IBM® Security Privileged Identity Manager
Version 1.0.1

Deployment Overview Guide

SC27-4382-02

IBM® Security Privileged Identity Manager
Version 1.0.1

Deployment Overview Guide

SC27-4382-02

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

Edition notice

Note: This edition applies to version 1.0.1 of *IBM Security Privileged Identity Manager* **(product number 5725-H30) and to all subsequent releases and modifications until otherwise indicated in new editions.**

Contents

Figures

Tables

About this publication

IBM Security Privileged Identity Manager Deployment Overview Guide describes the process of setting up and logging on to managed resources with privileged identities.

Access to publications and terminology

This section provides:

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

IBM® Security Privileged Identity Manager library

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

- *IBM Security Privileged Identity Manager Deployment Overview Guide*, SC27-4382-02
- *IBM Security Privileged Identity Manager Administrator Guide*, SC27-5619-01
- *IBM Security Privileged Identity Manager Virtual Appliance Deployment Guide*, SC27-5625-00

Online publications

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

IBM Security Privileged Identity Manager library
The product documentation site (http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.ispim.doc_1.0.1/kc-homepage.html) displays the welcome page and navigation for the library.

IBM Security Identity Manager library
The product documentation site (http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.isim.doc_6.0.0.2/kc-homepage.htm) displays the welcome page and navigation for the IBM Security Identity Manager product.

IBM Security Access Manager for Enterprise Single Sign-On library
The product documentation site (http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itamesso.doc_8.2.1/kc-homepage.html) displays the welcome page and navigation for the IBM Security Access Manager for Enterprise Single Sign-On product.

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

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

IBM Terminology website

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

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

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

Technical training

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

Support information

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

The *IBM Security Identity Manager Troubleshooting Guide* and *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting Guide* provides details about:

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

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

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

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES

NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Chapter 1. Privileged identity management

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

Overview of IBM Security Privileged Identity Manager

IBM Security Privileged Identity Manager is a software solution that is based on IBM Security Identity Manager and IBM Security Access Manager for Enterprise Single Sign-On.

The solution provides the following features:

- Centralized administration, secure access, and storage of privileged shared account credentials
- Role-based access control for shared accounts
- Lifecycle management of shared accounts ownership
- Single sign-on through automated check-out and check-in of shared credentials
- Auditing of shared credentials access activities
- Session recording and replay
- Integration with the broader Identity and Access Management Governance portfolio

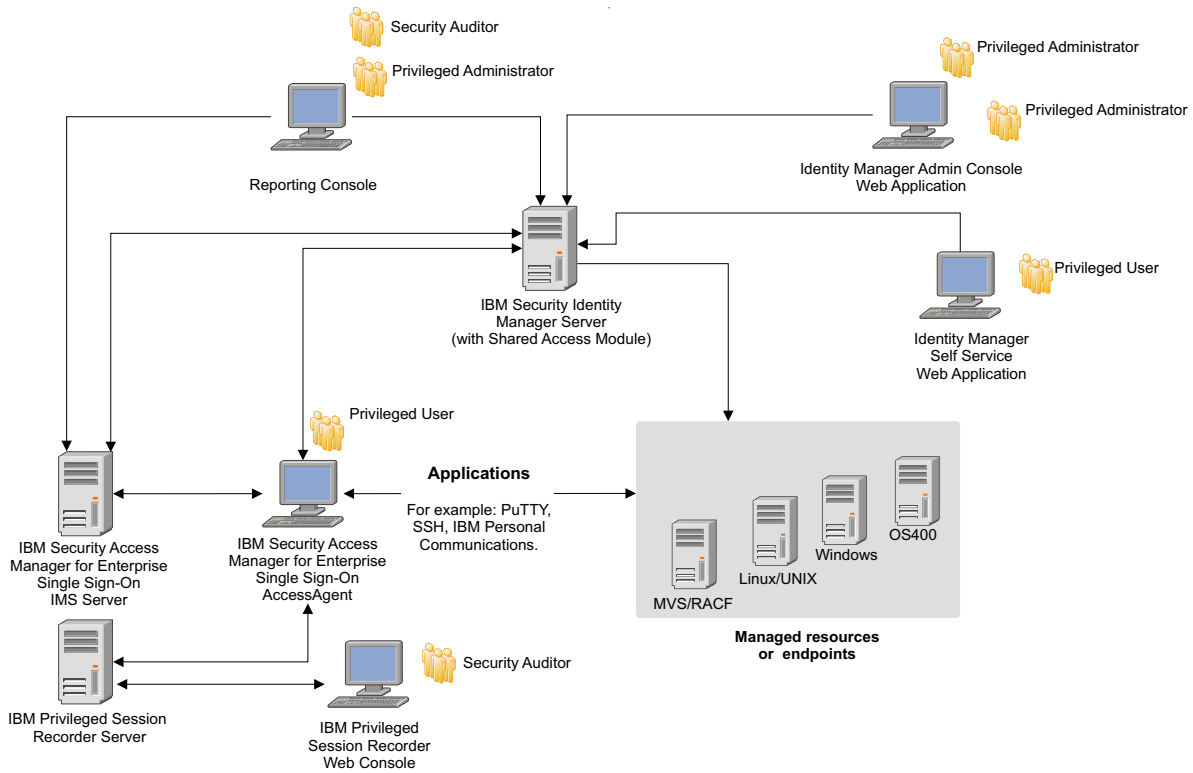

Figure 1. IBM Security Privileged Identity Manager users and components

Privileged identity refers to the pre-built accounts in nearly every operating system and application. Privileged accounts are general user identities distinguished by the assignment of security, administrative, or system authorities.

Privileged identities are typically distinguished by the names they use. For example, `administrator`, `sa`, `root`, `db2admin`.

Unlike a personal identity like `jdoe`, you can access privileged accounts only with a privileged password, and account access is hard to disable. In an enterprise environment, multiple Administrators might share access to a single user 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.

To better manage privileged identities, a user receives an individual identity to a system:

- If they need it.
- When they need it.
- On the condition that they need it.
- If they have access to it.

With a *reusable or shared access user ID*, you can log on to a system without any knowledge of the password for the privileged identity. Instead, a user can check out or lease a *reusable ID* from a shared access repository for a limited time.

How the solution works

You reestablish accountability and traceability when you can map check-out and check-in actions of shared privileged accounts to.

For example:

1. An organization defines privileged roles, for example *SystemAdmin_Staff* or *Operations_Database_Admin* in IBM Security Identity Manager. These roles are tied to appropriate system and account entitlements.

   You can also tie the roles to pools of accounts. For example, if multiple users might use a privilege simultaneously, you might tie a pool of 15 database administrator accounts to the *Operations_Database_Admin*.
2. When a user, for example *jdoe*, accesses a system where a privileged ID is required, the IBM Security Access Manager for Enterprise Single Sign-On client automatically checks out the required account.
3. The IBM Security Access Manager for Enterprise Single Sign-On client then automatically injects the credentials into the users session.

   You can configure the credential check-out automation to work for desktop applications, terminal applications, and mainframe applications.
4. After the user finishes the tasks that require the privileged account, the automatic check-in process returns the privileged user ID to the credential vault.

Primary user types

Each privileged identity management user type has a different role and objective to achieve with the solution.

Table 1. Privileged identity management users and tasks

User type	Tasks
Privileged Administrator	• Uses the IBM Security Identity Manager console to – Manage shared accounts, credentials, and credential pools. – Configure roles and policies for shared account and shared access. • Uses the IBM Tivoli® Common Reporting console to access shared access reports.
Privileged User	• Uses the IBM Security Identity Manager self-service user interface to manually check out and check in shared credentials. • Uses the IBM Security Access Manager for Enterprise Single Sign-On AccessAgent to access systems and applications with shared credentials.
Security Administrator	• Searches and reviews activities of privileged users. • Demonstrates compliance to regulations related to privileged users.
Security Auditor	• Verifies compliance to audit requirements by reviewing logs an auditor can understand instead of struggling with obscure system events.

Component software

IBM Security Privileged Identity Manager has several components.

IBM Security Identity Manager shared access module

IBM Security Identity Manager includes shared access management, which extends its core features. This module is the centerpiece of the IBM Security Privileged Identity Manager solution. The core features include user account provisioning and identity and access governance framework. Installing this module is optional during the IBM Security Identity Manager installation.

Highlights:

- Account provisioning framework provides centralized account and password management for privileged users.
- Shared access uses secure check-in, check-out, and logging of account credentials from a credential vault server.
- Administrative control of shared credential access ensures individual accountability.
- Java™ APIs and Web Services APIs make it possible for application clients to programmatically access shared credentials.
- There is role-based access control for shared credential access and shared account ownership.
- There is lifecycle management of privileged identities. These tasks include management of access requests; approval and revalidation of account ownership, role-based access requests; and shared credential access.
- There is end-to-end auditing for administration and shared credential access activities.
- There are web applications for shared credential administration and manual check-out and check-in.

IBM Privileged Session Recorder

Privileged Session Recorder is a virtual surveillance camera that captures user activity during an active session on a workstation. A session recording provides a complete, irrefutable record of what a user did.

Highlights:

- A Privileged Session Recorder agent is installed only on user workstations, without touching critical servers.
- When a privileged identity check-out occurs, the start of a recording is triggered. A Privileged Session Recorder AccessProfile widget triggers the start and stop of a recording.

For more information about session recording, see the *IBM Security Privileged Identity Manager Administrator Guide*.

IBM Security Access Manager for Enterprise Single Sign-On

IBM Security Access Manager for Enterprise Single Sign-On provides automated check-out and check-in of shared access credentials from the IBM Security Identity Manager Server.

AccessAgent connects to the Integrated Management System (IMS) Server. It provides the privileged identity management logon automation on clients from AccessProfiles on the IMS Server.

Administrators use AccessStudio to create and maintain AccessProfiles. An AccessProfile contains a definition of the logon and change password screen characteristics of an application. It also contains the workflow instructions on how to automate application logons.

Architecture overview

The privileged identity management solution consists of AccessProfiles on a client computer with AccessAgent. The AccessAgent communicates through web services with the IBM Security Identity Manager Server.

The IBM Privileged Session Recorder Client on the workstation is triggered with the Privileged Session Recorder widgets. The recordings are uploaded to the IBM Privileged Session Recorder Server.

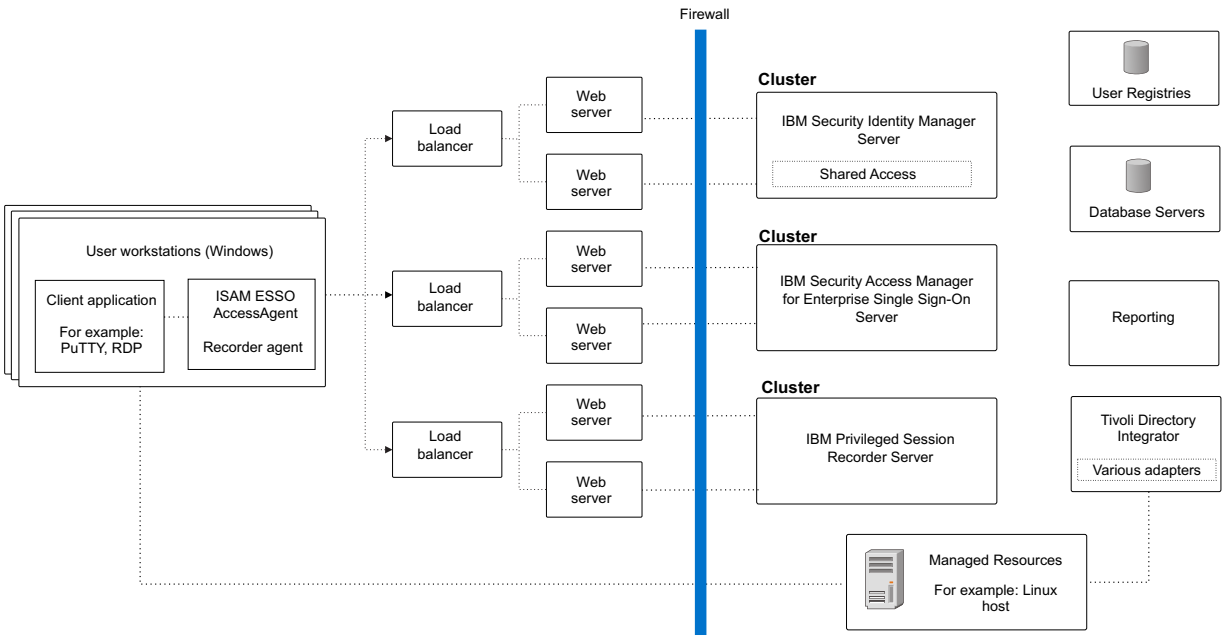

Figure 2. Deployment architecture with session recording components

The main components of the solution are:

- IBM Security Identity Manager Server
- IBM Security Access Manager for Enterprise Single Sign-On Adapter
- IBM Security Access Manager for Enterprise Single Sign-On IMS Server
- IBM Security Access Manager for Enterprise Single Sign-On AccessAgent client
- IBM Privileged Session Recorder Server

Chapter 2. Planning for installation

Installing and configuring IBM Security Privileged Identity Manager involves several steps. Review the prerequisites and roadmap before you begin the installation process.

What you must prepare

Follow this process to prepare for the IBM Security Privileged Identity Manager solution.

1. Review the hardware and software requirements.
2. Install and configure IBM Security Identity Manager, Version 6.0, if you did not yet do so. For installation instructions, see the IBM Security Identity Manager product documentation.

   Note: Install the Shared Access module.
3. Install and configure IBM Security Access Manager for Enterprise Single Sign-On, Version 8.2.1, if you have not done so.
   - Install IMS Server.
   - Install AccessAgent on Windows client computers that require automated check-out and check-in of credentials.
   - Install AccessStudio.

   For installation instructions, see the IBM Security Access Manager for Enterprise Single Sign-On product documentation.
4. Install and configure IBM Security Access Manager for Enterprise Single Sign-On adapter for IBM Security Identity Manager if you did not yet do so.

   See the *IBM Security Access Manager for Enterprise Single Sign-On Adapter Installation and Configuration Guide* in the IBM Security Identity Manager product documentation.
5. Install and configure IBM Privileged Session Recorder Server, Version 1.0.1. See "IBM Privileged Session Recorder, Version 1.0.1 installation" on page 54.

Hardware and software requirements

Check the hardware and software requirements before you install the IBM Security Privileged Identity Manager solution.

Prerequisite software requirements

The IBM Security Privileged Identity Manager solution supports the following software:

Table 2. Prerequisite software and versions.

Required software and components	Version
IBM Security Identity Manager • Shared Access module • IBM Security Access Manager for Enterprise Single Sign-On Adapter	6.0

Table 2. Prerequisite software and versions. (continued)

Required software and components	Version
IBM Security Access Manager for Enterprise Single Sign-On • IMS Server • AccessAgent • AccessStudio	8.2.1

To view the latest hardware and software requirements,

- For IBM Security Identity Manager, see http://www.ibm.com/support/docview.wss?uid=swg27020534.
- For IBM Security Access Manager for Enterprise Single Sign-On, see http://www.ibm.com/support/docview.wss?uid=swg27036350.

Requirements for the IBM Privileged Session Recorder Server

Hardware requirements depend on usage. For the hardware requirements of software that is not listed in this section, see the documentation that is provided with that product.

Note: The IBM Privileged Session Recorder Server runs on WebSphere® Application Server on Windows server operating systems only.

Hardware requirements

Table 3. Hardware requirements for the IBM Privileged Session Recorder Server.

Software	Hardware
IBM DB2®	Search for `installation requirements` in the following documentation: • IBM DB2, Version 10.1 product documentation • IBM DB2, Version 9.7 product documentation
IBM WebSphere Application Server	• 2x2 GHz processor • 80 GB disk space • 4 GB physical memory **Note:** Database not co-located.
IBM HTTP Server	• 1 GB physical memory • 1 GB disk space

Note: The amount of disk space you require for the database server might vary depending on your session activity and usage requirements.

Establish a plan to monitor and manage the growth of the database on a regular basis when session recordings are taken. For more information about database monitoring and storage maintenance, see the database documentation:

- IBM DB2, Version 10.1 product documentation
- IBM DB2, Version 9.7 product documentation

Supported operating systems

- Microsoft Windows Server 2008 R2 Enterprise Edition Service Pack 1 (x64)

Supported virtualization software

VMware ESXi version 5.1

Supported software

Install and configure the following software to before you install and run the IBM Privileged Session Recorder Server installer.

Note: Sample instructions and guidelines on installing the supported software are provided. For the detailed and up-to-date procedures, see the relevant product documentation.

Table 4. Middleware for the IBM Privileged Session Recorder Server.

Middleware	Supported software	Supported version
Application server and Web server	IBM WebSphere Application Server (Base and Network Deployment Edition) and IBM HTTP Server IBM WebSphere Application Server 7.0 Web 2.0 and Mobile Feature Pack	• 8.5 on Windows (x64) with fix pack 2 • 7.0 on Windows (x64) with fix pack 29 or later.
Database server	IBM DB2 Enterprise Server Edition	• 10.1 (x64) with fix pack 2 or later • 9.7 (x64) with the latest fix pack
Reporting tool	IBM Tivoli Common Reporting	• 2.1.1

Required fix packs

Download the latest fix packs for the following products:

- For IBM DB2, go to www.ibm.com/support/docview.wss?uid=swg27007053
- For IBM WebSphere Application Server v8.5, go to http://www.ibm.com/support/docview.wss?uid=swg27036319
- For IBM WebSphere Application Server v7.0 and related subcomponents, go to www.ibm.com/support/docview.wss?uid=swg27014463
  - IBM WebSphere Application Server v7.0
  - IBM HTTP Server v7.0
  - IBM HTTP Server v7.0 plug-in for WebSphere

  Download the latest version of the IBM Update Installer v7.0.

Required feature pack

For WebSphere Application Server Version 7.0: Download the IBM WebSphere Application Server Web 2.0 and Mobile Feature Pack from Passport Advantage®.

Requirements for the IBM Privileged Session Recorder console

The following web browsers are supported for the IBM Privileged Session Recorder console.

Supported web browsers

Table 5. Supported versions of web browsers.

Web browsers	Supported version
Microsoft Windows Internet Explorer	• 10 • 9
Mozilla Firefox Extended Support Release	• 17 • 10

Requirements for the IBM Security Privileged Identity Manager AccessProfiles

The bundled IBM Security Privileged Identity Manager AccessProfiles support the following applications.

PuTTY

32-bit PuTTY, Version 0.58, on the following operating systems:

- 32-bit Windows XP
- 32-bit and 64-bit Windows 7

Remote Desktop Connection client (English version only)

- 64-bit Remote Desktop Connection client on 64-bit Windows 7.
- 32-bit Remote Desktop Connection client on the following operating systems:
  - 32-bit Windows XP
  - 32-bit Windows 7

IBM Personal Communications client (English version only)

32-bit IBM Personal Communications client, Version 5.9, on the following operating systems:

- 32-bit Windows XP
- 32-bit and 64-bit Windows 7

VMware vSphere client (English version only)

32-bit VMware vSphere client, Version 5.0, on the following operating systems:

- 32-bit Windows XP
- 32-bit and 64-bit Windows 7

Important: If your IMS Server deployment uses customized AccessProfiles for any of the provided logon applications, consider taking steps to ensure that earlier versions are not overwritten by the bundled AccessProfiles. For example, back up the AccessProfiles. You cannot single sign-on to the same client application with multiple AccessProfiles that have the same signature.

Requirements for Citrix gateway deployment mode

The following software are supported for deploying IBM Security Privileged Identity Manager agent on a Citrix server:

- Microsoft Windows Server 2008 R2 SP2 (64-bit)
- Citrix XenApp Version 6.5

AccessProfile language support

Privileged identity management automation with AccessProfiles is supported only on the English language versions of the PuTTY Client, Microsoft Remote Desktop Connection Client, IBM Personal Communications, and the VMware vSphere Client.

Note: You access managed resources from Windows client computers.

Client deployment modes

The IBM Security Privileged Identity Manager uses the IBM Security Access Manager for Enterprise Single Sign-On AccessAgent as its client-side component. You can deploy the client either on user workstations or on a Citrix server acting as a gateway.

Client on user workstations

In this mode, IBM Security Privileged Identity Manager Client 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 IBM Security Privileged Identity Manager Client is installed must be configured as personal workstation 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, IBM Security Privileged Identity Manager Client can be deployed on a Citrix XenApp server that is acting 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 IBM Security Privileged Identity Manager Client 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. For more information, see the section *AccessAgent on Citrix and Terminal Server Guide* in the IBM Security Access Manager for Enterprise Single Sign-On product documentation.

Related information:

IBM Security Access Manager for Enterprise Single Sign-On product documentation
Learn more about the Virtual Channel Connector configuration and Lightweight mode in the IBM Security Access Manager for Enterprise Single Sign-On product documentation.

Managed resources support

The IBM Security Privileged Identity Manager supports automated check-out and check-in for managed resources.

Managed resources can run on the following architectures or operating systems:

- Linux/UNIX
- Windows
- Mainframes

Note: The AccessAgent client component provides automated check-in and check-out from Windows client computers.

Planning for high availability

High availability ensures that services are always available.

If you require a high availability deployment, allocate more resources for recovery processes, software, and hardware.

The following table lists the high availability solutions for each tier:

Table 6. High availability solutions for each tier

Tier	Solutions
Application tier	IBM WebSphere Application Server clustering
Data tier	• Active-passive configuration that is managed by high availability cluster-management software such as Tivoli System Automation for Multiplatforms • IBM DB2 clustering • DB2 high-availability data recovery (HADR)

For prerequisite software planning considerations, see the high availability considerations for the following products:

IBM Security Identity Manager, Version 6.0
See the IBM Security Identity Manager product documentation.

IBM Security Access Manager for Enterprise Single Sign-On, Version 8.2.1
See the IBM Security Access Manager for Enterprise Single Sign-On product documentation.

Roadmap for configuring shared access for a managed resource

This roadmap provides high-level steps for configuring shared access for a new managed resource in IBM Security Identity Manager.

Flowchart for configuring shared access for a managed resource

Configure shared access for a managed resource for one of the following reasons:

- Setting up the privileged identity management solution for the first time.
- Adding a service type or application.
- Adding a managed resource.

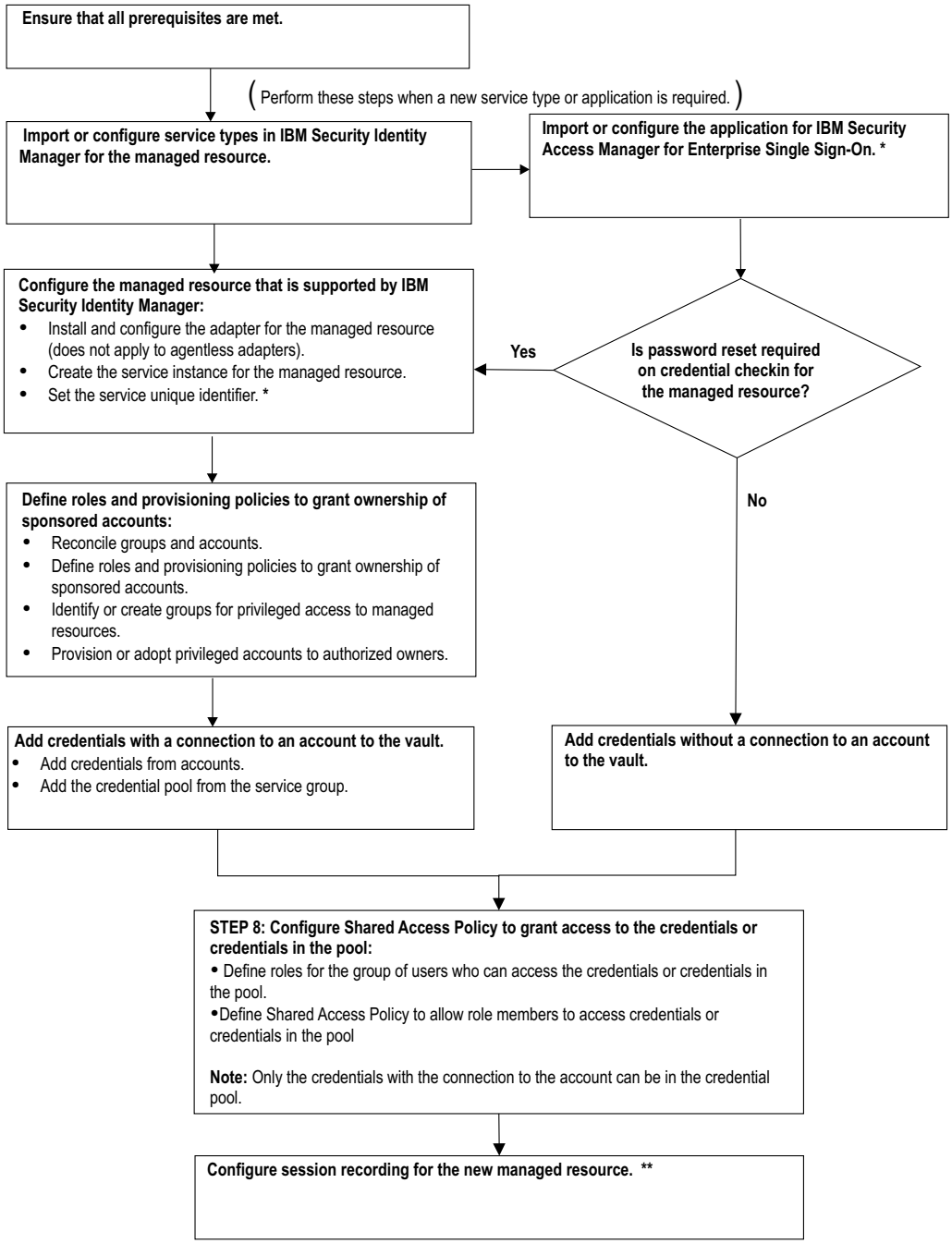

Figure 3. Flowchart for configuring shared access for a managed resource

Step 1: Ensure that all prerequisites are met

Verify the prerequisites for IBM Security Privileged Identity Manager.

Table 7. Ensuring that all prerequisites are met

Requirement	See
Install the Shared Access Module on the IBM Security Identity Manager Server.	"IBM Security Identity Manager, Version 6.0 installation" on page 53
Note: You can skip this step if you do not want to deploy automated single sign-on. Install the AccessAgent client on computers that require automated check-in and check-out.	"IBM Security Access Manager for Enterprise Single Sign-On, Version 8.2.1 installation" on page 53
Note: You can skip this step if you do not want to deploy session recording. Install the Privileged Session Recorder Server. If you have not done so, install the AccessAgent client on computers that you want to monitor. The AccessAgent client includes the Privileged Session Recorder agent.	"IBM Privileged Session Recorder, Version 1.0.1 installation" on page 54

Step 2: Import or configure service types in IBM Security Identity Manager for the managed resource

For each resource type, configure the profile information in IBM Security Identity Manager either by importing the service type or by creating the service type for a manual service.

See "Importing service types" and "Creating service types" in the *Configuration Guide* in the IBM Security Identity Manager product documentation.

Step 3: Import or configure the client application for IBM Security Access Manager for Enterprise Single Sign-On

Identify the client application that is used to access the managed resource. Complete the installation and configuration of the client application on client computers according to the vendor provided instructions. For the list of supported client applications, see "Hardware and software requirements" on page 7.

Remember: If the AccessProfiles are not yet uploaded for IBM Security Privileged Identity Manager, see "Uploading AccessProfiles to the IMS Server" on page 69.

Note: You can skip this step if you do not want to deploy automated single sign-on or session recording.

Is password reset required on credential checkin for managed resource

You can add a credential with or without a connection to an account. If the credential is connected to an account, you can optionally configure the credential

so that the password can be changed when you check in the credential. The password for both credential and account will be changed if this option is enabled.

Table 8. Determining if Password Reset is required on credential checkin for a managed resource

Is Password Reset required on credential checkin for managed resource?	**Action to take**
Yes	You must add the credential with a connection to an account.
No	You can add the credential without a connection to an account.

Configure the new managed resource in IBM Security Identity Manager

You must follow these steps every time there is a new managed resource on your system.

Table 9. Configuring managed resources that are supported by the IBM Security Identity Manager adapter

Steps	**See the following topics in the IBM Security Identity Manager documentation**
Note: This step does not apply to agentless adapters. Install and configure the IBM Security Identity Manager adapter for the managed resource.	IBM Security Identity Manager Adapters product documentation
Create the IBM Security Identity Manager service instance for the managed resource.	"Creating services" in the *Administration Guide*.
Note: You can skip this step if you do not want to deploy automated single sign-on. Set the service unique identifier in the managed resource service definition in IBM Security Identity Manager. Use the administrative console to set the unique identifier for connecting to the managed resource on the AccessAgent. For example, the unique identifier might be an IP address or host name of the server.	"Setting the service unique identifier" in the *Administration Guide*.

Define roles and provisioning policies to grant ownership of sponsored accounts

Perform these tasks in IBM Security Identity Manager.

Table 10. Defining roles and provisioning policies to grant ownership of sponsored accounts

Steps	**See the following topics in the IBM Security Identity Manager documentation**
Reconcile groups and accounts.	"Managing reconciliation schedules" in the *Administration Guide*.

Table 10. Defining roles and provisioning policies to grant ownership of sponsored accounts (continued)

Steps	See the following topics in the IBM Security Identity Manager documentation
Define roles and provisioning policies to grant ownership of sponsored accounts.	"Creating a provisioning policy" in the *Administration Guide*. "Creating roles" in the *Administration Guide*. "Specifying owners of a role" in the *Administration Guide*.
Identify or create groups for privileged access to managed resources.	"Creating groups" in the *Administration Guide*. "Defining access on a group" in the *Administration Guide*.
Provision or adopt privileged accounts to authorized owners. The account that is used for shared access must be a sponsored account. The ownership type for the account can be anything other than `Individual`.	If an account does not exist on the service, see "Requesting accounts on a service" in the *Administration Guide*. If an account exists on the service, see "Assigning an account to a user" in the *Administration Guide*. For general information about sponsored accounts, see "Managing accounts" in the *Administration Guide*.

Add credentials with a connection to an account to the vault

If you want the password on the credential and on the managed resource to be changed when you check in the credential, you must add the credential from the account. To add credentials with a connection to an account, you must either add the credential from an account or create a credential pool from the service group.

Table 11. Adding credentials with a connection to an account to the vault

Step	See the following topics in the IBM Security Identity Manager documentation
Add credentials from accounts	"Adding credentials that are connected to an account through Manage Credential Vault" in the *Administration Guide*.
Add the credential pool from the service group	"Creating credential pools" in the *Administration Guide*

Add credentials without a connection to an account to the vault

If you do not want the password on the credential and on the managed resource to be changed when you check in the credential, you can add the credential without a connection to an account.

Table 12. Adding credentials without a connection to an account to the vault

Steps	See the following topics in the IBM Security Identity Manager documentation
Add credentials that are not connected to accounts	"Adding credentials that are not connected to an account through Manage Credential Vault" in the *Administration Guide*.

Configure a shared access policy to grant access to the credentials or credentials in the pool

After you add the credentials or credential pool, you must configure the shared access policy to allow users to check out or check in the credentials or credential pools.

Note: Only credentials with a connection to an account can be in the credential pool.

Table 13. Configuring a shared access policy to grant access to the credentials

Steps	See the following topics in the IBM Security Identity Manager documentation
Define roles for the group of users who can access the credentials or credentials in the pool.	"Creating roles"
Define a shared access policy to allow role members to access credentials or credentials in the pool.	"Creating shared access policies"

Configure session recording for the new managed resource

Perform these tasks in IBM Security Access Manager for Enterprise Single Sign-On.

Note: You can skip this step if you do not want to deploy session recording for the new managed resource.

Table 14. Configuring session recording for the new managed resource

Task	See the following topics in the IBM Security Privileged Identity Manager documentation
Identify the client application that is used to access the managed resource. Complete the installation and configuration of the client application on client computers according to the instructions provided by the vendor.	For the list of supported client applications, see "Hardware and software requirements" on page 7.
If necessary, modify the AccessProfiles for custom client applications to enable session recording support.	See "Modifying AccessProfiles" in the *IBM Security Privileged Identity Manager Administrator Guide*.

For an overview of shared access, see the IBM Security Identity Manager product documentation and search for `shared access`.

Related information:

For more information about the Privileged Identity Manager deployment, see the IBM Security Identity Manager wiki.

Chapter 3. Installation prerequisites for the Privileged Session Recorder Server

Before you install the Privileged Session Recorder Server, prerequisite components must be installed and configured.

The Privileged Session Recorder Server requires the following components:

- IBM Security Identity Manager
- IBM Security Access Manager for Enterprise Single Sign-On
- IBM Security Access Manager for Enterprise Single Sign-On Adapter
- IBM DB2 database
- IBM WebSphere Application Server

Checklist: Installation prerequisites for the Privileged Session Recorder Server

Table 15. Checklist: Preparing to to install the Privileged Session Recorder Server

Task	For more information
Review the server requirements.	"Hardware and software requirements" on page 7
Build and test the hardware infrastructure.	See the hardware documentation.
Obtain the IBM Security Privileged Identity Manager software and any applicable fixes.	
On each computer, verify name resolution and open TCP port 443 for IBM Security Privileged Identity Manager across any firewalls.	
• Install and configure the database server. • Apply the latest fix packs.	"Database installation and configuration" on page 20
• Install and configure the WebSphere Application Server. • Apply the latest fix packs.	• "Preparing the WebSphere Software, Version 8.5" on page 21 • "Preparing the WebSphere Software, Version 7.0" on page 26
For WebSphere Application Server Version 7.0: Install the WebSphere Application Server Web 2.0 and Mobile feature pack. **Note:** Download the feature pack version for WebSphere Application Server, Version 7.0.	"Installing the IBM WebSphere Application Server Web 2.0 and Mobile feature pack" on page 29 For more information about the feature pack, go to the WebSphere Application Server Web 2.0 and Mobile Feature Pack website.
• Install the IBM HTTP Server. • Apply the latest fix packs.	• "Installing the IBM HTTP Server, Version 8.5" on page 24 • "Installing the IBM HTTP Server, Version 7.0" on page 29

Table 15. Checklist: Preparing to to install the Privileged Session Recorder Server (continued)

Task	For more information
Configure the WebSphere Application Server for one of the following configurations: • Stand-alone server • Clustered environment If your deployment requires specific key size security certificates, see the stand-alone server or clustered server prerequisite tasks.	• "Stand-alone server prerequisite tasks" on page 32 Optional: "Increasing the root CA key size for WebSphere Application Server 7.0 (stand-alone)" on page 93 • "Clustered server environment prerequisite tasks" on page 40 Optional:"Re-creating the root CA for WebSphere Application Server 7.0 on the deployment manager before creating member nodes" on page 97

Database installation and configuration

You must prepare a database server to store uploaded session recordings.

You can install a new database server or use an existing database server.

Tip: Record the following values:

- Database host name
- Port number
- Database Administrator user account

Installing IBM DB2

Install IBM DB2, if necessary, before you run the Privileged Session Recorder Server installation program.

Before you begin

- Ensure that your system meets the installation, memory, and disk requirements.
- Ensure that you have Administrator privileges.

About this task

Use the DB2 installation media that is provided with IBM Security Privileged Identity Manager to ensure that you are using the correct version.

Procedure

1. Obtain a DB2 database system installation package from IBM.
2. Install the DB2 database server as described in the DB2 database server documentation:
   - IBM DB2, Version 10.1 documentation: http://pic.dhe.ibm.com/infocenter/db2luw/v10r1/index.jsp
   - IBM DB2, Version 9.7 documentation: http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/index.jsp
3. Apply the latest fix packs. To download the latest fix packs, go to www.ibm.com/support/docview.wss?uid=swg27007053.

What to do next

Create a database in DB2.

Creating the database with IBM DB2

For IBM DB2, you must create the database for IBM Privileged Session Recorder Server.

Procedure

1. Launch the DB2 command line processor.
2. In the DB2 command line processor, enter the following line:

   ```
   CREATE DATABASE <DB name> AUTOMATIC STORAGE YES ON <Drive letter> DBPATH
   ON <Drive letter> USING CODESET UTF-8 TERRITORY US COLLATE USING SYSTEM
   PAGESIZE 8192
   ```

   where the following parameters are defined:

   Default buffer pool and table space page size
   You must specify the buffer pool and page size as 8192, the equivalent of 8K.

   Code set
   Specify the **UTF-8** code set.

   Territory
   Specify `US` as the territory.

   For example:

   ```
   CREATE DATABASE recdb AUTOMATIC STORAGE YES ON 'C:\' DBPATH ON 'C:\'
   USING CODESET UTF-8 TERRITORY US COLLATE USING SYSTEM PAGESIZE 8192
   ```

Results

You created a database for IBM Privileged Session Recorder Server.

What to do next

You can install and configure WebSphere Application Server.

- Version 8.5: “Installing WebSphere Application Server, Version 8.5” on page 23.
- Version 7.0: “Installing WebSphere Application Server, Version 7.0” on page 26.

WebSphere software installation

You must install and configure the WebSphere software before you install the IBM Privileged Session Recorder Server.

Note: The installation steps for WebSphere software Version 7.0 and 8.5 vary. It is important to identify the version of the application server that you want to install.

Preparing the WebSphere Software, Version 8.5

Prepare the WebSphere Software, Version 8.5 with the required fix packs for all the required components.

Installing the IBM Installation Manager

Use IBM Installation Manager to obtain the necessary product files for the WebSphere Application Server Version 8.5 installation.

Before you begin

- Ensure that your system meets the requirements. See IBM Installation Manager Version 1.6 product documentation.
- Review the prerequisites before installing the Installation Manager.

For the detailed instructions, see the WebSphere Application Server Version 8.5 product documentation and search for `installing Installation Manager and preparing to install the product`.

About this task

IBM Installation Manager is a tool that you can use to install and maintain your software packages.

The Installation Manager simplifies the installation and maintenance of the following WebSphere Application Server components:

- WebSphere Application Server fix packs
- IBM HTTP Server
- IBM HTTP Server plug-in for WebSphere

For more information on using Installation Manager, read the IBM Installation Manager Version 1.6 product documentation.

Procedure

1. Take one of the following options:
   - Access the IBM WebSphere Application Server Network Deployment, Version 8.5 media for your operating system.
   - Extract the files from the archive file that you downloaded from Passport Advantage.

     Note: The archive file name can be different. The archive file name depends on the distribution you download.
2. Navigate to the location containing the Installation Manager installation files.
3. Run the administrative installation program for the Installation Manager `install.exe`.
4. Ensure that the Installation Manager package is selected, and click **Next**.
5. Follow the instructions in the installation wizard, and click **Next** until you reach the summary information.
6. Verify the information, and click **Install**. When the installation process is complete, a message confirms the success of the process.
7. Add the product repository for WebSphere Application Server Version 8.5 and the supplements, such as IBM HTTP Server and plug-ins to your Installation Manager preferences.
   a. From the IBM Installation Manager, click **File** > **Preferences**.
   b. Select **Repositories**.
   c. Click **Add Repository**.
   d. Specify the location of the WebSphere Application Server repository files, `<somepath>\repository.config`. For example: `E:\WAS_ND_V8.5\repository.config`
   e. Click **OK**.
   f. Click **Add Repository**.

g. Specify the location of the WebSphere Application Server supplements. For example: `E:\WAS_V85_SUPPL\repository.config`
h. Click **OK**.

What to do next

Install WebSphere Application Server, Version 8.5

Installing WebSphere Application Server, Version 8.5

The Privileged Session Recorder application runs on the WebSphere Application Server. Install and configure the WebSphere Application Server before the Privileged Session Recorder Server installation.

Before you begin

- Ensure that you have installed the IBM Installation Manager and that you have configured the product repository. See "Installing the IBM Installation Manager" on page 21.
- Read the WebSphere Application Server documentation.
- Ensure that you have Administrator privileges.
- Ensure that your system meets the requirements. See Hardware and software requirements.
- Ensure that all required operating system fix packs are in place. For more information about tuning operating systems for the WebSphere Application Server, see the WebSphere Application Server documentation and search for `tuning operating systems`.

For more information about installing the WebSphere Application Server, see the WebSphere Application Server Version 8.5 documentation and search for `installing WebSphere Application Server`.

About this task

Record the values that are used in the planning worksheet. See "Planning worksheet" on page 113.

You can deploy IBM Security Access Manager for Enterprise Single Sign-On in a stand-alone configuration or a network deployment cluster.

Procedure

1. Start the IBM Installation Manager. For example, click **Start** > **All Programs** > **IBM Installation Manager** > **IBM Installation Manager**.
2. Ensure that you have configured the product repository. For more information, see "Installing the IBM Installation Manager" on page 21.
3. Click **Install**. A list of available packages to install are displayed.
4. Select the following package:
   - **IBM WebSphere Application Server Network Deployment**
5. Click **Check for Other Versions, Fixes, and Extensions** to display the WebSphere Application Server Version 8.5.0.2.

   Tip: Ensure that the **Show all versions** check box is selected to display all available versions.
6. Select the following package:
   - **IBM WebSphere Application Server Network Deployment**

– **Version 8.5.0.2**

CAUTION:
Selecting a package other than the ones mentioned earlier can produce undesirable results.

7. Click **Next**.
8. Select the following fix and click **Next**:
   - For x86 Windows operating systems: `8.5.0.0-WS-WASJavaSDK-WinX32-IFPM91292 8.5.0.20130723_1400`
   - For x64 Windows operating systems: `8.5.0.0-WS-WASJavaSDK-WinX64-IFPM91292 8.5.0.20130723_1359`
9. Follow the instructions in the Installation Manager, and click **Next** until you reach the summary information.
10. Review the installation summary and verify that the package for **IBM WebSphere Application Server Network Deployment Version 8.5.0.2** is selected.
11. Select the correct platform version.
12. Click **Install**. When the installation process is complete, a message confirms the success of the process.
13. Click **Finish**.

What to do next

Install the IBM HTTP Server Version 8.5.

Installing the IBM HTTP Server, Version 8.5

The IBM HTTP Server, Version 8.5 must be installed through the IBM Installation Manager.

Before you begin

- Ensure that you have installed the IBM Installation Manager and that you have configured the product repository. See "Installing the IBM Installation Manager" on page 21.
- Ensure that you have the supplemental images in the repository.
- Ensure that your system meets the requirements.
- Ensure that you have Administrator privileges.
- Ensure that there is no service listening to port 80, 443 and 8008.
- For detailed and up-to-date installation instructions, see the IBM HTTP Server documentation. In the WebSphere Application Server, Version 8.5 product documentation, search for `Installing IBM HTTP Server using the GUI`.

About this task

Use the IBM HTTP Server, Version 8.5.0.2 package in the IBM Installation Manager to install the IBM HTTP Server, Version 8.5.

Record any values that you use in the planning worksheet. See "Planning worksheet" on page 113.

Multiserver installations: If you are installing a cluster of HTTP servers for high availability, use a load balancer to distribute requests to servers in the cluster. When you use a load balancer, remember to record the IP address or target host

name of the load balancer in the "Planning worksheet" on page 113.

Procedure

1. Start the IBM Installation Manager. For example, click **Start** > **All Programs** > **IBM Installation Manager** > **IBM Installation Manager**.
2. Ensure that you have configured the product repository. For more information, see "Installing the IBM Installation Manager" on page 21.
3. Click **Install**. A list of available packages to install are displayed.
4. Select the following packages:
   - **IBM HTTP Server for WebSphere Application Server**
   - **Web Server Plug-ins for IBM WebSphere Application Server**
   - **WebSphere Customization Toolbox**

   CAUTION:
   Selecting a package other than the ones that are listed earlier can produce undesirable results.
5. Click **Check for Other Versions, Fixes, and Extensions**.

   Tip: Ensure that the **Show all versions** check box is selected to display all available versions.
6. Select the following packages:
   - **IBM HTTP Server for WebSphere Application Server**
     - **Version 8.5.0.2**
   - **Web Server Plug-ins for IBM WebSphere Application Server**
     - **Version 8.5.0.2**
   - **WebSphere Customization Toolbox**
     - **Version 8.5.0.2**

   CAUTION:
   Selecting a package other than the ones that are listed earlier can produce undesirable results.
7. Click **Next**.
8. Under **WebSphere Customization Toolbox 8.5.0.2**, ensure that **Web Server Plug-ins Configuration Tool** is selected.
9. Follow the instructions in the Installation Manager and in the following steps.
10. In the **Web Server Configuration** panel, complete the following steps and click **Next**:
    a. Verify that the **HTTP Port** is 80.
    b. Verify that **Run IBM HTTP Server as a Windows Service** is selected.
    c. Select **Log on as a local system account**.
    d. In the **Startup type** list, select **Automatic**.
11. Review the installation summary.
12. Click **Install** to start the installation. When the installation process is complete, a message confirms the success of the process.
13. Click **Finish**.

What to do next

1. Start the IBM HTTP Server service.

- Click **Start** > **All Programs** > **IBM HTTP Server <*version*>** > **Start HTTP Server**.

2. Verify that you can access the web server from a web browser. For example:
   - To access the web server on the local computer, type `http://localhost` or `http://mywebsvr1`.

     Where

     `mywebsvr1` is your computer name.
   - To access the web server remotely, when a name server is available to resolve host names, type `http://<fully_qualified_host_name>`. For example: `http://mywebsvr1.example.com`.

Preparing the WebSphere Software, Version 7.0

Prepare the WebSphere Software, Version 7.0 with the latest fix packs for all the required components.

Installing WebSphere Application Server, Version 7.0

The Privileged Session Recorder application runs on the WebSphere Application Server. Install and configure the WebSphere Application Server before you install the Privileged Session Recorder.

Before you begin

- If the WebSphere Application Server is already installed, you must ensure that you have the latest fix packs.
- Read the WebSphere Application Server documentation.
- Ensure that you have Administrator privileges.
- Ensure that your system meets the requirements. See Hardware and software requirements.
- Ensure that all required operating system fix packs are in place. For more information about tuning operating systems for the WebSphere Application Server, see the WebSphere Application Server documentation and search for `tuning operating systems`.
- When you install WebSphere Application Server on Windows Server 2008 R2 operating system, the prerequisites check can fail. To resolve the issue, see this technote.

For more information about installing the WebSphere Application Server, see:

- Support
- WebSphere Application Server Version 7.0 documentation

About this task

Use the WebSphere Application Server Network Deployment version included with the IBM Security Privileged Identity Manager installation media to ensure that you are using the correct version.

You can deploy IBM Security Privileged Identity Manager in a stand-alone configuration or a network deployment cluster.

Procedure

1. Take one of the following actions:
   - Access the IBM WebSphere Application Server Network Deployment, Version 7.0 media for your operating system.

- Extract the files from the archive file that you downloaded from Passport Advantage. For example: `C1G2JML.zip`

  Note: The archive file name can be different. The archive file name depends on the distribution you download.

2. Run the WebSphere installation program `launchpad.exe`.
3. Click **Launch the installation wizard for WebSphere Application Server Network Deployment**.
4. Follow the instructions in the installation wizard until you reach the **Installation Directory** page.
5. In the **Installation Directory** page, accept the default installation directory or change the value. The default installation location is `c:\Program Files\IBM\WebSphere\AppServer`.
6. In the **WebSphere Application Server Environments** page, choose **None**. You create required profiles manually through the Profile Management tool.
7. When the warning is displayed, click **Yes** to continue without creating profiles.
8. In the **Repository for Centralized Installation Managers** page, click **Next**.
9. Follow the rest of the instructions in the installation wizard.
10. When you see the **Installation Results** page, clear the **Create a new WebSphere Application Server profile using the Profile Management Tool** check box.
11. Click **Finish**.

What to do next

Install the WebSphere Update Installer to apply the latest WebSphere Application Server fix packs.

Installing the WebSphere Update Installer

Install the WebSphere Update Installer to apply maintenance fix packs.

Before you begin

- Download and use the latest version of the Update Installer from the support page: http://www.ibm.com/support/docview.wss?uid=swg24020448.
- Ensure that your system meets the requirements.
- Review the prerequisites before installing the Update Installer.
- For the detailed instructions, see the WebSphere Application Server documentation and search for `installing the Update Installer`.

About this task

The IBM Update Installer for WebSphere software simplifies the maintenance of the following WebSphere Application Server components:

- WebSphere Application Server
- IBM HTTP Server
- IBM HTTP Server plug-in for WebSphere

Procedure

1. Copy and extract the Update Installer compressed file to a writable disk.
   For example: `7.0.0.29-WS-UPDI-WinAMD64`

2. Browse to the extracted `UpdateInstaller` directory.
3. Run `install.exe` to start the installation wizard for the Update Installer.
4. Follow the instructions in the installation wizard.
5. Before you finish the installation, clear the **Launch IBM Update Installer for WebSphere software on exit** check box.
6. Click **Finish**.

What to do next

Apply the latest fix packs for WebSphere Application Server.

Installing WebSphere Application Server fix packs

You must apply the latest WebSphere Application Server fix pack before you run the Privileged Session Recorder Server installation program.

Before you begin

- If you already have an installed WebSphere Application Server, ensure that you are using the required level of fix packs. See "Hardware and software requirements" on page 7.
- If you are reusing an existing WebSphere Application Server with existing profiles, stop any WebSphere Application Server profiles that might be running.

  In a command prompt, type `<was_home>\profiles\<profile_name>\bin\stopServer.bat <server_name>`. For example: `C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\bin\stopServer.bat server1`.
- Download the latest IBM Update Installer from the IBM Support and Downloads website: http://www.ibm.com/support/docview.wss?uid=swg24020448.

About this task

For detailed and up-to-date installation instructions, see the WebSphere Application Server documentation.

In a clustered deployment, you must install the required WebSphere Application Server fix pack on the deployment manager and on each node of the cluster.

Procedure

1. Download the latest fix packs.
   a. Access the WebSphere Application Server support site at http://www.ibm.com/software/webservers/appserv/was/support/.
   b. Click the **Downloads** link.
   c. Follow the links and instructions on the page to determine the fix packs to download.
   d. Download fix packs for other WebSphere Application Server components. For example:
      - **<*architecture*> AMD/Intel AppServer**
      - **<*architecture*> AMD/Intel IBM HTTP Server**
      - **<*architecture*> AMD/Intel Java SDK**
   e. Optional: Copy the downloaded fix packs to the `<updi_home>\maintenance` directory. For example: copy `7.0.0-WS-WAS-WinX64-FP0000029.pak` to `C:\Program Files\IBM\WebSphere\UpdateInstaller\maintenance`.
2. Start the IBM Update Installer. (**Start** > **All Programs** > **IBM WebSphere** > **Update Installer for WebSphere V7.0 Software** > **Update Installer**)

3. In the Product Selection page, select the WebSphere installation directory and click **Next**. The default is `C:\Program Files\IBM\WebSphere\AppServer`.
4. Select **Install Maintenance Package** and click **Next**.
5. In the directory path, specify the location of the maintenance or fix pack.
6. Select the WebSphere Application Server fix packs and click **Next**. Select the WebSphere Application Server and SDK components.
7. After the prerequisites checker completes successfully, click **Next**.

Related information:

IBM WebSphere Application Server documentation

Installing the IBM WebSphere Application Server Web 2.0 and Mobile feature pack

You must install the Web 2.0 and Mobile feature pack on the WebSphere Application Server. For clustered deployments, you must install the feature pack on all the computers that are part of the cluster in the same path.

Before you begin

- Install and configure the WebSphere Application Server.
- Download the IBM WebSphere Application Server Web 2.0 and Mobile feature pack from Passport Advantage.

Procedure

1. Extract the feature packs files to a location on the WebSphere Application Server computer.
2. Install the feature pack by following the installation instructions included with the Web 2.0 and Mobile feature pack.

Installing the IBM HTTP Server, Version 7.0

You can install the web server on a separate server or on the same server as the WebSphere Application Server. The web server routes requests from client computers to the WebSphere Application Server or nodes in a cluster.

Before you begin

- Ensure that your system meets the requirements.
- Ensure that you have Administrator privileges.
- Ensure that there is no service listening to port 80, 443 and 8008.

For detailed and up-to-date installation instructions, see the IBM HTTP Server documentation. In the WebSphere Application Server, Version 7.0 product documentation, search for `Installing the IBM HTTP Server`.

About this task

Use the IBM HTTP Server installation media that is provided with IBM Security Privileged Identity Manager to ensure that you are using the correct version.

Multiserver installations: If you are installing a cluster of HTTP servers for high availability, use a load balancer to distribute requests to servers in the cluster.

Procedure

1. Take one of the following actions:
   - Access the WebSphere Application Server media for your operating system.

- Extract the files from the supplementary archive file that you downloaded from Passport Advantage. For example: `C1G2KML.zip`

  Note: The archive file name can be different. The archive file name depends on the distribution you download.

Browse to the `/IHS` directory. For example: `C:\Images\C1G2KML\IHS`.

2. Run `install.exe`.
3. Follow the instructions in the installation wizard and in the following steps.
4. In the **Port Values Assignment** panel, verify the following default values:

   HTTP Port
   80

   HTTP Administration Port
   8008
5. In the **Windows Service Definition** panel, complete the following steps:
   a. Verify that **Run IBM HTTP Server as a Windows service** is selected.
   b. Verify that **Run IBM HTTP Administration as a Windows service** is selected.
   c. Select the **Log on as a local system account** check box.
   d. In the **User Name** field, specify a local system account. For example: `administrator`.
   e. In the **Startup type** list, select **Automatic**.
6. In the **HTTP Administration Server Authentication** panel, complete the following steps and click **Next**:
   a. Select the **Create a user ID for IBM HTTP Server adminstration server authentication** check box.
   b. Specify the HTTP Administrator account and password. For example: `ihsadmin`.
7. In the **IBM HTTP Server Plug-in for WebSphere Application Server** panel, complete the following steps:
   a. Ensure the **Install the IBM HTTP Server Plug-in for IBM WebSphere Application Server** check box is selected and click **Next**.
   b. In **Web server definition**, change or verify the default web server definition name. For example, you can use the default name `webserver1`.

      Note: If your multiserver deployment plan requires you to set up another web server, you must specify a unique web server definition name for each web server. For example: `webserver2`.
   c. For **Host name or IP address for the Application Server**, specify the name of the application server. For example: `appsvr1.example.com`.
   d. Click **Next**.
8. Review the installation summary.
9. Click **Next** to start the IBM HTTP Server installation.
10. Click **Finish**.
11. Start the IBM HTTP Server and Admin Server service.
    a. Click **Start** > **All Programs** > **IBM HTTP Server V7.0** > **Start Admin Server**.
    b. Click **Start** > **All Programs** > **IBM HTTP Server V7.0** > **Start HTTP Server**.

12. Verify that you can access the web server from a web browser. For example:
    - To access the web server on the local computer, type `http://localhost` or `http://mywebsvr1`.

      Where

      `mywebsvr1` is your computer name.
    - To access the web server remotely, when a name server is available to resolve host names, type `http://<fully_qualified_host_name>`. For example: `http://mywebsvr1.example.com`.

What to do next

You are ready to apply the latest fix packs for IBM HTTP Server.

Installing the IBM HTTP Server fix packs

Apply the latest fix packs for the IBM HTTP Server.

Before you begin

- Install the WebSphere Application Server Update Installer.
- Download the latest fix packs.

About this task

If you have more than one IBM HTTP Server in your deployment, install the fix pack on each web server.

Procedure

1. Optional: Copy the fix pack that you downloaded to the `<was_home>/UpdateInstaller/maintenance`. For example: `7.0.0-WS-IHS-WinX64-FP0000029.pak` for Windows x64 platforms.
2. Stop the IBM HTTP Server. Click **Start** > **All Programs** > **IBM HTTP Server V7.0** > **Stop HTTP Server**.
3. Stop the Admin Server. Click **Start** > **All Programs** > **IBM HTTP Server V7.0** > **Stop Admin Server**.
4. Install the fix pack.
    a. Launch the Update Installer wizard. Click **Start** > **All Programs** > **IBM WebSphere** > **Update Installer for WebSphere V7.0 Software** > **Update Installer**.
    b. Click **Next**.
    c. From the **Product Selection** panel, select the IBM HTTP Server installation directory and click **Next**. For example: `C:\Program Files\IBM\HTTPServer`.
    d. From the **Maintenance Operation Selection** panel, select **Install maintenance package** and click **Next**.
    e. In the **Maintenance Package Directory Selection** page, browse to the `<updi_home>\maintenance` directory or the path where you copied the fix pack and click **Next**. The default value is `C:\Program Files\IBM\WebSphere\UpdateInstaller\maintenance`.
    f. From the **Available Maintenance Package to Install** panel, click **Select Recommended Updates**.
    g. Select the target update and click **Next**.
    h. On the **Installation Summary** screen, click **Next**.

5. Start the IBM HTTP Server. Click **Start** > **All Programs** > **IBM HTTP Server V7.0** > **Start HTTP Server**.
6. Start the Admin Server. Click **Start** > **All Programs** > **IBM HTTP Server V7.0** > **Start Admin Server**.

What to do next

If the WebSphere plug-in for IBM HTTP Server is already installed, you must also apply the latest fix packs for the web server plug-in.

Installing the IBM HTTP Server plug-in fix pack

The latest WebSphere plug-in fix pack is required. Use the Update Installer to install the WebSphere Application Server plug-in fix pack.

Before you begin

- Install the WebSphere Application Server Update Installer.
- Install the WebSphere Application Server fix packs.

Procedure

1. Optional: Copy the fix pack file to the `<updi_home>/maintenance` directory. For example: `7.0.0-WS-PLG-WinX64-FP0000029.pak` for x64 Windows.
2. Stop the IBM HTTP Server. For example: Click **Start** > **All Programs** > **IBM HTTP Server V7.0** > **Stop HTTP Server**.
3. Install the fix pack.
   a. Start the Update Installer wizard. Click **Start** > **All Programs** > **IBM WebSphere** > **Update Installer For WebSphere v7.0 Software** > **Update Installer** and click **Next**.
   b. From the **Product Selection** panel, select the IBM HTTP Server `Plugins` directory and click **Next**. For example: `c:\Program Files IBM\HTTPServer\Plugins` directory.
   c. From the **Maintenance Operation Selection** panel, select **Install maintenance package** and click **Next**.
   d. In the **Maintenance Package Directory Selection** page, browse to the `<updi_home>\maintenance` directory or the path where you copied the fix pack and click **Next**. The default value is `C:\Program Files\IBM\WebSphere\UpdateInstaller\maintenance`.
   e. From the **Available Maintenance Package to install** panel, click **Select Recommended Updates**.
   f. Select the target update and click **Next**.
   g. On the **Installation Summary** screen, click **Next**, to begin fix pack installation.
   h. Click **Finish**.
4. Start the IBM HTTP Server. For example: Click **Start** > **All Programs** > **IBM HTTP Server V7.0** > **Start HTTP Server**.

Stand-alone server prerequisite tasks

A stand-alone production deployment is typically used by smaller sites. A stand-alone server deployment can be deployed in demonstration configurations.

If you are reusing existing middleware that was previously deployed, apply the minimum supported fix packs before you install the Privileged Session Recorder Server.

Creating stand-alone profiles (Profile Management tool)

For a single-server or stand-alone environment, you can create a stand-alone WebSphere Application Server profile with the interactive Profile Management Tool.

Before you begin

- Log on to the system as a user with Administrator privileges.
- Prepare the WebSphere Application Server.

About this task

For complete information about creating profiles, search for `profile concepts` in the following documentation:

- WebSphere Software, Version 8.5 documentation: http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/index.jsp
- WebSphere Software, Version 7.0 documentation: http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp

Procedure

1. Open the Profile Management Tool. For example:

   WebSphere Application Server Version 7.0
   Click **Start** > **All Programs** > **IBM WebSphere** > **Application Server Network Deployment V7.0** > **Profile Management Tool**.

   WebSphere Application Server Version 8.5
   Click **Start** > **All Programs** > **IBM WebSphere** > **IBM Websphere Application Server** > **Tools** > **Profile Management Tool**.
2. On the **Welcome to the Profile Management Tool** panel, review the information.
3. Click **Launch Profile Management Tool**.
4. On the **Profiles** panel, click **Create** to set up a new profile.
5. On the **Environment Selection** panel, click **Application server** and click **Next**.
6. Click **Typical Profile Creation** and click **Next**.
7. Type the WebSphere Administrator user name and password and click **Next**. For example: `wasadmin`.

   Note: On the **Profile Creation Summary** page, you can record the server name, host name, and port numbers to be used. A Windows service is also created automatically for the server.
8. Click **Create**.
9. After the profile creation, ensure that the **Launch the First Steps console** check box is selected.
10. Click **Finish** to start the **First Steps** console.

    Tip: If the wizard does not start automatically, complete the following steps to manually start the wizard:

For WebSphere Application Server Version 7.0:
Click **Start** > **All Programs** > **IBM WebSphere** > **Application Server** **<*version*>** > **Profiles** > **<*profile_name*>** > **First steps**.

For WebSphere Application Server Version 8.5:
Click **Start** > **All Programs** > **IBM WebSphere** > **IBM Websphere Application Server** > **Profiles** > **<*profile_name*>** > **First steps**.

11. Click the **Installation verification** link. Verifying the installation starts the stand-alone server process automatically. If the server starts successfully, the First steps output window ends with the following example output:

```
ADMU3200I: Server launched. Waiting for initialization status.

ADMU3000I: Server server1 open for e-business; process id is 236
```

If the server does not start successfully, examine the `SystemOut.log` and `SystemErr.log` files in `<was_profile_home>\logs\server_name`

What to do next

Verify that you can log on to the administrative console. Log on with your WebSphere administrative user name and password. For example: `wasadmin`.

Use any of the following methods to start the administrative console:

- In the **First Steps** console, click **Administrative console**.
- For WebSphere Application Server Version 7.0, click **Start** > **All Programs** > **IBM WebSphere** > **Application Server** **<*version*>** > **Profiles** > **<*profile_name*>** > **Administrative console**.
- For WebSphere Application Server Version 8.5, click **Start** > **All Programs** > **IBM WebSphere** > **IBM Websphere Application Server** > **Profiles** > **<*profile_name*>** > **Administrative console**.
- In a web browser, go to `https://<was_hostname>:<admin_ssl_port>/ibm/console`. For example: `https://localhost:9043/ibm/console`.

Configuring the WebSphere Application Server

You must configure the WebSphere Application Server stand-alone environment.

About this task

You must configure the WebSphere Application Server for a stand-alone deployment before you install the Privileged Session Recorder Server. Configuring the WebSphere Application Server includes securing the deployment and tuning the Java Virtual Machine (JVM).

Complete the following steps for both optional or required configurations:

1. Optional: Increase the security certificate key size.

   If your deployment includes specific minimum key size or high security requirements, you can increase the security certificate key size.
2. Configure the JVM heap size memory.
3. Verify the Windows services for WebSphere Application Server.

Configuring the heap size for the application server

You can increase the minimum and maximum Java Virtual Machine (JVM) heap size limit in WebSphere Application Server. Increasing heap size improves startup, helps prevent out of memory errors, and reduces disk swapping.

Before you begin

Before you modify the Java heap size, ensure that the host has enough physical memory to support a JVM of 4.0 GB without swapping. If the physical memory of the host system exceeds 4 GB, you can increase the maximum heap size. However, if the heap size is too large, the system does not have enough physical memory and starts allocating virtual memory to hold the data.

About this task

Adjust the Java heap size before installing the component. To learn more, search for *Java virtual machine settings heap tuning* in the following documentation:

- WebSphere Software, Version 8.5 documentation: http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/index.jsp
- WebSphere Software, Version 7.0 documentation: http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp

If you have multiple servers, repeat this procedure for every server in the cluster.

Procedure

1. On the WebSphere Application Server host, for the Privileged Session Recorder Server, log on to the administrative console. For example: `https://localhost:9043/ibm/console/`.
2. Navigate to the Java virtual machine settings.
   a. Expand **Servers** > **Server Types** and select **WebSphere application servers**.
   b. Click the name of your server.
   c. Under the **Server Infrastructure** group, click to expand **Java and Process Management**.
   d. Click **Process Definition**.
   e. Under the **Additional Properties** group, click **Java Virtual Machine**.
3. Use the following settings (for a single server instance, 4 GB host):
   - **Initial Heap Size**: `1024`
   - **Maximum Heap Size**: `2048`
4. Click **OK**.
5. In the messages box, click **Save**.
6. Click **OK**.
7. In the messages box, click **Save**.
8. Restart the WebSphere Application Server.

Verifying the Windows service for WebSphere Application Server

Verify that a Windows service for the WebSphere Application Server is created.

Procedure

1. Open the Windows Services management console.
   a. Click **Start** > **Run**.
   b. Type `services.msc`.
2. Verify that the service is displayed in the list of services: `IBM WebSphere Application Server <version> - <node_name>`

Configuring the IBM HTTP Server plug-in (stand-alone)

Deploy the IBM HTTP Server plug-in and configure connection requests to forward connections over secure Secure Sockets Layer (SSL) to the WebSphere Application Server. The web server routes requests received from client workstations to the application server.

Before you begin

- If the server is installed on a computer that has no previous versions of the server, you can use the default values for the ports. Use a utility like **netstat**. For example, to check whether a port is already in use, specify **netstat** with the following parameters: **netstat -na -p tcp -o**.
- If there are other applications listening to port 80, shut down the applications before you install the IBM HTTP Server.
- Ensure that the following software is started:
  – IBM HTTP Server
  – IBM HTTP Server Administration Server
  – WebSphere Application Server

About this task

Configuring IBM HTTP Server is a three-stage process.

1. Grant remote server administration rights to the IBM HTTP Server configuration to simplify web server administration from the WebSphere administrative console.
2. Secure the connection between the IBM HTTP Server and WebSphere Application Server with a trusted SSL connection.
3. Centralize the connection points for each web server.

The following example steps apply to IBM HTTP Server Version 7.0. For specific steps that apply to IBM HTTP Server Version 8.5 and the plug-in, search for `Implementing a web server plug-in` in the IBM HTTP Server, Version 8.5 product documentation.

Procedure

1. Define the web server configuration for the WebSphere Application Server.

   If the IBM HTTP Server and WebSphere Application Server are on the same computer:

   a. Log on to the WebSphere administrative console, for example `https://localhost:9043/ibm/console`.
   b. In the navigation pane, click **Servers** > **Server types** > **Web servers**.
   c. Click **New**.
   d. Follow the instructions in the wizard to create a definition of the web server.

- For **Server name**, specify a web server entry name, which is unique within the node for the web server. For example: `webserver1`.

  Tip: The Server name is not the web server host name.
- For **Type**, specify the type of web server you prepared. For example: **IBM HTTP Server**.
- For **Host name**, specify the host name of the web server.
- In **Step 3** of the wizard, in the **Administration server properties** section, specify the IBM HTTP Server administration user credentials. For example: `ihsadmin`.
- Ensure the **Use SSL** check box is not selected.
- In the **Messages** box, click **Save**. The web server status is started.

If the IBM HTTP Server and WebSphere Application Server are not on the same computer, run the web server plug-in configuration script.

a. From `<ihs_home>\Plugins\bin`, on the IBM HTTP Server host, copy the `configure<web_server_definition_name>.bat` file. For example: `configurewebserver1.bat`.

b. On the application server, paste the `configure<web_server_definition_name>.bat` file to the `<was_home>\bin` folder. For example: `C:\Program Files\IBM\WebSphere\AppServer\bin`

c. From a command prompt, on the application server, run the following command.

```
configure<web_server_definition_name>.bat
-profileName <profile_name>
-user <was_admin_name>
-password <was_admin_password>
```

For example:

```
configurewebserver1.bat -profileName AppSrv01 -user wasadmin
-password p@ssw0rd
```

d. Close the command prompt after the command completes with the following line:

```
Configuration save is complete.
```

You successfully configured a web server definition on the WebSphere administrative console. For example: `webserver1`.

2. In the WebSphere administrative console, click **Servers** > **Server Types** > **Web servers**. Verify that the web server definition is displayed. For example: **webserver1**.
3. Grant remote server management rights to the WebSphere Application Server Administrator by supplying the IBM HTTP Server Administrator account.
   a. In the administrative console, click **Servers** > **Server Types** > **Web servers**.
   b. Click the *<Web_server_name>*. For example: `webserver1`.
   c. In the **Additional Properties** section on the **Configuration** tab, click **Remote Web Server Management**.
   d. Enter the IBM HTTP Server administration server authentication user ID and password. For example: `ihsadmin`.
   e. Clear the **Use SSL** check box.

f. Click **OK**.

g. In the **Messages** box, click **Save**.

4. (Complete this step only if the IBM HTTP Server and WebSphere Application Server are not on the same computer; or if you are using a load balancer.) Set up the SSL certificates signed by the WebSphere Application Server certificate authority.

   Note: The certificate uses the IBM HTTP Server computer name as the Common Name (CN). The purpose is to facilitate communication between the client and the IBM HTTP Server.

   a. On the IBM Integrated Solutions Console navigation pane, click **Security** > **SSL certificate and key management** > **Key stores and certificates** > **CMSKeyStore** > **Personal certificates**.

   b. Select the certificate named **default**.

   c. Click **Delete**.

   d. Click **Create** > **Chained Certificate**.

   e. Specify `default` as the alias for the certificate.

   f. In **Key size**, specify the certificate key size. If the root CA for WebSphere Application Server is a 2048 bits certificate, you can specify a 2048 bits key size. The default is 1024 bits.

      Important: Do not select 2048 bits if you did not recreate the root CA with a 2048 bits key size.

   g. In the **Common Name** field, you can enter one of the following names:
      - The fully qualified domain name of the computer where the IBM HTTP Server is installed. For example: `webserver1.example.com`.
      - The fully qualified host name of the load balancer if a load balancer is used.

   h. Optional: Enter the remaining optional information.

   i. Click **OK**.

   j. In the **Messages** box, click **Save**.

   k. If you have more than one IBM HTTP Server, for each IBM HTTP Server, repeat steps a to j.

   The **Personal Certificates** section displays the new certificate.

5. Synchronize the WebSphere Application Server keystore with the IBM HTTP Server keystore.

   a. On the IBM Integrated Solutions Console navigation pane, click **Servers** > **Server Types** > **Web servers**.

   b. Click the <*Web server name*>.

   c. In the **Additional Properties** section on the **Configuration** tab, click **Plug-in properties**.

   d. Click **Copy to Web Server key store directory**.

   e. Click **OK**.

   f. In the **Messages** box, click **Save**.

Enabling SSL directives on the IBM HTTP Server

You must enable the Secure Sockets Layer (SSL) directives to encrypt traffic to and from the IBM HTTP Server.

Before you begin

Determine the alias of the default SSL certifcate.

Tip: To determine the alias of the default SSL certificate, complete the following steps:

1. In the IBM Integrated Solutions Console navigation pane, click **Security** > **SSL certificate and key management**.
2. Under **Related Items**, click **Key stores and certificates**.
3. Click **CMSKeyStore**.
4. Under **Additional Properties**, click **Personal certificates**.

About this task

By default, SSL communication is disabled on the IBM HTTP Server. To enable SSL, you must add the SSL Apache directive to the `httpd.conf` file.

Complete this procedure for every web server.

Procedure

1. On the IBM Integrated Solutions Console, click **Servers** > **Server Types** > **Web servers**.
2. Click the <*Web server name*>.
3. In the **Additional Properties** section on the **Configuration** tab, click **Configuration File**.
4. Append the following lines to the end of the configuration file:

   ```
   LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
   Listen 0.0.0.0:443
   ## IPv6 support:
   #Listen [::]:443
   <VirtualHost *:443>
        SSLEnable
        SSLProtocolDisable SSLv2
   SSLServerCert default
   </VirtualHost>
   KeyFile "<ihs_home>\Plugins\config\<web_server_definition>\plugin-key.kdb"
   SSLDisable
   ```

   where

   default
   Specifies the alias of the default SSL certificate.

   <ihs_home>\Plugins\config<*web_server_definition*>**\plugin-key.kdb**
   Specifies the path to the plug-in key store file `plugin-key.kdb`.

   For example: `C:\Program Files\IBM\HTTPServer\Plugins\config\webserver1\plugin-key.kdb`.
5. Click **Apply**.
6. Click **OK**.
7. Select **General Properties** > **Apply**.
8. In the **Messages** box, click **Save**.
9. Restart the IBM HTTP Server.
   a. On the IBM Integrated Solutions Console, click **Servers** > **Server Types** > **Web servers**.

b. Select the check box of the corresponding web server. For example: `webserver1`.
c. Click **Stop**.
d. Select the check box for the web server again.
e. Click **Start**.

10. Verify that the SSL directives are enabled correctly. Type the following HTTPS address in a web browser. For example:
    - `https://<ihs_host>`

      For example: `https://mywebsvr.example.com`.

      A web browser security prompt might display because you are accessing a page over the secure HTTPS protocol. Follow the instructions in the dialog box to accept the security certificate and continue to the page.
    - `http://<ihs_host>`

      For example: `http://mywebsvr.example.com`.

      You can also verify that pages over HTTP protocol are still accessible.
11. If necessary, repeat the verification step 10 for each web server in your deployment.
12. If the verification fails, check whether the custom variables you specified in step 4 on page 39 are added and replaced correctly.

Clustered server environment prerequisite tasks

A clustered deployment is typically used in enterprise production environments.

Clusters enable you to scale your IBM Security Privileged Identity Manager configuration. Clusters enable enterprise applications to be highly available because requests are automatically routed to the running servers in the event of a failure.

If you are reusing existing middleware, apply the minimum supported fix packs before you install the IBM Security Privileged Identity Manager.

For a network deployment environment, follow this process:

1. Create a deployment manager profile before you create the other profiles.

   The deployment manager profile provides centralized management of application servers.
2. Optional: If your deployment requires security certificates of a specific key size, see “Re-creating the root CA for WebSphere Application Server 7.0 on the deployment manager before creating member nodes” on page 97
3. Create the following custom profile for each managed node.

   Managed member nodes or a *custom* profile does not have its own administrative console. It is managed under the deployment manager node. You can use the administrative console to install the **ISPIMRecorder** application to the cluster that was created with the custom nodes.
4. Create a cluster and cluster members.
5. Configure the WebSphere Application Server for a cluster.
6. Configure the IBM HTTP Server.

Note: If the server is newly installed on a computer that has no previous versions of the server, you can use the default values for the ports. Use a utility like

netstat to check whether a port is already in use. Changing the default ports is typically done by an experienced WebSphere Application Server Administrator.

The port numbers and setting used for each profile you create is always recorded in the `AboutThisProfile.txt` file. The file is stored in `<was_home>/profiles/<profile_name>/logs/`. This file is helpful when you must determine the correct port number for a stand-alone, custom node or deployment manager profile.

Deployment manager profiles

A deployment manager is a server that manages operations for a logical group, or cell, of other servers. In a network deployment, you use a group of servers to provide workload balancing and failover. The deployment manager is the central location for administering the servers and clusters in the cell.

To create a network deployment environment, the deployment manager profile is the first profile that you create.

Important:

- Do not provide a common user name like `administrator` as the WebSphere Application Server Administrator.
- Choose a user name that is least likely to conflict with your potential enterprise directory users.

Custom profiles

To configure a network deployment environment, create custom nodes and federate them into the deployment manager. Later, you can use the WebSphere Application Server administrative console to install the Privileged Session Recorder application on the various member nodes.

Unlike a stand-alone profile, a custom profile is an empty node that does not contain the default server that the stand-alone profile includes. After the custom profile is federated to the deployment manager, the node becomes a *managed node*.

A managed node, which contains a node agent, is managed by a deployment manager.

Creating a deployment manager profile (Profile Management Tool)

Create a deployment manager profile to manage all other IBM WebSphere Application Server processes running in the cell, including node agents and application server processes.

Before you begin

- Log on to the system as a user with Administrator privileges.
- Prepare the WebSphere Application Server.
- Ensure that two way host name resolution is set up between the deployment manager, the nodes, and every other node. You can add the entries to a DNS host or the hosts file.

About this task

For detailed and up-to-date installation instructions, see the WebSphere Application Server documentation.

The Profile Management Tool assigns port numbers that you must use during the Privileged Session Recorder Server configuration and administration. This information is recorded in the `AboutThisProfile.txt` file in `<was_home>/profiles/<profile_name>/logs`.

Procedure

1. Open the Profile Management Tool. For example:

   WebSphere Application Server Version 8.5
   Click **Start** > **All Programs** > **IBM WebSphere** > **IBM Websphere Application Server** > **Tools** > **Profile Management Tool**.

   WebSphere Application Server Version 7.0
   Click **Start** > **All Programs** > **IBM WebSphere** > **Application Server Network Deployment V7.0** > **Profile Management Tool**.
2. Click **Launch Profile Management Tool**, and click **Next**.
3. In the **Environment selection** page, click **Management**, and click **Next**.
4. In the **Server Type Selection** page, select **Deployment manager**, and click **Next**.
5. In the **Profile Creation Options** page, select **Typical profile creation**, and click **Next**.
6. In the **Administrative Security** page, ensure that the **Enable administrative security** check box is selected.
7. Specify a WebSphere user name and password and click **Next**. For example: `wasadmin`.
8. Review the settings in the **Profile Creation Summary** page. For example:
   - Location (Default is `C:\Program Files\IBM\WebSphere\AppServer\profiles\Dmgr01`)
   - Profile name (Default is `Dmgr01`)
   - Cell name
   - Node name
   - Host name
   - Administrative console port: (Default is `9060`)
   - Administrative console secure port (Default is `9043`)
   - Deployment manager bootstrap port (Default is `9809`)
   - Deployment manager SOAP connector port (Default is `8879`)
9. Click **Create**. The deployment manager profile creation process starts.
10. Ensure the **Launch the First Steps console** check box is selected.
11. Click **Finish** to start the **First Steps** console.

    Tip: If the wizard does not start automatically, complete the following steps to manually start the wizard:

    For WebSphere Application Server Version 8.5:
    Click **Start** > **All Programs** > **IBM WebSphere** > **IBM WebSphere Application Server** > **Profiles** > **<*profile_name*>** > **First steps**.

For WebSphere Application Server Version 7.0:
Click **Start** > **All Programs** > **IBM WebSphere** > **Application Server** **<*version*>** > **Profiles** > **<*profile_name*>** > **First steps**.

12. Click the **Installation verification** link. The last two lines are displayed. The deployment manager is started.

```
IVTL0070I: The Installation Verification Tool verification succeeded.
IVTL0080I: The installation verification is complete.
```

13. Verify that you can access the administrative console. For example: browse to `https://localhost:9043/ibm/console`.
14. Close the output window and browser.
15. If there are problems, examine the `SystemOut.log` and `SystemErr.log` files in `<was_profile_home>\logs\server_name`.

What to do next

Create a custom profile.

Creating a custom profile (Profile Management Tool)

Create a custom profile that contains the node agent process and the managed server process that is part of the cluster.

Before you begin

- Log on to the system as a user with Administrator privileges.
- Prepare the WebSphere Application Server.
- Install the WebSphere Application Server fix packs.
- Ensure that two way host name resolution is set up between the deployment manager, the nodes, and every other node. You can add the entries to a DNS host or a hosts files.

About this task

For detailed and up-to-date installation instructions, see the WebSphere Application Server documentation.

The Profile Management Tool assigns port numbers that you must use during the Privileged Session Recorder Server configuration and administration. This information is recorded in the `AboutThisProfile.txt` file in `<was_home>/profiles/<profile_name>/logs`.

Procedure

1. Open the Profile Management Tool. For example:

   WebSphere Application Server Version 7.0
   Click **Start** > **All Programs** > **IBM WebSphere** > **Application Server Network Deployment V7.0** > **Profile Management Tool**.

   WebSphere Application Server Version 8.5
   Click **Start** > **All Programs** > **IBM WebSphere** > **IBM WebSphere Application Server** > **Tools** > **Profile Management Tool**.

2. For each WebSphere Application Server node that you want to federate to a deployment manager, do the following steps:
   a. Click **Launch Profile Management Tool**.

b. Click **Create**.
c. In the **Environment selection** page, select **Custom profile**, and click **Next**.
d. Click **Typical profile creation**, and click **Next**.
e. In the **Federation** page, specify the connection values about the deployment manager host.

Deployment manager host name or IP address:
Specify the fully qualified domain name of the deployment manager host. For example: `appsvr1.example.com`.

Note: To ensure that federation completes successfully, for a standard installation, you must use the correct deployment manager host name.

Ensure that the node can resolve the fully qualified domain name of the deployment manager host.

Deployment manager SOAP port number (default 8879)
Accept the default value or change to a different port number.

User name
Specify the deployment manager Administrator user name. For example: `wasadmin`.

Password
Specify the deployment manager Administrator password.

f. Click **Next**.
g. Review the profile creation summary.
   - Profile name (default: `Custom01`)
   - Location (default: `C:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01`)
h. Click **Create** to start the profile creation.
i. Clear the **Launch the First steps console** check box.
j. Click **Finish**.

3. If there are problems, examine the `SystemOut.log` and `SystemErr.log` files in `<was_profile_home>\logs\server_name`.

What to do next

Create a cluster and cluster members.

Creating a cluster and cluster members

Create a cluster definition and add members to the cluster.

About this task

There can be only one cluster defined in the cell.

Remember: You must deploy each Privileged Session Recorder Server cluster in its own dedicated cell. The cell cannot contain any other type of server, which includes: IBM Security Identity Manager Server, IMS Server, or any standard application server instance that runs Java EE applications.

Procedure

1. Open the administrative console and log on to the Deployment Manager with Administrator privileges.
   a. For example: in a web browser, type `https://localhost:9043/ibm/console`.
   b. Log on with the WebSphere Administrator account. For example: `wasadmin`
2. Define a new cluster.
   a. Expand the **Servers** link, and select **Clusters** > **WebSphere application server clusters**.
   b. Click **New**.
   c. In the **Cluster name** field, enter a name for the cluster. For example: type `cluster1`.
   d. Select the **Configure HTTP session memory-to-memory replication** check box and click **Next**.
   e. In the **Member name** field, type a name for the first member of the cluster. For example, `server1`.
   f. In **Select Node**, choose the node that you want to add to the cluster.
   g. Verify **Create the member using an application server template** is set to **default** and click **Next**. You added a member of the node to the cluster.
   h. Do one of the following steps:
      - If you have no other cluster members to add, click **Next**.
      - If you have more cluster members to add, type the name. Select the correct node. Click **Add member**. Specify more cluster members before you click **Next**.
   i. Click **Finish**. You created a cluster and added members to the clusters.
   j. In the **Messages** box, click **Save**. The cluster status indicates that the cluster is not started.

What to do next

Determine if there are more WebSphere Application Server deployment-specific configuration requirements for the cluster.

To continue with the WebSphere Application Server configuration, ensure that the cluster is in a stopped state in the WebSphere administrative console.

Configure WebSphere Application Server for a cluster.

Configuring WebSphere Application Server for a cluster

Define the cluster and apply required security settings for WebSphere Application Server before you install the cluster.

Before you begin

- Ensure that the deployment manager is started.
- Create profiles for member nodes in the cluster.

About this task

Configuring WebSphere Application Server for a cluster involves the following tasks:

1. Configure the heap size for WebSphere Application Server.

2. Create a Windows service for the node agent.

Configuring the heap size for the application server

You can increase the minimum and maximum Java Virtual Machine (JVM) heap size limit in WebSphere Application Server. Increasing heap size improves startup, helps prevent out of memory errors, and reduces disk swapping.

Before you begin

Before you modify the Java heap size, ensure that the host has enough physical memory to support a JVM of 4.0 GB without swapping. If the physical memory of the host system exceeds 4 GB, you can increase the maximum heap size. However, if the heap size is too large, the system does not have enough physical memory and starts allocating virtual memory to hold the data.

About this task

Adjust the Java heap size before installing the component. To learn more, search for *Java virtual machine settings heap tuning* in the following documentation:

- WebSphere Software, Version 8.5 documentation: http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/index.jsp
- WebSphere Software, Version 7.0 documentation: http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp

If you have multiple servers, repeat this procedure for every server in the cluster.

Procedure

1. On the WebSphere Application Server host, for the Privileged Session Recorder Server, log on to the administrative console. For example: `https://localhost:9043/ibm/console/`.
2. Navigate to the Java virtual machine settings.
   a. Expand **Servers** > **Server Types** and select **WebSphere application servers**.
   b. Click the name of your server.
   c. Under the **Server Infrastructure** group, click to expand **Java and Process Management**.
   d. Click **Process Definition**.
   e. Under the **Additional Properties** group, click **Java Virtual Machine**.
3. Use the following settings (for a single server instance, 4 GB host):
   - **Initial Heap Size**: `1024`
   - **Maximum Heap Size**: `2048`
4. Click **OK**.
5. In the messages box, click **Save**.
6. Click **OK**.
7. In the messages box, click **Save**.
8. Restart the WebSphere Application Server.

Creating a Windows service for the node agent

In a network deployment configuration, you can create the node agent as a Windows service to make WebSphere Application Server nodes easier to start and manage.

About this task

Create the node agent as a Windows service so that the node agent starts automatically when the server is rebooted. An activated node agent communicates with the cell Deployment Manager to manage the set of servers on the node.

If you do not create the node agent as a service, you must run the **startNode** command manually. For example: <was_home>/profiles/<profile_name>/startNode.bat.

Procedure

1. Open a command prompt window.
2. Change the directory to <was_home>\bin. For example: type cd c:\Program Files\IBM\WebSphere\AppServer\bin
3. Type the **WASService** command with the following parameters:

   Note: The command is case-sensitive. Enter the command on a single line without line breaks.

   ```
   WASService -add <profile_name>_nodeagent -serverName nodeagent
   -profilePath "<was_home>\profiles\<profile_name>"
   -wasHome "<was_home>"
   -logRoot "<was_home>\profiles\<profile_name>\logs\nodeagent"
   -logFile "<was_home>\profiles\<profile_name>\logs\nodeagent\startServer.log"
   -restart true
   -startType automatic
   ```

   Where

   <was_home>
   Specifies the directory where WebSphere Application Server is installed. For example: C:\Program Files\IBM\WebSphere\AppServer

   <profile_name>
   Specifies the name of the custom node profile in Windows service. For example: Custom01.

   Example with sample values

   ```
   WASService -add Custom01_nodeagent -serverName nodeagent -profilePath
   "c:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01" -wasHome
   "c:\Program Files\IBM\WebSphere\AppServer" -logRoot "C:\Program
   Files\IBM\WebSphere\AppServer\profiles\Custom01\logs\nodeagent" -logFile
   "C:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01\logs\
   nodeagent\startServer.log" -restart true -startType automatic
   ```

4. Press **Enter**. The last line of the screen is displayed.

   ```
   IBM WebSphere Application Server <version> - Custom01_nodeagent service successfully
   added.
   ```

5. Close the command prompt.
6. Verify that the service is added to Windows services.
   a. Click **Start** > **Run**.
   b. Type services.msc.
   c. Verify that the node agent service is displayed. For example:IBM WebSphere Application Server <version> - Custom01_nodeagent.
7. If you have more nodes, repeat this task for other nodes in your cluster. For example: *Custom02*.

Configuring the IBM HTTP Server plug-in (network deployment)

Deploy the IBM HTTP Server plug-in and configure connection requests to forward connections over Secure Sockets Layer (SSL) to the WebSphere Application Server.

Before you begin

Ensure that the following software is started:

- IBM HTTP Server
- IBM HTTP Server Administration Server
- Deployment manager
- Node agent on the managed node

About this task

Configuring the IBM HTTP Server is a three-stage process.

1. Configure the IBM HTTP Server plug-in for WebSphere Application Server. If the IBM HTTP Server and the WebSphere Application Server are not on the same computer, you must set up a trusted SSL connection.
2. Synchronize the IBM HTTP Server and the WebSphere Application Server keystores.
3. Regenerate and propagate the web server plug-in configuration to centralize the connection points for each web server.

The following example steps apply to IBM HTTP Server Version 7.0. For specific steps that apply to IBM HTTP Server Version 8.5 and the plug-in, search for `Implementing a web server plug-in` in the IBM HTTP Server, Version 8.5 product documentation.

Repeat this procedure for every web server that you want to add.

Procedure

1. Run the web server plug-in configuration script.
   a. On the IBM HTTP Server host, from `<ihs_home>\Plugins\bin`, copy the `configure<web_server_definition_name>.bat` file. For example: `configurewebserver1.bat`
   b. On the deployment manager, paste the `configure<web_server_definition_name>.bat` file to the `<was_home>\bin` folder. For example: `C:\Program Files\IBM\WebSphere\AppServer\bin`
   c. Open the command prompt.
   d. Browse to `<was_home>\bin`.
   e. Run the following command on a single line:

      ```
      configure<web_server_definition_name>.bat
      -profileName <Dmgr_profile_name>
      -user <dmgr_admin_name>
      -password <dmgr_admin_password>
      ```

      For example:`configurewebserver1.bat` **`-profileName`** `Dmgr01` **`-user`** `wasadmin` **`-password`** `p@ssw0rd`
   f. Close the command prompt after the command completes with the following line:

```
Configuration save is complete.
```

Running the script plug-in added and configured a web server definition on the WebSphere administrative console (**Servers** > **Server types** > **Web servers**). For example, `webserver1`.

Note: Perform the following step (2) only if:

- The IBM HTTP Server and WebSphere Application Server are not co-located.
- You use a load balancer.

2. Set up SSL certificates signed by the WebSphere Application Server certificate authority.

   Note: The certificate uses the IBM HTTP Server computer name as the Common Name (CN). The purpose is to facilitate communication between the client and the IBM HTTP Server.

   a. On the IBM Integrated Solutions Console navigation pane, click **Security** > **SSL certificate and key management** > **Key stores and certificates** > **CMSKeyStore** > **Personal certificates**.
   b. Select the certificate named **default**.
   c. Click **Delete**.
   d. Click **Create** > **Chained Certificate**.
   e. Specify `default` as the alias for the certificate.
   f. Optional: In **Key size**, specify the certificate key size. If the root CA for WebSphere Application Server is a 2048 bit certificate, you can specify a 2048 bit key size. The default is 1024 bits.

      Important: Do not select 2048 bit if you did not recreate the root CA with a 2048 bit key size.

   g. In the **Common Name** field, you can enter one of the following names:
      - The fully qualified domain name of the computer where the IBM HTTP Server is installed. For example: `ibm-svr1.example.com`.
      - The fully qualified host name of the load balancer (if a load balancer is used).
   h. Optional: Enter the remaining optional information.
   i. Click **OK**.
   j. Click the **Save** link in the **Messages** box.

   The **Personal Certificates** section displays the new certificate.

3. Synchronize the WebSphere Application Server keystore with the IBM HTTP Server keystore.
   a. On the IBM Integrated Solutions Console navigation pane, click **Servers** > **Server Types** > **Web servers**.
   b. Click the <*Web server name*>.
   c. In the **Additional Properties** section on the **Configuration** tab, click **Plug-in properties**.
   d. Click **Copy to Web Server key store directory** and click **OK**.
   e. In the **Messages** box, click **Save**.
4. If you have multiple web servers, repeat steps 1 on page 48 to 3.
5. Regenerate and propagate the web server plug-in configuration.

Note: In a cluster environment, you want all requests to come through one central connection point so a single server URL is used. To define a central connection point, you must regenerate and propagate the WebSphere Application Server plug-in configuration for each web server.

a. Click **Servers** > **Server Types** > **Web Servers**.
b. Select the web server from the list. For example: `webserver1`.
c. Click **Generate Plug-in**.
d. Select the web server from the list. For example: `webserver1`.
e. Click **Propagate Plug-in**.

6. Synchronize the nodes with the deployment manager.

Enabling SSL directives on the IBM HTTP Server

You must enable the Secure Sockets Layer (SSL) directives to encrypt traffic to and from the IBM HTTP Server.

Before you begin

Determine the alias of the default SSL certifcate.

Tip: To determine the alias of the default SSL certificate, complete the following steps:

1. In the IBM Integrated Solutions Console navigation pane, click **Security** > **SSL certificate and key management**.
2. Under **Related Items**, click **Key stores and certificates**.
3. Click **CMSKeyStore**.
4. Under **Additional Properties**, click **Personal certificates**.

About this task

By default, SSL communication is disabled on the IBM HTTP Server. To enable SSL, you must add the SSL Apache directive to the `httpd.conf` file.

Complete this procedure for every web server.

Procedure

1. On the IBM Integrated Solutions Console, click **Servers** > **Server Types** > **Web servers**.
2. Click the *<Web server name>*.
3. In the **Additional Properties** section on the **Configuration** tab, click **Configuration File**.
4. Append the following lines to the end of the configuration file:

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 0.0.0.0:443
## IPv6 support:
#Listen [::]:443
<VirtualHost *:443>
     SSLEnable
     SSLProtocolDisable SSLv2
SSLServerCert default
</VirtualHost>
KeyFile "<ihs_home>\Plugins\config\<web_server_definition>\plugin-key.kdb"
SSLDisable
```

where

default
Specifies the alias of the default SSL certificate.

<ihs_home>\Plugins\config<*web_server_definition*>**\plugin-key.kdb**
Specifies the path to the plug-in key store file `plugin-key.kdb`.

For example: `C:\Program Files\IBM\HTTPServer\Plugins\config\webserver1\plugin-key.kdb`.

5. Click **Apply**.
6. Click **OK**.
7. Select **General Properties** > **Apply**.
8. In the **Messages** box, click **Save**.
9. Restart the IBM HTTP Server.
   a. On the IBM Integrated Solutions Console, click **Servers** > **Server Types** > **Web servers**.
   b. Select the check box of the corresponding web server. For example: `webserver1`.
   c. Click **Stop**.
   d. Select the check box for the web server again.
   e. Click **Start**.
10. Verify that the SSL directives are enabled correctly. Type the following HTTPS address in a web browser. For example:
    - `https://<ihs_host>`

      For example: `https://mywebsvr.example.com`.

      A web browser security prompt might display because you are accessing a page over the secure HTTPS protocol. Follow the instructions in the dialog box to accept the security certificate and continue to the page.
    - `http://<ihs_host>`

      For example: `http://mywebsvr.example.com`.

      You can also verify that pages over HTTP protocol are still accessible.
11. If necessary, repeat the verification step 10 for each web server in your deployment.
12. If the verification fails, check whether the custom variables you specified in step 4 on page 50 are added and replaced correctly.

Chapter 4. Installation

Install the IBM Security Privileged Identity Manager components that are required in your environment.

Note:

- To upgrade from earlier versions of installed product components, see “Upgrade to IBM Security Privileged Identity Manager” on page 63.
- Install IBM Security Identity Manager, IBM Security Access Manager for Enterprise Single Sign-On, and IBM Security Privileged Identity Manager Privileged Session Recorder on separate systems.

Complete the following tasks:

- “IBM Security Identity Manager, Version 6.0 installation”
- “IBM Security Access Manager for Enterprise Single Sign-On, Version 8.2.1 installation”
- “IBM Security Access Manager for Enterprise Single Sign-On Adapter, Version 6.0 installation” on page 54
- “IBM Privileged Session Recorder, Version 1.0.1 installation” on page 54

Related information:

For more information about the Privileged Identity Manager deployment, see the IBM Security Identity Manager wiki.

IBM Security Identity Manager, Version 6.0 installation

Install IBM Security Identity Manager with the shared access module.

To install IBM Security Identity Manager, follow the directions in the *IBM Security Identity Manager Installation Guide*. You can access the guide in the IBM Security Identity Manager documentation.

- The IBM Security Identity Manager installation wizard asks if you want to install the shared access module. **To deploy IBM Security Privileged Identity Manager, you must install the shared access module.**
- If you install the shared access module into a WebSphere cluster environment, you must complete configuration steps after the installation finishes. See the topic "Shared access module configuration" in the *IBM Security Identity Manager Installation Guide*.
- Before you begin installation, review the hardware and software requirements in IBM Security Identity Manager documentation.

IBM Security Access Manager for Enterprise Single Sign-On, Version 8.2.1 installation

Install IBM Security Access Manager for Enterprise Single Sign-On with the AccessAgent client to provide automated shared access credential check-in and check-out for IBM Security Privileged Identity Manager.

To install IBM Security Access Manager for Enterprise Single Sign-On, follow the directions in the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* in the IBM Security Access Manager for Enterprise Single Sign-On product documentation.

Use the instructions to install:

- IMS Server, Version 8.2.1
- AccessAgent, Version 8.2.1

  Note: To verify the installation, configure AccessAgent to communicate with the IMS Server.
- Optional: AccessStudio, Version 8.2.1

  To modify the bundled AccessProfiles, install AccessStudio on an administrative computer to develop custom AccessProfiles.

Note: If you have an earlier version of the components, see "Upgrading IBM Security Access Manager for Enterprise Single Sign-On" on page 64.

IBM Security Access Manager for Enterprise Single Sign-On Adapter, Version 6.0 installation

Install the IBM Security Access Manager for Enterprise Single Sign-On Adapter to manage provisioning of users to the IMS Server.

To install IBM Security Access Manager for Enterprise Single Sign-On Adapter, follow the instructions in the *IBM Security Access Manager for Enterprise Single Sign-On Adapter Installation and Configuration Guide* in the IBM Security Identity Manager product documentation.

After you install the IBM Security Access Manager for Enterprise Single Sign-On Adapter files, you must integrate the adapter into the IBM Security Privileged Identity Manager environment by completing the required configuration tasks. Follow the instructions in the *IBM Security Access Manager for Enterprise Single Sign-On Adapter Installation and Configuration Guide*.

IBM Privileged Session Recorder, Version 1.0.1 installation

Install the Privileged Session Recorder Server on WebSphere Application Server to manage and play back recordings. Install the Privileged Session Recorder agent on workstations that you want to monitor.

Privileged Session Recorder Server installation

You can install the Privileged Session Recorder Server by using the IBM Installation Manager.

Before you begin

- Review the system requirements and release notes.
- Complete the installation prerequisites.

About this task

You can set up the Privileged Session Recorder Server on a stand-alone WebSphere Application Server or on a WebSphere Application Server cluster. For a production

deployment, install the Privileged Session Recorder Server on a dedicated host for better performance.

Procedure

1. Install the Privileged Session Recorder Server.
2. Configure the Privileged Session Recorder Server.
3. Deploy the Privileged Session Recorder Server.
4. Configure connection request forwarding for the Privileged Session Recorder application.
5. For WebSphere Application Server, Version 7.0 only: Add the JAX-RS shared library.
6. Verify the Privileged Session Recorder installation.

Installing the Privileged Session Recorder Server application by using IBM Installation Manager

Install the Privileged Session Recorder Server to accept uploaded session recordings, and replay recordings.

Before you begin

- Install and configure WebSphere Application Server.

About this task

On a clustered WebSphere Application Server deployment, complete this task on the deployment manager.

Procedure

1. Extract the Privileged Session Recorder Server installation package to a location on the computer.
2. Start the Privileged Session Recorder Server installer `launchpad.exe`.
3. Click **Install IBM Privileged Session Recorder Server**.
4. In the Install Packages page, click **Next**.
5. Follow the instructions to install the Privileged Session Recorder Server. The contents are installed in the *<recorder_install_home>* location where *<recorder_install_home>* is the default installation path.

   For example: `C:\Program Files(x86)\IBM\IBM Privileged Session Recorder Server`
6. Follow the instructions to complete the installation process.

What to do next

Configure the Privileged Session Recorder Server.

Configuring the Privileged Session Recorder Server

Use the guided configuration tool to configure the WebSphere Application Server profile, provision a Privileged Session Recorder Administrator, and configure the data source for the Privileged Session Recorder Server.

Before you begin

- Complete the installation prerequisites.
- Install the Privileged Session Recorder Server by using IBM Installation Manager.

About this task

On a clustered WebSphere Application Server deployment, complete the following steps on the deployment manager.

Procedure

1. If the configuration tool is not already started, start the configuration tool. You can start the configuration tool manually from the following location `<recorder_install_home>/configtool/IBMCM.exe`.

   Note: After you install the Privileged Session Recorder Server with the IBM Installation Manager, the IBM Installation Manager, by default starts the configuration tool automatically.
2. When the configuration tool is displayed, click **Configure Privileged Session Recorder Server**.
3. Click **Guided Configuration**.
   a. In the WebSphere Application Server configuration page, provide the following information:

      Fully qualified host name
      Specify the host name for the WebSphere Application Server. For clustered deployments, specify the deployment manager. For stand-alone deployments, specify the application server. For example: `washost1.example.com`

      SOAP port
      Specify the SOAP Port. For example: `8880` is the default for WebSphere Application Server stand-alone deployments. `8879` is the default for the deployment manager on clustered deployments.

      Administrative security
      Select the box if the WebSphere administrative security setting is enabled. When administrative security is enabled, specify the WebSphere Administrator credentials.

      Administrator
      Specify the WebSphere Administrator user name. For example: `wasadmin`

      Password
      Specify the WebSphere Administrator password.

   b. Click **Next**.
   c. When the certificate prompt is displayed, review the details of the security certificate.
   d. Click **Yes** to continue.
   e. (For network deployments only) For the Discovered servers and clusters page, select the cluster.
   f. Click **Next**.
   g. In the Configure data source page, specify the following information:

      Database hostname
      Specify the database host name. For example: `dbsvr`

      Database port
      For example: `50000`

Database name
Specify the name of the datastore. For example: `ispimrecdb`

Database user name
Specify a database user with database Administrator privileges. For example: `db2admin`

Database user password
Specify the password for the database user name.

h. Click **Next**.

i. In the **Configure Security Settings** page, specify the following information:

The user credentials that you specify are used to log on to the web-based Privileged Session Recorder management console.

You can choose to create a new user, or specify an existing user.

If you choose to use an existing account, the user account must exist on WebSphere Application Server.

j. Click **Next**.

k. Review the configuration settings summary.

l. Click **Finish**. The configuration settings are applied. After the configuration process completes successfully, the configuration tool returns to the start page.

Important: Although you are returned to the start page, the WebSphere Application Server might still be restarting. Depending on your deployment environment, you might have to wait for a few minutes until the WebSphere Application Server restarts.

Note: If the configuration process is unsuccessful, an error message is displayed and the process automatically rolls back. If there are problems, you can examine the log files in `<recorder_install_home>\configtool\logs`.

What to do next

Deploy the Privileged Session Recorder Server with the configuration utility.

Deploying Privileged Session Recorder Server with the configuration utility

You can deploy the Privileged Session Recorder Server on WebSphere Application Server with the configuration utility.

Before you begin

Install the Privileged Session Recorder Server.

Procedure

1. If the configuration tool is not already started, start the configuration tool. You can start the configuration tool manually from the following location `<recorder_install_home>/configtool/IBMCM.exe`.
2. Click **Deploy Privileged Session Recorder Server**.
   a. Click **Guided Configuration**.
   b. Click **Next**.
   c. Provide information about the WebSphere Application Server.

For stand-alone deployments
Specify details for the WebSphere Application Server base profile. For example: `appsrv01`

For clustered deployments
Specify details for the WebSphere Application Server deployment manager profile. For example: `dmgr01`

3. Follow the instructions in the dialog box to complete the process.
4. If there are problems, you can examine the log files in `<recorder_install_home>\configtool\logs`.

What to do next

Configure the IBM HTTP Server for the Privileged Session Recorder application.

Configuring IBM HTTP Server for the Privileged Session Recorder application

Use the WebSphere Application Server administrative console to map the **ISPIMRecorder** application to the web-tier and application-tier hosts.

Before you begin

Ensure that the following components and applications are started:

- IBM HTTP Server admin server
- WebSphere Application Server (stand-alone) or the deployment manager (network deployment)
- (Network deployment) Node agents

Procedure

1. In the WebSphere Application Server administrative console navigation pane, click **Applications** > **Application types** > **WebSphere enterprise applications**.
2. Click **ISPIMRecorder**.
3. Under **Modules**, click **Manage Modules**. The Manage Modules page is displayed.
4. Select the check box for all the modules.
5. In the **Clusters and servers** box, select each of the target web servers, and the clusters or application servers in your deployment.

   Tip: To select multiple servers, press the Shift key and click to select multiple web servers and application servers.
6. Click **Apply**.
7. Click **OK**.
8. In the **Messages** box, click **Save**.
9. For clustered deployments, resynchronize the nodes.
   a. Click **System administration** > **Nodes**.
   b. Select the check box for each corresponding node.
   c. Click **Full Resynchronize**.
10. For clustered deployments, start the cluster.
    a. Click **Servers** > **Clusters** > **WebSphere application server clusters**.
    b. Select the check box for the cluster.
    c. Click **Stop**.

d. Click **Start**.

Note: Starting the cluster might take some time because each member node in the cluster is started.

Tip: You can click the **Refresh** command in the **Status** column to see whether the cluster status is updated.

Results

Privileged Session Recorder connection request URLs are forwarded correctly by the IBM HTTP Server to the **ISPIMRecorder** application.

Adding the JAX-RS shared library

Define a container-wide shared library in WebSphere Application Server that can be used by the deployed **ISPIMRecorder** application. This task is only for WebSphere Application Server Version 7.0.

Before you begin

- Install the WebSphere Application Server 7.0 Web 2.0 and Mobile feature pack.
- You must have WebSphere Application Server Administrator credentials.

About this task

Perform this task on the WebSphere Application Server. For clustered deployments, perform this task on the deployment manager.

Procedure

1. Log on to the WebSphere Application Server administrative console with Administrator privileges.
2. In the navigation pane, click **Environment** > **Shared libraries**.
3. In the **Scope** area, select a cell scope. For example: **Cell=HostNameNode01Cell**.
4. Click **New**.
5. In the **Name** field, type `jaxrslib`.
6. In the **Classpath** field, specify the following details:

```
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/commons-codec.jar
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/commons-lang.jar
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/httpclient.jar
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/httpcore.jar
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/ibm-wink-jaxrs.jar
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/jcl-over-slf4j.jar
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/jsr311-api.jar
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/slf4j-api.jar
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/slf4j-jdk14.jar
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/jackson/jackson-core-asl.jar
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/jackson/jackson-jaxrs.jar
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/jackson/jackson-mapper-asl.jar
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/jackson/jackson-xc.jar
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/webdav/wink-jaxrs-webdav.jar
```

7. Click **OK**.
8. Click **Save**.
9. Map the **ISPIMRecorder** application to the shared library.
   a. In the navigation pane, click **Applications** > **Application Types** > **WebSphere enterprise applications**.
   b. In the **Enterprise Applications** page, click **ISPIMRecorder**.

c. In the **Configuration** page, under **References**, click **Shared library references**.
d. Select **ISPIMRecorder**.
e. Click **Reference shared libraries**.
f. In the **Available** list, select the **jaxrslib** library.
g. Move the **jaxrslib** library to the **Selected** list by clicking **>>**.
h. Click **OK**.
i. Click **OK**.

10. Save the changes to WebSphere Application Server.
11. For clustered deployments, synchronize all the nodes.
12. Restart the **ISPIMRecorder** application.
    a. In the navigation pane, browse to **Applications** > **Application Types** > **WebSphere Enterprise Applications**.
    b. Select **ISPIMRecorder**.
    c. Click **Stop**.
    d. Click **Start**.

    The **ISPIMRecorder** application is restarted.

Verifying the Privileged Session Recorder Server configuration

Verify the Privileged Session Recorder Server installation and configuration are working.

Before you begin

Ensure that the following applications and components are started:

- **ISPIMRecorder**
- WebSphere Application Server
- IBM HTTP Server
- Database servers

Procedure

1. In a browser, go to the IBM Privileged Session Recorder console URL. For example:
   - `https://<ihs_host>/recorder/ui`
   - `https://<loadbalancer_host>:<port>/recorder/ui`

   The IBM Privileged Session Recorder console is displayed.
2. Log on to the Privileged Session Recorder Server with a user account.

Privileged Session Recorder Client installation

You can install the Privleged Session Recorder Client with the AccessAgent installer.

Before the client can communicate with the Privileged Session Recorder Server, you must configure a trusted SSL connection between the client computer and the server.

Obtaining the Privileged Session Recorder Server certificates for the client computers

Secure the channel of communication between the client computer and the IBM Privileged Session Recorder Server.

Procedure

1. Log on with Administrator privileges on the client computer.
2. Start Microsoft Internet Explorer with Administrator privileges and browse to the HTTPS URL for the Privileged Session Recorder Server. For example: `https://psr.example.com`.

   Alternatively, you can launch the URL for the IBM Privileged Session Recorder console.
3. In Microsoft Internet Explorer, export the security certificates to a file. Complete the following instructions:
   a. Click **File** > **Properties**.
   b. Click **Certificates**.
   c. Click **Certification Path** tab.
   d. Click **Details** tab.
   e. For each certificate marked with a red X in the certificate hierarchy:
      1) Click **View Certificate**.
      2) Click **Details**.
      3) Click **Copy to File**.
      4) Follow the instructions in the wizard with the following considerations:
         - When the **Export format** page is displayed, select the **DER encoded binary x.509 (CER)** format.
         - Save the certificates to a location on your computer. For example: `webhost.cer`.
4. Deploy the certificates on client computers. Choose one of the following ways:.
   - To deploy the certificates with the AccessAgent installation package, copy the CER files to the following locations in the installer package:

     Note: If the `SessionRecorder` folder does not exist in the `Config` folder, create the `SessionRecorder` folder first.

     For x86 operating systems

     `aa-<version_number>\{9713108D-08D5-474E-92A3-09CD7B63DB34}\Config\SessionRecorder`

     For x64 operating systems

     `aa-<version_number>_x64\{E72C4028-45BB-4EE6-8563-3066EEB39A84}\Config\SessionRecorder`

     To continue, see "Installing the Privileged Session Recorder client."
   - To configure SSL without using the AccessAgent installer, see "Deploying the SSL certificates on the client computers manually without using the AccessAgent installer" on page 62.

Installing the Privileged Session Recorder client

On client workstations that you want to monitor, install the AccessAgent. The AccessAgent client includes the Privileged Session Recorder client components.

Before you begin

- Install the IBM Privileged Session Recorder Server.

- If necessary, obtain the Privileged Session Recorder Server certicates. See "Obtaining the Privileged Session Recorder Server certificates for the client computers" on page 61.

About this task

For more information about creating customized installation packages or to install the AccessAgent silently, see the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.

Procedure

1. Extract the AccessAgent installation package.
2. Start the AccessAgent client installer.

   For x86 operating systems
   Start the installer from the package name `aa-<version_number>\setup.exe`

   For x64 operating systems
   Start the installer from the package name with the `x64` suffix. For example: `aa-<version_number>_x64\setup.exe`
3. Click **Next**.
4. Follow the instructions in the installation wizard to complete the process.
5. Restart the computer.

Results

The AccessAgent client is installed.

When a recording is in progress, a Privileged Session Recorder notification is displayed in the Windows notification area.

Deploying the SSL certificates on the client computers manually without using the AccessAgent installer

To deploy SSL certificates for the Privileged Session Recorder Server on a computer that is installed with the AccessAgent, copy the CER files to `<aa_home>\SessionRecorder`.

Before you begin

Obtain the Privileged Session Recorder Server certificates.

Procedure

1. On the client computer, copy the CER files to `<aa_home>\SessionRecorder`.
   where
   <aa_home> is the AccessAgent installation location.
   For example: `C:\Program Files\IBM\ISAM ESSO\AA\`
2. Restart the computer.

Upgrade to IBM Security Privileged Identity Manager

You can upgrade to IBM Security Privileged Identity Manager from existing deployments of the component software.

You can upgrade from any of these existing deployments:

- IBM Tivoli Identity Manager, Version 5.0 or 5.1

  See "Upgrading IBM Tivoli Identity Manager, Version 5.1."
- IBM Security Access Manager for Enterprise Single Sign-On, Version 8.2 or earlier.

  See "Upgrading IBM Security Access Manager for Enterprise Single Sign-On" on page 64
- A deployment that consists of all of the following products:
  - IBM Tivoli Identity Manager, Version 5.1 or 5.0
  - IBM Security Access Manager for Enterprise Single Sign-On, Version 8.2 or earlier
  - IBM Tivoli Access Manager for Enterprise Single Sign-On Adapter, Version 5.1.

  See "Upgrading IBM Tivoli Identity Manager and IBM Security Access Manager for Enterprise Single Sign-On" on page 66.

Upgrade considerations

What is available by default after the upgrade:

- IBM Security Identity Manager provisioning and governance for users and managed resources.
- Bundled adapters to manage various types of LDAP servers and UNIX servers, such as AIX®, HP-UX, Linux, and Solaris.
- IBM Security Role and Policy Modeler and Role loaders.
- Automated check-out, check-in, and single sign-on for target resources that are accessed directly through the following applications:
  - PuTTY
  - RDP
  - IBM Personal Communications
  - VMware vSphere
- Separate reports for IBM Security Identity Manager shared access events and AccessAgent check-in, check-out, or single sign-on events.

Types of common customizations that might require more effort:

- Customization of default AccessProfiles to meet local needs. For example, support for different languages, differing prompts, different commands in a command prompt or shell.
- Development of new AccessProfiles for more IBM Security Privileged Identity Manager applications.
- Consolidation of audit logs from IBM Security Identity Manager, IBM Security Access Manager for Enterprise Single Sign-On, and target resources into Security Information and Event Management (SIEM) solutions.

Upgrading IBM Tivoli Identity Manager, Version 5.1

Upgrade IBM Tivoli Identity Manager to IBM Security Identity Manager.

In this scenario, you previously deployed IBM Tivoli Identity Manager, Version 5.1. Now, you want to upgrade to IBM Security Privileged Identity Manager.

- If your IBM Security Privileged Identity Manager deployment does not require automated checkout and checkin, your only task is to upgrade IBM Tivoli Identity Manager, Version 5.1 to IBM Security Identity Manager, Version 6.0.
- If your IBM Security Privileged Identity Manager deployment requires automated checkout and checkin, you must first upgrade IBM Tivoli Identity Manager, Version 5.1, and then do a new installation of the other IBM Security Privileged Identity Manager components:
  - IBM Security Access Manager for Enterprise Single Sign-On, Version 8.2.1
  - IBM Security Access Manager for Enterprise Single Sign-On Adapter, Version 6.0

For IBM Tivoli Identity Manager upgrade, you can complete either an in-place system upgrade or a separate system upgrade with data migration. Most deployments use a separate system upgrade with data migration.

The IBM Security Identity Manager installation wizard runs as part of the upgrade. When prompted by the wizard, be sure to select the **Shared Access Module**. Follow the instructions for your upgrade type in the *IBM Security Identity Manager Installation Guide* in the IBM Security Identity Manager Information Center:

- "IBM Security Identity Manager upgrade"
- "Separate system upgrade and data migration"

Note: In the separate system upgrade, you do not immediately replace the IBM Tivoli Identity Manager Server. Instead, you create a separate deployment of IBM Security Identity Manager and migrate data from the old IBM Tivoli Identity Manager Server to the new IBM Security Identity Manager Server.

Upgrading IBM Security Access Manager for Enterprise Single Sign-On

In this case, you previously installed IBM Security Access Manager for Enterprise Single Sign-On. Now, you want to deploy IBM Security Privileged Identity Manager.

- Install IBM Security Identity Manager, Version 6.0, with the shared access module.

  See "IBM Security Identity Manager, Version 6.0 installation" on page 53.
- Upgrade IBM Security Access Manager for Enterprise Single Sign-On.

Table 16. Upgrade matrix

If you have	Action for the IMS Server	Action for AccessAgent	Action for AccessStudio
IBM Security Access Manager for Enterprise Single Sign-On, Version 8.2 or earlier	Install IMS Server, Version 8.2.1. See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.	Install AccessAgent, Version 8.2.1. See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.	Install AccessStudio, Version 8.2.1. See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.

Table 16. Upgrade matrix (continued)

If you have	Action for the IMS Server	Action for AccessAgent	Action for AccessStudio
• IMS Server, Version 8.2.0 with or without fix packs or interim fixes • AccessAgent, Version 8.2.0 with or without fix packs or interim fixes • AccessStudio, Version 8.2.0 with or without fix packs or interim fixes	Upgrade to IMS Server,8.2.1. See "Upgrading the IMS Server from 8.2.0 to 8.2.1."	Upgrade to AccessAgent, Version 8.2.1. See "Upgrading AccessAgent from 8.2.0 to 8.2.1."	Install AccessStudio, Version 8.2.1. See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.

- Install IBM Security Access Manager for Enterprise Single Sign-On Adapter, Version 6.0.

  See "IBM Security Access Manager for Enterprise Single Sign-On Adapter, Version 6.0 installation" on page 54.

Upgrading the IMS Server from 8.2.0 to 8.2.1

If you installed IMS Server, Version 8.2.0, with or without fix packs or interim fixes, upgrade the IMS Server to Version 8.2.1 to support privileged identity management.

Before you begin

Ensure that the client computer meets the hardware and software prerequisites. See "Hardware and software requirements" on page 7.

See the IBM Security Access Manager for Enterprise Single Sign-On product documentation.

About this task

For more information, see the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.

Upgrading AccessAgent from 8.2.0 to 8.2.1

If you installed AccessAgent, Version 8.2.0, you can upgrade the AccessAgent to Version 8.2.1.

Before you begin

Ensure that the client computer meets the hardware and software prerequisites. See "Hardware and software requirements" on page 7.

See the IBM Security Access Manager for Enterprise Single Sign-On product documentation.

About this task

Before you deploy the AccessAgent in a production environment with many computers, you can install the AccessAgent client on one computer. Then, complete and verify the rest of the IBM Security Privileged Identity Manager configuration tasks. If the verification is successful, continue with the AccessAgent deployment.

When you install AccessAgent, deploy the IBM Security Identity Manager SSL certificates on each AccessAgent client computer.

If you are deploying the AccessAgent on multiple computers, use a *wrapping* installation package that installs the AccessAgent fix pack and the IBM Security Identity Manager certificates.

Procedure

1. Upgrade the AccessAgent client component.
2. Run the following command or use an installation script to import the IBM Security Identity Manager certificates on the computer where you installed the AccessAgent.

   x86 operating system

   rundll32.exe *aa_installpath*\AA\ECSS\PIMSlnHelper.dll,Believe *isim_ip_host*

   x64 operating system

   rundll32.exe *aa_installpath*\AA\ECSS\PIMSlnHelper64.dll,Believe *isim_ip_host*

   For example: **rundll32.exe** c:\Program Files\IBM\ISAM ESSO\AA\ECSS\PIMSlnHelper.dll,Believe *"192.0.2.2"*

Upgrading IBM Tivoli Identity Manager and IBM Security Access Manager for Enterprise Single Sign-On

Upgrade an existing deployment of Tivoli Identity Manager plus IBM Security Access Manager for Enterprise Single Sign-On to an IBM Security Privileged Identity Manager deployment.

In this scenario, you previously deployed all of the following products:

- IBM Tivoli Identity Manager, Version 5.1
- IBM Security Access Manager for Enterprise Single Sign-On, Version 8.2
- IBM Tivoli Access Manager for Enterprise Single Sign-On Adapter, Version 5.1

Now, you want to upgrade to use IBM Security Privileged Identity Manager. The tasks are:

1. Upgrade IBM Tivoli Identity Manager, Version 5.1, to IBM Security Identity Manager, Version 6.0, with the shared access module.

   Complete the instructions in "Upgrading IBM Tivoli Identity Manager, Version 5.1" on page 63.
2. Upgrade IBM Security Access Manager for Enterprise Single Sign-On, Version 8.2, to IBM Security Access Manager for Enterprise Single Sign-On, Version 8.2.1.
   - If IBM Security Access Manager for Enterprise Single Sign-On, Version 8.2, or earlier is installed, upgrade to version 8.2.1.

See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.

- If IBM Security Access Manager for Enterprise Single Sign-On, Version 8.2 is installed:
  - Upgrade to IMS Server, Version 8.2.1.

    See "Upgrading the IMS Server from 8.2.0 to 8.2.1" on page 65.
  - Upgrade to AccessAgent, Version 8.2.1.

    See "Upgrading AccessAgent from 8.2.0 to 8.2.1" on page 65.
  - Install AccessStudio, Version 8.2.1

    See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.

3. Upgrade IBM Tivoli Access Manager for Enterprise Single Sign-On Adapter, Version 5.1, to IBM Security Identity Manager, Version 6.0.

   Upgrade the adapter to IBM Security Access Manager for Enterprise Single Sign-On Adapter, Version 6.0. Follow the instructions in the *IBM Security Access Manager Enterprise Single Sign-On Adapter Installation and Configuration Guide*. See the following sections:

   - Before you begin the upgrade, determine whether you must migrate existing group shared accounts. See "Migrating Group Sharing Account to Privileged Identity Management".
   - If you must remove group shared accounts, see "Removing the Group Sharing Account feature".
   - "Upgrading the IBM Security Access Manager Enterprise Single Sign-On Adapter".

Chapter 5. Configuration for the software after installation

To finish setting up IBM Security Privileged Identity Manager you must complete the required configuration tasks.

For optional configuration tasks, see Appendix A, "Optional configuration tasks," on page 93.

IBM Security Access Manager for Enterprise Single Sign-On configuration

Before check-in and check-out automation can work, some tasks are required to configure the AccessProfiles, group policies, IBM Security Identity Manager authentication service, and user policy templates.

Uploading AccessProfiles to the IMS Server

To activate and use the AccessProfiles, upload the AccessProfiles to the IMS Server.

Before you begin

If you have multiple AccessProfiles, see "Multiple AccessProfiles for the same client application" on page 107 for a better understanding before you upload AccessProfiles to the IMS Server.

About this task

There are four AccessProfiles available for upload to the IMS Server.

You must upload the following AccessProfiles:

- `Use_Shared_Credentials_Authentication_Service.eas`
- `Concurrent_profiles_bgMonitor_Wnd_Explorer.eas`

Then, upload either of these AccessProfiles:

- `PIM_Profiles_With_General_RDP_Flow.eas`

  This AccessProfile contains both privileged identity management workflows and non-privileged identity management workflows.

  Use this AccessProfile if the non-privileged identity management workflows for RDP are required for non-privileged identity management users.

  The non-privileged identity management workflows are provided in the IBM Security Access Manager for Enterprise Single Sign-On bundled AccessProfiles. The non-privileged identity management workflows that are included in this AccessProfile might be outdated. See the AccessProfiles Library for the latest version.

  Note:

  – This AccessProfile is just an example of a merged AccessProfile.

  – If the non-privileged identity management workflows included in this AccessProfile is outdated, download the latest version of the AccessProfile from the AccessProfiles Library. After you download the latest version, merge

it with the RDP AccessProfile for the privileged identity management workflow. The RDP Profile ID is `profile_RDP_main`.

- `PIM_Profiles.eas`

  This AccessProfile contains the privileged identity management workflows only.

  Use this AccessProfile if you want to use the privileged identity management workflows only.

You can get these AccessProfiles from the AccessProfiles Library.

If you cannot find or download these AccessProfiles from the AccessProfiles Library, you can get the files from this location:

<IMS Server installation folder>`\com.ibm.tamesso.ims-delhi.build.boot\src\config\data\config\pim\Profiles`.

For example: `C:\Program Files\IBM\ISAM ESSO\IMS Server\com.ibm.tamesso.ims-delhi.build.boot\src\config\data\config\pim\Profiles`.

Procedure

1. Open the command prompt.
2. Browse to *<IMS Server installation folder>*`\bin`.
3. Run the following command:

   uploadSync.bat *<was_admin>* *<was_admin_password>* --dataFile "*<accessprofile_absolute_path>*".

   For example:

   ```
   C:\Program Files\IBM\ISAM ESSO\IMS Server\bin>uploadSync.bat wasadmin
   p@ssw0rd --dataFile "C:\Program Files\IBM\ISAM ESSO\IMS
   Server\com.ibm.tamesso.ims-delhi.build.boot\src\config\data\config\pim\
   Profiles\Concurrent_profiles_bgMonitor_Wnd_Explorer.eas"
   ```

Related information:

AccessProfiles Library

Creating a user policy template only for privileged identity management users

Configure a user policy template in AccessAdmin to segregate privileged identity management and non-privileged identity management users. After segregation, you can configure prompts that display for selected groups of users and hide the prompt from the rest of the users. If there is no segregation, the dialog box prompt displays for every user when the privileged identity management client applications are used.

Before you begin

See “Configuring the shared access credential usage prompt” on page 78.

Procedure

1. Log on to AccessAdmin.
2. Create or modify an existing user policy template for privileged identity management users.
   a. Under **User Policy Templates**, click **New template**.
   b. Type a name for the template. For example: `PIM admins only`.

c. Expand the **Authentication Service Policies** group.
d. Expand **Use Shared Credentials**.
e. For **Password entry of injection policy per authentication service**, choose **Ask**.
f. Click **Update**.
g. Apply the user policy template to privileged identity management users. See the topic "Applying a User Policy Template" in the IBM Security Access Manager for Enterprise Single Sign-On product documentation.

3. Create or modify an existing user policy template for non-privileged identity management users. For example: `Non-PIM users only`.
   a. For the policy template, expand **Authentication Service Policies**.
   b. Expand **Use Shared Credentials**.
   c. For **Password entry of injection policy per authentication service**, choose **Never**.
   d. Click **Update**.
   e. Apply the user policy template to users that are not using privileged identity management. See the topic "Applying a User Policy Template" in the IBM Security Access Manager for Enterprise Single Sign-On product documentation.

Mapping the authentication service

Define an IBM Security Identity Manager authentication service. The credentials that are stored against the authentication service in the users Wallet are authenticated with IBM Security Identity Manager during check-out and check-in.

Before you begin

If you did not already do so:

- Obtain details about the authentication service ID that are required for this configuration.
  1. Log on to the IMS Configuration Utility.
  2. From the **Basic Settings** menu, select **Authentication Services**. A list of available authentication services is displayed.
  3. Select the appropriate authentication service to view the authentication service ID and the account data template.

About this task

For more information about authentication services, see the topic "Managing authentication services" in the *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide*.

You can choose to create an authentication service or use an existing authentication service. To create an authentication service, see the topic "Creating authentication services" in the *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide*.

If the IBM Security Access Manager for Enterprise Single Sign-On adapter is used then map the provisioned IBM Security Identity Manager credentials with the IBM Security Identity Manager authentication service as defined in the IBM Security Privileged Identity Manager configuration policy.

Procedure

1. Log on to AccessAdmin. For example: `https://ims_hostname:ihs_ssl_port/admin`
2. In the **System** group, click **System policies**.
3. In the **System policies** page, expand **IBM Security Privileged Identity Manager Configuration Policies**.
4. Specify the following values:

   IBM Security Identity Manager URL
   Specify the IBM Security Identity Manager URL. For example: `https://isim_host:port/itim/services/WSSharedAccessService`

   IBM Security Identity Manager Authentication Service ID
   Specify the configured IBM Security Identity Manager authentication service ID. For example: `pim_auth_service`.
5. Click **Update**.

Configuring a Windows Group Policy to prompt the client for passwords (RDP)

If you use a Remote Desktop Connection client for privileged access to a Windows host, configure the RDP policy to prompt for, not store, passwords.

Before you begin

You must have Administrator privileges to configure the Windows Group Policy.

About this task

The procedure that is documented here is an example only. For more information about configuring a Group Policy for the RDP client in Windows, go to the Microsoft website at http://www.microsoft.com. Search for `RDP Always prompt client for password upon connection`.

Procedure

1. Log on as an Administrator.
2. Start the Group Policy Editor tool.
   a. Click **Start** > **Run**.
   b. Type `gpedit.msc`.
   c. Press Enter.
3. Browse for the policy:

   Windows XP:
   Click **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Terminal Services** > **Encryption and Security** > **Always prompt client for password upon connection**.

   Windows 7:
   Click **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Connection Client** > **Do not allow passwords to be saved**.
4. From the **Action** menu, click **Edit**.
5. Choose **Enabled**.
6. Click **OK**.

Verifying the installation and configuration

Verify whether you successfully installed and configured the IMS Server and AccessAgent to support privileged identity management.

Before you begin

Ensure:

- The required components are installed and configured.
- The Privileged Identity Management AccessProfiles are uploaded in the IMS Server. See "Uploading AccessProfiles to the IMS Server" on page 69.

About this task

Before deploying AccessAgent to actual users for check-out and check-in automation, validate all the server configurations by using a single installation of AccessAgent.

Procedure

1. Start the managed resource client application.
2. Test the credential check-out and check-in automation. See the following scenarios:
   - "Logging on with PuTTY" on page 80
   - "Logging on with the Microsoft Remote Desktop Connection (RDP) client" on page 81
   - "Logging on with IBM Personal Communications" on page 82
   - "Logging on with the VMware vSphere Client" on page 83
3. Ensure that the privileged identity management scenarios work according to your requirements. If the test fails, see Chapter 7, "Troubleshooting," on page 85.

Shared access configuration

You can complete configuration tasks for shared access as needed for your deployment.

Table 17 describes configuration tasks that you might want to complete, depending on the requirements of your deployment.

Table 17. Shared access configuration tasks

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

Table 17. Shared access configuration tasks (continued)

Configuration task	Description
Shared access approval and recertification	You can add an approval process to the default operation for adding credentials to the vault. You can also define a custom workflow to recertify credentials in the vault.
Customizing the checkout form	You can customize the form that is used for checkout of shared accounts. You can add more attributes to be filled out during checkout. This customization increases individual accountability when credentials are shared.
Shared access Tivoli Common Reporting reports	You can configure reports that show: • Shared access audit history • Shared access entitlements for a specified owner • Shared access entitlements for a specified role.

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

- Shared access documentation

  In the IBM Security Identity Manager documentation, see the "System configuration" section to find links to the documentation for shared access configuration tasks.
- IBM Security Identity Manager documentation

  To find information about a task in Table 17 on page 73, go to this documentation. On the home page, locate the documentation search field, and enter the configuration task name as shown in the "Configuration task" column of the table. For example, to use an external credential vault server, enter "Configuring an external credential vault server".

Session recording configuration

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

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

Table 18. Session recording configuration tasks

Configuration task	Description
Required: Specifying the target IBM Privileged Session Recorder Server URL.	Specifies the URL of the target IBM Privileged Session Recorder Server in the following AccessAdmin system policy, **pid_recorder_server**: **Privileged Session Recorder Server URL** For example: `https://<psrhost>/recorder/collector` For more information, see the IBM Security Access Manager for Enterprise Single Sign-On product documentation and search for `pid_recorder_server`.

Table 18. Session recording configuration tasks (continued)

Configuration task	Description
Configuring additional IMS Server policies for session recording	Configures options for Privileged Session Recorder behavior. For example: • Modify the color depth of recordings. • Specify the keys to exclude or include from recordings. See the IBM Security Access Manager for Enterprise Single Sign-On product documentation and search for `policies for privileged identity management`.
Configuring members of the session recording Security Auditor roles	Configures the users for the session recording Security Auditor roles. See the *IBM Security Privileged Identity Manager Administrator Guide*.
Modifying AccessProfiles for session recording	Configures AccessProfiles with Privileged Session Recorder widgets to add session recording support to custom applications. See "Modifying AccessProfiles" in the *IBM Security Privileged Identity Manager Administrator Guide*.
Configuring IBM Privileged Session Recorder Tivoli Common Reporting reports	You can configure Tivoli Common Reporting to show the IBM Privileged Session Recorder report. See "IBM Tivoli Common Reporting configuration or administration" on page 103.

Chapter 6. Automating the credential check-out and check-in process

You can automate the check-out and check-in of shared access credentials from the IBM Security Identity Manager Server for convenience.

In some cases, you must customize the AccessProfiles that automates the check-out and check-in process. Learn when to customize the AccessProfiles.

Automation overview

A sequence of steps takes place when user initiates check-out and check-in. Learn the details of these associated processes.

Shared access credential check-out process

In a privileged identity management workflow, you can check out shared access credentials for a managed resource automatically.

You can log on to a managed resource with a shared access credential without knowing the shared access credential.

1. Choose the supported application for the managed resource. For example: PuTTY.

   See “Prerequisite software requirements” on page 7.
2. Specify the target managed resource.
3. When prompted, log on with shared credentials.

   Note: You can also choose not to log on to a managed resource with a shared access credential. See “Configuring the shared access credential usage prompt” on page 78.
4. When prompted with the AccessAgent reauthentication prompt, specify your IBM Security Access Manager for Enterprise Single Sign-On password. See “Configuring the reauthentication prompt” on page 78.

   IBM Security Access Manager for Enterprise Single Sign-On authenticates and retrieves your credentials from your single sign-on Wallet.
   - If your Wallet contains valid IBM Security Identity Manager credentials, IBM Security Access Manager for Enterprise Single Sign-On retrieves the list of credential pools from the IBM Security Identity Manager Server.
   - If your Wallet does not contain any IBM Security Identity Manager credentials, you are prompted to provide them.
5. When prompted, choose a credential pool to check out shared access credentials.

   After you choose the credential pool, IBM Security Privileged Identity Manager:
   a. Checks out the shared access credential from the IBM Security Identity Manager.
   b. Enters the shared access credential into the client application.

   You are logged on to the managed resource with a shared access credential. When you check out a credential through the automated check-out process, there is no option to enter the check-out justification comment.

6. If session recording is enabled, when prompted, provide your consent for session recording to begin.

   After you provide your consent, the IBM Security Privileged Identity Manager Privileged Session Recorder starts recording.

Configuring the shared access credential usage prompt

Use an injection policy to configure the prompt that asks the user whether to use shared credentials. The prompt is displayed when you log on to a managed resource, when you use any of the client applications.

Procedure

1. Open the Wallet Manager.
2. On the **Authentication Service** column, search for **Use shared credentials** and select any of the **Password Entry** options.

Table 19. Password entry options

Password entry	Description
Automatic logon	Use only shared credentials to log on to the managed resources.
Always	• Always asks the user to use shared credentials to log on or not. • Always use the selected IBM Security Identity Manager user.
Ask	• Asks the user to use shared credentials to log on or not. • Asks for the IBM Security Identity Manager user.
Never	Do not use shared credentials to log on to the managed resources.

Configuring the reauthentication prompt

For more security, IBM Security Access Manager for Enterprise Single Sign-On users can be asked to reauthenticate when they access managed resources. Configure whether to require the users to reauthenticate every time that a user accesses a client application or command that requires shared credentials.

Procedure

1. Start the **AccessAdmin**.
2. Click **Authentication service policies**.
3. Select the authentication service **Use Shared Credentials**.
4. Under **Password Policies**, specify whether to require reauthentication before you single sign-on by using the automatic sign-on mode.

Shared access credential check-in process

The software automatically checks in shared access credentials when you log out, exit, or close the client application.

If the credential check-in process is not triggered automatically, the credential remains checked out to the user until the lease time expires. You can check out a shared access credential only for a limited amount of time. The specific amount of

time is the *lease time*. See the IBM Security Identity Manager Information Center for more information about shared access credential lease.

IBM Security Identity Manager password change process

If there is a change in the IBM Security Identity Manager password, the IBM Security Access Manager for Enterprise Single Sign-On adapter automatically captures the password change.

To ensure that any password changes that you initiate for IBM Security Identity Manager is applied successfully for IBM Security Identity Manager, install the IBM Security Access Manager for Enterprise Single Sign-On adapter for IBM Security Identity Manager.

For more information, see the *IBM Security Access Manager for Enterprise Single Sign-On Adapter Installation and Configuration Guide*.

More examples that can trigger check-out and check-in automation

Different events can determine the automation behavior. For example, when you start multiple sessions or when sessions are ended abnormally.

Table 20. More events that can trigger automated check-out or check-in behavior.

When	Automated check-out or check-in behavior
You • Start a second client application session. • Connect to the same resource as your client application session. • Choose the same credential pool. The user is prompted whether to use an already checked out credential. The user can choose to reuse or check out a new credential. **Note:** If you choose a different credential pool, a separate check-out occurs.	No check-out is necessary. Check-out does not affect initial client application session credentials. AccessAgent reuses the checked out credential from the previous session.
• You use a client application. • A session is ended abnormally because of a system crash or deliberate termination.	AccessAgent checks in credentials that were used for the abnormally terminated application.
There is no connection to the IBM Security Identity Manager Server.	After the client application closes properly or ends, AccessAgent continuously attempts to check in all credentials that a user checked out. This process prevents any checked out credentials from being used outside the IBM Security Access Manager for Enterprise Single Sign-On domain.
You restart a client computer, and there are still credentials that are pending for check-in.	AccessAgent tries the check-in again when a corresponding user logs on to IBM Security Access Manager for Enterprise Single Sign-On. This approach avoids locking credentials so that they can be checked out by users.

Table 20. More events that can trigger automated check-out or check-in behavior. (continued)

When	Automated check-out or check-in behavior
You use the managed resource by using a checked out credential, from the client logon application, and after the lease expires on the checked out credential. For example: • You are finished with using the client logon application and the managed resource but forget to close the client logon application. • You are away from the computer for a long time.	AccessAgent checks in credentials when the IBM Security Identity Manager Administrator configured lease time expires. **Note:** One hour before the lease time expiration, a notification informs you when the lease time is almost expiring. You must stop the use of the credentials or have AccessAgent close the application when the lease expires. If you do not respond to the notification, the application is closed. See the IBM Security Identity Manager Information Center for more information about lease expiry configurations.
You use the managed resource by using a checked out credential, from the client logon application, and after the lease expires on the checked out credential. For example: The computer goes into hibernate mode, and the credential is not checked in.	IBM Security Identity Manager handles lease expiry that is based on how lease expiry handling is configured. For example: • The credentials can be checked in or • Notification emails can be sent out. See the IBM Security Identity Manager Information Center for more information.

Automatic check out and check in with client application logon

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

With single sign-on automation

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

Without single sign-on automation

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

Logging on with PuTTY

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

Before you begin

- Configure the managed resource that you are going to access from PuTTY for shared access.

- Upload the Privileged Identity Management AccessProfile for PuTTY to the IMS Server. See "Uploading AccessProfiles to the IMS Server" on page 69.
- Ensure that there are IBM Security Identity Manager credentials in the Wallet.

About this task

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

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

Procedure

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

Results

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

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

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

Before you begin

- Configure the managed resource that you are going to access from the RDP client for shared access.
- Upload the AccessProfile for the Microsoft Remote Desktop Connection RDP client to the IMS Server. See "Uploading AccessProfiles to the IMS Server" on page 69.
- Configure a group policy to always prompt RDP clients for a password before making a connection. See "Configuring a Windows Group Policy to prompt the client for passwords (RDP)" on page 72.

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

Procedure

1. Start the Microsoft Remote Desktop Connection client by clicking **Start** > **All Programs** > **Accessories** > **Remote Desktop Connection**.
2. Specify the target host name or IP address.
3. Click **Connect**.

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

Results

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

Logging on with IBM Personal Communications

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

Before you begin

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

About this task

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

Customization is necessary because:

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

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

Procedure

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

   Note: The window title of IBM Personal Communications must match the session name.
3. Select the application.
4. When prompted to log on with shared access credentials, choose **Yes**.
5. When prompted with the Shared Access Selection window, select one of the credential pools.
6. When prompted to provide consent to be recorded, choose **Yes**. Session recording is started.

Results

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

Logging on with the VMware vSphere Client

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

Before you begin

- Configure the managed resource for shared access.
- Upload the shared access AccessProfile for VMware vSphere Client to the IMS Server. See "Uploading AccessProfiles to the IMS Server" on page 69.

Procedure

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

   If you successfully checked out the shared access credentials, the credentials are injected into the VMware vSphere logon prompt. If the check-out failed, there are no credentials injected.
3. Click **Login**.
4. When prompted to log on with shared access credentials, choose **Yes**.
5. When AccessAgent prompts for reauthentication, enter the AccessAgent credentials.
6. When prompted with the Shared Access Selection window, select one of the credential pools.
7. When prompted to provide consent to be recorded, choose **Yes**. Session recording is started.

Results

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

Manual check-out

For workflows and applications that are not supported by the bundled privileged identity management AccessProfiles, you can check out the credentials manually. You can check out credentials manually through the IBM Security Identity Manager self-service user interface.

The privileged identity management authentication service policy configuration in the IMS Configuration Utility determines whether a prompt is displayed for an IBM Security Identity Manager managed resource.

For supported client applications, if you do not want AccessAgent to check out and inject credentials automatically, select **No**. See "Shared access credential check-out process" on page 77.

Session recording is not triggered with manual checkout.

Chapter 7. Troubleshooting

You can diagnose and troubleshoot errors that occur during the IBM Security Privileged Identity Manager installation.

Troubleshooting IBM Security Identity Manager Server connectivity and availability

A network connection problem or an unconfigured managed resource are common installation problems.

Problems

The IBM Security Identity Manager Server is not available or cannot be contacted.

Causes

Some possible causes:

- The network connection is disconnected.
- The managed resource is not configured for shared access.

Solutions

- Check the network connection.
- If you are the Administrator, ensure that the IBM Security Identity Manager Server is started.
- Ensure that the managed resource is already configured for shared access.
- Check out the credentials manually from the IBM Security Identity Manager Server and choose not to log on with shared credentials. Specify the logon credentials manually.

Troubleshooting uploads to the Privileged Session Recorder Server

If the Privileged Session Recorder Server is unavailable, the IBM Security Privileged Identity Manager Session Recorder service on the client computer stores the session recordings. The service resumes uploads of the recordings when the server is available.

Problems

The Privileged Session Recorder Server is not available or cannot be contacted.

The monitored client application either is not responding to mouse or keyboard input or the window is no longer moveable.

Session recordings from client computers are not available on the Privileged Session Recorder Server.

Causes

Some possible causes:

- The network connection is disconnected.

- The Privileged Session Recorder Server is not configured.
- The Privileged Session Recorder Server is not available.
- The Privileged Session Recorder Server host name cannot be resolved.
- The Privileged Session Recorder Server certificate has not been trusted.

To determine causes, see the message logs. For more information about the types of problems and possible solutions, see "Troubleshooting and diagnosing problems with logs" on page 87.

Solutions

- Check the network connection and attempt to restore the connection on the Privileged Session Recorder Server.
- If you are the Administrator, ensure that the Privileged Session Recorder Server is started.
- Ensure that the session recording host name and port number is configured correctly and the host can be resolved by client workstations.
- Review the session recording policies to configure the action to take on the client computer when the Privileged Session Recorder Server is not available.

Troubleshooting the audit log

Find solutions to audit log problems.

Table 21. Troubleshooting audit log problems and solutions.

Problem	Solution
Event number mismatch.	Update the AccessProfile custom audit log action if you are defining custom audit codes.
The event code changes are not reflected on the client.	Synchronize the AccessAgent computer with the IMS Server.

Troubleshooting checklist

Find possible solutions to common problems.

Table 22. Lists some of the common problems and possible solutions.

Problem	Solutions
When the IBM Security Identity Manager Server is not available.	• Check the network connection. • Ensure that the managed resource is configured for shared access.
The managed resource is not configured for shared access for IBM Security Identity Manager.	• Configure the managed resource for shared access with IBM Security Identity Manager. • Avoid logging with shared access credentials.
All the available shared access credentials are checked out.	• Wait for a few minutes until there are available shared credentials. • Find out the identity of checked out credentials from the IBM Security Identity Manager. Ask the credential owner to check in their credentials.

Table 22. Lists some of the common problems and possible solutions. (continued)

Problem	Solutions
There are no IBM Security Identity Manager Server credentials in the Wallet.	Follow the instructions on the screen to enter the credentials. The credentials must have privileges to check out shared access credentials.
The account that is used to log on to the managed resource does not have correct entitlements on IBM Security Identity Manager.	Use IBM Security Identity Manager to ensure that the account used to log on has correct permissions for the available shared access accounts.
Client application is not responding to keyboard or mouse input. For example: you cannot resize or move the window for the client application.	Verify that the Session Recorder service is: • Started on the client workstation. • Accessible from the client. The behaviour of the client application is determined by the privileged identity management policies in AccessAdmin.
Client application is closed unexpectedly.	• Verify that the Session Recorder service on the client workstation is started. • Verify that the Privileged Session Recorder Server is running and reachable from the client. The behaviour of the client application is determined by the privileged identity management policies in AccessAdmin.
IBM Security Access Manager for Enterprise Single Sign-On ends the active process but does not check in the shared access credential when the following conditions occur: • A shared access credential is checked out from IBM Security Identity Manager through IBM Security Access Manager for Enterprise Single Sign-On. • The credential is used by the user until the lease expires. Since the credential is not checked in, users cannot use the shared access credential unlessIBM Security Identity Manager is configured to check the credential back in.	If you want users use the shared access credential again, take the following steps: 1. Open the **IBM Security Identity Manager Console**. 2. Click **Manage Shared Access** > **Configure Credential Default Settings**. 3. Select **Notify violation and check in**.

Troubleshooting and diagnosing problems with logs

The following logs capture information about the processing and recording activities. You can use the log files that are generated to troubleshoot or diagnose potential deployment or configuration problems.

Privileged Session Recorder Client log (Recorder.log)

The IBM Privileged Session Recorder Client stores log messages in the `Recorder.log` file in `<aa_home>\logs` on the client computer. For example: `C:\Program Files\IBM\ISAM ESSO\AA\logs`.

The log level is determined by the **LogLevel** value on the client computer.

To configure the log level on the client computer, start the Registry Editor. Browse to the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\DeploymentOptions
```

Locate the `LogLevel` value.

Note: Increasing the log level can reduce computer performance. Reduce the log level after troubleshooting is complete.

For more information about configuring log levels on the client computer, see the IBM Security Access Manager for Enterprise Single Sign-On product documentation and search for `pid_log_level`.

SSL related messages are specified in the following format:

```
[SSL] <error-description>
```

Table 23. Known error descriptions for SSL messages in the Recorder.log file.

Error description: <error-description>	Required Log Level	Known causes or solutions
`The CA issuing the server certificate is not trusted.`	2	Ensure that the client computer trusts the signer of the SSL certificate. For more information, see the following topics: • "Obtaining the Privileged Session Recorder Server certificates for the client computers" on page 61. • "Deploying the SSL certificates on the client computers manually without using the AccessAgent installer" on page 62.
`Server certificate has invalid common name (host name field).`	2	Ensure that the host name part of the IBM Privileged Session Recorder Server URL is the same with the Common Name (Subject). For example, if the server certificates are issued to the `psr.example.com`, set the IBM Privileged Session Recorder Server URL to `https://psr.example.com/recorder/collector`. Ensure that the IBM Privileged Session Recorder Server host name can be resolved.

WinHTTP event log messages are specified in the following format:

```
[WinHTTP]<method-name> failed, err=<error-code>,desc=<error-description>
```

Table 24. Known error descriptions for WinHTTP messages in the Recorder.log file.

Error description: <error-description>	Required Log Level	Known causes or solutions
`The operation timed out.`	2	Open the **Registry Editor**, and add the following optional HTTP timeout registry entries in `HKEY_LOCAL_MACHINE\Software\IBM\SessionRecorder`. These registry values are DWORD values and specified in milliseconds. **`ResolveTimeout`** Timeout for resolving host name. (default: 5000 = 5 sec) **`ConnectTimeout`** Timeout for making connection to the server. (default: 5000 = 5 sec) **`SendTimeout`** Timeout for sending data, for example, one screen capture to the server. (default: 60000 = 1 min) **`ReceiveTimeout`** Timeout for receiving response from the server. There is no large data to download from the Privileged Session Recorder Server. (default: 10000 = 10 sec)
`The server name or address could not be resolved.`	2	Verify that there is a DNS entry for the host name or add the name to the hosts file.
`A security error occurred.`	2	See troubleshooting causes or solutions for SSL type log events.

HTTP-Status related messages are specified in the following format:

`[HTTP-Status] Status Code: <http-status-code>, Internal: <internal-status-code>`

Table 25. Known causes for http-status codes in the Recorder.log file.

HTTP status codes: <http-status-code>	Required Log Level	Known causes or solutions
`500`	2	Internal server error. • Verify that WebSphere Application Server profile is running and the **`ISPIMRecorder`** application is started. • Try restarting the WebSphere Application Server profile. • Look for exceptions in the server logs.
`404`	2	Page not found. • Ensure that the Privileged Session Recorder Server URL is in the following format: `https://<recorder_hostname>/recorder/collector`. • Verify that WebSphere Application Server profile is running and the **`ISPIMRecorder`** application is started. For more information, see the IBM Security Privileged Identity Manager product documentation and search for `pid_recorder_server`.
`401`	3	Unauthorized. If this message occurs every 30 minutes, this event indicates that the Privileged Session Recorder Server is authenticating with the Privileged Session Recorder Client. If this series of messages are accompanied by the following log message: `WARNING: This is attempt <number> for authorization.` Ensure that session affinity is configured properly.

Privileged Session Recorder Server logs (SystemOut.log)

The Privileged Session Recorder Server stores message logs in the WebSphere Application Server Java virtual machine (JVM) `SystemOut.log` file. For example: `<was_profile_home>\logs\<server_name>`.

Privileged Session Recorder Server configuration utility logs

The Privileged Session Recorder Server configuration utility stores message logs in `<recorder_install_home>\configtool\logs`.

IBM Security Identity Manager logs

For more information about the various log locations for IBM Security Identity Manager, see the IBM Security Identity Manager product documentation and search for `log files`.

IBM Security Access Manager for Enterprise Single Sign-On logs

For more information about the various log locations for IBM Security Access Manager for Enterprise Single Sign-On, see the IBM Security Access Manager for Enterprise Single Sign-On product documentation and search for `troubleshooting logs`.

Troubleshooting shared access

The IBM Security Identity Manager documentation provides more information about troubleshooting issues with shared access.

To troubleshoot the shared access module, see:

- "Fixing data replication errors for invalid object names" in the *IBM Security Identity Manager Installation Guide.*

  You might see a data replication error during installation, if you:

  – Run **DBConfig** to drop all database tables.

  – Do not run **SAConfig** to repopulate the tables that are specific to the shared access module.

  Complete the steps in the topic to reconfigure the shared access module.
- "Troubleshooting shared access module problems" in the *IBM Security Identity Manager Troubleshooting Guide*.

  Learn how to fix configuration problems that can prevent a credential from displaying in the Self Service user interface. It also describes how to reconfigure the shared access module when LDAP is configured.

Troubleshooting IBM Privileged Session Recorder console display issues on Microsoft Internet Explorer 9 and 10

The IBM Privileged Session Recorder console might not display correctly when you view the console in Microsoft Internet Explorer 9 and 10 with Compatibility View mode turned on.

Problem

The IBM Privileged Session Recorder console does not display correctly when viewed in Microsoft Internet Explorer 9 and 10.

Solution

Disable the Microsoft Internet Explorer Compatibility View mode for the IBM Privileged Session Recorder console web page. For more information, go to the Microsoft website at www.microsoft.com and search for `turn off Compatibility View Internet Explorer`.

Appendix A. Optional configuration tasks

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

Increasing the root CA key size for WebSphere Application Server 7.0 (stand-alone)

Change the root CA key size to a larger 2048 bit key size to offer an increased level of security. This task is optional. This task is not required if the profile is created after applying WebSphere Application Server,Version 7.0 Fix Pack 23.

Before you begin

- Check that your host names are resolving correctly.
- Ensure that the WebSphere Application Server is started.

About this task

This optional task applies only to new installations. If you choose to change your root CA key size to 2048 bit, complete these steps right after you create a WebSphere Application Server profile. The root CA certificate signs the default certificates in the keystore. The certificates secure internal WebSphere Application Server communications.

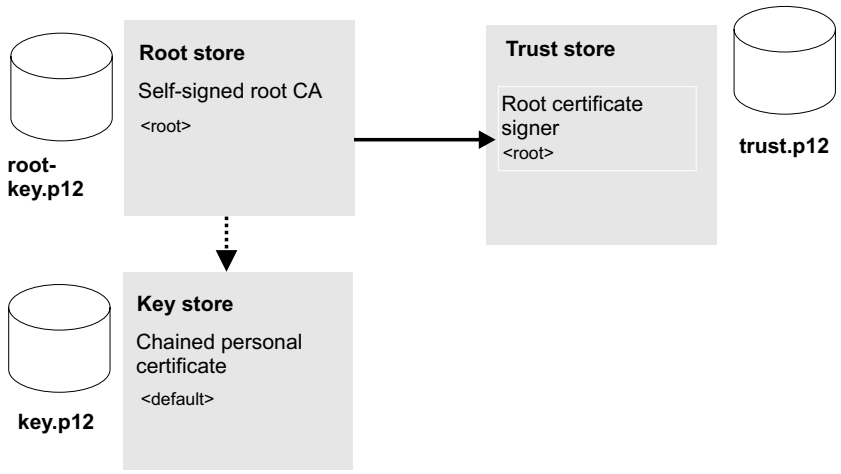

Figure 4. Replacing the root CA and key signers for WebSphere Application Server in the truststore with a new key size.

The process involves the following steps:

1. Create a 2048 bit self-signed root CA in the root store, replace the existing version, and extract it. See step 1 on page 94 to step 8 on page 95.
2. Create a 2048 bit chained personal certificate in the keystore, and replace the existing version. See step 10 on page 95.
3. Export the personal certificate to the truststore. See step 11 on page 96.

4. Use the **ikeyman** utility to add the root CA to the truststore. See step 12 on page 96.

Procedure

1. Select **Start** > **All Programs** > **IBM WebSphere** > **Application Server** **<*version*>** > **Profiles** > **<*profile name*>** > **Administrative console**.
2. Log on to the IBM Integrated Solutions Console.
3. On the Integrated Solutions Console navigation pane, select **Security** > **SSL certificate and key management**.
4. In **Related items**, click **Key stores and certificates**.
5. Create a temporary self-signed root CA in the default root store.

   The temporary root certificate is used to replace the older `root` certificate. The temporary root certificate is then replaced with a new 2048 bit root certificate.

   a. From the **Keystore usages** list, select **Root certificates keystore**.
   b. Click **NodeDefaultRootStore**.
   c. Under **Additional Properties**, click **Personal certificates**.
   d. Click **Create** > **Self-signed Certificate**.
   e. In **Alias**, enter a new alias name. For example: `root2`.
   f. In the **Common name** field, enter the fully qualified domain name of the computer where the WebSphere Application Server is installed. For example: `ibm-svr1.example.com`.
   g. Click **OK**.
   h. Click **Save**.
6. Replace the old root CA with the new root CA: `root2`. Replace the old `root` with the temporary `root2`.

   a. In the **Personal Certificates** page, select the check box for the older root certificate, `root`.
   b. Click **Replace**.
   c. From the **Replace with** list, choose the alias of the certificate you created.
   d. Select **Delete old certificate after replacement**.

      See the WebSphere Application Server, Version 7.0 product documentation on replacing a certificate for details:

      http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/tsec_sslreplaceselfsigncert.html
   e. Ensure that the **Delete old signer** check box is not selected.
   f. Click **OK**.
   g. Click **Save** to apply the changes to the master configuration.
7. Create the 2048 bit root CA. This root certificate is the 2048 bit certificate that you retain.

   a. Click **Create** > **Self-signed Certificate**.
   b. In **Alias**, enter `root`.

      Important: You must specify the alias name as `root` for this 2048 bit certificate.
   c. From the **Key size** list, select **2048**.
   d. In the **Common name** field, enter the fully qualified domain name of the computer where the WebSphere Application Server is installed. For example: `ibm-svr1.example.com`.

e. In the **Validity period** field, enter the validity period of the certificate. For example: A root certificate is typically used for `7300` days, which is approximately 20 years.
f. Optional: Complete the certificate with optional identification details.
g. Click **OK**.
h. Click **Save** to apply the changes to the master configuration.

8. Replace the temporary root certificate with the new 2048 bit root certificate that you retain.
   a. In the **Personal Certificates** page, select the check box for the temporary root certificate, `root2`.
   b. Click **Replace**.
   c. From the **Replace with** list, choose the new 2048 root certificate you created, `root`.
   d. Select **Delete old certificate after replacement**.
   e. Ensure that the **Delete old signer** check box is not selected.

      Important: Ensure that the **Delete old signer** check box is not selected.
   f. Click **OK**.
   g. Click **Save** to apply the changes to the master configuration.

   You successfully replaced the original 1024 bit root certificate with a new 2048 bit root certificate.
9. Extract the new root CA to a file.
   a. In the **Personal Certificates** page, select **Root**.
   b. Click **Extract**.
   c. In **Certificate file name**, enter the fully qualified path to the certificate to be extracted. For example: `C:\root2048.cer`.
   d. Click **OK**.
10. Create a chained personal certificate in the keystore.

    Important: Before you begin, be sure to check that your host names are resolving correctly.
    a. In the **Key stores and certificates** page, open the keystore.
    b. Click **NodeDefaultKeyStore**.
    c. In **Additional Properties**, click **Personal certificates**.
    d. Click **Create** > **Chained certificate** to create a personal certificate that replaces the old personal certificate.
    e. In the **Alias** field, enter a new alias name. For example: `default2`.
    f. In the **Root certificate used to sign the certificate** field, select the alias of the newly created Root CA.
    g. In the **Key size** field, select **2048**.
    h. In the **Common name** field, enter the fully qualified domain name of the computer where the WebSphere Application Server is installed. For example: `ibm-svr1.example.com`
    i. In the **Validity period** field, enter the validity period of the certificate. For example: `365` days.
    j. In the **Organization** field, enter the organization portion of the distinguished name.

Note: It is important that you specify the organization portion of the distinguished name.

k. In the **Country or Region** field, enter the country portion of the distinguished name.

Note: It is important that you specify the country portion of the distinguished name.

l. Optional: Enter information in the rest of the optional fields.

m. Click **OK**.

n. Click **Save** to apply the changes to the master configuration.

o. Replace the old default personal certificate with the new one.

1) In the **Personal Certificates** page, select the **default** check box.

2) Click **Replace**.

3) From the **Replace with** list, choose the alias of the certificate you created. For example: `default2`.

4) Select **Delete old certificate after replacement**.

Important: Be sure that the **Delete old signers** check box is not selected.

5) Click **OK**.

6) Click **Save** to apply changes to the master configuration.

Note: If the web browser alerts you that a certificate is revoked and a new certificate is available, click **Yes** to proceed.

11. Export the personal certificate to the keystore: `<was_home>\profiles\<profile_name>\etc\key.p12`.

a. In the **Personal Certificates** page, select the personal certificate check box. For example: `default2`.

b. Click **Export**.

c. In **Key store password**, enter the key store password For example: `WebAS`.

Note: The default key store password is documented in the WebSphere Application Server information center.

d. Select **Key store file**.

e. In **Key store file**, specify the key store location. For example: `<was_home>\profiles\<profile_name>\etc\key.p12`.

f. For **Type**, verify that the default **PKCS12** is selected.

g. In **Key file password**, type the password. For example: `WebAS`.

h. Click **OK**.

You successfully exported the personal certificate and private key to a keystore.

12. Use the IBM Key Management utility, `ikeyman`, to add the extracted root CA to the truststore.

a. Start the **`ikeyman`** utility. Locate the utility in `<was_home>\profiles\<profile_name>\bin\ikeyman.bat`.

b. Open the truststore. Click **Key Database File** > **Open**. In **Key database type**, select **PKCS12**.

c. Click **Browse** to locate the truststore. You can locate the truststore in `<was_home>\profiles\<profile_name>\etc\trust.p12`

d. Type the truststore password. For example: `WebAS`.
e. Add the root CA you extracted to the truststore.
   1) In **Key database content** area, select **Signer Certificates**.
   2) Click **Add**.
   3) Specify the location of the extracted root CA. For example: `C:\root2048.cer`.
   4) Specify a label for the root CA in the truststore. For example: `root2048_signer`.

   The root CA is added to the truststore and saved.

13. Stop and start the server.

Results

You successfully upgraded the key size for the root CA and personal certificates to 2048 bits.

What to do next

Verify that the certificates are upgraded. If the earlier administrative console window is still open, close the Web browser.

1. Open the WebSphere Application Server administrative console in a new instance of the Web browser.
2. Log on to the administrative console with the WebSphere Administrator credentials.
3. When you see the security prompt in the web browser, view the certificate details.
4. Verify that the key size of the reissued certificate is 2048 bits.

Re-creating the root CA for WebSphere Application Server 7.0 on the deployment manager before creating member nodes

Change the root CA key size to 2048 bit on the deployment manager node before you create any federated nodes. Use a 2048 bit key size to offer an increased level of security.

Before you begin

- Create the deployment manager node.
- Ensure that the deployment manager is started.
- Ensure that no nodes are federated.
- Check that your host names are resolving correctly.

About this task

This task is optional. It applies only to:

- New installations of the Privileged Session Recorder Server that include deployment requirements for an increased root certificate key size of 2048 bits.
- A new cluster where only the deployment manager node is created.

  Custom WebSphere Application Server profiles or member nodes of the cluster are not yet created or federated.

With this approach, you upgrade the root CA key size to a 2048 bit `root` certificate before you create member nodes on the cluster.

Complete this task to avoid upgrading the certificate of each node individually.

After you create the deployment manager, complete these steps. The root CA certificate signs the default certificates in the key store. The certificates are for securing internal WebSphere Application Server communications.

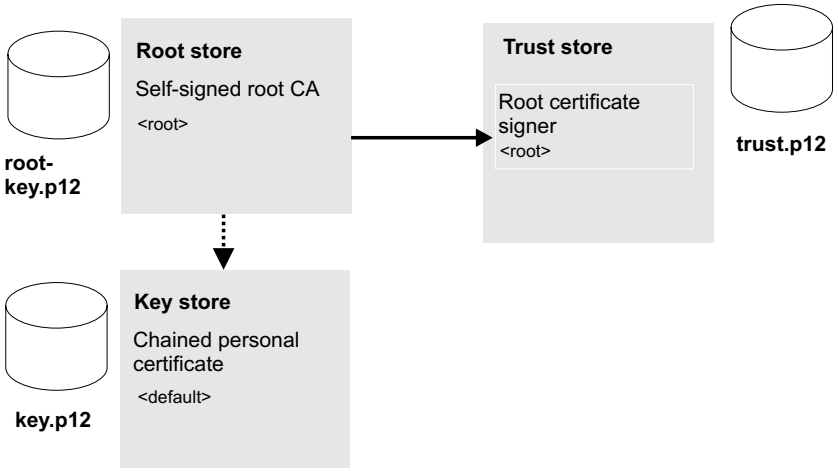

Figure 5. Replacing the root CA and key signers for WebSphere Application Server in the truststore with a new key size.

The process involves the following steps:

1. Replace the default 1024 bit `root` certificate with a new 2048 bit `root` certificate; then extract it. See step 1 to step 9 on page 100.
2. Create a 2048 bit chained personal certificate in the key store, replace the older version, and export the personal certificate to a keystore. See step 10 on page 100 to step 11 on page 101.
3. Use the **ikeyman** utility to add the extracted root CA to the truststore. See step 12 on page 101.

Procedure

1. Select **Start** > **All Programs** > **IBM WebSphere** > **Application Server** **<*version*>** > **Profiles** > **<*dmgr_profile_name*>** > **Administrative console**.
2. Log on to the IBM Integrated Solutions Console.
3. On the Integrated Solutions Console navigation pane, select **Security** > **SSL certificate and key management**.
4. In **Related items**, click **Key stores and certificates**.
5. Create a temporary self-signed root CA in the default root store.

   The temporary root certificate is used to replace the older `root` certificate. The temporary root certificate is then replaced with a new 2048 bit root certificate.

   a. From the **Keystore usages** list, select **Root certificates keystore**.
   b. Click **DmgrDefaultRootStore**.
   c. Under **Additional Properties**, click **Personal certificates**.
   d. Click **Create** > **Self-signed Certificate**.
   e. In **Alias**, enter a new alias name. For example: `root2`.

f. In the **Common name** field, enter the fully qualified domain name of the computer where the WebSphere Application Server is installed. For example: `ibm-svr1.example.com`.

g. Click **OK**.

h. Click **Save**.

6. Replace the old root CA with the new root CA: `root2`. Replace the old `root` with the temporary `root2`.

   a. In the **Personal Certificates** page, select the check box for the older root certificate, `root`.

   b. Click **Replace**.

   c. From the **Replace with** list, choose the alias of the certificate you created.

   d. Select **Delete old certificate after replacement**.

      Important: Be sure that the **Delete old signer** check box is not selected.

      See the WebSphere Application Server, Version 7.0 product documentation on replacing a certificate for details:

      http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/tsec_sslreplaceselfsigncert.html

   e. Click **OK**.

   f. Click **Save** to apply the changes to the master configuration.

7. Create the 2048 bit root CA. This root certificate is the 2048 bit certificate that you retain.

   a. Click **Create** > **Self-signed Certificate**.

   b. In **Alias**, enter `root`.

      Important: You must specify the alias name as `root` for this 2048 bit certificate.

   c. From the **Key size** list, select **2048**.

   d. In the **Common name** field, enter the fully qualified domain name of the computer where the WebSphere Application Server is installed. For example: `ibm-svr1.example.com`.

   e. In the **Validity period** field, enter the validity period of the certificate. For example: A root certificate is typically used for `7300` days, which is approximately 20 years.

   f. Optional: Complete the certificate with optional identification details.

   g. Click **OK**.

   h. Click **Save**.

8. Replace the temporary root certificate with the new 2048 bit root that you retain.

   a. In the **Personal Certificates** page, select the check box for the temporary root certificate: `root2`.

   b. Click **Replace**.

   c. From the **Replace with** list, choose the new 2048 root certificate you created: `root`.

   d. Select **Delete old certificate after replacement**.

   e. Ensure that the **Delete old signer** check box is not selected.

      Important: Be sure that the **Delete old signer** check box is not selected.

   f. Click **OK**.

g. Click **Save** to apply the changes to the master configuration.

You successfully replaced the original 1024 bit root certificate with a new 2048 bit root certificate.

9. Extract the new root CA to a file.
   a. In the **Personal Certificates** page, select **Root**.
   b. Click **Extract**.
   c. In **Certificate file name**, enter the fully qualified path to the certificate to be extracted. For example: `C:\root2048.cer`
   d. Verify **Data type** is **Base64-encoded ASCII data**
   e. Click **OK**.
10. Create a chained personal certificate in the default cell keystore: **CellDefaultKeystore**.
   a. In the **Key stores and certificates** page, click **CellDefaultKeyStore**.
   b. In **Additional Properties**, click **Personal certificates**.
   c. Click the **default** certificate. The distinguished name for the default certificate in the **CellDefaultKeystore** must be in the following form: `CN=<CN>,OU=<OU>,O=<Organization>,C=<Country>` For example: `CN=ibmsvr1.example.com, OU=Root Certificate, OU=ibmsvr1Cell01, OU=ibmsvr1CellManager01, O=IBM, C=US .`
   d. Click **Back**.
   e. Click **Create** > **Chained certificate**.
   f. In the **Alias** field, enter a new personal certificate alias. For example: `default2`.
   g. In the **Root certificate used to sign the certificate** field, select the alias **root**. This root certificate is the new 2048 bit root certificate.
   h. In the **Key size** field, select **2048**.
   i. In the **Common name** field, enter the fully qualified domain name of the computer where the WebSphere Application Server is installed.
   j. In the **Validity period** field, enter the validity period of the certificate. For example: a typical default value for a personal certificate is `365` days.
   k. Required: In the **Organization** field, specify the organization portion of the distinguished name.

      Important: It is important that you specify the organization portion of the distinguished name.
   l. Required: In the **Country or region** field, specify the country portion of the distinguished name.

      Important: It is important that you specify the country portion of the distinguished name.
   m. Optional: Enter more certificate identification information in the optional fields.
   n. Click **OK**.
   o. Click **Save** to apply the changes to the master configuration.
   p. Replace the old default personal certificate with the new one.
      1) In the **Personal Certificates** page, select the **default** check box.
      2) Click **Replace**.
      3) From the **Replace with** list, choose the alias of the certificate you created. For example: `default2`.

4) Select **Delete old certificate after replacement**.
5) Ensure that the **Delete old signer** check box is not selected.

   Important: Be sure that the **Delete old signer** check box is not selected.
6) Click **OK**.
7) Click **Save** to apply changes to the master configuration.

   Note: If the web browser alerts you that a certificate is revoked and a new certificate is available, click **Yes** to proceed. Follow instructions on the screen to accept any more security prompts of the new security certificate.

11. Export the personal certificate to the keystore: For example: `<was_home>\profiles\<dmgr_profile_name>\etc\key.p12`.
    a. In the **Personal Certificates** page, select the personal certificate check box. For example, `default2`.
    b. Click **Export**.
    c. In **Key store password**, enter the key store password For example: `WebAS`.

       Note: The default key store password is documented in the WebSphere Application Server information center.
    d. Select **Key store file**.
    e. In **Key store file**, specify the key store location. For example: `<was_home>\profiles\<dmgr_profile_name>\etc\key.p12`
    f. For **Type**, verify that the default **PKCS12** is selected.
    g. In **Key file password**, type the password. For example: `WebAS`.
    h. Click **OK**.

    You successfully exported the personal certificate and private key to a keystore.
12. Use the IBM Key Management utility, `ikeyman`, to add the extracted root CA to the deployment manager truststore.
    a. Start the **`ikeyman`** utility.

       You can locate the utility in the following location, for example: `<was_home>\profiles\<dmgr_profile>\bin\ikeyman.bat`
    b. Click **Key Database File** > **Open**.
    c. In **Key database type**, select **PKCS12**.
    d. Click **Browse** to locate the truststore. You can locate the truststore in *<was_home>*`\profiles\`*<Dmgr_profile>*`\etc\trust.p12`.
    e. Type the truststore password. For example: `WebAS`
    f. Add the root CA you extracted to the truststore.
       1) In **Key database content** area, select **Signer Certificates**.
       2) Click **Add**.
       3) Specify the location of the extracted root CA. For example: `C:\root2048.cer`
       4) Specify a label for the extracted root CA in the truststore. For example: `root2048_signer`

    The root CA is saved and added to the truststore.
13. Verify that the certificates are upgraded.

a. Log out of the administrative console and try logging in again.
b. When you see the security prompt in the web browser, view the certificate details.
c. Verify that the key size of the reissued certificate is 2048 bits.

14. Restart the deployment manager.

Results

You successfully increased the key size for the root CA and personal certificates.

What to do next

Continue with the process of creating custom profiles for the rest of the member nodes of a cluster in WebSphere Application Server. See "Creating a custom profile (Profile Management Tool)" on page 43.

Optional configuration for shared access

Complete the optional tasks to configure shared access if needed for your deployment.

Manual configuration of the shared access module

After the initial installation of IBM Security Identity Manager, you might have to reconfigure your directory server or your database. You can use the **ldapConfig** and the **DBConfig** tools that are provided by the IBM Security Identity Manager. If you use those tools to modify the IBM Security Identity Manager configuration, you must also reconfigure the shared access module.

You can use the **SAConfig** tool to populate the default data for the shared access module and regenerate key files for the credential vault server. See the topic *Shared access module configuration* in the *IBM Security Identity Manager Installation Guide*.

Configuration of an external credential vault server

The IBM Security Identity Manager installation automatically installs and configures a credential vault server. This server does the check-out and check-in of shared access credentials. A typical installation does not require any manual configuration of the credential vault server.

Optionally, you can deploy multiple IBM Security Identity Manager servers that all use one credential vault server. This configuration reduces the management activities that are required to update the credential vault servers when you change the credentials. For example, this configuration is useful in a WebSphere cluster.

You can configure each of the IBM Security Identity Manager servers to use an external credential vault server. See *Configuring an external credential vault server* in the *IBM Security Identity Manager documentation*.

Creating your own privileged identity management AccessProfiles

Use the IBM Security Privileged Identity Manager AccessProfile to start developing or enhancing your own privileged identity management scenarios.

Before you begin

If you did not, do:

- Install AccessStudio, Version 8.2.1.
- Ensure that you have the Privileged Identity Management AccessProfiles. You can download the AccessProfiles from the AccessProfiles Library.

Procedure

1. In AccessStudio, open the sample AccessProfile.
2. Build or enhance the Privileged Identity Management AccessProfile. For more information, see "Modifying AccessProfiles" in the *IBM Security Privileged Identity Manager Administrator Guide*.
3. Debug and start your AccessProfile.
4. Upload your AccessProfile to the IMS Server..

Lease time modifications

If you manually check out shared access credentials from IBM Security Identity Manager Server, you can modify the lease expiry time for shared access credentials.

To modify the lease time expiry for a credential, see the IBM Security Identity Manager product documentation and search for `credential setting lease expiration`. You cannot modify the lease expiry time when you check out or check in credentials automatically.

IBM Security Identity Manager host name or security certificate change

If the IBM Security Identity Manager host name or security certificate details change, you must manually import the IBM Security Identity Manager certificates on the computer where you installed the AccessAgent.

Run the following command to install or import the IBM Security Identity Manager certificates on the computer where you installed the AccessAgent:

x86 operating system

rundll32.exe *aa_installpath*\AA\ECSS\PIMSlnHelper.dll,Believe *isim_ip_host*

x64 operating system

rundll32.exe *aa_installpath*\AA\ECSS\PIMSlnHelper64.dll,Believe *isim_ip_host*

For example: **rundll32.exe** c:\Program Files\IBM\ISAM ESSO\AA\ECSS\PIMSlnHelper.dll,Believe *"192.0.2.2"*

IBM Tivoli Common Reporting configuration or administration

An Administrator can use IBM Tivoli Common Reporting to view the shared access reports that are available from IBM Security Access Manager for Enterprise Single Sign-On and IBM Security Identity Manager.

You can view, administer, and run the available reports with the IBM Tivoli Common Reporting software.

Note: For more information about customizing the default shared access report layouts, see the IBM Security Identity Manager product documentation.

Importing the reports into Tivoli Common Reporting

Importing the report packages places the reports in an IBM Tivoli Common Reporting instance that you can access.

Before you begin

- Install IBM Security Identity Manager, Version 6.0. For more information, see the *IBM Security Identity Manager Installation Guide*.
- Install IBM Security Access Manager for Enterprise Single Sign-On, Version 8.2.1. For more information, see the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.
- Install or upgrade to IBM Tivoli Common Reporting, Version 2.1.1. For more detailed and up-to-date instructions, see the IBM Tivoli Common Reporting product documentation.

About this task

Both IBM Security Access Manager for Enterprise Single Sign-On and IBM Security Identity Manager include a subset of reports that you can install into IBM Tivoli Common Reporting.

IBM Security Privileged Identity Manager includes Cognos-based reports for the Privileged Session Recorder feature that you can view with IBM Tivoli Common Reporting.

Procedure

1. Import the IBM Security Identity Manager, Version 6.0, report package into IBM Tivoli Common Reporting.
2. Import the IBM Security Access Manager for Enterprise Single Sign-On, Version 8.2.1, report package into IBM Tivoli Common Reporting.
3. Import the Cognos-based IBM Privileged Session Recorder, Version 1.0, report package into IBM Tivoli Common Reporting.
4. Configure the data source in IBM Tivoli Common Reporting to work with each report package. See the IBM Tivoli Common Reporting product documentation.

Results

Importing the reports places them in **Common Reporting** > **Public Folders** > **Tivoli Products**.

Connecting Tivoli Common Reporting to a DB2 database for Privileged Session Recorder

Connect IBM Tivoli Common Reporting to a DB2 database.

Before you begin

For detailed and up-to-date instructions, see the IBM Tivoli Common Reporting documentation.

Deploy the DB2 database client on the computer where the Cognos-based Tivoli Common Reporting engine is installed. The version of the client must match the version of your database.

Determine the service name of the DB2 server. To determine the value, open a DB2 command prompt. Type `get dbm cfg`. Look for `TCP/IP Service name (SVCENAME) = <value>`. You need the service name in the following example steps.

Procedure

1. Connect the DB2 database client to the database by running the Configuration Assistant.
2. Create a connection by using the Wizard.
   a. Select **Manually configure a connection to a database**.
   b. Select **TCP/IP** as the communications protocol.
   c. Specify the connection parameters.

      Host name
      Host name of the Privileged Session Recorder DB2 server.

      Service name
      Service name of the DB2 server.

      Port number
      If the first two values are correct, this field is automatically completed.
3. Specify the database details.

   Database name
   Specifies the name of the Privileged Session Recorder database.

   Database alias
   Specifies the target database for Tivoli Common Reporting.
4. Select **Register this database for CLI/ODBC**.
5. Provide details about the node.
6. Provide information about the system.
7. Select **Use authentication value in the server's DBM Configuration**.
8. Click **Finish**.
9. Test the connection.

Configuring the data source for IBM Privileged Session Recorder reports

Configure the data source in Tivoli Common Reporting to work with IBM Privileged Session Recorder reports.

Before you begin

- Install the IBM Privileged Session Recorder Server.
- Install IBM Tivoli Common Reporting Version 2.1.1. See the IBM Tivoli Common Reporting product documentation.

Procedure

1. Log on to Tivoli Integrated Portal.
2. Click **Reporting** > **Common Reporting**.
3. From the **Launch** menu, click **Administration**.

4. Click the **Configuration** tab.
5. Click **New Data Source**.
6. Specify a name. For example: `psrds`
7. For **Type**, select DB2.
8. For the DB2 connection string, consider the following options:
   - DB2 database name: Use the alias you created.
   - Ensure **Signons** is selected.
   - Select the **Password** checkbox.
   - Select the **Create a signon that the Everyone group can use**.
9. Test the connection.

What to do next

Import the IBM Privileged Session Recorder report into Tivoli Common Reporting.

Importing the Cognos-based IBM Privileged Session Recorder report into Tivoli Common Reporting

Importing the report package places the reports in an IBM Tivoli Common Reporting instance that you can access.

Before you begin

Configure the data source for Privileged Session Recorder. See the IBM Tivoli Common Reporting product documentation.

Procedure

1. Copy the `IBM Privileged Session Recorder Report.zip` file from `<recorder_install_home>\report` to the `Tivoli Common Reporting cognos\deployment` folder. For example: `C:\IBM\tivoli\tipv2Components\TCRComponent\cognos\deployment`
2. Log in to the Tivoli Integrated Portal. For example: `https://<server>:16311/ibm/console/`.
3. Click **Reporting** > **Common Reporting**.
4. From the **Common Reporting** portlet, go to the **Launch** drop-down list, and choose **Administration**.
5. Click the **Configuration** tab.
6. Click **Content Administration**.
7. Click **Import**.
8. Select the **IBM Privileged Session Recorder Report** and click **Next**.
9. In the **Specify a name and description** page, click **Next**.
10. Select the **IBM Privileged Session Recorder Package** checkbox.
11. Review the **Summary** and click **Next**.
12. Follow the instructions to complete the steps.

Related reference:

"Planning worksheet" on page 113
Use the planning worksheet as a reference for the default and sample values during the installation and configuration of the Privileged Session Recorder Server and required middleware.

Running the IBM Privileged Session Recorder report

You can run a report on demand or create a snapshot of it for later viewing.

Procedure

1. Log in to Tivoli Integrated Portal.
2. Click **Reporting** > **Common Reporting**.
3. Click the **IBM Privileged Session Recorder** link.
4. Select the **IBM Privileged Session Recorder Audit Report Query** check box.
5. Click **Play**.
6. Click **Run**.

Multiple AccessProfiles for the same client application

Each application signature for an AccessProfile must be unique. Single sign-on cannot occur if there are multiple AccessProfiles with the same application signature on the IMS Server. If you have more than one AccessProfile for the same application, consider deleting or modifying copies of the AccessProfile.

Note: Duplicate AccessProfiles with signature detection conflicts are also logged in the AccessAgent logs as errors.

For example, a Remote Desktop Connection (RDP) AccessProfile is already on the IMS Server.

- You might already have a custom Remote Desktop Connection (RDP) AccessProfile for logging on to remote desktops.
- If you upload a new privileged identity management AccessProfile with the same application signature, single sign-on does not trigger.
- Consider the actions that you can take to resolve the issue.
  - Delete the existing AccessProfile for the RDP application from the IMS Server if the AccessProfile is not in use.
  - Merge the AccessProfiles.

Important: Privileged identity management AccessProfiles work only with AccessAgent, Version 8.2.1

Identifying AccessProfile collision

You can use the AccessStudio message pane logs to determine whether there are multiple AccessProfiles for the same client application on the IMS Server.

Before deployment, complete these steps on a test computer with the AccessAgent installed:

1. Ensure that you are logged on to AccessAgent.
2. Import data from the IMS Server with AccessStudio.
3. Start the client application that you are testing for AccessProfile collision.
4. From the AccessStudio real-time logs, look for the phrase:

   ```
   ...multiple AccessProfiles were found.
   ```

Merging AccessProfiles

If you want both the privileged identity management AccessProfiles and the AccessProfiles you already have, then you must consider advanced AccessProfile merging.

For help with advanced AccessProfile merging, contact IBM Services.

Unconfiguring the Privileged Session Recorder Server settings on WebSphere Application Server

You can unconfigure the WebSphere Application Server and database settings for the Privileged Session Recorder Server.

Before you begin

Stop the ISPIMRecorder application on WebSphere Application Server. For more information, see the WebSphere Application Server, Version 7.0 product documentation and search for `stopping WebSphere enterprise applications`.

About this task

Unconfiguring the Privileged Session Recorder with the IBM Configuration Manager utility removes the configuration for the following items:

- Database

  Note: The Privileged Session Recorder database is not deleted. Only the database connection information is removed.
- WebSphere Application Server
- Message queue

Procedure

1. Start the IBM Configuration Manager utility.
2. Click **Configure Privileged Session Recorder Server**.
3. Click **Guided Unconfiguration**.
4. Follow the instructions in the wizard to complete the process.

What to do next

On the WebSphere Application Server, delete the `RecorderQ` folder by taking the following action:

- For network deployments, browse to the `<was_home>\AppServer\profiles\<custom_node>\` folder. Delete the folder `RecorderQ`. Repeat on each of the custom nodes.
- For stand-alone deployments, browse to the `<was_home>\AppServer\profiles\<app_server>\` folder. Delete the folder `RecorderQ`.

Undeploying the Privileged Session Recorder Server from WebSphere Application Server

You can use the IBM Configuration Manager utility to unconfigure a Privileged Session Recorder Server deployment.

Procedure

1. Start the IBM Configuration Manager utility.
2. Click **Deploy Privileged Session Recorder Server**.
3. Click **Guided Unconfiguration**.
4. Follow the instructions in the wizard to complete the process.

Appendix B. Uninstallation tasks

You can uninstall the Privileged Session Recorder Server and client components interactively.

Uninstalling the Privileged Session Recorder Server components

You can uninstall the Privileged Session Recorder Server components with the IBM Installation Manager.

Before you begin

- Log on with a user account that has the same privileges as the account that was used to install the packages.
- Stop the server and client components.

About this task

For more information about uninstalling IBM Installation Manager packages, go to the IBM Installation Manager documentation and search for `uninstalling packages`.

Procedure

1. Start IBM Installation Manager.
2. Click **Uninstall**.
3. In the Uninstall wizard, select the Privileged Session Recorder Server packages to uninstall.
4. Follow the instructions in the wizard to complete the process.

Results

The Privileged Session Recorder Server components are uninstalled.

Note: The Privileged Session Recorder database is not deleted. To delete a database in DB2, see the IBM DB2, Version 9.7 product documentation.

Uninstalling the Privileged Session Recorder Client components

On the Windows operating system, you can also use the Add/Remove Programs from the Windows Control Panel.

Before you begin

- Log on with a user account that has the same privileges as the account that was used to install the packages.
- Stop the client components.

About this task

Note: The Privileged Session Recorder Client components cannot be uninstalled separately from AccessAgent. The following steps will uninstall AccessAgent.

Procedure

1. On the Windows workstation, start the client software removal utility.

   On Microsoft Windows XP:
   Click **Start** > **Control Panel** > **Add or Remove Programs**.

   On Microsoft Windows 7
   Click **Start** > **Control Panel** > **Programs and Features**.
2. Select the **ISAM ESSO AccessAgent** package.
3. Click **Remove**.

Appendix C. References

IBM Security Privileged Identity Manager involves shared access-related reports and APIs.

Planning worksheet

Use the planning worksheet as a reference for the default and sample values during the installation and configuration of the Privileged Session Recorder Server and required middleware.

Installation directories and other paths

The following table contains the different path variables that are used throughout the guide and the corresponding default values. In some cases, the variable name matches the name of an environment variable that is set in the operating system. For example, `%TEMP%` represents the environment variable `%TEMP%` for Windows.

Table 26. Installation directories and other paths

Path variable	Component	Default directory
<aa_home>	AccessAgent	`C:\Program Files\IBM\ISAM ESSO\AA`
<as_home>	AccessStudio	`C:\Program Files\IBM\ISAM ESSO\AA\ECSS\AccessStudio`
<db_home>	DB2	`C:\Program Files\IBM\SQLLIB`
<ihs_home>	IBM HTTP Server	`C:\Program Files\IBM\HTTPServer`
<ims_home>	IBM Security Access Manager for Enterprise Single Sign-On IMS Server	`C:\Program Files\IBM\ISAM ESSO\IMS Server`
<jvm_home>	Java Virtual Machine	`C:\Program Files\Java\jre1.5.0_11`
<updi_home>	IBM Update Installer for WebSphere Application Server	`C:\Program Files\IBM\WebSphere\ UpdateInstaller`
<was_home>	WebSphere Application Server	`C:\Program Files\IBM\WebSphere\ AppServer`
<was_dmgr_home>	WebSphere Application Server Network Deployment deployment manager profile	`C:\Program Files\IBM\WebSphere\ AppServer\profiles\Dmgr01`
<%TEMP%>	Windows directory for temporary files	When logged on as `Administrator`, `C:\Documents and Settings\ Administrator\Local Settings\Temp`
<%PROGRAMFILES%>	Windows directory for installed programs	`C:\Program Files`

Table 26. Installation directories and other paths (continued)

Path variable	Component	Default directory
<*recorder_install_home*>	IBM Privileged Session Recorder Server installation directory	`C:\Program Files(x86)\IBM\IBM Privileged Session Recorder\`

Host names and ports

The following table contains the different variable host names and port numbers that are used throughout the guide.

Table 27. Host names and ports

Variable	Description
<*was_hostname*>	Name of the host where the WebSphere Application Server is installed.
<*dmgr_hostname*>	Name of the host where the WebSphere Application Server Network Deployment Manager is installed.
<*ihs_hostname*>	Name of the host where the IBM HTTP Server is installed.
<*loadbalancer_hostname*>	Name of the host where the load balancer is installed.
<*ims_hostname*>	Name of the host where the IMS Server is installed.
<*ihs_ssl_port*>	IBM HTTP Server SSL port number.
<*admin_ssl_port*>	Administrative console secure port number.

URLs and addresses

The following table contains the different URLs and addresses that are used throughout the guide. The values vary depending on whether you are using WebSphere Application Server stand-alone or WebSphere Application Server Network Deployment.

Table 28. URLs and addresses

Description	Format	Example value
IBM Integrated Solutions Console (WebSphere Application Server administrative console)	• If you are using WebSphere Application Server stand-alone: *https://<was_hostname>:<admin_ssl_port>/ibm/console* • If you are using WebSphere Application Server Network Deployment: *https://<dmgr_hostname>:<admin_ssl_port>/ibm/console*	`https://localhost:9043/ibm/console` or `http://localhost:9060/ibm/console`

Table 28. URLs and addresses (continued)

Description	Format	Example value
IMS Configuration Wizard	• If you are using WebSphere Application Server stand-alone: *https://<was_hostname>:<admin_ssl_port>/front* • If you are using WebSphere Application Server Network Deployment: *https://<dmgr_hostname>:<admin_ssl_port>/front*	`https://localhost:9043/front`
IMS Configuration Utility	• If you are using WebSphere Application Server stand-alone: *https://<was_hostname>:<admin_ssl_port>/webconf* • If you are using WebSphere Application Server Network Deployment: *https://<dmgr_hostname>:<admin_ssl_port>/webconf*	`https://localhost:9043/webconf`
AccessAdmin	• If you are using a load balancer: *https://<loadbalancer_hostname>:<ihs_ssl_port>/admin* • If you are not using a load balancer: *https://<ims_hostname>:<ihs_ssl_port>/admin* • If web server is configured properly: *https://ims_hostname>/admin*	• `https://imsserver:9443/admin` • `https://imsserver/admin`
AccessAssistant	• If you are using a load balancer: *https://<loadbalancer_hostname>:<ihs_ssl_port>/aawwp* • If you are not using a load balancer: *https://<ims_hostname>:<ihs_ssl_port>/aawwp*	`https://imsserver:9443/aawwp`
Web Workplace	• If you are using a load balancer: *https://<loadbalancer_hostname>:<ihs_ssl_port>/aawwp?isWwp=true* • If you are not using a load balancer: *https://<ims_hostname>:<ihs_ssl_port>/aawwp?isWwp=true*	`https://imsserver:9443/aawwp?isWwp=true`
IBM Privileged Session Recorder console	`https://<recorder_hostname>/recorder/ui`	`https://psrserver/recorder/ui`
IBM Privileged Session Recorder Server URL	`https://<recorder_hostname>/recorder/collector`	`https://psrserver/recorder/collector`

Users, profile names, and groups

The following table contains some of the users and groups that are created during the installation.

Table 29. Users, profile names, and groups

Variable	Description	Example value
<profile name>	WebSphere Application Server profile name. The profile name is defined when creating profiles for WebSphere Application Server with the `manageprofiles` command-line tool or graphical Profile Management tool.	• If you are using WebSphere Application Server stand-alone: `<AppSrv_profilename>` • If you are using WebSphere Application Server Network Deployment: – Deployment manager: `<Dmgr_profilename>` – Node `<Custom_profilename>`
<WAS Admin user ID>	WebSphere Administrator ID created during the installation of WebSphere Application Server.	`wasadmin`
<IHS Admin user ID>	HTTP Server Administrator user ID created during the installation of the IBM HTTP Server.	`ihsadmin`
<DB2 Admin user ID>	DB2 Administrator service user ID for Microsoft Windows created during the installation of IBM DB2.	`db2admin`
<IMS Admin user ID>	IBM Security Access Manager for Enterprise Single Sign-On Administrator. User ID created during installation of the IMS Server for administration of IBM Security Access Manager for Enterprise Single Sign-On.	`imsadmin`
<PSR Auditor user ID>	IBM Privileged Session Recorder auditor user ID created during configuration of the IBM Privileged Session Recorder Server.	`psrauditor`

Installing IBM DB2

The following table contains values that you must specify when you install a database server.

Table 30. Example or default values for IBM DB2 installation

Parameter	Default or Example Value
Installation directory	`C:\Program Files\IBM\SQLLIB`
User information for the DB2 Administration Server	
Domain	`None - use local user account`
User name	`db2admin`

Table 30. Example or default values for IBM DB2 installation (continued)

Parameter	Default or Example Value
Password	
DB2 instance	`Create the default DB2 instance`
Partitioning option for the default DB2 instance	`Single partition instance`
DB2 tools catalog	`None`
Set up your DB2 Server to send notifications	`No`
Enable operating system security	`Yes`
DB2 administrators group	
Domain	`None`
Group Name	`DB2ADMNS` **Note:** This value is an example. You can specify your own value.
DB2 users group	
Domain	`None`
Group Name	`DB2USERS` **Note:** This value is an example. You can specify your own value.
Port number	`50000`

Creating the Privileged Session Recorder database

The following table contains the values that you must specify to create the Privileged Session Recorder database.

Table 31. Example or default values for the creation of the Privileged Session Recorder database

Parameter	Default or Example Value
Database name	`recdb` **Note:** This value is an example. You can specify your own value.
Default path	`C:\`
Alias	`recdb` **Note:** This value is an example. You can specify your own value.
Comment	`DB for Session Recording` **Note:** This value is an example. You can specify your own value.
Let DB2 manage my storage (automatic storage)	`Yes`
Default buffer pool and table space page size	`8K`
Use the database path as a storage path	`Yes`
Code set	`UTF-8`
Collating sequence	
Region	Default

Creating a DB2 user manually

The following table contains the values that you must specify, if you are creating a separate database user for IBM Security Access Manager for Enterprise Single Sign-On.

Table 32. Example or default values for DB2 user creation

Parameter	Default or Example Value
DB2 user	`recdb2admin`
Administrative privileges	• Connect to database • Create tables • Create packages

Installing IBM Installation Manager for WebSphere software installation

The following table contains the values that you specify when you install the IBM Installation Manager.

Parameter	Default Or Example Value
Installation file (administrative installation)	`install.exe`
Installation directory	`C:\Program Files\IBM\InstallationManager`
Local repository path	`C:\repositories\`*`product_name`*`\local-repositories`

Installing WebSphere Application Server

The following table contains the values that you must specify when you install the WebSphere Application Server.

Table 33. Example or default values for WebSphere Application Server installation

Parameter	Default or Example Value
Installation directory	`<was_home>`
WebSphere Application Server Environment	(None) **Note:** Profiles are created only with the Profile Management tool or command-line interface after the WebSphere fix packs are applied. You can create the following profiles: For WebSphere Application Server stand-alone product deployments • Application server For WebSphere Application Server Network Deployment (cluster) • Deployment Manager • Custom
Enable Administrative Security	`Yes`
WebSphere Administration user name	`wasadmin`
Deployment Manager profile name	`<Dmgr_profilename>`
Custom profile name (node)	`<Custom_profilename>`
Application server profile name	`<AppSrv_profilename>`
Cell name	`<Server01Node01Cell01>`
Deployment Manager node name	`<Server01Cell01>`
Application server node name	`<Server01Node01>`
HTTP server installation location	`<ihs_home>`
HTTP port	`80`

Table 33. Example or default values for WebSphere Application Server installation (continued)

Parameter	Default or Example Value
HTTP admin server port	8080

Installing IBM Update Installer for WebSphere software installation

The following table contains the values that you must specify when you install the IBM Update Installer for WebSphere Software Installation.

Table 34. Example or default values for IBM Update Installer installation for WebSphere software

Parameter	Default or Example Value
Installation file	install.exe
Installation directory	C:\Program Files\IBM\WebSphere\UpdateInstaller

Installing the latest WebSphere Application Server Version 7.0 fix pack

The following table contains the values that you must specify when you install the latest WebSphere Application Server fix pack.

Table 35. Example or default values for WebSphere Application Server fix pack installation

Parameter	Default or Example Value
Installation file	7.0.0-WS-WAS-WinX64-FP000000X.pak
Installation directory	<was_home>
Maintenance Operation Selection	Install maintenance package
Maintenance package directory path	<updi_home>\maintenance

Installing IBM HTTP Server

The following table contains the values that you must specify when you install the IBM HTTP Server.

Table 36. Example or default values for IBM HTTP Server installation

Parameter	Default or Example Value
Installation directory	<ihs_home>
IBM HTTP Server HTTP Port	80
IBM HTTP Server HTTP Administration Port	8008
Run IBM HTTP Server as a Windows Service	Yes
Run IBM HTTP Administration as a Windows Service	Yes
Log on as a local system account	Yes
Log on as a specified user account	No

Table 36. Example or default values for IBM HTTP Server installation (continued)

Parameter	Default or Example Value
User name	`Administrator` **Note:** This value is an example. You can specify your own value.
Password	
Startup type	`Automatic`
Create a user ID for IBM HTTP Server administration server authentication	`Yes`
IBM HTTP Server administration server authentication user ID	`ihsadmin` **Note:** WebSphere Application Server account for administering IBM HTTP Server and the IBM HTTP Server plug-in.
IBM HTTP Server administration server authentication password	
Install IBM HTTP Server Plug-in for IBM WebSphere Application Server	`Yes`
Web server definition	`<webserver1>`
Host name or IP address for the Application Server	`was01.example.com`

Installing the latest IBM HTTP Server Version 7.0 fix pack

The following table contains the values that you must specify when you install the latest IBM HTTP Server fix pack.

Table 37. Example or default values for IBM HTTP Server fix pack installation

Parameter	Default or Example Value
Installation file	`7.0.0-WS-IHS-WinX64-FP000000X.pak`
Installation directory	`<ihs_home>`
Maintenance Operation Selection	`Install maintenance package`
Maintenance package directory path	`<was_home>\UpdateInstaller\maintenance`

Configuring the IBM HTTP Server Version 7.0

The following table contains the values that you must specify when you configure the IBM HTTP Server to work with the WebSphere Application Server.

Table 38. Example or default values for IBM HTTP Server configuration

Parameter	Default or Example Value
Windows batch file	`configure<webserver1>.bat`
Original Location	`<ihs_home>\Plugins\bin`
Target Location	`<was_home>\bin`
com.ibm.SOAP.requestTimeoutproperty	`6000`
Remote Web server management	
Port	`8008`
User name	`ihsadmin`
Password	

Table 38. Example or default values for IBM HTTP Server configuration (continued)

Parameter	Default or Example Value
Use SSL	No
Refresh configuration interval	60 seconds
Plug-in configuration file name	plugin-cfg.xml
Plug-in keystore file name	plugin-key.kdb
Plug-in configuration directory and file name	<ihs_home>\Plugins\config\<webserver1>\ plugin-cfg.xml
Plug-in keystore directory and file name	<ihs_home>\Plugins\config\<webserver1>\ plugin-key.kdb
Automatically generate the plug-in configuration file	Yes
Automatically propagate the plug-in configuration file	Yes

AccessAgent IBM Security Privileged Identity Manager API reference

Use the AccessAgent IBM Security Privileged Identity Manager API reference to identify the available IBM Security Privileged Identity Manager application programming interfaces.

CheckOut

Use `CheckOut` to check out a credential from the IBM Security Identity Manager.

```
HRESULT CheckOut(
 [in] ISERuntime* RuntimeObj,
 [in] BSTR ItimSvcUrl,
 [in] BSTR ItimAuthSvcId,
 [in] BSTR PrivCredBag,
 [in] VARIANT_BOOL IsPrivCredBagLocal,
 [in] BSTR ApplicationName,
 [in] VARIANT_BOOL ServiceLowerCaseConventionEnabled,
 [in] VARIANT_BOOL ReAuthPasscodeEnabled,
 [in] VARIANT_BOOL CheckInAllBeforeCheckOutEnabled,
 [in] BSTR RoleSelectionDlgParentHwndSignature,
 [in] VARIANT_BOOL SilentModeEnabled,
 [in, defaultvalue("true")] VARIANT_BOOL IsRegistrationEnabled,
 [out,retval] int* pRet);
```

RuntimeObj
Run time object obtained from the scripting host.

ItimSvcUrl
URL of the IBM Security Identity Manager service. For example: `https://itim.ibm.com:9081/WAR_CICO/services/CICOManager`.

ItimAuthSvcId
Authentication service ID of IBM Security Identity Manager. The user Wallet must contain the IBM Security Identity Manager credential.

PrivCredBag
Privileged credential bag stores:

- Checked-out privileged credentials.
- Application managed resource authentication service ID.

IsPrivCredBagLocal
Specify whether to use local bag for the privileged credential bag.

ItimTokenBag
This parameter is not used. It is included for compatibility with an earlier version.

IsItimTokenBagLocal
Specify whether to use local bag for IBM Security Identity Manager token bag.

CheckInAllBeforeCheckOutEnabled
Specify whether to reauthenticate user credentials before you check out.

ReAuthPasscodeEnabled
Specify whether to check in all credentials before checkout.

RoleSelectionDlgParentHwndSignature
Signature of the role selection dialog box parent window. If the parameter is an empty string, the role selection dialog box parent window is NULL.

SilentModeEnabled
If this parameter is true, no dialogs and prompts are displayed.

IsRegistrationEnabled
If this parameter is true, the background process automatically checks in the shared credential. It occurs when the process fails to check in the credential, for example, a user exits the program in an unexpected way.

CheckIn

Use `CheckIn` to check in shared access credentials into the IBM Security Identity Manager credential vault.

```
HRESULT CheckIn(
[in] ISERuntime* RuntimeObj,
[in] BSTR PrivCredBag,
[in] VARIANT_BOOL IsPrivCredBagLocal,
[out,retval] int* pRet);
```

RuntimObj
Runtime object obtained from the scripting host.

PrivCredBag
Privileged credential bag that contains the checked out credentials. It stores the:

- Checked-out credentials.
- Application (endpoint) authentication service ID.

IsPrivCredBagLocal
Specify whether the bag is local or global.

Privileged Session Recorder Server messages

These messages contain information about Privileged Session Recorder.

CTGSR0020E Cannot start the Lucene indexer.

Explanation: The indexer cannot start because there are errors.

System action: Privileged Session Recorder server playback performance is affected.

CTGSR0040E Cannot connect to the Privileged Session Recorder database.

Explanation: Unable to establish database connection.

System action: Privileged Session Recorder server cannot transfer the recordings to the database.

CTGSR0050E Privileged Session Recorder queue initialization failed.

Explanation: Recorder queues cannot be initialized because of errors.

System action: Privileged Session Recorder server

cannot accept new recordings.

CTGSR0055E Privileged Session Recorder database injectors cannot start.

Explanation: Recorder queue consumer threads were unable to start. Database injectors are tasks performed by these consumer threads.

System action: Privileged Session Recorder server cannot transfer the recordings to the database.

Administrator response: Check the connection pool for the WebSphere queue connection factory and check if the number of threads to allocate consumers are sufficient for the work manager.

CTGSR0201W Frame *frameStr* cannot be saved to the database at the moment.

Explanation: The frame cannot be stored at the moment because of some errors.

System action: The system will reattempt to save the frame later.

Administrator response: No action taken.

CTGSR0202W Image for frame with ID *frameStr* cannot be saved to the database at the moment.

Explanation: The image cannot be stored at the moment because of some errors.

System action: The system will reattempt to store the image later.

Administrator response: No action taken.

CTGSR0203W Caught exception while starting *taskId* daemon task by the *workMgrHashCode* work manager on WebSphere Application Server.

Explanation: Error occured while trying to assign the daemon task to the work manager.

System action: The task cannot run.

Administrator response: Check the work manager if it exists and check if there are free threads to run this task. Restart the server after fixing.

CTGSR0204W Unable to deploy the enterprise application resource *appName* to the application server using the EAR file *earFile*.

Explanation: Check the application server logs for errors.

System action: The application halts further configuration.

Administrator response: Ensure that the application server is running. Rectify any issues found in the application server logs. Ensure the application server management port is listening and accessible.

CTGSR0205W Unable to undeploy the enterprise application resource *appName* to the application server.

Explanation: Check the application server logs for errors.

System action: The application continues unconfiguration.

Administrator response: Ensure that the application server is running. Rectify any issues that are found in the application server logs. Ensure that the application server management port is listening and is accessible. The application might be removed manually through the application server administration facilities (web-based or command line).

CTGSR0401W Unable to restart the WebSphere Application Server *serverType serverName*.

Explanation: Attempts to restart the server failed. However, configuration tasks were completed and the changes were applied successfully.

System action: Changes cannot take effect until the WebSphere Application Server is restarted.

Administrator response: Restart the WebSphere Application Server manually.

CTGSR0402W Unable to save the changes to the WebSphere Application Server configuration.

Explanation: Configuration tasks were completed but the changes cannot be saved.

Administrator response: Ensure that the WebSphere Application Server did not go offline during the process and run the tool again.

CTGSR0421W Validation failed due to empty fields.

Explanation: Ensure that the required fields are completed.

Administrator response: Enter the necessary values and try again to continue.

CTGSR0422W Invalid port.

Explanation: Data source port is incorrect.

CTGSR0423W Unable to connect to the database.

Explanation: Attempts to connect to the database failed.

Administrator response: Ensure that the database is started and operational.

CTGSR0424W Invalid queue size.

Administrator response: Enter a valid size for the persistent queues.

CTGSR0425W Passwords do not match.

Explanation: The password you entered does not match.

Administrator response: Retype the password and try again.

CTGSR0426W Error occured while updating the JDBC classpath *classpath* on WebSphere Application Server.

Explanation: The JDBC driver cannot be copied to the WebSphere Application Server because of some errors.

System action: Data source might not work if the JDBC driver is not updated.

Administrator response: Copy the JDBC driver manually to the location.

CTGSR0427W Error starting the WebSphere AdminClient session.

CTGSR0428W Error creating the data source on WebSphere Application Server.

Explanation: WebSphere data source could not be created due to errors.

CTGSR0429W Error creating the schema while configuring the data source.

Explanation: While creating the data source, as the schema is not present, the task to create the schema was started but did not complete.

System action: The configuration tool was not able to create the schema.

Administrator response: Create the schema manually and run the tool to create a data source on WebSphere Application Server.

CTGSR0430W Error removing the data source on WebSphere Application Server.

Explanation: There was an error when removing the data source on WebSphere Application Server.

System action: Data source cannot be removed from this profile.

Administrator response: Check the configuration logs.

CTGSR0431W Error creating the security settings on WebSphere Application Server.

Explanation: There was an error when creating the security settings on WebSphere Application Server.

CTGSR0432W Error removing the security settings from WebSphere Application Server.

Explanation: An error was encountered when attempting to remove the security settings on WebSphere Application Server.

CTGSR0433W Error creating group *grpName* in WebSphere Application Server repository with realm *realmName*.

CTGSR0434W Error creating user *userName* in WebSphere Application Server repository with realm *realmName*.

CTGSR0435W User *userNameDn* does not exist in the WebSphere Application Server repository.

CTGSR0436W Error creating the queue settings on WebSphere Application Server.

Explanation: The queue settings cannot be applied.

System action: The IBM Privileged Session Recorder configuration tool was not able to apply configuration changes.

Administrator response: Run the configuration tool again.

CTGSR0437W Error removing queue settings from WebSphere Application Server.

CTGSR0438W Error syncing configurations across active managed nodes.

CTGSR0439W Deleting configuration failed with errors.

Explanation: Some of the IBM Privileged Session Recorder configurations cannot be removed.

Administrator response: Check logs for details and manually remove configuration.

CTGSR0440W Queue cannot be removed because it still contains messages.

Explanation: Recorder queue cannot be removed at this time because some of the recordings are in the queue.

Administrator response: Wait for the consumer threads to transfer the Privileged Session Recorder messages to the database and then run the tool to unconfigure the queue.

CTGSR0441W The username *userNameDn* already exists in the WebSphere Application Server repository.

Explanation: As this user name already exists on the default WebSphere Application Server file-based repository, a new user with the same user name cannot be provisioned.

CTGSR0500W Indexer refresh interval specified is invalid. (Min = 1).

CTGSR0501W Validation failed for the specified Indexer refresh interval.

CTGSR0502W Copying server configuration file to *grpName* failed.

Explanation: The file containing server configurations could not be copied to the profile.

System action: Server will continue using the defaults because the configuration is not present.

Administrator response: Manually create the configuration file, if needed, to overwrite the defaults.

Accessibility features for IBM Security Privileged Identity Manager

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

Accessibility features

IBM Security Privileged Identity Manager conforms to Section 508 standards for accessibility.

The following list includes the major accessibility features in IBM Security Privileged Identity Manager:

- Support for the Freedom Scientific JAWS screen reader application
- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternate input and output devices

The IBM Security Privileged Identity Manager documentation, and its related publications, are accessibility-enabled. The accessibility features of the documentation are described at http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.iehsc.doc/iehs34_accessibility.html.

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

Related accessibility information

You can view the publications for IBM Security Privileged Identity Manager in Adobe Portable Document Format (PDF) with the Adobe Acrobat Reader. The PDFs are available in the information center.

The following keyboard navigation and accessibility features are available in the form designer:

- You can use the tab keys and arrow keys to move between the user interface controls.
- You can use the Home, End, Page Up, and Page Down keys for additional navigation.
- You can start any applet, such as the form designer applet, in a separate window. The applet enables Alt+Tab to toggle between that applet and the web interface and for more screen workspace. To start the window, click **Launch as a separate window**.
- You can change the appearance of applets such as the form designer by using themes. Themes provide high contrast color schemes that help users with vision impairments to differentiate between controls.

IBM and accessibility

See the IBM Human Ability and Accessibility Center for information about the IBM commitment to accessibility.

Notices

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

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

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

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

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

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

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

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

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

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2012. All rights reserved.

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

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/us/en/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Privacy Policy Considerations

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

The IBM Security Access Manager for Enterprise Single Sign-On software uses other technologies that collect each user's user name, password or other personally identifiable information for purposes of session management, authentication, single sign-on configuration or other usage tracking or functional purposes. These technologies can be disabled, but disabling them will also eliminate the functionality they enable.

The IBM Security Identity Manager and Role Management software does not use cookies or other technologies to collect personally identifiable information. The only information that is transmitted between the server and the browser through a cookie is the session ID, which has a limited lifetime. A session ID associates the session request with information stored on the server.

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

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

Glossary

This glossary includes terms and definitions for IBM Security Privileged Identity Manager.

The following cross-references are used in this glossary:

- See refers you from a term to a preferred synonym, or from an acronym or abbreviation to the defined full form.
- See also refers you to a related or contrasting term.

To view glossaries for other IBM products, go to www.ibm.com/software/globalization/terminology (opens in new window).

A

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

adapter
An intermediary software component that allows two other software components to communicate with one another.

application server
A server program in a distributed network that provides the execution environment for an application program.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

C

collector
A web service that accepts uploads of recordings and stores them into a permanent storage medium. This web service is a component of the session recording server.

credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

D

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

E

endpoint
The system that is the origin or destination of a session.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

F

frame A unit of information in a recording. A frame can either be a screen capture or information about mouse events, keyboard events, or other relevant events.

I

IMS Server
An integrated management system for ISAM ESSO that provides a central point of secure access administration for an enterprise. It enables centralized management of user identities, AccessProfiles, authentication policies, provides loss management, certificate management, and audit management for the enterprise.

M

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

P

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

provisioning policy
A policy that defines the access to various managed resources, such as applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

R

recording
A collection of information about user actions performed on a monitored application for some time.

recording agent
A shared library loaded into a monitored application's process space that captures frames.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

resource
A hardware, software, or data entity. See also managed resource.

retriever
A web application that provides access to stored recordings.

S

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, specific credential, all pool or credentials with the same organization container context.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

SSO See single sign-on.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

Index

V

W

X

Printed in USA

SC27-4382-02