

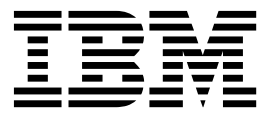
IBM Security Privileged Identity Manager
Version 2.1.1

Product Overview Guide



IBM Security Privileged Identity Manager
Version 2.1.1

Product Overview Guide



Note

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

Edition notice

Note: This edition applies to Version 2.1.1 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 2013, 2017.

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

Contents

Figures	v	Cognos Reports	18
Tables	vii	REST APIs.	19
Chapter 1. IBM Security Privileged Identity Manager overview	1	Chapter 7. Technical overview.	21
Chapter 2. New in Version 2.1.1	3	Chapter 8. Language support overview	25
Chapter 3. Obtaining software images.	5	Chapter 9. Cookbooks	27
Chapter 4. Hardware and software requirements	7	Chapter 10. Cross-product integration	29
Virtual appliance overview	7	Integration with IBM Security Access Manager	29
Client deployment modes	7	Overview	29
Managed resources support	8	Version requirements	30
Chapter 5. Known issues	11	IBM Security Access Manager Platform Reverse Proxy (WebSEAL) configuration	30
Chapter 6. Features overview	13	IBM Security Access Manager two-factor authentication (2FA) to IBM Security Privileged Identity Manager web consoles configuration	35
Shared access management	13	Integration with IBM QRadar Security Intelligence Platform	42
Automatic check-out and check-in of shared credentials.	13	Configuring the log sources	43
Manual check-out and check-in of shared credentials.	14	Enabling syslog on the IBM Security Privileged Identity Manager virtual appliance	43
Session recording	14	Integration with IBM Security Guardium	44
Screen-based recordings	15	Creating a user to access database views	44
Text-based recordings	15	Integration with IBM Security Identity Manager	45
Application identities	15	Integration with IBM Security Identity Manager scenarios	49
Privileged Session Gateway	16	Integration with SoftLayer	53
Password and SSH Key management.	17	Integration with IBM Security Identity Governance and Intelligence	54
Single sign-on	18	Notices	55
Request and approval workflows for access requests	18		

Figures

1. Session recording components. (Privileged Access Agent client deployments) 14
2. IBM Security Privileged Identity Manager components 21

Tables

1. Ways of using privileged credentials to access managed resources	13	13. Authenticated junctions for Privileged Session Recorder	42
2. Supported key formats and features.	17	14. Comparing features between a standalone IBM Security Privileged Identity Manager and one that is integrated with IBM Security Identity Manager	47
3. Available consoles	22	15. User experience differences	48
4. Supported languages	25	16. Types of users to be on-boarded	50
5. IBM Security Access Manager version requirements	30	17. Create an ISPIM administrative domain and ISPIM account	50
6. Types of Access Control Lists (ACLs)	30	18. Create a shared access policy.	50
7. Junctions for Privileged Credential Manager (PCM)	32	19. Assign Privileged Administrator as access owner	51
8. Junctions for IBM Security Access Manager for Enterprise Single Sign-On (ISAM ESSO)	32	20. Check out the administrative account	51
9. Junctions for Privileged Session Recorder (PSR)	32	21. Grant access to the Pinnacle Server	52
10. IBM Security advanced configuration	38		
11. Authenticated junctions for Privileged Credential Manager	42		
12. Authenticated junctions for IBM Security Access Manager for Enterprise Single Sign-On	42		

Chapter 1. IBM Security Privileged Identity Manager overview

IBM® Security Privileged Identity Manager helps organizations manage, automate, and track the use of shared privileged identities.

The solution provides the following features:

- Centralized administration, secure access, and storage of shared credentials
- Access control for shared credentials
- Lifecycle management of shared credential passwords and SSH Keys
- Single sign-on with automated check-out and check-in of shared credentials
- Shared credentials usage auditing
- Session recording and replay
- Integration with the broader Identity and Access Management Governance portfolio
- Application identity management

Privileged IDs are user IDs that have security, administrative, or system privileges. These IDs include pre-built administrative accounts found in operating systems and applications, such as root, administrator, sa, db2admin.

In an enterprise environment, multiple administrators might share access to a single privileged ID for easier administration. When multiple administrators share accounts, you can no longer definitively prove that an account was used by one administrator as opposed to another. You lose personal accountability and audit compliance.

With IBM Security Privileged Identity Manager, organizations can better manage privileged IDs. It ensures that a privileged user can acquire privileged credentials only:


- If they need it
- When they need it
- If they have access to it

When used with Privileged Access Agent or Privileged Session Gateway, privileged users can log on to a system without any knowledge of the password or SSH Key for the privileged identity.

Related information:

 [Demo: IBM Security Privileged Identity Manager](#)

This short video explains how privileged accounts are a key source of insider threats because of their "super user" access capabilities and because they are shared by multiple individuals.

 [Demo: Combat insider threats](#)

Learn how IBM can help organizations thwart insider threats by protecting and monitoring privileged user accounts and activities with IBM Security Privileged Identity Manager.

Chapter 2. New in Version 2.1.1

This version delivers new features, enhancements, currency support, and security product integration.

For the latest information about the release and how to download the latest fix packs, see Fix Packs.

2.1.1 Release

Virtual appliance platform

Some of the feature enhancements include:

- Local Management Interface (LMI) certificate configuration support. See "Managing certificates" in the *IBM Security Identity Manager Installation and Configuration Guide*.
- Local Management Interface (LMI) tracing can be enabled through the Virtual Appliance CLI
- Network gateway can be specified for the application interface
- Single network interface (NIC) to set up the virtual appliance

Note: 3 network interfaces (NICs) are necessary when you are configuring an application interface.

- IBM Security Directory Integrator adapters management. See
- VMware Virtual hardware version 11 support

SSH Key Management

IBM Security Privileged Identity Manager now supports SSH key pairs as an authentication method. The private keys of the key pair are stored in a key vault and SSH Key management at the account level on the end points is controlled by IBM Security Privileged Identity Manager. IBM Security Privileged Identity Manager also handles automatic and scheduled rotation of the private keys that it manages. Privileged Users can check out keys and securely connect to end points with Privileged Session Gateway. IBM Security Privileged Identity Manager also supports export and download of keys based on the administrative policy.

See "Password and SSH Key Management" in the *IBM Security Privileged Identity Manager Product Overview Guide*.

Web Service Integration

System Administrators can now create Web Service Integrations to integrate with other applications through REST calls in the check-out workflow.

See "Creating a Web Service Integration extension template in the *IBM Security Privileged Identity Manager Administrator Guide*.

Enhancements

Documentation updates

New *Cross-product integration* chapter. The chapter provides information about the integration of IBM Security Privileged Identity Manager with

other security products to deliver an integrated solution. See "Cross-product integration" in the *IBM Security Privileged Identity Manager Product Overview Guide*

New *Cookbooks* chapter. This chapter provides information about IBM Security Privileged Identity Manager cookbooks that provide how-to information and tasks on deployment scenarios. See "Cookbooks" in the *IBM Security Privileged Identity Manager Product Overview Guide*.

Chapter 3. Obtaining software images

IBM Security Privileged Identity Manager installation files can be obtained from the IBM Passport Advantage® website.

The installation files are available on the Passport Advantage website in the form of eAssembly packages for supported operating systems.

Instructions for downloading the software or the virtual appliance

Before you begin, see the *IBM Security Privileged Identity Manager Virtual Appliance Quick Start Guide*.

To download the appropriate installation packages, see <http://www.ibm.com/support/docview.wss?uid=swg24044287>.

To download the latest fix packs, go to Fix Central.

Installation procedure

For the list of late-breaking changes or known issues, see the Supplementary Release Notes.

To install, see *IBM Security Privileged Identity Manager Installation and Configuration Guide*.

Chapter 4. Hardware and software requirements

Verify that you meet the different requirements for each of the components. Compliance with requirements can prevent deployment issues.

Note: Hardware and software requirements are continuously updated. Ensure that you review the latest updates for these requirements at Software Product Compatibility Reports.

1. Click **Detailed system requirements**.
2. Enter Privileged Identity Manager in the **Full or partial product name** field.
3. Select the product version.
4. Click **Submit**.

Virtual appliance overview

The IBM Security Privileged Identity Manager virtual appliance provides a graphical management interface, a configuration wizard, tools, and a dashboard.

IBM Security Privileged Identity Manager virtual appliance includes the following features:

- A configuration wizard for the first time configuration of the IBM Security Privileged Identity Manager solution in 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, CPU utilization, and troubleshooting log files.
- Control of system settings, such as host name, date, time, and network settings.
- A graphical management interface for configuring the IBM Security Privileged Identity Manager features.

Client deployment modes

Privileged Access Agent is a client-side component that provides automatic check-out and check-in of credentials on managed resources. You can deploy the client either on user workstations, a Citrix gateway or Remote Desktop Gateway server that acts as a gateway.

Client on user workstations

In this mode, Privileged Access Agent performs automated check-out, check-in, and session recording operations on applications that are running on user workstations. This deployment mode is suitable when users do not have administrative privileges on their workstations.

The workstations where Privileged Access Agent is installed must be configured to run in the default "personal desktop" mode in IBM Security Access Manager for Enterprise Single Sign-On. *Shared desktop* and *private desktop* configurations are not supported.

Client on Citrix gateway

For enhanced security and easier management, Privileged Access Agent can be deployed on a Citrix XenApp server that acts as a gateway to the managed resources. The client performs automated check-out, check-in, and session recording operations on published applications that are running on the Citrix XenApp server.

Users access applications that are used for connecting to the managed resources, such as Remote Desktop Connection Client and PuTTY, through the Citrix Receiver application.

In this mode, the Privileged Access Agent does not need to be installed on user workstations. If the client is also on the workstation that is used to access the Citrix gateway, then the client on the Citrix gateway can use the Virtual Channel connection or operate in Lightweight mode. See *IBM Security Privileged Identity Manager Access Agent on a Gateway Guide*.

Client on a Remote Desktop Gateway

Remote Desktop Gateway, a role service that is part of the Remote Desktop Services server role on Windows Server 2012, enables organizations to provide access to standard Windows programs from virtually any location and from the Internet or an intranet.

Similar to the Citrix gateway, the Remote Desktop Gateway acts as a gateway to the managed resources. In this mode, the Privileged Access Agent client can be deployed on a Remote Desktop Gateway server as a RemoteApp. Programs published as RemoteApp programs are accessed remotely by users through Remote Desktop Services or Remote Desktop Web Access and appear as if they are running on the local computer.

Users can perform automated check-out, check-in, and session recording operations with privileged credentials that are managed by IBM Security Privileged Identity Manager and with other RemoteApp programs like PuTTY.

See "Access Agent on Virtual Desktop Infrastructure" in the *IBM Security Privileged Identity Manager Access Agent on a Gateway Guide*.

For more information, go to the Microsoft website and search for Remote Desktop Gateway 2012.

Managed resources support

The IBM Security Privileged Identity Manager supports automated check-out and check-in of credentials on many types of managed resources.

Some of the types resources include:

- Linux/UNIX, Windows operating systems
- Mainframe applications
- Web applications
- Database administration tools
- VMware vSphere server

IBM Security Privileged Identity Manager also supports automated password and SSH Key management of credentials through adapters for identity providers, such as local operating system registries, Active Directory or LDAP registries, and application-specific registries.

Chapter 5. Known issues

Review a list of known issues for IBM Security Privileged Identity Manager, Version 2.1.1.

Tip: To review a continuously updated list of known limitations, solutions, and workarounds for IBM Security Privileged Identity Manager, see Supplementary Release Notes.

For known limitations in the virtual appliance with prerequisite components at the time of release, see "Limitations" in the *IBM Security Privileged Identity Manager Troubleshooting Guide*.

Known issues are also documented in the form of individual tech notes in the Support knowledge base.

- Search technotes for product related issues
- Search technotes for virtual appliance related issues

For limitations that are related to other products in the IBM Security Privileged Identity Manager solution, see the following links:

- IBM Security Access Manager for Enterprise Single Sign-On product documentation
- IBM Security Identity Manager product documentation
- Identity Adapters product documentation
- IBM Security Directory Integrator product documentation

Note: Formerly known as IBM Tivoli® Directory Integrator.

- IBM Cognos® Business Intelligence product documentation

Chapter 6. Features overview

IBM Security Privileged Identity Manager provides shared access management, session recording, application identity management, single sign-on, automatic password and SSH Key management, access request workflows, and report generation features.

Shared access management

IBM Security Privileged Identity Manager supports automatic and manual check-out and check-in of shared credentials or SSH keys.

A shared credential enables multiple users to use the same account to access a resource. A credential consists of an account ID and password or SSH Key. If credential check-out is required, only one user can access the credential at a particular time. Otherwise, multiple users can access the credential at the same time.

Table 1. Ways of using privileged credentials to access managed resources

Who	Action	How
Privileged Users	Automatic credential check-out and check-in with a local client application.	Privileged Access Agent
	Automatic credential check-out and check-in for SSH sessions without a local client application.	Self-service console with Privileged Session Gateway configured.
	Manual credential check-out and check-in.	Self-service console
Privileged Administrators	Check in credentials on behalf of other users.	Service Center

Automatic check-out and check-in of shared credentials

Privileged users can automatically check out and check in shared access credentials from IBM Security Privileged Identity Manager for convenience.

Ways that credentials are checked out and checked in automatically:

- The Privileged Session Gateway automates the check-out and check-in of credentials for SSH managed resources with zero agents on client computers.
- The Privileged Access Agent client, when published on a desktop or application virtualization solution such as a Citrix or Microsoft Remote Desktop Services Gateway, automates the check-out and check-in of credentials with zero agents on client computers.
- The Privileged Access Agent client automates the check-out and check-in of shared access credentials on Windows-based client computers. Privileged Access Agent automatically checks in shared access credentials when you log out, exit, or close the resource.

AccessProfiles define the automatic logon process for different client applications.

Manual check-out and check-in of shared credentials

Some IBM Security Privileged Identity Manager deployments do not require automated access to shared credentials. Users who have sufficient privileges, such as membership in the Privileged Users group, can manually access shared credentials.

Privileged Users can manually check out shared credentials for workflows and applications that are not supported by the bundled Privileged Identity Management AccessProfiles. Privileged Users can also opt to check out SSH key authenticated credentials manually.

For supported client applications, Privileged Access Agent can be configured to prompt privileged users to use shared credentials. Privileged Access Agent checks out and injects credentials automatically to the logon prompt.

Note: Privileged Session Recording is not effective with manual check-out.

Privileged Users can use the Self-service console for manual check-out and checkin.

Session recording

You can record privileged identity sessions for auditing, security forensics, and compliance.

Recordings are stored in a centralized database. To find recorded sessions or play back recordings, you can use the web-based Privileged Session Recorder console.

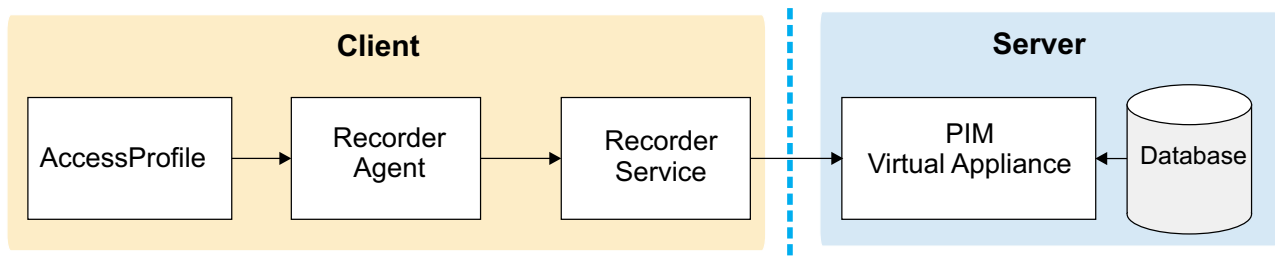


Figure 1. Session recording components. (Privileged Access Agent client deployments)

Recordings are either snapshots of the screen or a text-based representation of the console. Recordings include metadata that can be searched.

For deployments with the Privileged Session Gateway, SSH sessions are recorded and played back as text-based recordings.

The software includes some AccessProfiles that have session recording enabled for client deployments with the Privileged Access Agent.

The following client applications are supported:

PuTTY, or IBM Personal Communications for terminal sessions

Captured and played back as text-based recordings.

Microsoft Remote Desktop for remote desktop sessions

Captured as snapshots.

VMware vSphere for sessions on virtualized infrastructure

Captured as snapshots.

SQL Server Management Studio for database administrator sessions

Captured as snapshots.

SecureCRT for terminal sessions

Captured as snapshots.

IBM SoftLayer® for hosted cloud platform administrator sessions

Captured as snapshots.

IBM DB2® Data Studio for database administrator sessions

Captured as snapshots.

Note: To add session recording support for other client applications, you can design your own custom AccessProfiles. See “AccessProfiles” in the *IBM Security Privileged Identity Manager Installation Guide*.

For more information, see “Session recording administration” in the *IBM Security Privileged Identity Manager Administrator Guide*.

Screen-based recordings

Recordings are captured as a sequence of snapshots of the screen. Screen-based recordings typically apply to desktop-based or graphics-driven applications, such as VMware vSphere, SQL Server Management Studio, and Microsoft Remote Desktop.

Text-based recordings

Text-based recordings apply to terminal based applications, such as PuTTY, IBM Personal Communications, or the Privileged Session Gateway. Text that displays in the terminal window is captured.

Differences exist between different types of text-based recordings:

- For recordings that are triggered by Privileged Access Agent with PuTTY or Privileged Session Gateway to UNIX endpoints, commands that you enter during the session are captured.

When you play back recordings, the identified commands are indexed and displayed in a command list sidebar. In the Privileged Session Recorder console, global and advanced search is enhanced because you can find recordings by entering matching commands as keywords.

- For recordings that are triggered by the Privileged Access Agent with IBM Personal Communications to mainframe applications, commands are not captured.

Application identities

Application administrators can use IBM Security Privileged Identity Manager for Applications (App ID) to remove hardcoded and unsafely stored credentials from applications, application services, and scripts. App ID can also be used to manage the credential entitlements for each application, track the use of each credential, and automate periodic password.

App ID is a feature that must be activated separately. The App ID toolkit manages credentials that are used in the following applications:

Java EE Applications accessing databases

Credentials that are used for establishing a JDBC connection in supported Java™ EE application servers can be managed by installing the App ID Java EE data source. No code change is required for the applications that are running on the application server.

Java Applications

Credentials that are used by a Java application can be managed by modifying the applications to get the credentials by using the App ID Java SDK.

Scripts

Credentials that are stored in a script can be managed by modifying the script to get the credentials by running the Java-based App ID Command-Line tool.

Windows services

Credentials that are associated with Windows services can have passwords updated periodically by a service management agent by running the App ID Command-Line tool.

Windows Task Scheduler tasks

Credentials that are associated with Windows Task Scheduler tasks can be managed by a service management agent by running the Java-based App ID Command-Line tool.

The App ID Java EE data source, Java SDK, and CLT are packaged in a single JAR file.

See “Application identity management” in the *IBM Security Privileged Identity Manager Administrator Guide*.

Privileged Session Gateway

With the Privileged Session Gateway, privileged users can log on to SSH managed resources from a web-based console without installing extra client software on workstations.

The gateway is deployed between the privileged users end point and the managed resource.

The Privileged Session Gateway provides the following benefits:

Single sign-on

Secure privileged sessions with single sign-on without exposing privileged credentials to the client end points.

Agentless deployment

Privileged users can access the managed hosts without installing any additional agent software on their workstation.

Clientless access

Privileged users can access the managed hosts by using a web browser.

See “Privileged Session Gateway usage” in the *IBM Security Privileged Identity Manager Reference Guide*.

Password and SSH Key management

Automatic password or SSH Key management enables IBM Security Privileged Identity Manager to change the passwords or SSH Keys of connected credentials on a schedule that you determine.

The reset intervals can be set for privileged credentials in the Privileged Identity Manager Service Center during the on-boarding of credentials.

For more information, see the following topics:

- "Adding credentials in the Privileged Identity Manager Service Center" in *IBM Security Privileged Identity Manager Administrator Guide*
- "Connecting a credential to an identity provider" in *IBM Security Privileged Identity Manager Administrator Guide*
- "Configuring a reset interval for a credential" in *IBM Security Privileged Identity Manager Administrator Guide*
- "Configuring a lifecycle rule" in *IBM Security Privileged Identity Manager Administrator Guide*

Privileged Administrators can specify the credential type (Password or SSH Key) when creating credentials in the Privileged Identity Manager Service Center.

Verify that the SSH Key you are uploading meet the different key types, formats, and ciphers that IBM Security Privileged Identity Manager supports.

The following private key formats are supported:

- Legacy OpenSSH (PEM)
- New OpenSSH (after version 6.5)
- PKCS#8

Table 2. Supported key formats and features.

Key Algorithms	Key Size	Key Rotation	Privileged Session Gateway	Download Key Format		
				OpenSSH	OpenSSH (after version 6.5)	PuTTY
RSA	2048	Yes	Yes	Yes	Yes	Yes
	3072					
	4096					
ECDSA	256	Yes	No	Yes	Yes	No
	384					
	521					

The following ciphers are supported for each encrypted private key:

- AES-128-CBC
- AES-192-CBC
- AES-256-CBC
- DES-CBC
- DES-EDE3-CBC
- CAMELLIA-128-CBC

- CAMELLIA-192-CBC
- CAMELLIA-256-CBC
- SEED-CBC

Single sign-on

IBM Security Privileged Identity Manager provides single sign-on with Privileged Access Agent for supported applications or Privileged Session Gateway to SSH managed endpoints with automatic check-out and check-in of shared credentials.

- Single sign-on with Privileged Session Gateway is available for resource types that support the SSH-protocol.
- Single sign-on with Privileged Access Agent is available for resource types with a supported logon AccessProfile for the client application.

See “Automatic check-out and check-in of shared credentials” on page 13.

Request and approval workflows for access requests

Privileged Administrators can configure an approval workflow for an access entitlement.

See “Creating an access request workflow” in *IBM Security Privileged Identity Manager Administrator Guide*.

Cognos Reports

The IBM Security Privileged Identity Manager solution supports the IBM Cognos reporting framework for report generation.

The reporting package includes the following reports:

Application ID Registration Report

This report shows the registered application instances and the details about each registered instance, such as the host, instance name, and description.

Application Instance Activity Audit Report

This report shows the auditable events or actions that have occurred with privileged credentials on a registered application instance.

Shared Access Entitlements by Owner Report

This report shows the credentials and credential pools that are owned by the selected owner.

Shared Access Entitlements by Role Report

This report shows the information about the credentials and credential pools that are entitled by the selected role.

Shared Access Entitlement Definition Report

This report shows the configuration information of Privileged IDs and the Shared Access Policies that are associated with these Privileged IDs.

Shared Access History Report

This report shows the history of actions that are performed on the shared credentials.

Single Sign-On Privileged ID Audit Report

This report provides a log history of check-out and check-in actions that are performed for each privileged ID on the managed resource from

Privileged Access Agent. This report also includes a subreport that is called User Activity Audit Report. With this subreport, you can play back the user session recording or view the terminal commands that the user executed on the managed resource.

Privileged Session Recorder Report

This report shows the history of activities that occurred in the Privileged Session Recorder console. You can use this report to track and monitor the actions of the selected user in the Privileged Session Recorder console.

Management Activity Report

This report shows various administrator activities and the details of each activity, such as event category, resource, entity type, and identity provider name.

Check-In Check-Out Activity Per Resource Report

This report shows the details of check-in check-out activities under selected resources, such as number of checkouts, number of privileged users, and number of credentials.

Check-In Check-Out Activity History Report

This report shows the list of check-in and check-out activities on credentials.

Check-In Check-Out Activity Per Credential Report

This report shows the check-in and check-out activities related to selected credentials.

Check-In Check-Out Activity Per Resource and Privileged User Report

This report shows the check-in and check-out activities based on selected resources and privileged user names.

Privileged Session Gateway Access History Report

This report shows a list of Privileged Session Gateway access history.

See “Report descriptions and parameters” in *IBM Security Privileged Identity Manager Administrator Guide*.

REST APIs

You can develop custom applications by using the REST application programming interfaces (APIs) that come with IBM Security Privileged Identity Manager. The REST APIs are available so that you can administer the tasks outside of the user interface.

For more information, download the IBM Security Privileged Identity Manager REST API developer documentation at <http://www.ibm.com/support/docview.wss?uid=swg21903311>

Chapter 7. Technical overview

The privileged identity management solution consists of IBM Security Privileged Identity Manager, a database, managed resources, and endpoints.

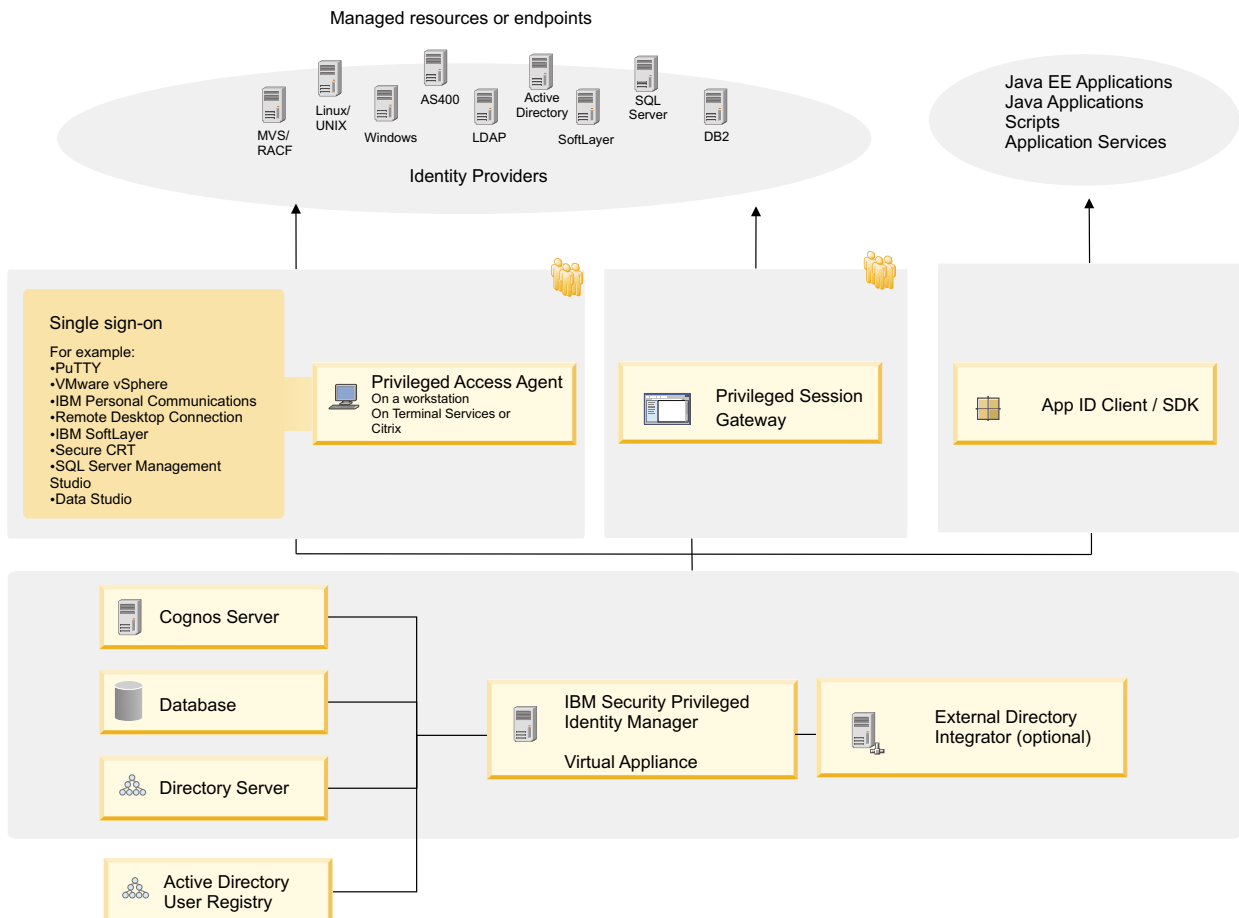


Figure 2. IBM Security Privileged Identity Manager components

IBM Security Privileged Identity Manager consists of the following components:

Privileged Credential Manager Virtual Appliance

The Privileged Credential Manager provides privileged administrators access to a credential or pool of shared credentials that are stored in a secure credential vault. It enforces access controls to credentials and automates or SSH Key password changes to these credentials. It also features user and system role management.

It provides the following consoles:

Table 3. Available consoles

Console	Description
Administrative console	<p>A Privileged Identity Manager Administrator and a privileged administrator can use this console to on-board credentials and setup access to these credentials.</p> <p>For information about the privileged administrator and Privileged Identity Manager Administrator, see "Roadmap of personas and tasks" in the <i>IBM Security Privileged Identity Manager Planning and Deployment Guide</i>.</p>
Privileged Identity Manager Service Center	A privileged administrator can use this console to on-board credentials and setup access to these credentials.
Self-service console	A privileged user can use this console to check out and check in entitled credentials and request access to credentials.

Privileged Access Agent

Provides single sign-on automation and session recording features when a privileged user needs to access a managed resource. It can be deployed on a user workstation or a gateway for shared workstation environments.

Single sign-on

Provides automated check-out and check-in of shared access credentials from the IBM Security Privileged Identity Manager Server.

Privileged Access Agent is the single sign-on client that is installed on user workstations. This agent automates the check-out and single sign-on with privileged credentials into various systems. Privileged Access Agent uses logon automation profiles (AccessProfiles) for specifications on how and when to check-out and single sign-on to different client applications. The Privileged Identity Manager Administrator uses the AccessStudio tool to create and maintain AccessProfiles that are uploaded to the virtual appliance for distribution to Privileged Access Agent. The Privileged Identity Manager Administrator uses the Single Sign-On administration console to configure the single sign-on and Session recording policies.

Session recording

Privileged Session Recorder is a virtual surveillance camera that captures user activity during an active session on a workstation.

The Privileged Session Recorder is comprised of a server component in the IBM Security Privileged Identity Manager virtual appliance and a client component in the Privileged Access Agent.

Privileged Access Agent consults the AccessProfile of an application for specifications of when to start and stop recording a session.

The captured recordings are submitted to the Privileged Session Recorder server component where they are stored in the IBM

Security Privileged Identity Manager database. You can later search and replay these recordings through the Privileged Session Recorder console.

App ID Toolkit

Manages privileged credentials that are embedded in applications, Windows services, scripts, or Java EE data sources when they are registered with App ID Toolkit.

Privileged Session Gateway

Provides Privileged Users access to SSH-enabled resources from a web-based console.

Cognos report server

Provides access to IBM Security Privileged Identity Manager reports.

IBM Security Privileged Identity Manager database

Stores credential data, access roles and policies, single sign-on AccessProfiles, audit logs and session recordings.

Directory server

Stores IBM Security Privileged Identity Manager user accounts and operational data.

Active Directory User Registry

IBM Security Privileged Identity Manager can use an external Active Directory server to perform user authentication.

Adapters

Automates password or SSH Key change of managed credentials. The virtual appliance includes an embedded Directory Integrator component with adapters for connecting to external systems. You can configure IIBM Security Privileged Identity Manager to connect to external adapters whenever you need them.

Chapter 8. Language support overview

The IBM Security Privileged Identity Manager virtual appliance is translated in several languages.

See the following table for the supported languages:

Table 4. Supported languages

Language	Supported
Arabic	No
Chinese (Simplified)	Yes
Chinese (Traditional)	Yes
Czech	No
Danish	No
Dutch	No
English (United States)	Yes
Finnish	No
French (Standard)	Yes
German	Yes
Greek	No
Hebrew	No
Hungarian	No
Italian	Yes
Japanese	Yes
Korean	Yes
Polish	No
Portuguese (Brazilian)	Yes
Russian	Yes
Spanish	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.

Chapter 9. Cookbooks

Cookbooks are scenario-based, step-by-step guides that provide how-to information and tasks so that you can successfully deploy the specified scenario.

IBM developers create Cookbooks, which are supplementary resources. They are located and updated in IBM IdentityDev. Documents in IBM IdentityDev might not be translated or supported by IBM Support.

Chapter 10. Cross-product integration

IBM Security Privileged Identity Manager can be used with other security products to deliver an integrated solution.

Integration with IBM Security Access Manager

This guide provides information about how to configure IBM Security Access Manager virtual appliance as a reverse proxy (WebSEAL) to front the IBM Security Privileged Identity Manager virtual appliance.

By using IBM Security Access Manager as a front proxy for the IBM Security Privileged Identity Manager virtual appliance, two-factor authentication (2FA) and other authentication mechanisms that are supported by IBM Security Access Manager Advanced Access Control can be achieved for IBM Security Privileged Identity Manager web consoles.

Overview

IBM Security Privileged Identity Manager integrates with IBM Security Access Manager to support 2-factor, or strong, authentication mechanisms.

IBM Security Privileged Identity Manager virtual appliance is configured with the IBM Security Access Manager Extended Trust Association Interceptor (ETAI) to create authentication tokens for authenticated requests from WebSEAL.

The user can single sign-on to the following consoles with this token:

- Administrative console (/itim/console)
- Self-service UI (/itim/self)
- Service Center (/ispim/ui)
- AccessAdmin (/admin)
- Session Recording Playback Console (/recorder/ui)

Note:

1. When the WebSEAL front proxy feature is enabled, single sign-on tokens are accepted by all previously mentioned consoles.
2. The WebSEAL front proxy feature cannot be enabled or disabled on individual consoles.
3. The preferred user ID of the IBM Security Privileged Identity Manager user must not contain any spaces, otherwise the single sign-on token will not be accepted by the administrative console, self-service UI, and service center. This is a limitation between WebSEAL and IBM Security Privileged Identity Manager.
4. Single sign-on is not applicable to requests from Privileged Access Agent, Session Recording Agent, App ID Toolkit (including Service Management Agent), and the Virtual Appliance console.

See the *IBM Security Access Manager Product Guide* to complete the following tasks:

- Create Access Control Lists (ACLs)
- Create Reverse Proxy junctions

Version requirements

Verify that your system meets the IBM Security Access Manager version requirements before you configure IBM Security Access Manager as a reverse proxy.

Table 5. IBM Security Access Manager version requirements

IBM Security Privileged Identity Manager version	Supported IBM Security Access Manager version	Features required
2.0.2	9.0 with Fix Pack 1	<ul style="list-style-type: none">• IBM Security Access Manager Platform IBM Security Access Manager Platform is equivalent to the IBM Security Access Manager for Web offering in earlier releases.• Advanced Access Control Module This module is equivalent to the unique capabilities of IBM Security Access Manager for Mobile in earlier releases.

IBM Security Access Manager Platform Reverse Proxy (WebSEAL) configuration

IBM Security Access Manager Platform reverse proxy supplies authenticated session tokens to achieve web single sign-on (SSO).

This reverse proxy is also known as WebSEAL. It operates by having *junctions* to map incoming requests to back-end servers based on the path specified in the URI.

Types of Access Control Lists (ACLs)

Access Control Lists (ACLs) are used in junctions for IBM Security Privileged Identity Manager.

The IBM Security Access Manager administrator can use the default WebSEAL access control, **default-webseal**, as a reference and add the following access control modifications when required.

Table 6. Types of Access Control Lists (ACLs)

Access Control Lists (ACLs)	Any-other	Unauthenticated
Authenticated	Trx	T
Passthrough-REST	Tmdrx	Tmdrx
Passthrough-SOAP	Trx	Trx
Passthrough-static	Tr	Tr

Tmdrx Means traverse, modify, delete, read, and execute.

Passthrough-SOAP ACL

Used for SOAP web services that recognizes GET and POST verbs.

Passthrough-REST ACL

Used for REST web services that recognizes GET, POST, PUT, and DELETE verbs.

Passthrough-static ACL

Used for static web resources.

See the *IBM Security Access Manager Product Guide* to create Access Control Lists (ACLs).

Create IBM Security Access Manager Reverse Proxy (WebSEAL)

You must configure IBM Security Access Manager Reverse Proxy to work with the IBM Security Access Manager ETAI that is used in the IBM Security Privileged Identity Manager application servers.

Use the following suggested configuration:

Standard SSL junction

Application servers in the IBM Security Privileged Identity Manager virtual appliance are fronted by the IBM HTTP Server that is configured to only accept SSL connection on port 443.

Transparent path

Some junctions require unauthenticated Access Control Lists (ACLs) attached to it so traffic can pass through. For example, **Passthrough-SOAP** and **Passthrough-REST**. This is necessary for web services used by Privileged Access Agent, Session Recording Agent, and the App ID toolkit. You must define multiple junctions with a transparent path that is passed as the request URI to IBM Security Privileged Identity Manager applications. You must also attach the correct access control. See “Types of Access Control Lists (ACLs)” on page 30.

For example, `/itim/console` is an authenticated junction, and `/itim/services` is an unauthenticated junction.

Basic authentication header

IBM Security Privileged Identity Manager accepts the principal provided by WebSEAL in the 'IV-USER' header. To ensure its acceptance, IBM Security Privileged Identity Manager must trust WebSEAL. The trust can be established through HTTP basic authentication by WebSEAL to IBM Security Privileged Identity Manager by using the WebSEAL login ID. The trusted WebSEAL login ID must be provisioned as a user in the IBM Security Privileged Identity Manager user registry (Security Directory Server or Active Directory). The basic authentication header is only required for junctions that have authenticated Access Control Lists (ACLs) attached. Include session cookies and insert the client IP address in the HTTP header setting for those junctions.

Non-LTPA

IBM Security Access Manager ETAI generates LTPA tokens for IBM Security Privileged Identity Manager applications. They are based on the principal provided by WebSEAL instead of the junction. With these tokens, you can perform setup without synchronizing the LTPA key in the IBM Security Privileged Identity Manager virtual appliance cluster or importing it into IBM Security Access Manager.

See the *IBM Security Access Manager Product Guide* to create Reverse Proxy junctions.

Junctions for Privileged Credential Manager:

This topic provides a list of junctions that are required for Privileged Credential Manager.

Table 7. Junctions for Privileged Credential Manager (PCM)

Path	Purpose	Access Control Lists (ACLs)
/itim/console	Administrative console	Authenticated
/itim/self	Self-service UI	Authenticated
/ispim/ui	Service Center	Authenticated
/itim/services	SOAP web services (used by Privileged Access Agent)	Passthrough-SOAP
/ispim/rest	REST web services	Passthrough-REST
/ispim/restlogin	REST web services login	Passthrough-REST
/ispim/uihelp	Service Center Page Help	Passthrough-static
/itim/messagehelp	TMS Message Detail	Passthrough-static
/itim/selfhelp	Self-service UI Page Help	Passthrough-static
/itim/consolehelp	Administrative Console Page Help	Passthrough-static
/ispim/ibm_security_logout	Log out url for clearing back-end sessions	Authenticated

Junctions for IBM Security Access Manager for Enterprise Single Sign-On:

This topic provides a list of junctions that are required for IBM Security Access Manager for Enterprise Single Sign-On.

Table 8. Junctions for IBM Security Access Manager for Enterprise Single Sign-On (ISAM ESSO)

Path	Purpose	Access Control Lists (ACLs)
/admin	AccessAdmin	Authenticated
/static	UI resources (used by AccessAdmin)	Passthrough-static
/ims/services	IMS SOAP APIs (used by Privileged Access Agent)	Passthrough-SOAP

Junctions for Privileged Session Recorder:

This topic provides a list of junctions that are required for Privileged Session Recorder.

Table 9. Junctions for Privileged Session Recorder (PSR)

Path	Purpose	Access Control Lists (ACLs)
/recorder/ui	Privileged Session Recorder console	Authenticated
/recorder/player	Retriever for REST web services	Passthrough-REST
/recorder/collector	Uploader for REST web services	Passthrough-REST

Edit the Advanced Configuration file

Edit the advanced configuration file on the IBM Security Access Manager Virtual Appliance to enable the IBM Security Privileged Identity Manager functions.

Specify the password of the WebSEAL login ID for basic authentication

The password of the WebSEAL login ID that is used when you enable WebSEAL integration in IBM Security Privileged Identity Manager virtual appliance must be specified to establish trust between WebSEAL and IBM Security Privileged Identity Manager through basic authentication.

```
[junction]
    basicauth-dummy-passwd = <the WebSEAL login ID password>
```

Enable HTTP Method PUT and DELETE

By default, WebSEAL blocks access to **PUT** and **DELETE** methods. To enable these methods, remove **PUT** and **DELETE** entries from `http-method-disabled-remote` in the WebSEAL configuration file.

```
[server]
    # Remove PUT, DELETE
    http-method-disabled-remote = TRACE,CONNECT
```

Client IP Forwarding

IBM Security Access Manager for Enterprise Single Sign-On audit logging and Privileged Session Recording fingerprint-based authentication requires the client IP address to be specified in the X-Forwarded-For header.

```
[header-name]
    client-ip-v4 = X-Forwarded-For
```

Reset cookies on user session logout

This setting removes the single sign-on token from the browser cookie when a user logs out from WebSEAL. It prevents a new user from logging in with the single sign-on token of the previously logged out user.

```
[junction]
    reset-cookies-list = JSESSION*,Ltpa*
```

Clearing back-end sessions on user session logout

With this setting configured, WebSEAL sends a request to the configured URI, including configured headers and cookies for the junction point on which it resides. Any session that might exist on the IBM Security Privileged Identity Manager back-end application servers are terminated.

```
[acct-mgt]
    single-signoff-uri = /ispim/ibm_security_logout
```

Configuring IBM Security Access Manager Reverse Proxy (WebSEAL) for Java Web Start Applications

Configure WebSEAL to allow Java Web Start applets to download JAR files through a custom Access Control List (ACL).

About this task

To access Java Web Start applets when IBM Security Privileged Identity Manager is protected by WebSEAL and single sign-on is enabled, configure WebSEAL so that the JAR files that are required by the applet are unprotected and can be fetched.

You can use the following procedures to configure the JAR files in the applet to **unprotected** mode in WebSEAL.

Procedure

1. Create an ACL and modify it to be accessible by an unauthenticated user with read-only permissions.
 - a. Access the IBM Security Access Manager CLI and login as an administrator.

In a command line, login as isam pdadmin with a sec_master credential by running the following commands:

```
www.isam.test>isam
www.isam.test:isam>admin
pdadmin>login
Enter user ID:sec_master
Enter password:
```

After you have successful login, run the following commands:

```
pdadmin sec_master>acl create unauth
pdadmin sec_master>acl modify unauth set unauthenticate Tr
pdadmin sec_master>acl modify unauth set any-other Tr
```

Note: If this ACL already exists in your environment, create a new ACL and provide another name.

2. Verify the parameters of the ACL that you just created by running the following commands:

```
pdadmin sec_master> acl show unauth
ACL Name: unauth
Description:
Entries:
  User sec_master TcmdbsvaBR1
  Unauthenticated Tr
  Any-other Tr
```

3. Run the following command to determine the WebSEAL object name space:**pdadmin sec_master>objectspace list**
4. Determine the applet object path from the /itim junction.

Run the following command to determine the applet object path:
pdadmin sec_master> object list /WebSEAL

All the WebSEAL object name is displayed. Identify the WebSEAL instance that is configured with IBM Security Privileged Identity Manager.

For example, /WebSEAL/www.isam.testisaminst, where isaminst is the WebSEAL instance name.

Run the following command to determine if the /itim junction exists:

pdadmin sec_master> object list /WebSEAL/www.isam.test-isaminst

The object that contains the /itim junction :/WebSEAL/<hostname fqdn>-<instance name>/junction is displayed. For example: /WebSEAL/www.isam.test-isaminst/itim.

Note: If the junction object space path is /WebSEAL/www.isam.test-isaminst/itim, then the path for the required jar files is /WebSEAL/www.isam.test-isaminst/itim/console/ applet.

5. Run the following command to attach the ACL to the applet object:**acl attach /WebSEAL/www.isam.test-isaminst/itim/console/applet unauth**
6. Run the following command to verify that the ACL is successfully attached to the applet object:

```
pdadmin sec_master> object show /WebSEAL/www.isam.test-isaminst/
itim/console/applet
Name: /WebSEAL/www.isam.test-isaminst/itim/console/applet
```

Description: Object from host isam.
Type: 16 (Management Object)
Is Policy Attachable: Yes
Extended Attributes:
Attached ACL: unauth
Attached POP:
Attached AuthzRule:

Effective Extended Attributes:
Effective ACL: unauth
Effective POP:
Effective AuthzRule:

7. Edit the WebSEAL configuration file by changing the property value in the instance with the `webseald.conf` file: **allow-unauth-ba-supply = yes**
8. Restart the runtime component and the WebSEAL instance.

IBM Security Access Manager two-factor authentication (2FA) to IBM Security Privileged Identity Manager web consoles configuration

By default, when users attempt to access an authenticated junction, WebSEAL authenticates users against its configured user registry. If more advanced authentication methods are desired, WebSEAL can delegate authentication of users to Advanced Access Control.

To avoid provisioning IBM Security Privileged Identity Manager users into WebSEAL user registry, it is recommended to use the IBM Security Privileged Identity Manager external authentication by importing the IBM Security Privileged Identity Manager custom authentication plug-in into Advanced Access Control. This will delegate the password check back to IBM Security Privileged Identity Manager.

IBM Security Access Manager Advanced Access Control supports an array of different authentication methods. For our purposes, we focus on the following authentication workflow:

1. External authentication against the IBM Security Privileged Identity Manager user registry by using the IBM Security Privileged Identity Manager custom authentication plug-in.
2. Two-factor authentication (2FA) in the form of One-Time Passwords (OTP) delivered by SMS or email by using the Advanced Access Control built-in OTP provider.

When the above configuration is combined, mobile numbers, or email addresses from the IBM Security Privileged Identity Manager user registry are passed on seamlessly to the OTP SMS Gateway or Simple Mail Transfer Protocol (SMTP) server to be used in OTP delivery, providing a smooth 2FA-secured user experience.

Ensure that you complete the following tasks before you configure the IBM Security Privileged Identity Manager external authentication and two-factor authentication (2FA):

- WebSEAL Configuration is enabled correctly in IBM Security Privileged Identity Manager virtual appliance. See *Configuring IBM Security Access Manager Reverse Proxy (WebSEAL) to front the virtual appliance*

- IBM Security Access Manager Reverse Proxy (WebSEAL) is configured correctly to front IBM Security Privileged Identity Manager. See “IBM Security Access Manager Platform Reverse Proxy (WebSEAL) configuration” on page 30.
- IBM Security Access Manager Reverse Proxy (WebSEAL) is configured correctly as the point-of-contact for Advanced Access Control Module. See the *IBM Security Access Manager Product Guide*.

The following topics describe the IBM Security Privileged Identity Manager external authentication and two-factor authentication (2FA) configuration.

IBM Security Privileged Identity Manager external authentication configuration

Configure the IBM Security Privileged Identity Manager external authentication to delegate the password check back to IBM Security Privileged Identity Manager to allow users to authenticate and access IBM Security Privileged Identity Manager junctions without requiring IBM Security Privileged Identity Manager users to be provisioned into the WebSEAL registry.

Perform the following tasks to configure the IBM Security Privileged Identity Manager external authentication:

- “Importing the IBM Security Privileged Identity Manager virtual appliance root signer certificate”
- “Importing and configuring the IBM Security Privileged Identity Manager custom authentication plug-in” on page 37
- “Configuring the Advanced Access Control advanced configuration settings” on page 38
- “Importing the IBM Security Privileged Identity Manager custom login pages” on page 39

Importing the IBM Security Privileged Identity Manager virtual appliance root signer certificate:

Import the IBM Security Privileged Identity Manager virtual appliance root signer certificate to IBM Security Access Manager Advanced Access Control.

Procedure

1. Import the IBM Security Privileged Identity Manager virtual appliance root signer certificate to IBM Security Access Manager Advanced Access Control.
 - a. In the IBM Security Access Manager virtual appliance console, click **Manage System Settings > SSL Certificates**.
 - b. Select **rt_profile_keys**.
 - c. Click **Manage > Edit SSL Certificate Database**.
 - d. In the Edit SSL Certificate Database- rt_profile_keys window, click **Manage > Import**.
 - e. Deploy the changes.
2. Restart the runtime server.
 - a. In the IBM Security Access Manager virtual appliance console, click **Secure Access Control > Runtime Parameters**.
 - b. Click the **Runtime Status** tab.
 - c. Click **Restart Local Runtime** and wait until the server is restarted. Check that the **Runtime Status** has changed to **Started**.

Importing and configuring the IBM Security Privileged Identity Manager custom authentication plug-in:

Procedure

1. Import the IBM Security Privileged Identity Manager custom authentication plug-in.
 - a. In the IBM Security Access Manager virtual appliance console, click **Secure Access Control > Extensions**.
 - b. Select the IBM Security Privileged Identity Manager custom authentication plug-in JAR file and click **Import**. For example, `com.ibm.ispim.authmech_1.0.0.0.jar`.
 - c. Deploy the changes.
2. Create a new authentication mechanism for the newly added authentication plug-in.
 - a. In the IBM Security Access Manager virtual appliance console, click **Secure Access Control > Authentication**.
 - b. Click the **Mechanisms** tab.
 - c. Click on the icon at the top left corner of the screen to add a new **IBM Security Privileged Identity Manager Authentication Mechanism**.
Fill in the information according to the attributes in the **General** tab.
Name Any name that identifies this authentication plug-in mechanism. For example, *ISPIM Username Password*.

Identifier

Enter `ispim`.

Fill in the information according to the attributes in the **Properties** tab.

Email Header

The email header name to store the email address that is fetched from the IBM Security Privileged Identity Manager user registry. This email header is used in the mapping rule or other authentication policy to retrieve the email address to send the One-Time-Password. For example, `ispim_email`. If this attribute is empty, by default it is set to `emailAddress` that is used by the default **MAC Email One-time Password** authentication policy for OTP delivery by email only.

Group to Assign

Group name in the local IBM Security Access Manager user registry to associate the external user for authentication. To create a new group in Policy Administration, see the *IBM Security Access Manager Product Guide*. If this attribute is empty, by default, it is set to `Security Group` which is already predefined in IBM Security Access Manager. It is suggested to create a new group.

Mobile Header

The mobile header name to store the mobile number that is fetched from the IBM Security Privileged Identity Manager user registry. This mobile header is used in the mapping rule or other authentication policy to retrieve the mobile number to send the One-Time-Password. For example, `ispim_mobile`. If this attribute is empty, by default, it is set to `mobileNumber` that is used by the default **MAC SMS One-time Password** authentication policy for OTP delivery by SMS only.

Server URLs

Enter the IBM Security Privileged Identity Manager hostname for external authentication. Multiple IBM Security Privileged Identity Manager servers can be specified. They are used in a failover method.

3. Create a new authentication policy for the IBM Security Privileged Identity Manager authentication mechanism that is added in Step 2.
 - a. In the IBM Security Access Manager virtual appliance console, click **Secure Access Control > Authentication**.
 - b. Click the **Policies** tab.
 - c. Click on the icon at the top left corner of the screen to add a new authentication policy.

Fill in the information according to the attributes.

Name Any name that identifies this authentication plug-in mechanism. For example, ISPIM Username Password.

Identifier

Enter `ispim`. Do not change this value. This identifier is used by the IBM Security Privileged Identity Manager custom login page.

- d. In **Workflow Steps**, select the IBM Security Privileged Identity Manager authentication mechanism added in Step 2.

Configuring the Advanced Access Control advanced configuration settings:

Configure the Advanced Access Control advanced configuration settings to use the correct External User EAI setting.

Procedure

Set the EAI header name to use the external user authentication.

1. In the IBM Security Access Manager virtual appliance console, select **Secure Federation > Global Settings > Point of Contact**.
2. Select **Access Manager Credential** and click **Create Like** to clone the profile.
3. In the Create Like Point of Contact Profile - Access Manager Credential window, follow the instructions on the screen and specify the following details:

Profile Name

Specify a profile name

Sign In

Specify the following details:

Table 10. IBM Security advanced configuration

Key	Value
<code>fim.attributes.response.header.name</code>	<code>am-eai-xattrs</code>
<code>fim.cred.response.header.name</code>	<code>am-eai-pac (by default)</code>
<code>fim.groups.response.header.name</code>	<code>am-eai-ext-user-groups</code>
<code>fim.target.response.header.name</code>	<code>am-eai-redirect-url</code>
<code>fim.user.request.header.name</code>	<code>iv-user</code>
<code>fim.user.response.header.name</code>	<code>am-eai-ext-user-id</code>

Importing the IBM Security Privileged Identity Manager custom login pages:

About this task

Note: Only English is supported in the custom login page in IBM Security Privileged Identity Manager 2.0.2.

Procedure

1. Modify the default WebSEAL login page to use the IBM Security Privileged Identity Manager custom login page.
 - a. In the IBM Security Access Manager virtual appliance console, select **Secure Web Settings > Reverse Proxy**
 - b. Select your WebSEAL instance.
 - c. Select **Manage > Management Root**
 - d. In the Manage Reverse Proxy Management Root- <WebSEAL instance name>, under **Management**, import `login.html`, `logout.html`, and `login_success.html` in all the sub folders.

Note: These files are located in the same bundle as the JAR file.

- e. Under **junction-root**, do the following tasks:
 - Create a **js** folder and import `nls.js`.
 - Create a **styles** folder and import `ispim.css`.
 - f. Deploy the changes and restart WebSEAL.
 - g. Use the Passthrough-static Access Control List. See the following topics:
 - “Types of Access Control Lists (ACLs)” on page 30
 - See “Manage ACL policies” in the *IBM Security Access Manager Product Guide*.
2. Import the IBM Security Privileged Identity Manager custom login page to **Advanced Access Control Module**.
 - a. In the IBM Security Access Manager virtual appliance console, select **Secure Access Control > Template Files**
 - b. Create a **pim** folder and import `pim/login.html` in `C/authsvc/authenticator`.

Note: This file is located in the same bundle as the JAR file.

Configuring Advanced Access Control built-in email and SMS One-time Password

Configure the IBM Security Access Manager Advanced Access Control to enable the built-in email and SMS One-Time-Password feature.

About this task

This configuration covers the scenario where the user is prompted to choose the OTP delivery options (SMS or email). Both the email and mobile number must be present for each user in the IBM Security Privileged Identity Manager user registry.

Procedure

1. Optional: Configure the Advanced Access Control built-in Mobile Active Code (MAC) One-time Password (OTP) provider.
 - a. In the IBM Security Access Manager virtual appliance console, select **Secure Access Control > Authentication**.

- b. Click the **Mechanisms** tab.
- c. Select **MAC One-time Password**.
- d. Click the **Modify Authentication Mechanism** icon to modify **MAC One-time Password**.

Set the values for the following properties:

- Password Character Set
- Password Length
- Store Entry Hash Algorithm
- Store Entry Lifetime (seconds)

- e. Click **Save** and deploy the changes.
2. Configure the SMTP Server information in the email One-time Password authentication mechanism.

- a. In the IBM Security Access Manager virtual appliance console, select **Secure Access Control > Authentication**.

- b. Click the **Mechanisms** tab.
- c. Select **Email One-time Password**.
- d. Click the **Modify Authentication Mechanism** icon to modify **Email One-time Password**.

Set the values for the following properties.

SMTP Host Name

Your SMTP hostname.

SMTP Port

Your SMTP port number.

Sender Email

The name of the sender.

Note: Modify the other properties as required by your SMTP Server.

- e. Click **Save** and deploy the changes.
3. Configure the SMS Gateway information in the SMS One-time Password authentication mechanism.

- a. In the IBM Security Access Manager virtual appliance console, select **Secure Access Control > Authentication**.

- b. Click the **Mechanisms** tab.
- c. Select **SMS One-time Password**.
- d. Click the **Modify Authentication Mechanism** icon to modify **SMS One-time Password**.

Set the values for the following properties.

Connection URL

The SMS gateway URL to send message.

HTTP Request Parameters

Specify the parameters required to send a message by your SMS gateway in comma-separated values. For example, `dest_num = $DEST_NO$, msg = MSG, mode = text. $DEST_NO$ and MSG` are IBM Security Access Manager macros to retrieve the mobile number set in mapping rules or authentication policy and the SMS message template.

Note: Modify the other properties as required by your SMS Gateway.

4. Modify the mapping rules to retrieve the email address and mobile number from the IBM Security Access Manager credentials after the IBM Security Privileged Identity Manager external authentication.
 - a. In the IBM Security Access Manager virtual appliance console, select **Secure Access Control > Authentication**.
 - b. Click the **Mapping Rules** tab.
 - c. Select OTPGetMethods and click the **Edit** icon.
 - d. In the Mapping Rules - OTPGetMethods window, modify the content to retrieve the email address and mobile number from the email and mobile header that you have previously set in the IBM Security Privileged Identity Manager external authentication mechanism.

```

---
if (useSMS) {
//var mobileNumber = "+12345678";
var mobileNumber = stsuaAttrs.getAttributeValueByName("ispim_mobile");
---
---
if (useEmail) {
//var emailAddress = "user@localhost";
var emailAddress = stsuaAttrs.getAttributeValueByName("ispim_email");
---

```

- e. Click **Save**.
 - f. Select OTPVerify and click the **Edit** icon.
 - g. On the Mapping Rules - OTPVerify window, remove all lines except the first commented line.
 - h. Click **Save**.
 - i. Deploy the changes.
5. Define an Access Control policy to protect IBM Security Privileged Identity Manager authenticated junctions with email or SMS One-time Password.
 - a. In the IBM Security Access Manager virtual appliance console, select **Secure Access Control > Access Control**.
 - b. Click the **Policies** tab.
 - c. Click the **Create Policy** icon.
 - d. In the Create Policy window, provide the following information.

Name Specify a name to identify the access control policy, For example, MAC Email or SMS OTP.

Rules Specify the rules for when the email or SMS One-time Password authentication is prompted. For example,

```

Precedence: `First`
*Rule 1*:
If `authenticationMechanismTypes` has member `"urn:ibm:security:authentication:asf:mechanism:ispim"`
and `authenticationMechanismTypes` has member `"urn:ibm:security:authentication:asf:mechanism:macotp"`
Then Permit
*Rule 2*:
If `authenticationMechanismTypes` has member `"urn:ibm:security:authentication:asf:mechanism:ispim"`
and not ( `authenticationMechanismTypes` has member `"urn:ibm:security:authentication:asf:mechanism:macotp"` )
Then Permit with Authentication `MAC One-time Password`

```

See the IBM Security Access Manager product documentation for creating advanced rules.

6. Attach the access control policy that is defined in Step 5 to the following IBM Security Privileged Identity Manager authenticated junctions.
 - a. In the IBM Security Access Manager virtual appliance console, select **Secure Access Control > Access Control**.
 - b. Click the **Resources** tab.

- c. Add the following IBM Security Privileged Identity Manager authenticated junctions as resources that are to be protected by the One-time Password.

Table 11. Authenticated junctions for Privileged Credential Manager

Path	Purpose
/itim/console	Admin Console
/itim/self	Self-service UI
/ispim/ui	Service Center

Table 12. Authenticated junctions for IBM Security Access Manager for Enterprise Single Sign-On

Path	Purpose
/admin	AccessAdmin

Table 13. Authenticated junctions for Privileged Session Recorder

Path	Purpose
/recorder/ui	Privileged Session Recorder console

- d. Select the junction. For example, /itim/console.
- e. Click **Attach**.
- f. In the Attach Policies window, select the access control policy that is defined in Step 5 and click **OK**.
- g. After adding all IBM Security Privileged Identity Manager authenticated junctions as resources protected by OTP, click **Publish All**.

Integration with IBM QRadar Security Intelligence Platform

The collection of events from IBM Security Privileged Identity Manager for analysis in IBM QRadar® Security Intelligence Platform is now supported with IBM QRadar Security Intelligence Platform Device Support Modules (DSMs) for IBM Security Privileged Identity Manager.

Download the IBM QRadar Security Intelligence Platform DSMs for IBM Security Privileged Identity Manager.

The following .rpm packages must be downloaded:

- 7.2.0-QRADAR-PROTOCOL-JDBC-7.2-<version>.noarch.rpm

Note: This is **not** applicable if the package is already installed.

DSMs:

- 7.2.0-QRADAR-DSM-IBMSecurityAccessManagerESS0-7.2-<version>.noarch.rpm
- 7.2.0-QRADAR-DSM-IBMSecurityPrivilegedIdentityManager-7.2-<version>.noarch.rpm
- 7.2.0-QRADAR-DSM-IBMPrivilegedSessionRecorder-7.2-<version>.noarch.rpm

Content package:

- 7.2.0-QRADAR-ContentPackage-CustomProperties-IBMSecurityPrivilegedIdentityManager-7.2-<version>.x86_64.rpm

- 7.2.0-QRADAR-ContentPackage-CustomProperties-IBMPrivilegedSessionRecorder-7.2-<version>.x86_64.rpm
- 7.2.0-QRADAR-ContentPackage-CustomProperties-IBMSecurityAccessManagerESS0-7.2-<version>.x86_64.rpm

Configuring the log sources

Configure the log sources for Privileged Credential Management, Privileged Session Recorder, and IBM Security Access Manager for Enterprise Single Sign-On so that IBM QRadar Security Intelligence Platform can process the database.

Procedure

1. Perform the following tasks to configure the log sources for Privileged Credential Management:
 - a. Review the The IBM Security QRadar DSM for IBM Security Privileged Identity Manager.
 - b. Create a database view. See Configuring IBM Security Privileged Identity Manager.
 - c. Configure a log source for IBM Security Privileged Identity Manager. See Adding a log source
2. Perform the following tasks to configure the log sources for Privileged Session Recorder:
 - a. Review the IBM Security QRadar DSM for Privileged Session Recorder.
 - b. Collect data from the IBM Security Privileged Identity Manager Session Recorder.
 - c. Configure a log source for IBM Privileged Session Recorder.
3. Perform the following tasks to configure the log sources for IBM Security Access Manager for Enterprise Single Sign-On:
 - a. Enable **syslog** by using the IBM Security Privileged Identity Manager CLI. See “Enabling syslog on the IBM Security Privileged Identity Manager virtual appliance”
 - b. Configure a log source for IBM Security Access Manager for Enterprise Single Sign-On.

Enabling syslog on the IBM Security Privileged Identity Manager virtual appliance

Enable syslog for the IBM Security Access Manager for Enterprise Single Sign-On server on the IBM Security Privileged Identity Manager virtual appliance.

Procedure

1. Log on to the IBM Security Privileged Identity Manager virtual appliance command line interface.
2. In the command line interface, type `update_syslog`.
3. Enable the syslog attributes. For example,


```
rwrangler.example.com:service_properties> update_syslog
```

```
Enable syslog
logSystemManagementActivity [true/false]: true
logUserAdminActivity [true/false]: true
logUserService [true/false]: true
logUserActivity [true/false]: true
Syslog server port: 514
Syslog server hostname: 10.1.13.127
```

Syslog logging facility:
Syslog field-separator: ###
Syslog settings will be updated.
Restart ISPM to apply the new settings.

where,

Enable syslog

Type true for each of the categories.

Syslog server port

Specify the server port number that is used for forwarding events to QRadar. Specify 514.

Syslog server hostname

Specify the IP address or hostname of your QRadar Console or event collector.

Syslog logging facility

Specify the facility of the events forwarded to QRadar. Default value: 20.

Syslog field-separator

Specify the characters used to separate name-value pair entries in syslog payload.

4. Restart the virtual appliance.

Results

The log source is added to QRadar. Syslog events are automatically discovered. Events forwarded to QRadar are displayed on the **Log Activity** tab.

Integration with IBM Security Guardium

The integration of IBM Security Guardium® with IBM Security Privileged Identity Manager provides an integrated solution to combat insider threats.

This integration introduces a new **database** resource type. See "#Resources type identifier column headers" in the *IBM Security Privileged Identity Manager Administrator Guide*.

To access the database views, you require a database user. For more information, see the following links:

- "Creating a user to access database views"
- "Database views" in the *IBM Security Privileged Identity Manager Reference Guide*

Creating a user to access database views

Create a database user to access the views that are required for the IBM Security Guardium integration

About this task

This database user is a read-only user and is only required for the Guardium integration.

Procedure

1. Create a database user.
 - a. Create an operating system user. For example, pimview
Add the operating system user pimview to the group, DB2USERS.
 - b. Change the password for user pimview.

Note:

- For Windows users, this step is not applicable if you set your password to **Never Expire** in the previous step.
- This step is compulsory for Unix and Linux users.

2. Grant the user permissions to access the views.

Note: Use the user that you created in "Installing and configuring a database server" in the *IBM Security Identity Manager Installation and Configuration Guide* or a database administrator account to grant the permissions.

```
db2 connect to idmdb user piminstu using <password>
GRANT SELECT ON V_PIM_CICO_HISTORY_DB_RSRC TO <username>
GRANT SELECT ON V_PIM_CRED_INFO_DB_RSRC TO <username>
GRANT SELECT ON V_PIM_CRED_DETAILS_DB_RSRC TO <username>
db2 disconnect current
```

Integration with IBM Security Identity Manager

IBM Security Privileged Identity Manager is a separate product offering from IBM Security Identity Manager, but these products can still be integrated when necessary. IBM Security Privileged Identity Manager account and role entitlements are managed and reported on at IBM Security Identity Manager. Shared credential entitlements are managed and reported at IBM Security Privileged Identity Manager.

New with integration

Existing IBM Security Identity Manager customers can deploy IBM Security Privileged Identity Manager without disrupting or changing their IBM Security Identity Manager deployment.

There is no need to upgrade IBM Security Identity Manager to support current IBM Security Privileged Identity Manager features. As such, the cost of migrating configuration, data, processes, and extensions; and the risk of destabilizing user provisioning services are avoided.

The following functions are available only through integration with IBM Security Identity Manager:

- User Account Provisioning and Lifecycle Management

IBM Security Privileged Identity Manager does not provision privileged credentials on target systems. The privileged accounts must already exist on the target system before the credentials are onboarded into the IBM Security Privileged Identity Manager credential vault.

- Service Reconciliation
- Access Request and Re-certification workflows

IBM Security Privileged Identity Manager Access Memberships are reconciled to IBM Security Identity Manager as groups and can be re-certified with IBM Security Identity Manager processes.

IBM Security Privileged Identity Manager contains a simplified user interface for setting up single or multiple-stage approval workflows (by Access Owner, User Manager, ISPIM Admin) for access requests.

Note: Privileged accounts can be provisioned by IBM Security Identity Manager but the privileged accounts must be onboarded separately onto IBM Security Privileged Identity Manager.

IBM Security Privileged Identity Manager shared access entitlements are managed only in IBM Security Privileged Identity Manager by respective privileged admins, and is not visible to IBM Security Identity Manager.

Existing customers:

- Use IBM Security Identity Manager for identity management and governance of all users in the organization, including privileged users. For users who must use IBM Security Privileged Identity Manager, IBM Security Identity Manager is used to provision ISPIM accounts for these users and to manage the access and system role (group) memberships of these accounts.
- Use IBM Security Privileged Identity Manager for managing and tracking the use of shared access credentials, automated password reset, and for recording sessions that use the managed credentials.
- IBM Security Privileged Identity Manager shared access entitlements are managed only in IBM Security Privileged Identity Manager by respective privileged administrators, and is not visible to IBM Security Identity Manager. There is no assumption or requirement that all the shared credentials managed by IBM Security Privileged Identity Manager is visible to IBM Security Identity Manager.

For a scenario, see “Integration with IBM Security Identity Manager scenarios” on page 49.

The IBM Security Privileged Identity Manager Adapter must be deployed on IBM Security Identity Manager.

The adapter is required to manage IBM Security Privileged Identity Manager users, access, groups, and administrative domains.

The IBM Security Privileged Identity Manager Adapter is supported on IBM Security Identity Manager 5.1, 6.0, and 7.0.

IBM Security Privileged Identity Manager Adapter

The IBM Security Privileged Identity Manager Adapter enables communication between the IBM Security Identity Manager and the IBM Security Privileged Identity Manager. The IBM Security Privileged Identity Manager Adapter automates the management of user accounts, ISPIM roles, ISPIM groups (system roles), and ISPIM administrative domains.

The IBM Security Privileged Identity Manager Adapter automates the following tasks:

User account management on the IBM Security Privileged Identity Manager server

- Adding user accounts
- Changing user account passwords

- Modifying user account attributes
- Suspending and restoring user accounts
- Retrieving user accounts for the first time
- Deleting user accounts
- Reconciliation of modified user accounts

Group management on the IBM Security Privileged Identity Manager server

- Adding groups
- Modifying group attributes, including adding and removing members
- Deleting groups
- Adding roles
- Modifying role attributes, including adding and removing members
- Deleting roles
- Adding and deleting administrative domains
- Modifying administrative domain attributes, including adding and removing administrators
- Reconciliation of other support data from the IBM Security Privileged Identity Manager server to IBM Security Identity Manager

For more information, see the IBM Security Privileged Identity Manager Adapter documentation in the IBM Security Identity Manager documentation site.

Feature comparison

Table 14. Comparing features between a standalone IBM Security Privileged Identity Manager and one that is integrated with IBM Security Identity Manager

Feature	Standalone	With IBM Security Identity Manager
Shared credential management with secure storage in a vault with access control with role-based policies	Supported.	With ability to use IBM Security Identity Manager to provision and manage ISPIM accounts and role and group memberships
Self-service check-in and check-out from web console	Supported.	Same as standalone.
Automated check-in and check-out with single sign-on with Privileged Access Agent	Supported.	Same as standalone.
Session recording with Privileged Access Agent	Supported.	Same as standalone.
Application identity management	Supported.	Same as standalone.
Cognos reports	Supported.	Same as standalone.
Account provisioning and lifecycle management of accounts on managed systems	Not supported. Lifecycle of shared credentials are not tied to individual employees.	Same as standalone. Note: You can configure IBM Security Identity Manager to provision shared credentials into target systems if required but the privileged credentials must be separately on-boarded into IBM Security Privileged Identity Manager
Service reconciliation	Full service reconciliation is not supported.	Same as standalone.

Table 14. Comparing features between a standalone IBM Security Privileged Identity Manager and one that is integrated with IBM Security Identity Manager (continued)

Feature	Standalone	With IBM Security Identity Manager
Access recertification	Not supported.	With ability to use IBM Security Identity Manager for managing and certifying users ISPIM account and ISPIM role memberships.
Adapter support	The virtual appliance includes the SoftLayer adapter. Supports adapters that include the self-change password mode.	Same as standalone.
2-factor authentication	Log on with RFID into Privileged Access Agent is supported. Log on with smartcards or fingerprint biometrics into the single sign-on Privileged Access Agent is not supported. Deployments of the IBM Security Privileged Identity Manager with IBM Security Access Manager for Web WebSEAL as a front-end is not supported. Step up-authentication by using OTP before automatic check-out is supported with the customization of single sign-on AccessProfiles.	Same as standalone.

Task comparison

Table 15. User experience differences

Tasks	Standalone	With IBM Security Identity Manager
On-boarding privileged administrators	You can use the IBM Security Privileged Identity Manager administrative console, HR feed, or APIs.	You can use IBM Security Identity Manager to on-board users into IBM Security Privileged Identity Manager.
On-boarding and managing unconnected credentials	You can use the IBM Security Privileged Identity Manager Service Center.	Same as standalone.
On-boarding and managing connected credentials	You can use the IBM Security Privileged Identity Manager Service Center.	Same as standalone.
Managing groups, roles, and memberships for groups and roles	You can use the IBM Security Privileged Identity Manager administrative console.	Users, groups, and roles in IBM Security Privileged Identity Manager can be reconciled and managed on IBM Security Identity Manager.

Table 15. User experience differences (continued)

Tasks	Standalone	With IBM Security Identity Manager
Role request and approval workflows	Simplified user interface for single or multiple-stage approval workflows (by Role Owner, User Manager, ISPIM Admin) for role requests.	Groups and roles in IBM Security Privileged Identity Manager are reconciled and can be managed in IBM Security Identity Manager. You can set up request approval workflows on these roles and groups with IBM Security Identity Manager, where requests are accomplished through the IBM Security Identity Manager Service Center.
Managing shared access policies	You can use the IBM Security Privileged Identity Manager administrative console.	Same as standalone.
Managing credential settings. For example: reset password on check-in	You can use the IBM Security Privileged Identity Manager Service Center.	Same as standalone.
Scheduled password reset	IBM Security Privileged Identity Manager administrator console.	Same as standalone.

Integration with IBM Security Identity Manager scenarios

Privileged Administrators, Privileged Users, and Privileged Identity Manager administrators can be on-boarded from IBM Security Identity Manager into IBM Security Privileged Identity Manager.

The following scenarios demonstrate how Annie Lewis (Privileged Administrator) accomplishes the following goals:

1. Add privileged accounts, for example root on a Linux host named *Pinnacle*, to the credential vault on IBM Security Privileged Identity Manager.
2. Define a policy to authorize who can use the privileged accounts that she creates on IBM Security Privileged Identity Manager.
3. Let users request access on the IBM Security Identity Manager console.
4. Approve such requests on IBM Security Identity Manager console.
5. Allow users to check out on IBM Security Privileged Identity Manager.

The following sections describe additional information for an integration scenario:

- Setting up a request and approval workflow for ISPIM roles on IBM Security Identity Manager
- Tasks that remain the same with or without integration with IBM Security Identity Manager
- Reports

Table 16. Types of users to be on-boarded

User	Description
Annie Lewis (Privileged Administrator)	<ul style="list-style-type: none"> • These employees own or are responsible for one or more privileged IDs on one or more systems. • Use IBM Security Privileged Identity Manager to manage and control the sharing of privileged credentials with co-workers.
James Smith (Privileged User)	These are employees who have a business need to access one or more privileged credentials that are managed by the IBM Security Privileged Identity Manager.
Jake Smith (Privileged Identity Manager Administrator)	This administrator can provision ISPIM accounts for Annie Lewis (Privileged Administrator) and James Smith (Privileged User) through IBM Security Identity Manager by adding Annie Lewis and James Smith into the correct ISPIM group (system role) when they take on the specified business roles.

Annie Lewis (Privileged Administrator) needs an ISPIM account and an ISPIM administrative domain. Annie Lewis (Privileged Administrator) requires the account and administrative domain so that she can add her privileged accounts, for example *root*, to the credential vault so that she can share them with other privileged users. Annie Lewis (Privileged Administrator) contacts Jake Smith (Privileged Identity Manager Administrator) to set up the account and administrative domain that she needs.

Table 17. Create an ISPIM administrative domain and ISPIM account

Persona	Jake Smith (Privileged Identity Manager Administrator)
Console	IBM Security Identity Manager Administrative console
Tasks	<ol style="list-style-type: none"> 1. Create an ISPIM administrative domain for Annie Lewis (Privileged Administrator) where she can manage her shared credentials. For example: <i>Annie domain</i>. See Administrator domains and Creating groups. 2. Create an ISPIM account for Annie Lewis (Privileged Administrator) on the ISPIM service. For example: <i>Annie Lewis</i>. 3. Associate the Annie Lewis (Privileged Administrator) ISPIM account with the <i>Privileged Administrator Group</i> and <i>Annie domain</i>. 4. Create an account request workflow for the ISPIM service. See Adding an entitlement workflow.

After Annie Lewis (Privileged Administrator) gets a domain that she can use to manage her accounts, Annie logs on to the IBM Security Privileged Identity Manager Administrative console to add her credential to the credential vault, create an ISPIM role, and create a shared access policy before James Smith (Privileged User) can check out the credential to install the DB2 database on a server.

Table 18. Create a shared access policy

Persona	Annie Lewis (Privileged Administrator)
----------------	--

Table 18. Create a shared access policy (continued)

Console	IBM Security Privileged Identity Manager Administrative console IBM Security Privileged Identity Manager Service Center
Tasks	<ol style="list-style-type: none"> 1. Add a shared access credential that requires check-out. See Credentials in the credential vault. <ol style="list-style-type: none"> a. Link the credential to the ISPIM administrative domain. In this setup: <i>Annie domain</i>. b. Specify the shared access credential in the User ID field. For example: <i>root</i>. c. Specify the managed resource. For example, set resource name as <i>Pinnacle</i>. d. Specify the check-out duration. For example: <i>1 week</i>. 2. Create an ISPIM role to represent the administrators who can check out the credential. For example: <i>Pinnacle admins</i>. See Creating roles. 3. Create a shared access policy to allow all members of the created ISPIM role to check out the created credential. For example: <i>Pinnacle admin access</i> policy. See Creating shared access policies. <ol style="list-style-type: none"> a. Add the <i>Pinnacle admins</i> role as members of the <i>Pinnacle admin access</i> policy. b. Set Entitlement as credential then specify the shared access credential. In this setup: <i>root</i>. on the Pinnacle system

Table 19. Assign Privileged Administrator as access owner

Persona	Jake Smith (Privileged Identity Manager Administrator)
Console	IBM Security Identity Manager Administrative console
Tasks	<p>Reconcile the ISPIM service to sync Annie Lewis (Privileged Administrator) <i>Pinnacle admins</i> role in IBM Security Identity Manager.</p> <ol style="list-style-type: none"> 1. Specify the group name. In this setup: Organization / <i>Annie domain</i> / <i>Pinnacle admins</i>. 2. Enable Annie's <i>Pinnacle admins</i> in IBM Security Identity Manager as an access and common access. Specify the shared access policy name <i>Pinnacle admin access</i>. 3. Assign Annie Lewis (Privileged Administrator) as the Access Owner.

James Smith (Privileged User) must check-out the administrative account, *root*, on *Pinnacle admin access* to install the IBM DB2 database for the reservation application.

Table 20. Check out the administrative account

Persona	James Smith (Privileged User)
Console	IBM Security Identity Manager, Version 7.0: IBM Security Identity Manager Service Center IBM Security Identity Manager, Version 5.1 and 6.0: IBM Security Identity Manager Self-service console

Table 20. Check out the administrative account (continued)

Tasks	Request access to <i>Pinnacle admin access</i> . An approval request is sent to Annie Lewis (Privileged Administrator). Note: After the request is approved, James Smith (Privileged User) can use IBM Security Access Manager for Enterprise Single Sign-On to check out the administrative account, <i>root</i> , on <i>Pinnacle</i> and install the DB2 database on the <i>Pinnacle server</i> .
--------------	---

Table 21. Grant access to the Pinnacle Server

Persona	Annie Lewis (Privileged Administrator)
Console	IBM Security Identity Manager, Version 7.0: IBM Security Identity Manager Service Center IBM Security Identity Manager, Version 5.1 and 6.0: IBM Security Identity Manager Self-service console
Tasks	Approve the request from James Smith (Privileged User) to access <i>Pinnacle admin access</i> .

Setting up a request and approval workflow for ISPIM roles on IBM Security Identity Manager

Annie Lewis (Privileged Administrator) uses IBM Security Privileged Identity Manager to on-board credentials (with IBM Security Privileged Identity Manager Service Center), create roles, and set up shared access policies (with IBM Security Privileged Identity Manager administrative console).

Annie Lewis (Privileged Administrator) needs to set up a role called Linux Admins and defines that this will use shared credentials under IBM Security Privileged Identity Manager.

To configure a request and approval workflow for ISPIM roles on IBM Security Identity Manager, the following steps occur:

1. On the IBM Security Identity Manager administrative console, Jake Smith (Privileged Identity Manager Administrator) sets up the ISPIM Service and reconciles the Linux Admin role into IBM Security Identity Manager.
2. On the IBM Security Identity Manager administrative console, Jake Smith (Privileged Identity Manager Administrator) enables the Linux Admin role as a common access and makes Annie Lewis (Privileged Administrator), the access owner, as an approver of the request.
See “Manage Access Approval Workflows” and “Manage Groups” in the IBM Security Identity Manager documentation.
3. On the IBM Security Identity Manager administrative console, James Smith (Privileged User) requests access to the Linux Admin role.
4. On the IBM Security Identity Manager administrative console, Annie Lewis (Privileged Administrator) approves the access request from James Smith (Privileged User).

Note: Approval workflows for the Linux Admin role are not associated on IBM Security Privileged Identity Manager. If you do this, access approvals are required from both IBM Security Identity Manager and IBM Security Privileged Identity Manager.

Tasks that remain the same with or without integration with IBM Security Identity Manager

IBM Security Privileged Identity Manager Privileged Administrator or Privileged Administrator tasks:

- On-boarding of credentials into the credential vault
- Management of credential settings
- Management of automatic password resets on credentials
- Setting up shared access roles and policies

Privileged user tasks:

- Manual check-in and check-out with self service console
- Automatic check-in and check-out with session recording through Privileged Access Agent.

Reports

IBM Security Privileged Identity Manager reports contains the shared access entitlements (role-based), and shared access history for privileged users. IBM Security Identity Manager reports contain a user's "individual" account entitlements (no shared access entitlements), including IBM Security Privileged Identity Manager account and role and group memberships.

Integration with SoftLayer

Privileged administrators can use IBM Security Privileged Identity Manager to manage privileged credentials that are used to log on to IBM SoftLayer.

SoftLayer AccessProfile

The SoftLayer AccessProfile provides single sign-on functionality to log on to SoftLayer.

The SoftLayer AccessProfile supports the following functions:

- Check out the credentials from IBM Security Privileged Identity Manager.
- Inject the credentials after the web browser is closed.
- Check in the credentials to IBM Security Privileged Identity Manager.

You must consider the following issues and limitations before using the SoftLayer AccessProfile:

- It can only be used in IBM Security Access Manager for Enterprise Single Sign-On supported web browsers. For example: Microsoft Internet Explorer 9, Microsoft Internet Explorer 10, or Mozilla Firefox 31.
- The profile is not checked in if a tab is closed. Close the web browser to check in the profile.
- The user is not prompted to check out the credential after restarting the web browser due to the cache that is maintained by the web browser. The user is logged on to SoftLayer automatically.

SoftLayer Adapter

The SoftLayer Adapter enables connectivity between the IBM Security Privileged Identity Manager and SoftLayer.

This adapter automates several administrative tasks on the SoftLayer server. You can use the adapter to automate the following tasks:

- Create, modify, suspend, restore, change password, and delete a user.
- Reconcile user and user attributes.

The SoftLayer Adapter is bundled with the IBM Security Privileged Identity Manager virtual appliance. As such, you only need to:

1. Create an identity provider for the SoftLayer profile (**SoftLayerProfile**) . See Adding identity providers.
 - a. Specify a name that defines the adapter service on the server. For example, SoftLayer.

Note: Do not use forward (/) or backward slashes (\) in the service name.

- b. Specify the URL which the adapter can use to communicate with SoftLayer. For the current SoftLayer release, use <https://api.softlayer.com>.
2. Create a credential and connect it to the SoftLayer identity provider that you created. See Adding credentials with Service Center and Connecting a credential to an identity provider.

Note: In the **Resource** field, specify `control.softlayer.com`.

3. Define access to credentials and grant privileged users membership to access. See Creating access.
4. (Optional) If the credential check-in fails because the default SoftLayer password policy is not strong enough, modify the password strength rule in **Manage Password Policies**.

Integration with IBM Security Identity Governance and Intelligence

An Identity Governance administrator can use IBM Security Privileged Identity Manager to manage shared access to privileged credentials.

The recertification of privileged user's access entitlements is performed in IBM Security Identity Governance and Intelligence. See IBM Security Identity Governance and Intelligence product documentation.

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. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

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 <http://www.ibm.com/legal/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.

This Software Offering 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, usage tracking, or functional purposes. These technologies can be disabled, but disabling them will also eliminate the functionality they enable.

This Software Offering does not use cookies 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".



Printed in USA