sure you want to delete all the core dump files from the system?
Enter 'YES' to confirm: YES
The core dump files were deleted.
pimvasrv:coredumps> delete_coredump
No coredump files were found.
pimvasrv:coredumps>

```

## What to do next

You can do the following actions:

- View the existing list of core dump files.
- Delete some core dump files from the existing list.

---

## IBM Security Privileged Identity Manager Virtual Appliance command line interface commands

The IBM Security Privileged Identity Manager Virtual Appliance CLI commands are broadly divided into the two sections such as current mode commands and global commands. The topic provides information about the IBM Security Privileged Identity Manager Virtual Appliance CLI commands for the following functions.

The following list gives a high-level overview of the functions available from the command line interface.

### fixpacks

The function works with the fix packs. The corresponding task can be completed by using the graphical user interface. Navigate to **Manage > Updates and Licensing > Fix Packs**.

**install** Installs the available fix packs on the inserted USB device.

**list** Lists the available fix packs on the inserted USB device.

#### rollback

Uninstalls the most recently installed fix pack.

#### view\_history

Shows the installation history for all fix packs.

### license

The function works with the licenses.

### management

**dns** Works with the virtual appliance DNS settings.

#### hostname

Works with the virtual appliance host name.

## **interfaces**

Works with the management interface settings.

## **set\_password**

Sets the virtual appliance password.

## **snapshots**

The function works with the snapshots. The corresponding task can be completed by using the graphical user interface. Navigate to **Manage > System Settings > Snapshots**.

**Note:** You must restart the virtual appliance after you apply the snapshot.

**apply** Applies a policy snapshot file to the system.

**create** Creates a snapshot of current policy files.

**delete** Deletes a policy snapshot file.

## **download**

Downloads a policy snapshot file to a USB flash drive.

## **get\_comment**

Views the comment that is associated with a policy snapshot file.

**list** Lists the policy snapshot files.

## **set\_comment**

Replaces the comment that is associated with a policy snapshot file.

## **upload**

Uploads a policy snapshot file from a USB flash drive.

## **support**

The function generates the support files. The corresponding task can be completed by using the graphical user interface. Navigate to **Manage > System Settings > Support Files**.

**create** Creates a support information file.

**delete** Deletes a support information file.

## **download**

Downloads a support information file to a USB flash drive.

## **get\_comment**

Views the comment that is associated with a support information file.

**list** Lists the support information files.

## **set\_comment**

Replaces the comment that is associated with a support information file.

## **tools**

### **nslookup**

Queries internet domain name servers.

**ping** Sends an ICMP ECHO\_REQUEST to network hosts.

### **tracert**

Traces a packet from a computer to a remote destination. Shows the

required number of hops for a packet that is required to reach the destination and the duration of each hop.

---

## Enabling trace for the virtual appliance services

You can add a service trace level through the CLI. From the **Appliance Dashboard**, restart the relevant virtual appliance service such as Identity, SingleSignOn, or SessionRecorder, and examine the log files for the new debug or trace messages.

### Procedure

1. Log on to the virtual appliance.

For example:

```
usernameA@example.com> ssh -l admin pimva.example.com
admin@pimva.example.com's password:
```

The following message is displayed:

```
Welcome to the IBM Security Privileged Identity Manager appliance
```

2. Enter the `ispim` command at the `pimva.example.com` prompt.
3. At the prompt, enter the **help** command for a list of available commands.
4. Enter the `service_trace` command at the `pimva.example.com:ispim` prompt.
5. At the prompt, enter the **help** command for a list of available commands. The following sub sections are listed under `service_trace`:

#### **add\_trace**

Adds a service trace level.

#### **list\_trace\_history**

Lists the service trace level history.

#### **update\_trace**

Updates a service trace level.

6. From the list of available commands, enter the `add_trace` command at the `pimva.example.com:service_trace` prompt.
7. Type an index for the name of the service. For example, type the input as 2 at **Enter index** for SingleSignOn. The **Name of the service** can be as follows:
  - 1: Identity
  - 2: SingleSignOn
  - 3: SessionRecorder
8. Type the name of the package for the selected service at **Name of the package**. For example, `encentuate.*`.

**Note:** The value for the name of the package can be only a single package or component name. For example, `encentuate.*`. Adding another package by using the **add\_trace** command overwrites the current trace level setting.

9. Type an index to assign the value for the trace level of the package. For example, type the input as 8 at **Enter index** to assign `audit`. The values can be as follows:
  - 1: all
  - 2: finest
  - 3: finer
  - 4: fine
  - 5: detail
  - 6: config
  - 7: info
  - 8: audit

```
9: warning
10: severe
11: fatal
12: off
```

## Results

The property is updated with the new value. Complete these steps to apply the new settings:

1. Restart IBM Security Privileged Identity Manager to apply the new settings.
2. Enter the `list_trace` command at the `pimva.example.com:service_trace` prompt.

View the following information:

```
pimServiceName:SingleSignOn pimPackageName:encentuate.* pimTraceValue:audit
```

## What to do next

Update a service trace level. For example, update the Identity virtual appliance service.

1. Enter the `update_trace` command at the `pimva.example.com:service_trace` prompt.
2. Type an index to assign the value for the trace level of the package. For example, type the input as 7 at **Enter index** to update to `info`.

**Note:** The default value for the trace level is `info`.

The following example shows the transcript to set the trace level for the Identity service:

```
usernameA@example.com> ssh -l admin pimva.example.com
admin@pimva.example.com's password:
Welcome to the IBM Security Privileged Identity Manager appliance
Enter "help" for a list of available commands
pimva.example.com> ispidm
Enter "help" for a list of available commands
1) firmware_update      Work with the ISPIM firmware settings.
2) service_properties  Work with the ISPIM properties settings.
3) service_trace       Work with the ISPIM trace settings.
pimva.example.com:ispidm> service_trace
pimva.example.com:service_trace> help
Current mode commands:
add_trace              Add a new service trace level.
list_trace_history     List the service trace level history.
update_trace           Update an service trace level.
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.
pimva.example.com:service_trace> update_trace
Name of the service :
1: Identity
2: SingleSignOn
3: SessionRecorder
Enter index: 2
Name of the package : *
Value for the trace level :
1: all
2: finest
3: finer
```

```
4: fine
5: detail
6: config
7: info
8: audit
9: warning
10: severe
11: fatal
12: off
Enter index: 7
pimva.example.com:service_trace> list_trace
  pimServiceName:SingleSignOn pimPackageName:* pimTraceValue:info
pimva.example.com:service_trace>
```



---

## Chapter 5. Managing the virtual appliance

For your virtual appliance, you can work with settings such as the session recorder activation, feed file upload, data store configuration, directory server configuration, mail server configuration, customization of server properties, and log management and configuration.

To manage the configured virtual appliance, log on to the **Appliance Dashboard** at [https://pimva\\_hostname](https://pimva_hostname). For example: <https://pimval.jk.example.com>.

---

### Enabling the Session Recording feature in the virtual appliance

You can enable the Session Recording feature in the IBM Security Privileged Identity Manager Virtual Appliance to record privileged identity sessions for auditing, security forensics, and compliance.

#### Before you begin

By default, session recording is not activated in the IBM Security Privileged Identity Manager Virtual Appliance. If you purchased the IBM Privileged Session Recorder feature and want to enable it, you must have the activation key to complete this task.

#### About this task

This task covers only how to enable the feature in the virtual appliance.

To enable the session recording for AccessAgent, modify the `pid_recorder_enabled` policy in AccessAdmin.

#### Procedure

1. From the top menu, click **Manage > Session Recording Activation**.
2. Enter your activation key.
3. Click **Activate** to enable session recording.

---

### Managing the Database Server configuration

Use the Database Server Configuration page to configure the database server for the IBM Security Privileged Identity Manager Virtual Appliance.

#### Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure > Manage External Entities > Database Server Configuration**.
2. Click the **Configure** menu to configure the Identity data store, Single Sign-On data store, or the Session Recording data store according to the order by which they are displayed.

**Note:** The next data store in the **Configure** menu, Single Sign-On data store, is only activated after you configure the Identity data store. Likewise, the Session Recording data store is activated in the **Configure** menu after you configure the Single Sign-On data store.

3. Specify the data store configuration details.

Table 13. Data stores configuration options

If you choose to configure the following data store:	Description
Identity data store	<p><b>Host name</b> The name of the computer that hosts the data store. Example: pimidstore.example.com.</p> <p><b>Port</b> The data store service port. Example: 50000.</p> <p><b>Database Name</b> The name of the IBM Security Identity Manager database. Example: isimdb.</p> <p><b>Database Administrator ID</b> The user with database administrator privileges. Example: piminst. <b>Note:</b> During the database configuration for a virtual appliance, the user must be the database owner. For example, piminst. This database owner must be the same user who created the database.</p> <p><b>Database Administrator Password</b> The password for the user with database administrator privileges.</p>
Single Sign-On data store	<p><b>Host name</b> The name of the computer that hosts the data store. Example: pimidstore.example.com.</p> <p><b>Port</b> The data store service port. Example: 50000.</p> <p><b>Database Name</b> The name of the IBM Security Access Manager for Enterprise Single Sign-On database. Example: essodb</p> <p><b>Database Administrator ID</b> The user with database administrator privileges. Example: piminst. <b>Note:</b> During the database configuration for a virtual appliance, the user must be the database owner. For example, piminst. This database owner must be the same user who created the database.</p> <p><b>Database Administrator Password</b> The password for the user with database administrator privileges.</p>

Table 13. Data stores configuration options (continued)

If you choose to configure the following data store:	Description
Session Recording data store	<p><b>Host name</b> The name of the computer that hosts the data store. Example: pimidstore.example.com.</p> <p><b>Port</b> The data store service port. Example: 50000.</p> <p><b>Database Name</b> The name of the IBM Security Privileged Identity Manager database. Example: pimrecdb.</p> <p><b>Database Administrator ID</b> The user with database administrator privileges. Example: piminst. <b>Note:</b> During the database configuration for a virtual appliance, the user must be the database owner. For example, piminst. This database owner must be the same user who created the database.</p> <p><b>Database Administrator Password</b> The password for the user with database administrator privileges.</p>

4. Click **Save Configuration** to complete this task.

---

## Managing the Directory Server configuration

Use the Directory Server Configuration page to configure the directory server in the IBM Security Privileged Identity Manager Virtual Appliance.

### Before you begin

Complete the following tasks:

- “Installing and configuring the directory server” on page 14.
- Create the directory server DN location.

### Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure > Manage External Entities > Directory Server Configuration**.
2. Click **Configure**.
3. In the Directory Server configuration details pane, specify the expected variables.

Table 14. Directory or LDAP server configuration details

Field name	Description and examples
Host name	The name of the computer that hosts the directory server.  The acceptable formats for the host name are IPv4, FQDN, and IPv6  Example: pimldap.example.com
Port	The directory service port.  Example: 389
Principal DN	The principal distinguished name.  Example: cn=root
Password	The password for the directory server.
Organization name	The name of the enterprise or the organization.  Example: JK Enterprises
Default organization short name	The abbreviation or short form of the organization name.  Example: jke
IBM Security Privileged Identity Manager DN Location	The directory server DN location.  Example: dc=com

- Click **Save Configuration** to complete this task.

**Note:** The Directory Server configuration takes some time. Do not refresh or close the page. Wait for the configuration process to complete.

---

## Configuring the Load Balancer

Use the Load Balancer Configuration page to configure the Load Balancer with the IBM Security Privileged Identity Manager Virtual Appliance.

### Before you begin

You must work from the Primary node to configure or reconfigure the Load Balancer.

### About this task

Configure the Load Balancer to support the working of your cluster or to distribute the workload across a cluster.

The Load Balancer Configuration page contains these columns:

#### Load Balancer DNS

Displays the DNS of the Load Balancer.

#### Last modified on

Displays the date and time when the current Load Balancer DNS was last modified.

## Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure > Manage External Entities > Load Balancer Configuration** to open the Load Balancer Configuration page.
2. Click **Configure** to open the Load Balancer details pane.
3. Provide the value in the **Load Balancer DNS** field. For example, enter the value as `pimval.jk.example.com`.

**Note:** The DNS must be a valid and a fully qualified domain name.

4. Click **Save Configuration** to complete the configuration.
5. Optional: To reconfigure the Load Balancer, do the following steps.
  - a. Select the **Load Balancer DNS** record from the Load Balancer Configuration page.
  - b. Click **Reconfigure**.
  - c. Follow steps 3 and 4.

The Load Balancer is reconfigured with the IBM Security Privileged Identity Manager Virtual Appliance.

---

## Managing mail configuration

Use the Mail Server Configuration page to configure the email notifications for the IBM Security Privileged Identity Manager Virtual Appliance.

### Procedure

1. From the top menu, select **Configure > E-mail Server Configuration** to configure the Mail Server.
2. Follow the instructions on the page to complete the process.

---

## Managing the server properties

You can update the property values in the IBM Security Privileged Identity Manager Virtual Appliance to customize the IBM Security Identity Manager Server.

### Before you begin

You must be familiar with the property keys and values of the IBM Security Identity Manager supplemental property files before you do this task. See the *Supplemental property files* section of the IBM Security Identity Manager documentation for details: [http://www.ibm.com/support/knowledgecenter/SSRMWJ\\_6.0.0.2/com.ibm.isim.doc\\_6.0.0.2/reference/ref/ref\\_ic\\_props\\_supp.htm](http://www.ibm.com/support/knowledgecenter/SSRMWJ_6.0.0.2/com.ibm.isim.doc_6.0.0.2/reference/ref/ref_ic_props_supp.htm).

### Procedure

1. From the menu, select **Configure > Update Property**.
2. Select the property to update from the list, and click **Edit**.
3. Edit its property value and click **Save Configuration**.

You can customize following IBM Security Identity Manager properties:

Table 15. Available IBM Security Identity Manager properties in the IBM Security Privileged Identity Manager Virtual Appliance

Supplemental property files	Properties and values
adhocreporting.properties	<p>applyACIAtRuntime = false</p> <p>availableForNonAdministrators = true</p>
ReportDataSynchronization.properties	<p>accountSynchronizationStrategy = old</p> <p>accountSynchronizationStrategy = old</p> <p>authorizationOwnerSynchronizationStrategy = old</p> <p>groupSynchronizationStrategy = old</p> <p>organizationalContainerSynchronizationStrategy = old</p> <p>personSynchronizationStrategy = old</p> <p>roleSynchronizationStrategy = old</p> <p>serviceSynchronizationStrategy = old</p>
SelfServiceUI.properties	<p>enrole.ui.pageSize = 10</p> <p>enrole.ui.pageLinkMax = 100</p> <p>enrole.ui.maxSearchResults = 1000</p> <p>enrole.ui.maxSearchResults.users = 100</p>
enRole.properties	<p>enrole.connectionpool.incrementcount = 3</p> <p>enrole.connectionpool.initialpoolsize = 50</p> <p>enrole.connectionpool.maxpoolsize = 100</p> <p>enrole.connectionpool.protocol = plain ssl</p> <p>enrole.workflow.notifyoption = 1</p> <p>enrole.workflow.notifypassword = true</p> <p>enrole.workflow.notifyaccountsonwarning = false</p> <p>enrole.workflow.maxretry = 2</p> <p>enrole.workflow.retrydelay = 60000</p> <p>enrole.workflow.skipapprovalforrequester = false</p> <p>enrole.workflow.disablerequesteeapproval = false</p> <p>enrole.workflow.disablerequesterapproval = false</p> <p>enrole.workflow.skipfornoncompliantaccount = true</p> <p>enrole.reconciliation.accountcachesize = 2000</p> <p>enrole.reconciliation.threadcount = 8</p> <p>remoteservices.remotepending.restart.retry = 1440</p> <p>remoteservices.remote.pending.testing.max.duration = 1200</p> <p>enrole.CreatePassword = true</p> <p>enrole.accesscontrollist.refreshInterval = 10</p> <p>enrole.recyclebin.enable = false</p> <p>enrole.lifecyclerule.partition.size = 100</p>

Table 15. Available IBM Security Identity Manager properties in the IBM Security Privileged Identity Manager Virtual Appliance (continued)

Supplemental property files	Properties and values
ui.properties	enrole.ui.customerLogo.image = ibm_banner.gif enrole.ui.customerLogo.url = www.ibm.com enrole.ui.pageSize = 50 enrole.ui.pageLinkMax = 10 enrole.ui.maxSearchResults = 1000 enrole.ui.report.maxRecordsInReport = 5000 ui.challengeResponse.showAnswers = true ui.userManagement.includeAccounts = true ui.challengeResponse.bypassChallengeResponse = true ui.passwordManagement.generatePassword = true

---

## Managing feed files

You can upload feed files and use them in the IBM Security Privileged Identity Manager Virtual Appliance as long as you put them in the prescribed location.

### Procedure

1. From the menu, select **Configure > Upload Feed File**.
2. Click **New**.
3. Click **Browse** to search for the feed file to upload. The feed files are in /userdata/identity/feeds.

The /userdata/identity/feeds location is required while creating feed in IBM Security Identity Manager Console.

---

## Changing a Member node to a Primary node

Use the Cluster Node Configuration page to change a Member node to Primary node in the IBM Security Privileged Identity Manager Virtual Appliance.

### Before you begin

No active Primary node must exist in this cluster.

### About this task

You might want to change a Member node to a Primary node in the cluster for maintenance and other tasks.

The **Configure > Manage Cluster** menu is displayed only in a cluster environment and not in a stand-alone environment.

### Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure > Manage Cluster > Cluster Node Configuration**.
2. Select the Member node that you want to make as a Primary node from the list of available nodes.

3. Click **Make Primary**.
4. Click **Yes** to confirm the changes.

---

## Changing a Primary node to a Member node

Use the Cluster Node Configuration page to change a Primary node to Member node in the IBM Security Privileged Identity Manager Virtual Appliance.

### Before you begin

You must work from a Primary node to change it to a Member node.

### About this task

You might want to change a Primary node to a Member node due to the following reasons:

- Change the node in the cluster for maintenance and other tasks. To promote some other Member node to Primary node, you must first change the current Primary node to Member node.
- Remove a damaged or affected Primary node from the cluster configuration. You must first remove such affected node from the Load Balancer configuration.

The **Configure > Manage Cluster** menu is displayed only in a cluster environment and not in a stand-alone environment.

### Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure > Manage Cluster > Cluster Node Configuration**.
2. Select the Primary node that you want to make as a Member node from the list of available nodes.
3. Click **Make Member**.
4. Click **Yes** to confirm the changes.

---

## Removing a node from the cluster

Use the Cluster Node Configuration page to remove a node from the cluster.

### Before you begin

Remove the node from the Load Balancer configuration so that no user requests are routed to this node.

### About this task

You can remove a Member node only from a Primary node, but you cannot remove the Primary node itself.

You might want to remove a damaged or affected Primary node from the cluster configuration. You must first remove such affected node from the Load Balancer configuration. After the node is removed, it no longer functions as part of the cluster unless you add it back to the cluster.

The **Configure > Manage Cluster** menu is displayed only in a cluster environment and not in a stand-alone environment.



## Procedure

1. From the **Appliance Dashboard** top-level menu, click **Configure > Manage Cluster > Cluster Node Configuration**.
2. Select a Member node that you want to remove from the list of available nodes.
3. Click **Remove Node**.
4. Click **Yes** to confirm.

## Results

The selected node is removed from the cluster.

---

## Reconnecting a node into the cluster

Use the Cluster Node Configuration page to reconnect a node into the cluster of the IBM Security Privileged Identity Manager Virtual Appliance.

### About this task

Depending on your requirement, you can reconnect a node into the cluster due to the following reasons:

- Adding a previously configured node to a cluster to increase scalability.
- A node that was shut off for maintenance is revived and must be introduced back in the cluster.
- If you see a reconnect notification on the **Appliance Dashboard** of a Member node.

You can reconnect only a Member node back to the cluster from the **Appliance Dashboard** of a Member node. You must provide the Primary node details to reconnect a node into the cluster.

The **Configure > Manage Cluster** menu is displayed only in a cluster environment and not in a stand-alone environment.

## Procedure

1. From the **Appliance Dashboard** top-level menu, click **Configure > Manage Cluster > Cluster Node Configuration**.
2. Select the Member node.
3. Click **Reconnect Node**. The Reconnect Node pane is displayed.
4. In the Reconnect Node pane, provide the details for the node that you want to reconnect into the cluster.

### Primary node host name

The host name of the Primary node. For example, pimval.jk.example.com.

### Primary node administrator

The user ID of the Primary node administrator. For example, admin.

### Primary node administrator password

The administrator password of the Primary node. For example, admin.

5. Click **Yes** to confirm.

## Results

The Member node is reconnected into the cluster.

---

## Synchronizing a Member node with a Primary node

Use the Cluster Node Configuration page to synchronize a Member node with a Primary node in the IBM Security Privileged Identity Manager Virtual Appliance.

### About this task

The **Configure > Manage Cluster** menu is displayed only in a cluster environment and not in a stand-alone environment.

In the Primary node virtual appliance console, all nodes in the cluster are displayed in the Cluster Node Configuration table.

In the Member node virtual appliance console, only the current Member node is displayed in the Cluster Node Configuration table.

Synchronize the following nodes in the cluster for any configuration changes that you make in the IBM Security Privileged Identity Manager Virtual Appliance.

#### Member node

In the Cluster Node Configuration table of the Cluster Node Configuration page, select a Member node for synchronization. The **Synchronize** button is not active until you select a node.

Wait for the synchronization process to complete.

#### Primary node

In the Cluster Node Configuration page, select one or more Member nodes except the Primary node for synchronization. The **Synchronize** button is not active when:

- The Primary node is selected.
- The status of the selected node is displayed as **Synchronizing** in the **Synchronization State** column of the Cluster Node Configuration table.

The Primary node submits the synchronization request to each of the node that was selected. You can view the synchronization status in the **Synchronization State** column of the Cluster Node Configuration table.

**Note:** Before you do a synchronization operation, address all the notifications on the Primary node.

The **Synchronization State** column displays these synchronization states:

Table 16. Synchronization state table

Status	Description	Action
Not Connected	Displays when a Member node cannot connect to a Primary node or when a Primary node cannot connect to the Member node.	Connect the Member node with the Primary node.  For a node with the Not Connected status, click <b>Reconnect Node</b> to connect that node into the cluster.  See “Reconnecting a node into the cluster” on page 59.
Not Synchronized	Displays when the Member node is not synchronized with the Primary node.	Synchronize the Member node with the Primary node. See the following procedure.
Synchronized	Displays when the Member node is synchronized with the Primary node.	No action is required.
Synchronizing	Displays when the Member node is synchronizing with the Primary node.	Wait until the synchronization is complete. Click the <b>Refresh</b> icon to get the most recent status.
Not Applicable	Displays if the cluster node is a Primary node because the Primary node does not require any synchronization.	No action is required.

## Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure > Manage Cluster > Cluster Node Configuration**.
2. Do the following actions.
  - From the Member node console, select the current Member node and click **Synchronize** to synchronize it with the Primary node.  
A progress bar indicates the synchronization process. It retrieves configuration information from the Primary node for any configuration changes and synchronizes within the same node.
  - From the Primary node console, select one or more Member nodes and click **Synchronize**.  
A synchronization request is submitted to each of the node that was selected.

## Results

The Member node is synchronized with the Primary node.

---

## Managing log configuration

You can view component-specific and appliance log files to troubleshoot any appliance-related issues better. You can also configure the file size and settings of the log files in the Log Configuration page.

## Procedure

1. From the menu, select **Manage > Log Retrieval and Configuration**.
2. Select the product from the tabs to view the available logs.

3. Select **Configure** to set the file size and roll over settings for the selected log file.

## Retrieving logs

Use the Log Retrieval and Configuration page to view the log files. You can also use the page to configure the server log settings for the IBM Security Privileged Identity Manager Virtual Appliance.

### Procedure

1. From the top menu, select **Manage > Log Retrieval and Configuration**.
2. Take any of the following actions:
  - To display a log file, click **View**.
  - To save a log file, click **Download**.
  - To remove a log file, click **Clear**.
  - To display all the log files again, click **Refresh**.

Table 17. Available logs to help you diagnose or troubleshoot

Tab	Log File Name	Description
<b>Appliance</b>  These files help you to debug any configuration failures that occur in the virtual appliance.	Identity Data store configuration	Identity data store configuration log file.
	Session Recording Data store configuration	Privileged Session Recorder data store configuration log file.
	Directory Server information	IBM Security Privileged Session Recorder user registry configuration log file.
	Server System out	Appliance system output log file.
	Server Message	Appliance server message log file.
	Server Console	Appliance server console log file.
<b>Identity</b>  Helps you identify issues in the identity applications.	Server System out	Identity Server system output log file.
	Server System err	Identity Server system error log file.
	Application message	Identity application message log file.
	Application trace	Identity application trace log file.
<b>Single Sign-On</b>  Helps you identify issues in the single sign-on application.	Server System out	Single Sign-On Server system output log file.
	Server System err	Single Sign-On Server system error log file.

Table 17. Available logs to help you diagnose or troubleshoot (continued)

Tab	Log File Name	Description
<b>Session Recording</b> Helps you identify issues in the session recording application.	Server System out	IBM Privileged Session Recorder Server system output log file.
	Server System err	IBM Privileged Session Recorder Server system error log file.

## Configuring logs

You can configure different options to manage the quantity and size of the log files.

### Procedure

1. From the top menu, select **Manage > Log Retrieval and Configuration**.
2. To set the log settings, click **Configure**.
3. Provide the following details:

#### Maximum size for log file rotation

The size of the log file that you want to keep.

#### Maximum number of historical log files

The maximum number of historical log files that you want to keep.

4. Click **Save Configuration**.

---

## Reconfiguring the data store connection

You can reconfigure the data store if the data store configuration changes.

### Procedure

1. Make a backup of the database. On the database server that runs DB2 Universal Database™ for IBM Security Privileged Identity Manager, complete the following steps:

- a. Log on as the instance owner. For example: db2admin.
- b. Close all connections to the IBM Security Identity Manager database. Stop WebSphere Application Server or any other tools. If necessary, run the following command to force all connections to close:

```
db2 force application all
```

- c. Back up the data store database:

```
db2 backup database IDM_DB to OLD_DB2_BACKUP_DIR
```

where

IDB\_DB is the name of the IBM Security Privileged Identity Manager data store database. For example: idmdb

OLD\_DB2\_BACKUP\_DIR is a directory path to store the backup. For example:

#### Linux or UNIX systems

```
/tmp/db2
```

#### Windows systems

```
c:\temp\db2
```

2. Restore the backup of the database.

Install the new version of DB2 Universal Database. For this reconfiguration, ensure that you create the database instance and database with the same name. Users must have the same rights and privileges as those setup on the previous system.

To create a new database instance and a database, see “Installing and configuring the database server” on page 12.

Copy the contents of the IBM Security Privileged Identity Manager data store backup directory to the target server. For example: tmp/db2.

Ensure that the database instance owner you create has permission to read the target directory and files within.

To restore the DB2 Universal Database data on the target database server, complete the following steps:

- a. Launch DB2 command line.

#### Windows

- 1) Launch the Windows command line.
- 2) Run the following command:  
set DB2INSTANCE=piminst where piminst is the database instance.
- 3) Run **db2cmd** to launch the DB2 command line.

#### Linux

Run the command `su - piminst` where piminst is the database instance.

- b. In the DB2 command line, enter the following commands to restore the database by using the migrated DB2 data: `restore db idmdb from OLD_DB2_TEMP_DATA`

where

idmdb is the IBM Security Privileged Identity Manager data store database name.

OLD\_DB2\_TEMP\_DATA is the location of the migrated DB2 data that you copied over from the previous version. For example: `c:\temp\db2`

- c. Stop and start the DB2 server to reset the configuration.

After you create the IBM Security Privileged Identity Manager data store database, stop, and start the DB2 server to allow the changes to take effect.

Enter the following commands:

```
db2stop
```

```
db2start
```

**Note:** If the `db2stop` fails and the database remains active, enter the following command to deactivate the database:

```
db2 force application all
```

Then, enter `db2stop` again.

3. For the Identity data store, clear the **Service Integration Bus**.

For reconfiguration of the Identity data store, you must clear out the Service Integration Bus (SIB) from the restored database.

To clear out the **Service Integration Bus** on the target DB2 server, complete the following steps:

- a. Ensure that the IBM Security Identity Manager database is running (IDMDB).
- b. Launch the DB2 command line:

#### Windows

- 1) Launch the Windows command line.
- 2) Run the following command:  
`set DB2INSTANCE=piminst` where piminst is the database instance.
- 3) Run **db2cmd** to launch the DB2 command line.

#### Linux

Run the command `su - piminst` where piminst is the database instance.

- c. In the DB2 command line, enter the DELETE SQL statements that you require to delete all data from the tables in the Service Integration Bus schemas.

Enter the following commands for each of the Service Integration Bus schema in your environment:

```
db2 delete from schema_name.SIB000
db2 delete from schema_name.SIB001
db2 delete from schema_name.SIB002
db2 delete from schema_name.SIBCLASSMAP
db2 delete from schema_name.SIBKEYS
db2 delete from schema_name.SIBLISTING
db2 delete from schema_name.SIBXACTS
db2 delete from schema_name.SIBOWNER
db2 delete from schema_name.SIBOWNER0
```

where the Service Integration Bus schema, schema\_name is ITIML000.

**Note:** The SIMOWNER0 might not exist in all Identity data store environments. If it does not exist and the delete statement fails, you can ignore the failure.

4. Reconfigure the data store.
  - a. From the IBM Security Privileged Identity Manager administrative console, click **Menu > Database Configuration**.
  - b. Select the existing data store that you want to set up and click **Reconfigure**. Provide the details and click **Save Configuration**.
  - c. Restart the server for the corresponding data store to complete the process.

---

## Reconfiguring the directory server connection

You can reconfigure the directory server if the directory server configuration changes.

### Procedure

1. Make a backup of the directory server.

On the server running IBM Security Directory Server for IBM Security Privileged Identity Manager, complete the following steps:

- a. Log on as an Administrator with root privileges.
- b. Open a command window.
- c. Go to the `TDS_HOME/sbin` directory and type the following command:

```
db2ldif -s ldap_suffix -o ldap_output_file -I ldap_instance_name
```

where:

ldap\_suffix is the name of the suffix. For example: dc=com.

ldap\_output\_file is the name of the ldif output file. For example: old\_ldif\_data.ldif.

ldap\_instance\_name is the name of the LDAP server instance, which can be obtained through the IBM Security Directory Server Instance Administration tool.

- d. Use the backup of the schema file V3.modifiedschema from the OLD\_ITDS\_INSTANCE\_HOME\etc directory of the IBM Security Directory Server instance home directory.
2. Restore the backup of the database.

Install a version of IBM Security Directory Server that IBM Security Privileged Identity Manager supports. For this reconfiguration, ensure that you take the following actions:

- Create and use the same root suffix.
- Use the same encryption seed value as the old Directory Server instance. If not, you must export the data from the old Directory Server instance to use the seed and salt keys from the new instance.

Copy the contents of the IBM Security Privileged Identity Manager directory server backup ldif file and schema file to the target server.

To restore the directory server data on the target directory server, complete the following steps:

- a. Log on as an Administrator with root privileges.
- b. Stop the LDAP server.
- c. Copy the schema file V3.modifiedschema that you copied over from the previous server to the NEW\_ITDS\_INSTANCE\_HOME\etc directory of the IBM Security Directory Server instance.

**Note:** If you customized or modified the schema files, manually merge the changes into the new schema files.

- d. From TDS\_HOME/sbin, run the command:

```
bulkload -i OLD_ITDS_TEMP_DATA\ldif_output_file -I ldap_instance_name
```

where:

OLD\_ITDS\_TEMP\_DATA is the temporary directory location of the IBM Security Directory Server data you copied over from the previous server. For example, C:\temp\51data\ids\.

ldif\_output\_file is the name of the file that you exported in a previous task. For example, old\_ldif\_data.ldif

ldap\_instance\_name is the name of the LDAP server instance. For example, itimldap. You can obtain use the IBM Security Directory Server Instance Administration tool to obtain the instance name.

For more information, see “Bulkload command errors” on page 99.

- e. Stop and start the IBM Security Directory Server to activate the changes.

3. Reconfigure the IBM Security Directory Server.

- a. From the IBM Security Privileged Identity Manager administrative console, go to **Menu > Directory Server Configuration**.
- b. Select the directory server and click **Reconfigure**. Provide the details and click **Save Configuration**.
- c. Restart the Identity server to complete the process.



---

## Chapter 6. Configuration

To check out and check in shared credentials or to use session recording, complete the required configuration tasks. Some configuration tasks are optional depending on your deployment requirements.

---

### IBM Security Access Manager for Enterprise Single Sign-On configuration

AccessProfiles, and policy templates are required before automatic check-out and check-in can work.

Table 18 describes configuration tasks that you might want to complete, depending on the requirements of your deployment.

*Table 18. Single Sign-On configuration tasks*

Configuration task	Description
Configure a Windows Group Policy to prompt the client for passwords (RDP)	If you use a Remote Desktop Connection client for privileged access to a Windows host, configure the RDP policy to prompt for, not store, passwords.  See "Configuring a Windows Group Policy to prompt the client for passwords (RDP)" in the <i>IBM Security Privileged Identity Manager Deployment Overview Guide</i> for the detailed procedures.

---

### Shared access configuration

You can specify configuration settings for shared access as needed for your deployment. You can specify default settings for credentials, configure an external credential vault server, define a unique ID for a service, and customize several different operations.

Table 19 describes configuration tasks that you might want to complete, depending on the requirements of your deployment.

*Table 19. Shared access configuration tasks*

Configuration task	Description
Configuring the credential default settings	Specifies the default settings for each credential that is added to the credential vault.
Customizing the service form template to include the unique identifier (eruri) attribute	Updates the managed resource service form template to include a field for the unique identifier that you use to connect to the managed resource.
Customization of the checkout operation	The shared access module supports both synchronous and asynchronous checkout of shared accounts. Synchronous checkout is enabled by default. If you want to use asynchronous checkout, you must enable and configure it.

Table 19. Shared access configuration tasks (continued)

Configuration task	Description
Shared access approval and recertification	You can add an approval process to the default operation for adding credentials to the vault. You can also define a custom workflow to recertify credentials in the vault.
Customizing the checkout form	You can customize the form that is used for checkout of shared accounts. You can add more attributes to be filled out during checkout. This customization increases individual accountability when credentials are shared.
Shared access Tivoli® Common Reporting reports	You can configure reports that show: <ul style="list-style-type: none"> <li>• Shared access audit history</li> <li>• Shared access entitlements for a specified owner</li> <li>• Shared access entitlements for a specified role.</li> </ul>

Consult the IBM Security Identity Manager documentation to understand which configuration tasks apply to your deployment:

- Shared access documentation  
In the IBM Security Identity Manager documentation, see the “System configuration” section to find links to the documentation for shared access configuration tasks.
- IBM Security Identity Manager documentation  
To find information about a task in Table 19 on page 67, go to this documentation. On the home page, locate the documentation search field, and enter the configuration task name as shown in the “Configuration task” column of the table. For example, to use an external credential vault server, enter “Configuring an external credential vault server”.

---

## Session recording configuration

You can complete configuration tasks for session recording as needed for your deployment.

Learn about the configuration tasks that you might want to complete for your deployment with session recording.

Table 20. Session recording configuration tasks

Configuration task	Description
Configure IMS Server policies for session recording	<p>Configure the Privileged Session Recorder behavior through IBM Security Access Manager for Enterprise Single Sign-On AccessAdmin. For example, you can customize the following options:</p> <ul style="list-style-type: none"> <li>• Enable or disable session recording. (<b>pid_recorder_enabled</b>)</li> <li>• Specify the Privileged Session Recorder Server URL. (<b>pid_recorder_server</b>)</li> <li>• Capture recording in full color or in grayscale for smaller recordings. (<b>pid_recorder_image_capture_option</b>)</li> <li>• Enable or disable key logging. (<b>pid_recorder_keyboard_capture_option</b>)</li> <li>• Specify the action to take on the client computer when the Privileged Session Recorder Server is not available. (<b>pid_collector_comm_fail_action</b>)</li> </ul> <p>For more information about the policies for session recording, see "Policies for Privileged Identity Management" in the IBM Security Access Manager for Enterprise Single Sign-On product documentation.</p>
Add Session Recorder Auditors	<p>Use the IBM Security Privileged Identity Manager console to add members of security auditors to the 'Session Recorder Auditor' group to access the Privileged Session Recorder console.</p> <p>Members of the 'Session Recorder Auditor' group have privileges to view session recordings on the Privileged Session Recorder console.</p> <ol style="list-style-type: none"> <li>1. Install and configure the Privileged Identity Manager Server in the virtual appliance. See "Setting up the virtual machine" on page 18.</li> <li>2. Follow the procedure in "Adding members to groups" in the <i>IBM Security Identity Manager Administration Guide</i>.</li> </ol> <p><b>Note:</b> In this case, service is <b>ITIM Service</b> and group is <b>Session Recorder Auditor</b>.</p>
Modify AccessProfiles for session recording	<p>Modify the AccessProfile to customize its functions for specific client applications. Configure the AccessProfiles with Privileged Session Recorder widgets to add session recording support to custom applications.</p> <p>See "Modifying AccessProfiles" in the <i>IBM Security Privileged Identity Manager Administrator Guide</i>.</p>

Table 20. Session recording configuration tasks (continued)

Configuration task	Description
Configure IBM Privileged Session Recorder Tivoli Common Reporting reports	Configure Tivoli Common Reporting to show the IBM Privileged Session Recorder report.

## Optional configuration tasks

There are several optional configuration tasks for IBM Security Privileged Identity Manager.

Table 21 describes configuration tasks that you might want to complete, depending on the requirements of your deployment.

Table 21. Optional configuration tasks

Configuration task	Description
Create your own privileged identity management AccessProfiles	<p>You can use the IBM Security Privileged Identity Manager AccessProfile to start developing or enhancing your own privileged identity management scenarios.</p> <ol style="list-style-type: none"> <li>1. Install AccessStudio Version 8.2.1.</li> <li>2. Ensure that you have the Privileged Identity Management AccessProfiles. You can download the AccessProfiles from the AccessProfiles Library.</li> <li>3. In AccessStudio, open the sample AccessProfile.</li> <li>4. Build or enhance the Privileged Identity Management AccessProfile. For more information, see "Modifying AccessProfiles" in the <i>IBM Security Privileged Identity Manager Administrator Guide</i>.</li> <li>5. Debug and start your AccessProfile.</li> <li>6. Upload the AccessProfile to the IMS Server.</li> </ol>
Modify the checkout lease time expiry for shared access credentials	See "Configuring the credential default settings" in the <i>IBM Security Identity Manager Configuration Guide</i> .
Delete or merge copies of the AccessProfile	<p>Each application signature for an AccessProfile must be unique. Single sign-on cannot occur if there are multiple AccessProfiles with the same application signature on the IMS Server.</p> <p>If you have more than one AccessProfile for the same application, consider deleting or modifying copies of the AccessProfile.</p> <p>If you want both the privileged identity management AccessProfiles and the AccessProfiles you already have, then you must consider advanced AccessProfile merging. For help with advanced AccessProfile merging, contact IBM Services.</p>
Configuring or administering the IBM Tivoli Common Reporting	Use IBM Tivoli Common Reporting to view the shared access reports that are available from IBM Security Access Manager for Enterprise Single Sign-On and IBM Security Identity Manager.

## Load Balancer settings and requirements

A load balanced cluster provides not only the expected high availability for the IBM Security Privileged Identity Manager Virtual Appliance, but also provides scalability. High Availability means that a system can tolerate some failures and errors, but can remain operational.

Load Balancing is a technique to extend user requests between two or more virtual appliances in a predefined cluster. Each virtual appliance in this cluster is called a node. Use of multiple nodes in such a cluster increases reliability and availability through redundancy.

### Load Balancer requirements

The most common mechanism to make a highly available deployment is to add a Load Balancer that distributes user requests to underlying servers. This deployment locks down any direct access to individual servers. In addition to making a highly available deployment of the IBM Security Privileged Identity Manager Virtual Appliance, it also provides horizontal scalability. See Figure 1.

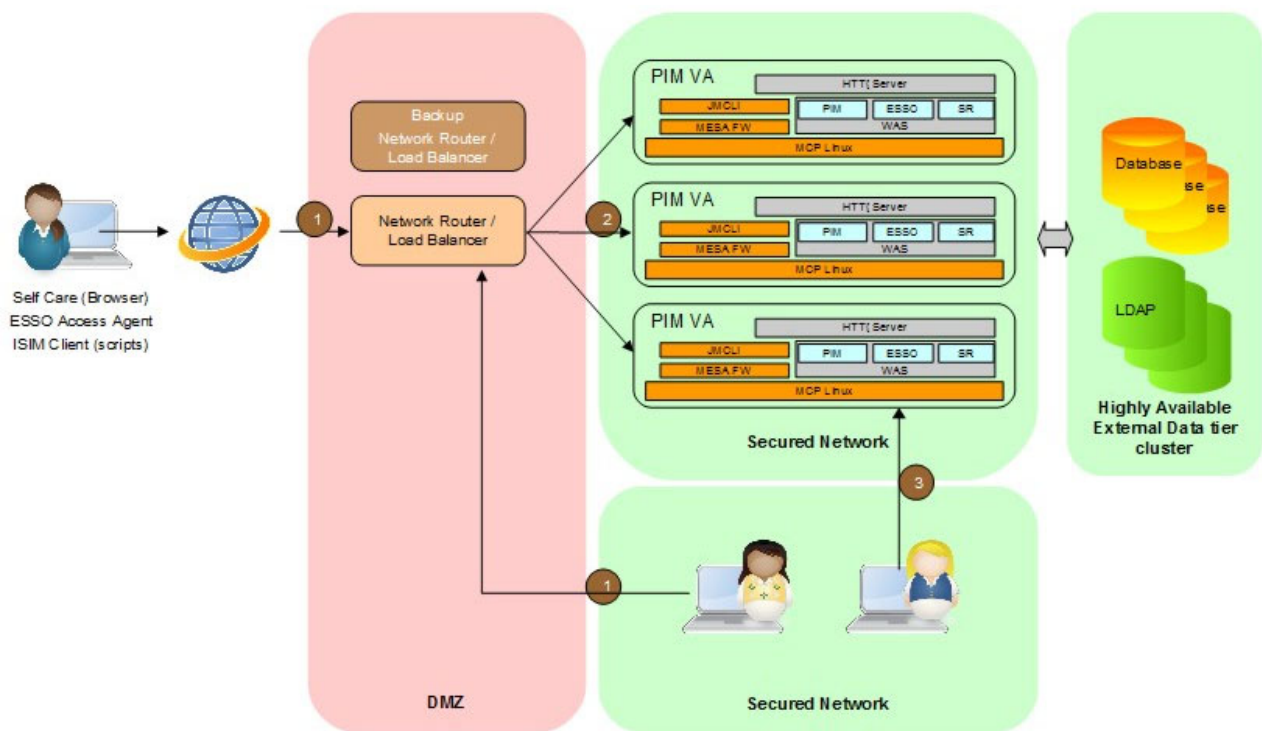


Figure 1. Deployment diagram of a typical Load Balancer in a customer environment

As shown in Figure 1, provide one or more backup Load Balancers or routers to avoid the Load Balancer itself from becoming a single point of failure.

The Load Balancer can be a dedicated hardware or software node that can route incoming requests to an IBM Security Privileged Identity Manager Virtual Appliance. This condition is true irrespective of whether the requests are coming from inside or outside a company network. See the request that is numbered as 1 in the diagram. Since these requests typically contain sensitive information such as

user IDs or passwords, both the traffic paths must be over SSL. For example, see requests 1 and 2. The client request over SSL (marked #1) ends at the Load Balancer and a new SSL request (marked #2) is sent to a virtual appliance.

## **Load Balancer installation requirements**

The Load Balancer must meet the following requirements:

- Choose Layer-7 Load Balancer for this installation. Layer-4 Load Balancers do not provide the required function and must not be used for this architecture.
- The Load Balancer must contain a valid SSL certificate for the IBM Security Access Manager for Enterprise Single Sign-On AccessAgent to connect. For a self-signed certificate, the Root CA certificate with which the Load Balancer certificate is signed must be imported in the client truststore.
- The AccessAgent must point to the Load Balancer as the IMS Server. The communication between the AccessAgent and the IMS Server is over SSL.
- The Load Balancer must be able to send separate SSL requests for each of the incoming requests.

## **Load Balancer configuration requirements**

In the Load Balancer configuration:

- Enable Session Affinity for the Load Balancer. Use a Load Balancer with session affinity to route the traffic for the same client session to the same virtual appliance.
- Set the client host IP into the X-Forward-For HTTP header. The IMS Server must know the client IP for its audit logs.
- The Load Balancer must detect unresponsive virtual appliances and stop directing any traffic to them.
- As shown in Figure 1 on page 71, keep one or more of the Load Balancer backups ready to avoid the Load Balancer being a single point of failure.
- Set the value of the underscores\_in\_headers custom header directive to on.

---

## Chapter 7. Shared credential check-out and check-in

To log on with a client application, you can use the shared access credentials that you checked out and checked in automatically or manually.

---

### Automatic check-out and check-in with client application logon

Use the IBM Security Access Manager for Enterprise Single Sign-OnAccessAgent client to provide check-out and check-in automation of shared access credentials. You must install and configure the AccessAgent client on computers from where the client application is accessed.

#### Logging on with PuTTY

You can use PuTTY to log on to a remote terminal host from Windows with shared privileged identities.

##### Before you begin

- Configure the managed resource that you are going to access from PuTTY for shared access.
- If the pre-configured Privileged Identity Management AccessProfile for PuTTY is modified, upload the updated AccessProfile to the IMS Server.

##### About this task

You can configure the PuTTY AccessProfile for different logon prompts. See “Modifying AccessProfiles for the PuTTY application” in the *IBM Security Privileged Identity Manager Administrator Guide*.

If session recording is enabled, a prompt is displayed requesting for your consent to start session recording.

##### Procedure

1. Start PuTTY.
2. Specify the target host name or IP address.
3. When prompted to log on with shared access credentials, choose **Yes**.
4. When prompted with the Shared Access Selection window, select one of the credential pools.
5. When prompted to provide consent to be recorded, choose **Yes**. Session recording is started.

##### Results

The AccessProfile checks out the credentials from IBM Security Identity Manager and injects the logon credential in the terminal server logon prompt.

#### Logging on with the Microsoft Remote Desktop Connection (RDP) client

You can log on to a remote desktop with shared privileged identities with Remote Desktop Connection.

## Before you begin

- Configure the managed resource that you are going to access from the RDP client for shared access.
- If the pre-configured Privileged Identity Management AccessProfile for Microsoft Remote Desktop Connection RDP client is modified, upload the updated AccessProfile to the IMS Server.
- Configure a group policy to always prompt RDP clients for a password before making a connection.

**Note:** The IBM Security Privileged Identity Manager AccessProfile for Microsoft Remote Desktop Connection (RDP) client does not support injection of shared credentials at the RDP lock screen on the computer to where the user did a remote desktop connection.

## Procedure

1. Start the Microsoft Remote Desktop Connection client by clicking **Start > All Programs > Accessories > Remote Desktop Connection**.
2. Specify the target host name or IP address.
3. Click **Connect**.
4. When prompted to log on with shared access credentials, choose **Yes**.
5. When prompted with the Shared Access Selection window, select one of the credential pools.
6. Enter the AccessAgent authentication credentials.
7. When prompted to provide consent to be recorded, choose **Yes**. Session recording is started.

## Results

The AccessProfile checks out the credentials from IBM Security Identity Manager, and injects the logon credential in the remote desktop logon prompt.

## Logging on with IBM Personal Communications

Use the IBM Personal Communications application to log on to a mainframe application with shared access identity. You must configure the bundled Privileged Identity Management AccessProfile for your mainframe application before check-out and check-in automation can work.

## Before you begin

Configure the AccessProfile for your mainframe application. See “Modifying AccessProfiles for the IBM Personal Communications application” in the *IBM Security Privileged Identity Manager Administrator Guide*.

## About this task

For check-out and check-in automation to work with your custom mainframe applications, you must apply specific changes to the bundled IBM Security Privileged Identity Manager AccessProfile.

**Note:** Customize the IBM Security Privileged Identity Manager AccessProfile for IBM Personal Communications application before you use it.

Customization is necessary because:



- Each mainframe or terminal application might contain different output phrases.
- The AccessProfile or application signature must contain a similar phrase as the one displayed by the mainframe application. So, when the application displays the phrase, the logon automation by the AccessProfile can proceed.

The following steps describe an outline of one of the ways that the shared credential check-out automation might work.

### Procedure

1. Start IBM Personal Communications.
2. Specify the target host name or IP address.

**Note:** The window title of IBM Personal Communications must match the session name.

3. Select the application.
4. When prompted to log on with shared access credentials, choose **Yes**.
5. When prompted with the Shared Access Selection window, select one of the credential pools.
6. When prompted to provide consent to be recorded, choose **Yes**. Session recording is started.

### Results

The AccessProfile checks out the credentials from IBM Security Identity Manager and injects the logon credential in the mainframe logon prompt.

## Logging on with the VMware vSphere Client

Use the VMware vSphere Client to log on to a virtual machine with shared access credentials.

### Before you begin

- Configure the managed resource for shared access.
- If the pre-configured Privileged Identity Management AccessProfile for VMware vSphere Client is modified, upload the updated AccessProfile to the IMS Server.

### Procedure

1. Start the **VMware vSphere Client**.
2. When the **ISAMESSO AccessAgent** dialog box is displayed:
  - a. Specify the target host name or IP address.
  - b. Click **OK**.

If you successfully checked out the shared access credentials, the credentials are injected into the VMware vSphere logon prompt. If the check-out failed, the credentials are not injected.

3. Click **Login**.
4. When prompted to log on with shared access credentials, choose **Yes**.
5. When AccessAgent prompts for reauthentication, enter the AccessAgent credentials.
6. When prompted with the Shared Access Selection window, select one of the credential pools.

7. When prompted to provide consent to be recorded, choose **Yes**. Session recording is started.

## Results

The AccessProfile checks out the credentials from IBM Security Identity Manager, and injects the logon credentials in the VMware vSphere Client logon prompt.

---

## Manual check-out and check-in of shared credentials

Use the IBM Security Identity Manager self-service user interface console to check out and check in shared access credentials for a resource. After you check out a credential, provide the shared access credentials when the client application prompts you.

### Checking out a credential or credential pool

Use the self-service console to use privileges that are not associated with your normal account.

#### About this task

Shared access credentials are used by multiple users that are based on roles. They enable users to temporarily access needed applications. The check-out process places an exclusive lock on the credential. No other user can use the same credential concurrently.

#### Procedure

1. Log on to the self-service console.
2. On the Home page, click **Check out Credential**.

The Check out Credential page lists the credentials that you are authorized to access.

  - If you see the credential you want to access, continue to step 3.
  - If you do not see the credential that you want, you can search for other credentials:
    - a. In the Search for Credential section of the page, click **Search**. The Search for Shared Credential page is displayed.
    - b. Enter the name of the credential or credential pool that you want to access or specify additional search criteria. Click **Search**.

You can filter based on Service Type, Account Type, or Organizational Unit. You can specify that the search includes credentials for which you do not have authorization. See the online help for more details on the filters.

Optionally, you can click **Browse** to search for organizational units. If you click **Browse**, the Search for Organizational Unit page is displayed. Specify search filters and click **Search**.

The search returns a Search Results table that contains a list of credentials.
3. Click the credential that you want to check out.
  - If the Checkout Information page is displayed, you are authorized to access the credential. Continue with step 4 on page 77.
  - If the Select Role page is displayed, you are *not* authorized to access the credential. You must request a role to access the credential or credential pool. Complete the following steps:

- a. Select a role that has access authority for the selected shared credential or credential pool.  
The table lists the roles that have access authority. You must obtain membership in one of the roles to check out the credential or credential pool.
  - b. Review the list of shared access entitlements for the role that you selected and click **Submit**. A new page describes the request that you submitted.
  - c. Select one of the action links at the bottom of the page:
    - Click **View My Requests** to look at the status of your request.  
You must wait until your request is completed to continue with the check out of the credential or credential pool.
    - Click **Check Out Credential** to check out another credential.
    - Click the **IBM Security Identity Manager Home** link to return to the home page for the self service console.
  - d. Return to step 2 on page 76.
4. Review the fields on the Checkout Information page and then complete the checkout.  
By default, the Checkout Information page contains only the **Credential checkout expiration time** field and the **Justification** field, but your Administrator might specify additional fields.
    - a. The **Credential checkout expiration time** field contains the date and time when your access to the credential expires. The Administrator specifies the default maximum allowed lifetime for each checked-out credential. You can modify the expiration time to shorten the lifetime of the checked-out credential; however, you cannot extend the lifetime.
    - b. In the **Justification** field, explain the reason for the access to the credential. By default, this field is optional.
    - c. Click **Check out**. The Checkout Confirmation page is displayed.

## What to do next

Use the user ID and password that you checked out to log on to the application that you want to use.

## Checking in credentials in a credential pool

As a Privileged Administrator, you can check in a credential that either you or any other user checked out by using the administrative console.

### Before you begin

Ensure that you have the following permission: Checking in a credential on behalf of others.

#### CAUTION:

**If the original user still has an active session open while another user has the same shared access account checked out, checking in a shared account for others might break individual accountability. IBM Security Identity Manager does not make session management on connection to a managed resource. This issue can be addressed by IBM Security Access Manager for Enterprise Single Sign-On integration and automated check-out or check-in.**

## Procedure

To check in credentials that are checked out, complete these steps:

1. From the navigation tree, click **Manage Shared Access > Manage Credential Pool**. The Select a Pool page is displayed.
2. On the Select a Pool page, click **Search** to locate the credential pool that you want to modify. If you do not specify any additional information, the search includes all credential pools. To limit the scope of the search, complete these steps:
  - a. Optional: In the **Pool name or description** field, specify the name or description that is associated with the credential pool. For example, type `acmepool` or `pool` for acme company accounts. You can also specify a wildcard, such as `*acme*` to find all pools that contain that term in the name or description.
  - b. Optional: Select a service type from the **Service type** list.
  - c. Optional: Specify a specific service name in the **Service name** field. For example, type `AIX_Service`. You can also specify a wildcard, such as `*AIX*` to find all services that contain that term in the name.
  - d. Optional: To select a different business unit, click **Search** next to the **Business unit** field.
  - e. On the Business Unit page, locate and select a service and click **OK**. The business unit name is displayed in the **Business unit** field.
  - f. Click **Search**. The credential pools that match the search criteria are displayed in the **Credential Pools** table.
3. Locate the row in the **Credential Pools** table that contains the credential pool that you want to check in. In the **Name** column, hover your cursor over the icon to display the action menu. Select **View Credentials in the Pool**.

**Note:** You do not need to select the check box for the credential in the **Select** column.

The View Credentials in the Pool panel is displayed.

4. In the **User ID** field, type the identification name of the credential that you want to check in.
5. Optional: Filter the search criteria by using one of the following options:
  - If you want to check in the credentials that are in the vault, select the **Only display credentials in the vault** check box.
  - If you want to check in the credentials that are checked out from the self-service user interface, select the **Only display credentials checked out** check box.

**Note:** Credentials that are marked with a warning icon are not available in the vault.

6. Click **Search**.

**Note:** If you leave the **User ID** field blank and click **Search**, all the accounts that are in a group or groups available in the pool are displayed.

7. In the **Credentials In The Pool** table, select one or more credentials that you want to check in.
8. Click **Check In**. A confirmation page is displayed.
9. On the Confirm page, specify the date and time for the check-in to occur, and then click **Check In**, or click **Cancel**. A message is displayed, indicating that you successfully checked in the credential.

## Checking in credentials from a credential vault

As a Privileged Administrator, you can check in a credential that either you or any other user that is checked out from a credential vault.

### Before you begin

Ensure that you have the following permission: Checking in a credential on behalf of others.

### Procedure

To check in credentials that are checked out, complete these steps:

1. From the navigation tree, click **Manage Shared Access > Manage Credential Vault**. The **Select a Credential** page is displayed.
2. Click **Search** to locate the credentials that you want to view. If you do not specify any additional information, the search includes all user IDs and services in the vault. To limit the scope of the search, complete these steps:
  - a. In the **User ID** field, specify a user ID associated with the account credentials. For example, type `bsmith`.
  - b. Enter a specific service name in the **Service name** field. For example, type `AIX_Service`. You can also specify a wildcard, such as `*AIX*` to find all services that contain that term in the name.
  - c. Optional: Click **Advanced**. The advanced search option opens a new page where you can specify other search criteria.

The credentials that match the search criteria are displayed in the **Credentials** table.

3. In the **Credentials** table, select one or more credentials that you want to check in.
4. Click **Check In**. A confirmation page is displayed.
5. On the Confirm page, specify the date and time for the check-in to occur.
6. Click **Check In**, or click **Cancel**. A message is displayed, indicating that you successfully checked in the credential.

**Note:** If the credentials that you are checking in are not connected to an account, the credential password is not changed at checkin even if the default configuration settings specify that **Change password upon checkin** is enabled.

7. Click **Close** to exit credential vault management.



---

## Chapter 8. Setting up a secondary virtual appliance for active-passive configuration

You can provide a basic level of disaster recovery by setting up the IBM Security Privileged Identity Manager Virtual Appliance into two virtual appliances with active-passive configuration.

Complete the following tasks to deploy an active-passive configuration for the virtual appliances:

1. "Setting up a primary virtual appliance."
2. Optional: "Backing up the primary virtual appliance."
3. "Creating a snapshot of the primary virtual appliance" on page 82.
4. "Setting up a secondary virtual appliance" on page 83.

---

### Setting up a primary virtual appliance

Set up the primary virtual appliance for the active-passive configuration.

#### Procedure

1. Create a virtual machine on the VMware ESXi Server by using the IBM Security Privileged Identity Manager Virtual Appliance ISO.
2. Complete the first steps configuration. For example, configure the host name and IP address.
3. Complete the virtual appliance configuration.
4. Log on to the applications by using the **Appliance Dashboard** console.
5. Verify that the applications are started.
6. Verify that the user can log on to IBM Security Identity Manager, IBM Security Access Manager for Enterprise Single Sign-On and the IBM Privileged Session Recorder console to complete operations.

---

### Backing up the primary virtual appliance

As an optional task, you can choose to back up the primary virtual appliance configuration.

#### About this task

The virtual appliance has two disk partitions, and at any time one is active and another is inactive. Backing up the primary virtual appliance is an optional procedure to back up the entire active partition to the inactive partition on the same virtual appliance.

#### Procedure

1. Stop the servers from the **Appliance Dashboard**. To stop the servers, click **Stop** from the **Server Status** pane.
2. Stop the directory server instance and database instance on the external data tier.
3. From the **Appliance Dashboard**, verify that the **Middleware and Server Monitor** widget indicates that all middleware and applications are stopped.

4. Create a backup of the active partition on the secondary partition.
  - a. From the virtual appliance user interface, select **Firmware Settings**.
  - b. Select the active partition and then click **Create Backup**.

The system restarts and backs up the primary partition.

**Related tasks:**

“Reverting the virtual appliance to its backup”

To revert the virtual appliance to its backup, start the virtual appliance through the inactive partition; the partition from where the backup was taken.

---

## Reverting the virtual appliance to its backup

To revert the virtual appliance to its backup, start the virtual appliance through the inactive partition; the partition from where the backup was taken.

### Procedure

1. On the virtual appliance user interface, select **Firmware Settings**.
2. Select the inactive partition and click **Set Active**.

---

## Creating a snapshot of the primary virtual appliance

Use the **Appliance Dashboard** to create a snapshot of the primary virtual appliance. A snapshot that is created from a configured virtual appliance can be applied on the same virtual appliance to restore the configuration and policy settings. A snapshot contains configuration and policy settings. It can also be used to synchronize the configuration and policy settings between the primary virtual appliance and a secondary virtual appliance.

### Procedure

1. From the **Appliance Dashboard**, stop the servers.
2. On the external data tier, stop the following instances.
  - Directory server
  - Database
3. From the **Appliance Dashboard**, verify that the **Middleware and Server Monitor** widget indicates that all the middleware and applications are stopped.
4. Under **Manage System Settings**, click **Snapshots**.
5. Click **New** to create a snapshot.
6. Under the **Comments**, specify helpful comments so that the snapshot is easy to identify from a primary virtual appliance that is synchronized with the external data tier.
7. Download and save the snapshot on the network file system.
8. Stop the primary virtual appliance. Complete one of the following tasks:
  - On the ESXi Server, suspend the virtual machine by using the VMware vSphere Client.
  - Stop the virtual appliance by using the command-line interface command: `shutdown`.

**Note:** Create the snapshot of the external data tier, such as the directory server and database system, at the same time to preserve the current state. The document does not describe how to create the snapshot of the external data tier systems.



---

## Setting up a secondary virtual appliance

Set up the secondary virtual appliance. The secondary virtual appliance can be configured to point to the same data tier as the primary virtual appliance for high availability configuration. It can also be configured to point to a replicated (standby) data tier for disaster recovery configuration.

### Procedure

1. Create a virtual machine on the VMware ESXi Server by using the IBM Security Privileged Identity Manager Virtual Appliance ISO.
2. Complete the first steps configuration. For example, configure the host name and IP address.

**Note:** The secondary virtual appliance can be configured to use its own unique IP address. However, the secondary virtual appliance must be configured to have the same host name as the primary virtual appliance. Use the same host name so that requests from AccessAgent can be rerouted to the secondary virtual appliance through a DNS change when the primary virtual appliance is down.

3. Log on to virtual appliance user interface for the virtual appliance activation. The following process displays the user interface.
4. From the activation screen, select **Snapshots**.
5. Upload the snapshots that are taken from the primary appliance. Wait until the **Comment** field is updated on the snapshot upload screen.
6. When the snapshot is uploaded, the screen is refreshed and it lists the snapshots.
7. Select the snapshot, which was captured from the primary virtual appliance that is based on the comments and time stamps from the list and click **Apply**.
8. After the snapshot is applied, log on to the command-line interface and shut down the secondary virtual appliance by using the **shutdown** command.
9. Start the directory server and database instance on the external data tier.
10. Start the secondary virtual appliance from the VMware Server.
11. When the secondary virtual appliance starts, you can log on to the virtual appliance user interface.
12. Go to the **Appliance Dashboard**.
13. From the **Appliance Dashboard**, verify that the **Middleware and Server Monitor** widget indicates that all middleware and applications are started.

### What to do next

Only one instance of the virtual appliance must be running at any time. As such, the secondary virtual appliance must be started up only when the primary virtual appliance is down.

Verify that the applications are started and that the user can log on to IBM Security Identity Manager, IBM Security Access Manager for Enterprise Single Sign-On, and the IBM Privileged Session Recorder console.

---

## Enhance availability by using monitoring URLs

Monitoring URLs is a facility for the customer to write scripts to monitor the uptime and the responsiveness of the IBM Security Privileged Identity Manager Virtual Appliance. It is used to monitor the health of the IBM Security Privileged Identity Manager server functions.

You do not have to authenticate to access Monitoring URI. These URIs can be used by any third-party tool to obtain data about responsiveness.

### Response format

Service name: response code, Time taken in milliseconds:ms (Response code is 0 if services are down and 200 if running.)

Example: "Identity":"0", "Time taken in milliseconds":401

### For Identity service -

URI: `https://appliance_hostname/monitor/response?Service=Identity`

Response: {"Identity":"0", "Time taken in milliseconds":401}

### For SingleSignOn service -

URI: `https://appliance_hostname/monitor/response?Service=SingleSignOn`

Response: {"SingleSignOn":"0","Time taken in milliseconds":8}

### For SessionRecorder service -

URI: `https://appliance_hostname/monitor/response?Service=SessionRecorder`

Response: {"SessionRecorder":"0","Time taken in milliseconds":2}

### For All in a single request -

URI: `https://appliance_hostname/monitor/response`

Response:

```
{"Identity":"200","SessionRecorder":"200","SingleSignOn":"200",  
"Identity Time taken in milliseconds":529,"SessionRecorder Time  
taken in milliseconds":400,"SingleSignOn Time taken in  
milliseconds":361}
```

---

## Chapter 9. Upgrading the IBM Security Privileged Identity Manager Virtual Appliance

Install the firmware update to upgrade the IBM Security Privileged Identity Manager Virtual Appliance.

### Before you begin

Before you apply the firmware update to upgrade the IBM Security Privileged Identity Manager Virtual Appliance, back up your data tier, which is all the databases and the directory server.

### About this task

The IBM Security Privileged Identity Manager Virtual Appliance has two partitions with separate firmware on each partition. The partitions are swapped during the firmware updates to roll back the firmware updates when required. Either of the partition can be active on the IBM Security Privileged Identity Manager Virtual 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 IBM Security Privileged Identity Manager Virtual Appliance restarts the system by using Partition 2, which is now the active partition.

The IBM Security Privileged Identity Manager Virtual Appliance version upgrade can be installed only by using the command-line interface (CLI).

### Procedure

1. Download the `ispim_*.pkg` build.
2. Access the command-line interface (CLI) of the virtual appliance by using either an `ssh` session or the console.
3. Copy the `ispim_*.pkg` to a USB device.
4. Attach the USB device to your virtual system.
5. In the virtual appliance CLI, run the `ispim` command to display the `ispim` prompt.
6. At the `ispim` prompt, run the `firmware_update` command.
  - a. Run the `list_firmware` command to list the firmware updates from a USB device.
  - b. Run the `transfer_firmware` command to transfer the firmware updates from a USB device to the virtual system.

**Note:** To install a firmware upgrade, you must first transfer it to the virtual system.

- c. Run the `install_firmware` command.
- d. Select the index of the firmware update that you want to install to the virtual system and press `Enter`.

The results are as follows:

- 1) The upgrade process formats Partition 2 and installs the new firmware update on it.
  - 2) When you apply the firmware update, your policies and settings are copied from Partition 1 to Partition 2.
  - 3) On completion, the process indicates you to restart the virtual system.
- e. Type the **reboot** command and press **Enter** to restart the virtual system by using Partition 2. Partition 2 is now the active partition.

The results are as follows:

- 1) After the virtual appliance restarts from the Partition 2, all the configuration that were part of Partition 1, is applied to the Partition 2.
  - 2) After the configuration is applied to the virtual appliance, the process indicates you to restart the virtual appliance.
- f. Restart the virtual appliance to complete the upgrade process.
- g. Upgrade the Session Recording data store. Do these steps:
- 1) Create a database for the Session Recording data store. See “Installing and configuring the database server” on page 12.
  - 2) Unconfigure the existing Session Recording data store. Do the following steps:
    - a) From the top-level menu of the **Appliance Dashboard**, click **Configure > Manage External Entities > Database Server Configuration**.
    - b) Select **Session Recording data store**, click **Unconfigure**, and wait for the process to complete.
    - c) From the **Appliance Dashboard**, locate the **Server control** widget and click **Restart**.
      - i. In the Reasons for restart pane, select **Session Recording data store configuration** from the list.
      - ii. Click **Save Configuration**.
  - 3) Configure the Session Recording data store. See “Managing the Database Server configuration” on page 51.
  - 4) From the **Appliance Dashboard**, locate the **Server control** widget and click **Restart**.
    - a) In the Reasons for restart pane, select **Session Recording data store configuration** from the list.
    - b) Click **Save Configuration**.
  - 5) Run the migration tool. Do these steps:
    - a) Edit the `psr_upgrade_tool.properties` file for the PSRUUpgradeTool with the following details.
      - Details of the database that is used by the older version of the Session Recording data store.
      - Details of the database that is used by the newer version of the Session Recording data store.
- Note:** Extract the `psr_upgrade_tool.properties` file from `com.ibm.security.recorder.data.UpgradeTool_v1.zip`. This archive is obtained from the package or the location from where you downloaded the ISO.
- b) Start the database migration process with the PSRUUpgradeTool:

- i. Go to the folder where the PSRUpgradeTool is located.

**Note:** If an error is displayed when the program is run, you must add the class path for Java to your Windows or Linux path.

- ii. Run the following command:

```
java -jar PsrUpgradeToolV1.jar psr_upgrade_tool.properties  
> migrate_tool_results.log
```

Where migrate\_tool\_results.log logs any results of the migration process.

**Note:** Use IBM Java Runtime Environment Version 6 to run the migration tool.

- h. For the Identity data store, clear the **Service Integration Bus**. See “Reconfiguring the data store connection” on page 63.
- i. Restart the Identity service.
- j. Optional: Back up Partition 2 in to Partition 1 after the successful completion of the firmware upgrade. The backup process overwrites the information that is in Partition 1.

Do the following actions:

- 1) Check and fix any errors if the upgrade process failed.
- 2) Use Partition 1 to set it as the active partition and restart it.

Partition 1 now becomes the active partition.



---

## Chapter 10. Troubleshooting and support

To help you understand, isolate, and resolve problems with your IBM software, use the troubleshooting and support information section for instructions and problem-determination resources that are provided with your IBM products.

---

### Restrict operations for a Member node

The IBM Security Privileged Identity Manager Virtual Appliance cluster is composed of one Primary node and other nodes that are called as Member nodes. To configure a virtual appliance, you must work from a Primary node.

The **Configure** menu contains the following configuration options:

- Directory Server Configuration
- Database Server Configuration
- E-mail Server Configuration
- Upload Feed File
- Update property
- Load Balancer configuration
- Session Recording activation
- Administrator settings
- Other CLI configuration options such as:
  - Service properties
  - Syslog properties
  - Set password

The operations for any of these configuration options are restricted for a Member node.

If you open any Configuration page from the **Configure** menu on the Member node to modify any configuration information, a warning message is displayed.

If you ignore the warning message and continue to modify any of the configuration information from the **Configure** menu, a warning message indicates that you cannot complete the operation.

The restriction exists because the IBM Security Privileged Identity Manager Virtual Appliance is a member of a cluster, which does not contain the role of a Primary node.

---

### Handling password synchronization issues



You encounter administrator password synchronization issues when you undo or redo a configuration for the Single Sign-On data store. The synchronization issues are between the Identity and Credential Vault Administration console, the Single Sign-On and Session Recorder Administration console, and the Session Replay Console.

## About this task

The administrator password is not synchronized with each of the following consoles when you undo and redo the configuration for the Single Sign-On data store:

- Identity and Credential Vault Administration console
- Single Sign-On and Session Recorder Administration console
- Session Replay Console

## Procedure

1. Log on to IBM Security Identity Manager Console with the pim manager credentials.
2. From the navigation tree, click **Manage Users** to display the Select a User page.
3. In the **Users** table, click the twistie icon  next to the user name whose password that you want to change.
4. Click **Accounts** to display the Accounts page.
5. On the Accounts page, click the twistie icon  next to the user ID.
6. Click **Change Password**.
7. On the Change Passwords page, select **Allow me to type a password**.
8. In the **Password** field, enter a password.
9. In the **Confirm Password** field, retype the password.

## Results

The password for the IBM Security Identity Manager Console, the Single Sign-On and Session Recorder Administration console, and the Session Replay Console is synchronized.

## What to do next

Log on to the following consoles by using the new password to verify whether it is synchronized:

- Identity and Credential Vault Administration console
- Single Sign-On and Session Recorder Administration console
- Session Replay Console

---

## Cluster bootstrap process

Bootstrapping refers to getting a cluster node up and running. When a cluster node recovers from failure, checks are made to keep the node state consistent with the rest of the nodes in the cluster.

When you encounter an unresponsive Primary node or Member node, take following actions:

- You remove it from the Load Balancer configuration, which stops user requests from being routed to the node.
- You troubleshoot or fix the errors by using the various methods that are documented in <http://www-01.ibm.com/support/knowledgecenter/SSRQBP/welcome>.
- Restart the Primary node or the Member node virtual appliance.



- Reconnect the Member node with the new Primary node if the earlier role of the node was changed from Primary to Member.
- Synchronize the Member node with the Primary node if the node continues to be a Member node, but missed a few virtual appliance configuration updates.
- This node becomes a stand-alone node if this node is removed from the cluster definition.

The following actions are done by the cluster bootstrap process:

- When a Primary node recovers from a failure and detects that no other node is promoted to Primary, it continues to be as Primary in that cluster.
- When a Member node recovers from a failure and detects that it continues to be part of the original cluster, synchronization might be needed if the virtual appliance configuration changes were made.
- When a Primary node recovers from a failure and detects that another node is promoted to Primary, the role of the current node is changed to Member and a reconnect notification request is set.
- When a Primary node or a Member node recovers from a failure and cannot connect with any of the previously known cluster members because the virtual appliance password changed, the current node is made a stand-alone node. A reconnect notification is set.

---

## Cluster monitor service

Cluster monitor service is a background process in the IBM Security Privileged Identity Manager Virtual Appliance that frequently checks for all business functions to be alive and running.

The cluster monitor service specifically checks for the following aspects:

- The three servers:
  - Identity
  - Single Sign-On
  - Session Recorder
- Data stores for the installed servers
- IBM Security Directory Server
- IBM Security Directory Integrator Service Connector

An administrator can check the status of the three servers by following the instructions that are provided in “Enhance availability by using monitoring URLs” on page 84. The status of all the IBM Security Privileged Identity Manager Virtual Appliance components is shown on the Middleware and Server Monitor widget of the IBM Security Privileged Identity Manager Virtual Appliance console. The IBM Security Directory Integrator Service Connector status is reflected in the availability status of the Identity Server.

The cluster monitor service checks the former function at a repeating and fixed interval of 4 seconds. When it finds that one or more of the services are not functional, the following actions are taken:

1. Automatically stops external access to the Identity, Single Sign-On, and the IBM Privileged Session Recorder functions. This action means that the business user requests for check-out or check-in of the shared credentials cannot be serviced by the IBM Security Privileged Identity Manager Virtual Appliance.

2. Sends an email notification to the IBM Security Privileged Identity Manager administrator with the URL for the IBM Security Privileged Identity Manager Virtual Appliance where one or some failures occurred.

Similarly, the cluster monitor service can detect service restoration when the failures are fixed. The following actions are taken:

1. Automatically enables external access to the Identity, Single Sign-On, and the IBM Privileged Session Recorder functions. This action means that the business user requests for check-out or check-in of the shared credentials can be serviced by the IBM Security Privileged Identity Manager Virtual Appliance.
2. Sends an email notification to the IBM Security Privileged Identity Manager administrator with the URL for the IBM Security Privileged Identity Manager Virtual Appliance where the service is restored after failures were fixed.

---

## Checking logs

Use the Log Retrieval and Configuration page to view the log files. You can also use this page configure the server log settings for the IBM Security Privileged Identity Manager Virtual Appliance.

### About this task

To learn more about the available log files, see “Retrieving logs” on page 62.

### Procedure

From the top menu, click **Manage > Log Retrieval and Configuration**.

---

## Common issues

You might encounter common issues during the deployment and usage of IBM Security Privileged Identity Manager in the IBM Security Privileged Identity Manager Virtual Appliance. For more information, see the following common issues and workaround sections.

### Data store configuration fails

Check the configuration of the database system.

On the Log Retrieval and Configuration page, click the **Appliance** tab and check the Identity, Single Sign-On and Session Recording data store configuration, Server System Out, and Server Messages.

### Directory Server Configuration fails

Check the configuration of the directory server.

On the Log Retrieval and Configuration page, click the **Appliance** tab and check the directory server configuration, Server System Out, and Server Messages.

### Unable to access the virtual appliance console

Make sure that the network configuration link IP, Subnet Mast, DNS, and Gateway are correct.

## **High Disk Usage Notification on Dashboard**

Reduce the setting for the **Maximum size for log file rotation** and **Maximum number of historical log files**.

Reduce the trace level from the command-line interface.

Clean the log files from **Manage > Maintenance > Log Retrieval and Configuration**.

## **Unable to access credentials by using AccessAgent on client system**

Make sure that the virtual appliance host name is registered with DNS or updated in the client system hosts file.

Restart the client system.

Make sure that the time in the client system where AccessAgent is installed and the time in the IBM Security Privileged Identity Manager Virtual Appliance are synchronized.

## **Test connection or reconciliation operation failed by using Identity and Credential Vault administration console**

Restart by using the **Server control dashboard** widget with the option **Others(Full restart)**. If the operation still fails, restart the virtual appliance.

## **Unable to access Identity and Credential Vault Administration console**

Check the **Middleware and Server Monitor** dashboard widget to verify the status of the Identity server, Directory server, and Identity data store. Then, take the appropriate action.

See the log files for more details.

## **Unable to access Single Sign-on and Session Recorder Administration console**

Check the **Middleware and Server Monitor** dashboard widget to verify the status of the Single Sign-On server and Single Sign-On data store. Then, take the appropriate action.

See the log files for more details.

## **Unable to access Session Recorder Replay console (if activated)**

Check the **Middleware and Server Monitor** dashboard widget to verify the status of the Session Recording server and Session Recording data store. Then, take the appropriate action.

See the log files for more details.

## For any other unrecoverable issues

Generate a support file by using the command-line interface or the virtual appliance console for the IBM Support Team.

### CLI

```
ispimva.example.com> support
ispimva.example.com:support> create
ispimva.example.com:support> download
1: ispim_1.0.1.1_20130925-014609_ispimva.example.com.zip
2: ispim_1.0.1.1_20130925-015645_ispimva.example.com.zip
Enter index: 1
Insert a USB drive into the USB port on the appliance.
Enter 'YES' to confirm: YES
```

### Console

1. Log on to the IBM Security Privileged Identity Manager Virtual Appliance console.
2. Select **Manage > System Settings > Support Files**.
3. Click **new** to create a new file.
4. Click **download** to save a copy of the support file.

## Unable to connect the IBM Security Privileged Identity Manager Server even with the correct host name

To resolve this issue, add the certificate to the client.

1. Log on with Administrator privileges on the client computer.
2. Start a web browser and go to the HTTPS URL for the IBM Security Privileged Identity Manager Server `https://hostname` where host name is the name of the computer that has the IBM Security Privileged Identity Manager Virtual Appliance Server.
3. In the web browser, export the security certificates to a file.
4. Complete the following instructions:
  - a. On the Microsoft Internet Explorer, click **File > Properties**.
  - b. Click **Certificates**.
  - c. Click the **Certification Path** tab.
  - d. Click the **Details** tab.
  - e. For each certificate marked with a red X in the certificate hierarchy, do the following actions:
    - 1) Click **View Certificate**.
    - 2) Click **Details**.
    - 3) Click **Copy to File**.
    - 4) Follow the instructions in the wizard with the following considerations:
      - When the Export format page is displayed, select the **DER encode binary x.509 (CER) format**.
      - Save the certificates on your local computer. For example: `webhost.cer`.
5. Copy the CER files to the following location: `aa_home\SessionRecorder`  
`aa_home` is the AccessAgent installation directory. For example: `C:\Program Files\IBM\ISAM ESSO\AA\`.
6. Restart the computer where AccessAgent is installed.

---

## Limitations

IBM Security Privileged Identity Manager limitations can affect how the IBM Security Privileged Identity Manager Virtual Appliance behaves or processes information that is received from IBM Security Identity Manager and IBM Security Access Manager for Enterprise Single Sign-On. In the same way, IBM Security Identity Manager and IBM Security Access Manager for Enterprise Single Sign-On limitations can affect how the IBM Security Privileged Identity Manager Virtual Appliance capabilities work.

### IBM Security Privileged Identity Manager Virtual Appliance limitations

- Reconfiguration options for the middleware are not available.
- An external repository (for example, Active Directory) cannot be configured with IBM Security Privileged Identity Manager Virtual Appliance server components (IBM Security Identity Manager and IBM Security Access Manager for Enterprise Single Sign-On).
- Non-English characters are not supported in the **Comment** fields of the following IBM Security Privileged Identity Manager Virtual Appliance panels:
  - Snapshot
  - Firmware Settings
  - Support Files
- The following file name display issues occur in several languages when a snapshot with a long file name is uploaded in the IBM Security Privileged Identity Manager Virtual Appliance:
  - The text in the **Comment** field is truncated.
  - The file name gets truncated in the **Snapshot** table.

### IBM Security Privileged Identity Manager limitations

- Data Tier and Reporting components  
The Data Tier and Reporting components must be installed separately or outside the IBM Security Privileged Identity Manager Virtual Appliance.
  - External repository (for example, Active Directory) cannot be configured with IBM Security Privileged Identity Manager Virtual Appliance server components.
  - IBM Cognos<sup>®</sup> reporting components are outside of the IBM Security Privileged Identity Manager Virtual Appliance.
  - Supports only DB2 and IBM Security Directory Server as the IBM Security Privileged Identity Manager data store on the external data tier.
- Limited IBM Security Identity Manager and IBM Security Access Manager for Enterprise Single Sign-On functions are supported.  
Customization is limited since there is no direct access to low-level IBM Security Identity Manager and IBM Security Access Manager for Enterprise Single Sign-On configuration files.
- Changing the IBM Security Privileged Identity Manager user logon ID on the IBM Security Privileged Identity Manager console and AccessAgent is not supported.
- Only one network adapter can be used.

### IBM Security Access Manager for Enterprise Single Sign-On limitations

- AccessAgent sign up

Sign-up is not allowed from Access Agent. Users are signed up through IBM Security Identity Manager.

- AccessAssistant/WebWorkplace  
This component is not required for IBM Security Privileged Identity Manager.
- Self-Service Sign-Up through IBM Security Access Manager for Enterprise Single Sign-On AccessAgent  
This feature is not supported because users are to be on-boarded through IBM Security Identity Manager.
- Self-Service Password Reset  
IBM Security Privileged Identity Manager Virtual Appliance users must use the equivalent feature in IBM Security Identity Manager instead.
- Change ISAM ESSO password  
Users must use the equivalent feature in the IBM Security Identity Manager Self-Service UI instead.
- Biometric and smart card second factor support with IBM Security Access Manager for Enterprise Single Sign-On Agent are not available in the IBM Security Privileged Identity Manager Virtual Appliance.
- RFID 2FA for AccessAgent is not supported.
- Only the default User Policy Template is supported. User Policy Templates that are based on arbitrary directory attributes are not supported.
- Third-party Provisioning System to provision or manage IBM Security Access Manager for Enterprise Single Sign-On accounts or Wallets  
This component is not required in the IBM Security Privileged Identity Manager Virtual Appliance because the IBM Security Access Manager for Enterprise Single Sign-On accounts are provisioned through IBM Security Identity Manager.
- IBM Security Access Manager for Enterprise Single Sign-On mobile  
This feature is not used with IBM Security Privileged Identity Manager.
- Mobile Active Code, One Time Password, or RADIUS are not supported
- AccessAgent Private and Shared Desktop modes are not supported.
- IMS Configuration wizard and CLTs are not supported.

#### **IBM Security Identity Manager limitations**

- Custom workflow extension configuration is not supported.
- Uploading of custom Java archive files, which implements IBM Security Identity Manager custom extensions, is not supported. For example, workflow.
- Custom adapters are not supported.
- IBM Security Identity Manager mobile is not supported.

---

## **Known issues and workarounds**

The Known issues and workarounds section helps you understand, isolate, and resolve problems with IBM Security Privileged Identity Manager Virtual Appliance. Descriptions about the events that generate the problems are listed along with symptoms, environment, possible causes, and suggestions for recovery. It also contains information about where logs are stored and how to run traces.

For other limitations that are related to IBM Security Privileged Identity Manager, see the *Known problems and workarounds* section of the IBM Security Privileged Identity Manager documentation, <http://www.ibm.com/support/knowledgecenter/SSRQBP/welcome>.

## Troubleshooting dashboard panel widget display issues on Microsoft Internet Explorer 10

Browser not supported message for any appliance panel.

### About this task

An attempt to view the IBM Security Privileged Identity Manager Virtual Appliance console or activation wizard in a Microsoft Internet Explorer, version 10 browser shows browser not supported message.

To solve the issue, complete these steps as a workaround:

### Procedure

1. Open the Microsoft Internet Explorer 10 browser.
2. After the activation steps are completed, change the browser setting:
  - a. Click **Tools**.
  - b. Deselect **Compatibility View**.
  - c. Open **Compatibility View Settings**.
  - d. Deselect the **Download updated compatibility lists from Microsoft** option.
3. Access the IBM Security Privileged Identity Manager Virtual Appliance console.

## Troubleshooting Logon to Session Reply Console

The Logon to Session Reply Console fails if the virtual appliance console and Session Reply Console are opened in the same browser window.

### About this task

An attempt to do the Logon to Session Reply Console opened in the same browser window where the virtual appliance console is open fails. To solve the issue, complete these steps as a workaround:

### Procedure

1. Clear the browser cache before you access the Session Reply Console.
2. Open a new browser window to access the Session Reply Console.

## Value for a property is not retained if update\_syslog command is executed without any value for other properties

If a user does not enter any value for a property before running the `update_syslog` command, default values are set for the property.

The default value of the following parameters is false if a user does not specify any value.

```
logSystemManagementActivity: false
logUserAdminActivity: false
logUserService: false
logUserActivity: false
```

For the syslog CLI utility, the default values for the IBM Security Privileged Identity Manager entries are:

```
rwrangler.example.com:ispim> list_syslog
  Enable syslog
    logSystemManagementActivity: false
    logUserAdminActivity: false
    logUserService: false
    logUserActivity: false
  Syslog server port: 514
  Syslog server hostname: localhost
  Syslog logging facility: 20
  Syslog field-separator: \n
```

## Startup problems with the IBM Security Privileged Identity Manager Virtual Appliance Dashboard

You might encounter some problems when you start the IBM Security Privileged Identity Manager Virtual Appliance Dashboard.

The possible startup problems are as follows:

- Startup or loading delays for several seconds or minutes.
- A notification prompts for a required restart.
- A component status prompts as started, but is not available.

### Symptom

You might experience some delays or other startup problems with the IBM Security Privileged Identity Manager Virtual Appliance Dashboard due to these conditions:

- The virtual appliance dashboard starts for the first time after configuration.
- All the widgets are not loaded.

### Resolving the problem

Wait for some time and refresh the widget to check the latest status of the virtual appliance.

## IBM Security Privileged Identity Manager Virtual Appliance Dashboard displays notifications about snapshots

The IBM Security Privileged Identity Manager Virtual Appliance Dashboard displays notifications that a snapshot is being applied.

### Symptom

Notifications about snapshots that are being applied are displayed by the IBM Security Privileged Identity Manager Virtual Appliance Dashboard.

### Resolving the problem

Snapshots might also change the network settings of the virtual appliance. When you apply a snapshot from the management interface of the virtual appliance, you are directed to a pop-up window. The window notifies you to go to the virtual appliance by using the IP or the host name that is specified in the snapshot.



If you log on to the virtual appliance while the snapshot process is in progress, in the Notification widget, you might see a notification such as 'Snapshot is getting applied'. Since the snapshot process takes some time, wait until the process completes. Refresh the Notification widget to retrieve the recent notifications.

## LDAP Server must run when IBM Security Privileged Identity Manager Virtual Appliance servers are restarted after LDAP configuration

The LDAP Server must be running when you restart the IBM Security Privileged Identity Manager Virtual Appliance servers after an LDAP configuration.

### Symptom

When the IBM Security Privileged Identity Manager Virtual Appliance servers are restarted after an LDAP configuration, the LDAP Server must be in a running state.

### Resolving the problem

Some of the post-configuration tasks start running after an LDAP configuration and when you start the IBM Security Privileged Identity Manager Virtual Appliance server. This task requires the LDAP Server to be in running state. Therefore, it is required that the LDAP Server is running.

---

## Bulkload command errors

When running the bulkload command, some errors might occur. The bulkload utility fails if any of the entries in the input LDIF file exist in LDAP.

This error might occur if the suffix you defined exists as an entry in the directory server. It might be necessary to delete all entries in the suffix (but leave the suffix) from LDAP before running the command. You can use the `ldapsearch` commands to check for existence of entries, and the `ldapdelete` command to remove these entries.

Error codes:

GLPCRY007E The directory key stash file is inconsistent with the associated encrypted data.

GLPBLK071E Bulkload is unable to run because of an initialization error.

GLPBLK030E Run DB2CMD.EXE first, and then run bulkload within the "DB2 CMD" command interpreter.

To correct these errors, you must know the encryption seed and salt values of the target instance. The target instance is the directory server instance where you are running the bulkload.

1. To determine the salt value of target instance, run the following command from `TDS_HOME/bin`:

```
ldapsearch -D bind DN -w password -h hostname -p port -s base -b  
cn=crypto,cn=localhost cn=*
```

where:

bind DN is the distinguished name (DN) of the directory server.

password is the DN password.

hostname is the name of the computer where IBM Security Directory Server is installed.

port is the port number on which IBM Security Directory Server is listening.

2. Replace the value of `ibm-slapdCryptoSync`, `ibm-slapdCryptoSalt` with the values returned by the **ldapsearch** command in the `ldap_output_file` file. This file is generated as output of the **db2ldif** command, for example `old_ldif_data.ldif`.
3. Run the **bulkload** command again.

**Note:** You can use the **-W OUT\_FILE\_NAME** option with the **bulkload** command. This option places the output from the command into the specified file. The **bulkload** command runs several instances of a DB2 command to load data. Each one has its own success, error, or warning messages. Without the **-W** option to save the output, it is difficult to check the result.

---

## Chapter 11. Sample configuration response file

You can set your configuration parameters for the IBM Security Privileged Identity Manager Virtual Appliance in a response file. After you complete the response file, you can upload the response file to configure the virtual appliance in the advanced configuration mode.

```
#####  
#  
# Complete initial configuration of IBM Security Privileged Identity Manager  
# Appliance by using a response file.  
# Update the response file with correct values and provide it during the advanced  
# mode of Initial configuration wizard.  
#  
#####  
#  
# Appliance Administrator User Credentials  
#  
ispim.appliance.adminUserPwd=<admin user password>  
  
#  
# Session Recording Activation Detail  
# If you want to activate session recording, provide the activation key.  
# Else, you can leave this field blank.  
#  
ispim.session.recording.activation.key=  
  
#  
# Certificate Information  
# If you want to use default certificate, then leave these fields blank.  
# Else, if you want to generate your own self-signed certificate,  
# ispim.root.ca.certificate.common.name is required. Other fields are optional.  
# Zipcode should be an integer  
# Country should be empty or of length 2 characters  
#  
ispim.root.ca.certificate.common.name=<Customer's CN>  
ispim.root.ca.certificate.organization=  
ispim.root.ca.certificate.organizational.unit=  
ispim.root.ca.certificate.locality=  
ispim.root.ca.certificate.state.province=  
ispim.root.ca.certificate.zipcode=  
ispim.root.ca.certificate.country=  
  
#  
# Identity Data store configuration Properties  
#  
ispim.identity.datastore.hostName=<hostname>  
ispim.identity.datastore.port=50000  
ispim.identity.datastore.adminUser=piminst  
ispim.identity.datastore.adminUserPwd=<admin password>  
ispim.identity.datastore.dbName=idmdb  
  
#  
# Enterprise Single Sign-On Data store configuration Properties  
#  
ispim.signon.datastore.hostName=<hostname>  
ispim.signon.datastore.port=50000  
ispim.signon.datastore.adminUser=piminst  
ispim.signon.datastore.adminUserPwd=<admin password>  
ispim.signon.datastore.dbName=essodb  
  
#
```

```
# Session Recording Data store configuration Properties
#
ispim.session.recording.datastore.hostName=<hostname>
ispim.session.recording.datastore.port=50000
ispim.session.recording.datastore.adminUser=piminst
ispim.session.recording.datastore.adminUserPwd=<admin password>
ispim.session.recording.datastore.dbName=psrdb

#
# Directory Server configuration properties
#
ispim.ldap.hostName=<hostname>
ispim.ldap.port=389
ispim.ldap.organization.shortname=org
ispim.ldap.organization.name=Organization
ispim.ldap.bindDN=cn=root
ispim.ldap.bindDNPwd=<password>
ispim.ldap.dnLocation=dc=com
ispim.ldap.connection.type=non-ssl

#
# Mail Server configuration properties
#
ispim.mail.server=localhost
ispim.mail.from=admin@example.com
```

---

## Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed 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 may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give 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 character set (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.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, 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 for the purpose of enabling: (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  
2Z4A/101  
11400 Burnet Road  
Austin, TX 78758 U.S.A.

Such information may 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 may vary significantly. Some measurements may 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 measurement may have been estimated through extrapolation. Actual results may 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 IBM's future direction or intent 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 conforming 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. 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 conforming to IBM's application programming interfaces.

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. 2012. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

## Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at <http://www.ibm.com/legal/us/en/copytrade.shtml>.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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



Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

## **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.

The IBM Security Access Manager for Enterprise Single Sign-On software uses other technologies that collect each user’s user name, password or other personally identifiable information for purposes of session management, authentication, single sign-on configuration or other usage tracking or functional purposes. These technologies can be disabled, but disabling them will also eliminate the functionality they enable.

The IBM Security Identity Manager and Role Management software does not use cookies or other technologies to collect personally identifiable information. The only information that is transmitted between the server and the browser through a cookie is the session ID, which has a limited lifetime. A session ID associates the session request with information stored on the server.

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/us/en> sections entitled “Cookies, Web Beacons and Other Technologies” and “Software Products and Software-as-a Service”.



---

## Glossary

This glossary includes terms and definitions for IBM Security Privileged Identity Manager.

The following cross-references are used in this glossary:

- See refers you from a term to a preferred synonym, or from an acronym or abbreviation to the defined full form.
- See also refers you to a related or contrasting term.

To view glossaries for other IBM products, go to [www.ibm.com/software/globalization/terminology](http://www.ibm.com/software/globalization/terminology) (opens in new window).

---

### A

#### account

An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

#### adapter

An intermediary software component that allows two other software components to communicate with one another.

#### application server

A server program in a distributed network that provides the execution environment for an application program.

#### audit trail

A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

---

### C

#### collector

A web service that accepts uploads of recordings and stores them into a permanent storage medium. This web service is a component of the session recording server.

#### credential

Information acquired during

authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

#### credential pool

A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

#### credential vault

A configured repository that stores credentials for shared access management.

---

### D

#### deprovision

To remove a service or component. For example, to deprovision an account means to delete an account from a resource.

#### digital certificate

An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

#### directory server

A server that can add, delete, change, or search directory information on behalf of a client.

---

### E

#### endpoint

The system that is the origin or destination of a session.

**event** An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

---

## F

**frame** A unit of information in a recording. A frame can either be a screen capture or information about mouse events, keyboard events, or other relevant events.

---

## I

### IMS Server

An integrated management system for ISAM ESSO that provides a central point of secure access administration for an enterprise. It enables centralized management of user identities, AccessProfiles, authentication policies, provides loss management, certificate management, and audit management for the enterprise.

---

## M

### managed resource

An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

---

## P

### password

In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

### permission

Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code.

### plug-in

A separately installable software module that adds function to an existing program, application, or interface.

**policy** A set of considerations that influence the behavior of a managed resource or a user.

### profile

Data that describes the characteristics of a user, group, resource, program, device, or remote location.

### provisioning policy

A policy that defines the access to various managed resources, such as applications

or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

---

## R

### recording

A collection of information about user actions performed on a monitored application for some time.

### recording agent

A shared library loaded into a monitored application's process space that captures frames.

### recording daemon

A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

### resource

A hardware, software, or data entity. See also managed resource.

### retriever

A web application that provides access to stored recordings.

---

## S

### shared access

Access to a resource or application using a shared credential. See also credential.

### shared access policy

A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, specific credential, all pool or credentials with the same organization container context.

### single sign-on (SSO)

An authentication process in which a user can access more than one system or application by entering a single user ID and password.

**SSO** See single sign-on.

---

## W

**wallet** A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

---

# Index

## A

- accessibility x
- AccessProfiles 73
  - IBM Personal Communications 74
  - VMware vSphere Client 75
- active-passive configuration, disaster recovery 81
- availability, enhance using monitoring URLs 84

## B

- bulkload command errors 99

## C

- client application logon, automatic check-out and check-in 73
- command line interface
  - clean 43
  - global commands 46
  - virtual appliance 41
  - virtual appliance services 48
- commands, IBM Security Privileged Identity Manager 41
- common issues 92
- configuration response samples 101
- configure
  - load balancer 54
- core dump
  - command line interface 43
- credential pool 76
  - checking in credential 77
- credential vault, checking in 79
- credentials
  - check-in 76
  - check-out 76
  - checking in, in credential pool 77
  - checking into the credential vault 79

## D

- data store, reconfiguration 63
- database
  - configuration, data store 51
- database server
  - configuration 12
  - installation 12
- directory server
  - configuration 53
  - installation 14
  - reconfiguration 65
- disaster recovery, active-passive configuration 81

## E

- education x

- enable trace
  - command line interface 48

## F

- features, overview 1
- feed files, management 57
- firmware settings, management 34
- fix pack, installation 35

## G

- global commands, command line interface 46

## H

- hardware and software requirements 2
- host, supported virtual hypervisors 3

## I

- IBM
  - Software Support x
  - Support Assistant x
- IBM Personal Communications 74

## K

- known issues and workaround 97
  - browser issues 97
  - dashboard panel widget display issues 97
  - Microsoft Internet Explorer 10 97
  - update\_syslog command issues 97

## L

- language support, internationalization 1
- LDAP
  - installation and configuration 14
  - management 53
- limitations
  - IBM Security Access Manager for Enterprise Single Sign-On 95
  - IBM Security Identity Manager 95
  - IBM Security Privileged Identity Manager 95
- logs
  - configuration 63
  - configuration management 61
  - retrieval 62

## M

- mail
  - configuration 23
  - management 55

- mainframe applications 74
- member node
  - wizard, initial configuration 25
- Microsoft Remote Desktop Connection 74
- Microsoft Remote Desktop Services (RDP)
  - See RDP
- Microsoft Remote Desktop Services (RDS)
  - terminal server
    - See terminal server

## N

- Nodes
  - member 58
  - primary 57
  - remove 58

## O

- online
  - publications ix
  - terminology ix
- overview
  - features 1
  - language supported 1

## P

- passwords 90
  - sync problems 90
- personas 6
- prerequisite software, installation 12
- problem-determination x
- properties
  - ad hoc reporting 55
  - enRole 55
  - management 55
  - ReportDataSynchronization 55
  - SelfServiceUI 55
  - ui 55
- publications
  - accessing online ix
  - list of for this product ix
- PuTTY, log on 73

## R

- RDP 74
- Remote Desktop Protocol (RDP)
  - See RDP
- Remote Desktop Services (RDS) RDP
  - See RDP
- remote terminals 73
- restart or shutdown 40
- restrict operations
  - member node 89
- roadmap
  - virtual appliance setup 3

## S

- server
  - configuration 23
  - installation 3
- session recording
  - configuration 68
  - enabling 51
- setup
  - directory server, SSL 15
- shared access
  - configuration 67, 70
  - settings 67
- shared credentials
  - check-in and check-out 67, 73
  - manual check-in 76
- snapshot
  - creating, primary virtual appliance 82
- snapshots, management 39
- SSL Certificate configuration 23
- sub sections, IBM Security Privileged Identity Manager commands 41
- support, troubleshooting 89
- synchronize
  - member node 60
  - primary node 60

## T

- terminal host 73
- terminal server 73
- terminology ix
- training x
- troubleshooting x
  - checking logs 92
  - cluster bootstrap process 90
  - LDAP Server running 99
  - logon to session reply console 97
  - support 89
  - virtual appliance
    - startup problems 98
  - virtual appliance snapshots 98

## U

- update\_syslog command
  - issues 97
- upgradeupgrade
  - IBM Security Privileged Identity Manager Virtual Appliance 85
- use cases 6

## V

- virtual appliance 75
  - command line interface 41
  - dashboard 26
  - first steps 23
  - format 3
  - getting started 5
  - initial settings 19
  - installation 19
  - logging on 26
  - managing 51
  - primary backup 81

- virtual appliance (*continued*)
  - primary, setting up 81
  - reconnect node 59
  - reverting to backup 82
  - secondary, setting up 83
- virtual appliance dashboard 29
  - administrator settings, configure 38
  - date and time, configure 38
  - manage mode selection 22
  - viewing about page 35
  - viewing and using quick links 32
  - viewing and using server control 31
  - viewing cluster status 29
  - viewing CPU utilization 36, 37
  - viewing deployment statistics 31
  - viewing disk usage 32
  - viewing IP addresses 32
  - viewing licensing 33
  - viewing memory utilization 36
  - viewing middleware and server monitor widget 31
  - viewing notifications 29
  - viewing partition information 33
  - viewing update history 33
- virtual machine 75
  - system settings configuration 18
- VMware
  - ESXi 5.0 3
  - ESXi 5.1 3
- VMware vSphere Client 75

## W

- wizard, initial configuration 23





Printed in USA

SC27-5625-01

