IBM Security Access Manager for Web
Version 7.0.0.1

Installation Guide

GC23-6502-03

IBM Security Access Manager for Web
Version 7.0.0.1

Installation Guide

GC23-6502-03

Note
Before using this information and the product it supports, read the information in "Notices" on page 417.

Edition notice

Note: This edition applies to version 7, release 0, modification 0 of IBM Security Access Manager (product number 5724-C87) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Tables

About this publication

IBM Security Access Manager for Web, formerly called IBM Tivoli Access Manager for e-business, is a user authentication, authorization, and web single sign-on solution for enforcing security policies over a wide range of web and application resources.

IBM Security Access Manager for Web Installation Guide explains how to install and configure Security Access Manager, including Security Access Manager systems, session management systems, and web security systems.

Intended audience

This guide is for system administrators responsible for the installation and deployment of Security Access Manager.

Readers should be familiar with the following topics:

- Supported operating systems
- Database architecture and concepts
- Security management
- Internet protocols, including HTTP, TCP/IP, File Transfer Protocol (FTP), and Telnet
- Lightweight Directory Access Protocol (LDAP) and directory services
- Authentication and authorization

If you are enabling Secure Sockets Layer (SSL) communication, you also should be familiar with SSL protocol, key exchange (public and private), digital signatures, cryptographic algorithms, and certificate authorities.

Access to publications and terminology

This section provides:

- A list of publications in the "IBM Security Access Manager for Web library."
- Links to "Online publications" on page xv.
- A link to the "IBM Terminology website" on page xvi.

IBM Security Access Manager for Web library

The following documents are in the IBM Security Access Manager for Web library:

- *IBM Security Access Manager for Web Quick Start Guide*, GI11-9333-01

  Provides steps that summarize major installation and configuration tasks.
- *IBM Security Web Gateway Appliance Quick Start Guide* – Hardware Offering

  Guides users through the process of connecting and completing the initial configuration of the WebSEAL Hardware Appliance, SC22-5434-00
- *IBM Security Web Gateway Appliance Quick Start Guide* – Virtual Offering

  Guides users through the process of connecting and completing the initial configuration of the WebSEAL Virtual Appliance.
- *IBM Security Access Manager for Web Installation Guide*, GC23-6502-02

Explains how to install and configure Security Access Manager.

- *IBM Security Access Manager for Web Upgrade Guide*, SC23-6503-02

  Provides information for users to upgrade from version 6.0, or 6.1.x to version 7.0.

- *IBM Security Access Manager for Web Administration Guide*, SC23-6504-03

  Describes the concepts and procedures for using Security Access Manager. Provides instructions for performing tasks from the Web Portal Manager interface and by using the **pdadmin** utility.

- *IBM Security Access Manager for Web WebSEAL Administration Guide*, SC23-6505-03

  Provides background material, administrative procedures, and reference information for using WebSEAL to manage the resources of your secure Web domain.

- *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*, SC23-6507-02

  Provides procedures and reference information for securing your Web domain by using a Web server plug-in.

- *IBM Security Access Manager for Web Shared Session Management Administration Guide*, SC23-6509-02

  Provides administrative considerations and operational instructions for the session management server.

- *IBM Security Access Manager for Web Shared Session Management Deployment Guide*, SC22-5431-00

  Provides deployment considerations for the session management server.

- *IBM Security Web Gateway Appliance Administration Guide*, SC22-5432-01

  Provides administrative procedures and technical reference information for the WebSEAL Appliance.

- *IBM Security Web Gateway Appliance Configuration Guide for Web Reverse Proxy*, SC22-5433-01

  Provides configuration procedures and technical reference information for the WebSEAL Appliance.

- *IBM Security Web Gateway Appliance Web Reverse Proxy Stanza Reference*, SC27-4442-01

  Provides a complete stanza reference for the IBM® Security Web Gateway Appliance Web Reverse Proxy.

- *IBM Security Access Manager for Web WebSEAL Configuration Stanza Reference*, SC27-4443-01

  Provides a complete stanza reference for WebSEAL.

- *IBM Global Security Kit: CapiCmd Users Guide*, SC22-5459-00

  Provides instructions on creating key databases, public-private key pairs, and certificate requests.

- *IBM Security Access Manager for Web Auditing Guide*, SC23-6511-03

  Provides information about configuring and managing audit events by using the native Security Access Manager approach and the Common Auditing and Reporting Service. You can also find information about installing and configuring the Common Auditing and Reporting Service. Use this service for generating and viewing operational reports.

- *IBM Security Access Manager for Web Command Reference*, SC23-6512-03

  Provides reference information about the commands, utilities, and scripts that are provided with Security Access Manager.

- *IBM Security Access Manager for Web Administration C API Developer Reference*, SC23-6513-02

  Provides reference information about using the C language implementation of the administration API to enable an application to perform Security Access Manager administration tasks.
- *IBM Security Access Manager for Web Administration Java Classes Developer Reference*, SC23-6514-02

  Provides reference information about using the Java™ language implementation of the administration API to enable an application to perform Security Access Manager administration tasks.
- *IBM Security Access Manager for Web Authorization C API Developer Reference*, SC23-6515-02

  Provides reference information about using the C language implementation of the authorization API to enable an application to use Security Access Manager security.
- *IBM Security Access Manager for Web Authorization Java Classes Developer Reference*, SC23-6516-02

  Provides reference information about using the Java language implementation of the authorization API to enable an application to use Security Access Manager security.
- *IBM Security Access Manager for Web Web Security Developer Reference*, SC23-6517-02

  Provides programming and reference information for developing authentication modules.
- *IBM Security Access Manager for Web Error Message Reference*, GI11-8157-02

  Provides explanations and corrective actions for the messages and return code.
- *IBM Security Access Manager for Web Troubleshooting Guide*, GC27-2717-01

  Provides problem determination information.
- *IBM Security Access Manager for Web Performance Tuning Guide*, SC23-6518-02

  Provides performance tuning information for an environment that consists of Security Access Manager with the IBM Tivoli Directory Server as the user registry.

Online publications

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

IBM Security Access Manager for Web Information Center
: The http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.isam.doc_70/welcome.html site displays the information center welcome page for this product.

IBM Security Systems Documentation Central and Welcome page
: IBM Security Systems Documentation Central provides an alphabetical list of all IBM Security Systems product documentation and links to the product information center for specific versions of each product.

  Welcome to IBM Security Systems Information Centers provides and introduction to, links to, and general information about IBM Security Systems information centers.

IBM Publications Center

The http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss site offers customized search functions to help you find all the IBM publications that 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.

Related publications

This section lists the IBM products that are related to and included with the Security Access Manager solution.

Note: The following middleware products are not packaged with IBM Security Web Gateway Appliance.

IBM Global Security Kit

Security Access Manager provides data encryption by using Global Security Kit (GSKit) version 8.0.x. GSKit is included on the *IBM Security Access Manager for Web Version 7.0* product image or DVD for your particular platform.

GSKit version 8 includes the command-line tool for key management, GSKCapiCmd (**gsk8capicmd_64**).

GSKit version 8 no longer includes the key management utility, iKeyman (**gskikm.jar**). iKeyman is packaged with IBM Java version 6 or later and is now a pure Java application with no dependency on the native GSKit runtime. Do not move or remove the bundled *java*/jre/lib/gskikm.jar library.

The *IBM Developer Kit and Runtime Environment, Java Technology Edition, Version 6 and 7, iKeyman User's Guide for version 8.0* is available on the Security Access Manager Information Center. You can also find this document directly at:

http://download.boulder.ibm.com/ibmdl/pub/software/dw/jdk/security/60/iKeyman.8.User.Guide.pdf

Note:

GSKit version 8 includes important changes made to the implementation of Transport Layer Security required to remediate security issues.

The GSKit version 8 changes comply with the Internet Engineering Task Force (IETF) Request for Comments (RFC) requirements. However, it is not compatible with earlier versions of GSKit. Any component that communicates with Security Access Manager that uses GSKit must be upgraded to use GSKit version 7.0.4.42, or 8.0.14.26 or later. Otherwise, communication problems might occur.

IBM Tivoli Directory Server

IBM Tivoli Directory Server version 6.3 FP17 (6.3.0.17-ISS-ITDS-FP0017) is included on the *IBM Security Access Manager for Web Version 7.0* product image or DVD for your particular platform.

You can find more information about Tivoli Directory Server at:

http://www.ibm.com/software/tivoli/products/directory-server/

IBM Tivoli Directory Integrator

IBM Tivoli Directory Integrator version 7.1.1 is included on the *IBM Tivoli Directory Integrator Identity Edition V 7.1.1 for Multiplatform* product image or DVD for your particular platform.

You can find more information about IBM Tivoli Directory Integrator at:

http://www.ibm.com/software/tivoli/products/directory-integrator/

IBM DB2 Universal Database™

IBM DB2 Universal Database Enterprise Server Edition, version 9.7 FP4 is provided on the *IBM Security Access Manager for Web Version 7.0* product image or DVD for your particular platform. You can install DB2® with the Tivoli Directory Server software, or as a stand-alone product. DB2 is required when you use Tivoli Directory Server or z/OS® LDAP servers as the user registry for Security Access Manager. For z/OS LDAP servers, you must separately purchase DB2.

You can find more information about DB2 at:

http://www.ibm.com/software/data/db2

IBM WebSphere® products

The installation packages for WebSphere Application Server Network Deployment, version 8.0, and WebSphere eXtreme Scale, version 8.5.0.1, are included with Security Access Manager version 7.0. WebSphere eXtreme Scale is required only when you use the Session Management Server (SMS) component.

WebSphere Application Server enables the support of the following applications:

- Web Portal Manager interface, which administers Security Access Manager.
- Web Administration Tool, which administers Tivoli Directory Server.
- Common Auditing and Reporting Service, which processes and reports on audit events.
- Session Management Server, which manages shared session in a Web security server environment.
- Attribute Retrieval Service.

You can find more information about WebSphere Application Server at:

http://www.ibm.com/software/webservers/appserv/was/library/

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.

Visit the IBM Accessibility Center for more information about IBM's commitment to accessibility.

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 Access Manager for Web Troubleshooting Guide* provides details about:

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

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

Part 1. Installation planning

Chapter 1. Installation overview

It is important that you create a deployment plan before you install Security Access Manager software on the systems in your distributed environment.

If you already have Security Access Manager software installed, review your previous deployment plan to determine the best method for upgrading to the most current version. Follow the instructions that are provided in the *IBM Security Access Manager for Web Upgrade Guide*.

Note: For the latest release information, including system requirements, disk space and memory requirements, and known defects and limitations, see the Release Notes section of the IBM Security Access Manager for Web Information Center or Technotes in the support knowledge database.

Deployment planning

Before you implement a particular Security Access Manager solution, you must determine the specific security and management capabilities that are required for your network.

The first step in planning the deployment of a Security Access Manager security environment is to define the security requirements for your computing environment. Defining security requirements means determining the business policies that must apply to users, programs, and data. This definition includes:

- Objects to be secured
- Actions that are permitted on each object
- Users that are permitted to perform the actions

Enforcing a security policy requires an understanding of the flow of access requests through your network topology. In your plan, identify correct roles and locations for firewalls, routers, and subnets. Deploying a Security Access Manager security environment also requires identifying the optimal points within the network for installing software that evaluates user access requests, and grants or denies the requested access.

Implementation of a security policy requires understanding the number of users, quantity of data, and throughput that your network must accommodate. You must evaluate performance characteristics, scalability, and the need for failover capabilities. Integration of previous versions of software, databases, and applications with Security Access Manager software must also be considered.

After you have an understanding of the features that you want to deploy, you can decide which Security Access Manager systems you need in your environment.

For useful planning documentation, including actual business scenarios, see supplemental product information at the following websites:

http://www.ibm.com/redbooks/

http://www.ibm.com/software/sysmgmt/products/support/Field_Guides.html

Secure domain overview

The computing environment in which Security Access Manager enforces security policies for authentication, authorization, and access control is called a *secure domain*.

The initial secure domain, called the *management domain*, is created when you install and configure the following systems:

Policy server
Maintains the master authorization database for the management domain. In addition, it updates authorization database replicas and maintains location information about other Security Access Manager servers.

Registry
Provides a database of the user identities that are known to Security Access Manager. It also provides a representation of groups in Security Access Manager roles that are associated with users.

These core systems must exist for Security Access Manager to complete fundamental operations, such as permitting or denying user access to protected objects (resources). All other Security Access Manager services and components are built on this base.

You can deploy Security Access Manager on multiple systems or install all the software necessary to configure and use the management domain on one stand-alone system. A single system setup is useful only when prototyping a deployment or developing and testing an application.

After you configure the policy server and registry server, you can set up more systems in the management domain. For example, you could set up an authorization server or application development system. You can also create more secure domains (if you use an LDAP registry) to securely partition data into separate, logical groupings. For information about creating multiple domains, see the *IBM Security Access Manager for Web Administration Guide*.

Security Access Manager installation components

Security Access Manager includes base and prerequisite components that are generally common to all Security Access Manager installations.

Use these components to set up Security Access Manager systems that are listed in "Components and prerequisites for Security Access Manager systems" on page 12.

Note: When you install Security Access Manager on a Windows operating system, you can specify a nondefault installation path. Ensure that the installation path that you specify does not include any globalization characters.

Security Access Manager base components

The Security Access Manager base system includes specific installation components.

These components are on the product media for the supported platforms. Use these installation components to set up base systems that are listed in "Components and prerequisites for Security Access Manager systems" on page 12.

Security Access Manager Application Development Kit

The Security Access Manager Application Development Kit provides a development environment in which you can code third-party applications to query the authorization server for authorization decisions.

This kit contains support for using both C APIs and Java classes for authorization and administration functions. To run the Java program or to compile and run your own Java programs, you must install and configure a Security Access Manager Runtime for Java system.

Security Access Manager Authorization Server

The Security Access Manager Authorization Server provides access to the authorization service for third-party applications that use the Security Access Manager authorization API in remote cache mode.

The authorization server also acts as a logging and auditing collection server to store records of server activity.

Security Access Manager Policy Proxy Server

The Security Access Manager Policy Proxy Server acts as an intermediary between a less trusted network and a more trusted network.

This server ensures security and provides administrative control and caching services. It is associated with, or part of:

- A gateway server that separates the enterprise network from the outside network.
- A firewall server that protects the enterprise network from outside intrusion.

In a Security Access Manager environment, the proxy server runs on behalf of the policy server for a specified number of authorization applications and administrative functions, such as **pdadmin** commands.

Security Access Manager Policy Server

The Security Access Manager Policy Server maintains the master authorization database for the management domain. It also maintains the policy databases that are associated with other secure domains that you might decide to create.

This server is key to the processing of access control, authentication, and authorization requests. It also updates authorization database replicas and maintains location information about other Security Access Manager servers.

Security Access Manager supports the use of one *standby* policy server on a supported platform.

In environments with a standby policy server, if the primary policy server goes down, the standby policy server takes over. It acts as the primary policy server until the primary policy server assumes its original role. In turn, the standby policy server reverts to a standby role. At any time, there is *only one* active policy server and *only one* shared copy of the policy databases.

If you want to set up a standby policy server, complete one of the following procedures:

- Appendix G, “Standby policy server (AIX) setup,” on page 357
- Appendix H, “Setup for a standby policy server with IBM Tivoli System Automation for Multiplatforms,” on page 373

Security Access Manager Runtime

The Security Access Manager Runtime contains runtime libraries and supporting files that applications can use to access Security Access Manager servers.

You must install and configure the Security Access Manager Runtime component on each system that runs Security Access Manager, except for:

- IBM Security Access Manager Runtime for Java systems
- Security Access Manager Attribute Retrieval Service systems
- Distributed sessions management systems

IBM Security Utilities

The IBM Security Utilities provides common utilities that are required by Security Access Manager Runtime.

This component is provided separately for each supported platform.

IBM Security Access Manager Runtime for Java

The IBM Security Access Manager Runtime for Java offers a reliable environment for developing and deploying Java applications in a Security Access Manager secure domain. Use it to add Security Access Manager authorization and security services to new or existing Java applications.

You can use the **pdjrtecfg** command to configure a Java Runtime Environment (JRE) to use Security Access Manager Java security.

If you plan to install the Web Portal Manager interface, this component is required. It is also required with the Security Access Manager Application Development Kit component if you are a developer using IBM Security Access Manager Runtime for Java classes. For more information, see the *IBM Security Access Manager for Web: Administration Java Classes Developer Reference* and the *IBM Security Access Manager for Web: Authorization Java Classes Developer Reference*.

Security Access Manager Web Portal Manager

The Security Access Manager Web Portal Manager is a web-based graphical user interface (GUI) used for Security Access Manager administration.

The GUI counterpart to the **pdadmin** command-line interface, Web Portal Manager provides management of users, groups, roles, permissions, policies, and other Security Access Manager tasks. A key advantage of using Web Portal Manager is that you can complete these tasks remotely, without requiring any special network configuration.

The Web Portal Manager interface also includes a set of delegated management services that enables a business to delegate user administration, group and role administration, security administration, and application access provisioning to

participants (subdomains) in the business system. These subdomains can further delegate management and administration to trusted subdomains under their control.

See the Release Notes in the Security Access Manager Information Center for a list of browsers that you can use with Web Portal Manager.

Security Access Manager License

This component contains license information for Security Access Manager. This component is provided separately for each supported platform.

Security Access Manager Web security components

Security Access Manager Web security includes several installation components.

These components are provided on the product media for each supported platforms. Use these installation components to set up Web security systems that are listed in "Security Access Manager Web security systems" on page 14.

Security Access Manager Attribute Retrieval Service

The Security Access Manager Attribute Retrieval Service is used with the WebSEAL authorization decision information (ADI) feature.

This service provides communication and format translation services between the WebSEAL entitlement service library and an external provider of authorization decision information. For more information, see the *IBM Security Access Manager for Web WebSEAL Administration Guide*.

Security Access Manager Plug-in for Web Servers

Security Access Manager Plug-in for Web Servers manages the security of your web-based resources by acting as the gateway between your clients and secure Web space.

The plug-in implements the security policies that protect your Web object space. The plug-in can provide single sign-on solutions, support Web servers running as virtual hosts and incorporate Web application server resources into its security policy. For more information, see the *IBM Security Access Manager for Web: Plug-in for Web Servers Administration Guide*.

Security Access Manager Web Security Runtime

The Security Access Manager Web Security Runtime contains shared authentication library files that are used for Web Security systems.

These shared files include Security Access Manager WebSEAL and the Security Access Manager Plug-in for Web Servers.

Security Access Manager Web Security Application Development Kit

The Security Access Manager Web Security ADK contains development APIs for Web Security components.

The APIs include Security Access Manager cross-domain authentication service (CDAS), the Security Access Manager cross-domain mapping framework (CDMF), and the Security Access Manager password strength module.

Security Access Manager WebSEAL

Security Access Manager WebSEAL is a security manager for web-based resources. WebSEAL is a high performance, multithreaded web server that applies fine-grained security policy to the protected web object space.

WebSEAL can provide single sign-on solutions and incorporate back-end web application server resources into its security policy.

Security Access Manager distributed sessions management components

The Security Access Manager distributed sessions management systems includes several installation components.

These components are on the product media for each of the supported platforms. Use these installation components to set up distributed sessions management systems that are listed in "Components and prerequisites for Security Access Manager systems" on page 12.

Security Access Manager Session Management Server

Security Access Manager Session Management Server (SMS) is an optional Security Access Manager component that runs as an IBM WebSphere Application Server service.

It manages user sessions across complex clusters of Security Access Manager security servers, ensuring that session policy remains consistent across the participating servers. The session management server allows Security Access Manager WebSEAL and the Security Access Manager Plug-in for Web Servers to share a unified view of all current sessions and enables an authorized user to monitor and administer user sessions. The session management server:

- Enables sharing of session information.
- Makes session statistics available.
- Provides secure and high-performance failover and single sign-on capabilities for clustered environments.

Administer and manage user sessions with the Security Access Manager Session Management Command Line or the Session Management Server console.

Security Access Manager Session Management Command Line

You can administer the session management server with the Security Access Manager Session Management Command Line component.

Use either the **pdadmin** command-line utility on the specified Security Access Manager authorization server, or use the **pdsmsadmin** utility.

Note: If you want to use **pdadmin** to administer the session management server, you must first install and configure the authorization server before you install the command-line interface.

Prerequisite products

Security Access Manager includes several products that are required when you set up specific Security Access Manager systems.

For a list of required installation components necessary to set up a Security Access Manager system, see Table 1 on page 13.

IBM Global Security Kit (GSKit)

IBM Global Security Kit (GSKit) provides Secure Sockets Layer (SSL) data encryption between Security Access Manager systems and supported registry servers.

The GSKit package also installs the GSKCapiCmd tool, which you can use to create key databases, public-private key pairs, and certificate requests.

You must install GSKit before you install most other Security Access Manager components. GSKit is a prerequisite to the Security Access Manager Runtime component, which is required on all Security Access Manager systems except for the Security Access Manager Attribute Retrieval Service, IBM Security Access Manager Runtime for Java, Security Access Manager Session Management Server or Security Access Manager Web Portal Manager.

Note: Previous versions of GSKit included a utility called **ikeyman**. This utility is part of IBM Java. For more information, see the *IBM Developer Kit and Runtime Environment, Java Technology Edition, Version 6 and 7 iKeyman User's Guide for version 8.0* http://download.boulder.ibm.com/ibmdl/pub/software/dw/jdk/security/60/iKeyman.8.User.Guide.pdf.

IBM Java Runtime

The IBM Java Runtime provided with Security Access Manager is required when you install and use language support packages.

The IBM Security Access Manager Runtime for Java component supports the IBM Java Runtime only.

IBM Tivoli® Directory Server client

You must install the IBM Tivoli Directory Server client on most Security Access Manager systems.

The client application is provided on the product media for the supported platforms.

You must install the IBM Tivoli Directory Server client on each system that runs Security Access Manager, with the following exceptions:

- The Security Access Manager system is on a supported Windows system that is either the Active Directory domain or is joined to the Active Directory domain where the Security Access Manager policy server is to be configured.
- You are setting up the Security Access Manager Attribute Retrieval Service, IBM Security Access Manager Runtime for Java, or Security Access Manager Web Portal Manager.

IBM Tivoli Directory Server

The IBM Tivoli Directory Server is one of several user registry options you have for your Security Access Manager environment. IBM Tivoli Directory Server provides an easy way to maintain directory information in a central location for storage, updates, retrieval, and exchange.

IBM Tivoli Directory Server is provided on the product media for the supported platforms. You can use this server as your Security Access Manager registry server or use one of the registry servers that is listed in "Supported registries." This Lightweight Directory Access Protocol (LDAP) directory runs as a stand-alone daemon. It is based on a client/server model that provides client access to an LDAP server.

IBM Tivoli Directory Server Web Administration Tool

IBM Tivoli Directory Server provides a Web Administration Tool for its administration.

This tool is an optional graphical user interface that runs on an application server, such as the IBM WebSphere Application Server. Use the Web Administration Tool to administer IBM Tivoli Directory Servers locally or remotely. You can install a single Web Administration console to manage multiple versions of IBM Tivoli Directory Server.

The Web Administration Tool is provided with the IBM Tivoli Directory Server product files.

IBM WebSphere Application Server

IBM WebSphere Application Server is required by several Security Access Manager components.

These components include:

- The Security Access Manager Web Portal Manager
- The Security Access Manager session management server
- The Security Access Manager Attribute Retrieval Service

IBM WebSphere Application Server is on its own product media for the supported platforms.

Note: IBM Tivoli Directory Server, on Windows systems only, includes the embedded version of IBM WebSphere Application Server for use with its Web Administration Tool.

The same WebSphere Application Server can be used for Web Portal Manager and the IBM Tivoli Directory Server Web Administration Tool.

Supported registries

Security Access Manager supports several user registries, their supported operating systems, and any prerequisite software.

See the IBM Security Access Manager for Web Information Center or Technotes in the support knowledge database to ensure that you reviewed the most recent

release information, including system requirements, disk space requirements, and known defects and limitations. Ensure that all necessary operating system patches are installed.

IBM Tivoli Directory Server

Security Access Manager supports the use of IBM Tivoli Directory Server as a registry.

Take note of the following information:

- IBM Tivoli Directory Server is included with Security Access Manager.
- IBM Tivoli Directory Server client is required when an LDAP user registry is selected during installation.
- You can install the IBM Tivoli Directory Server client on the same system as a previous version (such as 6.2, 6.1, or 6.0) of the IBM Tivoli Directory Server client.

Attention: If you have an existing IBM Tivoli Directory Server that you want to use for Security Access Manager, ensure that you upgrade the server to a supported level. For upgrade instructions, see the *IBM Security Access Manager for Web Upgrade Guide*.

IBM Tivoli Directory Server for z/OS

Security Access Manager supports the use of IBM Tivoli Directory Server for z/OS.

For product information, see the z/OS Internet Library website at:

http://www.ibm.com/servers/eserver/zseries/zos/bkserv/

Customers can also obtain softcopy publications on DVD *z/OS: Collection*, SK3T-4269.

Microsoft Active Directory

Security Access Manager supports the use of Microsoft Active Directory as a user registry.

Active Directory users can run Security Access Manager on all platforms that are currently supported in the Security Access Manager 7.0 product.

AIX, Linux, and Solaris platforms use the IBM Tivoli Directory Server client to communicate with Active Directory. This LDAP client is also used on Windows platforms where the Active Directory domain of the local host is different from the Active Directory domain where the policy server is to be configured.

Microsoft Active Directory Lightweight Directory Service (ADLDS)

Security Access Manager supports the use of Microsoft Active Directory Lightweight Directory Service as a user registry.

ADLDS users can run Security Access Manager with supported versions of Windows Server. See the Security Access Manager Release Notes in the information center for the list of supported versions.

Sun Java System Directory Server

Security Access Manager supports the use of the Sun Java System Directory Server as a user registry.

For installation information, consult the product documentation that came with your server. Sun Java System Directory Server product documentation is available at:

http://docs.sun.com/app/docs/prod/entsys

Novell eDirectory

Security Access Manager supports the use of Novell eDirectory as a user registry.

For installation information, consult the product documentation that came with your Novell eDirectory server. Novell eDirectory product documentation is available at:

http://www.novell.com/documentation/a-z.html

The latest patches to these products are available at:

http://support.novell.com/patches.html

Attention: If you have an existing Novell eDirectory server that you want to use for Security Access Manager, ensure that you upgrade the server to a supported level.

Components and prerequisites for Security Access Manager systems

All Security Access Manager deployments include several types of Security Access Manager systems that are set up in a secure domain.

Required installation components for each system type are provided with Security Access Manager. To retain flexibility and ensure efficient load balancing, consider setting up the policy server on a system that is separate from your registry server. However, other system types do not have to be stand-alone systems. For example, you can install the Web Portal Manager interface on the same system as the policy server.

Security Access Manager base systems

Each Security Access Manager base system has specific component requirements.

Table 1 on page 13 lists the types of Security Access Manager base systems that you can set up in your secure domain.

Note: You must install the IBM Tivoli Directory Server client on each system that runs Security Access Manager, with the following exceptions:

- The Security Access Manager system is on a supported Windows system that is either the Active Directory domain or is joined to the Active Directory domain where the Security Access Manager policy server is to be configured.
- You are setting up the Security Access Manager Attribute Retrieval Service, IBM Security Access Manager Runtime for Java, or Security Access Manager Web Portal Manager.

Table 1. Required components for the Security Access Manager base systems

System type	Installation components
Authorization server	• IBM Global Security Kit (GSKit) • IBM Tivoli Directory Server client (depending on the registry used) • Security Access Manager License • IBM Security Utilities • Security Access Manager Runtime • Security Access Manager Authorization Server
Development (ADK)	• IBM Global Security Kit (GSKit) • IBM Tivoli Directory Server client (depending on the registry used) • Security Access Manager License • IBM Security Utilities • Security Access Manager Runtime • Security Access Manager Application Development Kit
IBM Tivoli Directory Server	If you plan to install the IBM Tivoli Directory Server as your Security Access Manager registry, the following components are required: • IBM Global Security Kit (GSKit) • DB2 Enterprise Server Edition • IBM Tivoli Directory Server client • IBM Tivoli Directory Server server
Runtime for Java	• Security Access Manager License • IBM Java • IBM Security Access Manager Runtime for Java
Policy proxy server	• IBM Global Security Kit (GSKit) • IBM Tivoli Directory Server client (depending on the registry used) • Security Access Manager License • IBM Security Utilities • Security Access Manager Runtime • Security Access Manager Policy Proxy Server
Policy server	• IBM Global Security Kit (GSKit) • IBM Tivoli Directory Server client (depending on the registry used) • Security Access Manager License • IBM Security Utilities • Security Access Manager Runtime • Security Access Manager Policy Server
Runtime	• IBM Global Security Kit (GSKit) • IBM Tivoli Directory Server client (depending on the registry used) • Security Access Manager License • IBM Security Utilities • Security Access Manager Runtime

Table 1. Required components for the Security Access Manager base systems (continued)

System type	Installation components
Web Portal Manager	• IBM WebSphere Application Server (on separate DVD and Passport Advantage® image) • Security Access Manager License • IBM Java • IBM Security Access Manager Runtime for Java • Security Access Manager Web Portal Manager

Security Access Manager Web security systems

Each Security Access Manager web security system has specific component requirements.

Table 2 lists types of Web security systems that you can set up in your secure domain. Installation components for these systems are provided on the product media for your particular operating system.

Note: You must install the IBM Tivoli Directory Server client on each system that runs Security Access Manager, with the following exceptions:

- The Security Access Manager system is on a supported Windows system that is either the Active Directory domain or is joined to the Active Directory domain where the Security Access Manager policy server is to be configured.
- You are setting up Security Access Manager Attribute Retrieval Service, IBM Security Access Manager Runtime for Java, or Security Access Manager Web Portal Manager.

Table 2. Required components for the Security Access Manager Web security systems

System type	Installation components
Attribute Retrieval Service	• IBM WebSphere Application Server (on separate DVD and Passport Advantage image) • Security Access Manager Attribute Retrieval Service
WebSEAL	• IBM Global Security Kit (GSKit) • IBM Tivoli Directory Server client (depending on the registry used) • Security Access Manager License • IBM Security Utilities • Security Access Manager Runtime • Security Access Manager Web Security Runtime • Security Access Manager WebSEAL

Table 2. Required components for the Security Access Manager Web security systems (continued)

System type	Installation components
Web Security Application Development Kit (ADK) system	• IBM Global Security Kit (GSKit) • IBM Tivoli Directory Server client (depending on the registry used) • Security Access Manager License • IBM Security Utilities • Security Access Manager Runtime • Security Access Manager Application Development Kit • Security Access Manager Web Security Runtime • Security Access Manager Web Security Application Development Kit
Plug-in for Apache Web Server	• Apache Web Server (not provided with the Security Access Manager product) • IBM Global Security Kit (GSKit) • IBM Tivoli Directory Server client (depending on the registry used) • Security Access Manager License • IBM Security Utilities • Security Access Manager Runtime • Security Access Manager Web Security Runtime • Security Access Manager Plug-in for Web Servers • Security Access Manager Plug-in for Apache Web Server
Plug-in for IBM HTTP Server	• IBM HTTP Server (not provided with the Security Access Manager product) • IBM Global Security Kit (GSKit) • IBM Tivoli Directory Server client (depending on the registry used) • Security Access Manager License • IBM Security Utilities • Security Access Manager Runtime • Security Access Manager Web Security Runtime • Security Access Manager Plug-in for Web Servers • Security Access Manager Plug-in for IBM HTTP Server
Plug-in for Internet Information Services	• Internet Information Services (not provided with the Security Access Manager product) • IBM Global Security Kit (GSKit) • IBM Tivoli Directory Server client (depending on the registry used) • Security Access Manager License • IBM Security Utilities • Security Access Manager Runtime • Security Access Manager Web Security Runtime • Security Access Manager Plug-in for Web Servers • Security Access Manager Plug-in for Internet Information Services

Security Access Manager distributed sessions management systems

Each Security Access Manager session management system has specific component requirements.

Table 3 lists types of session management systems that you can set up in your secure domain. Installation components for these systems are provided on the product media for your particular platform.

Note: You must install the IBM Tivoli Directory Server client on each system that runs Security Access Manager, with the following exceptions:

- The Security Access Manager system is on a supported Windows system that is either the Active Directory domain or is joined to the Active Directory domain where the Security Access Manager policy server is to be configured.
- You are setting up Security Access Manager Attribute Retrieval Service, IBM Security Access Manager Runtime for Java, or Security Access Manager Web Portal Manager.

Table 3. Required components for the Security Access Manager session management systems

System type	Installation components
Session Management Server	• IBM WebSphere Application Server (on separate DVD or Passport Advantage image) • Security Access Manager License • Security Access Manager Session Management Server
Session Management Command Line	• IBM Global Security Kit (GSKit) • Security Access Manager Session Management Command Line • Security Access Manager License • IBM Security Utilities If you want to use the Security Access Manager **pdadmin** utility to administer sessions, the following components are also required: • Security Access Manager License • Security Access Manager Runtime • Security Access Manager Authorization Server • Security Access Manager Session Management Command Line • IBM Tivoli Directory Server client (depending on the registry used)

SSL and TLS compliance enablement

You can configure Security Access Manager to comply with various security standards. These standards are typically used to meet security requirements, such as those required by the US government.

Security Access Manager uses cryptography in the following areas:

- To create and replace internal, self-signed certificates. These certificates are used by Security Access Manager Runtime and Security Access Manager server to authenticate with each other.
- Secure communication between the runtime and servers.
- Secure communication to LDAP.
- Secure communication to Syslog servers.

The following security standards are required by the government:

FIPS 140-2

Federal Information Processing Standards (FIPS) that specify requirements on cryptographic modules. For more information, see the National Institute of Standards and Technology websitehttp://csrc.nist.gov/publications/PubsFIPS.html.

SP800-131

A requirement from the National Institute of Standards and Technology (NIST) that requires longer key lengths and stronger cryptography. The specification also provides a transition configuration to enable users to move to a strict enforcement of SP800-131. SP800-131 can be run in two modes, `transition` and `strict`.

Strict enforcement of SP800-131 requirements is:

- The use of TLSv1.2 protocol.
- Certificates must have a minimum length of 2048. Elliptical Curve (EC) certificate require a minimum size of 244-bit curves.
- Certificates must be signed with a signature algorithm of SHA256, SHA384, or SHA512. Valid signature algorithms include:
  - SHA256withRSA
  - SHA384withRSA
  - SHA512withRSA
  - SHA256withECDSA
  - SHA384withECDSA
  - SHA512withECDSA
  - SP800-131 approved Cipher suites

  For more information about this standard, see the National Institute of Standards and Technology website http://csrc.nist.gov/publications/PubsSPs.html.

Suite B

A requirement from the National Security Agency (NSA) to specify a cryptographic interoperability strategy. This standard is similar to SP800-131 with some tighter restrictions. Suite B can run in two modes: 128-bit or 192-bit. If you are using 192-bit mode with Security Access Manager Java applications, you must apply the unrestricted policy file to the JDK to use the stronger cipher that mode requires.

Suite B requirements are:

- The use of TLSv1.2 protocol.
- Suite B approved Cipher suites
- Certificates:
  - 128-bit mode certificates must be signed with SHA256withECDSA
  - 192-bit mode certificates must be signed with SHA384withECDSA
- Ciphers:
  - SSL_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - SSL_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Chapter 2. Installation methods

You have several choices for installing the Security Access Manager components and their prerequisite software.

The following tables describe the methods for each operating system.

Table 4. Installation methods for AIX, Linux, or Solaris

Method	Description
Command line	Provides platform-specific utilities to install Security Access Manager components. Using this method, you must manually install each component and its prerequisite software in the appropriate order.
Script	Provides the sample scripts for an unattended (silent) installation. When you run the script for each component, all prerequisites for that component are also installed. If the prerequisites are already installed, the script skips that installation and continues with the next installation until all prerequisites are installed. **Note:** You cannot install the Attribute Retrieval Service with the script. Use the command-line method.

Table 5. Installation methods for Windows

Method	Description
Launchpad	Provides a graphical user interface for step-by-step installation and the initial configuration. You can complete the following installation tasks with the Launchpad: • Install the prerequisite software, such as IBM Java Runtime and GSKit. • Install Tivoli Directory Server (if you want to use it as your user registry). • Install the Security Access Manager components. • Start the interactive configuration tool (pdconfig). **Note:** You cannot install the Attribute Retrieval Service with the launchpad. Use the command-line method.
Command line	Provides a Windows command that opens a graphical installer to install Security Access Manager components. Using this method, you must manually install each component and its prerequisite software in the appropriate order.

Table 5. Installation methods for Windows (continued)

Method	Description
Script	Provides the sample scripts for an unattended (silent) installation. When you run the script for each component, all prerequisites for that component are also installed. **Note:** You cannot install the Attribute Retrieval Service with the script. Use the command-line method.

Chapter 3. Installation roadmap

Use this step-by-step plan to set up your Security Access Manager environment.

Procedure

1. Plan your installation.

Table 6. Planning tasks

Task	For more information
Plan your Security Access Manager deployment. Ensure that you understand the business security requirements for which Security Access Manager is being deployed.	"Deployment planning" on page 3
Decide which combination of Security Access Manager systems you want to install. A supported registry and the policy server system are required to set up the initial management domain.	"Secure domain overview" on page 4
Decide which type of user registry to use.	"Supported registries" on page 10
Take note of which components you must install for your deployment.	"Components and prerequisites for Security Access Manager systems" on page 12
Choose an installation method.	Chapter 2, "Installation methods," on page 19

2. Prepare your systems for installation and install the prerequisite software.

Table 7. Prerequisite tasks

Task	For more information
Prepare your operating system for installation.	"Operating system preparation" on page 28
Determine the prerequisite tasks for your environment and installation method and complete those tasks.	Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

3. Install and configure the base system components.
   a. Install the policy server component to establish your management domain.

Table 8. Policy server tasks

Task	For more information
Install the policy server.	Chapter 6, "Setting up a policy server," on page 103
If you plan to use a standby policy server, install and configure it.	• Appendix G, "Standby policy server (AIX) setup," on page 357. • Appendix H, "Setup for a standby policy server with IBM Tivoli System Automation for Multiplatforms," on page 373

   b. Install and configure other Security Access Manager base systems as needed in your deployment.

Table 9. Base system component tasks

Task	For more information
Install and configure Security Access Manager Authorization Server.	Chapter 7, "Authorization server setup," on page 121
Install and configure Security Access Manager Application Development Kit (ADK).	Chapter 8, "Setting up a development system," on page 135
Install and configure IBM Security Access Manager Runtime for Java.	Chapter 9, "Setting up a IBM Security Access Manager Runtime for Java system," on page 145
Install and configure Security Access Manager Policy Proxy Server.	Chapter 10, "Setting up a policy proxy server system," on page 157
Install and configure Security Access Manager Runtime.	Chapter 11, "Setting up a runtime system," on page 169
Install and configure Security Access Manager Web Portal Manager.	Chapter 12, "Setting up a Web Portal Manager system," on page 181

4. Install Security Access Manager web security systems as needed in your deployment.

Table 10. Web security system component tasks

Task	For more information
Install and configure Security Access Manager Attribute Retrieval Service.	Chapter 13, "Setting up the Security Access Manager Attribute Retrieval Service," on page 207
Install and configure Security Access Manager Plug–in for Web Servers.	Chapter 14, "Setting up the plug-in for Web servers," on page 213
Install and configure Security Access Manager Web Security Application Development Kit (ADK).	Chapter 15, "Setting up a Web security development system," on page 235
Install and configure Security Access Manager WebSEAL.	Chapter 16, "Setting up WebSEAL," on page 247

5. Install Security Access Manager distributed sessions management systems as needed in your deployment.

Table 11. Session management tasks

Task	For more information
Install Security Access Manager Session Management Server.	Chapter 17, "Setting up a session management server," on page 263
Install Security Access Manager Session Management Command Line.	"Setting up the session management command line using the command-line utilities" on page 291

6. Use a certificate from a certificate authority (CA) to enable SSL communication between your supported registry server and IBM Tivoli Directory Server clients. See Appendix A, "Secure Sockets Layer (SSL) security setup," on page 305.
7. Optional: Install IBM Tivoli Directory Integrator if you need its capabilities in your environment.

   Tivoli Directory Integrator can enhance the security, accuracy, and integrity of generic and user identity data. It facilitates data migration, transformation to

other file formats, and synchronization between two or more systems. It also provides the IBM Tivoli Directory Integrator 7.1.1 Connector for Security Access Manager.

The connector enables the provisioning and management of Security Access Manager data sources to external applications. The data sources include:

- User accounts
- Groups
- Policies
- Domains
- SSO resources
- SSO resource groups
- SSO user credentials

The Connector uses the Security Access Manager Java API. For information about this connector and about the installation of Tivoli Directory Integrator (including system requirements), see the installation chapter in the*IBM Tivoli Directory Integrator Installation and Administrator Guide*. It is available in the Information Center http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDI.doc_7.1/toc.xml.

Part 2. Prerequisite software installation

Chapter 4. Prerequisite installation and configuration roadmap

Before you install Security Access Manager components, the systems in your environment must meet the installation requirements.

1. Complete the tasks in "Operating system preparation" on page 28.
2. The next steps depend on the following environment variables:
   - The operating system on which you are installing the components.
   - The installation method you plan to use.
   - The user registry you plan to use.

   See the table to determine your next steps.

Table 12. Tasks for installing and configuring prerequisite software

Operating system and component installation method	**Prerequisite tasks**
Windows using the LaunchPad	1. Set up your user registry. See Chapter 5, "User registry server installation and configuration," on page 51. 2. Install the components: • Part 3, "Base system component installation," on page 101 • Part 4, "Web security system component installation," on page 205 • Part 5, "Session management system component installation," on page 261
Windows, AIX, Linux, or Solaris using the script files	1. Set up your user registry. See Chapter 5, "User registry server installation and configuration," on page 51. 2. Install the components: • Part 3, "Base system component installation," on page 101 • Part 4, "Web security system component installation," on page 205 • Part 5, "Session management system component installation," on page 261

Table 12. Tasks for installing and configuring prerequisite software (continued)

Operating system and component installation method	Prerequisite tasks
Windows, AIX, Linux, or Solaris using the command line	1. Set up all software that is required for your environment. a. See "Components and prerequisites for Security Access Manager systems" on page 12. Make a note of which software you must install. b. Install the required software: • "IBM Java Runtime installation" on page 31 • "IBM Global Security Kit (GSKit) installation" on page 34 • "IBM Security Access Manager License installation" on page 37 • "IBM Security Utilities installation" on page 39 • "IBM Tivoli Directory Server client installation" on page 42 • "Installing WebSphere Application Server" on page 46 2. Set up the user registry. See Chapter 5, "User registry server installation and configuration," on page 51. 3. Install the components: • Part 3, "Base system component installation," on page 101 • Part 4, "Web security system component installation," on page 205 • Part 5, "Session management system component installation," on page 261

Operating system preparation

Before you begin the installation of the prerequisite software, ensure that your operating system is properly prepared.

Ensure that you have reviewed the most recent release information, including operating system patch requirements, system requirements, disk space requirements, and known defects and limitations. See the Release Notes in the information center and the Technotes in the support knowledge database.

- "Preparing an AIX system"
- "Preparing a Linux system" on page 29
- "Preparing a Windows system" on page 30
- "Preparing a Solaris system" on page 31

Preparing an AIX system

Before you install the prerequisite software on an AIX system, complete the steps in this task to ensure that the system is set up correctly.

Procedure

1. Review the most recent release information, including operating system patch requirements, system requirements, disk space requirements, and known defects and limitations. See the Release Notes in the information center and the Technotes in the support knowledge database.
2. Verify that your system is using 64-bit hardware. At a command prompt, enter:

   ```
   bootinfo –y
   ```

   If results display 64, your hardware is 64-bit. In addition, if you type the command **lsattr -El proc0**, the output of the command returns the type of processor for your server. The following types of processors are 64-bit: RS64 I, II, III, IV, POWER3, POWER3 II, POWER4 or POWER5
3. Verify that your system is using a 64-bit kernel. At a command prompt, enter:

   ```
   bootinfo –K
   ```

   If results display 64, the kernel is 64-bit. However, if results display 32, you must switch from the 32-bit kernel to 64-bit kernel. To do so, follow these steps:

   a. Ensure that you have the following 64-bit packages:

      ```
      bos.64bit
      bos.mp64
      ```

   b. To switch to the 64-bit kernel, enter the following commands:

      ```
      ln -sf /usr/lib/boot/unix_64 /unix
      ln -sf /usr/lib/boot/unix_64 /usr/lib/boot/unix
      lslv -m hd5
      ```

      The output of the **lslv** command is similar to the following output:

      ```
      #lslv -m hd5
      hd5:N/A
      LP PP1 PV1PP2 PV2PP3 PV3
      0001 0001 hdisk0
      ```

   c. Enter:

      ```
      bosboot -ad /dev/ipldevice
      ```

      where *ipldevice* is the hard disk device that is shown by running the **lslv** command. The output from the **bosboot** command is similar to the following output:

      ```
      #bosboot -ad/dev/hdisk0
      bosboot: Boot image is 13025 512 byte blocks
      ```

   d. Enter:

      ```
      shutdown -Fr
      ```
4. Ensure that asynchronous I/O is enabled. To do so, enter the following commands:

   ```
   /usr/sbin/mkdev -l aio0
   /usr/sbin/chdev -l aio0 -P
   /usr/sbin/chdev -l aio0 -P -a autoconfig=available
   ```
5. Optional: If you plan to install Tivoli Directory Server on AIX 6.1, you must upgrade to AIX 6.1 TL 2 or higher, which is required by DB2 9.7. See the DB2 documentation for up-to-date system requirements of IBM DB2 9.7: http://www.ibm.com/software/data/db2/udb/sysreqs.html

Preparing a Linux system

Before you install the prerequisite software on a Linux system, complete steps in this task to ensure that the system is set up correctly.

Procedure

1. **On Linux systems only (all operating systems)**, complete the following tasks:
   a. Review the most recent release information, including operating system patch requirements, system requirements, disk space requirements, and known defects and limitations. See the Release Notes in the information center and the Technotes in the support knowledge database.
   b. On certain versions of Linux, the Linux installation program does not install the Korn shell (`/bin/ksh`). Install the `ksh rpm` file that matches the hardware on which you are installing Security Access Manager. The appropriate `rpm` file can be found on the Linux installation media or downloaded from the specific Linux (SUSE, Red Hat, and so on) support web sites. If the `ksh rpm` file is not installed, scripts might fail to run during Security Access Manager configuration. An error is displayed stating that `/bin/ksh` was not found.
   c. If you installed the Red Hat Enterprise Linux operating system with `SELINUX` enabled (which is the default), instance creation fails. If the `SELINUX` setting is enabled, use the `setenforce 0` command to disable it. Then, in the `/etc/selinux/config` file, change `SELINUX=enforcing` to `SELINUX=disabled`
   d. If you are installing Tivoli Directory Server, you might need to manually specify some DB2 settings before you install Tivoli Directory Server. The settings include the preliminary kernel, operating system, and shell parameters. See the DB2 documentation for instructions on setting these parameters: http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/index.jsp
   e. Install any operating system requirements that are necessary for the version of DB2 that you are using. For DB2 requirements, go to http://www.ibm.com/software/data/db2/udb/sysreqs.html
   f. To install IBM Java Runtime successfully on a Red Hat Enterprise Linux 5 system, ensure that the following compatibility library is installed:

      ```
      compat-libstdc-++-33-3.2.3
      ```

2. **On Linux 64-bit systems only**, install the following 32-bit libraries from the *i686.rpm packages:

   ```
   ld-linux.so.2
   libstdc++.so.6
   ```

3. **On Linux on System z systems only**, complete the following tasks:
   a. Obtain access to the Linux `rpm` files from the product media for Linux on System z®. The `rpm` files are in the */package_path*`/linux_s390` directory.
   b. Ensure that you are using the 64-bit kernel: Enter the following command:

      ```
      uname -m
      ```

      If the result displays `s390x`, you are running a 64-bit kernel.

      If the result displays `s390`, you are not running a 64-bit kernel.
   c. IBM requires the machine network node hostname. To ensure that your system is set up correctly, enter the following command:

      ```
      uname -n
      ```

      If the result displays a node hostname, you can proceed to install and configure Security Access Manager. If it does not, see your operating system documentation for instructions on setting up the machine network node hostname.

Preparing a Windows system

Before you start prerequisite installation on a Windows system, complete steps in this task to ensure that the system is set up correctly.

Procedure

1. Review the most-recent release information, including operating system patch requirements, system requirements, disk space requirements, and known defects and limitations. See the Release Notes in the information center and the Technotes in the support knowledge database.
2. All of the Security Access Manager installation methods on a Windows system require IBM Java. Before you begin an installation, ensure that IBM Java is available in the environment. Take one of the following actions:
   - Allow the installation method (command line, Launchpad, or script) to install IBM Java for you. Continue with Chapter 6, "Setting up a policy server," on page 103 using your choice of installation method.
   - Install IBM Java before you start an installation procedure. See "Windows: Installing IBM Java Runtime" on page 34.
   - Make sure the path to an installation of Java is specified in the `PATH` variable of your environment. For example, at a Windows command prompt type:

     ```
     set Path=c:\Program Files\IBM\Java60\jre\bin;%Path%
     ```

Preparing a Solaris system

Before you install the prerequisite software on a Solaris system, complete the steps in this task to ensure that the system is set up correctly.

Procedure

1. Review the most-recent release information, including operating system patch requirements, system requirements, disk space requirements, and known defects and limitations. See the *IBM Security Access Manager for Web: Release Notes* and the Technotes in the support knowledge database.
2. Install any operating system requirements that are necessary for the version of DB2 that you are using. For DB2 requirements, go to http://www.ibm.com/software/data/db2/udb/sysreqs.html.

IBM Java Runtime installation

Install IBM Java Runtime before using the command-line methods to install IBM Security Access Manager for Web.

IBM Java Runtime is provided with Security Access Manager.

IBM Security Access Manager Runtime for Java supports only the IBM Java Runtime provided with Security Access Manager or the JRE provided with IBM WebSphere Application Server.

Complete the instructions that apply to your operating system.

AIX: Installing IBM Java Runtime

Install IBM Java Runtime on AIX before using the command-line methods to install IBM Security Access Manager for Web.

Before you begin

Complete the appropriate preinstallation tasks in "Operating system preparation" on page 28.

Procedure

1. Log on as **root**.
2. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. Install the following packages:

   ```
   installp -acgYXd package_path/usr/sys/inst.images packages
   ```

   where *package_path* is the directory where the DVD is mounted or the files are located and *packages* are as follows:

   Java6_64.samples
   Specifies the IBM Java Runtime sample files package.

   Java6_64.sdk
   Specifies the IBM Java Runtime software development kit (SDK) extensions package.

   Java6_64.source
   Specifies the IBM Java Runtime source files package.
4. After the installation completes successfully, do one of the following tasks:
   - Set the PATH environment variable. For example:

     ```
     export PATH=/usr/java6_64/bin:$PATH
     ```

     Note: To display whether IBM Java Runtime is already in the path, use the **java –version** command.
   - Set the JAVA_HOME environment variable to the path where you installed IBM Java Runtime. For example, use **ksh** and enter the following command to define JAVA_HOME:

     ```
     export JAVA_HOME=/usr/java6_64/
     ```

Results

After you install IBM Java Runtime, no additional configuration is necessary.

Linux: Installing IBM Java Runtime

Install IBM Java Runtime on Linux before using the command-line methods to install IBM Security Access Manager for Web.

Before you begin

Complete the appropriate preinstallation tasks in “Operating system preparation” on page 28.

Note to Linux on System z users: You must first obtain access to the Linux `rpm` files for Linux on System z from the DVD or Passport Advantage. The `rpm` files are in the */package_path*`/linux_s390` directory.

Procedure

1. Log on as **root**.
2. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. Change to the *package_path*`/`*distribution* directory where *package_path* is the mount point for your DVD or file location and *distribution* specifies `linux_x86` for x86-64 or `linux_s390` for System z.
4. Install the IBM Java Runtime package:

`rpm -ihv package`

where *package* is as follows:

Linux on x86-64	ibm-java-x86_64-sdk-6.0-10.0.x86_64.rpm (64-bit)
Linux on System z	ibm-java-s390x-sdk-6.0-10.0.s390x.rpm

5. Set the PATH environment variable:
   `export PATH=jre_path:$PATH`

   For example, to ensure that the IBM Java Runtime is accessible through the PATH system variable, enter the following command:
   `export PATH=/opt/ibm/java-x86_64-60/jre/bin:$PATH`

Results

After you install IBM Java Runtime, no additional configuration is necessary.

Solaris: Installing IBM Java Runtime

Install IBM Java Runtime on Solaris before using the command-line methods to install IBM Security Access Manager for Web.

Before you begin

Complete the appropriate preinstallation tasks in "Operating system preparation" on page 28.

Procedure

1. Log on as **root**.
2. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. Install the IBM Java Runtime package:
   a. Enter: `mkdir -p /opt/ibm/solaris`
   b. Extract the file:
      path_to_IBM_Java_package`/sol6460sr10hybrid-20111110_01-sdk.tar.Z`

      to the `/opt/ibm/solaris` directory.
4. After the installation ends successfully, do one of the following tasks.
   - Set the PATH environment variable.
     `export PATH=java_path:$PATH` For example:
     `export PATH=/opt/ibm/solaris/jre/bin:$PATH`

     Note:
     – The installation program expects the JRE to be installed in the default location, which is used in the example.
     – To display whether IBM Java Runtime is already in the path, use the **java –version** command.
   - If you plan to use an installation path other than the default, set the JAVA_HOME environment variable to the path where you plan to install IBM Java Runtime. For example, enter the following to define JAVA_HOME:
     `export JAVA_HOME=/opt/ibm/solaris`

Results

After you install IBM Java Runtime, no additional configuration is necessary.

Windows: Installing IBM Java Runtime

Install IBM Java Runtime on Windows before using the command-line methods to install IBM Security Access Manager for Web. You can also install IBM Java before you use the installation scripts or the Launchpad.

Before you begin

Complete the appropriate preinstallation tasks in "Operating system preparation" on page 28.

Procedure

1. Log on as any member of the Administrators group.
2. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. Enter the following command:

   ```
   package_path\windows\JDK\
   run ibm-java-sdk-60-win-x86_64.exe
   ```

4. Complete the online instructions as prompted. When you are prompted with the message `Install this Java Runtime Environment as the System JVM`, click **Yes**.
5. When installation ends, click **Finish**.
6. If you plan to use the iKeyman utility, do the following steps:
   a. Set the JAVA_HOME environment variable to the full path to your Java installation. For example:

      ```
      set JAVA_HOME=c:\Program Files\IBM\Java60\jre
      ```

   b. Add the GSKit `bin` and `lib` directories to the PATH variable. For example:

      ```
      set PATH="C:\Program Files\ibm\gsk8\bin";%PATH%
      set PATH="C:\Program Files\ibm\gsk8\lib";%PATH%
      ```

Results

After you install IBM Java Runtime, no additional configuration is necessary.

IBM Global Security Kit (GSKit) installation

Install IBM Global Security Kit (GSKit) before using the command-line methods to install IBM Security Access Manager for Web.

IBM Global Security Kit (GSKit) provides Secure Sockets Layer (SSL) data encryption between Security Access Manager systems and supported registry servers.

The GSKit package also installs the key management tool GSKCapiCmd, which you can use to create key databases, public-private key pairs, and certificate requests.

Complete the instructions that apply to your operating system.

See “Components and prerequisites for Security Access Manager systems” on page 12 for a list of components that require GSKit as a prerequisite.

Note: Previous versions of GSKit included a utility called **ikeyman**. This utility is now part of IBM Java. If you want to use iKeyman with Security Access Manager version 7.0 key database files, you must modify the `java.security` file and add the CMS Java security provider. For more information, see the *IBM Developer Kit and Runtime Environment, Java Technology Edition, Version 6 and 7 iKeyman User's Guide for version 8.0* http://download.boulder.ibm.com/ibmdl/pub/software/dw/jdk/security/60/iKeyman.8.User.Guide.pdf.

AIX: Installing the IBM Global Security Kit (GSKit)

Install GSKit on AIX before using the command-line methods to install IBM Security Access Manager for Web.

Before you begin

Complete the appropriate preinstallation tasks in “Operating system preparation” on page 28.

Procedure

1. Log on as **root**.
2. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. Enter the following commands to install runtime package:

   ```
   installp -acgXd . GSKit8.gskcrypt64.ppc.rte
   installp -acgXd . GSKit8.gskssl64.ppc.rte
   ```

   where:

   - `-a` stands for apply
   - `-c` stands for commit
   - `-g` automatically installs or commits any requisite software product
   - `-X` expands the file system if necessary
   - `-d` stands for device. This option specifies where the installation media can be found.

Results

After you install GSKit, no additional configuration is necessary.

Linux: Installing the IBM Global Security Kit (GSKit)

Install GSKit on Linux before using the command-line methods to install IBM Security Access Manager for Web.

Before you begin

Complete the appropriate preinstallation tasks in “Operating system preparation” on page 28.

Note to Linux on System z users: You must first obtain access to the Linux `rpm` files from the product media for Linux on System z. The `rpm` files are in the `/package_path/linux_s390` directory.

Procedure

1. Log on as **root**.
2. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. Change to the *package_path*/*distribution* directory where *package_path* is the mount point for your DVD or file location and *distribution* specifies `linux_x86` for x86-64 or `linux_s390` for System z.
4. Install the IBM Global Security Kit (GSKit) packages for your operating system.
   - Linux on x86-64

     ```
     rpm -ihv gskcrypt64-8.0.14.26.linux.x86_64.rpm
     rpm -ihv gskssl64-8.0.14.26.linux.x86_64.rpm
     ```

   - Linux on System z, 64-bit

     ```
     rpm -ihv gskcrypt64-8.0.14.26.linux.s390x.rpm
     rpm -ihv gskssl64-8.0.14.26.linux.s390x.rpm
     ```

Solaris: Installing the IBM Global Security Kit (GSKit)

Install GSKit on Solaris before using the command-line methods to install IBM Security Access Manager for Web.

Before you begin

Complete the appropriate preinstallation tasks in "Operating system preparation" on page 28.

About this task

The following procedure uses **pkgadd** to install the software package.

Attention: Use the **-G** option with the **pkgadd** utility on Solaris installations. The **-G** option adds the package into the current zone only.

Procedure

1. Log on as **root**.
2. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. Install IBM Global Security Kit (GSKit). Specify the following packages:

   ```
   pkgadd -d /package_path/solaris -a /package_path/solaris/pddefault -G
   gsk8cry64
   ```

   ```
   pkgadd -d /package_path/solaris -a /package_path/solaris/pddefault -G
   gsk8ssl64
   ```

   where *package_path* is the directory where the DVD is mounted or the files are located. The `-G` option adds the package to the current zone only.

Windows: Installing the IBM Global Security Kit (GSKit)

Install GSKit on Windows before using the command-line methods to install IBM Security Access Manager for Web.

Before you begin

Complete the appropriate preinstallation tasks in "Operating system preparation" on page 28.

Procedure

1. Log on as any member of the Administrators group.
2. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. Change to the `\windows\GSKit` directory.
4. Start the installation by entering the following command:
   `gsk8ssl64`
5. Click **Next**. The Choose Destination Location window is displayed.
6. Accept the default destination directory or click **Browse** to select a path to another directory on the local system. If the directory does not exist, you must confirm that you want the directory to be created or specify a directory that exists.
7. Click **Next** to install GSKit. The Setup Complete window is displayed.
8. Click **Finish** to exit the installation program.

Results

After you install GSKit, no additional configuration is necessary.

IBM Security Access Manager License installation

Install the IBM Security Access Manager license before using the command-line methods to install IBM Security Access Manager for Web.

Complete the instructions that apply to your operating system.

See "Components and prerequisites for Security Access Manager systems" on page 12 for a list of components that require the IBM Security Access Manager license as a prerequisite.

AIX, Linux, Solaris: Installing the IBM Security Access Manager License

Install the license before using the command-line methods to install IBM Security Access Manager for Web components on AIX, Linux, or Solaris operating systems.

About this task

The `isamLicense` script runs an interactive tool that displays the license text. On each page of the license, you are prompted to press Enter to continue viewing the license agreement, press 1 to accept the agreement or 2 to decline it, or press 99 to return the previous page. The script installs the license to the `/opt/PolicyDirector/license` directory. After you run the script and accept the license, you must install the license.

Note: When you accept the license, you agree to its terms and conditions.

Procedure

1. Log on as **root**.
2. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. Open a command window.
4. Change to the `/scripts` directory in the installation image.

5. Run the `isamLicense` script.

   ```
   isamLicense
   ```

   The `isamLicense` script has the following options:

   -q Quiet: Runs the script without displaying the license. This option is useful in automated installations.

   Attention: When you use this option, you automatically accept the license without viewing it.

   -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

   -t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

   -? Help: Displays the syntax of the script file.
6. Read the license.
7. Accept the license by pressing 1.
8. Install the license:

   AIX:

   ```
   installp -acgYXd package_path/usr/sys/inst.images PD.lic
   ```

   where: *package_path* is the directory where the DVD is mounted or the files are located.

   Linux:

   ```
   rpm -ihv package
   ```

   where *package* is:

   - **Linux on x86:** `PDlic-PD-7.0.0-0.x86_64.rpm`
   - **Linux on System z:** `PDlic-PD-7.0.0-0.s390.rpm`

   Solaris:

   ```
   pkgadd -d /package_path/solaris
     -a /package_path/solaris/pddefault PDlic
   ```

   where:

   /package_path/solaris
   Specifies the location of the package.

   /package_path/solaris/pddefault
   Specifies the location of the installation administration script.

   Note: When you install the PDlic package, the following message is displayed:

   ```
   The following files are already installed on the system and
   are being used by another package:
   * /opt/PolicyDirector/attribute_change_only
   * /-conflict with a file that does not belong to any package.
   Do you want to install these conflicting files [y, n, ?, q]
   ```

   Answer `y` to this question.

What to do next

The installation of the license is completed. Continue with the setup of another Security Access Manager prerequisite product or system. Follow the steps in the

Chapter 3, “Installation roadmap,” on page 21.

Windows: Installing the IBM Security Access Manager License

Install the license before using the command-line methods to install IBM Security Access Manager for Web components on Windows operating systems.

Procedure

1. Log on as a user with Administrator group privileges.
2. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. Run the **setup.exe** program that is located in this directory:

   `\windows\PolicyDirector\Disk Images\Disk1\PDLIC\Disk Images\Disk1`

   Follow the online instructions and select to install the Security Access Manager License.

What to do next

The installation of the license is completed. Continue with the setup of another Security Access Manager prerequisite product or system. Follow the steps in the Chapter 3, “Installation roadmap,” on page 21.

IBM Security Utilities installation

Install IBM Security Utilities before using the command-line methods to install IBM Security Access Manager for Web.

The IBM Security Utilities provides common utilities that are required by Security Access Manager Runtime.

Complete the instructions that apply to your operating system.

See “Components and prerequisites for Security Access Manager systems” on page 12 for a list of components that require the IBM Security Utilities as a prerequisite.

AIX: Installing the IBM Security Utilities

Install IBM Security Utilities before using the command-line methods to install IBM Security Access Manager for Web on AIX.

Before you begin

Complete the appropriate preinstallation tasks in “Operating system preparation” on page 28.

Procedure

1. Log on as **root**.
2. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. Enter the following command to install the package:

   `installp -acgYXd` *`package_path`*`/usr/sys/inst.images TivSec.Utl`

   where *`package_path`* is the directory where the DVD is mounted or the files are located.

Attention: You must install the IBM Security Utilities package first before installing the Security Access Manager Runtime package.

4. Unmount the DVD, if used.

Results

After you install IBM Security Utilities, no additional configuration is necessary.

This step completes the setup of the IBM Security Utilities. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Linux: Installing IBM Security Utilities

Install IBM Security Utilities before using the command-line methods to install IBM Security Access Manager for Web on Linux.

Before you begin

Complete the appropriate preinstallation tasks in "Operating system preparation" on page 28.

Procedure

1. Log on as **root**.
2. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. Change to the *package_path*/*distribution* directory where *package_path* is the mount point for your DVD or file location and *distribution* specifies `linux_x86` for x86-64 or `linux_s390` for System z.
4. Install the package:

   `rpm -ih package`

   where *package* is:

   - Linux on x86-64: `TivSecUtl-TivSec-7.0.0-0.x86_64.rpm`
   - Linux on System z: `TivSecUtl-TivSec-7.0.0-0.s390x.rpm`

   Attention: You must install the IBM Security Utilities package first before installing the Security Access Manager Runtime package.
5. Unmount the DVD, if used.

Results

After you install IBM Security Utilities, no additional configuration is necessary.

This step completes the setup of the IBM Security Utilities. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Solaris: Installing IBM Security Utilities

Install IBM Security Utilities before using the command-line methods to install IBM Security Access Manager for Web on Solaris.

Before you begin

Complete the appropriate preinstallation tasks in "Operating system preparation" on page 28.

About this task

The following procedure uses **pkgadd** to install the software package.

Attention: Use the **-G** option with the **pkgadd** utility on Solaris installations. The **-G** option adds the package into the current zone only.

This step completes the setup of the IBM Security Utilities. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Procedure

1. Log on as **root**.
2. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. To install the IBM Security Utilities package, enter:

   ```
   pkgadd -d /package_path/solaris -a /package_path/solaris/pddefault
   -G TivSecUtl
   ```

   where */package_path*/solaris specifies the location of the package and */package_path*/solaris/pddefault specifies the location of the installation administration script.

   Attention: You must install the IBM Security Utilities package first before installing the Security Access Manager Runtime package.

Results

After you install IBM Security Utilities, no additional configuration is necessary.

Windows: Installing IBM Security Utilities

Install IBM Security Utilities before using the command-line methods to install IBM Security Access Manager for Web on Windows.

Before you begin

Complete the appropriate preinstallation tasks in "Operating system preparation" on page 28.

Procedure

1. Log on as any member of the Administrators group.
2. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. Change to the following directory:

   ```
   \windows\TivSecUtl\Disk Images\Disk1
   ```

4. Run the **setup.exe** program from this directory.
5. Choose the language for the installation.
6. Click **Next**.

7. Click **Accept** to accept the license agreement. The Choose Destination Location window is displayed.
8. Accept the default destination directory or click **Browse** to select a path to another directory on the local system. If the directory does not exist, you must confirm that you want the directory to be created or specify a directory that exists.
9. Click **Next** to install IBM Security Utilities. The Setup Complete window is displayed.

Results

After you install IBM Security Utilities, no additional configuration is necessary.

This step completes the setup of the IBM Security Utilities. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

IBM Tivoli Directory Server client installation

Install the IBM Tivoli Directory Server client before you use the command-line methods to install IBM Security Access Manager for Web.

Note: If you plan to complete the server installation of IBM Tivoli Directory Server, you do not need to install the client separately. See Chapter 5, "User registry server installation and configuration," on page 51 for Tivoli Directory Server installation procedures that install both the client and server.

The IBM Tivoli Directory Server client is included with IBM Tivoli Directory Server on the Security Access Manager DVDs or Passport Advantage files for supported operating systems.

You must explicitly install the Tivoli Directory Server client on each system that runs Security Access Manager, with the following exceptions:

- The Security Access Manager system is a supported Windows system that is joined to an Active Directory domain.
- You are setting up a IBM Security Access Manager Runtime for Java, Security Access Manager Web Portal Manager, Security Access Manager Attribute Retrieval Service, or Security Access Manager session management server.

Complete the instructions that apply to your operating system.

See "Components and prerequisites for Security Access Manager systems" on page 12 for a list of components that require IBM Tivoli Directory Server client as a prerequisite.

Note: You can have multiple versions of the IBM Tivoli Directory Server client on the same system. Ensure that the newest available patch for the version of IBM Tivoli Directory Server client that you are running is installed.

AIX: Installing the IBM Tivoli Directory Server client

Install IBM Tivoli Directory Server client before using the command-line methods to install IBM Security Access Manager for Web on AIX.

Before you begin

Complete the appropriate preinstallation tasks in "Operating system preparation" on page 28.

Procedure

1. Log on as **root**.
2. Access the DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/usr/sys/inst.images/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
4. Install the client packages of IBM Tivoli Directory Server. At a command prompt, enter:

   ```
   installp -acgXd package_path/usr/sys/inst.images packages
   ```

   Table 13 lists the packages that are required for each client type. Install the packages for your client in the order specified.

   To install multiple packages, separate the package names by a blank space.

Table 13. Client packages for AIX

Client	Packages	Package descriptions
64-bit client (no SSL)	1. `idsldap.license63` 2. `idsldap.cltbase63` 3. `idsldap.clt64bit63`	1. License 2. Base Client runtime and Base Client SDK 3. 64-bit client (no SSL)
64-bit client (SSL)	1. `idsldap.license63` 2. `idsldap.cltbase63` 3. `idsldap.clt64bit63` 4. `idsldap.clt_max_crypto64bit63`	1. License 2. Base Client runtime and Base Client SDK 3. 64-bit client (no SSL) 4. 64-bit client (SSL)
Java client	`idsldap.cltjava63`	The Java client is required for X11 support

   Note: Full server versions require an X11 environment. For a client with no X11 requirements, install the 64-bit client as you would if you required an X11 environment.
5. Unmount the DVD, if used, as follows:

   ```
   umount /dvd
   ```

   where */dvd* is the mount point.

Results

After you install the IBM Tivoli Directory Server client, no additional configuration is necessary.

Linux: Installing the IBM Tivoli Directory Server client

Install IBM Tivoli Directory Server client before using the command-line methods to install IBM Security Access Manager for Web on Linux.

Before you begin

Complete the appropriate preinstallation tasks in "Operating system preparation" on page 28.

Note to Linux on System z users: You must first obtain access to the Linux `rpm` files. The `rpm` files are in the `/package_path/linux_s390` directory.

Procedure

1. Log on as **root**.
2. Access the DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. Change to the *package_path*`/distribution` directory where *package_path* is the mount point for your DVD or file location and *distribution* specifies `linux_x86` for x86-64 or `linux_s390` for System z.
4. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *package_path*`/distribution/tdsLicense/license` directory.
5. Install the client packages of IBM Tivoli Directory Server for your deployment.

   `rpm -ihv` *packages*

   Table 14 lists the packages that are required for each client type. Install the packages for your client in the order specified.

Table 14. Client packages for Linux operating systems

Client type	Packages	Package descriptions
Linux on x86-64, 64-bit client	1. `idsldap-license63-6.3.0-17.x86_64.rpm` 2. `idsldap-cltbase63-6.3.0-17.x86_64.rpm` 3. `idsldap-clt64bit63-6.3.0-17.x86_64.rpm` 4. `idsldap-cltjava63-6.3.0-17.x86_64.rpm`	1. License 2. Base client 3. 64-bit client 4. Java client
Linux on System z, 64-bit client	1. `idsldap-license63-6.3.0-17.s390.rpm` 2. `idsldap-cltbase63-6.3.0-17.s390.rpm` 3. `idsldap-clt64bit63-6.3.0-17.s390x.rpm` 4. `idsldap-cltjava63-6.3.0-17.s390.rpm`	1. License 2. Base client 3. 64-bit client 4. Java client

6. Unmount the DVD, if used.

Results

After you install the IBM Tivoli Directory Server client, no additional configuration is necessary.

Solaris: Installing the IBM Tivoli Directory Server client

Install IBM Tivoli Directory Server client before using the command-line methods to install IBM Security Access Manager for Web on Solaris.

Before you begin

Complete the appropriate preinstallation tasks in "Operating system preparation" on page 28.

About this task

The following procedure uses **pkgadd** to install software packages and the **pdconfig** utility to configure them.

Procedure

1. Log on as **root**.
2. Access the DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/solaris/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
4. Install the client packages of IBM Tivoli Directory Server for your operating system:

   ```
   pkgadd -d /package_path/solaris/packages -a /package_path/solaris/pddefault
   ```

   Table 15 lists the packages that are required for each client type. Install the packages for your client in the order specified.

Table 15. Client packages for Solaris

Client type	Packages	Package descriptions
64-bit client	1. `idsldap.license63.pkg` 2. `idsldap.cltbase63.pkg` 3. `idsldap.clt64bit63.pkg` 4. `idsldap.cltjava63.pkg`	1. License 2. Base client 3. 64-bit client 4. Java client

Note:

- During installation, you are asked if you want to use `/opt` as the base directory. If space permits, accept `/opt` as the base directory. To accept `/opt` as the base directory, press Enter.
- When you install client or server packages, the system might prompt you with the following query: `This package contains scripts which will be executed with super-user permission during the process of installing the package. Continue with installation?`

  Type `y` to continue. These scripts create the Tivoli Directory Server user ID.

Results

After you install the IBM Tivoli Directory Server client, no additional configuration is necessary.

Windows: Installing the IBM Tivoli Directory Server client

Install IBM Tivoli Directory Server client before using the command-line methods to install IBM Security Access Manager for Web on Windows.

Before you begin

Complete the appropriate preinstallation tasks in “Operating system preparation” on page 28.

Procedure

1. Log on as any member of the Administrators group.
2. Access the DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. Change to the `\windows\tds_client64` directory.
4. To install the IBM Tivoli Directory Server client, run the **install_tds.bat** file.

   The Choose Setup Language window is displayed.
5. Select the language that you want to use for the installation and click **OK**.
6. The Welcome window is displayed. Click **Next** to continue.
7. Read the license agreement. Select to accept the terms and then click **Next**. A window is displayed that informs you of the packages that are already installed and if any action is required. If necessary, satisfy any requirements and click **Next**.
8. Select to install the **C Client** feature and then click **Next**.
9. Review the configuration options that you selected. If you want to change any of your selections, click **Back**. Click **Next** to begin the installation.

Results

After you install the IBM Tivoli Directory Server client, no additional configuration is necessary.

Installing WebSphere Application Server

Install WebSphere Application Server on systems on which you plan to set up the Web Portal Manager, Attribute Retrieval Service, or the Session Management Server.

Before you begin

- Complete the appropriate preinstallation tasks in “Operating system preparation” on page 28.
- During the installation of WebSphere Application Server, you are prompted to select features to install. For information about the features, see the WebSphere Application Server, Network Deployment (Distributed platforms and Windows), Version 8.0 Information Center.
- If you are planning to deploy a Session Management Server in a WebSphere version 8.0 environment, you must install WebSphere Application Server version 8.0 FP5 (or later).
- If you use globalization characters, and you did not install WebSphere Application Server version 8.0 FP5 or later, choose one of the following actions to avoid character restrictions:
  - During profile creation, choose "Advanced profile creation" instead of Typical.
  - Install WebSphere Application Server 8.0 FP5 in step 8 on page 48 before you create the application server profile in step 7 on page 48.

Note: As an alternative to this task, you can automate the installation of WebSphere Application Server with script files. See:

- “Automating the installation of WebSphere Application Server (AIX, Linux, or Solaris)” on page 196
- “Automating the installation of WebSphere Application Server (Windows)” on page 198

About this task

The steps in this task are general and apply to WebSphere Application Server version 8.0. For detailed installation instructions, see its information center WebSphere Application Server, Network Deployment (Distributed platforms and Windows), Version 8.0.

If you are installing WebSphere Application Server version 7.0, see its information center: WebSphere Application Server, Network Deployment (Distributed platforms and Windows), Version 7.0.

Procedure

1. Obtain the WebSphere Application Server installation files and product repository. These files are available from:
   - The WebSphere Application Server DVDs that were provided with the IBM Security Access Manager DVDs.
   - The Passport Advantage site.
2. Copy the WebSphere Application Server files to the computer where you want to install WebSphere Application Server.
3. Extract all the WebSphere Application Server files from their compressed files into one directory.
4. Obtain Installation Manager from any of the following locations:
   - The Passport Advantage site
   - The IBM Installation Manager download website: http://www.ibm.com/support/entry/portal/All_download_links/Software/Rational/IBM_Installation_Manager

   a. Download the files.
   b. Extract the files into one directory. Consider using the same directory where the WebSphere Application Server files are located.
   c. Install Installation Manager on your system. Use the installation instructions that are provided with Installation Manager.
5. Add the product repository to your Installation Manger preferences.
   a. Start Installation Manager.
   b. In the top menu, click **File** > **Preferences**.
   c. Select **Repositories**.
   d. Click **Add Repository**.
   e. Enter the path to the `repository.config` file in the location that contains the repository file. For example:

      `/var/repositories/product_name/local-repositories`
   f. Click **OK**.
   g. In the Repositories window, clear any locations that you are not using.
   h. Click **Apply**.
   i. Click **OK**.
   j. Click **File** > **Exit** to close Installation Manager.
6. Install WebSphere Application Server:
   a. Start Installation Manager.
   b. Click **Install**.
   c. Select **IBM WebSphere Application Server Network Deployment** and the appropriate version.

d. Click **Next**.
e. Accept the terms of the license agreement. Click **Next**.
f. Specify the installation root directory for the product files, which are referred to as the core product files or system files.
g. Click **Next**.
h. Select the languages to install.
i. Click **Next**.
j. Select the features that you want to install.
k. Click **Next**.
l. Click **Install**.
m. Select **Profile Management Tool to create a profile**.
n. Click **Finish**.
o. Click **File** > **Exit** to close the Installation Manager. The Profile Management Tool opens.

7. Create an application server profile using the Profile Management Tool.
   a. In the Profile Management Tool, click **Create**.
   b. Select **Application server**.
   c. Click **Next**.
   d. Select **Typical profile creation**.
   e. Click **Next**.
   f. Click the **Administrative Security** check box and complete the fields on the panel to enable administrative security.
   g. Click **Next**.
   h. Review the information and click **Create**.
   i. Clear the check mark from the **Launch the First steps console** check box.
   j. Click **Finish**.
8. Install the latest fix pack for your installation. See the hardware and software requirements page of the IBM Security Access Manager information center for the minimum fix pack level required. Locate the fix pack on the WebSphere Application Server web-based repository or download the package and install it from a local repository.
   - To install it from the web-based repository:
     a. Click **Update** on the IBM Installation Manager window.
     b. Select **IBM WebSphere Application Server Network Deployment V8.0**.
     c. Click **Next**. Continue with the installation.
   - To install it from a local repository:
     a. Locate the fix pack on the WebSphere Application Server Support page: http://www.ibm.com/support/docview.wss?uid=swg27004980
     b. Download the fix pack into a local repository.
     c. Click **Update**.
     d. Select **IBM WebSphere Application Server Network Deployment V8.0**.
     e. Click **Next**. Continue with the installation. Use the accompanying readme file from the WebSphere Application Server Support page for assistance.
9. Start the application server. For example, type:

AIX, Linux, or Solaris

```
/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/
  bin/startServer.sh server1
```

Windows

```
C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\
  bin\startServer.bat server1
```

10. Optional: Install IBM HTTP Server and the corresponding web server plug-in if you want to install them for your environment. Use the instructions in the IBM WebSphere Application Server information center:WebSphere Application Server, Network Deployment (Distributed platforms and Windows), Version 8.0

    If you are installing WebSphere Application Server version 7.0, see its information center: WebSphere Application Server, Network Deployment (Distributed platforms and Windows), Version 7.0

Chapter 5. User registry server installation and configuration

The first step in establishing a management domain is to set up a registry server for use with Security Access Manager.

Review the information in "User registry differences."

Then, to install and configure a registry, do one of the following:

- To install and configure IBM Tivoli Directory Server (included with Security Access Manager), follow the instructions in one of the following topics:
  - "Installing IBM Tivoli Directory Server with the Tivoli Directory Server installation wizard" on page 58
  - "Installing Tivoli Directory Server with the Launchpad (Windows only)" on page 67
  - "Tivoli Directory Server setup with script files" on page 61

  You also can consult the IBM Tivoli Directory Server documentation available on the Web at:

  http://www.ibm.com/software/tivoli/products/directory-server
- To install a supported registry other than IBM Tivoli Directory Server, use the registry product's documentation. For a list of supported registries, see the Release Notes in the IBM Security Access Manager for Web Information Center. Ensure that all necessary operating system patches are installed.

  Note: The IBM Tivoli Directory Server client must be used as the registry client for LDAP-based user registries.
- To use an existing registry server with Security Access Manager, ensure that you have upgraded the server to a version that is supported by this release of Security Access Manager. For upgrade instructions for IBM Tivoli Directory Server, see the *IBM Security Access Manager for Web Upgrade Guide*. For other supported registries, consult the registry product's documentation. Then follow instructions in this section to configure your registry for use with Security Access Manager.

User registry differences

Each user registry presents unique considerations when integrated with Security Access Manager.

Security Access Manager supports LDAP and URAF user registries.

Use an LDAP user registry if you run Security Access Manager on AIX, Linux, Solaris, or Microsoft Windows. Security Access Manager supports the following LDAP user registries:

- Tivoli Directory Server
- IBM z/OS Security Server LDAP Server
- Novell eDirectory Server
- Sun Java System Directory Server
- Microsoft Active Directory Lightweight Directory Services (ADLDS)

Use a URAF user registry if you run Security Access Manager on Windows. URAF user registries cannot be used when Security Access Manager is run on an operating system other than Windows. Security Access Manager supports the following URAF user registry:

- Microsoft Active Directory Server

General considerations

A few general considerations apply to all the supported registries.

Review this information before configuring a user registry for your environment.

- Avoid using the forward slash (/) character when defining the names for users and groups when that name is defined using distinguished names strings. Each user registry treats this character differently.
- Avoid using leading and trailing blanks in user and group names. Each user registry treats blanks differently.

LDAP considerations

Several specific considerations apply to all the supported LDAP registries.

Review this information before configuring an LDAP registry for your environment.

- There are no configuration steps needed in Security Access Manager to make it support LDAP's own Password Policy. Security Access Manager does not assume the existence or non-existence of LDAP's own Password Policy at all.

  Security Access Manager enforces its own Password Policy first and foremost. Security Access Manager will attempt to update password in LDAP only when the provided password passes Security Access Manager's own Password Policy check.

  After that Security Access Manager tries to accommodate LDAP's own Password Policy to the best of its ability using the return code that its get from LDAP during a password related update.

  If Security Access Manager can map this return code without any ambiguity with the corresponding Security Access Manager error code, it will do so and will return a proper error message.
- To take advantage of the multi-domain support in Security Access Manager, you must use an LDAP user registry. When using a URAF user registry, only a single Security Access Manager domain is supported.
- When using an LDAP user registry, the capability to own global sign-on credentials must be explicitly granted to a user. After this capability is granted, it can subsequently be removed. Conversely, users that are created in a URAF user registry are automatically given this capability. This capability cannot be removed.
- Leading and trailing blanks in user names and group names are ignored when using an LDAP user registry in a Security Access Manager secure domain. To ensure consistent processing regardless of the user registry, define user names and group names without leading or trailing blanks.
- Attempting to add a single duplicate user to a group does not produce an error when using an LDAP user registry.
- The Security Access Manager authorization API provides a credentials attribute entitlements service. This service is used to retrieve user attributes from a user registry. When this service is used with an LDAP user registry, the retrieved

attributes can be string data or binary data. However, when used with a URAF user registry, the retrieved attributes can be string data, binary data, or integer data.

Sun Java System Directory Server considerations

In addition to the general LDAP-specific considerations, the following considerations are specific to Sun Java System Directory Server. Review this information before configuring a Sun Java System Directory Server for your environment.

- If the user registry contains more entries than the defined look-through limit, the directory server might return the following status that Security Access Manager treats as an error:

  `LDAP_ADMINLIMIT_EXCEEDED`

  When the directory server is installed, the default value is 5000. To modify this value, perform the following steps from the Sun Java System Directory Server Console:

  1. Select the **Configuration** tab.
  2. Expand the **Data** entry.
  3. Select **Database Settings**.
  4. Select the **LDBM Plug-in Settings** tab.
  5. In the **Look-through Limit** field, type the maximum number of entries that you want the server to check in response to the search, or type `-1` to define no maximum limit.

  If you bind the directory as the Directory Manager, the look-through limit is unlimited and overrides any settings specified in this field.

Microsoft Active Directory Lightweight Directory Services (AD LDS) considerations

In addition to the general LDAP-specific considerations, the following considerations are specific to Microsoft AD LDS. Review this information before configuring a Microsoft AD LDS registry for your environment.

- Policy Server configuration allows you to select between a standard or minimal data model for the user registry. Because AD LDS allows only a single naming attribute to be used when creating LDAP objects, AD LDS requires the minimal data model. Regardless of which data model is chosen during Policy Server configuration, Security Access Manager will always use the minimal data model when AD LDS is selected as the user registry.
- The common name (`cn`) attribute is a single-value attribute and can store only one value. The AD LDS registry requires the value of `cn` to be the same as the `cn` naming attribute in the distinguished name (`dn`) attribute. When creating a user or group in Security Access Manager, specify the same value for `cn` as the `cn` naming attribute in the `dn`. Security Access Manager ignores the value of the `cn` attribute if it is different from the value of the `cn` naming attribute in the `dn`. For example, you cannot use the following command to create a user because the value of the `cn` attribute, *`fred`*, is different from the `cn` naming attribute in the `dn`, *`user1`*:

  ```
  pdadmin user create user1 cn=user1,o=ibm,c=us fred smith password1
  ```

URAF considerations

Several specific considerations apply to all the supported URAF registries.

Review this information before configuring a URAF registry for your environment.

- To use a URAF user registry, you must be running Security Access Manager on a supported Microsoft Windows operating system. See the *IBM Security Access Manager for Web Release Notes* for a list of supported operating systems.
- When using a URAF user registry, only a single Security Access Manager domain is supported. To take advantage of the Security Access Manager multi-domain support, use an LDAP user registry.
- Users created in a URAF user registry are automatically given the capability to own global sign-on credentials. This capability cannot be removed. When using an LDAP user registry, this capability must be explicitly granted. After this capability is granted, it can subsequently be removed.
- The Security Access Manager authorization API provides a credentials attribute entitlements service. This service is used to retrieve user attributes from a user registry. When this service is used with a URAF user registry, the retrieved attributes can be string data, binary data, or integer data. However, when used with an LDAP user registry, the retrieved attributes can be only string data or binary data.

Microsoft Active Directory Server considerations

In addition to the general URAF-specific considerations, the following considerations are specific to Microsoft Active Directory Server. Review this information before configuring an Active Directory Server for your environment.

- Users created in Active Directory may have an associated primary group. The Active Directory default primary group is Domain Users.

  But Active Directory does not add the primary group information to the user's `memberOf` or the group's `member` attribute. This means that when Security Access Manager queries for a list of members of a group, the result does not include any members for whom the group is the primary group. Additionally, when Security Access Manager queries for all the groups to which a user belongs, the query result does not display the primary group of the user.

  For this reason, avoid using a Security Access Manager group as the Active Directory primary group for Security Access Manager users.
- Security Access Manager can be configured in an Active Directory single domain or multi-domain environment. For information about single domain or multi-domain environments, see the Active Directory product documentation.
- When Security Access Manager is configured to use the Active Directory user registry with multiple Active Directory domains, the policy server must be installed and configured only from the root Active Directory domain or a client of that root domain.
- If Security Access Manager is to be installed on a non-domain controller system, this system needs to join to the Active Directory domain where Security Access Manager is to be configured.
- For dynamic group related information, see the Active Directory product documentation.
- Microsoft supports two different types of Authorization Storages, Active Directory and XML, that store application groups such as dynamic groups. However, Security Access Manager limits support of dynamic groups only to the Active Directory Authorization Stores of dynamic groups.Security Access Manager does not support dynamic groups that are created in XML Authorization Storage.
- Security Access Manager supports only the security global group.
- To import an Active Directory user as a Security Access Manager user, use the Active Directory user's login name as the user ID for the Security Access Manager user.

- If you installed and configured Security Access Manager on a client of Active Directory (for example, Security Access Manager and Active Directory are on different systems), the client system must join the domain. You must sign on to the domain using the created Active Directory administrative user to perform Security Access Manager configuration on the client system.
- When using SSL to communicate with the Active Directory server, the SSL port is limited by Active Directory to the default SSL port number of **636**.
- If the Active Directory environment is behind a firewall, make sure that Microsoft-DS port 445 is open. For more information about the server message block (SMB) protocol over IP, see the Microsoft support site.
- The DNS in the network TCP/IP setting on the client system must be the same as the domain controller's network TCP/IP setting. You can use the root domain controller as the DNS server or you can use a separate DNS.
- When Security Access Manager is configured to use Active Directory as the user registry, the Global Catalog server must be running and accessible to Security Access Manager servers. Active Directory also uses the Global Catalog server for user authentication. The Global Catalog uses port 3268 for non-SSL authentication and port 3269 for SSL authentication.

  For more information about Global Catalog ports and requirements for user and computer logon, see the Microsoft support site.
- Security Access Manager does not support cross domain group membership or universal groups. Security Access Manager does not support importing these types of groups.
- When Security Access Manager imports a dynamic group, the `ivacld-servers` and `remote-acl-users` groups apply read permission on each authorization store to which the dynamic group belongs. This read permission enables Security Access Manager blade servers, such as WebSEAL, to have read permission to the registry authorization store; thus, providing the blade server with the ability to read dynamic group data, such as group membership for building Security Access Manager credentials. Manually removing this read permission while Security Access Manager is configured to the Active Directory registry results in adverse behavior, such as inaccurate group membership.
- If the option to change a user's password using LDAP APIs is enabled in an environment where the following two conditions exist:
  - Security Access Manager is configured to use the Active Directory user registry
  - Security Access Manager blade servers use LDAP APIs to communicate with the Active Directory server

  then, Security Access Manager must be configured with Secure Socket Layer (SSL) to allow connections between the LDAP client and the Active Directory server. The Active Directory environment must also be enabled to accept LDAP connections over Secure Socket Layer (SSL).
- When using an Active Directory user registry in a Security Access Manager configuration with blade servers that use LDAP APIs to communicate with the Active Directory server, Security Access Manager supports user password change requests using either the Policy Server or LDAP APIs. Change user password requests using the LDAP APIs do not require the Policy Server to be up-and-running.

  The use of LDAP APIs to communicate with the Active Directory Server for blade servers is a multi-platform support that allows blade servers to be installed on machines that are not clients of the same domain as the policy server. In this configuration, the policy server must be installed and configured on a Windows operating system.

- When using an Active Directory user registry, each user name and each group name in a domain must be unique. User and group short name values are stored in the sAMAccountName attribute of Active Directory user objects and group objects. Active Directory user objects and group objects both have the sAMAccountName attribute as one of their attributes. Microsoft requires that the sAMAccountName attributes be unique within an Active Directory domain.
- When using a multi-domain Active Directory user registry, multiple users and groups can be defined with the same short name as long as they are located in different domains. However, the full name of the user or group, including the domain suffix, must always be specified to Security Access Manager.
- Leading and trailing blanks in user names and group names are ignored when using Microsoft Active Directory Server as the user registry in a Security Access Manager secure domain. To ensure consistent processing, regardless of the user registry, define user names and group names without leading or trailing blanks.
- Security Access Manager supports the use of an email address or other alternate format of the userPrincipalName attribute of the Active Directory registry user object as a Security Access Manager user identity. This is an optional enhancement; when it is enabled, both the default and the email address or other alternate format of the userPrincipalName can co-exist in the Security Access Manager environment.

  The default format of the userPrincipalName registry attribute is `user_id@`*`domain_suffix`*, where *domain_suffix* is the Active Directory domain where the user identity is created.

  For example, `johndoe@tivoli.com` is the value of the userPrincipalName; **`tivoli.com`** is the Active Directory domain where the user identity is created. The Security Access Manager user identity corresponding to the registry user in this example is either**`johndoe@tivoli.com`** or **`johndoe`**, depending on whether Security Access Manager is configured to use Active Directory with multiple domains or a single domain, respectively.

  The alternate format of the userPrincipalName attribute is `user_id@any_suffix`, where `any_suffix` can be any domain (Active Directory or non-Active Directory) other than the Active Directory domain in which the user identity is created. For example, if the registry user `johndoe@other_domain.com` is created in Active Directory `tivoli.com`, and the registry user `johndoe@tivoli.com` is created in Active Directory domain `child_domain.tivoli.com`. Both of these users can be Security Access Manager users, and their user identities are `johndoe@other_domain.com` and `johndoe@tivoli.com`, respectively.

  The alternate user principal name (UPN) support must be enabled in all Security Access Manager run-time environments to ensure that Security Access Manager user identities work properly with alternate UPNs.

  Once the use of alternate UPN format as Security Access Manager user identity is enabled, it cannot be reversed without breaking Security Access Manager functionalities.
- Although users and groups can be created with names that use a distinguished name string that contain a forward slash (/) character, subsequent operations on the object might fail. Some Active Directory functions interpret the forward slash character as a separator between the object name and the host name. To avoid the problem, do not use a forward slash character to define the user.

Length of names

The maximum lengths of various names that are associated with Security Access Manager vary depending on the user registry in the environment.

See Table 16 for a comparison of the maximum lengths that are allowed and the recommended maximum length to use to ensure compatibility with all the user registries that are supported by Security Access Manager.

Table 16. Maximum lengths for names by user registry and the optimal length across user registries

Name	IBM Tivoli Directory Server	IBM z/OS Security Server	Novell eDirectory Server	Sun Java System Directory Server	Microsoft Active Directory Server	Active Directory Lightweight Directory Service (ADLDS)	Optimal length
First name (LDAP CN)	256	256	64	256	64	64	64
Middle name	128	128	128	128	64	64	64
Last name (surname)	128	128	128	128	64	64	64
Registry UID (LDAP DN)	1024	1024	1024	1024	2048	1024	255
Security Access Manager user identity	256	256	256	256	64	64	64
User password	unlimited	unlimited	unlimited	unlimited	256	128	256
User description	1024	1024	1024	1024	1024	1024	1024
Group name	256	256	256	256	64	64	64
Group description	1024	1024	1024	1024	1024	1024	1024
Single sign-on resource name	240	240	240	240	60	240	60
Single sign-on resource description	1024	1024	1024	1024	1024	1024	1024
Single sign-on user ID	240	240	240	240	60	240	60
Single sign-on password	unlimited	unlimited	unlimited	unlimited	256	unlimited	256
Single sign-on group name	240	240	240	240	60	240	60
Single sign-on group description	1024	1024	1024	1024	1024	1024	1024
Action name	1	1	1	1	1	1	1
Action description, action type	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Object name, object description	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited

Table 16. Maximum lengths for names by user registry and the optimal length across user registries (continued)

Name	IBM Tivoli Directory Server	IBM z/OS Security Server	Novell eDirectory Server	Sun Java System Directory Server	Microsoft Active Directory Server	Active Directory Lightweight Directory Service (ADLDS)	Optimal length
Object space name, object space description	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
ACL name, ACL descriptions	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
POP name, POP description	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited

Although the maximum length of an Active Directory distinguished name (registry UID) is 2048, the maximum length of each relative distinguished name (RDN®) is 64.

If you configure Security Access Manager to use multiple Active Directory domains, the maximum length of the user identity and group name does not include the domain suffix. When using multiple domains, the format of a user identity is *user_id@domain_suffix*. The maximum length of 64 applies only to the *user_id* portion. If you use an email address or other alternate format for the Security Access Manager user identity in the Active Directory, the maximum name length remains the same, but includes the suffix.

Although the lengths of some names can be of unlimited, excessive lengths can result in policy that is difficult to manage and might result in poor system performance. Choose maximum values that are logical for your environment.

Tivoli Directory Server installation and configuration

Tivoli Directory Server is provided with the Security Access Manager product. You can use a new installation or an existing installation of Tivoli Directory Server in your environment.

Review the information in "User registry differences" on page 51. Then, choose an installation method or to use an existing registry server with Security Access Manager, ensure that you have upgraded the server to a version that is supported by this release of Security Access Manager. For upgrade instructions for IBMTivoli Directory Server, see the *IBM Security Access Manager for Web Upgrade Guide*. For other supported registries, consult the registry product's documentation. Then follow instructions in this section to configure your registry for use with Security Access Manager.

Installing IBM Tivoli Directory Server with the Tivoli Directory Server installation wizard

Install IBM Tivoli Directory Server using the installation wizard in the "Typical installation path." It uses default values and automatically installs all the required Tivoli Directory Server components for Security Access Manager.

Before you begin

Note: If Tivoli Directory Server packages, such as client packages, are already installed at a level greater than 6.3.0.0, remove the packages before you run the installation wizard.

Complete the following tasks before you set up IBM Tivoli Directory Server:

- Complete the preinstallation tasks that are appropriate for your environment in “Operating system preparation” on page 28.
- Review the general considerations for user registries in “General considerations” on page 52
- Review the LDAP user registry considerations in “LDAP considerations” on page 52.
- Access the instructions for the "Typical installation path" method in the IBM Tivoli Directory Server version 6.3 Information Center.
  1. Go to http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm
  2. Search for "Typical installation path."

About this task

This task completes installations of the following components:

- All components that are required by Tivoli Directory Server.
- All the corequisite products that are required by Tivoli Directory Server, if they are not already installed. These products include:
  - GSKit
  - DB2
- The embedded version of WebSphere Application Server. This software is required by the Web Administration tool, which is installed automatically as part of the "Typical installation path" method.

This task also completes the following configuration:

- Deploys the Web Administration tool.
- Creates a default directory server instance named **dsrdbm01**.
- Creates the operating system user ID named **dsrdbm01** that owns the instance.
- Creates an Administrator DN named **cn=root**.
- Creates a default suffix named **o=sample**.

Procedure

1. Log on to the system.

   AIX, Linux, or Solaris
   Log on as `root`.

   Windows
   Log on as an administrator.
2. Use the following steps to prepare and start the installation program:
   a. Access the DVD or extract the files from the archive file that you downloaded from Passport Advantage.
   b. **For AIX, Linux, or Solaris systems:** Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*/

tdsV6.3FP/license directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.

c. Change to the *platform*/tdsV6.3/tds directory.

3. Run the installation program.

   AIX, Linux, or Solaris
   Run install_tds.bin.

   Windows
   Double-click the **install_tds.exe** icon.

4. Complete the installation by using the "Typical installation path" instructions in the IBM Tivoli Directory Server information center. For the IBM Tivoli Directory Server version 6.3 Information Center, see http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm

   Note: Record any passwords that you set during the installation so that you can use them in subsequent installation steps.

5. When the Tivoli Directory Server Instance Administration tool opens.
   a. Verify that the default instance is listed in the configuration.

      Note: If you are using Red Hat Enterprise Linux 6, the default instance is not displayed in the tool. To verify that it is listed in the configuration, use the **idsilist** command. See the IBM Tivoli Directory Server version 6.3 Information Center for details about the command. By default, this command is in /opt/ibm/ldap/V6.3/sbin/.

   b. Do not start the instance.
   c. Exit the tool.

6. Start the configuration process by using the command line. Create the suffix where Security Access Manager maintains its metadata with the **idscfgsuf** command. The command is in the following locations by default:

   AIX, Linux, or Solaris
   /opt/ibm/ldap/V6.3/sbin/idscfgsuf

   Windows
   c:\Program Files\IBM\LDAP\V6.3\sbin\idscfgsuf

   For example, run:

   ```
   idscfgsuf -s "secAuthority=domain_name"
   ```

   where *domain_name* is the management domain name.

   The default suffix is Default; for example:

   ```
   idscfgsuf -s "secAuthority=Default"
   ```

   If you specify a location for the metadata that is not a stand-alone suffix, ensure that the location exists in the LDAP server.

   This suffix is added to the ibmslapd.conf file for the default instance. If you have more than one instance, specify the instance name by using the *-I* option.

7. Optional: You can create additional suffixes to maintain user and group definitions. For example:

   ```
   idscfgsuf -s "c=US"
   ```

8. Start the LDAP server.

   AIX, Linux, or Solaris

```
ibmslapd&
```

Windows

From the **Services** window, start the following services:

```
IBM Tivoli Directory Server Instance V6.3 - instance_name
```

9. **For AIX, Linux, or Solaris systems only:** Update the installation to the appropriate fix pack level.

   Note: For Windows installations, the installation image includes the appropriate fix pack level.

   a. Stop all Tivoli Directory Server services.
   b. Access the DVD or extract the files from the archive file that you downloaded from Passport Advantage.
   c. Change to the appropriate directory for your operating system.

      platform/tdsV6.3FP
   d. See the readme file that is included with the fix pack for information and installation instructions.
   e. Run the installation program.

      ./idsinstall –u -f
10. When the installation completes, verify the installed versions.
    a. Open a command prompt.
    b. Type:

       idsversion

What to do next

- If you are setting up SSL communication, go to "Configuring IBM Tivoli Directory Server for SSL access" on page 69.
- Otherwise, continue with Chapter 6, "Setting up a policy server," on page 103.

Tivoli Directory Server setup with script files

The installation and configuration scripts can automate installations and perform unattended (*silent*) installations and configurations.

AIX, Linux, or Solaris: Automating the setup of Tivoli Directory Server

Use the script file to automate the installation of Tivoli Directory Server.

About this task

Automated installations can complete unattended (*silent*) installations. This task uses the **idsNative Install** command.

Procedure

1. Log on to the system with root privileges.
2. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. Extract the Tivoli Directory Server archive file to a directory with adequate disk space. For example, /tdsV6.3/. If you use a DVD to install Tivoli Directory Server, the files are in the tdsV6.3 directory.
4. Locate the following script files and change the permissions so that you can write to the files:

```
chmod +w image_path/tdsV6.3/responsefile.txt
chmod +w image_path/scripts/ISAMConfigTDS.sh
chmod +w image_path/scripts/ISAMGenSSLCert.sh
chmod +w image_path/platform/tdsV6.3/idsConfigServerSSL.sh
```

5. Install the Tivoli Directory Server license files by completing the following steps:
   a. Navigate to the *image_path*/tdsV6.3FP/license directory.
   b. Run the following script:

      ```
      idsLicense -q
      ```

      where the -q option installs the license files without displaying the license. If you use the -q option, you automatically accept the license without viewing it.
6. In the tdsV6.3 directory, locate the installation program file and the response file:
   - idsNativeInstall.sh
   - responseFile.txt

   These files must be in the same directory.
7. Update the following entries in the responseFile.txt file. By default, the values of the variable are set to false and their corresponding path variables are not set.
   - To install DB2, set the *db2FeatureInstall* variable to true. Update the *db2InstallimagePath* variable with the absolute path where the DB2 installation files are located.

     For example:

     ```
     db2FeatureInstall=true
     db2InstallimagePath=/image_path/platform/tdsV6.3/db2
     ```
   - To install GSKit, set the *gskitFeatureInstall* variable to true. Update the *gskitInstallimagePath* with the absolute path to where the GSKit installation files are located. For example:

     ```
     gskitFeatureInstall=true
     gskitInstallimagePath=/image_path/platform/tdsV6.3/gskit
     ```
   - To install embedded WebSphere Application Server (eWAS), set the *eWasFeatureInstall* variable to true. Update the *eWasInstallimagePath* with the absolute path to where the embedded WebSphere Application Server installation files are located. For example:

     ```
     eWasFeatureInstall=true
     eWasInstallimagePath=/image_path/platform/tdsV6.3/appsrv
     ```
   - To install Tivoli Directory Server, update the *tdsInstallimagePath* with the absolute path to where the Tivoli Directory Server installation files are located. Update the *tdsFixPackInstallimagePath* variable with the absolute path to where the Tivoli Directory Server fix pack installation files are located. For example:

     ```
     tdsInstallimagePath=/image_path/platform/tdsV6.3/
     tdsFixPackInstallimagePath=/image_path/platform/tdsV6.3FP
     ```

     Note: If you want to install the full Tivoli Directory Server , but there are already some Tivoli Directory Server packages installed, such as the client packages, remove the images before you run this script.
8. Save the responseFile.txt file.
9. **For Solaris systems only:**

a. Check that the /export/home directory exists. If the directory does not exist, create it.
b. Ensure that the following kernel parameters in the /etc/system file are set appropriately for your system. The following values are suggested as starting values:

```
set msgsys:msginfo_msgmax = 65535
set msgsys:msginfo_msgmnb = 65535
set shmsys:shminfo_shmmax = 2134020096
```

For more information, see the Solaris tuning documentation.

10. Open a command prompt and start the installation by typing **idsNativeInstall.sh**
11. Verify the installation by checking the installation log: /var/idsldap/V6.3/idsNativeInstall_*timestamp*.log
12. **For AIX, Linux, or Solaris systems only:** Update the installation to the appropriate fix pack level.

    Note: For Windows installations, the installation image includes the appropriate fix pack level.

    a. Stop all Tivoli Directory Server services.
    b. Access the DVD or extract the files from the archive file that you downloaded from Passport Advantage.
    c. Change to the appropriate directory for your operating system.
       platform/tdsV6.3FP
    d. See the readme file that is included with the fix pack for information and installation instructions.
    e. Run the installation program.

```
./idsinstall –u -f
```

13. Optional: If you want to use the Tivoli Directory Server Web Administration Tool, deploy Tivoli Directory Server into the embedded version of WebSphere Application Server:
    a. Open a command prompt.
    b. Run *ldaphome*/idstools/deploy_IDSWebApp. Replace *ldaphome* with the installation path.
14. Create the default instance and suffix:
    a. Open a command prompt.
    b. Change to the following directory: *image_path*/*platform*/tdsV6.3/
    c. Run the following command:

```
idsdefinst -p passworddn -w passworduser -e encryptseed
```

    where:

    passworddn
    The administration DN password. For example, cn=root password.

    passworduser
    The database owner password. For example, the password for the user ID dsrdbm01.

    encryptseed
    The encryption seed value. This value is used to create is used to generate a set of Advanced Encryption Standard (AES) secret key values. The length must be between 12 and 1016 characters.

15. Configure Tivoli Directory Server for Security Access Manager:
    a. Locate the *image_path*/scripts/ISAMConfigTDS.sh file.
    b. Open the file in a text editor.
    c. Set the adminPW to the cn=root password. This password was created when the **idsdefinst** tool was run.
    d. Review the other settings in the file. If you used the default values during the installation of Tivoli Directory Server, no further modification is required.
    e. Save and close the ISAMConfigTDS.sh file.
    f. Open a command prompt.
    g. Run *image_path*/scripts/ISAMConfigTDS.sh. Replace *image_path* with the path to the script files.
    h. Review output messages and verify that the script completed successfully.

       Note: If you used an improper database name, the script might exit with a return code of zero. Review all messages to ensure that the script completed successfully. The default database name is dsrdbm01. You do not need to change the default name if you used the defaults with the **idsdefinst** command.
16. Optional: If you are setting up Suite B and NIST compliance between your user registry and Security Access Manager components, see "Configuring IBM Tivoli Directory Server for SSL access" on page 69. If you want to configure basic SSL, continue with the following steps:
    a. To create a self-signed certificate:
       1) Open *image_path*/scripts/ISAMGenSSLCert.sh in a text editor.
       2) Set the password for the key database with the KEYFILEPWD variable.
       3) Save and close the file.
       4) Run *image_path*/scripts/ISAMGenSSLCert.sh. Replace *image_path* with the path to the script files.

          Note: The self-signed certificate is extracted to am_key.der.
    b. To enable SSL with Tivoli Directory Server:
       1) Open *image_path*/*platform*/tdsV6.3/idsConfigServerSSL.sh in a text editor.
       2) Set the values for the following variables. Values in bold are the typical default values. Use values that are specific and correct for your environment.

          ```
          tdsinstancename=dsrdbm01
          port=389
          ssl_port=636
          serverpwd=
          serverlabel=AMLDAP
          serverkeywithpath=/am_key.kdb
          user_dn=cn=root
          password_dn=
          ```

          Note: The password fields must be set to your passwords.
       3) Save and close the file.
       4) Run *image_path*/*platform*/tdsV6.3/idsConfigServerSSL.sh. Replace *image_path*/*platform* with the path to the Tivoli Directory Server installation files.

What to do next

Continue with Chapter 6, "Setting up a policy server," on page 103.

Windows: Automating the setup of Tivoli Directory Server

Use the script file to automate the installation of Tivoli Directory Server.

About this task

Automated installations can perform unattended (*silent*) installations. This task uses the **install_tdsSilent** command.

Procedure

1. Log on to the system with Administrator privileges.
2. Extract the Tivoli Directory Server archive file to a directory with adequate disk space, for example, `/tdsV6.3/`. If you use a DVD to install Tivoli Directory Server, the files are in the `tdsV6.3` directory.
3. Locate the following script files and change the permissions so that you can write to the files:

   image_path`\tds\optionsFile\InstallServer.txt`
   image_path`\scripts\ISAMConfigTDS.bat`
   image_path`\scripts\ISAMGenSSLCert.bat`
   image_path`\Windows\tdsV6.3\idsConfigServerSSL.bat`

   For example:
   a. For each file previously listed, right-click the file and click **Properties**.
   b. Click the **Security** tab.
   c. In the **Name** list box, select the user or group that you want to change.
   d. In the **Permissions** box, select **Write**.
   e. Click **OK**.
4. In the directory, locate the installation program file and the response file:
   - *image_path*`\windows\`*tdsV6.3*`\tds\install_tdsSilent.exe`
   - *image_path*`\windows\`*tdsV6.3*`\tds\optionsFile\InstallServer.txt`
5. Update the entries in the `InstallServer.txt` file with the appropriate values for your installation. Use the instructions in the text file. For more details, see the topics about the options files for silent installation in the Tivoli Directory Server information center:

   http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm
6. Save the `InstallServer.txt` file.
7. Open a command prompt and change to the following directory:

   image_path`\windows\tdsV6.3\tds`
8. Start the installation by running the following command:

   `install_tdsSilent -is:silent -options` *image_path*`\optionsFiles\InstallServer.txt`

   where *image_path* is the full path to the `optionsFiles` directory.
9. Verify the installation by checking the installation log:

   `C:\Program Files\IBM\LDAP\V6.3\var\ldapinst.log`
10. Create the default instance and suffix:
    a. Open a command prompt.
    b. Change to the following directory: *ldap_home*`\idstools`

c. Run the following command:

```
idsdefinst -p passworddn -w passworduser -e encryptseed
```

where:

passworddn
The administration DN password. For example, `cn=root` password.

passworduser
The database owner password. For example, the password for the user ID `dsrdbm01`.

encryptseed
The encryption seed value. This value is used to create is used to generate a set of Advanced Encryption Standard (AES) secret key values. The length must be between 12 and 1016 characters.

11. Configure Tivoli Directory Server for Security Access Manager:
    a. Locate the *image_path*`\scripts\ISAMConfigTDS.bat` file.
    b. Open the file in a text editor.
    c. Set the `adminPW` to the `cn=root` password.
    d. Review the other settings in the file. If you used the default values during the installation of Tivoli Directory Server, no further modification is required.
    e. Save and close the `ISAMConfigTDS.bat` file.
    f. Open a command prompt.
    g. Run *image_path*`\scripts\ISAMConfigTDS.bat`. Replace *image_path* with the path to the script files.
    h. Verify the configuration by checking the configuration log:
    `C:\Users\Administrator\ConfigTDSforISAM.log`
12. Optional: If you are setting up Suite B and NIST compliance between your user registry and Security Access Manager components, see "Configuring IBM Tivoli Directory Server for SSL access" on page 69. If you want to configure basic SSL, continue with the following steps:
    a. To create a self-signed certificate:
        1) Open *image_path*`\scripts\ISAMGenSSLCert.bat` in a text editor.
        2) Set the password for the key database with the `KEYFILEPWD` variable.
        3) Save and close the file.
        4) Run *image_path*`\scripts\ISAMGenSSLCert.bat`. Replace *image_path* with the path to the script files.

        Note: The self-signed certificate is extracted to `am_key.der`.
    b. To enable SSL with Tivoli Directory Server:
        1) Open *image_path*`\Windows\tdsV6.3\idsConfigServerSSL.bat` in a text editor.
        2) Set the values for the following variables. Values in bold are the typical default values. Use values that are specific and correct for your environment.

```
tdsinstancename=dsrdbm01
port=389
ssl_port=636
serverpwd=
```

```
serverlabel=AMLDAP
serverkeywithpath=C:\am_key.kdb
user_dn=cn=root
password_dn=
```

Note: The password fields must be set to your passwords.

3) Save and close the file.
4) Run *image_path*\Windows\tdsV6.3\idsConfigServerSSL.bat. Replace *image_path* with the path to the Tivoli Directory Server installation files.

What to do next

Continue with Chapter 6, “Setting up a policy server,” on page 103.

Installing Tivoli Directory Server with the Launchpad (Windows only)

Use the Launchpad installation method to install Tivoli Directory Server and its prerequisite software on a computer that is running the Windows operating system.

Before you begin

Complete the following tasks before you set up IBM Tivoli Directory Server:

- Complete the preinstallation tasks that are appropriate for your environment in “Operating system preparation” on page 28.
- Review the general considerations for user registries in “General considerations” on page 52.
- Review the LDAP user registry considerations in “LDAP considerations” on page 52.
- Access the instructions for the "Typical installation path" method in the IBM Tivoli Directory Server version 6.3 Information Center.
  1. Go to http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm.
  2. Search for "Typical installation path."

About this task

The Launchpad uses a graphical user interface to perform step-by-step installation and initial configuration. The Launchpad installs all the prerequisite software, if it is not already installed.

Then, the Launchpad starts the graphical user interface installation for the Tivoli Directory Server component.

This task installs the following components:

- All components required by Tivoli Directory Server.
- All the corequisite products required by Tivoli Directory Server, if they are not already installed. These products include:
  - GSKit
  - DB2

- The embedded version of WebSphere Application Server. This software is required by the Web Administration tool, which is installed automatically as part of the "Typical installation path" method.

This task also completes the following configuration:

- Deploys the Web Administration tool.
- Creates a default directory server instance named `dsrdbm01`.
- Creates the operating system user ID named `dsrdbm01` that owns the instance.
- Creates an Administrator DN named `cn=root`.
- Creates a default suffix named `o=sample`.

Procedure

1. Start the Launchpad.
   a. Locate the `launchpad64.exe` file.

      Note: If you are using archive files, ensure that all of them are extracted into the same directory. For example, ensure that the archive files for the IBM Security Access Manager package and the Tivoli Directory Server packages are extracted into the same directory.
   b. Double-click the file to start the Launchpad.
2. Select the language that you want to use during the installation and click **OK**. The Launchpad Welcome window opens.
3. Click **Next**.
4. Select the **IBM Tivoli Directory Server** component.
5. Click **Next**. The list on the left displays the component you selected and any prerequisite software that is required by that component but that is not already installed.
6. Click **Next**. The installation panel for the first component listed is displayed. An arrow next to a component name on the left indicates that the component is currently being installed. A check mark next to a component name indicates that the component is installed.
7. If the current component is IBM Global Security Kit, click **Install IBM Global Security Kit** to install it. When it completes, continue with step 8.
8. Click **Next**.
9. Respond to the prompts presented during the installation.
10. Click **Next** at the bottom of the Launchpad. The installation wizard for Tivoli Directory Server opens.
11. Respond to the prompts presented during the installation.
12. When prompted for the installation type, select **Typical**.
13. Complete the installation using the "Typical installation path" instructions in the IBM Tivoli Directory Server information center. For the IBM Tivoli Directory Server version 6.3 Information Center, see http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm.

      Note: Record any passwords that you set during the installation so that you can use them in subsequent installation steps.
14. When the Tivoli Directory Server Administrator tool opens.
    a. Verify that the default instance is listed in the configuration.
    b. Do not start the instance.

c. Exit the tool.

15. After Tivoli Directory Server is installed, you are prompted for the `cn=root` password that you provided during the installation.
16. Click the **Configure IBM Tivoli Directory Server** button.
17. When all installations and configurations are completed, a success or failure message is displayed. Take one of the following actions:
    - If the installation completed successfully, click **Next**.
    - If the installation failed or an error is displayed, review the log file in the default `%USERPROFILE%` location, such as `C:\Users\Administrator\ConfigTDSforISAM.log`. Make corrections or reinstall Tivoli Directory Server as indicated by the log file.
18. Click **Finish** to close the Launchpad.

What to do next

- If you are setting up SSL communication, go to "Configuring IBM Tivoli Directory Server for SSL access."
- Otherwise, continue with Chapter 6, "Setting up a policy server," on page 103.

Configuring IBM Tivoli Directory Server for SSL access

Enable SSL to secure communication between the Tivoli Directory Server and the Security Access Manager components.

Before you begin

Complete the following tasks:

- Install and configure Tivoli Directory Server.
- Install GSKit.

About this task

The following high-level steps are required to enable SSL support for Tivoli Directory Server for server authentication. See the information for securing directory communications in the *IBM Tivoli Directory Server Administration Guide* for the details of each step. These steps assume that you already installed and configured the Tivoli Directory Server.

Procedure

1. Create the key database, associated password stash file, and password on the Tivoli Directory Server system. For example, use the gsk8capicmd_64 to create a database, stash file, and password.

   ```
   gsk8capicmd_64 -keydb -create -db /key/myldap.kdb -pw passw0rd
     -type cms -stash -empty
   ```

2. If you do not already have a personal certificate or self-signed certificate, do *one* of the following procedures:

   For a personal certificate:

   a. Request a personal certificate from a certificate authority (CA).
   b. Receive that personal certificate into the key database file.
   c. Add a signer certificate for the certificate authority to the key database file.

   For a self-signed certificate:

a. Create a self-signed certificate. For example,

```
gsk8capicmd_64 -cert -create -db /key/myldap.kdb -pw serverpwd \
-sigalg algorithm_id -label serverlabel
-dn "cn=LDAP_Server,o=sample" -size keysize
```

where:

db Specifies the `.kdb` file that is the key database.

pw Specifies the password to access the key database.

sigalg Specifies the signing algorithm that is used to sign the message. Acceptable values that correspond to a compliance mode are listed in the following table.

Note: This setting requires a minimum version of Tivoli Directory Server 6.3.0.17. Skip this setting if you are using an earlier version of Tivoli Directory Server or if your environment does not require a compliance configuration.

Table 17. Compliance values for the keyfile

Compliance mode planned for Security Access Manager 7.0	*algorithm_id* **value**	*keysize* **value**
none	SHA1WithRSA	2048
fips	SHA1WithRSA	2048
sp800-131-transition	SHA256WithRSA	2048
sp800-131-strict	SHA256WithRSA	2048
suite-b-128	SHA256WithECDSA	256
suite-b-192	SHA384WithECDSA	384

label Specifies the label that is attached to the certificate. The label name is configured in Tivoli Directory Server. Either the label name must match the Tivoli Directory Server configured value, or you must update the name value in Tivoli Directory Server to match the label that you set here.

dn Indicates an X.500 distinguished name. An example format: `CN=common_name, O=organization, C=country`.

size The size of the new key pair to be created. This size ranges in value depending on the key type. **Note:** For some algorithms, you can specify a zero (0) value to use the default key size. This is typically the minimum size that is considered secure. Valid values are:

For RSA algorithms:
`512-4096`; key sizes in this range should be selected as per NIST SP800-131; 8192 is supported for validation only. **Note:** Available key sizes might vary according to security configurations. For example, you cannot generate 512 bit RSA keys in FIPS mode. The default value is `1024`.

For EC algorithms:
`224 - 512` **Note:** GSKit EC key generation only

supports P256, P384, and P521 curves. P521 curve keys use a 512 bit SHA2 hash. Default values are:

- 256 (SHA256)
- 384 (SHA384)
- 512 (SHA512)

b. Extract the certificate in ASCII format. For example, type:

```
gsk8capicmd_64 -cert -extract -db /key/myldap.kdb -pw serverpwd
-label myldap -format ascii -target myldap.cert
```

In a subsequent configuration task, you import this certificate to the signer section of the key database on all client systems that securely communicate with the server. **Note:** A client system is:

- Any Security Access Manager server system.
- Any other system that uses the Tivoli Directory Server client to securely communicate with the Tivoli Directory Server.
- Any system that uses the Security Access Manager Runtime component

See Appendix A, "Secure Sockets Layer (SSL) security setup," on page 305 for details.

3. Configure the Tivoli Directory Server instance to use the certificate in the configuration file.

Note: Create an `ldif` file with the appropriate configuration values in it to perform this step. For more information about `ldif` files, see the *Tivoli Directory Server Administration Guide*. If you do not create an `ldif` file for this step, you must use standard input to enter the configuration.

a. Create an `ldif` file that contains the following values. Use your own value for the values shown in italics.

```
dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSslAuth
ibm-slapdSslAuth: serverAuth
```

Note: Use `serverAuth` or the value that is appropriate for your environment. The other valid value is `serverClientAuth`.

```
dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSecurity
ibm-slapdSecurity: SSL
```

Note: Use `SSL` or the value that is appropriate for your environment. The valid values are `none`, `SSL`, `SSlOnly`, `TLS`, `SSLTLS`.

```
dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSslKeyDatabase
ibm-slapdSslKeyDatabase: /key/myldap.kdb

dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSslCertificate
ibm-slapdSslCertificate: serverlabel

dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSslKeyDatabasepw
ibm-slapdSslKeyDatabasepw: serverpwd
```

b. Save the file and name it. For example, name it`serverauth.ldif`.

c. Run the **`ldapmodify`** command.

```
idsldapmodify -h server.in.ibm.com -p 389 -D cn=root -w root \
-i /home/dsrdbm01/serverauth.ldif
```

where:

h *hostname*
Specifies the host on which the LDAP server is running.

p *port_number*
Specifies an alternate TCP port where the LDAP server is listening. The default LDAP port is 389. If -p is not specified and -Z is specified, the default LDAP SSL port 636 is used.

D *binddn*
Use *binddn* to bind to the LDAP directory. *binddn* is a string-represented DN. When used with -m DIGEST-MD5, it specifies the authorization ID. It can be either a DN or an authzId string that starts with "u:" or "dn:". **Note:** `-D binddn -w passwd` does not call bind functions on superuser DNs.

i *filename*
Specifies the entry modification information from an LDIF file instead of from standard input. If an LDIF file is not specified, you must use standard input to specify the update records in LDIF format.

4. Update the compliance type (such as FIPS), if required for your environment.

Note: This step requires a minimum version of Tivoli Directory Server 6.3.0.17. Skip this step if you are using an earlier version of Tivoli Directory Server or if your environment does not require a compliance configuration.
Create an `ldif` file with the appropriate configuration values in it to perform this step. For more information about `ldif` files, see the *Tivoli Directory Server Administration Guide*. If you do not create an `ldif` file for this step, you must use standard input to enter the configuration.

a. Chose the compliance mode you want to use in your environment.
   - `none`
   - `fips`
   - `sp800-131-transition`
   - `sp800-131-strict`
   - `suite-b-128`
   - `suite-b-192`

   For descriptions of these compliance modes, see the documentation that came with the Tivoli Directory Server fix pack.

b. Create an `ldif` file that contains the appropriate values for the compliance mode you want to use.

Table 18. Compliance attribute values

Compliance mode	Values for **cn=Front End, cn=Configuration**	**Attributes for** cn=SSL, cn=Configuration
none	ibm-slapdSetenv: IBMSLAPD_SECURITY_PROTOCOL= SSLV3,TLS10,TLS11,TLS12	ibm-slapdSecurity: SSLTLS ibm-slapdSslFIPSModeEnabled: false ibm-slapdSslFIPSProcessingMode: false ibm-slapdSslCipherSpec: AES ibm-slapdSslCipherSpec: AES-128 ibm-slapdSslCipherSpec: RC4-128-MD5 ibm-slapdSslCipherSpec: RC4-128-SHA ibm-slapdSslCipherSpec: TripleDES-168 ibm-slapdSslCipherSpec: DES-56 ibm-slapdSslCipherSpec: RC2-40-MD5 ibm-slapdSslCipherSpec: RC4-40-MD5 ibm-slapdSslCipherSpec: TLS_RSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_256_GCM_SHA384 ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_256_CBC_SHA256 ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ibm-slapdSslCipherSpec: TLS_RSA_WITH_RC4_128_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_RC4_128_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
fips	ibm-slapdSetenv: IBMSLAPD_SECURITY_PROTOCOL= TLS10,TLS11,TLS12	ibm-slapdSecurity: SSLTLS ibm-slapdSslFIPsProcessingMode: true ibm-slapdSslCipherSpec: AES ibm-slapdSslCipherSpec: AES-128 ibm-slapdSslCipherSpec: TripleDES-168 ibm-slapdSslCipherSpec: TLS_RSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_256_GCM_SHA384 ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_256_CBC_SHA256 ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Table 18. Compliance attribute values (continued)

Compliance mode	Values for **cn=Front End, cn=Configuration**	Attributes for cn=SSL, cn=Configuration
sp800-131-transition	ibm-slapdSetenv: IBMSLAPD_SECURITY_PROTOCOL= TLS10,TLS11,TLS12	ibm-slapdSecurity: SSLTLS ibm-slapdSslFIPsProcessingMode: true ibm-slapdSslCipherSpec: AES ibm-slapdSslCipherSpec: AES-128 ibm-slapdSslCipherSpec: TripleDES-168 ibm-slapdSslCipherSpec: TLS_RSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_256_GCM_SHA384 ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_256_CBC_SHA256 ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
sp800-131-strict	ibm-slapdSetenv: IBMSLAPD_SECURITY_PROTOCOL=TLS12 ibm-slapdSetenv: IBMSLAPD_SSL_EXTN_SIGALG= GSK_TLS_SIGALG_RSA_WITH_SHA224, GSK_TLS_SIGALG_RSA_WITH_SHA256, GSK_TLS_SIGALG_RSA_WITH_SHA384, GSK_TLS_SIGALG_RSA_WITH_SHA512, GSK_TLS_SIGALG_ECDSA_WITH_SHA224, GSK_TLS_SIGALG_ECDSA_WITH_SHA256, GSK_TLS_SIGALG_ECDSA_WITH_SHA384, GSK_TLS_SIGALG_ECDSA_WITH_SHA512	ibm-slapdSecurity: SSLTLS ibm-slapdSslFIPsProcessingMode: true ibm-slapdSslCipherSpec: TLS_RSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_256_GCM_SHA384 ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_256_CBC_SHA256 ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
suite-b-128	ibm-slapdSetenv: IBMSLAPD_SUITEB_MODE=128	ibm-slapdSecurity: SSLTLS
suite-b-192	ibm-slapdSetenv: IBMSLAPD_SUITEB_MODE=192	ibm-slapdSecurity: SSLTLS

c. Save the file and name it. For example, name it `compmode.ldif`.

d. Run the **ldapmodify** command. Replace the values in italics with your own values.

```
idsldapmodify -h server.in.ibm.com -p 389 -D cn=root -w root \
-i /home/dsrdbm01/compmode.ldif
```

where:

h *hostname*
Specifies the host on which the LDAP server is running.

p *port_number*
Specifies an alternate TCP port where the LDAP server is listening. The default LDAP port is 389. If -p is not specified and -Z is specified, the default LDAP SSL port 636 is used.

D *binddn*

Use *binddn* to bind to the LDAP directory. *binddn* is a string-represented DN. When used with -m DIGEST-MD5, it specifies the authorization ID. It can be either a DN or an authzId string that starts with "u:" or "dn:". **Note:** `-D binddn -w passwd` does not call bind functions on superuser DNs.

i *filename*

Specifies the entry modification information from an LDIF file instead of from standard input. If an LDIF file is not specified, you must use standard input to specify the update records in LDIF format.

5. Make a note of the SSL secure port number on this server. The default secure port number is `636`.
6. Copy the signer certificate and have it available to copy onto the computer on which Security Access Manager components are installed and with which you want to enable SSL communication. In a subsequent task, you add this certificate to the key database on that computer.

What to do next

When you successfully enable SSL communication on the Tivoli Directory Server, continue with Chapter 6, "Setting up a policy server," on page 103.

IBM Tivoli Directory Server for z/OS installation and configuration

Use this task to prepare the LDAP server on z/OS for Security Access Manager.

Particular emphasis is given to configuring Security Access Manager against a Tivoli Directory Server for z/OS that has been configured to use its native authentication facility. This native authentication facility uses a System Authorization Facility (SAF) registry.

These guidelines assume a new LDAP server instance dedicated to the Security Access Manager registry. For more information, consult the *LDAP Server Administration and Use* manual for your particular release of z/OS. This document is available through the z/OS library at:

http://www.ibm.com/systems/z/os/zos/bkserv/

Schema file updates

You must update the z/OS schema to support the current version of Security Access Manager.

This must be done following the application of the schema.user.ldif and schema.IBM.ldif files supplied with the server. For instructions on applying these schema files, see the *IBM Tivoli Directory Server for z/OS Administration and Use* documentation at:

http://www.ibm.com/systems/z/os/zos/bkserv/

To apply the Security Access Manager schema to the Tivoli Directory Server, use the **`ivrgy_tool`** utility. For instructions, see the *IBM Security Access Manager for Web Command Reference*.

Suffix creation

Security Access Manager requires that you create a suffix which maintains Security Access Manager metadata.

You must add this suffix only once, when you first configure the LDAP server. This suffix enables Security Access Manager to easily locate and manage the data. It also secures access to the data, avoiding integrity or corruption problems.

For more information about management domains, and creating a location for the metadata, see "Security Access Manager management domains" on page 104 and "Management domain location example" on page 105.

To add suffixes to the LDAP server's `slapd.conf` file, consult the *Tivoli Directory Server for z/OS Administration and Use* manual at:

http://www.ibm.com/systems/z/os/zos/bkserv/

Note: Restart the LDAP server for changes to take effect.

If you decide to add suffixes after the Security Access Manager policy server has been configured, you must apply the appropriate ACLs to the newly created suffix. You can use the **ivrgy-tool** to apply the ACLs to the new suffix. For more information about the **ivrgy-tool**, see the *IBM Security Access Manager for Web Command Reference*.

See the *Tivoli Directory Server for z/OS Administration and Use Guide* for details on updating the security server configuration file.

Suffix definitions for Security Access Manager

By default, Security Access Manager processes all defined LDAP suffixes.

If there are suffixes defined on the LDAP server that should not be used by Security Access Manager, add them to the */access_mgr_install_dir*`/etc/ldap.conf` file using the `ignore-suffix` keyword when configuring Security Access Manager for LDAP on z/OS.

For example:

```
ignore-suffix = sysplex=UTCPLXJ8
ignore-suffix = "o=Your Company"
ignore-suffix = o=MQuser
```

In this example, the `sysplex=UTCPLXJ8` suffix is used to access the z/OS SDBM (RACF®) database. The LDAP administrator ID used by Security Access Manager during configuration is not a RACF user ID on the z/OS system, and, therefore, does not have the authority to do SDBM searches. If this suffix was not added to the `ignore-suffix` list, Security Access Manager would receive a return code `x'32' - LDAP_INSUFFICIENT_ACCESS`, during configuration.

The other suffixes in the list are used by other applications on z/OS, and can be ignored by Security Access Manager.

Note that Security Access Manager supports LDAP failover and load-balancing for read operations. If you configured a replica server, you can provide the replica host name to Security Access Manager in the `ldap.conf` file, which is installed with Security Access Manager in the `etc` subdirectory.

Native authentication user administration

Native authentication provides the added feature of many-to-one mapping of Security Access Manager users to SAF user IDs.

The majority of administrative tasks remain unchanged with the addition of native authentication. Operations such as **user create**, **user show**, adding a user to an ACL entry or group, and all **user modify** commands (except password) work the same as Security Access Manager configured against any other LDAP registry. Users can change their own SAF passwords with the Web-based **pkmspasswd** utility.

Multiple users can have the same **ibm-nativeId**, and all bind with the same password. For this reason, prevent many-to-one mapped users from changing the SAF password (otherwise there is an increased risk that users might inadvertently lock their peers out of their accounts).

```
pdadmin sec_master> group modify SAFusers add user1
pdadmin sec_master> acl create deny_pkms
pdadmin sec_master> acl modify deny_pkms set group SAFusers T
pdadmin sec_master> acl attach /Webseal/server_name/pkmspasswd deny_pkms
```

Furthermore, there is no out-of-the-box administration command to set the `ibm-nativeId` entry for a user. To that end, the following instructions assist the management of Security Access Manager users with an associated `nativeId`.

The **user create** command does not change:

```
pdadmin sec_master> user create user1 cn=user1,o=tivoli,c=us user1 user1 ChangeMe1
pdadmin sec_master> user modify user1 account-valid yes
```

The password (`ChangeMe1`, in this example) is set to the user's `userpassword` entry in LDAP, which has no effect with native authentication enabled. In production environments, use the utility program provided with the Tivoli Directory Server for z/OS to remove `userpassword` values from LDAP. This prevents password access if native authentication is inadvertently disabled.

To set the `ibm-nativeId` entry for a user, create an `ldif` file, called a *schema file*, similar to the following:

```
dn: cn=user1,o=tivoli,c=us
changetype: modify
objectclass: ibm-nativeAuthentication
ibm-nativeId: SAF_username
```

You can load the `ldif` file using the **ldapmodify** command on z/OS as follows:

```
ldapmodify -h host_name -p port -D bind_DN
-w bind_pwd -f schema_file
```

Note: to run the **idsldapmodify** from an Tivoli Directory Server client on a distributed system, the format of the ldif file changes slightly to:

```
dn: cn=user1,o=tivoli,c=us
objectclass: inetOrgPerson
objectclass: ibm-nativeAuthentication
ibm-nativeId: SAF_username
```

The SAF command to reset a user's password is as follows:

```
ALTUSER SAF_username PASSWORD(new_password)
```

In addition to resetting the password, the command marks the password as expired, which requires the password to be changed during the next login. If desired, the `NOEXPIRED` option can be added to the command to prevent that behavior.

Note: The SAF_username must be defined as a z/OS Unix System Services user. That is, the SAF_username must be defined on z/OS with an OMVS segment. The following is an example of a SAF command to define SAF_username as a UNIX System Services user:

```
altuser SAF_username omvs(home(/u/SAF_username) program(/bin/sh) uid(123456))
```

Note that to use native authentication, you must turn off the `auth-using-compare` stanza entry. To do so, edit the `[ldap]` stanza of the `ivmgrd.conf` and `webseald.conf` file and change the line as follows:

```
auth-using-compare = no
```

By default, authentications to LDAP are made with a compare operation, rather than a bind.

For more information on setting up native authentication, see the *IBM Tivoli Directory Server for z/OS Administration and Use* documentation at:

http://www.ibm.com/systems/z/os/zos/bkserv/

After you configure the IBM Tivoli Directory Server for z/OS for use with Security Access Manager, the next step is to set up the policy server. For instructions, see Chapter 6, “Setting up a policy server,” on page 103.

Configuring IBM Tivoli Directory Server for z/OS for SSL access

When Security Access Manager and LDAP services are not on the same protected network, enable SSL communication between the LDAP server and the clients that support Security Access Manager software. This protocol provides secure, encrypted communications between each server and client. Security Access Manager uses these communications channels as part of the process for making authentication and authorization decisions.

About this task

To configure SSL/TLS communications, consult the *IBM Tivoli Directory Server for z/OS for Administration and Use* manual for your particular release of z/OS. This document is at

http://www.ibm.com/systems/z/os/zos/bkserv/

The following high-level steps are required to enable SSL/TLS support on z/OS. These steps assume that you installed and configured the LDAP directory server, installed z/OS Cryptographic Services System SSL, and set `STEPLIB`, `LPALIB`, or `LINKLIST`.

Procedure

1. Configure the LDAP server to listen for LDAP requests on the SSL port for server authentication and, optionally, client authentication. See “Security options in the ibmslapd.conf file” on page 79.

2. Generate the LDAP server private key and server certificate. Mark the certificate as the default in the key database or key ring, or identify the certificate by using its label on the `sslCertificate` option in the configuration file.

   The z/OS LDAP Server can use certificates in a key ring that is managed with the RACF **RACDCERT** command.

   The **gskkyman** utility, which was used in previous releases, also can be used and an example of using that utility to create a key database file can be found in "Creating a key database file" on page 80.

   More information about the **RACDCERT** command can be found in the *IBM z/OS Security Server RACF Command Language Reference* manual for your particular release of z/OS. This document is at

   http://www.ibm.com/systems/z/os/zos/bkserv/

3. Restart the LDAP server.

Security options in the ibmslapd.conf file

Use the following options for SSL in the `ibmslapd.conf` file.

listen *ldap_URL*
: Specifies, in LDAP URL format, the IP address, (or host name) and the port number where the LDAP server listens to incoming client requests. This parameter can be specified more than one time in the configuration file.

sslAuth {**serverAuth** | **serverClientAuth**}
: Specifies the SSL/TLS authentication method. The **serverAuth** method allows the LDAP client to validate the LDAP server on the initial contact between the client and the server. The **serverAuth** method is the default.

sslCertificate {*certificateLabel* | **none**}
: Specifies the label of the certificate that is used for server authentication. This option is needed if a default certificate is not set in the key database file or key ring, or if a certificate other than the default one is required. If this option is omitted, the default certificate is used.

sslCipherSpecs {*string* | **ANY**}
: Specifies the SSL/TLS cipher specifications that can be accepted from clients. For a complete list of the ciphers that are supported by your z/OS LDAP Server, consult the *IBM Tivoli Directory Server for z/OS Administration and Use* manual for your particular release of z/OS. This document is at

  http://www-03.ibm.com/systems/z/os/zos/bkserv/

sslKeyRingFile *filename* | *keyring*
: Specifies the path and file name of the SSL/TLS key database file or key ring for the server.

sslKeyRingFilePW *string*
: Specifies the password that protects access to the SSL/TLS key database file.

  When a RACF key ring is used instead of a key database file, do not specify this option in the configuration file.

  Note: Use of the **sslKeyRingFilePW** configuration option is discouraged. As an alternative, use either the RACF key ring support or the **sslKeyRingPWStashFile** configuration option. This eliminates this password from the configuration file.

sslKeyRingPWStashFile *filename*

Specifies a file name where the password for the server key database file is stashed. If this option is present, then the password from this stash file overrides the value that is specified for the **sslKeyRingFilePW** configuration option. Use the **gskkyman** utility with the **–s** option to create a key database password stash file.

When a RACF key ring is used instead of a key database file, do not specify this option in the configuration file.

Creating a key database file

The following example shows you how to use the **gskkyman** utility to create a key database file.

Procedure

1. Start the **gskkyman** utility from a shell prompt (OMVS or rlogin session) as follows:

   ```
   $ gskkyman
   ```

2. Enter option 1 to create a new key database file.
3. Type a key database name or accept the default (**key.kdb**).
4. Press Enter
5. Create a password to protect the key database.
6. Re-enter the database password for verification.
7. Type a password expiration interval in days or accept the default (no expiration date).
8. Type a database record length or accept the default (**2500**).
   The key database is created and a message is displayed indicating the success or failure of this operation
9. From the Key Management Menu, select option **6** to create a self-signed server certificate and follow the prompts.
10. After the certificate is created, you must extract this certificate so it can be sent to the LDAP client system and added as a trusted CA certificate. To do so, follow these steps:
    a. Select option 1 to manage keys and certificates.
    b. From the Key and Certificate List, enter the label number of the certificate to be exported.
    c. From the Key and Certificate Menu, enter option 6 to export the certificate to a file.
    d. From the Export File Format dialog, select the export format. For example, select option **1** to export to `Binary ASN.1 DER`.
    e. Enter the export file name.

Results

The certificate is exported. You can now transfer the exported file to the LDAP client system, and add it as a trusted CA certificate. Since the file format of `binary DER` is specified on the export, this same file type must be specified to the **gsk7ikm** utility on the LDAP client system during the **Add** operation.

What to do next

Continue with Chapter 6, “Setting up a policy server,” on page 103.

Installing and configuring Microsoft Active Directory

Install and configure Microsoft Active Directory using the documentation provided with the product. This task summarizes the steps and highlights information that is specific to setting up Active Directory in a Security Access Manager environment.

Before you begin

Before you create and setup an Active Directory domain, set up a DNS server to host the Active Directory domain. Change the TCP\IP setting to have the DNS server point to the computer where Active Directory is configured.

Review all the considerations in the following topics:

- "URAF considerations" on page 53
- "Microsoft Active Directory Server considerations" on page 54

About this task

Use the Microsoft Active Directory documentation to perform the steps outlined in this task.

Procedure

1. Use the **dcpromo** to install Active Directory Domain Services.
2. After the domain is created and the computer restarts, verify that the DNS service location records have been created:
   a. Start the DNS Administrator Console. Click **Start** > **Administrative Tools** > **DNS**.
   b. Expand the server name, **Forward Lookup Zones**, and the domain.
   c. Verify that the following folders are present:
      - **_msdcs**
      - **_sites**
      - **_tcp**
      - **_udp**

      These folders and the service location records they contain are critical to Active Directory and Windows Server operations.
3. Join the computer to the Active Directory domain.
4. Create a user in the domain.
5. Add the user to the Active Directory Admin Groups.
6. Raise the domain to a functional level.
7. Create an Authorization Store.
8. Create a dynamic group in the Authorization Store.
9. Add Enterprise Administrator privileges to the Active Directory Store Administrator Role.

   By default, the Authorization Store can be managed only by the domain administrator where the Authorization Store is created.

   To use the Dynamic Group support in the Security Access Manager multiple domain environment, add the Enterprise Administrator group to the Administrator Role. As a result, the dynamic groups from Active Directory domains outside the root domain can be used with Security Access Manager.

10. Change the following Active Directory replication settings to the intervals at which you want notifications to occur between the domain controller and its replication partners.
    - **Replicator notify pause after modify (secs)**
    - **Replicator notify pause between DSAs (secs)**
11. If you want to enable SSL to secure communication between Active Directory and the Security Access Manager components, complete the remaining steps. SSL encrypts the data that is transmitted between the Security Access Manager services and Active Directory to provide data privacy and integrity. Consider enabling SSL to protect information such as user passwords and private data. SSL is not required for Security Access Manager to operate.
    a. Create a certificate that contains the public and private key on the computer where Active Directory is installed. See the Microsoft documentation for Windows and Active Directory.
    b. Verify that SSL is configured and that port 636 is in use.
    c. Export the certificate *without* its private key. Keep a copy of this certificate available. After all of your Security Access Manager systems are installed, you import this certificate on each of those systems.

What to do next

After you set up an Active Directory domain for use with Security Access Manager, the next step is to set up the policy server on a Windows system. For instructions, see Chapter 6, "Setting up a policy server," on page 103.

Microsoft Active Directory Lightweight Directory Service (AD LDS) installation and configuration

Use this task to prepare the AD LDS server for use with Security Access Manager.

Before you install Microsoft Active Directory Lightweight Directory Service, read "Installing and configuring Active Directory Lightweight Directory Service (ADLDS) for Security Access Manager," which provides a summary of important Security Access Manager considerations and requirements when installing and configuring AD LDS.

For complete download, installation and configuration instructions, see the AD LDS documentation provided by Microsoft Corporation.

Installing and configuring Active Directory Lightweight Directory Service (ADLDS) for Security Access Manager

The following overview provides guidelines for installing and configuring Active Directory Lightweight Directory Service (ADLDS) to use as a user registry with Security Access Manager.

Procedure

1. When installing ADLDS, log on to the system using an account that belongs to the local Administrators group. Use the Active Directory Lightweight Directory Service Setup Wizard to configure your ADLDS instance.
2. When you create an ADLDS instance, you must specify an ADLDS instance name which will be used to uniquely identify the instance and name the ADLDS service.

3. Specify the ports used for both non-SSL and SSL connection types within the ADLDS instance. Make note of the port numbers you specify because they must be entered when you configure Security Access Manager.
4. On the Application Directory Partition pane of the Active Directory Lightweight Directory Service Setup Wizard, create an application directory partition to contain the user and group definitions that you use.

   Below the directory partition, you can create other Directory Information Tree (DIT) entries as needed.
5. On the Importing LDIF Files pane of the Active Directory Lightweight Directory Service Setup Wizard, import the following LDIF files to update the schema used by this instance of ADLDS:
   - MS-InetOrgPerson.LDF
   - MS-User.LDF
   - MS-UserProxy.LDF
6. When you finish installing ADLDS, ensure that the installation completed successfully and did not contain any errors. `adamsetup.log` and `adamsetup_loader.log` contain information that can help you troubleshoot ADLDS setup failure.

Configuring the Security Access Manager schema for Active Directory Lightweight Directory Service (AD LDS)

Security Access Manager defines its own set of LDAP entry types and attributes that it uses to track user, group, and policy information.

Before you begin

Prior to adding Security Access Manager schema extensions, ensure that you have defined inetOrgPerson and user schema definitions included with AD LDS. If the inetOrgPerson and user schema extensions have not been added yet, they can also be added using the **ldifde.exe** command-line tool and should be done prior to adding the Security Access Manager schema.

About this task

These extensions to the basic LDAP server schema must be added to Active Directory Lightweight Directory Service (AD LDS) before configuring Security Access Manager.

After you install AD LDS and configure the AD LDS instance using the Active Directory Lightweight Directory Service Setup Wizard, the Security Access Manager schema extensions can be added to AD LDS using the **ldifde.exe** command-line tool included with AD LDS.

To add inetOrgPerson and user schema extensions, use the following procedure. After you run these commands, the AD LDS schema will include the AD LDS, inetOrgPerson and user objectclasses and attribute definitions. If these schema extensions have already been added, you can skip this procedure:

Procedure

1. Apply the `tam-adamschema.ldf` schema file on the AD LDS server. The file is in the following directories:
   - AIX®: `/opt/PolicyDirector/etc`
   - Solaris: `/opt/PolicyDirector/etc`

- Linux: `/opt/PolicyDirector/etc`
- Windows: *`install base`*`\etc`

  Where *`install-base`* is the installation directory. The default directory is `C:\Program Files\Tivoli\Policy Director`.

Note: Although `tam-adamschema.ldf` is installed as part of the Security Access Manager runtime component on all platforms, you must apply the schema on the AD LDS server, which runs on a Windows platform only. If you use Security Access Manager on an operating system other than Windows when using AD LDS, you must copy the schema definition file from the Security Access Manager runtime installation to the Windows system on which AD LDS is running.

2. Click **Start** > **Programs** > **Accessories**.
3. Right-click **Command Prompt**.
4. Click **Run as administrator**.
5. At the command prompt, type the following command and then press Enter:

   ```
   ldifde –i –f ms-inetorgperson.ldf –s servername:portnumber –k –j . –c
    "CN=Schema,CN=Configuration,DC=X" #schemaNamingContext
   ```

   where *servername* represents the workstation name and *portnumber* is the LDAP connection port of your AD LDS instance. If AD LDS is running on your local workstation, you can also use `localhost` as the workstation name.
6. Type the following command, and then press Enter:

   ```
   ldifde –i –f ms-user.ldf –s servername:portnumber –k –j . –c
    "CN=Schema,CN=Configuration,DC=X" #schemaNamingContext
   ```

   where *servername* represents the workstation name and *portnumber* is the LDAP connection port of your AD LDS instance. If AD LDS is running on your local workstation, you can also use `localhost` as the workstation name.
7. After you have ensured that the AD LDS schema includes the inetOrgPerson and user definitions, add the Security Access Manager schema extensions:
   a. Click **Start** > **Programs** > **Accessories**.
   b. Right-click **Command Prompt**.
   c. Click **Run as administrator**.
   d. At the command prompt, type the following command and then press Enter:

      ```
      ldifde –i –e –f tam-adamschema.ldf –s servername:portnumber –k –j . –c
       "CN=Schema,CN=Configuration" #schemaNamingContext
      ```

      where *servername* represents the workstation name and *portnumber* is the LDAP connection port of your AD LDS instance. If AD LDS is running on your local workstation, you can also use `localhost` as the workstation name. The `tam-adamschema.ldf` file is included with the Security Access Manager AD LDS feature.

Management domain data location for Active Directory Lightweight Directory Service (AD LDS)

The user registry creates and stores metadata that tracks information about the Security Access Manager management domain. You must specify the location for the metadata storage.

The management domain is created when the Security Access Manager policy server is configured. The management domain is the initial security domain.

During policy server configuration, the administrator specifies the name of the management domain or uses the default name of `Default`.

The administrator also specifies the location in the registry where this metadata is stored by specifying the management domain location DN. The location that is specified must exist in the user registry. If the administrator chooses to use the default management domain location, the information is maintained in specific Active Directory Lightweight Directory Service (AD LDS) partition, which must be called

`secAuthority=`*`management_domain_name`*

where *management_domain_name* is the management domain name specified. For example, if the default management domain name is used, the partition would be called `secAuthority=Default`. If the administrator does not use the default location and specifies the management domain location DN, any existing location within the AD LDS registry can be used as long as it is a container object.

Note: You must choose a location DN within the same directory partition where the user and group information is stored. AD LDS requires the policy server to exist in the same directory partition as the user and group information.

The policy server cannot maintain user and group information that is outside of the AD LDS directory partition where the policy server itself is defined.

For this reason, do not use the default management location during policy server configuration when AD LDS is used as the Security Access Manager registry. Instead, choose a management domain location within the AD LDS partition in which you wish to maintain the user and groups which reflects your enterprise structure.

Attention: If you chose the default management location during policy server configuration, the option to permanently remove domain information from registry deletes all data in the AD LDS partition of the default domain management location, including registry-specific data, when you unconfigure the Security Access Manager. To retain registry-specific data, choose the management domain location in the AD LDS partition in which you want to maintain users and groups. The default management location is the location for Security Access Manager metadata.

Configuring a Security Access Manager directory partition

By default, Security Access Manager maintains its metadata information within a specific Active Directory Lightweight Directory Service (AD LDS) directory partition (also known as a naming context or suffix). This default Security Access Manager metadata directory partition is called `secAuthority=Default`.

About this task

You must create the partition after the Security Access Manager schema extensions are added to AD LDS and before the Security Access Manager Policy Server is configured. For more information about adding schema extensions, see “Configuring the Security Access Manager schema for Active Directory Lightweight Directory Service (AD LDS)” on page 83.

To create the default Security Access Manager metadata directory partition, use the AD LDS administration tool **ldp.exe**. This tool is installed as part of the AD LDS administration tool set. To use the**ldp.exe** tool, you must connect and bind to the AD LDS instance using the following procedure.

Alternatively, you can choose a non-default Management Domain name and location DN. The Management Domain name must be unique within the LDAP server and the location DN must already exist. You are prompted for this information during installation of the policy server; see Appendix D, "pdconfig options," on page 317 for instructions on how to set these parameters for the Security Access Manager Policy Server.

Note: You must choose a location DN within the same directory partition where you will store user and group information. This is required because AD LDS requires that the policy server must exist in the same directory partition in which user and group information is maintained. The policy server cannot maintain user and group information outside the directory partition in which the policy server itself is defined.

Procedure

1. Connect to the AD LDS instance:
   a. At a command prompt, type `ldp` and then press **ENTER**. The **ldp** window is displayed.
   b. On the **Connection** menu, click **Connect....**
   c. In the **Server** field, type the host or DNS name of the system running AD LDS. When the AD LDS instance is running locally, you can also type `localhost` for this field value.
   d. In the **Port** field, type the LDAP or SSL port number for the AD LDS instance to which you want to connect. Then click **OK**. The ldp tool connects to the AD LDS instance and displays progress information obtained from the root DSE in the pane on the right side of the window.
2. Bind to the AD LDS instance:
   a. From the **Connection** menu, select **Bind...**
   b. To bind using the credentials you are logged on with, click **Bind as currently logged on user**.
   c. When you are finished specifying bind options, click **OK**. The ldp tool will bind to the AD LDS instance using the method and credentials specified.
3. Add children:
   a. From the **Browse** menu, select **Add child**.
   b. In the **Dn** field, type `secAuthority=Default` as the distinguished name for the new directory partition.
   c. In the **Edit Entry** field, type the following and then click **ENTER**.
      - In the **Attribute** field, type `ObjectClass`.
      - In the **Values** field, type `secAuthorityInfo`.
   d. In the **Edit Entry** field, type the following and then click **ENTER**.
      - In the **Attribute** field, type `secAuthority`.
      - In the **Values** field, type `Default`.
   e. In the **Edit Entry** field, type the following and then click **ENTER**.
      - In the **Attribute** field, type `version`.
      - In the **Values** field, type `7.0`.

f. In the **Edit Entry** field, type the following and then click **ENTER**.
   - In the **Attribute** field, type `cn`
   - In the **Values** field, type `secAuthority`

g. In the **Edit Entry** field, type the following and then click **ENTER**.
   - In the **Attribute** field, type `instanceType`.
   - In the **Values** field, type `5`.

   The set of attributes and values appear in the Entry List pane.

h. Ensure the **Synchronous** option is selected and click **Run**. This will add the required Security Access Manager metadata directory partition to the AD LDS instance. To verify that the partition has been properly added, you can use the AD LDS ADSI Edit tool to connect to and view the partition.

Adding an administrator to the Security Access Manager metadata directory partition

After adding Security Access Manager schema to the Active Directory Lightweight Directory Service (AD LDS) instance, and specifying the Security Access Manager metadata directory location, add an AD LDS user administrator for the Security Access Manager metadata directory partition. The AD LDS user has administrative authority for the Security Access Manager metadata directory partition and is specified as the LDAP administrator during Security Access Manager configuration.

About this task

The following example assumes that you accepted the default management domain and location. If you specified a different domain name or location, add the AD LDS user administrator to the AD LDS partition you specified.

Procedure

1. Create the AD LDS LDAP administrator:
   a. Start the ADSI Edit program (`Adsiedit.msc`).
   b. On the **Action** menu, click **Connect To...** The "Connection Settings" dialog box appears.
   c. In the **Connection name** field, you can type a label under which this connection will appear in the console tree of AD LDS ADSI Edit. For this connection, type: `secAuthority`.
   d. In the **Server name** field, type the host or DNS name of the system on which the AD LDS instance is running. If the AD LDS instance is on the local system, you can use `localhost` as the server name.
   e. In the **Port** field, type the LDAP or SSL communication port in use by this AD LDS instance.

      Note: To list the port numbers that are used by AD LDS instances, at the command prompt, type:

      ```
      dsdbutil "list instances" quit
      ```

      on the system where the AD LDS instance is running.
   f. Under **Connect to the following node**, select **Distinguished name (DN) or naming context** and enter `"secAuthority=Default"` for the default distinguished name. If you use a different directory partition, select that partition. This example assumes the default partition.

g. Under **Connect using these credentials**, click **The account of the currently logged on user**.
h. Click **OK**. The term, secAuthority, should now appear in the console tree.

2. Select user attributes:
   a. Expand the secAuthority tree by double-clicking **secAuthority** and then double-click on **SECAUTHORITY=DEFAULT**.
   b. Highlight and right click the **SECAUTHORITY=DEFAULT** container, point to **New,** and then click **Object...**
   c. Under **Select a class**, click **user**.
   d. Click **Next**.
   e. For the value of the `cn` attribute, type the common name for the administrator you want to create. For example, type `tam`.
   f. Click **Next**.
   g. Click **More Attributes**.
   h. Select and set the following properties:

      msDS-UserDontExpirePassword
      Set to **True**. This setting prevents the default password expiration time policy from applying to this administrator. If you would prefer that the password policy applies to this administrator, then this property can be left unset.

      msDS-UserAccountDisabled
      Set to **False**. This setting enables the instance that you created.

   i. Click **OK**.
   j. No additional attributes are required but if you want to set more attributes, click **More Attributes**, select the attributes that you wish to set and enter the values. When you are finished, click **Finish**. The user is created with a Distinguished Name (DN) of `cn=tam,secAuthority=Default`.
   k. To set the administrator password, highlight and then right click the user you created. Select **Reset password...**
   l. In the "Reset Password" pane, enter and confirm the password that you wish to use. When finished, click **OK**. Remember the user DN and password that you create because this will be specified as the LDAP Administrator DN and password when Security Access Manager is configured.

3. Add the user to the Administrators group for the partition:
   a. Within the SECAUTHORITY=DEFAULT directory partition, there are three containers that are called CN=LostAndFound, CN=NTDSQuotas and CN=Roles.
      1) Highlight the **CN=Roles** container by single clicking it. In the details pane on the right side of the AD LDS ADSI Edit tool, the groups within the Roles container will be displayed.
      2) Highlight the **CN=Administrators** group by clicking it once.
      3) Right-click on the **CN=Administrators** group and select **Properties**. The **CN=Administrators Properties** page is displayed.
   b. Under **Attributes**, scroll down to locate and click member.
   c. Click **Edit**.
   d. Click **Add ADLDS Account...**. Type the distinguished name of the administrator user that you created into the **DN** field.
   e. Click **OK**. The administrator user is added to the Administrators group and is displayed as a member.

f. Click **OK** to complete the membership update. Click **OK** to close the "CN=Administrators Properties" page.

Allowing anonymous bind

In order for Security Access Manager to be configured with Active Directory Lightweight Directory Service (AD LDS), AD LDS must be configured to allow anonymous bind.

About this task

By default, AD LDS does not allow anonymous bind. Security Access Manager configuration, however, uses anonymous bind to check on the validity of the configured LDAP hostname, port, and SSL parameters.

If you want to disable anonymous bind during normal operation, you can reset the option on the AD LDS server after configuration is complete.

Procedure

1. Click **Start** > **All Programs** > **ADLDS** > **ADLDS ADSI Edit**.
2. In the console tree, click **ADLDS ADSI Edit**.
3. From the **Action** menu, click **Connect To...** . The "Connection Settings" dialog box appears.
4. In the **Connection name** field, type: `Configuration`.
5. In the **Server name** field, type the host or DNS name of the system on which the AD LDS instance is running. If the AD LDS instance is on the local system, you can use `localhost` as the server name.
6. In the **Port** field, type the LDAP or SSL communication port in use by this AD LDS instance.

   Note: To list the port numbers that are used by AD LDS instances, click **Start** > **All Programs** > **ADLDS** > **ADLDS Tools Command Prompt**. At the command prompt, type: `dsdbutil "list instances" quit` on the system where the AD LDS instance is running.
7. Under **Connect to the following node**, select **Well-known naming context:** and choose **Configuration** from the pull down list.
8. Under **Connect using these credentials**, click **The account of the currently logged on user**.
9. Click **OK**. Configuration now displays in the console tree.
10. Expand the Configuration subtree by double-clicking **Configuration**.
11. Double-click **CN=Configuration,CN=**{*GUID*}, where *GUID* was generated when the configuration of the AD LDS instance was performed.
12. Double-click the **CN=Services** folder to expand it, then double-click **CN=Windows NT**.
13. Highlight and right-click **CN=Directory Service** and click **Properties**.
14. Click **dsHeuristics**.
15. Click **Edit**.
16. Edit the value. Modify the seventh character (counting from the left) to 2. The value should be similar to `0000002001001` in the String Attribute Editor.
17. Click **OK**.
18. Click **OK**. Anonymous bind is now allowed.

What to do next

- If you are setting up SSL communication, go to "Configuring Active Directory Lightweight Directory Service (AD LDS) to use SSL."
- Otherwise, continue with Chapter 6, "Setting up a policy server," on page 103.

Configuring Active Directory Lightweight Directory Service (AD LDS) to use SSL

Enable SSL to secure communication between the Active Directory Lightweight Directory Service and the Security Access Manager components.

Before you begin

Install and configure Active Directory Lightweight Directory Service, including the Internet Information Service and the Web Management Service.

About this task

SSL encrypts the data that is transmitted between the Security Access Manager services and Active Directory Lightweight Directory Service. Consider enabling SSL to protect information such as user passwords and private data. SSL is not required for Security Access Manager to operate.

The following task summarizes the steps that are required for enabling SSL communications.

Note: For details about enabling SSL on Active Directory Lightweight Directory Service, see the Microsoft documentation for Windows 2008 and Active Directory Lightweight Directory Service.

Procedure

1. Create a certificate that contains the public and private key on the computer where Active Directory Lightweight Directory Service is installed.
2. Export the certificate with its private key.
3. Locate the exported key file, double-click it, and install the certificate in all the folders in the Personal and Trusted Authorities folder.
4. Using the mmc console, import this certificate into the Personal and Trusted Root certificate authorities folders for the Active Directory Lightweight Directory Service instance.
5. Change the file permissions of the private keys in the certificate. See the Microsoft documentation for details.
6. Restart the Active Directory Lightweight Directory Service instance.
7. Using the mmc console, export the certificate (*do not export the private key)* from the *AD_LDS_instance*\Personal folder and save the certificate as a `.cer` file.
8. Copy this `.cer` file to the computer where the Security Access Manager component is installed. Use this certificate to configure Security Access Manager with SSL enabled.

What to do next

After you successfully enabled SSL communication on the Active Directory Lightweight Directory Service, continue with Chapter 6, "Setting up a policy server," on page 103.

Novell eDirectory installation and configuration

Use this task to set up Novell eDirectory as the user registry in your Security Access Manager environment.

Before you begin, ensure that you completed the basic server installation and configuration for Novell eDirectory and the ConsoleOne tool as described in the Novell product documentation.

Note: If you are setting up SSL communication between your user registry and Security Access Manager components, see Appendix A, "Secure Sockets Layer (SSL) security setup," on page 305.

Configuring the Novell eDirectory for Security Access Manager

If you are installing a new Security Access Manager secure domain, the Security Access Manager schema is installed on the Novell eDirectory Server (NSD) automatically when the Security Access Manager policy server is configured. However, before configuring the policy server, you must make several modifications to Novell eDirectory server.

About this task

Note: The default Novell eDirectory schema assumes that the directory does not use the X.500 object classes of `inetOrgPerson` or `groupOfNames`. By default, these classes are mapped into the eDirectory classes of User and Group. Because Security Access Manager uses the `inetOrgPerson` and `groupOfNames` object classes for creating its own users and groups, modifications to the default eDirectory schema are required.

You can configure the Novell eDirectory for Security Access Manager by using either of the following tools:

- Novell eDirectory ConsoleOne directory management utility
- Novell iManager web-based administration console

To configure Novell eDirectory for Security Access Manager by using the Novell eDirectory ConsoleOne directory management utility, complete the following steps:

Procedure

1. Start the Novell ConsoleOne directory management utility.
2. Select the organization object within your Novell eDirectory tree. A list of objects is displayed on the right side of the ConsoleOne window.
3. Right-click the **LDAP group** object (not LDAP server), and click **Properties** from the menu.
4. Click the **Class Map** tab and the table of LDAP class names. The Novell eDirectory class names are displayed.
5. Delete the entries with LDAP classes of `inetOrgPerson` and `groupOfNames`.
6. Click **Apply**.
7. Click **Close**.
8. Click the **Attribute Map** tab and the table of LDAP attribute names. The Novell eDirectory attribute names are displayed.

9. Scroll through the table and find the Novell eDirectory attribute `member`. Check the value of the corresponding LDAP attribute. If the LDAP attribute value is `member`, then no change is needed. If the attribute is showing the default value of `uniqueMember`, you need to modify it as follows.
   - Click **Modify**. The Attribute Mapping window is displayed.
   - Change the **Primary LDAP Attribute** field from `uniqueMember` to `member`.
   - Change the **Secondary LDAP attribute** field from `member` to `uniqueMember`.
   - In the Attribute window, click **OK** to accept the changes.
10. If you are using Solaris, proceed to the next step. If you are using Windows NT, you might add another mapping for the LDAP attribute `ndsHomeDirectory` as follows:
    - On the right side of the Attribute Mappings window, click **Add**. The Attribute Mapping window repaints and is displayed again.
    - From the Novell eDirectory **NSD Attribute** field menu, click **Home Directory**.
    - In the **Primary LDAP Attribute** field, click `ndsHomeDirectory`.
    - In the Attribute Mapping window, click **OK** to accept the changes.
11. In the Properties window, click **OK**.

To configure Novell eDirectory for Security Access Manager by using the Novell iManager web-based administration console, complete the following steps:

Procedure

1. Launch the iManager web page and log in as the administrator for the Novell eDirectory tree to be updated.
2. Click the **Roles and Tasks** icon at the top of the iManager window to open the Roles and Tasks view.
3. In the Roles and Tasks navigation frame, expand the **LDAP** category.
4. In the expanded list, click the **LDAP Options** task.
5. On the LDAP Options page, click the LDAP Group listed.

   Note: If the LDAP group object is missing, make sure that the plug-ins for eDirectory were installed when eDirectory was installed. You can download the eDir_88_iMan27_Plugins.npm from the Novell Download Site at http://download.novell.com.
6. Click **Class Map** to display the Novell eDirectory class to LDAP class mappings.
7. Remove mappings to `inetOrgPerson` and `groupOfNames`.
   - Scroll through the list and look for mappings of eDirectory classes to the LDAP class `inetOrgPerson`.
   - If a mapping exists, select the row and click the **Remove Mapping** icon to remove the mapping.
   - Click **OK** in the pop-up window to confirm the removal of the mapping.
   - Click **Apply** to apply the changes.
   - Repeat this step to remove a mapping for the LDAP class `groupOfNames`.
8. Click **OK**, to accept the changes that you made.
9. In the Roles and Tasks navigation frame, expand the **LDAP** category.
10. In the expanded list, click the **LDAP Options** task.
11. On the LDAP Options page, click the LDAP Group listed.

12. Click **Attribute Map** to access the Novell eDirectory attribute to LDAP attribute mappings.
13. Scroll through the table and find the Novell eDirectory attribute member. Check the value of the corresponding LDAP attribute. If the LDAP attribute value is `member`, no change is needed. If the attribute is showing the default value of `uniqueMember`, you need to modify it as follows:
    - Select the row and click the **View/Edit Mapping** icon.
    - Change the **Primary LDAP Attribute** field from `uniqueMember` to `member`.
    - Change the **Secondary LDAP attribute** field from `member` to `uniqueMember`.
    - Click **OK** in the pop-up window to confirm the change.
    - Click **Apply** to apply the changes.
14. Enable LDAP clear-text passwords.

    Follow steps 1 - 10 of the **Enabling LDAP Clear-Text Passwords** procedure from the Novell Access Manager 3.1 Documentation, *6.4.4 Configuring an Identity Injection Policy for Basic Authentication* section in: http://www.novell.com/documentation//novellaccessmanager31/basicconfig/data/b6z0c3k.html#bbk7tko.
15. If you are using Solaris, proceed to the next step. If you are using Windows, you might need to add another mapping for the LDAP attribute `ndsHomeDirectory`. To add another mapping for the LDAP attribute `ndsHomeDirectory`:
    - Click the **Add Mapping** icon in the right side of the window. A pop-up window to define the mapping is displayed.
    - In the **eDirectory Attribute** field, select **Home Directory**.
    - In the Primary LDAP Attribute field, type `ndsHomeDirectory`.
    - Click **OK** to confirm the mapping and close the pop-up window.
16. Click **OK** in the Attribute Map window to accept the changes.

After you set up Novell eDirectory for use with Security Access Manager, the next step is to set up the policy server. For instructions, see Chapter 6, “Setting up a policy server,” on page 103.

Users and groups in Novell eDirectory

Novell eDirectory defines the objectclasses `User` and `Group` as part of its base schema. Instances of these objectclasses are created by an eDirectory administrator when defining a user or a group respectively.

Both of these objectclasses are defined by eDirectory as *leaf nodes*. eDirectory adds an attribute `X-NDS_NOT_CONTAINER '1'` to each of these objectclass definitions that specifies that they are not container objects. Objects that are not specified as container objects cannot be defined beneath instances of these objectclasses.

Security Access Manager requires the ability to append its own objects beneath pre-existing eDirectory users and groups in order to import them and make them usable by Security Access Manager. When Security Access Manager adds its own objectclass definitions to the eDirectory schema, it also redefines the eDirectory `User` and `Group` objectclasses to allow instances of these classes to be container objects. Novell eDirectory allows this change to its schema definition.

The following Novell eDirectory administrator actions will cause the Security Access Manager modification to the `User` objectclass to be undone. The `Group` objectclass is not affected.

- Running the eDirectory database repair tool, **ndsrepair** using the **rebuild schema** option.
- Running Basic Repair from the iManager console and running **local database repair** using the **rebuild operational schema** option.
- Applying a patch update to Novell eDirectory.
- Upgrading Novell eDirectory to a more recent version.

Should it be necessary to perform any of these operations after Security Access Manager has been configured into the eDirectory server, run the following Security Access Manager utility immediately to ensure that the definition of the `User` objectclass is restored.

```
ivrgy_tool -h host -p port -D dn -w password schema
```

where:

host Specifies the LDAP server (Novell eDirectory) host name, which is required.

port Specifies the LDAP server (Novell eDirectory) port number.

dn Specifies the LDAP server (Novell eDirectory) bind distinguished name.

password
Specifies the LDAP server (Novell eDirectory) bind password.

schema Specifies the name of the Novell eDirectory schema file.

The **ivrgy_tool.exe** is located in the `sbin` subdirectory. For example:

- On Windows systems: `d:\Program Files\Tivoli\Policy Director\sbin`
- On AIX, Linux, or Solaris systems: `/opt/PolicyDirector/sbin`

You must run this utility from the `sbin` directory because Security Access Manager does not add the `sbin` directory to the system `PATH`. For more information about this utility, see the *IBM Security Access Manager for Web Command Reference*.

Management domain location

Security Access Manager permits you to specify a management domain location which maintains Security Access Manager metadata unless you use the default management domain location.

Create this location in the Novell eDirectory server before configuring the Security Access Manager policy server.

Security Access Manager extends the Novell eDirectory schema to add Security Access Manager metadata objectclasses and attributes. The `secAuthorityInfo` objectclass, a Security Access Manager-defined objectclass, is explicitly defined to be contained under the following common objectclasses:

- `treeRoot`
- `container`
- `organization`
- `organizationalUnit`
- `domain`
- `country`

The Novell eDirectory strictly enforces the containment rule. If you specify a management domain location with an objectclass other than the common objectclasses listed here, you must manually modify the schema file `novschema.def` to include the objectclass.

Note: You must modify the schema file before you configure the Security Access Manager.

The complete Security Access Manager Novell eDirectory schema file path is *[Security Access Manager installation directory]*`/etc/novschema.def`. The following example illustrates how to modify the schema file.

1. Open the schema file.
2. Replace this portion:

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectClasses: (
1.3.6.1.4.1.4228.1.8
NAME 'secAuthorityInfo'
DESC 'Security Authority Information'
SUP 'eApplicationSystem'
STRUCTURAL
MUST ( secAuthority $ version )
X-NDS_NAMING 'secAuthority'
X-NDS_CONTAINMENT ( 'treeRoot' )
 )
-
add: objectclasses
objectClasses: (
1.3.6.1.4.1.4228.1.8
NAME 'secAuthorityInfo'
DESC 'Security Authority Information'
SUP 'eApplicationSystem'
STRUCTURAL
MUST ( secAuthority $ version )
X-NDS_NAMING 'secAuthority'
X-NDS_CONTAINMENT ( 'treeRoot' 'container' 'organization'
 'organizationalUnit' 'domain' 'country')
 )
```

   with

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectClasses: (
1.3.6.1.4.1.4228.1.8
NAME 'secAuthorityInfo'
DESC 'Security Authority Information'
SUP 'eApplicationSystem'
STRUCTURAL
MUST ( secAuthority $ version )
X-NDS_NAMING 'secAuthority'
X-NDS_CONTAINMENT ( 'treeRoot' )
 )
-
add: objectclasses
objectClasses: (
1.3.6.1.4.1.4228.1.8
NAME 'secAuthorityInfo'
DESC 'Security Authority Information'
SUP 'eApplicationSystem'
STRUCTURAL
MUST ( secAuthority $ version )
```

```
X-NDS_NAMING 'secAuthority'
X-NDS_CONTAINMENT ( 'treeRoot' 'container' 'organization'
'organizationalUnit' 'domain' 'country'
 'your_object_class_goes_here')
 )
```

For more information about management domains and creating a location for the metadata, see “Security Access Manager management domains” on page 104 and “Management domain location example” on page 105.

SSL access on Novell eDirectory server

Secure Socket Layer (SSL) allows the data, which is transmitted between the Security Access Manager services and the Novell eDirectory server, to be encrypted to provide data privacy and integrity.

Administrators should consider enabling SSL to protect information, such as user passwords and private data. However, SSL is not required for Security Access Manager to operate. If SSL is not required in your Security Access Manager environment, skip this section.

Security Access Manager supports server-side authentication with Novell eDirectory only. To configure the Novell eDirectory server for SSL, ensure that the ConsoleOne tool is installed and complete the following sections.

- “Creating an organizational certificate authority object”
- “Creating a self-signed certificate” on page 97
- “Creating a server certificate for the LDAP server” on page 97
- “Enabling SSL” on page 98

Note: For more information, see Novell product documentation at http://www.novell.com

Creating an organizational certificate authority object

During installation of eDirectory, an **NDSPKI:Certificate Authority** object is created by default (if one does not exist in the network).

About this task

It is important that the subject name (not the object name) be a valid signatory. The subject name must have an **organization** field and a country field to be recognized as valid by Security Access Manager. The default subject name is as follows:

`0=`*`organizational_entry_name`*`.OU=Organizational DVD`

This is not a valid signatory. To change it, you must re-create the Certificate Authority object with a valid subject name. To do so, follow these steps:

Procedure

1. Start ConsoleOne.
2. Select the **Security** container object. Objects are displayed in the right pane of the window.
3. Select the Organization CA object and delete it.
4. Right-click the **Security** container object again and click **New → Object**.
5. From the list box in the New Object dialog, double-click **NDSPKI: certificate authority**. The Create an Organizational Certificate Authority Object dialog is displayed. Follow the online instructions.

6. Select the target server and enter an eDirectory object name. For example:
   Host Server Field = `C22Knt_NDS.AM`
   Object Name Field = `C22KNT-CA`
7. In Creation Method, select **Custom**.
8. Click **Next**. Depending on the installed version of Novell eDirectory, two more screens might display.
9. Click **Next** twice to continue.
10. Accept the default Subject name or enter a valid distinguished name for the certificate authority being defined. All certificates that are generated by the certificate authority are placed in this location.
11. The Organizational certificate authority is displayed in ConsoleOne as `C22KNT-CA`.

Creating a self-signed certificate

To enable SSL, you need a certificate. You can create a self-signed certificate to meet this requirement.

Procedure

1. Go to the properties of the Organizational certificate authority (`C22KNT-CA`). The Properties window is displayed.
2. Select the **Certificate** tab and then select **Self Signed Certificate** from the menu.
3. Validate the certificate.
4. Export the certificate. The Export a Certificate window is displayed.
5. Accept the default values and write down the location where the self-signed certificate is saved. For example:

   ```
   c:\c22knt\CA-SelfSignedCert.der
   ```
6. Transfer (FTP) the file to the Security Access Manager host directory. For example:

   ```
   c:\Program Files\Tivoli\Policy Directory\keytab
   ```

   Note that this is a binary file.

Creating a server certificate for the LDAP server

A server certificate is required to enable SSL.

Procedure

1. To create a server certificate for the LDAP server, right-click the Organization entry.
2. Click **New → Object**. A New Object window is displayed.
3. Select **NDSPKI: Key Material**.
4. Click **OK**. The Create Server Certificate (Key Material) window is displayed.
5. Enter the certificate name. For example, `AM`
6. Select **Custom** for the creation method.
7. Click **Next**.
8. Use the default values for **Specify the certificate authority option**, which signs the certificate.
9. Click **Next**.
10. Specify the key size, and accept default values for all other options.
11. Click **Next**.

Note: The default key size for Novell eDirectory Version 8.6.2 is **1024** bits; **2048** bits for Version 8.7.

12. In the Specify the Certificate Parameters window, click the **Edit** button next to the **Subject Name** field. The Edit Subject window is displayed.
13. Enter the subject name.
14. Click **OK**. The Create Server Certificate (Key Material) window is displayed with the **Subject Name** field updated.
15. Click **Next** to continue.
16. To accept the default values in the following windows, click **Next** twice.
17. Click **Finish** to create a key material. The Creating Certificate window is temporarily displayed. When it clears, the right pane of ConsoleOne is updated with a Key Material entry named `AM`. This entry is the server certificate.

Enabling SSL

Use the following procedure to enable SSL.

Procedure

1. In the right pane of ConsoleOne, locate an entry named **LDAP Server –** *hostname* and right-click it.
2. From the menu, select **Properties**. From the Properties notebook, select the SSL Configuration tab.
3. Click the **Tree Search** icon next to the **SSL Certificate** field. The Select SSL Certificate window is displayed. The SSL Certificate List pane displays the certificates that are known to the organization.
4. Select the `AM` certificate.
5. Click **OK**. The Properties of LDAP Server – *hostname* window is redisplayed with an updated **SSL Certificate** field.
6. Copy the signer certificate and have it available to copy to the Security Access Manager servers that you want to set up SSL communication with.

What to do next

Continue with Chapter 6, “Setting up a policy server,” on page 103.

Installing and configuring the Sun Java System Directory Server

You can use a supported version of Sun Java System Directory Server as the user registry for Security Access Manager.

Before you begin

Review the considerations in the following topics before you configure the Sun Java System Directory Server in your environment:

- “LDAP considerations” on page 52
- “Sun Java System Directory Server considerations” on page 53

About this task

Complete the basic server installation and configuration as described in the Sun Java System Directory Server product documentation. For example, for Sun Java System Directory Server version 7.0, see:

- Installation guide: http://download.oracle.com/docs/cd/E19424-01/820-4807/820-4807.pdf
- Administration guide: http://download.oracle.com/docs/cd/E19424-01/820-4809/820-4809.pdf

Then, use the same documentation to create a suffix for Security Access Manager.

Procedure

1. Create the management domain location that maintains Security Access Manager data.

   Use the suffix DN of the location; for example: `secAuthority=Default`.

   The name must be in the relative distinguished name (DN) format and consist of one attribute-value pair. If multiple attribute-value pairs, separate the pairs by commas. The default location is `secAuthority=Default`.

   For more information about management domains, and creating a location for the metadata, see:

   - "Security Access Manager management domains" on page 104
   - "Management domain location example" on page 105
2. Change the name of the database when creating a suffix.

   Attention: Do not accept the default value for the database name when creating a suffix. By default, the location of database files for this suffix is chosen automatically by the server. By default, the suffix maintains only the system indexes, no attributes are encrypted, and replication is not configured. If you accept the default value, the Sun Java Directory Server stores the suffix under the **Default** database name. Your data is removed when the Sun Java Directory Server is restarted.
3. Ensure that the suffix was created. If you chose to create a suffix to maintain user and group data, follow this procedure again to create another suffix either in the default database or in a new database. For example, you could create a suffix named `o=ibm,c=us` in the same database.
4. Complete the appropriate action:
   - If you did not add any suffixes other than the management domain location, configuration is complete. A directory entry for the management domain location is automatically added when the policy server is configured.
   - If you added suffixes other than the management domain location, create directory entries for each new suffix.
5. If you want to enable SSL communication between the Directory Server and Security Access Manager, continue with the remaining steps:
   a. Start the instance of the Sun Java System Directory Server.
   b. Obtain a certificate for the instance and store it in the key database. The certificate can be issued by a certificate authority (CA) or it can be self-signed. The certificate includes a server certificate and a private key. Use the methods that are described in the Sun Java System Directory Server documentation.
   c. Make a note of the secure SSL port number on the server. The default port number is `636`.
   d. Obtain the signer certificate.

      Note: If the certificate is issued by a CA, the server certificate includes a signer certificate. If the certificate is self-signed, the server certificate acts as the signer certificate.

e. Copy the signer certificate to a temporary directory on the computer where Security Access Manager components are installed and with which you want to enable SSL communication.

What to do next

After you set up the Directory Server for use with Security Access Manager, you can set up the policy server. See Chapter 6, “Setting up a policy server,” on page 103. Use the following values in your configuration:

- Value of LDAP administrator ID for the Sun Directory Server is `cn=Directory Manager`. The default value for this attribute is `cn=root`, however, it is not appropriate for the Sun Directory Server.
- Value of LDAP management domain location DN for the Sun Directory Server is a suffix (for example, `dc=ibm,dc=isam`) created under the directory instance. The default value for this attribute is blank and it is not appropriate for the Sun Directory Server.

Part 3. Base system component installation

Chapter 6. Setting up a policy server

The Security Access Manager policy server maintains the master authorization database for the management domain as well as the policy databases that are associated with other secure domains that you might decide to create.

This server is key to the processing of access control, authentication, and authorization requests. It also updates authorization database replicas and maintains location information about other Security Access Manager servers.

You must install and configure only one policy server for each secure management domain.

To retain flexibility and ensure efficient load balancing, consider setting up the policy server on a system that is separate from your registry server.

Set up this system by following the appropriate instructions for your operating system.

Optional: You can also set up a standby policy server to use in the event of a system failure. This capability requires additional software and hardware. For more information, see:

- Appendix G, "Standby policy server (AIX) setup," on page 357
- Appendix H, "Setup for a standby policy server with IBM Tivoli System Automation for Multiplatforms," on page 373

The policy server requires the installation of the following prerequisite products and Security Access Manager components:

- IBM Global Security Kit (GSKit)
- IBM Tivoli Directory Server client (depending on the registry used)
- Security Access Manager License
- IBM Security Utilities
- Security Access Manager Runtime
- Security Access Manager Policy Server

Note: Security Access Manager does not consider the registry native password policies when it creates server accounts during configuration. The registry native password policies might cause server configuration failure. Before configuration, disable any registry native password policies, such as the registry default or global password policies. After configuration, set exceptions on the registry so that the new server accounts are not affected by any registry native password policies. Then, you can enable the registry native password policies.

LDAP data format selection

During the configuration of the policy server, select which LDAP data format to use for user and group tracking information.

The two LDAP data formats available for user and group information are:

Minimal

Minimal format uses fewer LDAP objects to maintain user and group tracking information. Using this format reduces the size of your user registry information because minimal user and group tracking information is stored.

Standard

Standard format uses more LDAP objects to maintain user and group tracking. This format was also used in versions of IBM Tivoli Access Manager for e-business before version 6.0.

If the user and group information in the LDAP registry is used by other Security Access Manager products, such as IBM Tivoli Access Manager for Operating Systems or IBM Tivoli Federated Identity Manager, the same LDAP data format must be used for all products.

Security Access Manager management domains

If you use LDAP as your user registry, Security Access Manager provides for one or more administrative domains. A domain consists of all the users, groups, and resources that require protection along with the associated security policy used to protect those resources.

Depending on the installed resource managers, resources can be any physical or logical entity, including objects such as files, directories, web pages, printer and network services, and message queues. Any security policy that is implemented in a domain affects only the objects in that domain. Users with authority to complete tasks in one domain do not necessarily have the authority to complete those tasks in other domains.

The initial domain in an LDAP registry is called the *management domain* and is created when the policy server is configured. During policy server configuration, you are prompted for the management domain name and the management domain location Distinguished Name (DN) within the LDAP Directory Information Tree (DIT) on the LDAP server where the information about the domain will be maintained. See Appendix D, “pdconfig options,” on page 317 for instructions on how to set these parameters for the Security Access Manager policy server.

If the management domain location is not specified, the management domain location is assumed to be a stand-alone suffix on the LDAP server. Whether you use the default location or specify a different location in the LDAP DIT, the location that is specified for the management domain must exist unless the user registry is Novell eDirectory. For Novell eDirectory, if you do not specify the management domain location, Security Access Manager uses the root location as the management domain location. The root location is a domain location that does not have a suffix. If you enter a specific location for the management domain, ensure that the location you are specifying exists.

When a Security Access Manager domain is created, including the initial management domain, an entry is created in the LDAP server that is called a secAuthorityInfo object. This object represents the Security Access Manager domain and is named according to the secAuthority attribute with the name of the domain as its value; for example: `secAuthority=<domain_name>`.

If you do not provide a different name, the default name of the management domain is `Default`, making the secAuthorityInfo object name `secAuthority=Default`.

Management domain location example

If you want to specify a nondefault location for the management domain, you can use any location within the LDAP DIT.

For example, if the LDAP server is configured with a suffix of `c=us`, and the administrator specifies the management domain location DN as `ou=austin,o=ibm,c=us`, this object might be created by using a file that contains the following LDIF:

```
dn: c=us
objectClass: top
objectClass: country
c: US

dn: o=ibm,c=us
objectClass: top
objectClass: organization
o: IBM

dn: ou=austin,o=ibm,c=us
objectClass: top
objectClass: organizationalunit
ou: Austin
```

The object might then be created by using the **idsldapadd** command-line utility as follows:

```
idsldapadd –h <ldap_hostname> -p <ldap_port> -D <ldap_admin_DN>
-w <ldap_admin_pwd> -v –f example_DIT
```

where:

- *ldap_hostname* is the host name of the LDAP server.
- *ldap_port* is the port of the LDAP server.
- *ldap_admin_DN* is the Distinguished Name of the LDAP server administrator.
- *ldap_admin_pwd* is the password of the LDAP server administrator.
- *example_DIT* is the name of the file that contains the LDIF.

Modify this example for the specific LDAP namespace appropriate for your organization.

After the LDAP object is created, you can specify it as the management domain location DN during policy server configuration. See Appendix D, “pdconfig options,” on page 317 for instructions on how to set these parameters for the Access Manager policy server.

Note:

If the following conditions exist, a WebSEAL instance cannot change user passwords because of the absence of ACL settings that are required to search domain locations:

- You configured the policy server in a nondefault location, that is a location other than `secAuthority=Default`.
- You create Security Access Manager subdomains under the new location.
- You configured a WebSEAL instance in any of the new subdomains.

If you configure the policy server in a nondefault location and find that these other conditions exist, see the *IBM Security Access Manager for Web Troubleshooting Guide* for information about setting the correct ACL.

Management domain location for an Active Directory Lightweight Directory Service (AD LDS) registry

If Active Directory Lightweight Directory Service (AD LDS) is being used as the LDAP registry, you must choose a location DN within the same directory partition where you want to store user and group information.

AD LDS has a restriction that the policy server must exist in the same directory partition in which user and group information is maintained. The policy server cannot maintain user and group information outside the directory partition in which the policy server itself is defined.

Policy server installation using the command line

Use platform-specific command-line utilities to install the policy server. This method is one of several installation methods you can use.

For more information, see Chapter 2, “Installation methods,” on page 19.

When you use the command-line utilities, you must manually install each component and its prerequisite software in the appropriate order.

Complete the prerequisite installations first. See Part 2, “Prerequisite software installation,” on page 25.

The platform-specific installation utilities that are used are:

AIX **`installp`**

Linux **`rpm`**

Solaris
`pkgadd`

Note: Installations on Solaris systems should use the **-G** option with the **`pkgadd`** utility. The **-G** option adds the package into the current zone only. When the **-G** option is used in the global zone, the package is added to the global zone only and is not propagated to any existing or yet-to-be-created non-global zone. When used in a non-global zone, the package(s) are added to the non-global zone only.

Windows
`setup.exe`

After you complete the installation, use the appropriate configuration commands. For example, if the Security Access Manager Runtime component is installed on your system, you can use the **`pdconfig`** utility to configure Security Access Manager components and, if the Security Access Manager Runtime component is *not* installed, you can use component-specific utilities, such as **`pdjrtecfg`** to configure the IBM Security Access Manager Runtime for Java component or **`amwpmcfg`** to configure the Security Access Manager Web Portal Manager component.

Note: For more information about these utilities, see the *IBM Security Access Manager for Web Command Reference*.

AIX: Installing the policy server

Use **installp** to install software packages and the **pdconfig** utility to configure them on AIX.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

Procedure

1. Log on as **root**.
2. Ensure that your registry server is up and running in normal mode before you install the policy server.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
4. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "AIX: Installing the IBM Global Security Kit (GSKit)" on page 35.
5. Install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "AIX: Installing the IBM Tivoli Directory Server client" on page 42.
6. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
7. Install the IBM Security Utilities, if not already installed. For instructions, see page "AIX: Installing the IBM Security Utilities" on page 39.
8. Install the Security Access Manager packages:

   ```
   installp -acgYXd package_path/usr/sys/inst.images packages
   ```

   where:

   - *package_path* is the directory where the DVD is mounted or the files are located.
   - *packages* are:

     PD.RTE Specifies the Security Access Manager Runtime package.

     PD.Mgr Specifies the Security Access Manager policy server package.

   Attention: You must *not* configure the Security Access Manager Runtime until the policy server is installed.
9. Unmount the DVD, if used.
10. To view status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
11. Configure the Security Access Manager packages as follows:

a. Start the configuration utility: `pdconfig`
   The Security Access Manager Setup Menu is displayed.
b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
c. Select the menu number of the package that you want to configure, one at a time. Configure the Security Access Manager Runtime followed by the Security Access Manager policy server package.
   Depending on the package that you selected, you are prompted for configuration options. For assistance with these configuration options, see Appendix D, “pdconfig options,” on page 317.
   When a message displays that indicates the package was successfully configured, press Enter to configure another package or select the **x** (Exit) option twice to close the configuration utility.

Note: If you configure the Security Access Manager security standard in the `ssl-compliance` option to Suite B, NIST SP800-131, or FIPS, and not the default of "`none`," then during Web Portal Manager configuration, you must also configure WebSphere Application Server to enable the same security standard. If the security standard settings do not match, Web Portal Manager configuration fails. To enable the same security setting in WebSphere Application Server, see http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=%2Fcom.ibm.websphere.nd.multiplatform.doc%2Finfo%2Fae%2Fae%2Fcsec_security_standards.html

Results

This step completes the setup of the Security Access Manager policy server system. To set up another Security Access Manager system, follow the steps in the Chapter 3, “Installation roadmap,” on page 21.

Note that configuration of the Security Access Manager policy server creates a default SSL certificate authority file named `pdcacert.b64`. The SSL key file and certificate are created by using algorithms appropriate for the configured compliance type.

After successful configuration of the Security Access Manager Policy Server component, a message similar to the following is displayed:

```
Security Access Manager Policy Server configuration completed successfully.
The Manager's CA certificate is base64-encoded and saved in text file
/var/PolicyDirector/keytab/pdcacert.b64
You must distribute this file to each machine in your secure domain.
It is needed for successful configuration.
```

For a Security Access Manager runtime system to authenticate to Security Access Manager servers, each runtime system requires a copy of this file. To obtain this file, do one of the following:

- During configuration of the Security Access Manager Runtime package (using the **pdconfig** utility), select to download the `pdcacert.b64` file automatically.
- Manually copy the `pdcacert.b64` file to the Security Access Manager system before you configure the Security Access Manager Runtime component.

Linux: Installing the policy server

Use **rpm** to install software packages and the **pdconfig** utility to configure them on Linux.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

Note to Linux on System z users: You must first obtain access to the Linux `rpm` files which are in the */package_path*`/linux_s390` directory.

Note to all Linux users: If you are installing on a Linux system and SELinux is enabled, you must run the following commands to start the policy and authorization server:

```
chcon -t textrel_shlib_t /usr/local/ibm/gsk8_64/lib64/C/icc/osslib/libcryptoIBM080.so.0.9.8
chcon -t textrel_shlib_t /usr/local/ibm/gsk8_64/lib64/N/icc/osslib/libcryptoIBM081.so.0.9.8
chcon -t textrel_shlib_t /opt/PolicyDirector/lib/libamzcars.so
chcon -t textrel_shlib_t /usr/local/ibm/gsk8_64/lib64/libgsk8krsw.so
chcon -t textrel_shlib_t /opt/PolicyDirector/lib/libamcars.so
```

Procedure

1. Log on as **root**.
2. Ensure that your registry server is up and running (in normal mode) before you install the policy server.
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
4. Change to the *package_path*`/`*distribution* directory where *package_path* is the mount point for your DVD or file location and *distribution* specifies `linux_x86` for x86-64 or `linux_s390` for System z.
5. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Linux: Installing the IBM Global Security Kit (GSKit)" on page 35.
6. Install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Linux: Installing the IBM Tivoli Directory Server client" on page 43.
7. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
8. Install the IBM Security Utilities, if not already installed. For instructions, see page "Linux: Installing IBM Security Utilities" on page 40.
9. Install the Security Access Manager packages.

	Linux on x86-64	Linux on System z
Security Access Manager Runtime package	`PDRTE-PD-7.0.0-0.x86_64.rpm`	`PDRTE-PD-7.0.0-0.s390.rpm`
Security Access Manager Policy Server package	`PDMgr-PD-7.0.0-0.x86_64.rpm`	`PDMgr-PD-7.0.0-0.s390.rpm`

   Attention: You must *not* configure the Security Access Manager Runtime until the policy server is installed.
10. Unmount the DVD, if used.

11. To view status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
12. Configure the Security Access Manager packages as follows:
    a. Start the configuration utility: `pdconfig`
       The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure, one at a time. Configure the Security Access Manager Runtime package followed by the Security Access Manager policy server package.
       Depending on the package that you selected, you are prompted for configuration options. For assistance with these configuration options, see Appendix D, "pdconfig options," on page 317.
       When a message is displayed that indicates the package was successfully configured, press Enter to configure another package or select the **x** (Exit) option twice to close the configuration utility.

    Note: If you configure the Security Access Manager security standard in the `ssl-compliance` option to Suite B, NIST SP800-131, or FIPS, and not the default of "none," then during Web Portal Manager configuration, you must also configure WebSphere Application Server to enable the same security standard. If the security standard settings do not match, Web Portal Manager configuration fails. To enable the same security setting in WebSphere Application Server, see http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=%2Fcom.ibm.websphere.nd.multiplatform.doc%2Finfo%2Fae%2Fae%2Fcsec_security_standards.html

Results

This step completes the setup of the Security Access Manager policy server system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Note that configuration of the Security Access Manager policy server creates a default SSL certificate authority file named `pdcacert.b64`. The SSL key file and certificate are created by using algorithms appropriate for the configured compliance type.

After successful configuration of the Security Access Manager policy server component, a message similar to the following is displayed:

```
Security Access Manager Policy Server configuration completed successfully.
The Manager's CA certificate is base64-encoded and saved in text file
/var/PolicyDirector/keytab/pdcacert.b64
You must distribute this file to each machine in your secure domain.
It is needed for successful configuration.
```

For a Security Access Manager runtime system to authenticate to Security Access Manager servers, each runtime system requires a copy of this file. To obtain this file, do one of the following options:

- During configuration of the Security Access Manager Runtime package with the **pdconfig** utility, select to download the `pdcacert.b64` file automatically.
- Manually copy the `pdcacert.b64` file to the Security Access Manager system before you configure the Security Access Manager Runtime component.

Solaris: Installing the policy server

Use **pkgadd** to install software packages and the **pdconfig** utility to configure them on Solaris.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

About this task

Attention: Installations on Solaris systems should use the **-G** option with the **pkgadd** utility. The **-G** option adds the package into the current zone only.

Procedure

1. Log on as **root**.
2. Ensure that your registry server is up and running (in normal mode) before you install the policy server.
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
4. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Solaris: Installing the IBM Global Security Kit (GSKit)" on page 36.
5. Install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Solaris: Installing the IBM Tivoli Directory Server client" on page 44.
6. Install the IBM Security Access Manager for Web License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
7. Install the IBM Security Utilities, if not already installed. For instructions, see page "Solaris: Installing IBM Security Utilities" on page 40.
8. Install these Security Access Manager packages:

   ```
   pkgadd -d /package_path/solaris
     -a /package_path/solaris/pddefault -G packages
   ```

   where:

   /*package_path*/solaris
   Specifies the location of the package.

   /*package_path*/solaris/pddefault
   Specifies the location of the installation administration script.

   and where the *packages* are as follows:

   PDRTE Specifies the Security Access Manager Runtime package.

   PDMgr Specifies the Security Access Manager policy server package.

   Attention: You must *not* configure the Security Access Manager Runtime until the policy server is installed.

When the installation process is complete for each package, the following message is displayed:

```
Installation of package successful.
```

9. To view status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
10. Configure the Security Access Manager packages as follows:
    a. Start the configuration utility:

       ```
       pdconfig
       ```

       The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure, one at a time. Configure the Security Access Manager Runtime, followed by the Security Access Manager Policy Server package.

       Depending on the package that you selected, you are prompted for configuration options. For assistance with these configuration options, see Appendix D, "pdconfig options," on page 317.

       When a message is displayed that indicates the package was successfully configured, press Enter to configure another package or select the **x** option twice to close the configuration utility.

Note: If you configure the Security Access Manager security standard in the `ssl-compliance` option to Suite B, NIST SP800-131, or FIPS, and not the default of "`none`," then during Web Portal Manager configuration, you must also configure WebSphere Application Server to enable the same security standard. If the security standard settings do not match, Web Portal Manager configuration fails. To enable the same security setting in WebSphere Application Server, see http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=%2Fcom.ibm.websphere.nd.multiplatform.doc%2Finfo%2Fae%2Fae%2Fcsec_security_standards.html

Results

This step completes the setup of the Security Access Manager policy server system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Note that configuration of the Security Access Manager policy server creates a default SSL certificate authority file named `pdcacert.b64`. The SSL key file and certificate are created by using algorithms appropriate for the configured compliance type.

After successful configuration of the Security Access Manager Policy Server component, a message similar to the following is displayed:

```
Security Access Manager Policy Server configuration completed successfully.
The Manager's CA certificate is base64-encoded and saved in text file
/var/PolicyDirector/keytab/pdcacert.b64
You must distribute this file to each machine in your secure domain.
It is needed for successful configuration.
```

For a Security Access Manager runtime system to authenticate to Security Access Manager servers, each runtime system requires a copy of this file. To obtain this file, do one of the following options:

- During configuration of the Security Access Manager Runtime package with the **pdconfig** utility, select to download the `pdcacert.b64` file automatically.
- Manually copy the `pdcacert.b64` file to the Security Access Manager system before you configure the Security Access Manager Runtime component.

Windows: Installing the policy server

Use the **setup.exe** program to install software packages and the **pdconfig** utility to configure them on Windows.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

Procedure

1. Log on as a user with Administrator group privileges.
2. Ensure that your registry server is up and running (in normal mode) before you install the policy server.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
3. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Windows: Installing the IBM Global Security Kit (GSKit)" on page 36.
4. If using an LDAP-based user registry, install the IBM Tivoli Directory Server client, if it is not already installed. For instructions, see page "Windows: Installing the IBM Tivoli Directory Server client" on page 45.
5. Install the Security Access Manager license, if not already installed. For instructions, see "Windows: Installing the IBM Security Access Manager License" on page 39.
6. Install the IBM Security Utilities, if not already installed. For instructions, see page "Windows: Installing IBM Security Utilities" on page 41.
7. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
8. Install the Security Access Manager packages. To do so, run the **setup.exe** program in this directory:

   `\windows\PolicyDirector\Disk Images\Disk1`

   Follow the online instructions and select to install the following packages:

   - Security Access Manager Runtime
   - Security Access Manager Policy Server

   Attention: You must *not* configure the Security Access Manager Runtime until the policy server is installed.
9. To view status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
10. Configure the Security Access Manager packages as follows:

a. Start the configuration utility:

   ```
   pdconfig
   ```

   The Security Access Manager Configuration window is displayed.

b. Select the **Security Access Manager Runtime** package and click **Configure**.

c. Select the **Security Access Manager Policy Server** package and click **Configure**.

Depending on the package that you selected, you are prompted for configuration options. For assistance with these configuration options, see Appendix D, “pdconfig options,” on page 317.

Note: If you configure the Security Access Manager security standard in the `ssl-compliance` option to Suite B, NIST SP800-131, or FIPS, and not the default of "`none`," then during Web Portal Manager configuration, you must also configure WebSphere Application Server to enable the same security standard. If the security standard settings do not match, Web Portal Manager configuration fails. To enable the same security setting in WebSphere Application Server, see http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=%2Fcom.ibm.websphere.nd.multiplatform.doc%2Finfo%2Fae%2Fae%2Fcsec_security_standards.html

Results

This step completes the setup of the Security Access Manager policy server system. To set up another Security Access Manager system, follow the steps in the Chapter 3, “Installation roadmap,” on page 21.

Note that configuration of the Security Access Manager policy server creates a default SSL certificate authority file named `pdcacert.b64`. The SSL key file and certificate are created by using algorithms appropriate for the configured compliance type.

After successful configuration of the Security Access Manager Policy Server component, a message similar to the following is displayed:

```
Security Access Manager Policy Server configuration completed successfully.
The Manager's CA certificate is base64-encoded and saved in text file
C:\PROGRA~1\Tivoli\POLICY~1\keytab\pdcacert.b64
You must distribute this file to each machine in your secure domain.
It is needed for successful configuration.
```

For a Security Access Manager runtime system to authenticate to Security Access Manager servers, each runtime system requires a copy of this file. To obtain this file, do one of the following options:

- During configuration of the Security Access Manager Runtime package with the **`pdconfig`** utility, select to download the `pdcacert.b64` file automatically.
- Manually copy the `pdcacert.b64` file to the Security Access Manager system before you configure the Security Access Manager Runtime component.

Installing a policy server using the Launchpad (Windows)

Use the Launchpad installation method to install and configure the policy server and its prerequisite software on Windows using a graphical user interface.

Before you begin

Ensure that you completed the following prerequisite tasks:

- "Operating system preparation" on page 28
- Chapter 5, "User registry server installation and configuration," on page 51.

About this task

The Launchpad provides a graphical user interface for step-by-step installation and initial configuration.

This task installs the following components:

- IBM Global Security Kit (GSKit)
- IBM Tivoli Directory Server client
- IBM Security Utilities
- Security Access Manager License
- Security Access Manager Runtime
- Security Access Manager Policy Server

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the Launchpad image files are in a directory path that does not contain any spaces.
2. Start the Launchpad.
   a. Locate the `launchpad64.exe` file.
   b. Double-click the file to start the Launchpad.
3. Select the language that you want to use during the installation and click **OK**. The Launchpad Welcome window opens.
4. Click **Next**.
5. Select the **Policy Server** component.
6. Click **Next**. A list displays the component that you selected and any prerequisite software that is required by that component but that is not already installed.
7. Click **Next**. An arrow next to a component name indicates that component is being installed. A check mark next to a component name indicates that component is installed.
8. If the current component is IBM Global Security Kit, click **Install IBM Global Security Kit** to install it. When it completes, continue with step 9.
9. Click **Next**.
10. Respond to the prompts presented during the installation.
11. Click **Next** at the bottom of the Launchpad to continue.
12. Complete the installation.
    - If the installation fails, correct the error that is described in the error message and restart the Launchpad.
    - If the installation is successful, continue with step 13.
13. Click **Next** to start the configuration.

Note: The configuration tool is displayed in the language that is selected for your operating system locale. If the tool is displayed in English and is not displayed in the operating system locale, review the language pack installation log at `%USERPROFILE%\ISAMLangPacksInstall.log`. Correct any errors that are reported in the log file. Then, install the language pack as described in Appendix E, "Language support installation," on page 339.

14. Click **Configure Security Access Manager**. The configuration tool opens.
15. Select the component.
16. Click **Configure**.
17. Complete the configuration. For help completing the prompts, see Appendix D, "pdconfig options," on page 317.

    Note: If you configure the Security Access Manager security standard in the `ssl-compliance` option to Suite B, NIST SP800-131, or FIPS, and not the default of "`none`," then during Web Portal Manager configuration, you must also configure WebSphere Application Server to enable the same security standard. If the security standard settings do not match, Web Portal Manager configuration fails. To enable the same security setting in WebSphere Application Server, see http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=%2Fcom.ibm.websphere.nd.multiplatform.doc%2Finfo%2Fae%2Fae%2Fcsec_security_standards.html
    When all installations and configurations are completed, a success or failure message is displayed.
18. Take one of the following actions:
    - If the configuration completed successfully, click **Next**.
    - If the configuration failed or an error is displayed, review the log file in the default `%USERPROFILE%` location, such as `C:\Users\Administrator\LaunchPDConfigforISAM.log`.

      Make corrections as indicated by the log file. Then, configure the component by using the **`pdconfig`** utility at a command line or by clicking **Start** > **Programs** > **IBM Security Access Manager for Web** > **Configuration**.
19. Click **Finish** to close the Launchpad.

Policy server installation using script files

The installation and configuration scripts can automate installations and complete unattended (*silent*) installations and configurations.

Use the scripts in their original state or modify them to suit the requirements of your environment.

The scripts install the following prerequisite software and Security Access Manager components, if they are not already installed:

- IBM Global Security Kit (GSKit)
- IBM Tivoli Directory Server client
- Security Access Manager License
- IBM Security Utilities
- Security Access Manager Runtime
- Security Access Manager Policy Server

Automating the installation of a policy server (AIX, Linux, or Solaris)

Use the script file to automate the installation of a policy server.

About this task

Automated installations can complete unattended (*silent*) installations.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the `install_isam.sh` script file in the `scripts` directory.
3. Run the script as follows:

   ```
   ./install_isam.sh -i PolicyServer -d path_to_packages -a [accept|display]
   ```

   where

   - *path_to_packages* is the location of the component installation packages.

     For example, if you are installing from a DVD:

     AIX
     dvd_mount_point`/usr/sys/inst.images`

     Linux x86-64
     `/mnt/dvd/linux_x86`

     Linux on System z
     `/linux_s390`

     Solaris
     `/dvd/`*dvd0*`/solaris`

   - `-a [accept|display]`

     The `-a accept` option automatically accepts the license without displaying the license. The `-a display` option displays the license and you must manually accept the license.

   For example, if you are installing on Linux x86-64:

   ```
   ./install_isam.sh -i PolicyServer -d /mnt/dvd/linux_x86 -a accept
   ```

   The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.
4. Optional: To list the required packages without installing, use the `-l` option.

   ```
   ./install_isam.sh -l PolicyServer
   ```

What to do next

When the installation is completed, continue with "Automating the configuration of a policy server" on page 119.

Automating the installation of a policy server (Windows)

Use the script file to automate the installation of a policy server on Windows.

Before you begin

The installation script uses the following default destination directories:

IBM Security Access Manager
C:\Program Files\Tivoli\Policy Director

Tivoli Directory Server client
C:\Program Files\IBM\ldap\V6.3

IBM Security Utilities
C:\Program Files\Tivoli\TivSecUtl

If you want to change these directories, you must do so before you run the script:

1. Copy *all* of the `.iss` files from the DVD or extracted archive files to a temporary directory on your computer. The files that you can modify are:

   IBM Security Access Manager
   `ISAMLicense.iss`

   IBM Tivoli Directory Server client
   `LDAPClient.iss`

   IBM Security Utilities
   `IBMSecurityUtils.iss`
2. Use a text editor to change the destination path in one or all three files.
3. Save the files.
4. Copy the script command file, `install_isam.bat`, from the DVD or extracted archive file into the same directory on your computer.
5. Run the script command as described in the following task.

About this task

Automated installations can complete unattended (*silent*) installations.

Attention: The installation script requires administrator privileges. Run the script file command, `install_isam.bat`, after you log in using an administrator ID or from a command window that you open with **Run as administrator**.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the `install_isam.bat` script file in the `scripts` directory. This directory is on the product DVD or in the directory where you extracted the product files. Ensure that the `.bat` file and all the `.iss` files are in the same directory.
3. Run the script as follows:
   ```
   install_isam.bat /i PolicyServer /d path_to_packages
   ```

   where:

   path_to_packages is the path to the product DVD or the directory where you extracted the product files. For example, to install the policy server, type:
   ```
   install_isam.bat /i PolicyServer /d c:\isam_images
   ```

   where `c:\isam_images` is the directory where the extracted subdirectories and product files are located. The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.
4. Optional: To list the required packages without installing, use the -l option.
   ```
   install_isam.bat /l PolicyServer
   ```

What to do next

When the installation is completed, continue with "Automating the configuration of a policy server."

Automating the configuration of a policy server

Use the script file to automate the configuration of a policy server.

Before you begin

- Complete the installation of the policy server. See:
  - "Automating the installation of a policy server (AIX, Linux, or Solaris)" on page 117
  - "Automating the installation of a policy server (Windows)" on page 117
- To view status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.

If you are running this script on Windows, open a new command window. Do not perform this task in the same window where you ran the installation script.

About this task

Automated configuration performs unattended (*silent*) configuration.

The script files and template files that are used in this task are installed in the following locations by default:

AIX, Linux, and Solaris: `/opt/PolicyDirector/example/config`

Windows: `C:\Program Files\Tivoli\Policy Director\example\config`

Procedure

1. Create an options file for the component you want to configure.
   a. Locate the options file template for the component.

      AIX, Linux, or Solaris
      `configure_policysvr.options.template`

      Windows
      `configure_policysvr.options.template.cmd`

   b. Copy the file to a temporary directory. You can copy the file to the temporary directory with a name that is unique to your environment.

      Attention: You must keep the `.cmd` extension for Windows template files. The Windows template files run as commands.

   c. Modify the content of the file to specify settings for your environment. The comments in the file explain the settings and provide examples.

      Note: If you configure the Security Access Manager security standard in the `ssl-compliance` option to Suite B, NIST SP800-131, or FIPS, and not the default of "`none`," then during Web Portal Manager configuration, you must also configure WebSphere Application Server to enable the same security standard. If the security standard settings do not match, Web Portal Manager configuration fails. To enable the same security setting in

WebSphere Application Server, see http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=%2Fcom.ibm.websphere.nd.multiplatform.doc%2Finfo%2Fae%2Fae%2Fcsec_security_standards.html.

d. Save the file.

2. Optional: By default, passwords you specified in the options files are stored in clear text. To obfuscate these passwords:
   a. On Windows, copy the `configure_isam.conf` file to the same directory where you copied the options files.
   b. See Appendix F, "Password management," on page 351 for instructions on using the `-obfuscate` option with the `pdconf` tool to obfuscate the passwords in the options files. For more information about `pdconf`, see the *IBM Security Access Manager for Web Command Reference*.
   c. Return to these instructions to run the configuration script.
3. Run the configuration script and use the options file for input.

   AIX, Linux, or Solaris

   ```
   ./configure_isam.sh -f options_file
   ```

   Windows

   ```
   configure_isam.cmd -f options_file.cmd
   ```

   where *options_file* and *options_file*`.cmd` are the text files that contain the configuration options.

   For example:

   AIX, Linux, or Solaris

   ```
   ./configure_isam.sh -f my_configure_policysvr.options
   ```

   Windows

   Windows, type:

   ```
   configure_isam.cmd -f my_configure_policysvr.options.cmd
   ```

Chapter 7. Authorization server setup

The Security Access Manager Authorization Server provides access to the authorization service for third-party applications that use the Security Access Manager authorization API in remote cache mode. The authorization server also acts as a logging and auditing collection server to store records of server activity.

Set up this system by following the appropriate instructions for your operating system.

Note:

1. Security Access Manager does not consider the registry native password policies when it creates server accounts during configuration. The registry native password policies might cause server configuration failure. Before configuration, disable any registry native password policies, such as the registry default or global password policies. After configuration, set exceptions on the registry so that the new server accounts are not affected by any registry native password policies. Then, you can enable the registry native password policies.
2. Under both of the following conditions, you must set `[ldap] auth-using-compare` to `no` in `ivacld.conf` after authorization server installation:
   - You are installing an authorization server on an upgraded version of Security Access Manager.
   - You are using the Tivoli Directory Server registry to install the authorization server.

   The upgrade process does not automatically update the Security Access Manager ACLEntry in Tivoli Directory Server to permit the authorization server to use this method of authentication.

   Alternatively, you can verify whether the ACLEntry is updated on each LDAP suffix under which Security Access Manager accounts are stored. The updated ACLEntry is:

   ```
   ACLEntry=group:CN=IVACLD-SERVERS,CN=SECURITYGROUPS
   ,SECAUTHORITY=DEFAULT:normal:rsc
   :system:rsc:at.userPassword:wc:at.secAcctValid:rwsc:at.secPwdFailCountTime
   :rwsc:at.secPwdFailures:rwsc:at.secPwdLastChanged
   :rwsc:at.secPwdLastFailed:rwsc:at.secPwdLastUsed:rwsc:at
   .secPwdUnlockTime:rwsc:at.secPwdValid:rwsc
   ```

   Note the addition of `at.userPassword:wc:` to the access list.
3. You can configure multiple authorization servers on a single machine.

Authorization server installation using the command line

Use platform-specific command-line utilities to install an authorization server system. This method is one of several installation methods you can use.

For more information, see Chapter 2, “Installation methods,” on page 19.

When you use the command-line utilities, you must manually install each component and its prerequisite software in the appropriate order.

Complete the prerequisite installations first. See Part 2, “Prerequisite software installation,” on page 25.

The platform-specific installation utilities that are used are:

AIX **installp**

Linux **rpm**

Solaris
pkgadd

Note: Installations on Solaris systems should use the **-G** option with the **pkgadd** utility. The **-G** option adds the package into the current zone only. When the **-G** option is used in the global zone, the package is added to the global zone only and is not propagated to any existing or yet-to-be-created non-global zone. When used in a non-global zone, the package(s) are added to the non-global zone only.

Windows
setup.exe

After you complete the installation, use the appropriate configuration commands. For example, if the Security Access Manager Runtime component is installed on your system, you can use the **pdconfig** utility to configure Security Access Manager components and, if the Security Access Manager Runtime component is *not* installed, you can use component-specific utilities, such as **pdjrtecfg** to configure the IBM Security Access Manager Runtime for Java component or **amwpmcfg** to configure the Security Access Manager Web Portal Manager component.

Note: For more information about these utilities, see the *IBM Security Access Manager for Web Command Reference*.

AIX: Installing an authorization server

Use **installp** to install software packages and the **pdconfig** utility to configure them on AIX.

Before you begin

Complete the appropriate preinstallation tasks in Chapter 4, "Prerequisite installation and configuration roadmap," on page 27.

Procedure

1. Log on as **root**.
2. Ensure that the registry server and policy server are up and running (in normal mode).
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
4. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "AIX: Installing the IBM Global Security Kit (GSKit)" on page 35.
5. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "AIX: Installing the IBM Tivoli Directory Server client" on page 42.

6. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
7. Install the IBM Security Utilities, if not already installed. For instructions, see page "AIX: Installing the IBM Security Utilities" on page 39.
8. Install the Security Access Manager packages.

   `installp -acgYXd package_path/usr/sys/inst.images packages`

   where *package_path* is the directory where the DVD is mounted or the files are located and the *packages* are:

   PD.RTE Specifies the Security Access Manager Runtime package.

   PD.Acld
   Specifies the Security Access Manager Authorization Server package.
9. Unmount the DVD, if used.
10. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
11. Configure the Security Access Manager Runtime and Policy Server packages followed by the Security Access Manager Authorization Server package as follows:
    a. Start the configuration utility:`pdconfig` The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure, one at a time.
    Depending on the package that you selected, you are prompted for configuration options. For assistance with these configuration options, see Appendix D, "pdconfig options," on page 317.

Results

When a message is displayed that indicates the package was successfully configured, press Enter to configure another package or select the **x** option twice to close the configuration utility.

This step completes the setup of a Security Access Manager authorization server system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Linux: Installing an authorization server

Use **rpm** to install software packages and the **pdconfig** utility to configure them on Linux.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

About this task

Note to Linux on System z users: You must first obtain access to the Linux `rpm` files which are in the */package_path*`/linux_s390` directory.

Note to all other Linux users:

- If you are installing on a Linux system and SELinux is enabled, and you must run the following commands to start the policy and authorization servers:

```
chcon -t textrel_shlib_t /usr/local/ibm/gsk8_64/lib64/C/icc/osslib/libcryptoIBM080.so.0.9.8
chcon -t textrel_shlib_t /usr/local/ibm/gsk8_64/lib64/N/icc/osslib/libcryptoIBM081.so.0.9.8
chcon -t textrel_shlib_t /opt/PolicyDirector/lib/libamzcars.so
chcon -t textrel_shlib_t /usr/local/ibm/gsk8_64/lib64/libgsk8krsw.so
chcon -t textrel_shlib_t /opt/PolicyDirector/lib/libamcars.so
```

Procedure

1. Log on as **root**.
2. Ensure that the registry server and policy server are up and running (in normal mode).
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
4. Change to the `package_path/`*`distribution`* directory where `package_path` is the mount point for your DVD or file location and *`distribution`* specifies `linux_x86` for x86-64 or `linux_s390` for System z.
5. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Linux: Installing the IBM Global Security Kit (GSKit)" on page 35.
6. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Linux: Installing the IBM Tivoli Directory Server client" on page 43.
7. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
8. Install the IBM Security Utilities, if not already installed. For instructions, see page "Linux: Installing IBM Security Utilities" on page 40.
9. Install the packages:

   `rpm -ihv` *`packages`*

   where *`packages`* are as follows:

	Linux on x86-64	Linux on System z
Security Access Manager Runtime package	`PDRTE-PD-7.0.0-0.x86_64.rpm`	`PDRTE-PD-7.0.0-0.ppc.rpm`
Security Access Manager Authorization Server package	`PDAcld-PD-7.0.0-0.x86_64.rpm`	`PDAcld-PD-7.0.0-0.ppc.rpm`

10. Unmount the DVD, if used.
11. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.

12. Configure the Security Access Manager Runtime and Policy Server packages followed by the Security Access Manager Authorization Server package as follows:
    a. Start the configuration utility: `pdconfig` The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure, one at a time.
    Depending on the package that you selected, you are prompted for configuration options. For assistance with these configuration options, see Appendix D, "pdconfig options," on page 317.

Results

When a message is displayed that indicates the package was successfully configured, press Enter to configure another package or select the **x** option twice to close the configuration utility.

This step completes the setup of a Security Access Manager authorization server system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Solaris: Installing an authorization server

Use **pkgadd** to install software packages and the **pdconfig** utility to configure them on Solaris.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

About this task

Attention: Installations on Solaris systems should use the **-G** option with the **pkgadd** utility. The **-G** option adds the package into the current zone only.

Procedure

1. Log on as **root**.
2. Ensure that the registry server and policy server are up and running (in normal mode).
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
4. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Solaris: Installing the IBM Global Security Kit (GSKit)" on page 36.
5. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Solaris: Installing the IBM Tivoli Directory Server client" on page 44.

6. Install the IBM Security Access Manager for Web License, if not already installed. For instructions, see “AIX, Linux, Solaris: Installing the IBM Security Access Manager License” on page 37.
7. Install the IBM Security Utilities, if not already installed. For instructions, see page “Solaris: Installing IBM Security Utilities” on page 40.
8. Install the Security Access Manager packages, one at a time:

   ```
   pkgadd -d /package_path/solaris
      -a /package_path/solaris/pddefault -G packages
   ```

   where:

   /package_path/solaris
   Specifies the location of the package.

   /package_path/solaris/pddefault
   Specifies the location of the installation administration script.

   and where *packages* are:

   PDRTE Specifies the Security Access Manager Runtime package.

   PDAcld Specifies the Security Access Manager Authorization Server package.

   When the installation process is complete for each package, the following message is displayed:

   ```
   Installation of package successful.
   ```
9. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see “Installing language support packages for Security Access Manager” on page 340.
10. Configure the Security Access Manager Runtime and Policy Server packages followed by the Security Access Manager Authorization Server package as follows:
    a. Start the configuration utility:

       ```
       pdconfig
       ```

       The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure, one at a time.

       Depending on the package that you selected, you are prompted for configuration options. For assistance with these configuration options, see Appendix D, “pdconfig options,” on page 317.

Results

When a message is displayed that indicates the package was successfully configured, press Enter to configure another package or select the **x** option twice to close the configuration utility.

This step completes the setup of the Security Access Manager policy server system. To set up another Security Access Manager system, follow the steps in the Chapter 3, “Installation roadmap,” on page 21.

Windows: Installing an authorization server

Use the **setup.exe** program to install software packages and the **pdconfig** utility to configure them on Windows.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

Procedure

1. Log on as a user with Administrator group privileges.
2. Ensure that the registry server and policy server are up and running (in normal mode).
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
4. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Windows: Installing the IBM Global Security Kit (GSKit)" on page 36.
5. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if it is not already installed. For instructions, see page "Windows: Installing the IBM Tivoli Directory Server client" on page 45.
6. Install the Security Access Manager license, if not already installed. For instructions, see "Windows: Installing the IBM Security Access Manager License" on page 39.
7. Install the IBM Security Utilities, if not already installed. For instructions, see page "Windows: Installing IBM Security Utilities" on page 41.
8. Install the Security Access Manager packages. To do so, run the **setup.exe** program in the following directory:

   ```
   \windows\PolicyDirector\Disk Images\Disk1
   ```

   Follow the online instructions and select to install the following packages:

   - Security Access Manager Runtime
   - Security Access Manager Authorization Server
9. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
10. Configure the Security Access Manager Runtime and Policy Server packages followed by the Security Access Manager Authorization Server package as follows:
    a. Start the configuration utility:

       ```
       pdconfig
       ```

       The Security Access Manager Configuration window is displayed.
    b. Select the **Security Access Manager Runtime** package and click **Configure**.
    c. Select the **Security Access Manager Authorization Server** package and click **Configure**.

Depending on the package that you selected, you are prompted for configuration options. For assistance with these configuration options, see Appendix D, “pdconfig options,” on page 317.

Results

This step completes the setup of a Security Access Manager authorization server system. To set up another Security Access Manager system, follow the steps in the Chapter 3, “Installation roadmap,” on page 21.

Installing an authorization server using the Launchpad (Windows)

Use the Launchpad installation method to install and configure the authorization server and its prerequisite software on Windows using a graphical user interface.

Before you begin

Ensure that you complete the following prerequisite tasks:

- “Operating system preparation” on page 28
- Chapter 5, “User registry server installation and configuration,” on page 51.

About this task

The Launchpad uses a graphical user interface to complete step-by-step installation and initial configuration.

This task installs the following components:

- IBM Global Security Kit (GSKit)
- IBM Tivoli Directory Server client
- IBM Security Utilities
- Security Access Manager License
- Security Access Manager Runtime
- Security Access Manager Authorization Server

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the Launchpad image files are in a directory path that does not contain any spaces.
2. Start the Launchpad.
   a. Locate the `launchpad64.exe` file.
   b. Double-click the file to start the Launchpad.
3. Select the language that you want to use during the installation and click **OK**. The Launchpad Welcome window opens.
4. Click **Next**.
5. Select the **Authorization Server** component.
6. Click **Next**. A list displays the component that you selected and any prerequisite software that is required by that component but that is not already installed.

7. Click **Next**. An arrow next to a component name on the left indicates that component is being installed. A check mark next to a component name indicates that component is installed.
8. If the current component is IBM Global Security Kit, click **Install IBM Global Security Kit** to install it. When it completes, continue with step 9.
9. Click **Next**.
10. Respond to the prompts presented during the installation.
11. Click **Next** at the bottom of the Launchpad to continue.
12. Complete the installation.
    - If the installation fails, correct the error that is described in the error message and restart the Launchpad.
    - If the installation is successful, continue with step 13.
13. Click **Next** to start the configuration.

    Note: The configuration tool is displayed in the language that is selected for your operating system locale. If the tool is displayed in English and is not displayed in the operating system locale, review the language pack installation log at `%USERPROFILE%\ISAMLangPacksInstall.log`. Correct any errors that are reported in the log file. Then, install the language pack as described in Appendix E, "Language support installation," on page 339.
14. Click **Configure Security Access Manager**. The configuration tool opens.
15. Select the component.
16. Click **Configure**.
17. Complete the configuration. For help completing the prompts, see Appendix D, "pdconfig options," on page 317. When all installations and configurations are completed, a success or failure message is displayed.
18. Take one of the following actions:
    - If the configuration completed successfully, click **Next**.
    - If the configuration failed or an error is displayed, review the log file in the default `%USERPROFILE%` location, such as `C:\Users\Administrator\LaunchPDConfigforISAM.log`.

      Make corrections as indicated by the log file. Then, configure the component with the **`pdconfig`** utility at a command line or by clicking **Start** > **Programs** > **IBM Security Access Manager for Web** > **Configuration**.
19. Click **Finish** to close the Launchpad.

Authorization server installation using script files

The installation and configuration scripts can automate installations and perform unattended (*silent*) installations and configurations.

Use the scripts in their original state or modify them to suit the requirements of your environment.

Automating the installation of an authorization server (AIX, Linux, or Solaris)

Use the script file to automate the installation of an authorization server.

About this task

Automated installations can perform unattended (*silent*) installations.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the `install_isam.sh` script file in the `scripts` directory.
3. Run the script as follows:

   ```
   ./install_isam.sh -i AuthServer -d path_to_packages -a [accept|display]
   ```

   where

   - *path_to_packages* is the location of the component installation packages.

     For example, if you are installing from a DVD:

     AIX *dvd_mount_point*`/usr/sys/inst.images`

     Linux x86-64
     `/mnt/dvd/linux_x86`

     Linux on System z
     `/linux_s390`

     Solaris
     `/dvd/`*dvd0*`/solaris`
   - `-a [accept|display]`

     The `-a accept` option automatically accepts the license without displaying the license. The `-a display` option displays the license and you must manually accept the license.

   For example, if you are installing on Linux x86-64:

   ```
   ./install_isam.sh -i AuthServer -d /mnt/dvd/linux_x86 -a accept
   ```

   The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.
4. Optional: To list the required packages without installing, use the `-l` option.

   ```
   ./install_isam.sh -l AuthServer
   ```

What to do next

When the installation is completed, continue with "Automating the configuration of an authorization server" on page 131.

Automating the installation of an authorization server (Windows)

Use the script file to automate the installation of an authorization server on Windows.

Before you begin

The installation script uses the following default destination directories:

IBM Security Access Manager
`C:\Program Files\Tivoli\Policy Director`

Tivoli Directory Server client
`C:\Program Files\IBM\ldap\V6.3`

IBM Security Utilities
`C:\Program Files\Tivoli\TivSecUtl`

If you want to change these directories, you must do so before you run the script:

1. Copy *all* of the `.iss` files from the DVD or extracted archive files to a temporary directory on your computer. The files that you can modify are:

   IBM Security Access Manager
   `ISAMLicense.iss`

   IBM Tivoli Directory Server client
   `LDAPClient.iss`

   IBM Security Utilities
   `IBMSecurityUtils.iss`
2. Use a text editor to change the destination path in one or all three files.
3. Save the files.
4. Copy the script command file, `install_isam.bat`, from the DVD or extracted archive file into the same directory on your computer.
5. Run the script command as described in the following task.

About this task

Automated installations can perform unattended (*silent*) installations.

Attention: The installation script requires administrator privileges. Run the script file command, `install_isam.bat`, after you log in using an administrator ID or from a command window that you open with **Run as administrator**.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the `install_isam.bat` script file in the `scripts` directory. This directory is on the product DVD or in the directory where you extracted the product files. Ensure that the `.bat` file and all the `.iss` files are in the same directory.
3. Run the script as follows:

   ```
   install_isam.bat /i AuthServer /d path_to_packages
   ```

   where *`path_to_packages`* is the path to the product DVD or the directory where you extracted the product files. For example, to install the authorization server, type:

   ```
   install_isam.bat /i AuthServer /d c:\isam_images
   ```

   where `c:\isam_images` is the directory where the extracted subdirectories and product files are located. The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.
4. Optional: To list the required packages without installing, use the /l option.

   ```
   install_isam.bat /l AuthServer
   ```

What to do next

When the installation is completed, continue with "Automating the configuration of an authorization server."

Automating the configuration of an authorization server

Use the script file to automate the configuration of an authorization server.

Before you begin

- Complete the installation of the authorization server. See:
  - "Automating the installation of an authorization server (AIX, Linux, or Solaris)" on page 129
  - "Automating the installation of an authorization server (Windows)" on page 130
- To view status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.

If you are running this script on Windows, open a new command window. Do not perform this task in the same window where you ran the installation script.

About this task

Automated configuration performs unattended (*silent*) configuration.

The script files and template files that are used in this task are installed in the following locations by default:

AIX, Linux, and Solaris: `/opt/PolicyDirector/example/config`

Windows: `C:\Program Files\Tivoli\Policy Director\example\config`

Procedure

1. Create an options file for the component you want to configure.
   a. Locate the options file template for the component. For the authorization server:

      AIX, Linux, or Solaris
      `configure_authzsvr.options.template`

      Windows
      `configure_authzsvr.options.template.cmd`

   b. Copy the file to a temporary directory.
   c. Save the file with a name that is unique to your environment.

      Attention: You must keep the `.cmd` extension for Windows template files. The Windows template files run as commands.

   d. Modify the content of the file to specify settings for your environment. The comments in the file explain the settings and provide examples.
   e. Save the file.
2. Optional: By default, passwords you specified in the options files are stored in clear text. To obfuscate these passwords:
   a. On Windows, copy the `configure_isam.conf` file to the same directory where you copied the options files.
   b. See Appendix F, "Password management," on page 351 for instructions on using the `-obfuscate` option with the `pdconf` tool to obfuscate the passwords in the options files. For more information about `pdconf`, see the *IBM Security Access Manager for Web: Command Reference*.
   c. Return to these instructions to run the configuration script.
3. Run the configuration script and use the options file for input.

AIX, Linux, or Solaris

```
./configure_isam.sh -f options_file
```

Windows

```
configure_isam.cmd -f options_file.cmd
```

where *options_file* and *options_file*.cmd are the text files that contain the configuration options.

For example:

AIX, Linux, or Solaris

```
./configure_isam.sh -f my_configure_authzsvr.options
```

Windows

```
configure_isam.cmd -f my_configure_authzsvr.options.cmd
```

Chapter 8. Setting up a development system

The Security Access Manager Application Development Kit provides a development environment that you can use to code third-party applications to query the authorization server for authorization decisions.

Set up this system by following the appropriate instructions for your operating system.

Setting up a development system using the command line

Use platform-specific command-line utilities to install a development system. This method is one of several installation methods you can use.

For more information, see Chapter 2, "Installation methods," on page 19.

When you use the command-line utilities, you must manually install each component and its prerequisite software in the appropriate order.

Complete the prerequisite installations first. See Part 2, "Prerequisite software installation," on page 25.

The platform-specific installation utilities that are used are:

AIX **`installp`**

Linux **`rpm`**

Solaris
`pkgadd`

Note: Installations on Solaris systems should use the **-G** option with the **`pkgadd`** utility. The **-G** option adds the package into the current zone only. When the **-G** option is used in the global zone, the package is added to the global zone only and is not propagated to any existing or yet-to-be-created non-global zone. When used in a non-global zone, the package(s) are added to the non-global zone only.

Windows
`setup.exe`

After you complete the installation, use the appropriate configuration commands. For example, if the Security Access Manager Runtime component is installed on your system, you can use the **`pdconfig`** utility to configure Security Access Manager components and, if the Security Access Manager Runtime component is *not* installed, you can use component-specific utilities, such as **`pdjrtecfg`** to configure the IBM Security Access Manager Runtime for Java component or **`amwpmcfg`** to configure the Security Access Manager Web Portal Manager component.

Note: For more information about these utilities, see the *IBM Security Access Manager for Web Command Reference*.

AIX: Installing a development (ADK) system

Use **installp** to install software packages and the **pdconfig** utility to configure them on AIX.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

Procedure

1. Log on as **root**.
2. Ensure that the registry server and policy server are up and running (in normal mode).
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
4. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "AIX: Installing the IBM Global Security Kit (GSKit)" on page 35.
5. Install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "AIX: Installing the IBM Tivoli Directory Server client" on page 42.
6. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
7. Install the IBM Security Utilities, if not already installed. For instructions, see page "AIX: Installing the IBM Security Utilities" on page 39.
8. Install the Security Access Manager packages:

   ```
   installp -acgYXd package_path/usr/sys/inst.images packages
   ```

   where:

   - *package_path* is the directory where the DVD is mounted or the files are located
   - *packages* are as follows:

     PD.RTE Specifies the Security Access Manager Runtime package.

     PD.AuthADK
     Specifies the Security Access Manager Application Development Kit package.
9. Unmount the DVD, if used.
10. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.

Results

When a message is displayed that indicates the package was successfully configured, select the **x** option twice to close the configuration utility.

This step completes the setup of a Security Access Manager development (ADK) system. To set up another Security Access Manager system, follow the steps in the Chapter 3, “Installation roadmap,” on page 21.

Linux: Installing a development (ADK) system

Use **rpm** to install software packages and the **pdconfig** utility to configure them on Linux.

Before you begin

Complete the appropriate preinstallation tasks in:

- “Operating system preparation” on page 28.
- Chapter 4, “Prerequisite installation and configuration roadmap,” on page 27

About this task

Note to Linux on System z users: You must first obtain access to the Linux `rpm` files which are in the `/package_path/linux_s390` directory.

Procedure

1. Log on as **root**.
2. Ensure that the registry server and policy server are up and running (in normal mode).
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
4. Change to the `package_path`*`distribution`* directory where `package_path` is the mount point for your DVD or file location and *`distribution`* specifies `linux_x86` for x86-64 or `linux_s390` for System z.
5. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page “Linux: Installing the IBM Global Security Kit (GSKit)” on page 35.
6. If using an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page “Linux: Installing the IBM Tivoli Directory Server client” on page 43.
7. Install the IBM Security Access Manager License, if not already installed. For instructions, see “AIX, Linux, Solaris: Installing the IBM Security Access Manager License” on page 37.
8. Install the IBM Security Utilities, if not already installed. For instructions, see page “Linux: Installing IBM Security Utilities” on page 40.
9. Install the packages:

   `rpm -ihv packages`

   where *`packages`* are:

	Linux on x86-64	Linux on System z
Security Access Manager Runtime package	`PDRTE-PD-7.0.0-0.x86_64.rpm`	`PDRTE-PD-7.0.0-0.s390.rpm`
Security Access Manager Application Development Kit package	`PDAuthADK-PD-7.0.0-0.x86_64.rpm`	`PDAuthADK-PD-7.0.0-0.s390.rpm`

10. Unmount the DVD, if used.
11. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.

Results

When a message is displayed that indicates the package was successfully configured, select the **x** option twice to close the configuration utility.

This step completes the setup of a Security Access Manager development (ADK) system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Solaris: Installing a development (ADK) system

Use **pkgadd** to install software packages and the **pdconfig** utility to configure them on Solaris.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

About this task

Attention: Installations on Solaris systems should use the **-G** option with the **pkgadd** utility. The **-G** option adds the package into the current zone only.

Procedure

1. Log on as **root**.
2. Ensure that the registry server and policy server are up and running (in normal mode).
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
4. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Solaris: Installing the IBM Global Security Kit (GSKit)" on page 36.
5. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Solaris: Installing the IBM Tivoli Directory Server client" on page 44.
6. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
7. Install the IBM Security Utilities, if not already installed. For instructions, see page "Solaris: Installing IBM Security Utilities" on page 40.
8. Install the Security Access Manager packages (one at a time):

   ```
   pkgadd -d /package_path/solaris
     -a /package_path/solaris/pddefault -G packages
   ```

   where:

/package_path/solaris
Specifies the location of the package.

/package_path/solaris/pddefault
Specifies the location of the installation administration script.

and *packages* are as follows:

PDRTE Specifies the Security Access Manager Runtime package.

PDAuthADK
Specifies the Security Access Manager Application Development Kit package.

When the installation process is complete for each package, the following message is displayed:

`Installation of package successful.`

9. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.

Results

When a message is displayed that indicates the package was successfully configured, press Enter to configure another package or select the **x** option twice to close the configuration utility.

This step completes the setup of a Security Access Manager development (ADK) system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Windows: Installing a development (ADK) system

Use the **setup.exe** program to install software packages and the **pdconfig** utility to configure them on Windows.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

Procedure

1. Log on as a user with Administrator group privileges.
2. Ensure that the registry server and policy server are up and running (in normal mode).
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
4. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Windows: Installing the IBM Global Security Kit (GSKit)" on page 36.
5. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Windows: Installing the IBM Tivoli Directory Server client" on page 45.

6. Install the Security Access Manager license, if not already installed. For instructions, see "Windows: Installing the IBM Security Access Manager License" on page 39.
7. Install the IBM Security Utilities, if not already installed. For instructions, see page "Windows: Installing IBM Security Utilities" on page 41.
8. Install the packages. To do so, run the **setup.exe** program in the following directory:

   ```
   \windows\PolicyDirector\Disk Images\Disk1
   ```

   Follow the online instructions and select to install the following packages:
   - Security Access Manager Runtime
   - Security Access Manager Application Development Kit
9. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.

Results

This step completes the setup of a Security Access Manager development (ADK) system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Setting up a development system using the Launchpad (Windows)

Use the Launchpad installation method to install and configure a development system and its prerequisite software on Windows using a graphical user interface.

Before you begin

Ensure that you complete the following prerequisite tasks:
- "Operating system preparation" on page 28
- Chapter 5, "User registry server installation and configuration," on page 51.

About this task

The Launchpad uses a graphical user interface to perform step-by-step installation and initial configuration.

This task installs the following components:
- IBM Global Security Kit (GSKit)
- IBM Tivoli Directory Server client
- IBM Security Utilities
- Security Access Manager License
- Security Access Manager Runtime
- Security Access Manager Application Development Kit

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the Launchpad image files are in a directory path that does not contain any spaces.

2. Start the Launchpad.
   a. Locate the `launchpad64.exe` file.
   b. Double-click the file to start the Launchpad.
3. Select the language that you want to use during the installation and click **OK**. The Launchpad Welcome window opens.
4. Click **Next**.
5. Select the **Application Development Kit** component.
6. Click **Next**. A list displays the component that you selected and any prerequisite software that is required by that component but that is not already installed.
7. Click **Next**. An arrow next to a component name on the left indicates that component is being installed. A check mark next to a component name indicates that component is installed.
8. If the current component is IBM Global Security Kit, click **Install IBM Global Security Kit** to install it. When it completes, continue with step 9.
9. Click **Next**.
10. Respond to the prompts presented during the installation.
11. Click **Next** at the bottom of the Launchpad to continue.
12. Complete the installation.
    - If the installation fails, correct the error that is described in the error message and restart the Launchpad.
    - If the installation is successful, continue with step 13.
13. Click **Next** to start the configuration.

    Note: The configuration tool is displayed in the language that is selected for your operating system locale. If the tool is displayed in English and is not displayed in the operating system locale, review the language pack installation log at `%USERPROFILE%\ISAMLangPacksInstall.log`. Correct any errors that are reported in the log file. Then, install the language pack as described in Appendix E, "Language support installation," on page 339.
14. Click the **Configure Application Development Kit** button.
15. Select the component.
16. Click **Configure**.
17. Complete the configuration. For help completing the prompts, see Appendix D, "pdconfig options," on page 317. When all installations and configurations are completed, a success or failure message is displayed.
18. Take one of the following actions:
    - If the configuration completed successfully, click **Next**.
    - If the configuration failed or an error is displayed, review the log file in the default `%USERPROFILE%` location, such as `C:\Users\Administrator\LaunchPDConfigforISAM.log`.

      Make corrections as indicated by the log file. Then, configure the component by using the **pdconfig** utility at a command line or by clicking **Start** > **Programs** > **IBM Security Access Manager for Web** > **Configuration**.
19. Click **Finish** to close the Launchpad.

Setting up a development system using script files

The installation and configuration scripts can automate installations and perform unattended (*silent*) installations and configurations.

Use the scripts in their original state or modify them to suit the requirements of your environment.

Automating the installation of a development system (AIX, Linux, or Solaris)

Use the script file to automate the installation of a development system.

About this task

Automated installations can perform unattended (*silent*) installations.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the `install_isam.sh` script file in the `scripts` directory.
3. Run the script as follows:

   ```
   ./install_isam.sh -i ADK -d path_to_packages -a [accept|display]
   ```

   where

   - *path_to_packages* is the location of the component installation packages.

     For example, if you are installing from a DVD:

     AIX
     dvd_mount_point`/usr/sys/inst.images`

     Linux x86-64
     `/mnt/dvd/linux_x86`

     Linux on System z
     `/linux_s390`

     Solaris
     `/dvd/`*dvd0*`/solaris`

   - `-a [accept|display]`

     The `-a accept` option automatically accepts the license without displaying the license. The `-a display` option displays the license and you must manually accept the license.

   For example, if you are installing on Linux x86-64:

   ```
   ./install_isam.sh -i ADK -d package_path/linux_x86 -a accept
   ```

   The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.
4. Optional: To list the required packages without installing, use the `-l` option.

   ```
   ./install_isam.sh -l ADK
   ```

What to do next

To view the status and messages in a language other than English, which is the default, install your language support package. For instructions, see "Installing

language support packages for Security Access Manager" on page 340.

Automating the installation of a development system (Windows)

Use the script file to automate the installation of a development system on Windows.

Before you begin

The installation script uses the following default destination directories:

IBM Security Access Manager
`C:\Program Files\Tivoli\Policy Director`

Tivoli Directory Server client
`C:\Program Files\IBM\ldap\V6.3`

IBM Security Utilities
`C:\Program Files\Tivoli\TivSecUtl`

If you want to change these directories, you must do so before you run the script:

1. Copy *all* of the `.iss` files from the DVD or extracted archive files to a temporary directory on your computer. The files that you can modify are:

   IBM Security Access Manager
   `ISAMLicense.iss`

   IBM Tivoli Directory Server client
   `LDAPClient.iss`

   IBM Security Utilities
   `IBMSecurityUtils.iss`
2. Use a text editor to change the destination path in one or all three files.
3. Save the files.
4. Copy the script command file, `install_isam.bat`, from the DVD or extracted archive files into the same directory on your computer.
5. Run the script command as described in the following task.

About this task

Automated installations can perform unattended (*silent*) installations.

Attention: The installation script requires administrator privileges. Run the script file command, `install_isam.bat`, after you log in using an administrator ID or from a command window that you open with **Run as administrator**.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the `install_isam.bat` in the `scripts` directory. This directory is on the product DVD or in the directory where you extracted the product files. Ensure that the `.bat` file and all the `.iss` files are in the same directory.
3. Run the script as follows:
   `install_isam.bat /i ADK /d path_to_packages`

   where:

- *path_to_packages* is the path to the product DVD or the directory where you extracted the product files.
- For example, to install the ADK, type:

  ```
  install_isam.bat /i ADK /d c:\isam_images
  ```

  where `c:\isam_images` is the directory where the extracted subdirectories and product files are located. The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.

4. Optional: To list the required packages without installing, use the /l option.

   ```
   install_isam.bat /l ADK
   ```

What to do next

To view the status and messages in a language other than English, which is the default, install your language support package. For instructions, see "Installing language support packages for Security Access Manager" on page 340.

Chapter 9. Setting up a IBM Security Access Manager Runtime for Java system

The IBM Security Access Manager Runtime for Java offers a reliable environment for developing and deploying Java applications in a Security Access Manager secure domain. Use it to add Security Access Manager authorization and security services to new or existing Java applications.

Set up this system by following the instructions that are appropriate for your operating system.

IBM Security Access Manager Runtime for Java configures additional security features into the specified JRE.

Note:

1. IBM Security Access Manager Runtime for Java supports only the following Java runtime environments (JREs):
   - IBM Java Runtime provided with Security Access Manager
   - The JRE provided with WebSphere Application Server.
2. If you reinstall and reconfigure the Security Access Manager policy server, or install any IBM WebSphere Application Server patches, you must unconfigure and reconfigure IBM Security Access Manager Runtime for Java.
3. If you configure the Security Access Manager security standard in the `ssl-compliance` option to Suite B, NIST SP800-131, or FIPS, and not the default of "`none`," then during Web Portal Manager configuration, you must also configure WebSphere Application Server to enable the same security standard. If the security standard settings do not match, Web Portal Manager configuration fails. To enable the same security setting in WebSphere Application Server, see http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=%2Fcom.ibm.websphere.nd.multiplatform.doc%2Finfo%2Fae%2Fae%2Fcsec_security_standards.html

Setting up a Security Access Manager Runtime for Java system using the command line

Use platform-specific command-line utilities to install the runtime for Java system. This method is one of several installation methods you can use.

For more information, see Chapter 2, “Installation methods,” on page 19.

When you use the command-line utilities, you must manually install each component and its prerequisite software in the appropriate order.

Complete the prerequisite installations first. See Part 2, “Prerequisite software installation,” on page 25.

The platform-specific installation utilities that are used are:

AIX `installp`

Linux `rpm`

Solaris

pkgadd

Note: Installations on Solaris systems should use the **-G** option with the **pkgadd** utility. The **-G** option adds the package into the current zone only. When the **-G** option is used in the global zone, the package is added to the global zone only and is not propagated to any existing or yet-to-be-created non-global zone. When used in a non-global zone, the package(s) are added to the non-global zone only.

Windows

setup.exe

After you complete the installation, use the appropriate configuration commands. For example, if the Security Access Manager Runtime component is installed on your system, you can use the **pdconfig** utility to configure Security Access Manager components and, if the Security Access Manager Runtime component is *not* installed, you can use component-specific utilities, such as **pdjrtecfg** to configure the IBM Security Access Manager Runtime for Java component or **amwpmcfg** to configure the Security Access Manager Web Portal Manager component.

Note: For more information about these utilities, see the *IBM Security Access Manager for Web Command Reference*.

AIX: Installing IBM Security Access Manager Runtime for Java

Use **installp** to install IBM Security Access Manager Runtime for Java and the **pdjrtecfg** utility to configure it on AIX.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

Procedure

1. Log on as **root**.
2. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
3. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
4. Install the packages:

   ```
   installp -acgYXd package_path/usr/sys/inst.images PDJ.rte
   ```

   where *package_path* is the directory where the DVD is mounted or the files are located.
5. Ensure that either IBM Java Runtime provided with Security Access Manager or the JRE provided with WebSphere Application Server is installed. For instructions on installing IBM Java Runtime, see page "AIX: Installing IBM Java Runtime" on page 31.

IBM Security Access Manager Runtime for Java configures additional security features into the specified JRE and only these two JREs are supported.

6. Unmount the DVD, if used.
7. To view status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
8. To set up an IBM Security Access Manager Runtime for Java system with a configuration type of **Full**, ensure that both the policy server and registry server are running. If the configuration type is **standalone**, this step is not required.
9. Before you configure the IBM Security Access Manager Runtime for Java component, ensure that either the IBM Java Runtime provided with Security Access Manager or the JRE provided with WebSphere Application Server can be located by using the PATH environment variable.
10. To configure the IBM Security Access Manager Runtime for Java component, change to the `/opt/PolicyDirector/sbin` directory and enter the following command:

    ```
    ./pdjrtecfg -action config -interactive
    ```

Results

This step completes the setup of the Security Access Manager IBM Security Access Manager Runtime for Java component. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Linux: Installing IBM Security Access Manager Runtime for Java

Use **rpm** to install the IBM Security Access Manager Runtime for Java system and the **pdjrtecfg** utility to configure it on Linux.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

About this task

Note to Linux on System z users: You must first obtain access to the Linux `rpm` files which are in the */package_path*`/linux_s390` directory.

Procedure

1. Log on as **root**.
2. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
3. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.

4. Change to the *package_path*/*distribution* directory where *package_path* is the mount point for your DVD or file location and *distribution* specifies `linux_x86` for x86-64 or `linux_s390` for System z.
5. Install the package:

   `rpm -ihv package`

   where *package* is one of the following options:

	Linux on x86-64	Linux on System z
Security Access Manager Runtime for Java package	`PDJrte-PD-7.0.0-0.x86_64.rpm`	`PDJrte-PD-7.0.0-0.s390.rpm`

6. Ensure that either IBM Java Runtime provided with Security Access Manager or the JRE provided with WebSphere Application Server is installed. For instructions on installing IBM Java Runtime, see page "Linux: Installing IBM Java Runtime" on page 32.
   IBM Security Access Manager Runtime for Java configures additional security features into the specified JRE and only these two JREs are supported.
7. Unmount the DVD, if used.
8. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
9. To set up IBM Security Access Manager Runtime for Java with a configuration type of **Full**, ensure that both the policy server and registry server are running. If the configuration type is **standalone**, this step is not required.
10. Before you configure the IBM Security Access Manager Runtime for Java component, ensure that either the IBM Java Runtime provided with Security Access Manager or the JRE provided with WebSphere Application Server can be located by using the PATH environment variable.
11. To configure the IBM Security Access Manager Runtime for Java component, change to the `/opt/PolicyDirector/sbin` directory and enter the following command:`./pdjrtecfg -action config -interactive`

Results

This step completes the setup of the Security Access Manager IBM Security Access Manager Runtime for Java component. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Solaris: Installing IBM Security Access Manager Runtime for Java

Use **pkgadd** to install the IBM Security Access Manager Runtime for Java package and the **pdjrtecfg** utility to configure it on Solaris.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

About this task

Attention: Installations on Solaris systems should use the **-G** option with the **pkgadd** utility. The **-G** option adds the package into the current zone only.

Procedure

1. Log on as **root**.
2. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
3. Install the IBM Security Access Manager for Web License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
4. Install the Security Access Manager packages:

   ```
   pkgadd -d /package_path/solaris
     -a /package_path/solaris/pddefault -G PDJrte
   ```

   where

   /package_path/solaris
   Specifies the location of the package.

   /package_path/solaris/pddefault
   Specifies the location of the installation administration script.
5. Ensure that either IBM Java Runtime provided with Security Access Manager or the JRE provided with WebSphere Application Server is installed. For instructions on installing IBM Java Runtime, see page "Solaris: Installing IBM Java Runtime" on page 33.

   IBM Security Access Manager Runtime for Java configures additional security features into the specified JRE and only these two JREs are supported.
6. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
7. To set up IBM Security Access Manager Runtime for Java with a configuration type of **Full**, ensure that both the policy server and registry server are running. If the configuration type is **standalone**, this step is not required.
8. Before you configure the IBM Security Access Manager Runtime for Java component, ensure that either the IBM Java Runtime provided with Security Access Manager or the JRE provided with WebSphere Application Server can be located by using the PATH environment variable.
9. To configure the IBM Security Access Manager Runtime for Java component, change to the `/opt/PolicyDirector/sbin` directory and enter the following command:

   ```
   ./pdjrtecfg -action config -interactive
   ```

Results

This step completes the setup of the Security Access Manager IBM Security Access Manager Runtime for Java component. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Windows: Installing IBM Security Access Manager Runtime for Java

Use the **setup.exe** program to install the IBM Security Access Manager Runtime for Java package and the **pdjrtecfg** utility to configure it on Windows.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

Procedure

1. Log on as a user with Administrator group privileges.
2. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
3. Install the Security Access Manager license, if not already installed. For instructions, see "Windows: Installing the IBM Security Access Manager License" on page 39.
4. Install the Security Access Manager package. To do so, run the **setup.exe** file, in the following directory:

   ```
   \windows\PolicyDirector\Disk Images\Disk1
   ```

   Follow the online instructions and select **IBM Security Access Manager Runtime for Java**.
5. Ensure that either IBM Java Runtime provided with Security Access Manager or the JRE provided with WebSphere Application Server is installed. For instructions on installing IBM Java Runtime, see page "Windows: Installing IBM Java Runtime" on page 34.

   IBM Security Access Manager Runtime for Java configures additional security features into the specified JRE and only these two JREs are supported.
6. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
7. To set up IBM Security Access Manager Runtime for Java with a configuration type of **Full**, ensure that both the policy server and registry server are running. If the configuration type is **standalone**, this step is not required.
8. To configure the IBM Security Access Manager Runtime for Java component, change to the `c:\Program Files\Tivoli\Policy Director\sbin` directory and enter the following command:

   ```
   pdjrtecfg -action config -interactive
   ```

What to do next

This step completes the setup of the Security Access Manager IBM Security Access Manager Runtime for Java component. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Setting up a runtime for Java system using the Launchpad (Windows)

Use the Launchpad installation method to install and configure the policy server and its prerequisite software on Windows by using a graphical user interface.

Before you begin

Ensure that you complete the following prerequisite tasks:

- "Operating system preparation" on page 28
- Chapter 5, "User registry server installation and configuration," on page 51.

About this task

The Launchpad uses a graphical user interface to perform step-by-step installation and initial configuration.

This task installs the following components:

- Security Access Manager License
- Security Access Manager Runtime for Java
- IBM Java SDK

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the Launchpad image files are in a directory path that does not contain any spaces.
2. Start the Launchpad.
   a. Locate the `launchpad64.exe` file.
   b. Double-click the file to start the Launchpad.
3. Select the language that you want to use during the installation and click **OK**. The Launchpad Welcome window opens.
4. Click **Next**.
5. Select the **Java Runtime** component.
6. Click **Next**. A list displays the component that you selected and any prerequisite software that is required by that component but that is not already installed.
7. Click **Next**. An arrow next to a component name on the left indicates that component is being installed. A check mark next to a component name indicates that component is installed.
8. Click **Next**. The installation of the first component begins.
9. Respond to the prompts presented during the installation.
10. Click **Next** at the bottom of the Launchpad to continue.
11. Complete the installation.
    - If the installation fails, correct the error that is described in the error message and restart the Launchpad.
    - If the installation is successful, continue with step 12.
12. Click **Next** to start the configuration.

    Note: The configuration tool is displayed in the language that is selected for your operating system locale. If the tool is displayed in English and is not

displayed in the operating system locale, review the language pack installation log at %USERPROFILE%\ISAMLangPacksInstall.log. Correct any errors that are reported in the log file. Then, install the language pack as described in Appendix E, "Language support installation," on page 339.

13. Click the **Configure Java Runtime** button.
14. Complete the configuration. For help completing the prompts, see Appendix D, "pdconfig options," on page 317. When all installations and configurations are completed, a success or failure message is displayed.
15. Take one of the following actions:
    - If the installation completed successfully, click **Next**.
    - If the configuration failed or an error is displayed, review the log file in the default %USERPROFILE% location, such as C:\Users\Administrator\LaunchPDConfigforISAM.log.

      Make corrections as indicated by the log file. Then, configure the component by using the **pdconfig** utility at a command line or by clicking **Start** > **Programs** > **IBM Security Access Manager for Web** > **Configuration**.
16. Click **Finish** to close the Launchpad.

Setting up a runtime for Java server using script files

The installation and configuration scripts can automate installations and perform unattended (*silent*) installations and configurations.

Use the scripts in their original state or modify them to suit the requirements of your environment.

Automating the installation of a runtime for Java system (AIX, Linux, or Solaris)

Use the script file to automate the installation of a runtime for Java system.

About this task

Automated installations can perform unattended (*silent*) installations.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the install_isam.sh script file in the scripts directory.
3. Run the script as follows:

   ```
   ./install_isam.sh -i RuntimeJava -d path_to_packages -a [accept|display]
   ```

   where
   - *path_to_packages* is the location of the component installation packages.

     For example, if you are installing from a DVD:

     AIX *dvd_mount_point*/usr/sys/inst.images

     Linux x86-64
     /mnt/dvd/linux_x86

     Linux on System z
     /linux_s390

Solaris

/dvd/*dvd0*/solaris

- `-a [accept|display]`

  The `-a accept` option automatically accepts the license without displaying the license. The `-a display` option displays the license and you must manually accept the license.

For example, if you are installing on Linux x86-64:

```
./install_isam.sh -i RuntimeJava -d /mnt/dvd/linux_x86 -a accept
```

The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.

4. Optional: To list the required packages without installing, use the -l option.

   ```
   ./install_isam.sh -l RuntimeJava
   ```

What to do next

When the installation is completed, continue with "Automating the configuration of a runtime for Java system" on page 154.

Automating the installation of a runtime for Java system (Windows)

Use the script file to automate the installation of a runtime for Java system on Windows.

About this task

Automated installations can perform unattended (*silent*) installations.

Attention: The installation script requires administrator privileges. Run the script file command, `install_isam.bat`, after you log in using an administrator ID or from a command window that you open with **Run as administrator**.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the `install_isam.bat` in the `scripts` directory. This directory is on the product DVD or in the directory where you extracted the product files. Ensure that the `.bat` file and all the `.iss` files are in the same directory.
3. Run the script as follows:

   ```
   install_isam.bat /i RuntimeJava /d path_to_packages
   ```

   where :

   - *path_to_packages* is the path to the product DVD or the directory where you extracted the product files.
   - For example, to install the runtime for Java component, type:

     ```
     install_isam.bat /i RuntimeJava /d c:\isam_images
     ```

     where `c:\isam_images` is the directory where the extracted subdirectories and product files are located.

The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.

4. Optional: To list the required packages without installing, use the /l option.

```
install_isam.bat /l RuntimeJava
```

What to do next

When the installation is completed, continue with "Automating the configuration of a runtime for Java system."

Automating the configuration of a runtime for Java system

Use the script file to automate the configuration of a runtime for Java system.

Before you begin

- Complete the installation of the runtime for Java. See:
  - "Automating the installation of a runtime for Java system (AIX, Linux, or Solaris)" on page 152
  - "Automating the installation of a runtime for Java system (Windows)" on page 153
- To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.

If you are running this script on Windows, open a new command window. Do not perform this task in the same window where you ran the installation script.

About this task

Automated configuration performs unattended (*silent*) configuration.

The script files and template files that are used in this task are installed in the following locations by default:

AIX, Linux, and Solaris: `/opt/PolicyDirector/example/config`

Windows: `C:\Program Files\Tivoli\Policy Director\example\config`

Procedure

1. Create an options file for the component you want to configure.
   a. Locate the options file template for the component. For the runtime for Java component, use the following template:

      AIX, Linux, or Solaris

      ```
      configure_javarte.options.template
      ```

      Windows

      ```
      configure_javarte.options.template.cmd
      ```

   b. Copy the file to a temporary directory. You can copy the file to the temporary directory with a name that is unique to your environment.

      Attention: You must keep the `.cmd` extension for Windows template files. The Windows template files run as commands.

c. Modify the content of the file to specify settings for your environment. The comments in the file explain the settings and provide examples.
d. Save the file.

2. Optional: By default, passwords you specified in the options files are stored in clear text. To obfuscate these passwords:
   a. On Windows, copy the `configure_isam.conf` file to the same directory where you copied the options files.
   b. See Appendix F, "Password management," on page 351 for instructions on using the `-obfuscate` option with the `pdconf` tool to obfuscate the passwords in the options files. For more information about `pdconf`, see the *IBM Security Access Manager for Web: Command Reference*.
   c. Return to these instructions to run the configuration script.
3. Run the configuration script and use the options file for input.

   AIX, Linux, or Solaris

   ```
   ./configure_isam.sh -f options_file
   ```

   Windows

   ```
   configure_isam.cmd -f options_file.cmd
   ```

   where *options_file* and *options_file*`.cmd` are the text files that contain the configuration options.

   For example:

   AIX, Linux, or Solaris

   ```
   ./configure_isam.sh -f my_configure_javarte.options
   ```

   Windows

   ```
   configure_isam.cmd -f my_configure_javarte.options.cmd
   ```

Chapter 10. Setting up a policy proxy server system

The Security Access Manager policy proxy server sets up a proxy server. A proxy server acts as an intermediary between a less trusted network and a more trusted network. This server ensures security and provides administrative control and caching services. It is associated with, or part of, a gateway server that separates the enterprise network from the outside network, and a firewall server that protects the enterprise network from outside intrusion. In a Security Access Manager environment, the proxy server runs on behalf of the policy server for a specified number of authorization applications and administrative functions, such as **pdadmin** commands.

Set up this system by following the appropriate instructions for your operating system.

Note: Security Access Manager does not consider the registry native password policies when it creates server accounts during configuration. The registry native password policies might cause server configuration failure. During configuration, disable the registry native policies, such as LDAP default or global policies, that might affect new server accounts.

After you create the accounts, set policies such that the accounts are not affected when you enable the disabled policies.

For LDAP registries, do not enable `pwdMustChange` during configuration. You do not have to enable `pwdMustChange` after configuration because Security Access Manager does not update server accounts.

Ensure that LDAP `pwdMaxAge` does not cause Security Access Manager server accounts to expire after configuration.

Security Access Manager generates strong passwords that are 8 - 20 characters long and contain at least one uppercase, one lowercase, and one number. But if the registry password policies are sufficiently restrictive, Security Access Manager configuration might fail when setting the generated password. So disable the registry password policies during configuration.

Setting up a policy proxy server using the command line

Use platform-specific command-line utilities to install the policy proxy server. This method is one of several installation methods you can use.

For more information, see Chapter 2, “Installation methods,” on page 19.

When you use the command-line utilities, you must manually install each component and its prerequisite software in the appropriate order.

Complete the prerequisite installations first. See Part 2, “Prerequisite software installation,” on page 25.

The platform-specific installation utilities that are used are:

AIX **`installp`**

Linux **rpm**

Solaris

pkgadd

Note: Installations on Solaris systems should use the **-G** option with the **pkgadd** utility. The **-G** option adds the package into the current zone only. When the **-G** option is used in the global zone, the package is added to the global zone only and is not propagated to any existing or yet-to-be-created non-global zone. When used in a non-global zone, the package(s) are added to the non-global zone only.

Windows

setup.exe

After you complete the installation, use the appropriate configuration commands. For example, if the Security Access Manager Runtime component is installed on your system, you can use the **pdconfig** utility to configure Security Access Manager components and, if the Security Access Manager Runtime component is *not* installed, you can use component-specific utilities, such as **pdjrtecfg** to configure the IBM Security Access Manager Runtime for Java component or **amwpmcfg** to configure the Security Access Manager Web Portal Manager component.

Note: For more information about these utilities, see the *IBM Security Access Manager for Web Command Reference*.

AIX: Installing a policy proxy server

Use **installp** to install software packages and the **pdconfig** utility to configure them on AIX.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

Procedure

1. Log on as **root**.
2. Ensure that the registry server and policy server are up and running (in normal mode).
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
4. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "AIX: Installing the IBM Global Security Kit (GSKit)" on page 35.
5. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "AIX: Installing the IBM Tivoli Directory Server client" on page 42.
6. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.

7. Install the IBM Security Utilities, if not already installed. For instructions, see page "AIX: Installing the IBM Security Utilities" on page 39.
8. Install the Security Access Manager packages:

   ```
   installp -acgYXd package_path/usr/sys/inst.images packages
   ```

   where *package_path* is the directory where the DVD is mounted or the files are located and *packages* are:

   PD.RTE Specifies the Security Access Manager Runtime package.

   PD.MgrProxy
   Specifies the Security Access Manager Proxy Policy Server package.
9. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
10. Configure the Security Access Manager Runtime and Policy Server followed by the Security Access Manager Policy Proxy Server package as follows:
    a. Start the configuration utility:

       ```
       pdconfig
       ```

       The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure, one at a time.
       Depending on the package that you selected, you are prompted for configuration options. For assistance with these configuration options, see Appendix D, "pdconfig options," on page 317.

Results

When a message is displayed that indicates the package was successfully configured, press Enter to configure another package or select the **x** option twice to close the configuration utility.

This step completes the setup of a Security Access Manager policy proxy server system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Linux: Installing a policy proxy server

Use **rpm** to install software packages and the **pdconfig** utility to configure them on Linux.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

About this task

Note to Linux on System z users: You must first obtain access to the Linux `rpm` files which are in the */package_path*`/linux_s390` directory.

Procedure

1. Log on as **root**.
2. Ensure that the registry server and policy server are up and running (in normal mode).
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
4. Change to the `package_path/distribution` directory where `package_path` is the mount point for your DVD or file location and *`distribution`* specifies `linux_x86` for x86-64 or `linux_s390` for System z.
5. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Linux: Installing the IBM Global Security Kit (GSKit)" on page 35.
6. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Linux: Installing the IBM Tivoli Directory Server client" on page 43.
7. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
8. Install the IBM Security Utilities, if not already installed. For instructions, see page "Linux: Installing IBM Security Utilities" on page 40.
9. Install the Security Access Manager packages. `rpm -ihv packages`

   where *`packages`* are:

	Linux on x86-64	Linux on System z
Security Access Manager Runtime package	`PDRTE-PD-7.0.0-0.x86_64.rpm`	`PDRTE-PD-7.0.0-0.s390.rpm`
Security Access Manager Policy Proxy Server package	`PDMgrPrxy-PD-7.0.0-0.x86_64.rpm`	`PDMgrPrxy-PD-7.0.0-0.s390.rpm`

10. Unmount the DVD, if used.

    ```
    pdconfig
    ```

    The Security Access Manager Setup Menu is displayed.
11. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
12. Configure the Security Access Manager Runtime and Policy Server followed by the Security Access Manager Policy Proxy Server package as follows:
    a. Start the configuration utility:
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure, one at a time.
       Depending on the package that you selected, you are prompted for configuration options. For assistance with these configuration options, see Appendix D, "pdconfig options," on page 317.

Results

When a message is displayed that indicates the package was successfully configured, press Enter to configure another package or select the **x** option twice to close the configuration utility.

This step completes the setup of a Security Access Manager policy proxy server system. To set up another Security Access Manager system, follow the steps in the Chapter 3, “Installation roadmap,” on page 21.

Solaris: Installing a policy proxy server

Use **pkgadd** to install software packages and the **pdconfig** utility to configure them on Solaris.

Before you begin

Complete the appropriate preinstallation tasks in:

- “Operating system preparation” on page 28.
- Chapter 4, “Prerequisite installation and configuration roadmap,” on page 27

About this task

Attention: Installations on Solaris systems should use the **-G** option with the **pkgadd** utility. The **-G** option adds the package into the current zone only.

Procedure

1. Log on as **root**.
2. Ensure that the registry server and policy server are up and running (in normal mode).
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
4. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page “Solaris: Installing the IBM Global Security Kit (GSKit)” on page 36.
5. If using an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page “Solaris: Installing the IBM Tivoli Directory Server client” on page 44.
6. Install the IBM Security Access Manager License, if not already installed. For instructions, see “AIX, Linux, Solaris: Installing the IBM Security Access Manager License” on page 37.
7. Install the IBM Security Utilities, if not already installed. For instructions, see page “Solaris: Installing IBM Security Utilities” on page 40.
8. Install the Security Access Manager packages, one at a time:

   ```
   pkgadd -d /package_path/solaris
     -a /package_path/solaris/pddefault -G packages
   ```

   where:

   /*package_path*/solaris
   Specifies the location of the package.

/package_path/**solaris/pddefault**
Specifies the location of the installation administration script.

and where the *packages* are as follows:

PDRTE Specifies the Security Access Manager Runtime package.

PDMgrPrxy
Specifies the Security Access Manager Policy Proxy Server package.

When the installation process is complete for each package, the following message is displayed:

```
Installation of package successful.
```

9. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
10. Configure Security Access Manager Runtime and Policy Server followed by the Security Access Manager Policy Proxy Server package as follows:
    a. Start the configuration utility:

    ```
    pdconfig
    ```

    The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure, one at a time.

    Depending on the package that you selected, you are prompted for configuration options. For assistance with these configuration options, see Appendix D, "pdconfig options," on page 317.

Results

When a message is displayed that indicates the package was successfully configured, press Enter to configure another package or select the **x** option twice to close the configuration utility.

This step completes the setup of a Security Access Manager policy proxy server system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Windows: Installing a policy proxy server

Use the **setup.exe** program to install software packages and the **pdconfig** utility to configure them on Windows.

Procedure

1. Log on as a user with Administrator group privileges.
2. Ensure that the registry server and policy server are up and running (in normal mode).
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.

4. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Windows: Installing the IBM Global Security Kit (GSKit)" on page 36.
5. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Windows: Installing the IBM Tivoli Directory Server client" on page 45.
6. Install the Security Access Manager license, if not already installed. For instructions, see "Windows: Installing the IBM Security Access Manager License" on page 39.
7. Install the IBM Security Utilities, if not already installed. For instructions, see page "Windows: Installing IBM Security Utilities" on page 41.
8. Install the Security Access Manager packages. To do so, run the **setup.exe** program in the following directory:

   ```
   \windows\PolicyDirector\Disk Images\Disk1
   ```

   Follow the online instructions and select to install the following packages:
   - Security Access Manager Runtime
   - Security Access Manager Policy Proxy Server
9. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
10. Configure the Security Access Manager Runtime and Policy Server package followed by the Security Access Manager Policy Proxy Server package as follows:
    a. Start the configuration utility:

       ```
       pdconfig
       ```

       The Security Access Manager Configuration window is displayed.
    b. Select the **Security Access Manager Runtime** package and click **Configure**.
    c. Select the **Security Access Manager Policy Proxy Server** package and click **Configure**.

    Depending on the package that you selected, you are prompted for configuration options. For assistance with these configuration options, see Appendix D, "pdconfig options," on page 317.

Results

This step completes the setup of a Security Access Manager policy proxy server system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Setting up a policy proxy server using the Launchpad (Windows)

Use the Launchpad installation method to install and configure the policy proxy server and its prerequisite software on Windows using a graphical user interface.

Before you begin

Ensure that you complete the following prerequisite tasks:

- "Operating system preparation" on page 28
- Chapter 5, "User registry server installation and configuration," on page 51.

About this task

The Launchpad uses a graphical user interface to complete step-by-step installation and initial configuration.

This task installs the following components:

- IBM Global Security Kit (GSKit)
- IBM Tivoli Directory Server client (depending on the registry used)
- IBM Security Utilities
- Security Access Manager License
- Security Access Manager Runtime
- Security Access Manager Policy Proxy Server

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the Launchpad image files are in a directory path that does not contain any spaces.
2. Start the Launchpad.
   a. Locate the `launchpad64.exe` file.
   b. Double-click the file to start the Launchpad.
3. Select the language that you want to use during the installation and click **OK**. The Launchpad Welcome window opens.
4. Click **Next**.
5. Select the **Policy Proxy Server** component.
6. Click **Next**. A list displays the component that you selected and any prerequisite software that is required by that component but that is not already installed.
7. Click **Next**. An arrow next to a component name on the left indicates that component is being installed. A check mark next to a component name indicates that component is installed.
8. If the current component is IBM Global Security Kit, click **Install IBM Global Security Kit** to install it. When it completes, continue with step 9.
9. Click **Next**.
10. Respond to the prompts presented during the installation.
11. Click **Next** at the bottom of the Launchpad to continue.
12. Complete the installation.
    - If the installation fails, correct the error that is described in the error message and restart the Launchpad.
    - If the installation is successful, continue with step 13.
13. Click **Next** to start the configuration.

    Note: The configuration tool is displayed in the language that is selected for your operating system locale. If the tool is displayed in English and is not displayed in the operating system locale, review the language pack installation log at `%USERPROFILE%\ISAMLangPacksInstall.log`. Correct any errors that are reported in the log file. Then, install the language pack as described in Appendix E, “Language support installation,” on page 339.
14. Click **Configure Security Access Manager**. The configuration tool opens.

15. Select the component.
16. Click **Configure**.
17. Complete the configuration. For help completing the prompts, see Appendix D, "pdconfig options," on page 317. When all installations and configurations are completed, a success or failure message is displayed.
18. Take one of the following actions:
    - If the configuration completed successfully, click **Next**.
    - If the configuration failed or an error is displayed, review the log file in the default `%USERPROFILE%` location, such as `C:\Users\Administrator\LaunchPDConfigforISAM.log`.

      Make corrections as indicated by the log file. Then, configure the component by using the **pdconfig** utility at a command line or by clicking **Start** > **Programs** > **IBM Security Access Manager for Web** > **Configuration**.
19. Click **Finish** to close the Launchpad.

Setting up a policy proxy server using script files

The installation and configuration scripts can automate installations and perform unattended (*silent*) installations and configurations.

Use the scripts in their original state or modify them to suit the requirements of your environment.

Automating the installation of a policy proxy server system (AIX, Linux, or Solaris)

Use the script file to automate the installation of a policy proxy server system.

About this task

Automated installations can perform unattended (*silent*) installations.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the `install_isam.sh` script file in the `scripts` directory.
3. Run the script as follows:

   ```
   ./install_isam.sh -i ProxyServer -d path_to_packages -a [accept|display]
   ```

   where
   - *path_to_packages* is the location of the component installation packages.

     For example, if you are installing from a DVD:

     AIX *dvd_mount_point*`/usr/sys/inst.images`

     Linux x86-64
     `/mnt/dvd/linux_x86`

     Linux on System z
     `/linux_s390`

     Solaris
     `/dvd/`*dvd0*`/solaris`
   - `-a [accept|display]`

The `-a accept` option automatically accepts the license without displaying the license. The `-a display` option displays the license and you must manually accept the license.

For example, if you are installing on Linux x86-64:

```
./install_isam.sh -i ProxyServer -d /mnt/dvd/linux_x86 -a accept
```

The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.

4. Optional: To list the required packages without installing, use the `-l` option.

   ```
   ./install_isam.sh -l ProxyServer
   ```

What to do next

When the installation is completed, continue with "Automating the configuration of a policy proxy server" on page 167.

Automating the installation of a policy proxy system (Windows)

Use the script file to automate the installation of a policy proxy system on Windows.

About this task

Automated installations can perform unattended (*silent*) installations.

Attention: The installation script requires administrator privileges. Run the script file command, `install_isam.bat`, after you log in using an administrator ID or from a command window that you open with **Run as administrator**.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the `install_isam.bat` script file in the `scripts` directory. This directory is on the product DVD or in the directory where you extracted the product files. Ensure that the `.bat` file and all the `.iss` files are in the same directory.
3. Run the script as follows:

   ```
   install_isam.bat /i ProxyServer /d path_to_packages
   ```

   where :

   - *path_to_packages* is the path to the product DVD or the directory where you extracted the product files.
   - For example, to install the policy proxy server component, type:

     ```
     install_isam.bat /i ProxyServer /d c:\isam_images
     ```

     where `c:\isam_images` is the directory where the extracted subdirectories and files are located.

   The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.
4. Optional: To list the required packages without installing, use the `/l` option.

   ```
   install_isam.bat /l ProxyServer
   ```

What to do next

When the installation is completed, continue with "Automating the configuration of a policy proxy server."

Automating the configuration of a policy proxy server

Use the script file to automate the configuration of a policy proxy server.

Before you begin

- Complete the installation of the policy proxy server. See:
  - "Automating the installation of a policy proxy server system (AIX, Linux, or Solaris)" on page 165
  - "Automating the installation of a policy proxy system (Windows)" on page 166
- To view status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.

If you are running this script on Windows, open a new command window. Do not perform this task in the same window where you ran the installation script.

About this task

Automated configuration performs unattended (*silent*) configuration.

The script files and template files that are used in this task are installed in the following locations by default:

AIX, Linux, and Solaris: `/opt/PolicyDirector/example/config`

Windows: `C:\Program Files\Tivoli\Policy Director\example\config`

Procedure

1. Create an options file for the component you want to configure.
   a. Locate the options file template for the component.

      AIX, Linux, or Solaris

      ```
      configure_policysvrproxy.options.template
      ```

      Windows

      ```
      configure_policysvrproxy.options.template.cmd
      ```

   b. Copy the file to a temporary directory. You can copy the file to the temporary directory with a name that is unique to your environment.

      Attention: You must keep the `.cmd` extension for Windows template files. The Windows template files run as commands.

   c. Modify the content of the file to specify settings for your environment. The comments in the file explain the settings and provide examples.
   d. Save the file.
2. Optional: By default, passwords you specified in the options files are stored in clear text. To obfuscate these passwords:
   a. On Windows, copy the `configure_isam.conf` file to the same directory where you copied the options files.

b. See Appendix F, "Password management," on page 351 for instructions on using the `-obfuscate` option with the `pdconf` tool to obfuscate the passwords in the options files. For more information about `pdconf`, see the *IBM Security Access Manager for Web Command Reference*.

c. Return to these instructions to run the configuration script.

3. Run the configuration script and use the options file for input.

   AIX, Linux, or Solaris

   ```
   ./configure_isam.sh -f options_file
   ```

   Windows

   ```
   configure_isam.cmd -f options_file.cmd
   ```

   where *options_file* and *options_file*.cmd are the text files that contain the configuration options.

   For example:

   AIX, Linux, or Solaris

   ```
   ./configure_isam.sh -f my_configure_policysvrproxy.options
   ```

   Windows

   ```
   configure_isam.cmd -f my_configure_policysvrproxy.options.cmd
   ```

Chapter 11. Setting up a runtime system

The Security Access Manager Runtime contains runtime libraries and supporting files that applications can use to access Security Access Manager servers. You must install and configure the Security Access Manager Runtime component on each system that runs Security Access Manager, except for Security Access Manager Runtime for Java systems, the Security Access Manager Attribute Retrieval Service, and the distributed sessions management systems.

Set up this system by following appropriate instructions for your operating system.

Setting up a runtime server using the command line

Use platform-specific command-line utilities to install the runtime server. This method is one of several installation methods you can use.

For more information, see Chapter 2, “Installation methods,” on page 19.

When you use the command-line utilities, you must manually install each component and its prerequisite software in the appropriate order.

Complete the prerequisite installations first. See Part 2, “Prerequisite software installation,” on page 25.

The platform-specific installation utilities that are used are:

AIX **`installp`**

Linux **`rpm`**

Solaris
`pkgadd`

Note: Installations on Solaris systems should use the **-G** option with the **`pkgadd`** utility. The **-G** option adds the package into the current zone only. When the **-G** option is used in the global zone, the package is added to the global zone only and is not propagated to any existing or yet-to-be-created non-global zone. When used in a non-global zone, the package(s) are added to the non-global zone only.

Windows
`setup.exe`

After you complete the installation, use the appropriate configuration commands. For example, if the Security Access Manager Runtime component is installed on your system, you can use the **`pdconfig`** utility to configure Security Access Manager components and, if the Security Access Manager Runtime component is *not* installed, you can use component-specific utilities, such as **`pdjrtecfg`** to configure the IBM Security Access Manager Runtime for Java component or **`amwpmcfg`** to configure the Security Access Manager Web Portal Manager component.

Note: For more information about these utilities, see the *IBM Security Access Manager for Web Command Reference*.

AIX: Installing Security Access Manager Runtime

Use **installp** to install software packages and the **pdconfig** utility to configure them on AIX.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

Procedure

1. Log on as **root**.
2. Ensure that the registry server and policy server are up and running (in normal mode).
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
4. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "AIX: Installing the IBM Global Security Kit (GSKit)" on page 35.
5. Install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "AIX: Installing the IBM Tivoli Directory Server client" on page 42.
6. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
7. Install the IBM Security Utilities, if not already installed. For instructions, see page "AIX: Installing the IBM Security Utilities" on page 39.
8. Install the Security Access Manager packages:

   ```
   installp -acgYXd package_path/usr/sys/inst.images PD.RTE
   ```

   where *package_path* is the directory where the DVD is mounted or the files are located.
9. Unmount the DVD, if used.
10. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
11. Configure the Security Access Manager Runtime package as follows:
    a. Start the configuration utility:

       ```
       pdconfig
       ```

       The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure, one at a time. For assistance with configuration options, see Appendix D, "pdconfig options," on page 317.
       When a message is displayed that indicates the package was successfully configured, press Enter to configure another package or select the **x** option twice to close the configuration utility.

Results

This step completes the setup of a Security Access Manager runtime system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Linux: Installing Security Access Manager Runtime

Use **rpm** to install software packages and the **pdconfig** utility to configure them on Linux.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

About this task

Note to Linux on System z users: You must first obtain access to the Linux `rpm` files which are in the */package_path*`/linux_s390` directory.

Procedure

1. Log on as **root**.
2. Ensure that the registry server and policy server are up and running (in normal mode).
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
4. Change to the *package_path*`/`*distribution* directory where:
   - *package_path* is the mount point for your DVD or location of the packages
   - *distribution* specifies `linux_x86` for x86-64 or `linux_s390` for System z
5. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Linux: Installing the IBM Global Security Kit (GSKit)" on page 35.
6. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Linux: Installing the IBM Tivoli Directory Server client" on page 43.
7. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
8. Install the IBM Security Utilities, if not already installed. For instructions, see page "Linux: Installing IBM Security Utilities" on page 40.
9. Install the Security Access Manager packages:

   ```
   rpm -ihv package
   ```

   where *package* is:

	Linux on x86-64	Linux on System z
Security Access Manager Runtime package	`PDRTE-PD-7.0.0-0.x86_64.rpm`	`PDRTE-PD-7.0.0-0.s390.rpm`

10. Unmount the DVD, if used.
11. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
12. Configure the Security Access Manager Runtime package as follows:
    a. Start the configuration utility:
    ```
    pdconfig
    ```
    The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.

Results

When a message is displayed that indicates the package was successfully configured, select the **x** option twice to close the configuration utility.

This step completes the setup of a Security Access Manager runtime system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Starting Security Access Manager components on SUSE Linux Enterprise Server 10

After you install Security Access Manager on a SUSE Linux Enterprise Server 10 system, the components do not start automatically when you restart the system. You must complete the steps that are described here to start the components.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

Procedure

1. Locate and remove the following files:
   - `/etc/init.d/rc0.d/K005pd`
   - `/etc/init.d/rc3.d/S590pd`
   - `/etc/init.d/rc5.d/S590pd`
2. Enable editing of the `/opt/PolicyDirector/bin/pd_start` file by running the following command:
   ```
   chmod +w /opt/PolicyDirector/bin/pd_start
   ```
3. Add the following lines after the first line in the `/opt/PolicyDirector/bin/pd_start` file:
   ```
   ### BEGIN INIT INFO
   # Provides:pd
   # Required-Start: $network
   # Required-Stop:
   # Default-Start:3 5
   # Default-Stop:
   # Description:Script to start and stop Security Access Manager.
   ### END INIT INFO
   ```

4. Run the following command to enable Security Access Manager servers to start during system startup:

   ```
   chkconfig pd on
   ```

   This command creates the following start and stop script links:

   ```
   lrwxrwxrwx 1 root root 5 Mar 15 16:11 /etc/init.d/rc3.d/K16pd -> ../pd
   lrwxrwxrwx 1 root root 5 Mar 15 16:11 /etc/init.d/rc3.d/S06pd -> ../pd
   lrwxrwxrwx 1 root root 5 Mar 15 16:11 /etc/init.d/rc5.d/K16pd -> ../pd
   lrwxrwxrwx 1 root root 5 Mar 15 16:11 /etc/init.d/rc5.d/S06pd -> ../pd
   ```

Results

Note:

1. Run the following command before uninstalling Security Access Manager runtime from your computer:

   ```
   chkconfig pd off
   ```

2. If Tivoli Directory Server is installed on the same computer as Security Access Manager, add Tivoli Directory Server to the `# Required-Start:` line of the `/opt/PolicyDirector/bin/pd_start` file.

   Run the following commands in this order:

   a. `chkconfig pd off`

   b. `chkconfig pd on`

   Running these commands ensures that the Security Access Manager log files do not have messages that indicate that the LDAP server failed and recovered.

Solaris: Installing Security Access Manager Runtime

Use **pkgadd** to install software packages and the **pdconfig** utility to configure them on Solaris.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

About this task

Attention: Installations on Solaris systems should use the **-G** option with the **pkgadd** utility. The **-G** option adds the package into the current zone only.

Procedure

1. Log on as **root**.
2. Ensure that the registry server and policy server are up and running (in normal mode).
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
4. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Solaris: Installing the IBM Global Security Kit (GSKit)" on page 36.

5. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Solaris: Installing the IBM Tivoli Directory Server client" on page 44.
6. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
7. Install the IBM Security Utilities, if not already installed. For instructions, see page "Solaris: Installing IBM Security Utilities" on page 40.
8. Install the Security Access Manager packages:

   ```
   pkgadd -d /package_path/solaris
          -a /package_path/solaris/pddefault -G PDRTE
   ```

   where:

   /package_path/**solaris**
   Specifies the location of the package.

   /package_path/**solaris/pddefault**
   Specifies the location of the installation administration script.

   When the installation process is complete for each package, the following message is displayed: `Installation of package successful.`
9. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
10. Configure the Security Access Manager Runtime package as follows:
    a. Start the configuration utility:

       ```
       pdconfig
       ```

       The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure. For assistance with configuration options, see Appendix D, "pdconfig options," on page 317.

Results

When a message is displayed that indicates the package was successfully configured, press Enter to configure another package or select the **x** option twice to close the configuration utility.
This step completes the setup of a Security Access Manager runtime system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Windows: Installing Security Access Manager Runtime

Use the **setup.exe** program to install software packages and the **pdconfig** utility to configure them on Windows.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

Procedure

1. Log on as any member of the Administrators group.
2. Log on as a user with administrator privileges.
3. Ensure that the registry server and policy server are up and running (in normal mode).
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
5. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Windows: Installing the IBM Global Security Kit (GSKit)" on page 36.
6. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Windows: Installing the IBM Tivoli Directory Server client" on page 45.
7. Install the Security Access Manager license, if not already installed. For instructions, see "Windows: Installing the IBM Security Access Manager License" on page 39.
8. Install the IBM Security Utilities, if not already installed. For instructions, see page "Windows: Installing IBM Security Utilities" on page 41.
9. Install the Security Access Manager packages. To do so, run the **setup.exe** program in this directory:

   ```
   \windows\PolicyDirector\Disk Images\Disk1
   ```

   Follow the online instructions and select to install the **Security Access Manager Runtime**.
10. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
11. Configure the Security Access Manager Runtime package as follows:
    a. Open a new command-line window.
    b. Start the configuration utility:

       ```
       pdconfig
       ```

       The Security Access Manager Configuration window is displayed.
    c. Select the **Security Access Manager Runtime** package and click **Configure**.

    You are prompted for configuration options. For assistance with these configuration options, see Appendix D, "pdconfig options," on page 317.

Results

This step completes the setup of a Security Access Manager runtime system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Setting up a runtime server using the Launchpad (Windows)

Use the Launchpad installation method to install runtime system components and their prerequisite software on a computer that is running the Windows operating system.

Before you begin

Ensure that you complete the following prerequisite tasks:

- "Operating system preparation" on page 28
- Chapter 5, "User registry server installation and configuration," on page 51.

About this task

The Launchpad uses a graphical user interface to perform step-by-step installation and initial configuration.

This task installs the following components:

- IBM Global Security Kit (GSKit)
- IBM Tivoli Directory Server client
- IBM Security Utilities
- Security Access Manager License
- Security Access Manager Runtime

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the Launchpad image files are in a directory path that does not contain any spaces.
2. Start the Launchpad.
   a. Locate the `launchpad64.exe` file.
   b. Double-click the file to start the Launchpad.
3. Select the language that you want to use during the installation and click **OK**. The Launchpad Welcome window opens.
4. Click **Next**.
5. Select the **Runtime** component.
6. Click **Next**. The list on the left displays the component that you selected. The list also displays any prerequisite software that is required by that component but that is not already installed.
7. Click **Next**. The installation panel for the first component that is listed is displayed. An arrow next to a component name on the left indicates that component is being installed. A check mark next to a component name indicates that component is installed.
8. If the current component is IBM Global Security Kit, click **Install IBM Global Security Kit** to install it. When it completes, continue with step 9.
9. Click **Next**.
10. Respond to the prompts presented during the installation.
11. Click **Next** at the bottom of the Launchpad to continue.
12. Complete the installation.
    - If the installation fails, correct the error that is described in the error message and restart the Launchpad.
    - If the installation is successful, continue with step 13.
13. Click **Next** to start the configuration.

    Note: The configuration tool is displayed in the language that is selected for your operating system locale. If the tool is displayed in English and is not

displayed in the operating system locale, review the language pack installation log at %USERPROFILE%\ISAMLangPacksInstall.log. Correct any errors that are reported in the log file. Then, install the language pack as described in Appendix E, "Language support installation," on page 339.

14. Click **Configure Security Access Manager**. The configuration tool opens.
15. Select one or more components.
16. Click **Configure**.
17. Complete the configuration. For help completing the prompts, see Appendix D, "pdconfig options," on page 317. When all installations and configurations are completed, a success or failure message is displayed.
18. Take one of the following actions:
    - If the installation completed successfully, click **Next**.
    - If the installation failed or an error is displayed, review the log file in the default %USERPROFILE% location, such as C:\Users\Administrator\LaunchPDConfigforISAM.log. Make corrections or reinstall the policy server as indicated by the log file.
19. Click **Finish** to close the Launchpad.

Setting up a runtime server using script files

The installation and configuration scripts can automate installations and perform unattended (*silent*) installations and configurations.

Use the scripts in their original state or modify them to suit the requirements of your environment.

Automating the installation of a runtime system (AIX, Linux, or Solaris)

Use the script file to automate the installation of a runtime system.

About this task

Automated installations can perform unattended (*silent*) installations.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the install_isam.sh script file in the scripts directory.
3. Run the script as follows:

   ```
   install_isam.sh -i Runtime -d path_to_packages -a [accept|display]
   ```

   where

   - *path_to_packages* is the location of the component installation packages.

     For example, if you are installing from a DVD:

     AIX *dvd_mount_point*/usr/sys/inst.images

     Linux x86-64
     /mnt/dvd/linux_x86

     Linux on System z
     /linux_s390

Solaris

/dvd/*dvd0*/solaris

- `-a [accept|display]`

  The `-a accept` option automatically accepts the license without displaying the license. The `-a display` option displays the license and you must manually accept the license.

For example, if you are installing on Linux x86-64:

```
install_isam.sh -i Runtime -d /mnt/dvd/linux_x86 -a accept
```

The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.

4. Optional: To list the required packages without installing, use the `-l` option.

   ```
   install_isam.sh -l Runtime
   ```

What to do next

When the installation is completed, continue with "Automating the configuration of a runtime system" on page 179.

Automating the installation of a runtime system (Windows)

Use the script file to automate the installation of a runtime system on Windows.

About this task

Automated installations can perform unattended (*silent*) installations.

Attention: The installation script requires administrator privileges. Run the script file command, `install_isam.bat`, after you log in using an administrator ID or from a command window that you open with **Run as administrator**.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the `install_isam.bat` script file in the `scripts` directory. This directory is on the product DVD or in the directory where you extracted the product files. Ensure that the `.bat` file and all the `.iss` files are in the same directory.
3. Run the script as follows:

   ```
   install_isam.bat /i Runtime /d path_to_packages
   ```

   where :

   - *path_to_packages* is the path to the product DVD or the directory where you extracted the product files.
   - For example, to install the runtime component, type:

     ```
     install_isam.bat /i Runtime /d c:\isam_images
     ```

   where `c:\isam_images` is the directory where the extracted subdirectories and product files are located. The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.
4. Optional: To list the required packages without installing, use the `/l` option.

   ```
   install_isam.bat /l component
   ```

What to do next

When the installation is completed, continue with "Automating the configuration of a runtime system."

Automating the configuration of a runtime system

Use the script file to automate the configuration of a runtime system.

Before you begin

- Complete the installation of the runtime server. See:
  - "Automating the installation of a runtime system (AIX, Linux, or Solaris)" on page 177
  - "Automating the installation of a runtime system (Windows)" on page 178
- To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.

If you are running this script on Windows, open a new command window. Do not perform this task in the same window where you ran the installation script.

About this task

Automated configuration performs unattended (*silent*) configuration.

The script files and template files that are used in this task are installed in the following locations by default:

AIX, Linux, and Solaris: `/opt/PolicyDirector/example/config`

Windows: `C:\Program Files\Tivoli\Policy Director\example\config`

Procedure

1. Create an options file for the component you want to configure.
   a. Locate the options file template for the component. For the runtime for Java component, use the following template:

      AIX, Linux, or Solaris
      `configure_runtime.options.template`

      Windows
      `configure_runtime.options.template.cmd`

   b. Copy the file to a temporary directory. You can copy the file to the temporary directory with a name that is unique to your environment.

      Attention: You must keep the `.cmd` extension for Windows template files. The Windows template files run as commands.

   c. Modify the content of the file to specify settings for your environment. The comments in the file explain the settings and provide examples.
   d. Save the file.
2. Optional: By default, passwords you specified in the options files are stored in clear text. To obfuscate these passwords:
   a. On Windows, copy the `configure_isam.conf` file to the same directory where you copied the options files.

b. See Appendix F, "Password management," on page 351 for instructions on using the `-obfuscate` option with the `pdconf` tool to obfuscate the passwords in the options files. For more information about `pdconf`, see the *IBM Security Access Manager for Web Command Reference*.

c. Return to these instructions to run the configuration script.

3. Run the configuration script and use the options file for input.

   AIX, Linux, or Solaris

   ```
   configure_isam.sh -f options_file
   ```

   Windows

   ```
   configure_isam.cmd -f options_file.cmd
   ```

   where *options_file* and *options_file*`.cmd` are the text files that contain the configuration options.

   For example:

   AIX, Linux, or Solaris

   ```
   configure_isam.sh -f my_configure_runtime.options
   ```

   Windows

   ```
   configure_isam.cmd -f my_configure_runtime.options.cmd
   ```

Chapter 12. Setting up a Web Portal Manager system

The Security Access Manager Web Portal Manager is a web-based graphical user interface (GUI) used for Security Access Manager administration. The GUI counterpart to the **pdadmin** command-line interface, Web Portal Manager provides management of users, groups, roles, permissions, policies, and other Security Access Manager tasks. A key advantage of using Web Portal Manager is that you can complete these tasks remotely, without requiring any special network configuration.

Set up this system by following appropriate instructions for your operating system.

Before you begin, review the following information:

- If any IBM WebSphere Application Server patches or fix packs are applied that modify the `PD.jar` file, then you must also unconfigure and reconfigure IBM Security Access Manager Runtime for Java to use the `PD.jar` file that is shipped with Security Access Manager 7.0.
- If you reinstall or reconfigure the Security Access Manager policy server, you must also unconfigure and reconfigure the IBM Security Access Manager Runtime for Java component, which is a prerequisite component on a Web Portal Manager system.
- If you configure the Security Access Manager security standard in the `ssl-compliance` option to Suite B, NIST SP800-131, or FIPS, and not the default of "`none`," then during Web Portal Manager configuration, you must also configure WebSphere Application Server to enable the same security standard. If the security standard settings do not match, Web Portal Manager configuration fails. To enable the same security setting in WebSphere Application Server, see http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=%2Fcom.ibm.websphere.nd.multiplatform.doc%2Finfo%2Fae%2Fae%2Fcsec_security_standards.html

Setting up a Web Portal Manager system using the command line

Use platform-specific command-line utilities to install the Web Portal Manager. This method is one of several installation methods you can use.

For more information, see Chapter 2, “Installation methods,” on page 19.

When you use the command-line utilities, you must manually install each component and its prerequisite software in the appropriate order.

Complete the prerequisite installations first. See Part 2, “Prerequisite software installation,” on page 25.

The platform-specific installation utilities that are used are:

AIX **`installp`**

Linux **`rpm`**

Solaris
`pkgadd`

Note: Installations on Solaris systems should use the **-G** option with the **pkgadd** utility. The **-G** option adds the package into the current zone only. When the **-G** option is used in the global zone, the package is added to the global zone only and is not propagated to any existing or yet-to-be-created non-global zone. When used in a non-global zone, the package(s) are added to the non-global zone only.

Windows

```
setup.exe
```

After you complete the installation, use the appropriate configuration commands. For example, if the Security Access Manager Runtime component is installed on your system, you can use the **pdconfig** utility to configure Security Access Manager components and, if the Security Access Manager Runtime component is *not* installed, you can use component-specific utilities, such as **pdjrtecfg** to configure the IBM Security Access Manager Runtime for Java component or **amwpmcfg** to configure the Security Access Manager Web Portal Manager component.

Note: For more information about these utilities, see the *IBM Security Access Manager for Web Command Reference*.

AIX: Installing a Web Portal Manager system

Use **installp** to install software packages and the **pdjrtecfg** and **amwpmcfg** utilities to configure them on AIX.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

Procedure

1. Log on as **root**.
2. Ensure that the registry server and policy server are up and running (in normal mode).
3. Ensure that you have a supported Web browser that is installed on a system in your secure domain. See the *IBM Security Access Manager for Web Release Notes* for a list of supported browsers.
4. Ensure that IBM Java Runtime provided with Security Access Manager is installed. For instructions, see page "AIX: Installing IBM Java Runtime" on page 31.
5. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
6. Install IBM WebSphere Application Server. For instructions, see "Installing WebSphere Application Server" on page 46.
7. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
8. Install the Security Access Manager packages:

   ```
   installp -acgYXd package_path/usr/sys/inst.images packages
   ```

where:

- *package_path* is the directory where the DVD is mounted or the files are located
- *packages* are:

  PDJ.rte
  Specifies the IBM Security Access Manager Runtime for Java package.

  PD.WPM Specifies the Security Access Manager Web Portal Manager package.

Note: These packages must be installed on the same system as IBM WebSphere Application Server.

9. Unmount the DVD, if used.
10. Optional: You can use the IBM WebSphere Application Server **setupCmdLine** script to reset environment variables, including the location of IBM Java Runtime, before you configure IBM Security Access Manager Runtime for Java and Web Portal Manager.
    a. Run the **which java** command from the command line to show the default PATH settings that are used. For example, the command shows that Java is being run from the `/usr/bin/java` directory.
    b. To update the *PATH* environment variable and reset the *JAVA_HOME* variable, edit the `setupCmdLine.sh` file and change the environment variable as needed.
    c. Enter: `/opt/IBM/WebSphere/AppServer/bin/setupCmdLine.sh`
    d. Set the *JAVA_HOME* variable to the Java Runtime Environment that is configured for IBM Security Access Manager Runtime for Java. The *JAVA_HOME* variable should be set to the top directory. `/opt/IBM/WebSphere/AppServer/java`
11. To view status and messages for the IBM Security Access Manager Runtime for Java component in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
12. Configure the IBM Security Access Manager Runtime for Java component for use within the Java Runtime Environment that is installed with WebSphere. To do so, follow these steps:
    a. Stop the WebSphere Application Server and the IBM HTTP Server.
    b. Change to the `/opt/PolicyDirector/sbin` directory and enter the following command: `./pdjrtecfg -action config -interactive`
    c. Select the **Full** configuration type.
    d. Specify the Java Runtime Environment that is installed with IBM WebSphere Application Server. For example: `/usr/IBM/WebSphere/AppServer/java/jre`
    e. Specify the policy server host name, port, and domain. For more information about this utility, see the *IBM Security Access Manager for Web Command Reference*.
13. Restart the WebSphere Application Server and the IBM HTTP Server.
    To restart the WebSphere Application Server, run the **startServer.sh** script, in the `/opt/IBM/WebSphere/AppServer/bin` directory as follows:

    ```
    ./startServer.sh server1
    ```

    To restart the IBM HTTP Server, enter the following command:`/opt/IBM/HTTPServer/bin/apachectl restart` **Note:** If you installed a registry server

that does not use IBM HTTP Server *and* you are installing Web Portal Manager on the same system, ensure that the Web server ports are different. To change the IBM HTTP Server default port:

a. Edit the `/usr/HTTPServer/conf/httpd.conf` file.

b. Change default port `80` to an unused port, such as `8080`.

c. Restart the IBM HTTP Server.`# Port: The port the standalone listens to. Port 8080`

14. Configure the Security Access Manager Web Portal Manager package by running the **amwpmcfg** command, in the `/opt/PolicyDirector/sbin/` directory as follows: `./amwpmcfg -action config -interactive`.

    Specify the necessary configuration parameters, such as IBM WebSphere Application Server installation path, the policy server host name and port number, and the Security Access Manager administrator ID and password. For more information about this utility and all of its parameters, see the *IBM Security Access Manager for Web Command Reference*.

15. To access the Web Portal Manager interface, enter the following address in your Web browser: `http://`*`hostname`*`:`*`port`*`/ibm/console`
    where *hostname* is the host name of the system and port where IBM WebSphere Application Server is running, and *port* is the port number that is being used, such as `9060`. For example:`http://wpm14.example.com:9060/ibm/console`

What to do next

This step completes the setup of a Security Access Manager Web Portal Manager system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21. For information about Web Portal Manager administration tasks, see the *IBM Security Access Manager for Web Administration Guide*.

Note that Security Access Manager does not provide a default certificate to enable Web Portal Manager to have a secure connection between the browser and the HTTP server that is used by WebSphere Application Server. Purchase a CA certificate and then configure it into the Web Portal Manager environment.

Linux: Installing a Web Portal Manager system

Use **rpm** to install software packages and the **pdjrtecfg** and **amwpmcfg** utilities to configure them on Linux.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

Procedure

1. Log on as **root**.
2. Ensure that the registry server and policy server are up and running (in normal mode).
3. Ensure that you installed a supported Web browser on a system in your secure domain. See the *IBM Security Access Manager for Web Release Notes* for a list of supported browsers.

4. Ensure that IBM Java Runtime provided with Security Access Manager is installed. For instructions, see page "Linux: Installing IBM Java Runtime" on page 32.

   Note: If you configure Web Portal Manager against Java Runtime Environments other than the Java Runtime Environment supported by Security Access Manager, the configuration might fail.
5. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
6. Install IBM WebSphere Application Server. For instructions, see "Installing WebSphere Application Server" on page 46.
7. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
8. Change to the *package_path*/*distribution* directory

   where:

   - *package_path* is the mount point for your DVD or file location.
   - *distribution* specifies `linux_x86` for x86-64 or `linux_s390` for System z.
9. Install the Security Access Manager packages:

   `rpm -ihv package`

   where *package* is:

	Linux on x86-64	Linux on System z
IBM Security Access Manager Runtime for Java package	`PDJrte-PD-7.0.0-0.x86_64.rpm`	`PDJrte-PD-7.0.0-0.s390.rpm`
Security Access Manager Web Portal Manager package	`PDWPM-PD-7.0.0-0.x86_64.rpm`	`PDWPM-PD-7.0.0-0.s390.rpm`

   Note: These packages must be installed on the same system as IBM WebSphere Application Server.
10. Unmount the DVD, if used.
11. Optional: You can use the IBM WebSphere **setupCmdLine** script to reset environment variables, including the location of the Java Runtime Environment, before you configure IBM Security Access Manager Runtime for Java and Web Portal Manager.
    a. Run the **which java** command from the command line to show the default PATH settings that are used. For example, the command shows that Java is being run from the `/usr/bin/java` directory.
    b. To update the *PATH* environment variable and reset the *JAVA_HOME* variable, edit the `setupCmdLine.sh` file and change the environment variable as needed.
    c. Enter: `. /opt/IBM/WebSphere/AppServer/bin/setupCmdLine.sh`
    Set the *JAVA_HOME* variable to the Java Runtime Environment that is configured for IBM Security Access Manager Runtime for Java. The *JAVA_HOME* variable should be set to the top directory. `/opt/WebSphere/AppServer/java`
12. To view the status and messages for the IBM Security Access Manager Runtime for Java component in a language other than English, which is the

default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.

13. Configure the IBM Security Access Manager Runtime for Java component for use within the Java Runtime Environment that is installed with WebSphere. To do so, follow these steps:
    a. Stop the WebSphere Application Server and the IBM HTTP Server.
    b. Change to the `/opt/PolicyDirector/sbin` directory and enter the following command:
       ```
       ./pdjrtecfg -action config -interactive
       ```
    c. Select the **Full** configuration type.
    d. Specify the Java Runtime Environment that is installed with IBM WebSphere Application Server. For example:
       ```
       /opt/WebSphere/AppServer/java/jre
       ```
    e. Specify the policy server host name, port, and domain.
       For more information about this utility, see the *IBM Security Access Manager for Web Command Reference*.
14. Restart the WebSphere Application Server and the IBM HTTP Server.
    To restart the IBM WebSphere Application Server, run the **startServer.sh** script, in the `/opt/IBM/WebSphere/AppServer/bin` directory as follows:
    ```
    ./stopServer.sh server1 ./startServer.sh server1
    ```

    To restart the IBM HTTP Server, enter the following command:`/opt/IBM/HTTPServer/bin/apachectl restart`

    Note: If you installed a registry server that does not use IBM HTTP Server *and* you are installing Web Portal Manager on the same system, ensure that the Web server ports are different. To change the IBM HTTP Server default port, edit the `/opt/IBMHTTPServer/conf/httpd.conf` file, change default port `80` to `8080` as shown, and then restart the IBM HTTP Server.`# Port: The port the standalone listens to. Port 8080`
15. Configure the Security Access Manager Web Portal Manager package by running the **amwpmcfg** command, in the `/opt/PolicyDirector/sbin/` directory as follows:
    ```
    ./amwpmcfg -action config -interactive
    ```

    Specify the necessary configuration parameters, such as IBM WebSphere Application Server installation path, the policy server host name and port number, and the Security Access Manager administrator ID and password. For more information about this utility and all of its parameters, see *IBM Security Access Manager for Web Command Reference*.
16. To access the Web Portal Manager interface, enter the following address in your Web browser: `http://`*`hostname`*`:`*`port`*`/ibm/console`
    where *hostname* is the host name of the system and port where IBM WebSphere Application Server is running, and *port* is the port number that is used, such as `9060`. For example:
    ```
    http://wpm14.example.com:9060/ibm/console
    ```

What to do next

This step completes the setup of a Security Access Manager Web Portal Manager system. To set up another Security Access Manager system, follow the steps in the

Chapter 3, “Installation roadmap,” on page 21. For information about Web Portal Manager administration tasks, see the *IBM Security Access Manager for Web Administration Guide*.

Note that Security Access Manager does not provide a default certificate to enable Web Portal Manager to have a secure connection between the browser and the HTTP server that is used by WebSphere Application Server. Purchase a CA certificate and then configure it into the Web Portal Manager environment.

Solaris: Installing a Web Portal Manager system

Use **pkgadd** to install software packages and the **pdjrtecfg** and **amwpmcfg** utilities to configure them on Solaris.

Before you begin

Complete the appropriate preinstallation tasks in:

- “Operating system preparation” on page 28.
- Chapter 4, “Prerequisite installation and configuration roadmap,” on page 27

About this task

Attention: Installations on Solaris systems should use the **-G** option with the **pkgadd** utility. The **-G** option adds the package into the current zone only.

Procedure

1. Log on as **root**.
2. Ensure that the registry server and policy server are up and running (in normal mode).
3. Ensure that you installed a supported Web browser on a system in your secure domain. See the *IBM Security Access Manager for Web Release Notes* for a list of supported browsers.
4. Ensure that IBM Java Runtime provided with Security Access Manager is installed. For instructions, see page “Solaris: Installing IBM Java Runtime” on page 33.
5. Install the IBM Security Access Manager License, if not already installed. For instructions, see “AIX, Linux, Solaris: Installing the IBM Security Access Manager License” on page 37.
6. Install IBM WebSphere Application Server. For instructions, see “Installing WebSphere Application Server” on page 46.
7. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
8. Install the Security Access Manager packages, one at a time:

   ```
   pkgadd -d /package_path/solaris
     -a /package_path/solaris/pddefault -G packages
   ```

   where:

   /*package_path*/solaris
   : Specifies the location of the package.

   /*package_path*/solaris/pddefault
   : Specifies the location of the installation administration script.

and where *packages* are:

PDJrte Specifies the IBM Security Access Manager Runtime for Java package.

PDWPM Specifies the Security Access Manager Web Portal Manager package.

Note: These packages must be installed on the same system as IBM WebSphere Application Server.

9. Optional: You can use the IBM WebSphere **setupCmdLine** script to reset environment variables, including the location of the Java Runtime Environment, before you configure IBM Security Access Manager Runtime for Java and Web Portal Manager.
   a. Run the **which java** command from the command line to show the default PATH settings that are used. For example, the command shows that Java is being run from the `/usr/bin/java` directory.
   b. To update the *PATH* environment variable and reset the *JAVA_HOME* variable, edit the `setupCmdLine.sh` file and change the environment variable as needed.
   c. Enter:

      ```
      ./opt/IBM/WebSphere/AppServer/bin/setupCmdLine.sh
      ```

      Set the *JAVA_HOME* variable to the Java Runtime Environment that is configured for IBM Security Access Manager Runtime for Java. The *JAVA_HOME* variable should be set to the top directory.

      ```
      /opt/WebSphere/AppServer/java
      ```
10. To view status and messages for the IBM Security Access Manager Runtime for Java component in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
11. Configure the IBM Security Access Manager Runtime for Java component for use within the Java Runtime Environment that is installed with WebSphere. To do so, follow these steps:
    a. Stop the WebSphere Application Server and the IBM HTTP Server.
    b. Change to the `/opt/PolicyDirector/sbin` directory and enter the following command:

       ```
       ./pdjrtecfg -action config -interactive
       ```
    c. Select the **Full** configuration type.
    d. Specify the Java Runtime Environment that is installed with IBM WebSphere Application Server. For example:

       ```
       /opt/WebSphere/AppServer/java/jre
       ```
    e. Specify the policy server host name, port, and domain.

       For more information about this utility, see *IBM Security Access Manager for Web Command Reference*.
12. Restart the WebSphere Application Server and the IBM HTTP Server. To restart the WebSphere Application Server, run the **startServer.sh** script, in the `/opt/WebSphere/AppServer/bin` directory as follows:

    ```
    ./stopServer.sh server1
    ./startServer.sh server1
    ```

    To restart the IBM HTTP Server, enter the following command:

    ```
    /opt/IBMHTTPServer/bin/apachectl restart
    ```

Note: If you installed a registry server that does not use IBM HTTP Server *and* you are installing Web Portal Manager on the same system, ensure that the Web server ports are different. To change the IBM HTTP Server default port, edit the `/opt/IBMHTTPServer/conf/httpd.conf` file, change default port `80` to `8080` as shown, and then restart the IBM HTTP Server.

```
# Port: The port the standalone listens to.
Port 8080
```

13. Configure the Security Access Manager Web Portal Manager package:

    ```
    ./amwpmcfg -action config -interactive
    ```

    Specify the necessary configuration parameters, such as IBM WebSphere Application Server installation path, the policy server host name and port number, and the Security Access Manager administrator ID and password.

    For more information about this utility and all of its parameters, see the *IBM Security Access Manager for Web Command Reference*.

14. To access the Web Portal Manager interface, enter the following address in your Web browser:

    `http://`*`hostname`*`:`*`port`*`/ibm/console`

    where *hostname* is the host name of the system and port where IBM WebSphere Application Server is running, and *port* is the port number that is used, such as `9060`. For example:

    ```
    http://wpm14.example.com:9060/ibm/console
    ```

What to do next

This step completes the setup of a Security Access Manager Web Portal Manager system. To set up another Security Access Manager system, follow the steps in the Chapter 3, “Installation roadmap,” on page 21. For information about Web Portal Manager administration tasks, see the *IBM Security Access Manager for Web Administration Guide*.

Note that Security Access Manager does not provide a default certificate to enable Web Portal Manager to have a secure connection between the browser and the HTTP server that is used by WebSphere Application Server. Purchase a CA certificate and then configure it into the Web Portal Manager environment.

Windows: Installing a Web Portal Manager system

Use **`setup.exe`** to install software packages and the **`pdjrtecfg`** and **`amwpmcfg`** utilities to configure them on Windows.

Before you begin

Complete the appropriate preinstallation tasks in:

- “Operating system preparation” on page 28.
- Chapter 4, “Prerequisite installation and configuration roadmap,” on page 27

Procedure

1. Log on as any member of the Administrators group.
2. Ensure that the registry server and policy server are up and running (in normal mode).
3. Ensure that you installed a supported Web browser on a system in your secure domain. See the *IBM Security Access Manager for Web Release Notes* for a list of supported browsers.

4. Ensure that IBM Java Runtime provided with Security Access Manager is installed. For instructions, see page "Windows: Installing IBM Java Runtime" on page 34.
5. Install IBM WebSphere Application Server. See "Installing WebSphere Application Server" on page 46.
6. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
7. Install the Security Access Manager license, if not already installed. For instructions, see "Windows: Installing the IBM Security Access Manager License" on page 39.
8. Install the Security Access Manager packages. To do so, run the **setup.exe** file in the following directory:

   `\windows\PolicyDirector\Disk Images\Disk1`

   Follow the online instructions and select to install the following packages:
   - IBM Security Access Manager Runtime for Java
   - Security Access Manager Web Portal Manager

   Note: These packages must be installed on the same system as IBM WebSphere Application Server.
9. Optional: You can use the IBM WebSphere **setupCmdLine** script to reset environment variables, including the location of the Java Runtime Environment, before you configure IBM Security Access Manager Runtime for Java and Web Portal Manager.
   a. Run the **which java** command from the command line to show the default PATH settings that are used. For example, the command shows that Java is being run from the `C:\Program Files\IBM\WebSphere\AppServer\java` directory.
   b. To update the *PATH* environment variable and reset the *JAVA_HOME* variable, edit the `setupCmdLine.bat` file and change the environment variable as needed.
   c. Enter:

      `C:\Program Files\IBM\WebSphere\AppServer\bin\setupCmdLine.bat`

      Set the *JAVA_HOME* variable to the Java Runtime Environment that is configured for IBM Security Access Manager Runtime for Java. The *JAVA_HOME* variable should be set to the top directory.

      `C:\Program Files\IBM\WebSphere\AppServer\java`
10. To view the status and messages for the IBM Security Access Manager Runtime for Java component in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
11. Configure the IBM Security Access Manager Runtime for Java component for use within the Java Runtime Environment that is installed with WebSphere. To do so, follow these steps:
    a. Stop the WebSphere Application Server and the IBM HTTP Server.
    b. Change to the *install_dir*`\sbin` directory (for example, `C:\Program Files\Tivoli\Policy Director\sbin`), and enter the following command:

       `pdjrtecfg -action config -interactive`
    c. Select the **Full** configuration type.

d. Click **Next**. For descriptions of the configuration options, click **Help**.
e. Specify the Java Runtime Environment that is installed with IBM WebSphere Application Server. For example:
```
C:\Program Files\IBM\WebSphere\AppServer\java\jre
```
f. Click **Next** to continue.
g. Specify the policy server host name, port, and domain.
h. Click **OK** to start configuration.
i. When configuration completes successfully, click **OK** to exit the configuration utility.
For more information about this utility, see the *IBM Security Access Manager for Web Command Reference*.

12. Restart the IBM WebSphere Application Server and IBM HTTP Server. For example, select **Start → Settings → Control Panel → Administrative Tools** and then double-click the **Services** icon to restart these servers.

    Note: If you installed a registry server that does not use IBM HTTP Server *and* you are installing Web Portal Manager on the same system, ensure that the Web server ports are different. To change the IBM HTTP Server default port, edit the `C:\Program Files\IBMHTTPServer\conf\httpd.conf` file, change default port `80` to `8080` as shown, and then restart the IBM HTTP Server.
    ```
    # Port: The port the standalone listens to. Port 8080
    ```
13. Configure the Security Access Manager Web Portal Manager package. To do so, follow these steps:
    a. Change to the *install_dir*`\sbin` directory (for example, `C:\Program Files\Tivoli\Policy Director\sbin`), and enter the following command:
    ```
    amwpmcfg -action config -interactive
    ```
    Specify the necessary configuration parameters, such as IBM WebSphere Application Server installation path, the policy server host name and port number, and the Security Access Manager administrator ID and password. For more information about this utility and all of its parameters, see *IBM Security Access Manager for Web Command Reference*.
    b. When configuration completes successfully, click **OK** to exit the configuration utility.
14. To access the Web Portal Manager interface, enter the following address in your Web browser: `http://`*hostname*`:`*port*`/ibm/console`
    where *hostname* is the host name of the system and port where IBM WebSphere Application Server is running, and *port* is the port number that is used, such as `9060`. For example:
    ```
    http://wpm14.example.com:9060/ibm/console
    ```

What to do next

This step completes the setup of a Security Access Manager Web Portal Manager system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21. For information about Web Portal Manager administration tasks, see the *IBM Security Access Manager for Web Administration Guide*.

Note that Security Access Manager does not provide a default certificate to enable Web Portal Manager to have a secure connection between the browser and the HTTP server that is used by WebSphere Application Server. Purchase a CA certificate and then configure it into the Web Portal Manager environment.

Setting up a Web Portal Manager system using the Launchpad (Windows)

Use the Launchpad installation method to install and configure a Web Portal Manager and its prerequisite software on Windows by using a graphical user interface.

Before you begin

Ensure that you completed the following prerequisite tasks:

- "Operating system preparation" on page 28
- Chapter 5, "User registry server installation and configuration," on page 51
- Web Portal Manager requires a supported version of IBM WebSphere Application Server. Use the version that is provided with IBM Security Access Manager or see the Release Information in the IBM Security Access Manager information center for a list of supported versions.

About this task

The Launchpad uses a graphical user interface to perform step-by-step installation and initial configuration.

This task installs the following components:

- IBM WebSphere Application Server, including IBM Installation Manager (if it is not already installed)
- Security Access Manager License
- Security Access Manager Runtime for Java
- Security Access Manager Web Portal Manager

If a supported version of WebSphere Application Server is already installed, you can skip its installation during this procedure and continue with the installation of the remaining components.

Attention: If WebSphere Application Server is already installed, ensure that Java is specified in your PATH environment variable before you run the Launchpad. For example, type:

```
set Path=c:\Program Files\IBM\Java60\jre\bin;%Path%
```

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage. You need the files for the following products:
   - WebSphere Application Server
   - Installation Manager
   - IBM Security Access Manager

   Attention: Ensure that the image files are in a directory path that does not contain any spaces.
2. Start the Launchpad in the IBM Security Access Manager files.
   a. Locate the `launchpad64.exe` file.
   b. Double-click the file to start the Launchpad.
3. Select the language that you want to use during the installation.

4. Click **OK**. The Launchpad Welcome window opens.
5. Click **Next**.
6. Select the **Web Portal Manager** component.
7. Click **Next**. The list on the left displays the component that you selected and any prerequisite software that is required by that component but that is not already installed.
8. Install WebSphere Application Server or if WebSphere Application Server is already installed, click **Next**. To install WebSphere Application Server:
   a. Click **Install WebSphere Application Server Components** to install WebSphere Application Server.
   b. Select the path to the IBM Installation Manager image.

      Note: The path to the Installation Manager image is restricted in length to 172 characters or less.
   c. Click **OK**.

      Note: After Installation Manager is installed, there is a 30-second delay before it opens and begins the WebSphere Application Server installation.
   d. In the Installation Manager console, click **Install** to begin the WebSphere Application Server installation.
   e. Click **File** > **Preferences**.
   f. Select **Repositories**.
   g. Click **Add Repository**.
   h. Select the location of the `repository.config` file in the WebSphere Application Server image.
   i. Click **OK**.
   j. Click **Install**. Complete the installation as prompted. The default selections that are provided by the IBM WebSphere Application Server installation program are sufficient for IBM Security Access Manager. At the end of the installation, a list of the installed package and a prompt for program to start is displayed.
      - If the installation is successful, a list of the installed packages and a prompt for starting the Profile Management Tool is displayed. Continue with 8k.
      - If the installation of Installation Manager or WebSphere Application Server fails or an error is displayed, review the log files and complete the actions that they indicate. The files are in the default `%USERPROFILE%` location, such as `C:\Users\Administrator\`.

        Installation Manager logs

        `IMInstall.log`

        `IMInstallLog.xml`

        WebSphere Application Server installation log

        `LaunchIMforWAS.log`
   k. Select the **Profile Management Tool** to create a profile.
   l. Click **Finish**. The WebSphere Customization Toolbox opens the Profile Management Tool.
   m. In the Profile Management Tool, click **Create**.
   n. Start the First Steps tool and click **Start the server**. The `open for e-business` message is displayed.

o. Close the following windows:
   - First Steps
   - WebSphere Customization Toolbox

p. Install the latest fix pack for your installation. See the hardware and software requirements page of the IBM Security Access Manager information center for the minimum fix pack level required.

q. Locate the fix pack on the WebSphere Application Server web-based repository or download the package and install it from a local repository.
   - To install it from the web-based repository:
     1) Click **Update** on the IBM Installation Manager window.
     2) Select **IBM WebSphere Application Server Network Deployment V8.0**.
     3) Click **Next**. Continue with the installation.
   - To install it from a local repository:
     1) Locate the fix pack on the WebSphere Application Server Support page: http://www.ibm.com/support/docview.wss?uid=swg27004980
     2) Download the fix pack into a local repository.
     3) Click **Update**.
     4) Select **IBM WebSphere Application Server Network Deployment V8.0**.
     5) Click **Next**. Continue with the installation. Use the accompanying readme file from the WebSphere Application Server Support page for assistance.

r. Start the IBM WebSphere Application Server.
   1) Click **Start** > **Administrative Tools** > **Services**.
   2) Select the IBM WebSphere Application Server that was added.
   3) Right-click the service and click **Start**.

s. Close the IBM Installation Manager window.

t. Return to the Launchpad window.

9. Click **Next**. The installation panel for the next component displays. An arrow next to a component name on the left indicates that component is being installed. A check mark next to a component name indicates that component is installed.
10. Click **Next**. The installation of the first component begins.
11. Respond to the prompts presented during the installation.
12. Click **Next** at the bottom of the Launchpad to continue.
13. Complete the installation.
    - If the installation fails, correct the error that is described in the error message and restart the Launchpad.
    - If the installation is successful, continue with step 14.
14. Click **Next** to start the configuration.

    Note: The configuration tool is displayed in the language that is selected for your operating system locale. If the tool is displayed in English and is not displayed in the operating system locale, review the language pack installation log at `%USERPROFILE%\ISAMLangPacksInstall.log`. Correct any errors that are reported in the log file. Then, install the language pack as described in Appendix E, "Language support installation," on page 339.
15. Click **Configure Java Runtime**.

16. Specify the location of the WebSphere Application Server Java. For example, specify:

    ```
    C:\Program Files (x86)\IBM\WebSphere\AppServer\java\jre
    ```

17. Click **Next**.
18. Click **Configure Web Portal Manager**.
19. Complete the configuration. For help completing the prompts, see "Security Access Manager Web Portal Manager" on page 333. When all installations and configurations are completed, a success or failure message is displayed.
20. Click **OK**.
21. Take one of the following actions:
    - If the installation and configuration completed successfully, click **Next**.
    - If the installation or configuration failed or an error is displayed, review the log files in the default `%USERPROFILE%` location:

      Installation Manager

      `IMInstall.log`

      `IMInstallLog.xml`

      Installation of WebSphere Application Server

      `LaunchIMforWAS.log`

      Configuration of WebSphere Application Server

      `ConfigJRTEforWAS.log`

      Configuration of Web Portal Manager

      `ConfigAMWPM.log`

      Make corrections or reinstall the component as indicated by the log file. See the *IBM Security Access Manager for Web Troubleshooting Guide* for assistance.
22. Click **Finish** to close the Launchpad.

Setting up a Web Portal Manager using script files

The installation and configuration scripts can automate installations and perform unattended (*silent*) installations and configurations.

Use the scripts in their original state or modify them to suit the requirements of your environment.

Web Portal Manager requires WebSphere Application Server. If WebSphere Application Server is not already installed, install and configure it using either of the following methods:

- "Installing WebSphere Application Server" on page 46 to manually install and configure it.
- "Setting up WebSphere Application Server using script files" to automate its installation and configuration.

Setting up WebSphere Application Server using script files

The installation and configuration scripts can automate installations and perform unattended (*silent*) installations and configurations.

Use the scripts in their original state or modify them to suit the requirements of your environment.

Automating the installation of WebSphere Application Server (AIX, Linux, or Solaris)

Use the script file to automate the installation of WebSphere Application Server on AIX, Linux, or Solaris.

About this task

Automated installations can perform unattended (*silent*) installations. WebSphere Application Server is a prerequisite product for the following components:

- Web Portal Manager
- Attribute Retrieval Service
- Session Management Server

Installation Manager is required to install WebSphere Application Server.

Procedure

1. Obtain the WebSphere Application Server installation files and product repository from any of the following locations:
   - The WebSphere Application Server product media provided with the Security Access Manager DVDs.
   - The Passport Advantage site.
2. Copy the WebSphere Application Server files onto the computer where you want to install WebSphere Application Server.
3. Extract all the WebSphere Application Server files from their compressed files into one directory.
4. Obtain Installation Manager from any of the following locations:
   - The Passport Advantage site.
   - The IBM Installation Manager download web site:

     http://www.ibm.com/support/entry/portal/All_download_links/Software/Rational/IBM_Installation_Manager
5. Copy the Installation Manager files onto the computer where you want to install WebSphere Application Server.
6. Extract the Installation Manager files into its own directory.
7. Copy the `install_was.sh` from the `scripts` directory on the Security Access Manager product media to a temporary location on the computer where you want to install WebSphere Application Server.
8. Copy the appropriate `WASInstall_*.xml` file for your platform from the `scripts` directory on the Security Access Manager product media to the same temporary location where you copied the `install_was.sh` file. The response files are:

   Linux x86-64
   `WASInstall_linux_x86.xml`

   Linux s390
   `WASInstall_linux_s390x.xml`

   AIX `WASInstall_aix_ppc.xml`

   Solaris
   `WASInstall_solaris_sparc.xml`
9. Open the copy of the `install_was.sh` by using a text editor.

10. Modify the Installation Manager path in the `install_was.sh` file to specify where the Installation Manager images are located. For example, change the following line:

    ```
    INSTALL_MGR_DIR=/images/InstallationManager
    ```

11. Modify the `WAS_RESPONSE_FILE` variable to specify the name of the response file to use when you run the script. Use the name of the appropriate response file for your platform:

    Linux x86-64
    `WASInstall_linux_x86.xml`

    Linux s390
    `WASInstall_linux_s390x.xml`

    AIX `WASInstall_aix_ppc.xml`

    Solaris
    `WASInstall_solaris_sparc.xml`

    For example, on Linux for x86-64, specify:

    ```
    WAS_RESPONSE_FILE=./WASInstall_linux_x86.xml
    ```

12. Save and close the file.
13. Open the copy of the `WASInstall_*.xml` file by using a text editor.
14. Modify the repository location path in the `WASInstall_*.xml` file where your WebSphere Application Server images are located. For example, change the following line:

    ```
    <repository location='/images/WebSphere'/>
    ```

15. Optional: Modify the location where WebSphere Application Server is installed by the script. The default installation locations are:

    Linux or Solaris
    `/opt/IBM/WebSphere/AppServer`

    AIX `/usr/IBM/WebSphere/AppServer`

    To change the location, change the following lines in the `WASInstall_*.xml` file:

    ```
    <profile id='IBM WebSphere Application Server Network Deployment V8.0'
       installLocation='/opt/IBM/WebSphere/AppServer'>
    <data key='eclipseLocation' value='/opt/IBM/WebSphere/AppServer'/>
    ```

16. Save the response file.
17. Run the script file.

    ```
    install_was.sh
    ```

    Attention: If you specify a repository file name incorrectly in step 14, an error is displayed. Repeat the modification instructions in step 14 to correct the repository file name. Then, remove the incorrect repository from Installation Manager before running the script again:

    a. On a command line, change directory to the installation directory for Installation Manager:

       ```
       /opt/IBM/InstallationManager/eclipse
       ```

    b. Run `IBMIM`.
    c. Remove the incorrect repository.
    d. Rerun the script.

18. After the installation of WebSphere Application Server is completed, create an Application Server profile by using the WebSphere Application Server **`manageprofiles`** command.

For example, type:

```
/opt/IBM/WebSphere/AppServer/bin/manageprofiles.sh -create -templatePath
/opt/IBM/WebSphere/AppServer/profileTemplates/default
```

For details about the **manageprofiles** command, see the WebSphere Application Server Information Center:

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp

19. Start the application server.

    For example, type:

    ```
    /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin/startServer.sh server1
    ```

20. Install the latest fix pack for your installation. See the hardware and software requirements page of the IBM Security Access Manager information center for the minimum fix pack level required.
    a. Locate the fix pack on the WebSphere Application Server Support page. http://www.ibm.com/support/docview.wss?uid=swg27004980
    b. Download the fix pack and use the instructions in the accompanying readme to install it.

What to do next

Continue with "Automating the installation of a Web Portal Manager system (AIX, Linux, or Solaris)" on page 200.

Automating the installation of WebSphere Application Server (Windows)

Use the script file to automate the installation of WebSphere Application Server on Windows.

Before you begin

Attention: The installation script requires administrator privileges. Run the script file command, `install_was.bat`, after you log in by using an administrator ID or from a command window that you open with **Run as administrator**.

About this task

Automated installations can perform unattended (*silent*) installations. WebSphere Application Server is a prerequisite product for the following components:

- Web Portal Manager
- Attribute Retrieval Service
- Session Management Server

Installation Manager is required to install WebSphere Application Server.

Procedure

1. Obtain the WebSphere Application Server installation files and product repository from any of the following locations:
   - The WebSphere Application Server product media provided with the Security Access Manager DVDs.
   - The Passport Advantage site.
2. Copy the WebSphere Application Server files onto the computer where you want to install WebSphere Application Server.

3. Extract all the WebSphere Application Server files from their compressed files into one directory.
4. Obtain Installation Manager from any of the following locations:
   - The Passport Advantage site.
   - The IBM Installation Manager download web site:

     http://www.ibm.com/support/entry/portal/All_download_links/Software/Rational/IBM_Installation_Manager
5. Copy the Installation Manager files onto the computer where you want to install WebSphere Application Server.
6. Extract the Installation Manager files into its own directory.
7. Copy the `install_was.bat` from the `scripts` directory of the Security Access Manager product media to a temporary location on the computer where you want to install WebSphere Application Server.
8. Copy the `WASInstall.xml` file from the `scripts` directory of the Security Access Manager product media to the same temporary location where you copied the `install_was.bat` file.
9. Open the copy of the `install_was.bat` by using a text editor.
10. Modify the Installation Manager path in the `install_was.bat` file to specify where the Installation Manager images are located. For example, change the following line:

    ```
    set INSTALL_MGR_DIR=C:\images\Installation Manager
    ```
11. Save and close the file.
12. Open the copy of `WASInstall.xml` file by using a text editor.
13. Modify the repository location path in the `WASInstall.xml` file where your WebSphere Application Server images are located. For example, change the following line:

    ```
    <repository location='C:\images\WebSphere'/>
    ```
14. Optional: Modify the location where WebSphere Application Server is installed by the script. For example, change the following lines:

    ```
    <profile id='IBM WebSphere Application Server Network Deployment V8.0'
      installLocation='C:\Program Files\IBM\WebSphere\AppServer'/>
    <data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere\AppServer'/>
    ```
15. Run the script file.

    ```
    install_was.bat
    ```
16. After the installation of WebSphere Application Server is completed, create an Application Server profile by using the WebSphere Application Server **manageprofiles** command.

    For example, type:

    ```
    C:\Program Files\IBM\WebSphere\AppServer\bin\manageprofiles.bat -create
      -templatePath "C:\Program Files\IBM\WebSphere\AppServer\
       profileTemplates\default"
    ```

    For details about the **manageprofiles** command, see the WebSphere Application Server Information Center:

    http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp
17. Start the application server.

    For example, type:

    ```
    C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\bin\
    startServer.bat server1
    ```

18. Install the latest fix pack for your installation. See the hardware and software requirements page of the IBM Security Access Manager information center for the minimum fix pack level required.
    a. Locate the fix pack on the WebSphere Application Server Support page. http://www.ibm.com/support/docview.wss?uid=swg27004980
    b. Download the fix pack and use the instructions in the accompanying readme to install it.

What to do next

Continue with "Automating the installation of a Web Portal Manager (Windows)" on page 201.

Automating the installation of a Web Portal Manager system (AIX, Linux, or Solaris)

Use the script file to automate the installation of a Web Portal Manager system.

Before you begin

Ensure that WebSphere Application Server is installed and configured.

- "Installing WebSphere Application Server" on page 46 to manually install and configure it.
- "Setting up WebSphere Application Server using script files" on page 195 to automate its installation and configuration.

About this task

Automated installations can perform unattended (*silent*) installations.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the `install_isam.sh` script file in the `scripts` directory.
3. Run the script as follows:

   ```
   ./install_isam.sh -i WPM -d path_to_packages -a [accept|display]
   ```

   where

   - *path_to_packages* is the location of the component installation packages.

     For example, if you are installing from a DVD:

     AIX *dvd_mount_point*`/usr/sys/inst.images`

     Linux x86-64
     `/mnt/dvd/linux_x86`

     Linux on System z
     `/linux_s390`

     Solaris
     `/dvd/`*dvd0*`/solaris`
   - `-a [accept|display]`

     The `-a accept` option automatically accepts the license without displaying the license. The `-a display` option displays the license and you must manually accept the license.

For example, if you are installing on Linux x86-64:

```
./install_isam.sh -i WPM -d /mnt/dvd/linux_x86 -a accept
```

The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.

4. Optional: To list the required packages without installing, use the `-l` option.

```
./install_isam.sh -l WPM
```

What to do next

When the installation is completed, continue with "Automating the configuration of Web Portal Manager" on page 202.

Automating the installation of a Web Portal Manager (Windows)

Use the script file to automate the installation of a Web Portal Manager system on Windows.

Before you begin

Web Portal Manager requires WebSphere Application Server. Before you begin this task, install and configure WebSphere Application Server, if it is not already installed:

- "Installing WebSphere Application Server" on page 46 to manually install and configure it.
- "Automating the installation of WebSphere Application Server (Windows)" on page 198 to automate its installation and configuration.

About this task

Automated installations can perform unattended (*silent*) installations.

Attention: The installation script requires administrator privileges. Run the script file command, `install_isam.bat`, after you log in using an administrator ID or from a command window that you open with **Run as administrator**.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the `install_isam.bat` file in the `scripts` directory. This directory is on the product DVD or in the directory where you extracted the product files. Ensure that the `.bat` file and all the `.iss` files are in the same directory.
3. Run the script as follows:

```
install_isam.bat /i WPM /d path_to_packages
```

where:

- `WPM` is the name of the Web Portal Manager component.
- *`path_to_packages`* is the path to the product DVD or the directory where you extracted the product files.

For example, to install the Web Portal Manager component, type:

```
install_isam.bat /i WPM /d c:\isam_images
```

where `c:\isam_images` is the directory where the extracted subdirectories and product files are located. The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.

4. Optional: To list the required packages without installing, use the /l option.

```
install_isam.bat /l WPM
```

What to do next

When the installation is completed, continue with "Automating the configuration of Web Portal Manager."

Automating the configuration of Web Portal Manager

Use the script file to automate the configuration of Web Portal Manager.

Before you begin

- Complete the installation of the Web Portal Manager. See:
  - "Automating the installation of a Web Portal Manager system (AIX, Linux, or Solaris)" on page 200
  - "Automating the installation of a Web Portal Manager (Windows)" on page 201
- To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.

If you are running this script on Windows, open a new command window. Do not perform this task in the same window where you ran the installation script.

About this task

Automated configuration performs unattended (*silent*) configuration.

The script files and template files that are used in this task are installed in the following locations by default:

AIX, Linux, and Solaris: `/opt/PolicyDirector/example/config`

Windows: `C:\Program Files\Tivoli\Policy Director\example\config`

Procedure

1. Create an options file for the component you want to configure.
   a. Locate the options file template for the component. For the runtime for Java component, use the following template:

      AIX, Linux, or Solaris

      ```
      configure_wpm.options.template
      ```

      Windows

      ```
      configure_wpm.options.template.cmd
      ```

   b. Copy the file to a temporary directory. You can copy the file to the temporary directory with a name that is unique to your environment.

      Attention: You must keep the `.cmd` extension for Windows template files. The Windows template files run as commands.

c. Modify the content of the file to specify settings for your environment. The comments in the file explain the settings and provide examples.
d. Save the file.

2. Optional: By default, passwords you specified in the options files are stored in clear text. To obfuscate these passwords:
   a. On Windows, copy the `configure_isam.conf` file to the same directory where you copied the options files.
   b. See Appendix F, "Password management," on page 351 for instructions on using the `-obfuscate` option with the `pdconf` tool to obfuscate the passwords in the options files. For more information about `pdconf`, see the *IBM Security Access Manager for Web Command Reference*.
   c. Return to these instructions to run the configuration script.
3. Run the configuration script and use the options file for input.

   AIX, Linux, or Solaris

   ```
   ./configure_isam.sh -f options_file
   ```

   Windows

   ```
   configure_isam.cmd -f options_file.cmd
   ```

   where *options_file* and *options_file*`.cmd` are the text files that contain the configuration options.

   For example:

   AIX, Linux, or Solaris

   ```
   ./configure_isam.sh -f my_configure_wpm.options
   ```

   Windows

   ```
   configure_isam.cmd -f my_configure_wpm.options.cmd
   ```

Configuring WebSphere Application Server security

You must configure the WebSphere Application Server security settings so that the Web Portal Manager single sign-on works properly.

Procedure

1. To start the IBM Integrated Solutions Console, select **Start** > **All Programs** > **IBM WebSphere Application Server <version>** > **Profiles** > **<profile name>** > **Administrative console**.
2. Click **Security** > **Secure administration, applications and infrastructure**.
3. Expand **Web security** on the right to display:
   - **General settings**
   - **Single sign-on**
   - **Trust association**
4. Click **General settings**.
5. Ensure that the **Authenticate only when the URI is protected** check box is selected.
6. Select the **Use available authentication data when an unprotected URI is accessed** check box is selected.
7. Click **OK**.

Part 4. Web security system component installation

Chapter 13. Setting up the Security Access Manager Attribute Retrieval Service

The Security Access Manager Attribute Retrieval Service is used with the WebSEAL authorization decision information (ADI) feature. This service provides communication and format translation services between the WebSEAL entitlement service library and an external provider of authorization decision information. For more information, see the *IBM Security Access Manager for Web WebSEAL Administration Guide*.

Set up this system by following the appropriate instructions for your operating system.

Setting up the Attribute Retrieval Service using the command line

Use platform-specific command-line utilities to install the Attribute Retrieval Service.

Note: If you would like to create and deploy a custom attribute retrieval service, a WSDL file is included in the Security Access Manager Application Development Kit to get you started. The file is in the following path:

AIX, Linux, or Solaris

```
/opt/PolicyDirector/example/amwebars/azn_ent_amwebars.wsdl
```

Windows

```
C:\Program Files\Tivoli\Policy Director\example\amwebars\
azn_ent_amwebars.wsdl
```

See the *IBM Security Access Manager for Web WebSEAL Administration Guide* for more information about using the WSDL file.

When you use the command-line utilities, you must manually install each component and its prerequisite software in the appropriate order.

Complete the prerequisite installations first. See Part 2, “Prerequisite software installation,” on page 25.

The platform-specific installation utilities that are used are:

AIX **`installp`**

Linux **`rpm`**

Solaris

`pkgadd`

Note: If you are installing on Solaris 10 and above, use the **-G** option. The **-G** option ensures that packages are added in the current zone only. When the **-G** option is used in the global zone, the package is added to the global zone only and is not propagated to any existing or yet-to-be-created non-global zone. When used in a non-global zone, the package(s) are added to the non-global zone only.

Windows

```
setup.exe
```

After completing installation, use the appropriate configuration commands.

Note: For more information about these utilities, see the *IBM Security Access Manager for Web Command Reference*.

AIX: Installing the Security Access Manager Attribute Retrieval Service using the command line

Use **installp** to install software packages on AIX.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

Procedure

1. Log on as **root**.
2. Ensure that the IBM Java Runtime version provided with Security Access Manager is installed. For instructions, see page "AIX: Installing IBM Java Runtime" on page 31.
3. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
4. Install IBM WebSphere Application Server. For instructions, see "Installing WebSphere Application Server" on page 46.
5. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
6. Install the following package:

   ```
   installp -acgYXd package_path/usr/sys/inst.images PDWeb.ARS
   ```

   where:

   - *package_path* is the directory where the DVD is mounted or the files are located
   - PDWeb.ARS is the Security Access Manager Attribute Retrieval Service package

   Note: This package must be installed on the same system as IBM WebSphere Application Server.
7. Unmount DVD, if used.
8. To deploy the Security Access Manager Attribute Retrieval Service into the IBM WebSphere Application Server environment, run the Deploy.sh file and follow instructions in the Readme.deploy file, in the /opt/pdwebars/ directory.
9. To configure WebSEAL to use the Security Access Manager Attribute Retrieval Service, see the *IBM Security Access Manager for Web WebSEAL Administration Guide*.

What to do next

This step completes the setup of the Security Access Manager Attribute Retrieval Service. To set up another Security Access Manager system, follow the steps in the Chapter 3, “Installation roadmap,” on page 21.

For information about the Security Access Manager Attribute Retrieval Service, see the *IBM Security Access Manager for Web WebSEAL Administration Guide*.

Linux: Installing the Security Access Manager Attribute Retrieval Service using the command line

Use **rpm** to install software packages on Linux.

Before you begin

Complete the appropriate preinstallation tasks in:

- “Operating system preparation” on page 28.
- Chapter 4, “Prerequisite installation and configuration roadmap,” on page 27

Procedure

1. Log on as **root**.
2. Ensure that the IBM Java Runtime provided with Security Access Manager is installed. For instructions, see page “Linux: Installing IBM Java Runtime” on page 32.
3. Install the IBM Security Access Manager License, if not already installed. For instructions, see “AIX, Linux, Solaris: Installing the IBM Security Access Manager License” on page 37.
4. Install IBM WebSphere Application Server. For instructions, see “Installing WebSphere Application Server” on page 46.
5. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
6. Change to the *package_path*/*distribution* directory

   where:

   - package_path is the mount point for your DVD or file location
   - *distribution* specifies linux_x86 for x86-64 or linux_s390 for System z.
7. Install the following package:rpm -ihv *package*
   where *package* is:

	Security Access Manager Attribute Retrieval Service
Linux on x86-64	PDWebARS-PD-7.0.0-0.x86_64.rpm
Linux on System z	PDWebARS-PD-7.0.0-0.s390x.rpm

   Note: This package must be installed on the same system as IBMWebSphere Application Server.
8. Unmount the DVD, if used.
9. To deploy the Security Access Manager Attribute Retrieval Service into the WebSphere Application Server environment, run the Deploy.sh file and follow instructions in the Readme.deploy file, in the /opt/pdwebars/ directory.

10. To configure WebSEAL to use the Security Access Manager Attribute Retrieval Service, see the *IBM Security Access Manager for Web: WebSEAL Administration Guide*.

What to do next

This step completes the setup of the Security Access Manager Attribute Retrieval Service. To set up another Security Access Manager system, follow the steps in the Chapter 3, “Installation roadmap,” on page 21.

For information about the Security Access Manager Attribute Retrieval Service, see the *IBM Security Access Manager for Web WebSEAL Administration Guide*.

Solaris: Installing the Security Access Manager Attribute Retrieval Service using the command line

Use **pkgadd** to install software packages on Solaris.

Before you begin

Complete the appropriate preinstallation tasks in:

- “Operating system preparation” on page 28.
- Chapter 4, “Prerequisite installation and configuration roadmap,” on page 27

About this task

Attention: Installations on Solaris systems should use the **-G** option with the **pkgadd** utility. The **-G** option adds the package into the current zone only.

Procedure

1. Log on as **root**.
2. Ensure that the IBM Java Runtime version provided with Security Access Manager is installed. For instructions, see page “Solaris: Installing IBM Java Runtime” on page 33.

   Note: If you configure the Security Access Manager Attribute Retrieval Service against Java Runtime Environments other than the Java Runtime Environment supported by Security Access Manager, the configuration might fail.
3. Install the IBM Security Access Manager License, if not already installed. For instructions, see “AIX, Linux, Solaris: Installing the IBM Security Access Manager License” on page 37.
4. Install IBM WebSphere Application Server. For instructions, see “Installing WebSphere Application Server” on page 46.
5. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
6. Install the following packages, one at a time:

   ```
   pkgadd -d /package_path/solaris -a /package_path/solaris/pddefault -G PDWebARS
   ```

   where:

   -d /*package_path*/solaris
   Specifies the location of the package.

-a */package_path*/**solaris/pddefault**
Specifies the location of the installation administration script.

and `PDWebARS` specifies the Security Access Manager Attribute Retrieval Service package.

Note: This package must be installed on the same system as IBM WebSphere Application Server.

7. To deploy the Security Access Manager Attribute Retrieval Service into the WebSphere Application Server environment, run the `Deploy.sh` file and follow instructions in the `Readme.deploy` file, in the `/opt/pdwebars/` directory.
8. To configure WebSEAL to use the Security Access Manager Attribute Retrieval Service, see the *IBM Security Access Manager for Web WebSEAL Administration Guide*.

What to do next

This step completes the setup of the Security Access Manager Attribute Retrieval Service. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

For information about the Security Access Manager Attribute Retrieval Service, see the *IBM Security Access Manager for Web WebSEAL Administration Guide*.

Windows: Installing the Security Access Manager Attribute Retrieval Service using the command line

Use **`setup.exe`** to install software packages on Windows.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

Procedure

1. Log on as a user with administrator privileges.
2. Ensure that the IBM Java Runtime version provided with Security Access Manager is installed. For instructions, see page "Windows: Installing IBM Java Runtime" on page 34.
3. Install IBM WebSphere Application Server. See "Installing WebSphere Application Server" on page 46.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
5. Install the Security Access Manager Attribute Retrieval Service package. To do so, run the **`setup.exe`** file in the following directory:

   `\windows\PolicyDirector\Disk Images\Disk1`

   Follow the online instructions to complete the installation.**Note:** This package must be installed on the same system as IBM WebSphere Application Server.

6. To deploy the Security Access Manager Attribute Retrieval Service into the WebSphere Application Server environment, run the `Deploy.bat` file and follow instructions in the `Readme.deploy` file, in the `C:\Program Files\Tivoi\PDWebARS\` directory.
7. To configure WebSEAL to use the Security Access Manager Attribute Retrieval Service, see the *IBM Security Access Manager for Web: WebSEAL Administration Guide*.

What to do next

This step completes the setup of the Security Access Manager Attribute Retrieval Service. To set up another Security Access Manager system, follow the steps in the Chapter 3, “Installation roadmap,” on page 21.

For information about the Security Access Manager Attribute Retrieval Service, see the *IBM Security Access Manager for Web WebSEAL Administration Guide*.

Chapter 14. Setting up the plug-in for Web servers

Security Access Manager Plug-in for Web Servers manages the security of your web-based resources by acting as the gateway between your clients and secure Web space.

The plug-in implements the security policies that protect your Web object space. The plug-in can provide single sign-on solutions, support Web servers that run as virtual hosts and incorporate Web application server resources into its security policy. For more information, see the *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*

IBM Security Access Manager plug-in for Web servers supports these servers and platforms:

- Apache Web Server on AIX, Linux on x86-64, Linux on System z, and Solaris
- IBM HTTP Server on AIX, Linux on x86-64, Linux on System z, and Solaris.
- Internet Information Services on Windows

See the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge base for more information about which versions of the Web servers are supported. For more information about these Web Security components, see the *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.

Complete the instructions that apply to your Web server.

Preinstallation requirements

Before you install and configure the Security Access Manager Plug-in for Web Servers component, ensure that the following requirements are met. These requirements are applicable, regardless of which installation method you plan to use.

- Complete the appropriate tasks in "Operating system preparation" on page 28.
- Complete the appropriate tasks inChapter 4, "Prerequisite installation and configuration roadmap," on page 27
- Ensure that all necessary operating system patches are installed. Review the most recent release information, including system requirements, disk space requirements, and known defects and limitations. See the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge base.
- Ensure that a Security Access Manager registry server and the policy server are set up in your secure domain. For instructions on setting up these systems, see Part 3, "Base system component installation," on page 101.
- Ensure that forward/reverse proxy is disabled in your Web server environment.
- Ensure that your Web server is installed and configured on this system. In addition, your Web server must be configured for SSL, client certificates, or both if you intend to enable SSL communication.
- Ensure that Security Access Manager supports the platform on which you are running your Web server.

- Ensure that IIS 6 Management Compatibility is installed on Windows systems with Internet Information Services (IIS). The Security Access Manager Plug-in for Internet Information Services requires IIS 6 Management Compatibility.
- Ensure that the Apache Web server has Dynamic Shared Objects (DSO) support enabled, because the Security Access Manager Plug-in for Apache Web Server requires DSO.
- For Solaris, ensure that the Apache modules previously compiled with the GNU Compiler Collection (GCC) version 3.2 or higher to prevent errors.
- A valid Group ID is required to access the Apache Web Server by using the plug-in. The default Group ID value of -1 in the Apache configuration file is not valid. Before the configuration of the Security Access Manager Plug-in for Web Servers, you must change the Group ID value to a known system group in the Group configuration entry of the Apache configuration file. This change is required only when for Apache that runs on Red Hat Enterprise Linux 5.

Installing the plug-in for Apache Web Server using the command line

Use these instructions to install the plug-in for the Apache Web Server.

About this task

Complete the instructions that apply to your operating system.

For more information, see the *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.

AIX: plug-in for Apache Web Server

Use **installp** to install software packages and the **pdconfig** utility to configure them on AIX.

Procedure

1. Log on as **root**.
2. Ensure that all necessary operating system patches are installed. Also review the most-recent release information, including system requirements, disk space requirements, and known defects and limitations in the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
3. Ensure that you meet the requirements that are listed in "Preinstallation requirements" on page 213.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
5. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "AIX: Installing the IBM Global Security Kit (GSKit)" on page 35.
6. Install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "AIX: Installing the IBM Tivoli Directory Server client" on page 42.
7. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.

8. Install the IBM Security Utilities, if not already installed. For instructions, see page "AIX: Installing the IBM Security Utilities" on page 39.
9. Install the Security Access Manager packages:

   ```
   installp -acgYXd package_path/usr/sys/inst.images packages
   ```

   where:

   - *package_path* is the directory where the DVD is mounted or the files are located
   - *packages* are:

     PD.RTE Specifies the Security Access Manager Runtime package.

     PD.WebRTE
     Specifies the Security Access Manager Web Security Runtime package.

     PD.WPI Specifies the Security Access Manager Plug-in for Web Servers package.

     PD.WPIApache
     Specifies the Security Access Manager Plug-in for Apache Web Server package.

   Note: These packages must be installed on the same system as the Apache Web Server.
10. Unmount the DVD, if used.
11. To view status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
12. Set the AIX Extended Shared Memory Support (EXTSHM) environment variable to **ON** before you configure the Security Access Manager Plug-in for Apache Web Server component and also before you start the plug-in for Apache Web Server proxy server or the Apache Web server.
13. Configure the Security Access Manager Runtime followed by the Security Access Manager Plug-in for Web Servers package as follows:
    a. Start the configuration utility:

       ```
       pdconfig
       ```

       The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure, one at a time. For assistance with configuration options, see Appendix D, "pdconfig options," on page 317.

       When a message displays indicating that the package was successfully configured, select the **x** option twice to close the configuration utility.
14. Restart the Web server.
15. Customize the `pdwebpi.conf` file for your particular Web server. For information, see the *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.
16. To start the plug-in process, change to the `/opt/pdwebpi/bin` directory and enter the following command:

    ```
    pdwebpi_start start
    ```

Results

This step completes the setup of the Security Access Manager Web server plug-in for Apache Server on AIX. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Linux on x86-64: plug-in for Apache Web Server

Use **rpm** to install software packages and the **pdconfig** utility to configure them on Linux x86-64.

Procedure

1. Log on as **root**.
2. Ensure that all necessary operating system patches are installed. Ensure that you review the most recent release information, including system requirements, disk space requirements, and known defects and limitations in the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
3. Ensure that you meet the requirements that are listed in "Preinstallation requirements" on page 213.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
5. Change to the *package_path*/linux_x86 directory where *package_path* is the mount point for your DVD or file location.
6. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "AIX: Installing the IBM Global Security Kit (GSKit)" on page 35.
7. Install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "AIX: Installing the IBM Tivoli Directory Server client" on page 42.
8. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
9. Install the IBM Security Utilities, if not already installed. For instructions, see page "AIX: Installing the IBM Security Utilities" on page 39.
10. Install the Security Access Manager packages:

    ```
    rpm -ihv packages
    ```

    where *packages* are:

Package	Linux on x86-64
Security Access Manager Runtime package	PDRTE-PD-7.0.0-0.x86_64.rpm
Security Access Manager Web Security Runtime package	PDWebRTE-PD-7.0.0-0.x86_64.rpm
Security Access Manager Plug-in for Web Servers package	PDWPI-PD-7.0.0-0.x86_64.rpm
Security Access Manager Plug-in for Apache Web Server package	PDWPI-Apache-7.0.0-0.x86_64.rpm

Note: These packages must be installed on the same system as Apache Web Server.

11. Unmount the DVD, if used.
12. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
13. Configure the Security Access Manager Runtime followed by the Security Access Manager Plug-in for Web Servers package as follows:
    a. Start the configuration utility:

       ```
       pdconfig
       ```

       The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure, one at a time. For assistance with configuration options, see Appendix D, "pdconfig options," on page 317.

       When a message displays indicating that the package was successfully configured, select the **x** option twice to close the configuration utility.
14. Restart the Web server.
15. Customize the `pdwebpi.conf` file for your particular Web server. For information, see the *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.
16. To start the plug-in process, change to the `/opt/pdwebpi/bin` directory and enter the following command:

    ```
    pdwebpi_start start
    ```

Results

This step completes the setup of the Security Access Manager Web server plug-in for Apache Server on Linux x86-64. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Linux on System z: plug-in for Apache Web Server

Use **rpm** to install software packages and the **pdconfig** utility to configure them on Linux on System z. To install the Web server plug-in for Apache Web Server (31-bit only) for Linux on System z, complete the following steps.

About this task

Note to Linux on System z users: You must first obtain access to the Linux `rpm` files which are in the */package_path*`/linux_s390` directory.

Procedure

1. Log on as **root**.
2. Ensure that all necessary operating system patches are installed. Review the most recent release information, including system requirements, disk space requirements, and known defects and limitations in the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
3. Ensure that you meet the requirements that are listed in "Preinstallation requirements" on page 213.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

Attention: Ensure that the files are in a directory path that does not contain any spaces.

5. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Linux: Installing the IBM Global Security Kit (GSKit)" on page 35.
6. Install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Linux: Installing the IBM Tivoli Directory Server client" on page 43.
7. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
8. Install the IBM Security Utilities, if not already installed. For instructions, see page "Linux: Installing IBM Security Utilities" on page 40.
9. Install the Security Access Manager packages:

   `rpm -ihv packages`

   here *packages* are as follows:

Package	Linux on System z
Security Access Manager Runtime package	PDRTE-PD-7.0.0-0.s390.rpm
Security Access Manager Web Security Runtime package	PDWebRTE-PD-7.0.0-0.s390.rpm
Security Access Manager Plug-in for Web Servers package	PDWPI-PD-7.0.0-0.s390.rpm
Security Access Manager Plug-in for Apache Web Server package	PDWPI-Apache-7.0.0-0.s390.rpm

   Note: These packages must be installed on the same system as the Apache Web Server.

10. Unmount the DVD, if used.
11. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
12. Configure the Security Access Manager packages as follows:
    a. Start the configuration utility: `pdconfig` The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure, one at a time. Configure the Security Access Manager Runtime followed by the Security Access Manager Plug-in for Web Servers package.
    d. Depending on the package that you selected, you are prompted for configuration options. For assistance with configuration options, see Appendix D, "pdconfig options," on page 317.
    When a message displays indicating that the package was successfully configured, select the **x** option twice to close the configuration utility.
13. Restart the Web server.
14. Customize the `pdwebpi.conf` file for your particular Web server. For information, see the *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.

15. To start the plug-in process, change to the `/opt/pdwebpi/bin` directory and enter the following command: `pdwebpi_start start`

Results

This step completes the setup of the Security Access Manager Web server plug-in for Apache Web Server for Linux on System z. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Solaris: plug-in for Apache Web Server

Use **pkgadd** to install software packages and the **pdconfig** utility to configure them on Solaris.

Attention: Installations on Solaris systems should use the **-G** option with the **pkgadd** utility. The **-G** option adds the package into the current zone only.

Procedure

1. Log on as **root**.
2. Ensure that all necessary operating system patches are installed. Review the most recent release information, including system requirements, disk space requirements, and known defects and limitations in the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
3. Ensure that you meet the requirements that are listed in "Preinstallation requirements" on page 213.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
5. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Solaris: Installing the IBM Global Security Kit (GSKit)" on page 36.
6. Install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Solaris: Installing the IBM Tivoli Directory Server client" on page 44.
7. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
8. Install the IBM Security Utilities, if not already installed. For instructions, see page "Solaris: Installing IBM Security Utilities" on page 40.
9. Install the Security Access Manager packages (one at a time):

   `pkgadd -d /package_path/solaris -a /package_path/solaris/pddefault -G packages`

   where:

   /*package_path*/solaris
   Specifies the location of the package.

   /*package_path*/solaris/pddefault
   Specifies the location of the installation administration script.

   and *packages* are as follows:

   PDRTE Specifies the Security Access Manager Runtime package.

PDWebRTE
Specifies the Security Access Manager Web Security Runtime package.

PDWPI Specifies the Security Access Manager Plug-in for Web Servers package.

PDWPIapa
Specifies the Security Access Manager Plug-in for Apache Web Server package.

Note: These packages must be installed on the same system as the Apache Web Server.

10. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
11. Set the shared memory kernel parameters to values that are larger than the default values. Add the following lines to the `/etc/system` file to increase the parameters to acceptable values:

```
set shmsys:shminfo_shmmax=0x2000000
set shmsys:shminfo_shmseg=256
set shmsys:shminfo_shmmni=256
```

    Restart your system for these changes to take effect.
12. Configure the Security Access Manager packages as follows:
    a. Start the configuration utility:

```
pdconfig
```

    The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure, one at a time. Configure the Security Access Manager Runtime followed by the Security Access Manager Plug-in for Web Servers package.

    Depending on the package that you selected, you are prompted for configuration options. For assistance with configuration options, see Appendix D, "pdconfig options," on page 317.

    When a message displays indicating that the package was successfully configured, select the **x** option twice to close the configuration utility.
13. Restart the Web server.
14. Customize the `pdwebpi.conf` file for your particular Web server. For information, see the *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.
15. To start the plug-in process, change to the `/opt/pdwebpi/bin` directory and enter the following command:

```
pdwebpi_start start
```

This step completes the setup of the Security Access Manager Web server plug-in for Apache Web Server on Solaris. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Installing the plug-in for IBM HTTP Server using the command line

Use these instructions to install the plug-in for the IBM HTTP Server.

About this task

Complete the instructions that apply to your operating system.

For more information, see the *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.

AIX: plug-in for IBM HTTP Server

Use **installp** to install software packages and the **pdconfig** utility to configure them on AIX.

Procedure

1. Log on as **root**.
2. Ensure that all necessary operating system patches are installed. Review the most recent release information, including system requirements, disk space requirements, and known defects and limitations in the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
3. Ensure that you meet the requirements that are listed in "Preinstallation requirements" on page 213.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
5. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "AIX: Installing the IBM Global Security Kit (GSKit)" on page 35.
6. Install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "AIX: Installing the IBM Tivoli Directory Server client" on page 42.
7. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
8. Install the IBM Security Utilities, if not already installed. For instructions, see page "AIX: Installing the IBM Security Utilities" on page 39.
9. Install the Security Access Manager packages:

   ```
   installp -acgYXd package_path/usr/sys/inst.images packages
   ```

   where:

   - *package_path* is the directory where the DVD is mounted or the files are located
   - *packages* are:

     PD.RTE Specifies the Security Access Manager Runtime package.

     PDWeb.RTE
     Specifies the Security Access Manager Web Security Runtime package.

     PD.WPI Specifies the Security Access Manager Plug-in for Web Servers package.

     PD.WPIIHS
     Specifies the Security Access Manager Plug-in for IBM HTTP Server package.

Note: These packages must be installed on the same system as IBM HTTP Server.

10. Unmount the DVD, if used.
11. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
12. Set the EXTSHM environment variable to **ON** before you configure the Security Access Manager Plug-in for IBM HTTP Server component and before you start either the plug-in for IBM HTTP Server proxy server or the IBM HTTP Server.
13. Configure the Security Access Manager packages as follows:
    a. Start the configuration utility:

       ```
       pdconfig
       ```

       The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure, one at a time. Configure the Security Access Manager Runtime followed by the Security Access Manager Plug-in for Web Servers package.

       Depending on the package that you selected, you are prompted for configuration options. For assistance with configuration options, see Appendix D, "pdconfig options," on page 317.

       When a message displays indicating that the package was successfully configured, select the **x** option twice to close the configuration utility.
14. Restart the Web server.
15. Customize the `pdwebpi.conf` file for your particular Web server. For information, see the *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.
16. To start the plug-in process, change to the `/opt/pdwebpi/bin` directory and enter the following command:

    ```
    pdwebpi_start start
    ```

Results

This step completes the setup of the Security Access Manager Web server plug-in for IBM HTTP Server on AIX. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Linux: plug-in for IBM HTTP Server

Use **`rpm`** to install software packages and the **`pdconfig`** utility to configure them on Linux.

About this task

Note to Linux on System z users: You must first obtain access to the Linux `rpm` files which are in the `/package_path/linux_s390` directory.

Procedure

1. Log on as **root**.

2. Ensure that all necessary operating system patches are installed. Review the most recent release information, including system requirements, disk space requirements, and known defects and limitations in the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
3. Ensure that you meet the requirements that are listed in "Preinstallation requirements" on page 213.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
5. Change to the *package_path*/*distribution* directory

   where:

   - *package_path* is the mount point for your DVD or file location
   - *distribution* specifies `linux_x86` for x86-64 or `linux_s390` for System z
6. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Linux: Installing the IBM Global Security Kit (GSKit)" on page 35.
7. Install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Linux: Installing the IBM Tivoli Directory Server client" on page 43.
8. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
9. Install the IBM Security Utilities, if not already installed. For instructions, see page "Linux: Installing IBM Security Utilities" on page 40.
10. Install the Security Access Manager packages:

    `rpm -ihv` *packages*

    where *packages* are:

Package	Linux on x86-64	Linux on System z
Security Access Manager Runtime package	`PDRTE-PD-7.0.0-0.x86_64.rpm`	`PDRTE-PD-7.0.0-0.s390.rpm`
Security Access Manager Web Security Runtime package	`PDWebRTE-PD-7.0.0-0.x86_64.rpm`	`PDWebRTE-PD-7.0.0-0.s390.rpm`
Security Access Manager Plug-in for Web Servers package	`PDWPI-PD-7.0.0-0.x86_64.rpm`	`PDWPI-PD-7.0.0-0.s390.rpm`
Security Access Manager Plug-in for IBM HTTP Web Server package	`PDWPI-IHS-7.0.0-0.x86_64.rpm`	`PDWPI-IHS-7.0.0-0.s390.rpm`

    Note: These packages must be installed on the same system as IBM HTTP Server.
11. Unmount the DVD, if used.
12. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
13. Configure the Security Access Manager packages as follows:

a. Start the configuration utility:

   ```
   pdconfig
   ```

   The Security Access Manager Setup Menu is displayed.

b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.

c. Select the menu number of the package that you want to configure, one at a time. Configure the Security Access Manager Runtime followed by the Security Access Manager Plug-in for Web Servers package.
   Depending on the package that you selected, you are prompted for configuration options. For assistance with configuration options, see Appendix D, "pdconfig options," on page 317.
   When a message displays indicating that the package was successfully configured, select the **x** option twice to close the configuration utility.

14. Restart the Web server.
15. Customize the `pdwebpi.conf` file for your particular Web server. For information, see the *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.
16. To start the plug-in process, change to the `/opt/pdwebpi/bin` directory and enter the following command:

    ```
    pdwebpi_start start
    ```

Results

This step completes the setup of the Security Access Manager Web server plug-in for IBM HTTP Server on Linux. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Solaris: plug-in for IBM HTTP Server

Use **pkgadd** to install software packages and the **pdconfig** utility to configure them on Solaris.

About this task

Attention: Installations on Solaris systems should use the **-G** option with the **pkgadd** utility. The **-G** option adds the package into the current zone only.

Procedure

1. Log on as **root**.
2. Ensure that all necessary operating system patches are installed. Review the most recent release information, including system requirements, disk space requirements, and known defects and limitations in the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
3. Ensure that you meet the requirements that are listed in "Preinstallation requirements" on page 213.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
5. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Solaris: Installing the IBM Global Security Kit (GSKit)" on page 36.

6. Install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Solaris: Installing the IBM Tivoli Directory Server client" on page 44.
7. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
8. Install the IBM Security Utilities, if not already installed. For instructions, see page "Solaris: Installing IBM Security Utilities" on page 40.
9. Install the Security Access Manager packages (one at a time):

   ```
   pkgadd -d /package_path/solaris -a /package_path/solaris/pddefault -G packages
   ```

   where:

   /*package_path*/solaris
   Specifies the location of the package.

   /*package_path*/solaris/pddefault
   Specifies the location of the installation administration script.

   and where *packages* are as follows:

   PDRTE Specifies the Security Access Manager Runtime package.

   PDWebRTE
   Specifies the Security Access Manager Web Security Runtime package.

   PDWPI Specifies the Security Access Manager Plug-in for Web Servers package.

   PDWPIihs
   Specifies the Security Access Manager Plug-in for IBM HTTP Server package.

   Note: These packages must be installed on the same system as IBM HTTP Server.
10. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
11. Set the shared memory kernel parameters to values that are larger than the default values. Add the following lines to the `/etc/system` file to increase the parameters to acceptable values:

    ```
    set shmsys:shminfo_shmmax=0x2000000
    set shmsys:shminfo_shmseg=256
    set shmsys:shminfo_shmmni=256
    ```

    Restart your system for these changes to take effect.
12. Configure the Security Access Manager packages as follows:
    a. Start the configuration utility:

       ```
       pdconfig
       ```

       The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure, one at a time. Configure the Security Access Manager Runtime followed by the Security Access Manager Plug-in for Web Servers package.

Depending on the package that you selected, you are prompted for configuration options. For assistance with configuration options, see Appendix D, "pdconfig options," on page 317.

When a message displays indicating that the package was successfully configured, select the **x** option twice to close the configuration utility.

13. Restart the Web server.
14. Customize the `pdwebpi.conf` file for your particular Web server. For information, see the *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.
15. To start the plug-in process, change to the `/opt/pdwebpi/bin` directory and enter the following command:

    ```
    pdwebpi_start start
    ```

Results

This step completes the setup of the Security Access Manager Web server plug-in for IBM HTTP Server on Solaris. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Installing the plug-in for Internet Information Services using the command line

The Web server plug-in for Internet Information Services is available on supported Windows platforms only. Use **setup.exe** program to install software packages and the **pdconfig** utility to configure them.

Before you begin

Ensure that IIS 6 Management Compatibility is installed on the Windows system. The Security Access Manager Plug-in for Internet Information Services requires IIS 6 Management Compatibility.

Procedure

1. Log on as any member of the Administrators group that has Administrator privileges.
2. Ensure that all necessary operating system patches are installed. Review the most recent release information, including system requirements, disk space requirements, and known defects and limitations in the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
3. Ensure that you meet the requirements that are listed in "Preinstallation requirements" on page 213.
4. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Windows: Installing the IBM Global Security Kit (GSKit)" on page 36.
5. Install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Windows: Installing the IBM Tivoli Directory Server client" on page 45.
6. Install the Security Access Manager license, if not already installed. For instructions, see "Windows: Installing the IBM Security Access Manager License" on page 39.
7. Install the IBM Security Utilities, if not already installed. For instructions, see page "Windows: Installing IBM Security Utilities" on page 41.

8. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
9. Install the Security Access Manager packages. To do so, run the **setup.exe** program, in the following directory:

   `\windows\PolicyDirector\Disk Images\Disk1`

   The Choose Setup Language dialog is displayed.
10. Select the language that you want to use for the installation.
11. Click **OK**. The Welcome window is displayed.
12. Click **Next** to continue.
13. Read the license agreement and click **Yes** if you agree to the terms.
14. Select the following packages:
    - Security Access Manager Runtime
    - Access Manager Web Security Runtime
    - Access Manager Plug-in for Web Servers
15. Click **Next**.
16. Accept the default destination directory or click **Browse** to select a path to another directory on the local system. If the directory does not exist, you must confirm that you want to create the directory or specify a directory that exists.
17. To start copying files to the destination folder, click **Next**.
18. Click **Finish** to exit the setup program.
19. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
20. You must configure IIS to use one of the default identities when you run Security Access Manager Plug-in for Microsoft Internet Information Services (IIS) on a WindowsDomain Controller. Because of a limitation of the Windows operating system, using an identity other than the default user identities causes a `503 Service Unavailable` error.
21. Configure the Security Access Manager Runtime followed by the Security Access Manager Plug-in for Web Servers package. To do so, click **Start** > **Programs** > **IBM Security Access Manager for Web** > **Configuration**.

    For assistance with configuration options, see Appendix D, "pdconfig options," on page 317.

    Note: You can also configure Security Access Manager components by using the **pdconfig** utility from a command line.
22. Restart the Web server.
23. Customize the `pdwebpi.conf` file for your particular Web server. For information, see the *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.

Results

This step completes the setup of the Security Access Manager Web server plug-in for IIS Web Server on Windows. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Note: Before you install another component, open a new command-line window.

Setting up a plug-in for Internet Information Services using the Launchpad (Windows)

Use the Launchpad installation method to install and configure the plug-in for Internet Information Services on Windows using a graphical user interface.

Before you begin

Ensure that you complete the following prerequisite tasks:

- "Operating system preparation" on page 28
- Chapter 5, "User registry server installation and configuration," on page 51.

Ensure that IIS 6 Management Compatibility is installed on the Windows system. The Security Access Manager Plug-in for Internet Information Services requires IIS 6 Management Compatibility.

About this task

The Launchpad uses a graphical user interface to perform step-by-step installation and initial configuration.

This task installs the following components:

- IBM Global Security Kit (GSKit)
- IBM Tivoli Directory Server client
- IBM Security Utilities
- Security Access Manager License
- Security Access Manager Runtime
- Security Access Manager Web Security Runtime
- Security Access Manager Plug-in for Web Servers

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the Launchpad image files are in a directory path that does not contain any spaces.
2. Start the Launchpad.
   a. Locate the `launchpad64.exe` file.
   b. Double-click the file to start the Launchpad.
3. Select the language that you want to use during the installation.
4. Click **OK**. The Launchpad Welcome window opens.
5. Click **Next**.
6. Select the **Plug-in for Web Servers** component.
7. Click **Next**. A list displays the component that you selected and any prerequisite software that is required by that component but that is not already installed.
8. Click **Next**. An arrow next to a component name on the left indicates that component is being installed. A check mark next to a component name indicates that component is installed.

9. If the current component is IBM Global Security Kit, click **Install IBM Global Security Kit** to install it. When it completes, continue with step 10.
10. Click **Next**.
11. Respond to the prompts presented during the installation.
12. Click **Next** at the bottom of the Launchpad to continue.
13. Complete the installation.
    - If the installation fails, correct the error that is described in the error message and restart the Launchpad.
    - If the installation is successful, continue with step 14.
14. Click **Next** to start the configuration.

    Note: The configuration tool is displayed in the language that is selected for your operating system locale. If the tool is displayed in English and is not displayed in the operating system locale, review the language pack installation log at `%USERPROFILE%\ISAMLangPacksInstall.log`. Correct any errors that are reported in the log file. Then, install the language pack as described in Appendix E, "Language support installation," on page 339.
15. Click **Configure Security Access Manager**. The configuration tool opens.
16. Select the component.
17. Click **Configure**.
18. Complete the configuration. For help completing the prompts, see Appendix D, "pdconfig options," on page 317. When the configuration is completed, a success or failure message is displayed.
19. Take one of the following actions:
    - If the configuration completed successfully, click **Next**.
    - If the configuration failed or an error is displayed, review the log file in the default `%USERPROFILE%` location, such as `C:\Users\Administrator\LaunchPDConfigforISAM.log`.

      Make corrections as indicated by the log file. Then, configure the component by using the **pdconfig** utility at a command line or by clicking **Start** > **Programs** > **IBM Security Access Manager for Web** > **Configuration**.
20. Click **Finish** to close the Launchpad.

Setting up the plug-in for Web servers using script files

The installation and configuration scripts automate installations and perform unattended (*silent*) installations and configurations.

Use the scripts in their original state or modify them to suit the requirements of your environment.

Automating installation of the Apache Server plug-in or IBM HTTP Server plug-in

Use the script file to automate the installation of the Apache Server plug-in or the IBM HTTP Server plug-in.

Before you begin

Ensure that your system meets the preinstallation requirements, including the installation of the Web server. See "Preinstallation requirements" on page 213.

About this task

Automated installations perform unattended (*silent*) installations.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the `install_isam.sh` script file in the `scripts` directory.
3. Run the script as follows:

   ```
   ./install_isam.sh -i component -d path_to_packages -a [accept|display]
   ```

   where
   - *component* is the name of the component you want to install. The component names for the plug-ins are:
     - `PluginApache`
     - `PluginIBMHTTP`
   - *path_to_packages* is the location of the component installation packages.

     For example, if you are installing from a DVD:

     AIX *dvd_mount_point*`/usr/sys/inst.images`

     Linux */dvd_mount_point*`/linux_x86`

     Solaris
     /dvd_mount_point`/solaris`
   - `-a [accept|display]`

     The `-a accept` option automatically accepts the license without displaying the license. The `-a display` option displays the license and you must manually accept the license.
   - For example, on Linux to install the Apache Server plug-in:

     ```
     ./install_isam.sh -i PluginApache -d /mnt/dvd/linux_x86 -a accept
     ```
4. Optional: To list the required packages without installing, use the -l option.

   ```
   ./install_isam.sh -l component
   ```

What to do next

When the installation is completed, continue with "Automating configuration of the Apache Server plug-in or IBM HTTP Server plug-in."

Automating configuration of the Apache Server plug-in or IBM HTTP Server plug-in

Use the script file to automate the configuration of the Apache Server plug-in or the IBM HTTP Server plug-in.

Before you begin

Complete the installation of the web security components. See "Automating installation of the Apache Server plug-in or IBM HTTP Server plug-in" on page 229.

To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.

About this task

Automated configuration performs unattended (*silent*) configuration.

The script files and template files that are used in this task are installed in the `/opt/PolicyDirector/example/config` directory.

Procedure

1. Create an options file for the component you want to configure.
   a. Locate the options file template for the component. The Plug-in for Web Servers template location is:

      `/opt/PolicyDirector/example/config/configure_webpi.options.template`
   b. Copy the file to a temporary directory.
   c. Save the file with a name that is unique to your environment.
   d. Modify the content of the file to specify settings for your environment. The comments in the file explain the settings and provide examples.
   e. Save the file.
2. Optional: By default, passwords you specified in the options files are stored in clear text. To obfuscate these passwords:
   a. See Appendix F, "Password management," on page 351 for instructions on using the `-obfuscate` option with the `pdconf` tool to obfuscate the passwords in the options files. For more information about `pdconf`, see the *IBM Security Access Manager for Web Command Reference*.
   b. Return to these instructions to run the configuration script.
3. Run the configuration script and use the options file for input.

   `./configure_isam.sh -f options_file`

   where *options file* is the text file that contains the configuration options. For example:

   `./configure_isam.sh -f my_configure_webpi.options`

Automating installation of the Internet Information Services plug-in

Use the script file to automate the installation of the Internet Information Services plug-in.

About this task

Automated installations perform unattended (*silent*) installations.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the `install_isam.bat` script file in the `scripts` directory. This directory is on the product DVD or in the directory where you extracted the product files.
3. Run the script as follows:

   ```
   install_isam.bat /i PluginIIS /d path_to_packages
   ```

   where
   - `PluginIIS` is the component name.
   - *`path_to_packages`* is the path to the product DVD or the directory where you extracted the product files.
   - For example, type:

     ```
     install_isam.bat /i PluginIIS /d path_to_packages
     ```

   The script installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.
4. Optional: To list the required packages without installing, use the /l option.

   ```
   install_isam.bat /l PluginIIS
   ```

What to do next

When the installation is completed, continue with "Automating configuration of the Internet Information Service plug-in."

Automating configuration of the Internet Information Service plug-in

Use the script file to automate the configuration of the Internet Information Service plug-in.

Before you begin

Complete the installation of the Internet Information Service plug-in. See "Automating installation of the Internet Information Services plug-in" on page 231.

Ensure that IIS 6 Management Compatibility is installed on the Windows system. The Security Access Manager Plug-in for Internet Information Services requires IIS 6 Management Compatibility.

To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.

Open a new window. Do not perform this task in the same window where you ran the installation script.

About this task

Automated configuration performs unattended (*silent*) configuration.

To use the script:

1. Create an options file that contains the specific configuration settings for your environment.
2. Run the script and use the options file as input.

Procedure

1. Create an options file for the component you want to configure.
   a. Locate the options file template for the component. The Plug-in for Web Servers template location is:

      ```
      C:\Program Files\Tivoli\PDWebPI\etc\
      configure_webpi.options.template.cmd
      ```

   b. Copy the file to a temporary directory.
   c. Save the file with a name that is unique to your environment.
   d. Modify the content of the file to specify settings for your environment. The comments in the file explain the settings and provide examples.
   e. Save the file.
2. Optional: By default, passwords you specified in the options files are stored in clear text. To obfuscate these passwords:
   a. Copy the `configure_isam.conf` file from the `C:\Program Files\Tivoli\Policy Director\example\config` directory to the same directory where you copied the options files.
   b. See Appendix F, "Password management," on page 351 for instructions on using the `-obfuscate` option with the `pdconf` tool to obfuscate the passwords in the options files. For more information about `pdconf`, see the *IBM Security Access Manager for Web Command Reference*.
   c. Return to these instructions to run the configuration script.
3. Copy the `configure_isam.cmd` from the `C:\Program Files\Tivoli\Policy Director\example\config` directory to the same directory where you saved the template file.
4. Run the configuration script and use the options file for input.

   ```
   configure_isam.cmd -f options_file
   ```

   where *options_file* is the text file that contains the configuration options. For example:

   ```
   configure_isam.cmd -f my_configure_webpi.options.cmd
   ```

Chapter 15. Setting up a Web security development system

The Security Access Manager Web Security ADK contains development APIs for Web Security components. The APIs include Security Access Manager cross-domain authentication service (CDAS), the Security Access Manager cross-domain mapping framework (CDMF), and the Security Access Manager password strength module.

For more information about this Web security system, see the *IBM Security Access Manager for Web: WebSEAL Administration Guide*.

Complete the instructions that apply to your operating system.

Setting up a Web security development system using the command line

Use platform-specific command-line utilities to install the Web security development system. This method is one of several installation methods you can use.

For more information, see Chapter 2, "Installation methods," on page 19.

When you use the command-line utilities, you must manually install each component and its prerequisite software in the appropriate order.

Complete the prerequisite installations first. See Part 2, "Prerequisite software installation," on page 25.

The platform-specific installation utilities that are used are:

AIX `installp`

Linux `rpm`

Solaris
`pkgadd`

Note: If you are installing on Solaris 10 and above, use the **-G** option. The **-G** option ensures that packages are added in the current zone only. When the **-G** option is used in the global zone, the package is added to the global zone only and is not propagated to any existing or yet-to-be-created non-global zone. When used in a non-global zone, the package(s) are added to the non-global zone only.

Windows
`setup.exe`

After you complete installation, use the appropriate configuration commands.

Note: For more information about these utilities, see the *IBM Security Access Manager for Web Command Reference*.

AIX: Installing a Web security development (WebADK) system using the command line

Use **installp** to install software packages and the **pdconfig** utility to configure them on AIX.

Before you begin

Complete the appropriate preinstallation tasks in Chapter 4, "Prerequisite installation and configuration roadmap," on page 27.

Procedure

1. Log on as **root**.
2. Ensure that all necessary operating system patches are installed. Review the most recent release information, including system requirements, disk space requirements, and known defects and limitations in the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
3. Ensure that the registry server and policy server are up and running (in normal mode).
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
5. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "AIX: Installing the IBM Global Security Kit (GSKit)" on page 35.
6. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "AIX: Installing the IBM Tivoli Directory Server client" on page 42.
7. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
8. Install the IBM Security Utilities, if not already installed. For instructions, see page "AIX: Installing the IBM Security Utilities" on page 39.
9. Install the Security Access Manager packages:

   ```
   installp -acgYXd package_path/usr/sys/inst.images packages
   ```

   where:

   - *package_path* is the directory where the DVD is mounted or the files are located
   - *packages* are:

     PD.RTE Specifies the Security Access Manager Runtime package.

     PDWeb.RTE
     Specifies the Security Access Manager Web Security Runtime package.

     PD.AuthADK
     Specifies the Security Access Manager Application Development Kit package.

     PDWeb.ADK
     Specifies the Security Access Manager Web Services Application Development Kit package.

10. Unmount the DVD, if used.
11. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
12. Configure the Security Access Manager Runtime package as follows:
    a. Start the configuration utility:

       ```
       pdconfig
       ```

       The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Follow the steps on the `pdconfig` utility to complete configuration.

Results

This step completes the setup of a Security Access Manager Web security development (ADK) system. To set up another Security Access Manager system, Follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Linux: Installing a Web security development (WebADK) system using the command line

Use **`rpm`** to install software packages and the **`pdconfig`** utility to configure them on Linux.

Before you begin

Complete the appropriate preinstallation tasks in Chapter 4, "Prerequisite installation and configuration roadmap," on page 27.

Note to Linux on System z users: You must first obtain access to the Linux `rpm` files which are in the */package_path*`/linux_s390` directory.

Procedure

1. Log on as **root**.
2. Ensure that all necessary operating system patches are installed. Review the most recent release information, including system requirements, disk space requirements, and known defects and limitations in the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
3. Ensure that the registry server and policy server are up and running (in normal mode).
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
5. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
6. Change to the *package_path*`/`*distribution* directory where *package_path* is the mount point for your DVD or file location and *distribution* specifies `linux_x86` for x86-64 or `linux_s390` for System z.

7. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Linux: Installing the IBM Global Security Kit (GSKit)" on page 35.
8. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Linux: Installing the IBM Tivoli Directory Server client" on page 43.
9. Install the IBM Security Utilities, if not already installed. For instructions, see page "Linux: Installing IBM Security Utilities" on page 40.
10. Install the Security Access Manager packages:

    `rpm -ihv packages`
    where *packages* are as follows:

Package	Linux on x86-64	Linux on System z
Security Access Manager Runtime package	PDRTE-PD-7.0.0-0.x86_64.rpm	PDRTE-PD-7.0.0-0.s390.rpm
Security Access Manager Web Security Runtime package	PDWebRTE-PD-7.0.0-0.x86_64.rpm	PDWebRTE-PD-7.0.0-0.s390.rpm
Security Access Manager Application Development Kit package	PDAuthADK-PD-7.0.0-0.x86_64.rpm	PDAuthADK-PD-7.0.0-0.s390.rpm
Security Access Manager Web Services Application Development Kit package	PDWebADK-PD-7.0.0-0.x86_64.rpm	PDWebADK-PD-7.0.0-0.s390.rpm

11. Unmount the DVD, if used.
12. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
13. Configure the package as follows:
    a. Start the configuration utility: `pdconfig`
       The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Follow the steps on the `pdconfig` utility to complete configuration.

What to do next

This step completes the setup of a Security Access Manager Web security development (ADK) system. To set up another Security Access Manager system, Follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Solaris: Installing a Web security development (WebADK) system using the command line

Use **pkgadd** to install software packages and the **pdconfig** utility to configure them on Solaris.

Before you begin

Complete the appropriate preinstallation tasks in Chapter 4, "Prerequisite installation and configuration roadmap," on page 27.

About this task

Attention: Installations on Solaris systems should use the **-G** option with the **pkgadd** utility. The **-G** option adds the package into the current zone only.

Procedure

1. Log on as **root**.
2. Ensure that all necessary operating system patches are installed. Review the most recent release information, including system requirements, disk space requirements, and known defects and limitations in the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
3. Ensure that the registry server and policy server are up and running (in normal mode).
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
5. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Solaris: Installing the IBM Global Security Kit (GSKit)" on page 36.
6. Install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Solaris: Installing the IBM Tivoli Directory Server client" on page 44.
7. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
8. Install the IBM Security Utilities, if not already installed. For instructions, see page "Solaris: Installing IBM Security Utilities" on page 40.
9. Install the Security Access Manager packages:

   ```
   pkgadd -d /package_path/solaris
     -a /package_path/solaris/pddefault -G packages
   ```

   where:

   - `-d /package_path/solaris` specifies the location of the package
   - *packages* are:

     PDRTE Specifies the Security Access Manager Runtime package.

     PDWebRTE
     Specifies the Security Access Manager Web Security Runtime package.

     PDADK Specifies the Security Access Manager Application Development Kit package.

     PDWebADK
     Specifies the Security Access Manager Web Services Application Development Kit package.

   When a message queries `Do you want to install these as setuid/setgid?`, type **Y** and press Enter. When prompted to continue, type **Y** and press Enter.

   When the installation process is complete for each package, the following message is displayed:

   ```
   Installation of packages successful.
   ```

10. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
11. Configure the Security Access Manager Runtime package as follows:
    a. Start the configuration utility:

       ```
       pdconfig
       ```

       The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Follow the steps on the `pdconfig` utility to complete configuration.

Results

This step completes the setup of a Security Access Manager Web security development (ADK) system. To set up another Security Access Manager system, Follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Windows: Installing a Web security development (WebADK) system using the command line

Use **`setup.exe`** program to install software packages and the **`pdconfig`** utility to configure them on Windows.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

Procedure

1. Log on as a user with Administrator group privileges.
2. Ensure that all necessary operating system patches are installed. Review the most recent release information, including system requirements, disk space requirements, and known defects and limitations in the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
3. Ensure that the registry server and policy server are up and running (in normal mode).
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
5. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Windows: Installing the IBM Global Security Kit (GSKit)" on page 36.
6. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Windows: Installing the IBM Tivoli Directory Server client" on page 45.
7. Install the Security Access Manager license, if not already installed. For instructions, see "Windows: Installing the IBM Security Access Manager License" on page 39.

8. Install the IBM Security Utilities, if not already installed. For instructions, see page "Windows: Installing IBM Security Utilities" on page 41.
9. Install the Security Access Manager packages. To do so, run the **setup.exe** program in the following directory:

   ```
   \windows\PolicyDirector\Disk Images\Disk1
   ```

   Follow the online instructions and select to install the following packages:
   - Security Access Manager Runtime
   - Access Manager Web Security Runtime
   - Security Access Manager Application Development Kit
   - Access Manager Web Security Application Development Kit
10. To view the status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
11. Configure the Security Access Manager Runtime package as follows:
    a. Start the configuration utility:

       ```
       pdconfig
       ```

       The Security Access Manager Configuration window is displayed.
    b. Select **Security Access Manager Runtime** and click **Configure**.

    Depending on the package that you selected, you are prompted for configuration options. For assistance with these configuration options, see Appendix D, "pdconfig options," on page 317.

Results

This step completes the setup of a Security Access Manager Web security development (ADK) system. To set up another Security Access Manager system, Follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Note: Before you install another component, open a new command-line window.

Setting up a Web security development system using the Launchpad (Windows)

Use the Launchpad installation method to install and configure the Web security development system and its prerequisite software on Windows by using a graphical user interface.

Before you begin

Ensure that you complete the following prerequisite tasks:
- "Operating system preparation" on page 28
- If you plan to use a user registry other than IBM Tivoli Directory Server, continue with Chapter 5, "User registry server installation and configuration," on page 51.

About this task

The Launchpad uses a graphical user interface to perform step-by-step installation and initial configuration.

This task installs the following components:

- IBM Global Security Kit (GSKit)
- IBM Tivoli Directory Server client
- IBM Security Utilities
- Security Access Manager License
- Security Access Manager Runtime
- Security Access Manager Web Security Runtime
- Security Access Manager Application Development Kit
- Security Access Manager Web Security Application Development Kit

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the Launchpad image files are in a directory path that does not contain any spaces.
2. Start the Launchpad.
   a. Locate the `launchpad64.exe` file.
   b. Double-click the file to start the Launchpad.
3. Select the language that you want to use during the installation.
4. Click **OK**. The Launchpad Welcome window opens.
5. Click **Next**.
6. Select the **Web Security Application Development Kit** component.
7. Click **Next**. A list displays the component that you selected and any prerequisite software that is required by that component but that is not already installed.
8. Click **Next**. An arrow next to a component name on the left indicates that component is being installed. A check mark next to a component name indicates that component is installed.
9. If the current component is IBM Global Security Kit, click **Install IBM Global Security Kit** to install it. When it completes, continue with step 10.
10. Click **Next**.
11. Respond to the prompts presented during the installation.
12. Click **Next** at the bottom of the Launchpad to continue.
13. Complete the installation.
    - If the installation fails, correct the error that is described in the error message and restart the Launchpad.
    - If the installation is successful, continue with step 14.
14. Click **Next** to start the configuration.

    Note: The configuration tool is displayed in the language that is selected for your operating system locale. If the tool is displayed in English and is not displayed in the operating system locale, review the language pack installation log at `%USERPROFILE%\ISAMLangPacksInstall.log`. Correct any errors that are reported in the log file. Then, install the language pack as described in Appendix E, "Language support installation," on page 339.
15. Click **Configure Security Access Manager**. The configuration tool opens.
16. Select the component.
17. Click **Configure**.

18. Complete the configuration. For help completing the prompts, see Appendix D, "pdconfig options," on page 317. When all installations and configurations are completed, a success or failure message is displayed.
19. Take one of the following actions:
    - If the installation completed successfully, click **Next**.
    - If the configuration failed or an error is displayed, review the log file in the default `%USERPROFILE%` location, such as `C:\Users\Administrator\LaunchPDConfigforISAM.log`.

      Make corrections as indicated by the log file. Then, configure the component by using the **pdconfig** utility at a command line or by clicking **Start** > **Programs** > **IBM Security Access Manager for Web** > **Configuration**.
20. Click **Finish** to close the Launchpad.

Setting up the Web security development system using script files

The installation and configuration scripts automate installations and perform unattended (*silent*) installations and configurations.

Use the scripts in their original state or modify them to suit the requirements of your environment.

Automating installation of a Web security development system (AIX, Linux, Solaris)

Use the script file to automate the installation of the Web security development system.

About this task

Automated installations perform unattended (*silent*) installations.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the `install_isam.sh` script file in the `scripts` directory.
3. Run the script as follows:

   ```
   ./install_isam.sh -i WebADK -d path_to_packages -a [accept|display]
   ```

   where
   - `WebADK` is the name of the component.
   - *path_to_packages* is the location of the component installation packages.

     For example, if you are installing from a DVD:

     AIX *dvd_mount_point*`/usr/sys/inst.images`

     Linux */dvd_mount_point*`/linux_x86`

     Solaris
     /dvd_mount_point`/solaris`
   - `-a [accept|display]`

     The `-a accept` option automatically accepts the license without displaying the license. The `-a display` option displays the license and you must manually accept the license.

For example, if you are installing on Linux:

```
./install_isam.sh -i WebADK -d /mnt/dvd/linux_x86 -a accept
```

The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.

4. Optional: To list the required packages without installing, use the `-l` option.

```
./install_isam.sh -l WebADK
```

What to do next

To view the status and messages in a language other than English, which is the default, install your language support package. For instructions, see "Installing language support packages for Security Access Manager" on page 340.

Automating the installation of a Web security development system (Windows)

Use the script file to automate the installation of a Web security development system on Windows.

Before you begin

The installation script uses the following default destination directories:

IBM Security Access Manager

```
C:\Program Files\Tivoli\Policy Director
```

Tivoli Directory Server client

```
C:\Program Files\IBM\ldap\V6.3
```

IBM Security Utilities

```
C:\Program Files\Tivoli\TivSecUtl
```

If you want to change these directories, you must do so before you run the script:

1. Copy *all* of the `.iss` files from the DVD or extracted archive files to a temporary directory on your computer. The files that you can modify are:

   IBM Security Access Manager

   ```
   ISAMLicense.iss
   ```

   IBM Tivoli Directory Server client

   ```
   LDAPClient.iss
   ```

   IBM Security Utilities

   ```
   IBMSecurityUtils.iss
   ```

2. Use a text editor to change the destination path in one or all three files.
3. Save the files.
4. Copy the script command file, `install_isam.bat`, from the DVD or extracted archive files into the same directory on your computer.
5. Run the script command as described in the following task.

About this task

Automated installations can perform unattended (*silent*) installations.

Attention: The installation script requires administrator privileges. Run the script file command, `install_isam.bat`, after you log in using an administrator ID or from a command window that you open with **Run as administrator**.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the `install_isam.bat` script file in the `scripts` directory. This directory is on the product DVD or in the directory where you extracted the product files. Ensure that the `.bat` file and all the `.iss` files are in the same directory.
3. Run the script as follows:

   ```
   install_isam.bat /i WebADK /d path_to_packages
   ```

   where :

   - `WebADK` is the component name.
   - *`path_to_packages`* is the path to the product DVD or the directory where you extracted the product files.

   For example, to install the Web security ADK, type:

   ```
   install_isam.bat /i WebADK /d c:\isam_images
   ```

   where `c:\isam_images` is the directory where the extracted subdirectories and product files are located. The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.
4. Optional: To list the required packages without installing, use the `/l` option.

   ```
   install_isam.bat /l WebADK
   ```

What to do next

To view the status and messages in a language other than English, which is the default, install your language support package. For instructions, see “Installing language support packages for Security Access Manager” on page 340.

Chapter 16. Setting up WebSEAL

Security Access Manager WebSEAL is a security manager for Web-based resources. WebSEAL is a high performance, multithreaded Web server that applies fine-grained security policy to the protected Web object space. Use the instructions in this section to install and configure a WebSEAL system by using the command line.

For more information about this Web security system, see the *IBM Security Access Manager for Web WebSEAL Administration Guide*.

Note: Before you install WebSEAL on an AIX system, make sure the **xlC.rte** > **xlC.aix50.rte** components are at the 8.0.0.4 level.

Complete the instructions that apply to your operating system.

Setting up a WebSEAL system using the command line

Use platform-specific command-line utilities to install the Web security development system. This method is one of several installation methods you can use.

For more information, see Chapter 2, "Installation methods," on page 19.

When you use the command-line utilities, you must manually install each component and its prerequisite software in the appropriate order.

Complete the prerequisite installations first. See Part 2, "Prerequisite software installation," on page 25.

The platform-specific installation utilities that are used are:

AIX `installp`

Linux `rpm`

Solaris
`pkgadd`

Note: If you are installing on Solaris 10 and above, use the **-G** option. The **-G** option ensures that packages are added in the current zone only. When the **-G** option is used in the global zone, the package is added to the global zone only and is not propagated to any existing or yet-to-be-created non-global zone. When used in a non-global zone, the package(s) are added to the non-global zone only.

Windows
`setup.exe`

After you complete installation, use the appropriate configuration commands.

Note: For more information about these utilities, see the *IBM Security Access Manager for Web Command Reference*.

AIX: Installing WebSEAL using the command line

Use **installp** to install the software packages and the **pdconfig** utility to configure them on AIX.

Before you begin

Complete the appropriate preinstallation tasks in Chapter 4, "Prerequisite installation and configuration roadmap," on page 27.

About this task

Attention: Before you install WebSEAL on an AIX system, make sure the **xlC.rte** and **xlC.aix50.rte** components are at the 8.0.0.4 level.

Procedure

1. Log on as **root**.
2. Ensure that all necessary operating system patches are installed. Review the most recent release information, including system requirements, disk space requirements, and known defects and limitations in the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
3. Ensure that the registry server and policy server are up and running (in normal mode).
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
5. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "AIX: Installing the IBM Global Security Kit (GSKit)" on page 35.
6. Install the IBM Directory Server client, if not already installed. For instructions, see page "AIX: Installing the IBM Tivoli Directory Server client" on page 42.
7. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
8. Install the IBM Security Utilities, if not already installed. For instructions, see page "AIX: Installing the IBM Security Utilities" on page 39.
9. Install the Security Access Manager packages:

   ```
   installp -acgYXd package_path/usr/sys/inst.images packages
   ```

   where:

   - *package_path* is the directory where the DVD is mounted or the files are located
   - *packages* are:

     PD.RTE Specifies the Security Access Manager Runtime package.

     PDWeb.RTE
     Specifies the Security Access Manager Web Security Runtime package.

     PDWeb.Web
     Specifies the Security Access Manager WebSEAL package.
10. Unmount the DVD, if used.

11. To view status and messages in a language other than English, which is the default, install your language support package *before* configuring packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
12. Configure the Security Access Manager Runtime followed by the Security Access Manager WebSEAL package as follows:
    a. Start the configuration utility:
       ```
       pdconfig
       ```
       The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure, one at a time.
       Depending on the package that you selected, you are prompted for configuration options. For assistance with these configuration options, see Appendix D, "pdconfig options," on page 317.
       When a message is displayed that indicates the package has been successfully configured, press Enter to configure another package or select the **x** option twice to close the configuration utility.

Results

This step completes the setup of a Security Access Manager WebSEAL system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Note: The Security Access Manager WebSEAL system supports multiple instances of WebSEAL on each host computer. See the *IBM Security Access Manager for Web WebSEAL Administration Guide* for information on configuring multiple instances of WebSEAL.

Linux: Installing WebSEAL using the command line

Use **rpm** to install the software packages and the **pdconfig** utility to configure them on Linux.

Before you begin

Complete the appropriate preinstallation tasks in Chapter 4, "Prerequisite installation and configuration roadmap," on page 27.

About this task

Note to Linux on System z users: You must first obtain access to the Linux `rpm` files which are in the `/package_path/linux_s390x` directory.

Procedure

1. Log on as **root**.
2. Ensure that all necessary operating system patches are installed. Review the most recent release information, including system requirements, disk space requirements, and known defects and limitations in the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
3. Ensure that the registry server and policy server are up and running (in normal mode).

4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
5. Change to the *package_path*/*distribution* directory, where:
   - *package_path* is the mount point for your DVD or file location
   - *distribution* specifies linux_x86 for x86-64 or linux_s390 for System z
6. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Linux: Installing the IBM Global Security Kit (GSKit)" on page 35.
7. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Linux: Installing the IBM Tivoli Directory Server client" on page 43.
8. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
9. Install the IBM Security Utilities, if not already installed. For instructions, see page "Linux: Installing IBM Security Utilities" on page 40.
10. Install the Security Access Manager packages:

    ```
    rpm -ihv packages
    ```

    where *packages* are:

Package	Linux on x86-64	Linux on System z
Security Access Manager Runtime package	PDRTE-PD-7.0.0-0.x86_64.rpm	PDRTE-PD-7.0.0-0.s390x.rpm
Security Access Manager Web Security Runtime package	PDWebRTE-PD-7.0.0-0.x86_64.rpm	PDWebRTE-PD-7.0.0-0.s390x.rpm
Security Access Manager WebSEAL package	PDWeb-PD-7.0.0-0.x86_64.rpm	PDWeb-PD-7.0.0-0.s390x.rpm

11. Unmount the DVD, if used.
12. To view status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
13. Configure the Security Access Manager Runtime followed by the Security Access Manager WebSEAL package as follows:
    a. Start the configuration utility:

       ```
       pdconfig
       ```

       The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure, one at a time.
       Depending on the package that you selected, you are prompted for configuration options. For assistance with these configuration options, see Appendix D, "pdconfig options," on page 317.

When a message is displayed that indicates the package was successfully configured, press Enter to configure another package or select the **x** option twice to close the configuration utility.

What to do next

This step completes the setup of a Security Access Manager WebSEAL system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Note: The Security Access Manager WebSEAL system supports multiple instances of WebSEAL on each host computer. See the *IBM Security Access Manager for Web WebSEAL Administration Guide* for information about configuring multiple instances of WebSEAL.

Solaris: Installing WebSEAL using the command line

Use the **pkgadd** to install the software packages and the **pdconfig** utility to configure them on Solaris.

Before you begin

Complete the appropriate preinstallation tasks in Chapter 4, "Prerequisite installation and configuration roadmap," on page 27.

About this task

Attention: Installations on Solaris systems should use the **-G** option with the **pkgadd** utility. The **-G** option adds the package into the current zone only.

Procedure

1. Log on as **root**.
2. Ensure that all necessary operating system patches are installed. Review the most recent release information, including system requirements, disk space requirements, and known defects and limitations in the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
3. Ensure that the registry server and policy server are up and running (in normal mode).
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Solaris: Installing the IBM Global Security Kit (GSKit)" on page 36.
6. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Solaris: Installing the IBM Tivoli Directory Server client" on page 44.
7. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
8. Install the IBM Security Utilities, if not already installed. For instructions, see page "Solaris: Installing IBM Security Utilities" on page 40.
9. Install the Security Access Manager packages (one at a time):

```
pkgadd -d package_path/solaris
  -a /package_path/solaris/pddefault -G packages
```

where:

/package_path/**solaris**
: Specifies the location of the package.

/package_path/**solaris/pddefault**
: Specifies the location of the installation administration script.

and *packages* are as follows:

PDRTE Specifies the Security Access Manager Runtime package.

PDWebRTE
: Specifies the Security Access Manager Web Security Runtime package.

PDWeb Specifies the Security Access Manager WebSEAL package.

When a message queries `Do you want to install these as setuid/setgid`, type **Y** and press Enter. When prompted to continue, type **Y** and press Enter.

When the installation process is complete for each package, the following message is displayed:

`Installation of packages successful.`

10. To view status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
11. Configure the Security Access Manager Runtime followed by the Security Access Manager WebSEAL package, as follows:
    a. Start the configuration utility:

       ```
       pdconfig
       ```

       The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure, one at a time.

       Depending on the package that you selected, you are prompted for configuration options. For assistance with these configuration options, see Appendix D, "pdconfig options," on page 317.

       When a message is displayed that indicates the package was successfully configured, press Enter to configure another package or select the **x** option twice to close the configuration utility.

Results

This step completes the setup of a Security Access Manager WebSEAL system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Note: The Security Access Manager WebSEAL system supports multiple instances of WebSEAL on each host computer. See the *IBM Security Access Manager for Web WebSEAL Administration Guide* for information about configuring multiple instances of WebSEAL.

Windows: Installing WebSEAL using the command line

Use the **setup.exe** program to install the software packages and the **pdconfig** utility to configure them on Windows.

Before you begin

Complete the appropriate preinstallation tasks in:

- "Operating system preparation" on page 28.
- Chapter 4, "Prerequisite installation and configuration roadmap," on page 27

Procedure

1. Log on as any member of the Administrators group.
2. Ensure that all necessary operating system patches are installed. Review the most recent release information, including system requirements, disk space requirements, and known defects and limitations in the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
3. Ensure that the registry server and policy server are up and running (in normal mode).
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Windows: Installing the IBM Global Security Kit (GSKit)" on page 36.
6. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Windows: Installing the IBM Tivoli Directory Server client" on page 45.
7. Install the Security Access Manager license, if not already installed. For instructions, see "Windows: Installing the IBM Security Access Manager License" on page 39.
8. Install the IBM Security Utilities, if not already installed. For instructions, see page "Windows: Installing IBM Security Utilities" on page 41.
9. Install the Security Access Manager packages. To do so, run the **setup.exe** program in the following directory:

   ```
   \windows\PolicyDirector\Disk Images\Disk1
   ```

   Follow the online instructions and select to install the following packages:

   - Security Access Manager Runtime
   - Access Manager Web Security Runtime
   - Security Access Manager WebSEAL
10. To view status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
11. Configure the Security Access Manager Runtime followed by the Security Access Manager WebSEAL package as follows:

    a. Start the configuration utility:

       ```
       pdconfig
       ```

       The Security Access Manager Configuration window is displayed.

    b. Select the **Security Access Manager Runtime** package and click **Configure**.

    c. Select the **Security Access Manager WebSEAL** package and click **Configure**.

    Depending on the package that you selected, you are prompted for configuration options. For assistance with these configuration options, see Appendix D, "pdconfig options," on page 317.

Results

This step completes the setup of a Security Access Manager WebSEAL system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Note: The Security Access Manager WebSEAL system supports multiple instances of WebSEAL on each host computer. See the *IBM Security Access Manager for Web WebSEAL Administration Guide* for information about configuring multiple instances of WebSEAL.

Setting up a WebSEAL system using the Launchpad (Windows)

Use the Launchpad installation method to install and configure the WebSEAL and its prerequisite software on Windows using a graphical user interface.

Before you begin

Ensure that you complete the following prerequisite tasks:

- "Operating system preparation" on page 28
- Chapter 5, "User registry server installation and configuration," on page 51

About this task

The Launchpad uses a graphical user interface to perform step-by-step installation and initial configuration.

This task installs the following components:

- IBM Global Security Kit (GSKit)
- IBM Tivoli Directory Server client
- IBM Security Utilities
- Security Access Manager License
- Security Access Manager Runtime
- Security Access Manager Web Security Runtime
- Security Access Manager WebSEAL

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the Launchpad image files are in a directory path that does not contain any spaces.
2. Start the Launchpad.
   a. Locate the `launchpad64.exe` file.
   b. Double-click the file to start the Launchpad.
3. Select the language that you want to use during the installation.
4. Click **OK**. The Launchpad Welcome window opens.
5. Click **Next**.
6. Select the **WebSEAL** component.
7. Click **Next**. A list displays the component that you selected and any prerequisite software that is required by that component but that is not already installed.

8. Click **Next**. An arrow next to a component name on the left indicates that component is being installed. A check mark next to a component name indicates that component is installed.
9. If the current component is IBM Global Security Kit, click **Install IBM Global Security Kit** to install it. When it completes, continue with step 10.
10. Click **Next**.
11. Respond to the prompts presented during the installation.
12. Click **Next** at the bottom of the Launchpad to continue.
13. Complete the installation.
    - If the installation fails, correct the error that is described in the error message and restart the Launchpad.
    - If the installation is successful, continue with step 14.
14. Click **Next** to start the configuration.

    Note: The configuration tool is displayed in the language that is selected for your operating system locale. If the tool is displayed in English and is not displayed in the operating system locale, review the language pack installation log at `%USERPROFILE%\ISAMLangPacksInstall.log`. Correct any errors that are reported in the log file. Then, install the language pack as described in Appendix E, "Language support installation," on page 339.
15. Click **Configure Security Access Manager**. The configuration tool opens.
16. Select the component.
17. Click **Configure**.
18. Complete the configuration. For help completing the prompts, see Appendix D, "pdconfig options," on page 317. When all installations and configurations are completed, a success or failure message is displayed.
19. Take one of the following actions:
    - If the configuration completed successfully, click **Next**.
    - If the configuration failed or an error is displayed, review the log file in the default `%USERPROFILE%` location, such as `C:\Users\Administrator\LaunchPDConfigforISAM.log`.

      Make corrections as indicated by the log file. Then, configure the component by using the **pdconfig** utility at a command line or by clicking **Start** > **Programs** > **IBM Security Access Manager for Web** > **Configuration**.
20. Click **Finish** to close the Launchpad.

Setting up the WebSEAL system using script files

The installation and configuration scripts automate installations and perform unattended (*silent*) installations and configurations.

Use the scripts in their original state or modify them to suit the requirements of your environment.

Automating installation of a WebSEAL system (AIX, Linux, Solaris)

Use the script file to automate the installation of the WebSEAL system.

About this task

Automated installations perform unattended (*silent*) installations.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the `install_isam.sh` script file in the `scripts` directory.
3. Run the script as follows:

   ```
   ./install_isam.sh -i WebSEAL -d path_to_packages -a [accept|display]
   ```

   where
   - `WebSEAL` is the component name.
   - *`path_to_packages`* is the location of the component installation packages.

     For example, if you are installing from a DVD:

     AIX *`dvd_mount_point`*`/usr/sys/inst.images`

     Linux x86-64
     `/dvd_mount_point``/linux_x86`

     Linux on System z
     `/dvd_mount_point``/linux_s390`

     Solaris
     `/dvd_mount_point``/solaris`
   - `-a [accept|display]`

     The `-a accept` option automatically accepts the license without displaying the license. The `-a display` option displays the license and you must manually accept the license.

   For example, if you are installing on Linux x86-64:

   ```
   ./install_isam.sh -i WebSEAL -d /mnt/dvd/linux_x86 -a accept
   ```

   The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.
4. Optional: To list the required packages without installing, use the `-l` option.

   ```
   ./install_isam.sh -l WebSEAL
   ```

Automating the installation of a WebSEAL system (Windows)

Use the script file to automate the installation of a WebSEAL system on Windows.

Before you begin

The installation script uses the following default destination directories:

IBM Security Access Manager
`C:\Program Files\Tivoli\Policy Director`

Tivoli Directory Server client
`C:\Program Files\IBM\ldap\V6.3`

IBM Security Utilities
`C:\Program Files\Tivoli\TivSecUtl`

If you want to change these directories, you must do so before you run the script:

1. Copy *all* of the `.iss` files from the DVD or extracted archive files to a temporary directory on your computer. The files that you can modify are:

   IBM Security Access Manager
   `ISAMLicense.iss`

   IBM Tivoli Directory Server client
   `LDAPClient.iss`

   IBM Security Utilities
   `IBMSecurityUtils.iss`
2. Use a text editor to change the destination path in one or all three files.
3. Save the files.
4. Copy the script command file, `install_isam.bat`, from the DVD or extracted archive files into the same directory on your computer.
5. Run the script command as described in the following task.

About this task

Automated installations can perform unattended (*silent*) installations.

Attention: The installation script requires administrator privileges. Run the script file command, `install_isam.bat`, after you log in using an administrator ID or from a command window that you open with **Run as administrator**.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the `install_isam.bat` script file in the `scripts` directory. This directory is on the product DVD or in the directory where you extracted the product files. Ensure that the `.bat` file and all the `.iss` files are in the same directory.
3. Run the script as follows:
   ```
   install_isam.bat /i WebSEAL /d path_to_packages
   ```

   where:
   - `WebSEAL` is the component name.
   - *`path_to_packages`* is the path to the product DVD or the directory where you extracted the product files.
   - For example, to install the WebSEAL component, type:
     ```
     install_isam.bat /i WebSEAL /d c:\isam_images
     ```

     where `c:\isam_images` is the directory where the extracted subdirectories and product files are located.

   The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.
4. Optional: To list the required packages without installing, use the `/l` option.
   ```
   install_isam.bat /l WebSEAL
   ```

Automating configuration of a WebSEAL system

Use the script file to automate the configuration of a WebSEAL system.

Before you begin

- Complete the installation of the Web Portal Manager. See:
  - "Automating installation of a WebSEAL system (AIX, Linux, Solaris)" on page 255
  - "Automating the installation of a WebSEAL system (Windows)" on page 256
- To view status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.

If you are running this script on Windows, open a new command window. Do not perform this task in the same window where you ran the installation script.

About this task

Automated configuration performs an unattended (*silent*) configuration.

Procedure

1. Create an options file for the component you want to configure.
   a. Locate the options file template for the component.

      AIX, Linux, or Solaris

      ```
      /opt/PolicyDirector/example/config/
      configure_webseal.options.template
      ```

      Windows

      ```
      C:\Program Files\Tivoli\PDWeb\etc\
      configure_webseal.options.template.cmd
      ```

   b. Copy the file to a temporary directory. You can copy the file to the temporary directory with a name that is unique to your environment.

      Attention: You must keep the `.cmd` extension for Windows template files. The Windows template files run as commands.

   c. Modify the content of the file to specify settings for your environment. The comments in the file explain the settings and provide examples.

   d. Save the file.
2. Optional: By default, passwords you specified in the options files are stored in clear text. To obfuscate these passwords:
   a. Copy the `configure_isam.conf` file to the same directory where you copied the options files. The file is in the following locations:

      AIX, Linux, or Solaris

      ```
      /opt/PolicyDirector/example/config/
      ```

      Windows

      ```
      C:\Program Files\Tivoli\Policy Director\example\config\
      ```

   b. See Appendix F, "Password management," on page 351 for instructions on using the `-obfuscate` option with the `pdconf` tool to obfuscate the passwords in the options files. For more information about `pdconf`, see the *IBM Security Access Manager for Web Command Reference*.

   c. Return to these instructions to run the configuration script.
3. Copy the script file from its original location to the same directory where you copied the options file. The script files are in the following locations:

   AIX, Linux, or Solaris

   Directory: `/opt/PolicyDirector/example/config/`

File name: `configure_isam.sh`

Windows

Directory: `C:\Program Files\Tivoli\Policy Director\example\config\`

File name: `configure_isam.cmd`

4. Run the configuration script and use the options file for input.

   AIX, Linux, or Solaris

   ```
   ./configure_isam.sh -f options_file
   ```

   Windows

   ```
   configure_isam.cmd -f options_file.cmd
   ```

   where *options_file* is the text file that contains the configuration options. For example:

   AIX, Linux, or Solaris

   ```
   ./configure_isam.sh -f my_configure_webseal.options
   ```

   Windows

   ```
   configure_isam.cmd -f my_configure_webseal.options.cmd
   ```

Part 5. Session management system component installation

Chapter 17. Setting up a session management server

The session management server is an optional component of Security Access Manager. It runs as a service of the IBM WebSphere Application Server.

Before you begin, review the following information about the session management server:

- The session management server can manage and monitor sessions across dispersed, clustered Web servers.
- If you want to set up and configure cluster members to be part of a node group that represents a WebSphere eXtreme Scale zone, complete the task before you deploy and configure the SMS. For details, see the WebSphere eXtreme Scale discussion in the *IBM Security Access Manager for Web Shared Session Management Administration Guide*.
- Using the session management server allows for the Security Access Manager WebSEAL and Security Access Manager Plug-in Web Servers components to share a unified view of all current sessions. Session management server permits any authorized user to monitor and administer user sessions.
- The session management server records various session information, including: session inactivity and lifetime timeout information, login activity, and concurrent log in information. The session management server records session statistics information, such as the number of users that are currently logged in.
- The extent of a session within the cluster is known as the *session realm*. The session management server can provide a seamless single sign-on experience across the session realm. Configure by adding or removing session realms.
- The session management server ensures that session policy remains consistent across clusters of Web security servers. *Replica sets* within a session realm share the Security Access Manager registry and policy database.
- To configure the session management server system, use the **smscfg** utility. Run the command from the system where the session management server is installed.
- You can administer the session management server either by using any (or all) of the following tools:

  pdadmin
  : Is installed as part of the Security Access Manager Runtime package. Use this interface to manage access control lists, groups, servers, users, objects, and other resources in your secure domain. You can also automate certain management functions by writing scripts that use **pdadmin** commands.

  pdsmsadmin
  : Uses the SOAP protocol to communicate directly with a session management server installed on WebSphere Application Server.

  The session management server console
  : A graphical user interface on the WebSphere Application Server that is installed as an extension to the administrative console.

For more information about distributed sessions management, see the *IBM Security Access Manager for Web Shared Session Management Administration Guide*.

Complete the instructions that apply to your operating system.

Preinstallation requirements

Before you install and configure a Security Access Manager session management server, you must perform several preinstallation tasks.

These requirements are applicable, regardless of which installation method you plan to use.

- Complete the appropriate tasks in "Operating system preparation" on page 28.
- Complete the appropriate tasks in Chapter 4, "Prerequisite installation and configuration roadmap," on page 27
- When you deploy the session management server to a cluster, the ObjectGrid toolkit automatically deploys to handle the distribution and management of session data between the different nodes within the cluster. The installation of this toolkit requires approximately 600 MB of disk space on the partitions which hold the WebSphere installation for each node. If you intend to deploy the session management server to a cluster, ensure that you have adequate disk space to install the ObjectGrid toolkit.
- If the IBM WebSphere Application Server is installed, the session management server can be run as a service. The IBM WebSphere Application Server can also be installed as a stand-alone server, and the session management server can be deployed to an application server or to a cluster.
- A Security Access Manager environment must exist before you install the session management server.
- After you install the session management server, you must reconfigure the Security Access Manager WebSEAL, or Security Access Manager Plug-in for Web Servers (or both) to use the session management server for managing sessions.
- The structure of your session realms and associated replica set must be planned and mapped.
- Determine whether you want to replicate session management server instances that provide failover capability and improved performance.
- If you want to administer the session management system by using the **pdadmin** utility, install and configure an instance of the Security Access Manager authorization server.
- If WebSphere Application Server is running as a non-root user on an AIX, Linux, or Solaris system, the following steps must be completed:
  - As the root user, grant the WebSphere user write permission to the following directories (and all subdirectories) in the WebSphere Application Server base installation directory:

    ```
    deploytool
    java
    lib
    ```

    These permissions can be removed after the session management server is configured.
  - If Tivoli Common Directory is being enabled on the system for the first time, as the root user, create the following directories and grant the WebSphere user permission to create subdirectories in them:

    ```
    /etc/ibm
    /var/ibm
    ```
  - If Tivoli Common Directory is enabled, grant the WebSphere user write access to the base log directory, such as `/var/ibm/tivoli/common`.

    This permission can be removed after the session management server is configured.

  - If Tivoli Common Directory is enabled, grant the WebSphere user write access to the session management server log subdirectory, `CTGSM`, in the base log directory.
- Decide whether you want to enable WebSphere global security to ensure that administration actions are secured.

  See the information in the topics about setting up and enabling security in WebSphere Application Server information center at:

  http://www.ibm.com/software/webservers/appserv/was/library/
- If WebSphere global security is enabled, create three groups in WebSphere Application Server that can be used to manage the session management server environment:
  - A group for administrators, for example: **sms-administrators**
  - A group for delegators for example: **sms-delegators**
  - A group for clients, for example: **sms-clients**

  The group names must follow the naming conventions of the user registry that is used by WebSphere Application Server. You can use existing groups for this purpose.
- Determine whether you want to enable Secure Sockets Layer (SSL) for session management server communications. You can enable SSL between the Security Access Manager servers in the replica set and the IBM WebSphere Application Server where the session management server is installed.
- If you plan to use Security Access Manager certificates to authenticate with SMS, or if you want to use the Security Access Manager sec_master user (or other users and groups that are defined in the `secAuthority=Default` suffix) to administer SMS by using either the session management command line or console, then you must unconfigure the base DN in the LDAP user registry that is used by WebSphere Application Server.

  Information about modifying the base DN for the WebSphere Application Server user registry can be found in the topics about configuring Lightweight Directory Access Protocol user registries in the WebSphere Application Server information center at:

  http://www.ibm.com/software/webservers/appserv/was/library/

Setting up the session management server using the command line

Use platform-specific command-line utilities to install the session management server. This method is one of several installation methods you can use.

For more information, see Chapter 2, “Installation methods,” on page 19.

When you use the command-line utilities, you must manually install each component and its prerequisite software in the appropriate order.

Complete the prerequisite installations first. See Part 2, “Prerequisite software installation,” on page 25.

The platform-specific installation utilities that are used are:

AIX **`installp`**

Linux **`rpm`**

Solaris

pkgadd

Note: Installations on Solaris systems should use the **-G** option with the **pkgadd** utility. The **-G** option adds the package into the current zone only. When the **-G** option is used in the global zone, the package is added to the global zone only and is not propagated to any existing or yet-to-be-created non-global zone. When used in a non-global zone, the package(s) are added to the non-global zone only.

Windows

setup.exe

After installation completes, use the appropriate configuration commands.

Note: For more information about these utilities, see the *IBM Security Access Manager for Web Command Reference*.

AIX: Installing a session management server system

Setting up a session management server system on AIX is a three-part process that consists of installation, deployment to the application server or cluster, and configuration.

Procedure

1. Log on as **root**.
2. Perform the preinstallation tasks as listed in "Preinstallation requirements" on page 264.
3. Ensure that the registry server and policy server are up and running (in normal mode).
4. Install the IBM WebSphere Application Server. For instructions, see "Installing WebSphere Application Server" on page 46.
5. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
6. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
7. Install the following Security Access Manager packages:

   `installp -acgYXd` *`package_path`*`/usr/sys/inst.images` *`packages`*

   where:

   - *`package_path`* is the directory where the DVD is mounted or the files are located
   - *`packages`* are:

     `PD.SMS` Specifies the Security Access Manager Session Management Server package.
8. Unmount the DVD, if used.
9. If you are intending to use a DB2 database to store login history information, you must create the database as described in "Creating the login history database" on page 269.

What to do next

If you intend to use a DB2 database to store login history information, create the database before you deploy the Session Management Server application. See "Creating the login history database" on page 269. Otherwise, continue with "Deploying the Session Management Server application" on page 273 and "Configuring the session management server" on page 274.

Linux: Installing a session management server system

Setting up a session management server system on Linux is a three-part process that consists of installation, deployment to the application server or cluster, and configuration.

About this task

Note to Linux on System z users: You must first obtain access to the Linux `rpm` files which are in the */package_path*`/linux_s390` directory.

Procedure

1. Log on as **root**.
2. Ensure that the registry server and policy server are up and running (in normal mode).
3. Install the IBM WebSphere Application Server. For instructions, see "Installing WebSphere Application Server" on page 46.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
5. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
6. Change to the *package_path*`/`*distribution* directory

   where:

   - *package_path* is the mount point for your DVD or file location
   - *distribution* specifies `linux_x86` for x86-64 or `linux_s390` for System z
7. Install the Security Access Manager packages:

   `rpm -ihv` *packages*

   where *packages* are:

Package	Linux on x86-64	Linux on System z
Security Access Manager Session Management Server package	`PDSMS-PD-7.0.0-0.x86_64.rpm`	`PDSMS-PD-7.0.0-0.s390.rpm`

8. Unmount the DVD, if used.
9. If you are intending to use a DB2 database to store login history information, you must create the database as described in "Creating the login history database" on page 269.

What to do next

If you intend to use a DB2 database to store login history information, create the database before you deploy the Session Management Server application. See "Creating the login history database" on page 269. Otherwise, continue with "Deploying the Session Management Server application" on page 273 and "Configuring the session management server" on page 274.

Solaris: Installing a session management server system

Setting up a session management server system on Solaris is a three-part process that consists of installation, deployment to the application server or cluster, and configuration.

About this task

The following procedure uses **pkgadd** to install software packages.

Attention: Installations on Solaris systems should use the **-G** option with the **pkgadd** utility. The **-G** option adds the package into the current zone only.

Procedure

1. Log on as **root**.
2. Perform the preinstallation tasks as listed in "Preinstallation requirements" on page 264.
3. Ensure that the registry server and policy server are up and running (in normal mode).
4. Install the IBM WebSphere Application Server. For instructions, see "Installing WebSphere Application Server" on page 46.
5. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
6. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
7. Install the Security Access Manager packages:

   `pkgadd -d /package_path/solaris -a /package_path/solaris/pddefault -G packages`

   where:

   /*package_path*/solaris
   Specifies the location of the package.

   /*package_path*/solaris/pddefault
   Specifies the location of the installation administration script.

   and *packages* are:

   PDSMS Specifies the Security Access Manager Session Management Server package.

   When the installation process is complete for each package, the following message is displayed:

   `Installation of package successful.`
8. If you are intending to use a DB2 database to store login history information, you must create the database as described in "Creating the login history database" on page 269.

What to do next

If you intend to use a DB2 database to store login history information, create the database before you deploy the Session Management Server application. See "Creating the login history database." Otherwise, continue with "Deploying the Session Management Server application" on page 273 and "Configuring the session management server" on page 274.

Windows: Installing a session management server system

Setting up a session management server system is a three-part process that consists of installation, deployment to the application server or cluster, and configuration.

Procedure

1. Log on as any member of the Administrators group.
2. Perform the preinstallation tasks as listed in "Preinstallation requirements" on page 264.
3. Ensure that the registry server and policy server are up and running (in normal mode).
4. Install the IBM WebSphere Application Server. For instructions, see "Installing WebSphere Application Server" on page 46.
5. Install the Security Access Manager license, if not already installed. For instructions, see "Windows: Installing the IBM Security Access Manager License" on page 39.
6. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
7. Install the Security Access Manager Session Management Server package. To do so, run the **setup.exe** program in the following directory: `\windows\PolicyDirector\Disk Images\Disk1`
   Follow the online instructions and select **Access Manager Session Management Server**.
8. If you are intending to use a DB2 database to store login history information, you must create the database as described in "Creating the login history database."

What to do next

If you intend to use a DB2 database to store login history information, create the database before you deploy the Session Management Server application. See "Creating the login history database." Otherwise, continue with "Deploying the Session Management Server application" on page 273 and "Configuring the session management server" on page 274.

Creating the login history database

If you intend to use a DB2 database to store login history information, you must create the database before you deploy the Session Management Server application.

About this task

If you are not planning to use a DB2 database, continue with "Deploying the Session Management Server application" on page 273.

Procedure

1. A user on the DB2 database server system must own the DB2 database. Create a user on the system and setup that user with a valid password. If consistent with the security policy for your organization, you might choose to indicate that the password never expires. For example, you might call this user `isamloginuser`.
2. Create a database in DB2. For example, you might call the database `isamLOGIN`. Configure the database to permit TCP/IP connections on port `50000`.
3. Open the **DB2 Control Center** and locate your database.
4. Click **User and Group Objects** > **DB Users** and then click **Add New User**.
5. Add the user and grant the authorities of **Connect to database** > **Create tables**.
6. Click **OK**.
7. Configure WebSphere Application Server to access the database.

   Information about performing this task can be found in the WebSphere Application Server information center for the version you are using:

   http://www.ibm.com/software/webservers/appserv/was/library/

   Specifically, see the following tasks:

   - Creating and configuring a JDBC provider and data source
   - Vendor-specific data sources minimum required settings
8. Make the IBM DB2 JDBC driver available to WebSphere Application Server by copying the `db2jcc.jar` and `db2jcc_license_cu.jar` files from the DB2 directory tree to the `lib` directory of your application server.

   AIX, Linux, and Solaris
   `/opt/IBM/WebSphere/AppServer/lib`
9. Verify that the IBM JDBC driver works in WebSphere by changing to the `lib` subdirectory and entering the following command:

   ```
   java -classpath db2jcc.jar com.ibm.db2.jcc.DB2Jcc -version
   ```
10. Open the WebSphere Application Server administrative console and log in, if necessary.
11. Click **Environment** > **WebSphere Variables**.
12. Set the `DB2UNIVERSAL_JDBC_DRIVER_PATH` variable to the directory where the `db2jcc.jar` file is located. Save your changes.
13. Log out of the WebSphere Application Server administrative console.
14. Restart your application servers. If you use WebSphere Application Server Network Deployment, you also must restart the deployment manager and node manager.
15. Open the WebSphere Application Server administrative console and log in again.
16. Click **Resources** > **JDBC Providers**.
17. In a single server environment, select your application server node; in WebSphere Application Server Network Deployment, select your cluster.
18. Click **New** to create a JDBC provider.
19. In the **Database type** field, select DB2 and specify the following information:

    Provider type
    DB2 Universal JDBC Driver Provider

    Implementation type
    Connection pool data source

20. Click **Next** to continue.
21. On the JDBC Providers Summary page, click **Apply** to accept the default settings.

    Do not restart WebSphere Application Server now.
22. On the JDBC Providers page, select DB2 Universal JDBC Provider.
23. Click **Data sources**.
24. Click **New** to create a data source and specify the following information:

    Database name
    isamLOGIN

    Driver type
    4

    Server name
    host_name_of_DB2_system

    Port number
    50000
25. Click **Apply**. You are returned to the previous page.
26. On the JDBC Providers page, select DB2 Universal JDBC Driver DataSource.
27. Click **Related items** and then click **J2EE Connector Architecture (J2C) authentication data entries**.
28. Click **New** to create an authentication data entry and specify the following information:

    Alias logindbuser

    User ID
    isamloginuser

    Password
    password_for_isamloginuser

    Description
    Access to login History Database
29. Click **Apply**. You are returned to the previous page.
30. Return to the DB2 Universal JDBC Driver data source properties and under **Component managed authentication alias**, select the `logindb2user` alias.
31. Click **Apply**.
32. Log off from the WebSphere Application Server administrative console.
33. Restart your application servers. If you use WebSphere Application Server Network Deployment, you also must restart the deployment manager and node manager.
34. Open the WebSphere Application Server administrative console and log in again.
35. Click **Resources** > **JDBC Providers** > **DB2 Universal JDBC Driver Provider** > **Data Sources**.
36. Select your data source and click **Test connection**. If the test is not successful, diagnose and correct the problem. Otherwise, continue with "Deploying the Session Management Server application" on page 273.

Deploying the console extension

The Session Management Server console extension is a graphical user interface (GUI) that can deploy, configure, and administer the Session Management Server.

After you install the session management server by using native installation utilities, you can deploy the console by using the **smscfg** utility.

About this task

Note: The following instructions assume that you are running the **smscfg** utility in interactive mode.

To deploy the ISC extension by using the **smscfg** utility. This utility is in the following locations by default:

AIX, Linux, or Solaris:

```
/opt/pdsms/bin
```

Windows:

```
C:\Program Files\Tivoli\PDSMS\bin
```

See the *IBM Security Access Manager for Web Shared Session Management Administration Guide* for more detailed deployment information.

Procedure

1. Before you run **smscfg**, run the WebSphere `setupCmdLine.bat` (on Windows) or `setupCmdLine.sh` (on AIX, Linux, or Solaris) script.
2. Deploy the console by using the configuration utility:

   ```
   smscfg -action deploy
   ```
3. When prompted, specify `ISC` as the instance name.

What to do next

Continue with "Logging in and logging out of the Session Management Server console."

Logging in and logging out of the Session Management Server console

Access the IBM Security Access Manager Session Management Server console by opening a web browser and typing the appropriate URL.

Before you begin

To form the appropriate URL, you need to know the settings for the console. For example, the URL might be: `https://isam.example.com:9043/ibm/console`

This URL consists of:

- The name of the host system that runs the console.
- The port number of the console. The port for the Session Management Server console is the same one as the console of the hosting WebSphere Application Server.
- The URL for accessing the console login page. This part of the URL is always the same:

  ```
  /ibm/console
  ```

After you establish the correct URL, you must know the administrator user name and password for the console. The name and password were specified during configuration.

Procedure

1. Enter the console URL in the address bar of your browser. For example, for the URL of a system with a host name of `isam.example.com` and the default port number, enter:

   `https://isam.example.com:9043/ibm/console`
2. Enter the administrator ID and password. The console Welcome panel is displayed.
3. Use the navigation links on the left to view and work with the console tasks.

   Attention: Do not use the **Back** button in your browser to move in the console.
4. To log out, click **Logout** in the upper right corner of the panel.

Deploying the Session Management Server application

After completing installation of the session management server by using native installation utilities, deploy the `DSess.ear` file by using the **smscfg** utility or by using the Session Management Server console.

Deploying using the smscfg utility

You can deploy the application using the **smscfg** utility.

About this task

Note: The instructions in this section assume that you are running the **smscfg** utility in interactive mode.

Procedure

1. Before running **smscfg** run the WebSphere `setupCmdLine.bat` (on Windows) or `setupCmdLine.sh` (on AIX, Linux, or Solaris) script.
2. Deploy the Session Management Server application using the configuration utility: `smscfg -action deploy`
   See the *IBM Security Access Manager for Web: Shared Session Management Administration Guide* for detailed deployment information.

Deploying using the Session Management Server console

You can deploy an instance of the Session Management Server application using the Session Management Server console.

About this task

Note: To use the console to deploy the Session Management Server, you must first deploy the console extension. See "Deploying the console extension" on page 271 for more information.

See the *IBM Security Access Manager for Web: Shared Session Management Administration Guide* for detailed deployment information.

Procedure

1. Log in to the session management server console as the Session Management Server administrator. See "Logging in and logging out of the Session Management Server console" on page 272 for assistance.
2. Select **Session Management Server** > **Deployment**.
3. In the **Application name** field, enter the name of the Session Management Server application. This field is required.

4. Enter the WebSphere Application Server cell element to deploy the Session Management Server instance to in the **Target** field.
5. In the **Virtual host** field, enter the web server virtual hosts that will service the Session Management Server application instance.
6. Enter the data source to use with the Session Management Server application instance in the **Data source** field.
7. When you are ready to deploy, click **Deploy**.

Configuring the session management server

After you install the session management server using native utilities and deploying the DSess.ear application, you can configure the session management server using the **smscfg** utility or the Session Management Server console.

Configuring the session management server using the `smscfg` utility

You can configure the session management server using the **smscfg** utility.

Procedure

1. Run the IBM WebSphere Application Server **`setupCmdLine`** script to set up the correct execution environment for running the session management server configuration tool. The **`setupCmdLine`** script is in the IBM WebSphere Application Server `bin` directory of the profile you are using. For example:

   AIX, Linux, or Solaris

   `/app_server_root/application_server``/bin/setupCmdLine.sh`

   Windows

   `app_server_root``\bin\setupCmdLine.bat`

   where *`app_server_root`* is the location of your WebSphere Application Server profile.
2. To view status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
3. Configure the Security Access Manager Session Management Server package using the configuration utility:

   ```
   smscfg -action config
   ```

   See the *IBM Security Access Manager for Web Shared Session Management Administration Guide* for detailed configuration information.

Results

This step completes the setup of a Security Access Manager session management server system. After configuration of the session management server, you must configure the Security Access Manager WebSEAL, or Security Access Manager Plug-in for Web Servers (or both) to use the session management server for managing sessions. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Configuring the session management server using the console

Before you can use the session management server, you must configure it. You can configure it using the Session Management Server console.

Procedure

1. Configure session realms:
   a. Log in to the Session Management Server console as the Session Management Server administrator. See "Logging in and logging out of the Session Management Server console" on page 272 for assistance.
   b. Select **Session Management Server** > **Configuration**.
   c. Select the Session Management Server instance that you want to configure.

      Note: If you deployed or started an instance and it does not display in the list of Session Management Server instances, click **Update SMS instance list**.
   d. Click **Configure**.
   e. Select **Session Realms**.
   f. Select whether enforcement of session limit and displacement policy is enabled.
   g. In the **Session realm name** field, enter the name of the session realm that is being configured.
   h. Select the **Limit maximum session for this session realm** check box to limit the maximum number of simultaneous sessions that is stored in this session realm. Enter the maximum number of simultaneous sessions to be stored in the Maximum sessions field.
   i. When you enter the session realm information, click **Update session realms**. The session realm table is updated with the configuration values you specified.
   j. To create a replica set, select the session realm name from the **Session realm name** drop-down menu.
   k. Specify the name of the replica that is set being configured in the **Replica set name** field.
   l. Click **Update replica sets** to update the replica set table with the replica set values you specified.
2. Click **Database storage**. If you want the Session Management Server to store session information in a database select the **Enable the database storage** check box.
3. Click **IBM Security Access Manager integration**. Specify whether Security Access Manager integration is enabled. To enable Security Access Manager integration, select the **Enable Security Access Manager integration check box**.
4. Click **Last login recording**. Specify whether recording of last login information is enabled. To enable recording of last login information, select the **Enable recording of last login information** check box.
5. Click **TCD logging**. To configure Tivoli Common Directory (TCD) logging, specify the following information:
   - Select the **Enable Tivoli Common Directory logging** check box to enable Tivoli Common Directory logging.
   - Specify a directory to use as the Tivoli Common Directory in the **Log directory** field. If a Tivoli Common Directory is already configured on this machine, this value is not used. The configured Tivoli Common Directory is used instead.
6. Click **Auditing**. Specify whether auditing is enabled. To enable auditing, select the **Enable auditing check box**.
7. Click **Timeout**s. Specify the client idle timeout and key lifetime:

- Enter the length of time, in seconds, after which a client is considered idle. This applies only if the client is not actively requesting updates from the Session Management Server.
- Enter the number of days, calculated from the generation of a session signing key, after which the Session Management Server automatically generates a new session signing key.

8. Click **Summary**. Review the configuration options that you selected.
9. When you are ready to configure, click **Finish**.

   This step completes the setup of a Security Access Manager session management server system.

What to do next

After configuration of the session management server, you must configure the Security Access Manager WebSEAL, or Security Access Manager Plug-in for Web Servers (or both) to use the session management server for managing sessions. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

See the *IBM Security Access Manager for Web Shared Session Management Administration Guide* for detailed configuration information.

Setting up a session management server with the Launchpad (Windows)

Use the Launchpad installation method to install and configure the session management server software on Windows. The Launchpad is a graphical user interface.

Before you begin

Complete the following prerequisite tasks:

- "Operating system preparation" on page 28
- If you plan to use a user registry other than IBM Tivoli Directory Server, complete the instructions in Chapter 5, "User registry server installation and configuration," on page 51.
- Review the introduction to the *IBM Security Access Manager for Web Shared Session Management Administration Guide*. The introduction describes the features of the session management server. It also presents several deployment and security considerations that are important to review before you install the session management server.

About this task

Use the Launchpad graphical user interface to complete step-by-step installation and initial configuration of the following components:

- IBM WebSphere Application Server
- Security Access Manager License
- Security Access Manager Session Management Server

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage. You need the files for the following products:
   - WebSphere Application Server
   - Installation Manager
   - IBM Security Access Manager

   Attention: The image files must be in a directory path that does not contain any spaces.
2. Start the Launchpad.
   a. Locate the `launchpad64.exe` file.
   b. Double-click the file to start the Launchpad.
3. Select the language to use for the installation.
4. Click **OK** The Launchpad Welcome window opens.
5. Click **Next**.
6. Select the **Session Management Server** component.
7. Click **Next**. A list displays the component that you selected and any prerequisite software that is required by that component but that is not already installed.
8. Take one of the following actions:
   - If WebSphere Application Server is already installed, go to step 9 on page 279.
   - If WebSphere Application Server is not installed:
     a. Click **Install WebSphere Application Server Components**.
     b. Select the path to the IBM Installation Manager image.

        Note: The path to the Installation Manager image is restricted in length to 172 characters or less.
     c. Click **OK**.

        Note: After Installation Manager is installed, there is a 30-second delay before it opens and begins the WebSphere Application Server installation.
     d. In the Installation Manager console, click **Install** to begin the WebSphere Application Server installation.
     e. Click **File** > **Preferences**.
     f. Select **Repositories**.
     g. Click **Add Repository**.
     h. Select the location of the `repository.config` file in the WebSphere Application Server image.
     i. Click **OK**.
     j. Click **Install**. Complete the installation as prompted. The default selections that are provided by the IBM WebSphere Application Server installation program are sufficient for IBM Security Access Manager.
        – If the installation is successful, a list of the installed packages and a prompt for starting the Profile Management Tool is displayed. Continue with 8k on page 278.

– If the installation of Installation Manager or WebSphere Application Server fails or an error is displayed, review the log files and complete the actions that they indicate. The files are in the default `%USERPROFILE%` location, such as `C:\Users\Administrator\`.

Installation Manager logs

`IMInstall.log`

`IMInstallLog.xml`

WebSphere Application Server installation log

`LaunchIMforWAS.log`

k. Select **Profile Management Tool to create a profile**.

l. Click **Finish**.

m. Click **Create**. You are prompted for several configuration settings for the WebSphere Application Server profile.

Note: Among these settings is WebSphere Application Server administrative security. To enable SSL on the WebSphere Application Server, select the **Enable administrative security** check box and complete the **User name** and **Password** fields. Make a note of these settings to use in step 14 on page 279.

n. Start the First Steps tool and click **Start the server**. The `open for e-business` message is displayed.

o. Close the following windows:
   – First Steps
   – WebSphere Customization Toolbox

p. Install the latest fix pack for your installation. See the hardware and software requirements page of the IBM Security Access Manager information center for the minimum fix pack level required.

q. Locate the fix pack on the WebSphere Application Server web-based repository or download the package and install it from a local repository.
   – To install it from the web-based repository:
     1) Click **Update** on the IBM Installation Manager window.
     2) Select **IBM WebSphere Application Server Network Deployment V8.0**.
     3) Click **Next**. Continue with the installation.
   – To install it from a local repository:
     1) Locate the fix pack on the WebSphere Application Server Support page: http://www.ibm.com/support/docview.wss?uid=swg27004980
     2) Download the fix pack into a local repository.
     3) Click **Update**.
     4) Select **IBM WebSphere Application Server Network Deployment V8.0**.
     5) Click **Next**. Continue with the installation. Use the accompanying readme file from the WebSphere Application Server Support page for assistance.

r. Start the IBM WebSphere Application Server.
   1) Click **Start** > **Administrative Tools** > **Services**.
   2) Select the IBM WebSphere Application Server that was added.

3) Right-click the service and click **Start**.

s. Close the IBM Installation Manager window.

t. Return to the Launchpad window.

9. Click **Next**. The installation panel for the next component that is listed is displayed.
   - An arrow next to a component name on the left indicates that component is being installed.
   - A check mark next to a component name indicates that component is installed.
10. Click **Next**. The installation of the first component begins.
11. Respond to the prompts presented during the installation.
12. Click **Next** at the bottom of the Launchpad to continue.
13. Complete the installation.
    - If the installation fails, correct the error that is described in the error message and restart the Launchpad.
    - If the installation is successful, continue with step 14.
14. Specify the WebSphere Application Server security settings. By default, the **SSL is enabled on the IBM WebSphere Application Server** check box is selected.
    - If SSL is not enabled on the WebSphere Application Server, clear the check mark. Then, click **Next**.
    - If SSL is enabled on the WebSphere Application Server, specify the SSL settings. Then, click **Next**. The settings that you are prompted for were configured during the creation of the WebSphere Application Server profile:

      WebSphere Application Server Administrator ID
      The identifier for an administrator account for the IBM WebSphere Application Server.

      WebSphere Application Server Administrator Password
      The password for the specified IBM WebSphere Application Server administrator ID.

      SSL truststore file
      The truststore file. Browse and choose the file. For example:
      ```
      C:\Program Files (x86)\IBM\WebSphere\AppServer\profiles\
        AppSrv01\etc\trust.p12
      ```

      SSL truststore password
      The password for the truststore. The default password is `WebAS`.

      SSL key file
      The key file. Browse and choose an existing key file. For example:
      ```
      C:\Program Files (x86)\IBM\WebSphere\AppServer\profiles\
        AppSrv01\etc\key.p12
      ```

      SSL key file password
      The password for the key file. The default password is `WebAS`.
15. Click **Next**.
16. Click **Deploy Session Management Server console**.
    - If the deployment completed successfully, click **Next**.
    - If the deployment failed or an error is displayed:

      a. Review the log file in the default `%USERPROFILE%` location, such as `C:\Users\Administrator\deploySMSconsole.log`.

b. Make corrections as indicated by the log file.
c. Either click **Deploy Session Management Server console** or run the **smscfg.bat** command.

   This file is in the *installation_directory*\bin\ directory, where *installation_directory* is the directory where you installed the component, for example, C:\Program Files\Tivoli\PDSMS. See the *IBM Security Access Manager for Web Command Reference* for more details about the **smscfg.bat** command.

17. Click **Finish** to close the Launchpad.
18. Log in to the Session Management Server console as the Session Management Server administrator. See "Logging in and logging out of the Session Management Server console" on page 272 for assistance.
19. If security is enabled on the WebSphere Application Server, you must add the sms-administrator role to the users or groups who administer the session management server.
    a. In the console, click **Users and Groups** > **Administrative users roles**.
    b. Click **Add**.
    c. Search for and select one or more users.
    d. Select **sms-administrator** and **Administrator** in the Role list.
    e. Click **OK**.
    f. Close the console.
20. Create the instance.
    a. Log in to the Session Management Server console as one of the users to which you assigned the **sms-adminstrator** and **Administrator** roles in the previous step. See "Logging in and logging out of the Session Management Server console" on page 272 for assistance.
    b. Select **Session Management Server** > **Deployment**.
    c. In the **Application name** field, enter the name of the Session Management Server application.
    d. Enter the WebSphere Application Server cell element to deploy the Session Management Server instance to in the **Target** field.
    e. In the **Virtual host** field, enter the web server virtual hosts that service the Session Management Server application instance.
    f. Enter the data source to use with the Session Management Server application instance in the **Data source** field.
    g. When you are ready to deploy, click **Deploy**.

What to do next

After the instance is deployed, you must configure it. See the *IBM Security Access Manager for Web Shared Session Management Administration Guide* for configuration instructions.

Setting up a session management server using script files

The installation and configuration scripts automate installations and perform unattended (*silent*) installations and configurations. Use the scripts in their original state or modify them to suit the requirements of your environment.

A session management server requires WebSphere Application Server. If WebSphere Application Server is not already installed, install and configure it using either of the following methods:

- "Installing WebSphere Application Server" on page 46 to manually install and configure it.
- "Setting up WebSphere Application Server using script files" on page 195 to automate its installation and configuration.

Setting up WebSphere Application Server using script files

The installation and configuration scripts can automate installations and perform unattended (*silent*) installations and configurations.

Use the scripts in their original state or modify them to suit the requirements of your environment.

Automating the installation of WebSphere Application Server (AIX, Linux, or Solaris)

Use the script file to automate the installation of WebSphere Application Server on AIX, Linux, or Solaris.

About this task

Automated installations can perform unattended (*silent*) installations. WebSphere Application Server is a prerequisite product for the following components:

- Web Portal Manager
- Attribute Retrieval Service
- Session Management Server

Installation Manager is required to install WebSphere Application Server.

Procedure

1. Obtain the WebSphere Application Server installation files and product repository from any of the following locations:
   - The WebSphere Application Server product media provided with the Security Access Manager DVDs.
   - The Passport Advantage site.
2. Copy the WebSphere Application Server files onto the computer where you want to install WebSphere Application Server.
3. Extract all the WebSphere Application Server files from their compressed files into one directory.
4. Obtain Installation Manager from any of the following locations:
   - The Passport Advantage site.
   - The IBM Installation Manager download web site:

     http://www.ibm.com/support/entry/portal/All_download_links/Software/Rational/IBM_Installation_Manager
5. Copy the Installation Manager files onto the computer where you want to install WebSphere Application Server.
6. Extract the Installation Manager files into its own directory.
7. Copy the `install_was.sh` from the `scripts` directory on the Security Access Manager product media to a temporary location on the computer where you want to install WebSphere Application Server.

8. Copy the appropriate WASInstall_*.xml file for your platform from the scripts directory on the Security Access Manager product media to the same temporary location where you copied the install_was.sh file. The response files are:

   Linux x86-64
   WASInstall_linux_x86.xml

   Linux s390
   WASInstall_linux_s390x.xml

   AIX WASInstall_aix_ppc.xml

   Solaris
   WASInstall_solaris_sparc.xml
9. Open the copy of the install_was.sh by using a text editor.
10. Modify the Installation Manager path in the install_was.sh file to specify where the Installation Manager images are located. For example, change the following line:

    ```
    INSTALL_MGR_DIR=/images/InstallationManager
    ```
11. Modify the WAS_RESPONSE_FILE variable to specify the name of the response file to use when you run the script. Use the name of the appropriate response file for your platform:

    Linux x86-64
    WASInstall_linux_x86.xml

    Linux s390
    WASInstall_linux_s390x.xml

    AIX WASInstall_aix_ppc.xml

    Solaris
    WASInstall_solaris_sparc.xml

    For example, on Linux for x86-64, specify:

    ```
    WAS_RESPONSE_FILE=./WASInstall_linux_x86.xml
    ```
12. Save and close the file.
13. Open the copy of the WASInstall_*.xml file by using a text editor.
14. Modify the repository location path in the WASInstall_*.xml file where your WebSphere Application Server images are located. For example, change the following line:

    ```
    <repository location='/images/WebSphere'/>
    ```
15. Optional: Modify the location where WebSphere Application Server is installed by the script. The default installation locations are:

    Linux or Solaris
    /opt/IBM/WebSphere/AppServer

    AIX /usr/IBM/WebSphere/AppServer

    To change the location, change the following lines in the WASInstall_*.xml file:

    ```
    <profile id='IBM WebSphere Application Server Network Deployment V8.0'
       installLocation='/opt/IBM/WebSphere/AppServer'>
    <data key='eclipseLocation' value='/opt/IBM/WebSphere/AppServer'/>
    ```
16. Save the response file.
17. Run the script file.

    ```
    install_was.sh
    ```

Attention: If you specify a repository file name incorrectly in step 14 on page 282, an error is displayed. Repeat the modification instructions in step 14 on page 282 to correct the repository file name. Then, remove the incorrect repository from Installation Manager before running the script again:

a. On a command line, change directory to the installation directory for Installation Manager:

   ```
   /opt/IBM/InstallationManager/eclipse
   ```

b. Run `IBMIM`.

c. Remove the incorrect repository.

d. Rerun the script.

18. After the installation of WebSphere Application Server is completed, create an Application Server profile by using the WebSphere Application Server **`manageprofiles`** command.

    For example, type:

    ```
    /opt/IBM/WebSphere/AppServer/bin/manageprofiles.sh -create -templatePath
    /opt/IBM/WebSphere/AppServer/profileTemplates/default
    ```

    For details about the **`manageprofiles`** command, see the WebSphere Application Server Information Center:

    http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp

19. Start the application server.

    For example, type:

    ```
    /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin/startServer.sh server1
    ```

20. Install the latest fix pack for your installation. See the hardware and software requirements page of the IBM Security Access Manager information center for the minimum fix pack level required.

    a. Locate the fix pack on the WebSphere Application Server Support page. http://www.ibm.com/support/docview.wss?uid=swg27004980

    b. Download the fix pack and use the instructions in the accompanying readme to install it.

What to do next

Continue with "Automating the installation of a session management server (AIX, Linux, or Solaris)" on page 285.

Automating the installation of WebSphere Application Server (Windows)

Use the script file to automate the installation of WebSphere Application Server on Windows.

About this task

Automated installations can perform unattended (*silent*) installations. WebSphere Application Server is a prerequisite product for the following components:

- Web Portal Manager
- Attribute Retrieval Service
- Session Management Server

Installation Manager is required to install WebSphere Application Server.

Procedure

1. Obtain the WebSphere Application Server installation files and product repository from any of the following locations:
   - The WebSphere Application Server product media provided with the Security Access Manager DVDs.
   - The Passport Advantage site.
2. Copy the WebSphere Application Server files onto the computer where you want to install WebSphere Application Server.
3. Extract all the WebSphere Application Server files from their compressed files into one directory.
4. Obtain Installation Manager from any of the following locations:
   - The Passport Advantage site.
   - The IBM Installation Manager download web site:

     http://www.ibm.com/support/entry/portal/All_download_links/Software/Rational/IBM_Installation_Manager
5. Copy the Installation Manager files onto the computer where you want to install WebSphere Application Server.
6. Extract the Installation Manager files into its own directory.
7. Copy the `install_was.bat` from the `scripts` directory of the Security Access Manager product media to a temporary location on the computer where you want to install WebSphere Application Server.
8. Copy the `WASInstall.xml` file from the `scripts` directory of the Security Access Manager product media to the same temporary location where you copied the `install_was.bat` file.
9. Open the copy of the `install_was.bat` by using a text editor.
10. Modify the Installation Manager path in the `install_was.bat` file to specify where the Installation Manager images are located. For example, change the following line:

    ```
    set INSTALL_MGR_DIR=C:\images\Installation Manager
    ```
11. Save and close the file.
12. Open the copy of `WASInstall.xml` file by using a text editor.
13. Modify the repository location path in the `WASInstall.xml` file where your WebSphere Application Server images are located. For example, change the following line:

    ```
    <repository location='C:\images\WebSphere'/>
    ```
14. Optional: Modify the location where WebSphere Application Server is installed by the script. For example, change the following lines:

    ```
    <profile id='IBM WebSphere Application Server Network Deployment V8.0'
      installLocation='C:\Program Files\IBM\WebSphere\AppServer'/>
    <data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere\AppServer'/>
    ```
15. Run the script file.

    ```
    install_was.bat
    ```
16. After the installation of WebSphere Application Server is completed, create an Application Server profile by using the WebSphere Application Server **manageprofiles** command.

    For example, type:

    ```
    C:\Program Files\IBM\WebSphere\AppServer\bin\manageprofiles.bat -create
      -templatePath "C:\Program Files\IBM\WebSphere\AppServer\
       profileTemplates\default"
    ```

For details about the **manageprofiles** command, see the WebSphere Application Server Information Center:

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp

17. Start the application server.

    For example, type:

    ```
    C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\bin\
    startServer.bat server1
    ```

18. Install the latest fix pack for your installation. See the hardware and software requirements page of the IBM Security Access Manager information center for the minimum fix pack level required.
    a. Locate the fix pack on the WebSphere Application Server Support page. http://www.ibm.com/support/docview.wss?uid=swg27004980
    b. Download the fix pack and use the instructions in the accompanying readme to install it.

What to do next

Continue with "Automating the installation of a session management server (Windows)" on page 286.

Automating the installation of a session management server (AIX, Linux, or Solaris)

Use the script file to automate the installation of a Security Access Manager session management server.

Before you begin

A session management server requires WebSphere Application Server. Before you begin this task, install and configure WebSphere Application Server, if it is not already installed. Use one of the following tasks:

- "Installing WebSphere Application Server" on page 46 to manually install and configure it.
- "Setting up WebSphere Application Server using script files" on page 281 to automate its installation and configuration.

About this task

Automated installations perform unattended (*silent*) installations.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the `install_isam.sh` script file in the `scripts` directory.
3. Run the script as follows:

   ```
   ./install_isam.sh -i SMS -d path_to_packages -a [accept|display]
   ```

   where
   - `SMS` is the component name.
   - *path_to_packages* is the location of the component installation packages.

     For example, if you are installing from a DVD:

     AIX *dvd_mount_point*`/usr/sys/inst.images`

Linux x86-64
/dvd_mount_point/linux_x86

Linux on System z
/dvd_mount_point/linux_x390

Solaris
/dvd_mount_point/solaris

- `-a [accept|display]`

  The `-a accept` option automatically accepts the license without displaying the license. The `-a display` option displays the license and you must manually accept the license.

For example, on Linux x86-64, type the following command to install a session management server:

```
./install_isam.sh -i SMS -d /mnt/dvd/linux_x86 -a accept
```

The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.

4. Optional: To list the required packages without installing, use the `-l` option.

```
./install_isam.sh -l SMS
```

What to do next

When the installation is completed, continue with "Automating configuration of a session management server" on page 287.

Automating the installation of a session management server (Windows)

Use the script file to automate the installation of a Security Access Manager session management server on Windows.

Before you begin

A session management server requires WebSphere Application Server. Before you begin this task, install and configure WebSphere Application Server, if it is not already installed. Use one of the following tasks:

- "Installing WebSphere Application Server" on page 46 to manually install and configure it.
- "Automating the installation of WebSphere Application Server (Windows)" on page 283 to automate its installation and configuration.

About this task

Automated installations can perform unattended (*silent*) installations.

Attention: The installation script requires administrator privileges. Run the script file command, `install_isam.bat`, after you log in using an administrator ID or from a command window that you open with **Run as administrator**.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

2. Locate the `install_isam.bat` script file in the `scripts` directory. This directory is on the product DVD or in the directory where you extracted the product files. Ensure that the `.bat` file and all the `.iss` files are in the same directory.
3. Run the script as follows:

   ```
   install_isam.bat /i SMS /d path_to_packages
   ```

   where:
   - `SMS` is the component name.
   - *`path_to_packages`* is the path to the product DVD or the directory where you extracted the product files.

   For example, to install the session management server, type:

   ```
   install_isam.bat /i SMS /d c:\isam_images
   ```

   where `c:\isam_images` is the directory where the extracted subdirectories and product files are located. The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.
4. Optional: To list the required packages without installing, use the `/l` option.

   ```
   install_isam.bat /l SMS
   ```

What to do next

When the installation is completed, continue with "Automating configuration of a session management server."

Automating configuration of a session management server

Use the script file to automate the configuration of session management server.

Before you begin

- Complete the installation of the session management server. See:
  - "Automating the installation of a session management server (Windows)" on page 286
  - "Automating the installation of a session management server (AIX, Linux, or Solaris)" on page 285
- To view status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.

If you are running this script on Windows, open a new command window. Do not perform this task in the same window where you ran the installation script.

About this task

Automated configuration performs unattended (*silent*) configuration.

Procedure

1. Create an options file for the component you want to configure.
   a. Locate the options file template for the component. There are two files for the session management server. Run the deployment script first.

      AIX, Linux, or Solaris
      Directory: `/opt/PolicyDirector/example/config/`

Deployment template: `deploy_sms.options.template`

Configuration template: `configure_sms.options.template`

Windows

Directory: `C:\Program Files\Tivoli\PDSMS\etc`

Deployment template: `deploy_sms.options.template.cmd`

Configuration template: `configure_sms.options.template.cmd`

b. Copy both files to a temporary directory. You can copy the files to the temporary directory and rename the files to names that are unique to your environment.

Attention: You must keep the `.cmd` extension for Windows template files. The Windows template files run as commands.

c. Modify the content of the files to specify settings for your environment. The comments in the files explain the settings and provide examples.

d. Save the files.

2. Optional: By default, passwords you specified in the options files are stored in clear text. To obfuscate these passwords:

a. Copy the `configure_isam.conf` file to the same directory where you copied the options files. The file is in the following locations:

AIX, Linux, or Solaris

`/opt/PolicyDirector/example/config/`

Windows

`C:\Program Files\Tivoli\Policy Director\example\config\`

b. See Appendix F, "Password management," on page 351 for instructions on using the `-obfuscate` option with the `pdconf` tool to obfuscate the passwords in the options files. For more information about `pdconf`, see the *IBM Security Access Manager for Web Command Reference*.

c. Return to these instructions to run the configuration script.

3. Copy the script file from its original location to the same directory where you copied the options file. The script files are in the following locations:

AIX, Linux, or Solaris

Directory: `/opt/PolicyDirector/example/config/`

File name: `configure_isam.sh`

Windows

Directory: `C:\Program Files\Tivoli\Policy Director\example\config\`

File name: `configure_isam.cmd`

4. Run the WebSphere Application Server **`setupCmdLine`** script to set up the correct execution environment for running the session management server configuration tool.

AIX

`. /usr/IBM/WebSphere/AppServer/profiles/`*`profile_name`*`/bin/setupCmdLine.sh`

Linux or Solaris

`. /opt/IBM/WebSphere/AppServer/profiles/`*`profile_name`*`/bin/setupCmdLine.sh`

Windows

`C:\Program Files\IBM\WebSphere\AppServer\profiles\`*`profile_name`*`\bin\setupCmdLine.bat`

where *profile_name* is the name of your WebSphere Application Server profile, such as AppSrv01.

5. Run the configuration script and use the deploy_sms.options file for input.

   AIX, Linux, or Solaris

   ```
   ./configure_isam.sh -f options_file
   ```

   Windows

   ```
   configure_isam.cmd -f options_file.cmd
   ```

   where *options_file* and *options_file*.cmd are the text files that contain the configuration options.

   For example:

   AIX, Linux, or Solaris

   ```
   ./configure_isam.sh -f my_deploy_sms.options
   ```

   Windows

   ```
   configure_isam.cmd -f my_deploy_sms.options.cmd
   ```

6. Run the configuration script and use the configure_sms.options file for input.

   AIX, Linux, or Solaris

   ```
   ./configure_isam.sh -f options_file
   ```

   Windows

   ```
   configure_isam.cmd -f options_file.cmd
   ```

   where *options_file* and *options_file*.cmd are the text files that contain the configuration options.

   For example:

   AIX, Linux, or Solaris

   ```
   ./configure_isam.sh -f my_configure_sms.options
   ```

   Windows

   ```
   configure_isam.cmd -f my_configure_sms.options.cmd
   ```

Chapter 18. Setting up the session management command line

You can administer the session management server by using the Security Access Manager Session Management Command Line component. You can use either the **pdadmin** command-line utility on the specified Security Access Manager authorization server, or the **pdsmsadmin** utility.

Note: If you want to use **pdadmin** to administer the session management server, you must first install and configure the authorization server before you install the command-line interface.

Preinstallation requirements

Before you install and configure the Security Access Manager session management command-line interface, you must perform several preinstallation tasks.

- During Security Access Manager configuration on Linux operating systems, scripts might fail to run, stating that `/bin/ksh` was not found. On certain versions of SUSE Linux Enterprise Server, Yast-based installation does not install the Korn shell at `/bin/ksh`.

  Install the `pdksh .rpm` file that matches the hardware on which you are installing Security Access Manager. The appropriate `.rpm` file can be found on either the SUSE Linux Enterprise Server installation media, or downloaded from the SUSE Linux Enterprise Server or Novell support websites.
- The configuration requires the name and port number of the Web server that is used to access the WebSphere Application Server that hosts the session management server.
- Determine whether you want to enable Secure Sockets Layer (SSL) for session management command-line interface communications. You can enable SSL between the session management server and the Security Access Manager authorization server so that all **pdadmin** command communications are secure.
- If you plan to use the Security Access Manager `sec_master` user (or other users and groups that are defined in the `secAuthority=Default` suffix) to administer SMS by using the session management command line, then you must unconfigure the base DN in the LDAP user registry that is used by WebSphere Application Server.

  Information about modifying the base DN for the WebSphere Application Server user registry can be found in the configuring Lightweight Directory Access Protocol user registries topics in the WebSphere Application Server information center at:

  http://www.ibm.com/software/webservers/appserv/was/library/

Setting up the session management command line using the command-line utilities

You can install and configure a Security Access Manager session management command-line system by using the command line.

To configure the session management command-line system, use the **pdsmsclicfg** utility. If you want to administer the session management server by using the **pdadmin** utility, run the **pdsmsclicfg** command from the system that hosts the authorization server. The **pdsmsclicfg** utility writes to the host authorization server configuration file, `ivacld.conf`

You can set up a session management command-line system by using one of the following installation methods.

Complete the instructions that apply to your operating system.

Note: The Security Access Manager Runtime (PD.RTE) and Security Access Manager Authorization Server (PD.Acld) packages are required only if you want to administer with the **pdadmin** utility.

AIX: Installing the session management command line

Use the **installp** utility to install the software packages and the **pdsmsclicfg** utility to configure them on AIX.

Procedure

1. Log on as **root**.
2. Perform the preinstallation tasks as listed in "Preinstallation requirements" on page 291.
3. Ensure that the registry server and policy server are up and running (in normal mode).
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
5. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "AIX: Installing the IBM Global Security Kit (GSKit)" on page 35.
6. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "AIX: Installing the IBM Tivoli Directory Server client" on page 42.
7. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
8. Install the IBM Security Utilities, if not already installed. For instructions, see page "AIX: Installing the IBM Security Utilities" on page 39.
9. Install the following Security Access Manager packages:

   ```
   installp -acgYXd package_path/usr/sys/inst.images packages
   ```

   where:

   - *package_path* is the directory where the DVD is mounted or the files are located
   - *packages* are:

     PD.RTE Specifies the Security Access Manager Runtime package.

     PD.Acld
     Specifies the Security Access Manager Authorization Server package.

PD.SMSCLI
Specifies the Security Access Manager Session Management Server Command Line package.

10. Unmount the DVD, if used.
11. To view status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
12. Configure the Security Access Manager Runtime and Security Access Manager Authorization Server packages as follows:
    a. Start the configuration utility:
    ```
    pdconfig
    ```
    The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure, one at a time.
    When a message is displayed that indicates the package was successfully configured, press **Enter** to configure another package or select the **x** option twice to close the configuration utility.
13. Configure the Security Access Manager Session Management Command Line package by running the **pdsmsclicfg** utility:
    ```
    pdsmsclicfg –action config
    ```
    For assistance with configuration options, see the *IBM Security Access Manager for Web Command Reference*.
14. You must manually start the authorization server that is hosting the session management command line after configuration.

Results

This step completes the setup of a Security Access Manager session management command-line system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Linux: Installing the session management command line

Use the **rpm** utility to install the software packages and the **pdsmsclicfg** utility to configure them on Linux.

About this task

Note to Linux on System z users: You must first obtain access to the Linux `rpm` files which are in the `/package_path/linux_s390` directory.

Procedure

1. Log on as **root**.
2. Perform the preinstallation tasks as listed in "Preinstallation requirements" on page 291.
3. Ensure that the registry server and policy server are up and running (in normal mode).
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

Attention: Ensure that the files are in a directory path that does not contain any spaces.

5. Change to the *package_path*/*distribution* directory.

   where:

   - *package_path* is the mount point for your DVD or file location
   - *distribution* specifies `linux_x86` for x86-64 or `linux_s390` for System z

6. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Linux: Installing the IBM Global Security Kit (GSKit)" on page 35.
7. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Linux: Installing the IBM Tivoli Directory Server client" on page 43.
8. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
9. Install the IBM Security Utilities, if not already installed. For instructions, see page "Linux: Installing IBM Security Utilities" on page 40.
10. Install the Security Access Manager packages:

    ```
    rpm -ihv packages
    ```

    where *packages* are as follows:

Package	Linux on x86-64	Linux on System z
Security Access Manager Runtime package	`PDRTE-PD-7.0.0-0.x86_64.rpm`	`PDRTE-PD-7.0.0-0.s390.rpm`
Security Access Manager Authorization Server package	`PDAcld-PD-7.0.0-0.x86_64.rpm`	`PDAcld-PD-7.0.0-0.s390.rpm`
Security Access Manager Session Management Command Line package	`PDSMS-CLI-7.0.0-0.x86_64.rpm`	`PDSMS-CLI-7.0.0-0.s390.rpm`

11. To view status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
12. Configure the Security Access Manager Runtime and Security Access Manager Authorization Server packages as follows:
    a. Start the configuration utility:

       ```
       pdconfig
       ```

       The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
       Select the menu number of the package that you want to configure.
       When a message is displayed that indicates the package was successfully configured, select the **x** option twice to close the configuration utility.
13. Configure the Security Access Manager Session Management Command Line package by running the **pdsmsclicfg** utility:

    ```
    pdsmsclicfg –action config
    ```

    For assistance with configuration options, see the *IBM Security Access Manager for Web Command Reference*.
14. Manually start the authorization server that is hosting the session management command line after configuration.

Results

When a message is displayed that indicates the package was successfully configured, select the **x** option twice to close the configuration utility.

This step completes the setup of a Security Access Manager session management command-line system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Solaris: Installing the session management command line

Use the **pkgadd** to install the software packages and the **pdsmsclicfg** utility to configure them on Solaris.

About this task

Attention: Installations on Solaris systems should use the **-G** option with the **pkgadd** utility. The **-G** option adds the package into the current zone only.

Procedure

1. Log on as **root**.
2. Perform the preinstallation tasks as listed in "Preinstallation requirements" on page 291.
3. Ensure that the registry server and policy server are up and running (in normal mode).
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.
5. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Solaris: Installing the IBM Global Security Kit (GSKit)" on page 36.
6. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Solaris: Installing the IBM Tivoli Directory Server client" on page 44.
7. Install the IBM Security Access Manager License, if not already installed. For instructions, see "AIX, Linux, Solaris: Installing the IBM Security Access Manager License" on page 37.
8. Install the IBM Security Utilities, if not already installed. For instructions, see page "Solaris: Installing IBM Security Utilities" on page 40.
9. Install the Security Access Manager packages:

   ```
   pkgadd -d /package_path/solaris -a /package_path/solaris/pddefault -G packages
   ```

   where:

   /*package_path*/solaris
   Specifies the location of the package.

   /*package_path*/solaris/pddefault
   Specifies the location of the installation administration script.

   and where *packages* are as follows:

   PDRTE Specifies the Security Access Manager Runtime package.

   PDAcld Specifies the Security Access Manager Authorization Server package.

PDSMSCLI
Specifies the Security Access Manager Session Management Command Line package.

When the installation process is complete for each package, the following message is displayed:

```
Installation of package successful.
```

10. To view status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
11. Configure the Security Access Manager Runtime and Security Access Manager Authorization Server packages as follows:
    a. Start the configuration utility:

    ```
    pdconfig
    ```

    The Security Access Manager Setup Menu is displayed.
    b. Type menu number 1 for **Configure Package**. The Security Access Manager Configuration Menu is displayed.
    c. Select the menu number of the package that you want to configure.
12. Configure the Security Access Manager Session Management Command Line package by running the **pdsmsclicfg** utility:

    ```
    pdsmsclicfg –action config
    ```

    For assistance with configuration options, see the *IBM Security Access Manager for Web Command Reference*.
13. You must manually start the authorization server that is hosting the session management command line after configuration.

Results

When a message is displayed that indicates the package was successfully configured, press Enter to configure another package or select the **x** option twice to close the configuration utility.

This step completes the setup of a Security Access Manager session management command-line system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Windows: Installing the session management command line

Use the **setup.exe** program to install the software packages and the **pdsmsclicfg** utility to configure them on Windows.

Procedure

1. Log on as a user with administrator privileges.
2. Perform the preinstallation tasks as listed in "Preinstallation requirements" on page 291.
3. Ensure that the registry server and policy server are up and running (in normal mode).
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the files are in a directory path that does not contain any spaces.

5. Install IBM Global Security Kit (GSKit), if not already installed. For instructions, see page "Windows: Installing the IBM Global Security Kit (GSKit)" on page 36.
6. If you use an LDAP-based user registry, install the IBM Tivoli Directory Server client, if not already installed. For instructions, see page "Windows: Installing the IBM Tivoli Directory Server client" on page 45.
7. Install the Security Access Manager license, if not already installed. For instructions, see "Windows: Installing the IBM Security Access Manager License" on page 39.
8. Install the IBM Security Utilities, if not already installed. For instructions, see page "Windows: Installing IBM Security Utilities" on page 41.
9. Install the Security Access Manager packages. To do so, run the **setup.exe** program in the following directory:`\windows\PolicyDirector\Disk Images\Disk1`
   Follow the online instructions and select to install the following package:
   - Access Manager Session Management Command Line

     Also, select the following packages if the Security Access Manager framework (**pdadmin**) is used to manage the Session Management Server:
   - Security Access Manager Runtime
   - Security Access Manager Authorization Server
10. To view status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.
11. Configure the packages in either of the following ways:
    - If you are using the Security Access Manager framework to manage the session management server, use the **pdconfig** graphical configuration utility.
      a. Open a new command-line window.
      b. Start the utility. Type: `pdconfig`
      c. If you installed the Runtime, select the **Security Access Manager Runtime** package.
      d. Click **Configure**.
      e. If you installed the Authorization Server, select the **Security Access Manager Authorization Server** package.
      f. Click **Configure**.
      g. Select the **Session Management Server Command Line Interface** package.
      h. Click **Configure**.
    - Otherwise, run the **pdsmsclicfg** graphical configuration utility: `pdsmsclicfg`. For assistance with configuration options, see the *IBM Security Access Manager for Web Command Reference*.

    You are prompted for configuration options.

Results

This step completes the setup of a Security Access Manager session management command-line system. To set up another Security Access Manager system, follow the steps in the Chapter 3, "Installation roadmap," on page 21.

Setting up a session management command line using the Launchpad (Windows)

Use the Launchpad installation method to install and configure the session management command-line software on Windows by using a graphical user interface.

Before you begin

Ensure that you complete the following prerequisite tasks:

- "Operating system preparation" on page 28
- If you plan to use a user registry other than IBM Tivoli Directory Server, continue with Chapter 5, "User registry server installation and configuration," on page 51.

About this task

The Launchpad uses a graphical user interface to perform step-by-step installation and initial configuration.

This task installs the following components:

- IBM GSKit
- IBM Tivoli Directory Server client
- IBM Security Utilities
- Security Access Manager License
- Security Access Manager Runtime
- Security Access Manager Authorization Server
- Security Access Manager Session Management Command Line

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

   Attention: Ensure that the Launchpad image files are in a directory path that does not contain any spaces.
2. Start the Launchpad.
   a. Locate the `launchpad64.exe` file.
   b. Double-click the file to start the Launchpad.
3. Select the language that you want to use during the installation.
4. Click **OK** The Launchpad Welcome window opens.
5. Click **Next**.
6. Select the **Session Management Server Command Line** component.
7. Click **Next**. A list displays the component that you selected and any prerequisite software that is required by that component but that is not already installed.
8. Click **Next**. An arrow next to a component name on the left indicates that component is being installed. A check mark next to a component name indicates that component is installed.
9. If the current component is IBM Global Security Kit, click **Install IBM Global Security Kit** to install it. When it completes, continue with step 10.
10. Click **Next**.

11. Respond to the prompts presented during the installation.
12. Click **Next** at the bottom of the Launchpad to continue.
13. Complete the installation.
    - If the installation fails, correct the error that is described in the error message and restart the Launchpad.
    - If the installation is successful, continue with step 14.
14. Click **Next** to start the configuration.

    Note: The configuration tool is displayed in the language that is selected for your operating system locale. If the tool is displayed in English and is not displayed in the operating system locale, review the language pack installation log at `%USERPROFILE%\ISAMLangPacksInstall.log`. Correct any errors that are reported in the log file. Then, install the language pack as described in Appendix E, "Language support installation," on page 339.
15. Click **Configure Session Management Server command line**. The configuration tool opens.
16. Select the component.
17. Click **Configure**.
18. Complete the configuration. For help completing the prompts, see Appendix D, "pdconfig options," on page 317. When all installations and configurations are completed, a success or failure message is displayed.
19. Take one of the following actions:
    - If the configuration completed successfully, click **Next**.
    - If the configuration failed or an error is displayed, review the log file in the default `%USERPROFILE%` location, such as `C:\Users\Administrator\LaunchPDConfigforISAM.log`.

      Make corrections as indicated by the log file. Then, configure the component by using the **pdconfig** utility at a command line or by clicking **Start** > **Programs** > **IBM Security Access Manager for Web** > **Configuration**.
20. Click **Finish** to close the Launchpad.

Setting up a session management command line using script files

The installation and configuration scripts automate installations and perform unattended (*silent*) installations and configurations. Use the scripts in their original state or modify them to suit the requirements of your environment.

Automating the installation of a session management command line (AIX, Linux, or Solaris)

Use the script file to automate the installation of the session management command line.

About this task

Automated installations perform unattended (*silent*) installations.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
2. Locate the `install_isam.sh` script file in the `scripts` directory.

3. Run the script as follows:

   ```
   ./install_isam.sh -i SMSCLI -d path_to_packages -a [accept|display]
   ```

   where

   - `SMSCLI` is the component name.
   - *path_to_packages* is the location of the component installation packages. For example, if you are installing from a DVD:

     AIX */dvd_mount_point*`/usr/sys/inst.images`

     Linux x86-64
     /dvd_mount_point`/linux_x86`

     Linux on System z
     /dvd_mount_point`/linux_s390`

     Solaris
     /dvd_mount_point`/solaris`
   - `-a [accept|display]`

     The `-a accept` option automatically accepts the license without displaying the license. The `-a display` option displays the license and you must manually accept the license.

   For example, on Linux x86-64, type the following command to install a session management server:

   ```
   ./install_isam.sh -i SMSCLI -d /mnt/dvd/linux_x86 -a accept
   ```

   The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.
4. Optional: To list the required packages without installing, use the `-l` option.

   ```
   ./install_isam.sh -l SMSCLI
   ```

What to do next

When the installation is completed, continue with "Automating configuration of a session management command line" on page 301.

Automating the installation of a session management command line (Windows)

Use the script file to automate the installation of a Security Access Manager session management command line on Windows.

About this task

Automated installations can perform unattended (*silent*) installations.

Attention: The installation script requires administrator privileges. Run the script file command, `install_isam.bat`, after you log in using an administrator ID or from a command window that you open with **Run as administrator**.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

2. Locate the `install_isam.bat` script file in the `scripts` directory. This directory is on the product DVD or in the directory where you extracted the product files. Ensure that the `.bat` file and all the `.iss` files are in the same directory.
3. Run the script as follows:

   ```
   install_isam.bat /i SMSCLI /d path_to_packages
   ```

   where :
   - `SMSCLI` is the component name.
   - *`path_to_packages`* is the path to the product DVD or the directory where you extracted the product files.

   For example, to install the session management command line, type:

   ```
   install_isam.bat /i SMSCLI /d c:\isam_images
   ```

   where `c:\isam_images` is the directory where the extracted subdirectories and product files are located. The script for each component installs all the prerequisites for that component. If the prerequisites are already installed, the script goes to the next component installation.
4. Optional: To list the required packages without installing, use the `/l` option.

   ```
   install_isam.bat /l SMSCLI
   ```

What to do next

When the installation is completed, continue with "Automating configuration of a session management command line."

Automating configuration of a session management command line

Use the script file to automate the configuration of session management command line.

Before you begin

- Complete the installation of the session management command line. See:
  - "Automating the installation of a session management command line (Windows)" on page 300
  - "Automating the installation of a session management command line (AIX, Linux, or Solaris)" on page 299
- To view status and messages in a language other than English, which is the default, install your language support package *before* you configure packages. For instructions, see "Installing language support packages for Security Access Manager" on page 340.

If you are running this script on Windows, open a new command window. Do not perform this task in the same window where you ran the installation script.

About this task

Automated configuration performs unattended (*silent*) configuration.

Procedure

1. Create an options file for the component you want to configure.
   a. Locate the options file template for the component.

AIX, Linux, or Solaris

```
/opt/PolicyDirector/example/config/
configure_smscli.options.template
```

Windows

```
C:\Program Files\Tivoli\PDSMS\etc\
configure_smscli.options.template.cmd
```

b. Copy the file to a temporary directory. You can copy the file to the temporary directory with a name that is unique to your environment.

Attention: You must keep the `.cmd` extension for Windows template files. The Windows template files run as commands.

c. Modify the content of the file to specify settings for your environment. The comments in the file explain the settings and provide examples.

d. Save the file.

2. Optional: By default, passwords you specified in the options files are stored in clear text. To obfuscate these passwords:

a. Copy the `configure_isam.conf` file to the same directory where you copied the options files. The file is in the following locations:

AIX, Linux, or Solaris

```
/opt/PolicyDirector/example/config/
```

Windows

```
C:\Program Files\Tivoli\Policy Director\example\config\
```

b. See Appendix F, "Password management," on page 351 for instructions on using the `-obfuscate` option with the `pdconf` tool to obfuscate the passwords in the options files. For more information about `pdconf`, see the *IBM Security Access Manager for Web Command Reference*.

c. Return to these instructions to run the configuration script.

3. Copy the script file from its original location to the same directory where you copied the options file. The script files are in the following locations:

AIX, Linux, or Solaris

Directory: `/opt/PolicyDirector/example/config/`

File name: `configure_isam.sh`

Windows

Directory: `C:\Program Files\Tivoli\Policy Director\example\config\`

File name: `configure_isam.cmd`

4. Run the configuration script and options file.

AIX, Linux, or Solaris

```
./configure_isam.sh -f options_file
```

Windows

```
configure_isam.cmd -f options_file.cmd
```

where *options_file* and *options_file*`.cmd` are the text files that contain the configuration options.

For example:

AIX, Linux, or Solaris

```
./configure_isam.sh -f my_configure_smscli.options
```

Windows

```
configure_isam.cmd -f my_configure_smscli.options.cmd
```

Part 6. Appendixes

Appendix A. Secure Sockets Layer (SSL) security setup

You can enable Secure Sockets Layer (SSL) security between the Security Access Manager servers and your user registry server.

When SSL is enabled, data exchanged between the Security Access Manager servers and the user registry server is encrypted. Both server authentication and client authentication are supported.

When you enable SSL communication, you configure SSL on the following systems in the order shown:

1. The user registry server. See the instructions in Chapter 5, "User registry server installation and configuration," on page 51.
2. Each Security Access Manager server.
3. Any other system that communicates with the user registry server by using the IBM Tivoli Directory Server client.

Configuring SSL on the Security Access Manager servers

After you enable SSL access on the LDAP server, set up SSL access on the client systems. In this context, *the client systems* are the systems on which your Security Access Manager components run.

You must create a key database file on the client system to hold the signer certificate of the LDAP server. The signing certificate is either the self-signed certificate or the signer certificate of a server certificate that is issued by a certificate authority (CA). The LDAP SSL client validates the LDAP server certificate by ensuring that it is signed by one of the signer certificates in its key database.

The process for configuring a client system is:

1. "Creating a database and adding the signer certificate."
2. "Configuring SSL communications" on page 306.
3. "Testing SSL access" on page 307.

Creating a database and adding the signer certificate

Create a key database file on the client and add the signer certificate from the LDAP server with the GSKit key management utility, **GSKCapiCmd**.

About this task

For more information about **GSKCapiCmd**, see the *GSKCapiCmd User's Guide*.

Procedure

1. Open a command prompt.
2. Locate the **gsk8capicmd_64** in the GSKit installation directory and change to that directory.
3. Use the **gsk8capicmd_64** command to create the key database. For example, type:

```
gsk8capicmd_64 -keydb -create -db /key/isam.kdb -pw passw0rd
  -type cms -stash -empty
```

4. Add the LDAP server certificate to the key database.
   a. Copy the signer certificate to the client system.
      - If the server uses a certificate from a certificate authority (CA), copy the file that contains the signer certificate to the client system.
      - If the server uses a self-signed certificate, copy the certificate that you extracted from the key database file on the server to the client system.
   b. Use the **gsk8capicmd_64** command to add the signer certificate to the key database. For example, to add a signer certificate that is in ASCII PEM format, type:

      ```
      gsk8capicmd_64 -cert -add -db /key/isam.kdb -pw passw0rd -type cms -file
        /temp/LDAPserver-cert.pem -trust enable -format ascii -label ldapsigner
      ```

5. Verify that SSL access was enabled. Enter the following command on the Security Access Manager system where you configured SSL:

   ```
   idsldapsearch -h server_name -Z -K client_keyfile -P keyfile_pwd
   -p ldapport -b "" -s base objectclass=*
   ```

   The command variables are:

   server_name
   The DNS host name of the LDAP server.

   client_keyfile
   The fully qualified path name of the generated client key database.

   keyfile_pwd
   The password of the generated key database.

   -p *ldapport*
   Specifies the port where the LDAP server is listening. If it is not specified, the default LDAP SSL port 636 is used.

   -Z Indicates to use SSL to establish the connection with the LDAP server.

   This command returns the LDAP base information, which includes the suffixes on the LDAP server.

What to do next

Continue with "Configuring SSL communications."

Configuring SSL communications

Use the Security Access Manager **pdconfig** utility to unconfigure and then reconfigure a Security Access Manager component.

The Security Access Manager **pdconfig** utility is helpful, if you:

- Did not enable SSL.
- Want to change the SSL configuration. For example, you might select a different key database file or specify a different certificate label.

For a description of configuration options, see "Security Access Manager Runtime: LDAP" on page 317.

The configuration requires several values. Most come from the previous SSL setup tasks. One (a port number) comes from the LDAP server.

Table 19. SSL configuration values

SSL configuration values	Descriptions and examples
SSL key file name with full path The file and location of the key database file that you created on the Security Access Manager component.	`/key/isam.kdb`
SSL key file password The password of the key database file. t	`passw0rd`
LDAP server SSL port The secure port value of the user registry server.	`636`
Certificate label The label that is assigned when the server certificate is imported into the client key database.	`sds`

Testing SSL access

Test SSL access to ensure that the configuration is completed.

Enter the following command on the Security Access Manager system where you configured SSL:

```
idsldapsearch -h server_name -Z -K client_keyfile -P keyfile_pwd
-p ldapport -b "" -s base objectclass=*
```

The command variables are:

server_name
: The DNS host name of the LDAP server.

client_keyfile
: The fully qualified path name of the generated client key database.

keyfile_pwd
: The password of the generated key database.

-p *ldapport*
: Specifies the port where the LDAP server is listening. If it is not specified, the default LDAP SSL port 636 is used.

-Z
: Indicates that SSL is to be used to establish the connection with the LDAP server.

This command returns the LDAP base information, which includes the suffixes on the LDAP server.

Configuring Tivoli Directory Server client for client authentication

During the configuration of your LDAP server to enable SSL access, you must choose either *server authentication* or *server and client authentication*. If you chose *server and client authentication*, you must establish a certificate for the client system (that is, the Security Access Manager component system). In this mode of authentication, after the client authenticates the server, the server requests the client certificate and uses it to authenticate the client identity.

Before you begin

Install and configure the Tivoli Directory Server client on the computer where your Security Access Manager components are installed.

About this task

The following high-level steps are required to enable client authentication on the Security Access Manager component. See the information for securing directory communications in the *IBM Tivoli Directory Server Administration Guide* for the details of each step.

Procedure

1. Take *one* of the following actions:
   - Request a personal certificate from a certificate authority (CA) and receive that personal certificate into the key database file. You also might need to add a signer certificate to the key database file.
   - Create a self-signed certificate and extract the certificate and make it available on all client systems that securely communicate with the server.
2. Create the key database, associated password stash file, and password on the client system. For example, use the **gsk8capicmd** to create a database, stash file, and password.
3. After you create the key database file on the client system, change the file ownership of the key database file to user `ivmgr` and group `ivmgr`. Use the appropriate operating system command for changing file ownership. For example, on AIX, Linux, and Solaris systems, enter the following command: `chown ivmgr:ivmgr client_keyfile`
4. Receive the certificate into the key database.
5. Configure the Tivoli Directory Server client and enable SSL.
6. Copy and add the signer certificate to the key database on the Tivoli Directory Server with which you want to enable SSL communication.

What to do next

Continue with "Testing SSL access when using server and client authentication."

Testing SSL access when using server and client authentication

After the LDAP server recognizes the personal certificate of the client, test SSL access.

Use the following command on the LDAP client:

```
idsldapsearch -h server_name -Z -K client_keyfile -P keyfile_pwd -N \
client_label -p ldapport -b "" -s base objectclass=*
```

The command variables are as follows:

server_name
The DNS host name of the LDAP server.

client_keyfile
The fully qualified path name of the generated client key database.

keyfile_pwd
The password of the generated key database.

client_label
The label that is associated with the key, if any. This field is needed only when the LDAP server is configured to perform server and client authentication.

-p *ldapport*
Specifies the port where the LDAP server is listening. If it is not specified, the default LDAP SSL port 636 is used.

-Z Indicates that SSL is to be used to establish the connection with the LDAP server.

The **idsldapsearch** command returns the LDAP base information, which includes the suffixes on the LDAP server. Notice that the **–N** parameter indicates the label that was specified when the personal certificate of the client was added to the key database file of the client.

Note: *Do not specify the signer certificate label of the LDAP server.* The **–N** option indicates to GSKit which client certificate is sent to the server when requested. If no label is specified, then the default personal certificate is sent when the server requests the client certificate.

Appendix B. Groups and administrator identities on AIX, Linux, and Solaris systems

User IDs and groups are created automatically by the installation process if they do not exist. If you want to assign specific group IDs (GID) or user IDs (UID) for these groups and users, you can create them before installation.

Table 20 lists the user IDs and groups that are used by Security Access Manager and its prerequisite software during installation on AIX, Linux, or Solaris systems.

Table 20. Users and groups required by Security Access Manager

ID	Type	Description	Group membership

`ivmgr`	group	Security Access Manager Runtime installs files and directories that are owned by the group `ivmgr`. The installation process creates the group by using the next available GID. To choose your own GID for Security Access Manager Runtime:
		Linux and Solaris:
		`groupadd –g gid ivmgr`
		AIX:
		`mkgroup id=gid ivmgr`
			`ivmgr, root`

`ivmgr`	user	Security Access Manager installs files and directories that are owned by the user `ivmgr`. The installation process creates the user by using the next available UID. To choose your own UID for Security Access Manager Runtime:
		Linux and Solaris:
		`useradd –u uid –g ivmgr`
		`-s /bin/false`
		`–d /opt/PolicyDirector`
		`–c "Security Access Manager User" ivmgr`
		AIX:
		`mkuser id=uid groups=ivmgr`
		`gecos="Security Access Manager User"`
		`home=/opt/PolicyDirector ivmgr`	

Table 20. Users and groups required by Security Access Manager (continued)

ID	Type	Description	Group membership

`tivoli`	group	Security Access Manager Runtime also creates a group ID named `tivoli` for use with the Tivoli Common Directory scheme. Note that other Tivoli products can create the group ID `tivoli` and that its creation is not unique to Security Access Manager Runtime. The installation process creates the group ID by using the next available GID. To choose your own GID for Security Access Manager Runtime to be used with Tivoli Common Directory:
		Linux and Solaris:
		`groupadd –g gid tivoli`
		AIX:
		`mkgroup id=gid tivoli`
			`tivoli, ivmgr, root`

`tivoli`	user	Security Access Manager Runtime also creates a user ID named `tivoli` for use with the Tivoli Common Directory scheme. Note that other Tivoli products can create the user ID `tivoli` and that its creation is not unique to Security Access Manager Runtime. The installation process creates the user ID `tivoli` by using the next available UID. To choose your own UID for Security Access Manager Runtime to be used with Tivoli Common Directory:
		Linux and Solaris:
		`useradd –u uid –g tivoli –c "Owner of Tivoli Common Files" tivoli`
		`usermod –G tivoli ivmgr`
		AIX:
		`mkuser id=uid groups=tivoli gecos="Owner of Tivoli Common Files" tivoli`
		`chuser pgrp=staff groups=ivmgr,tivoli ivmgr`
			`tivoli`

`idsldap`	group	The IBM Tivoli Directory Server installs files and directories that are owned by group `idsldap`. The installation process creates the group by using the next available GID. To choose your own GID:
		Linux and Solaris:
		`groupadd –g gid idsldap`
		AIX:
		`mkgroup id=gid idsldap`	

Table 20. Users and groups required by Security Access Manager (continued)

ID	Type	Description	Group membership
idsldap	user	The IBM Tivoli Directory Server installs files and directories that are owned by user idsldap. The installation process creates the user by using the next available UID. To choose your own UID: **Linux and Solaris:** useradd –u *uid* –g idsldap –d /home/idsldap –s /bin/ksh idsldap **AIX:** mkuser id=*uid* pgrp=staff groups=idsldap	idsldap
sys	group	The installation process creates the group for IBM Global Security Kit (GSKit).	root

The IBM Tivoli Directory Server installation also requests a local user ID to own the directory server instance and DB2 instance.

Appendix C. Default port numbers

The installation uses several port numbers by default.

Table 21. Default port numbers used during Security Access Manager installation

Installation components	Fields to be completed	Default port
Security Access Manager Policy Server	Policy server port	7135
Security Access Manager Policy Server Security Access Manager Runtime Security Access Manager Runtime for Java Security Access Manager Web Portal Manager	Policy server SSL port	7135
Security Access Manager Authorization Server	Authorization request port	7136
Security Access Manager Authorization Server	Administration request port	7137
Security Access Manager Policy Proxy Server	Policy request port	7138
Security Access Manager Policy Proxy Server	Authorization request port	7139
Security Access Manager WebSEAL	WebSEAL listening port	7234
Security Access Manager Session Management Server	IBM WebSphere Application Server port	8879
LDAP servers	Non-SSL port	389
LDAP servers	SSL port	636
Security Access Manager WebSEAL	HTTP port	80
Security Access Manager WebSEAL	HTTPS port	443

Appendix D. pdconfig options

During Security Access Manager configuration with the **pdconfig** utility, you are prompted for several options.

Use the descriptions to help you provide the correct values. Depending on whether you are installing on a Windows, AIX, Linux, or Solaris platform, you might be prompted for these options in a different sequence than listed.

Security Access Manager Runtime: LDAP

Table 22 lists options that are prompted during configuration of the Security Access Manager Runtime package with an LDAP registry.

Table 22. Security Access Manager Runtime configuration options: LDAP. * indicates a required option.

Configuration option	Description
Will you install the policy server on this machine	Indicates whether the policy server will be installed on the same machine.
Enable Tivoli Common Directory for logging	Select to enable Tivoli Common Directory. Tivoli Common Directory is a central location on systems that run IBM Tivoli software for storing files, such as trace and message logs.

Table 22. Security Access Manager Runtime configuration options: LDAP (continued). * indicates a required option.

Configuration option	Description
Directory Name (for Tivoli Common Directory)	Specifies the fully qualified path for the Tivoli Common Directory. • If the location of the Tivoli Common Directory is already established on the system by the installation of another Tivoli application, the directory location is displayed in the field and cannot be modified. • If the location of the Tivoli Common Directory was not previously established on the system, you can specify its location. If Tivoli Common Directory is enabled and the directory location was not previously established, the default common directory names are: • Windows: `C:\Program Files\ibm\tivoli\common` • AIX, Linux, or Solaris: `/var/ibm/tivoli/common` Beneath the Tivoli Common Directory, each Tivoli product stores its information in a product-specific subdirectory. Each product-specific directory is named with a three-character identifier. For example, for IBM Security Access Manager for Web: *`tivoli_common_dir`*`/HPD` See the *IBM Security Access Manager for Web Troubleshooting Guide* for a complete list of three-character identifiers. If Tivoli Common Directory is not enabled, Security Access Manager writes its message and trace log data to the following location: • Windows: `C:\Program Files\Tivoli\Policy Director\log` • AIX, Linux, or Solaris: `/var/PolicyDirector/log`
Registry	Specifies the type of registry server to be set up for Security Access Manager. Select **LDAP**.
LDAP server host name	Specifies the host name or IP address of the LDAP type of registry server. You can specify the fully qualified host name with or without the domain extension. Examples: `ldapserver` or `ldapserver.example.com`
LDAP server port	Specifies the port number on which the LDAP type of registry server listens. The default port number is **389**.
If the Security Access Manager policy server is *not* installed on the same system as the Security Access Manager Runtime, you are prompted for the next values:	

Table 22. Security Access Manager Runtime configuration options: LDAP (continued). * indicates a required option.

Configuration option	Description

Policy server host name	Specifies the host name or IP address of the Security Access Manager policy server (`pdmgrd`).
	
	The policy server manages the policy database (sometimes known as *master authorization database*), updates the database replicas whenever a change is made to the master database, and replicates the policy information throughout the domains. The policy server also maintains location information about other resource managers that operate in the domain.
	
	There must be at least one policy server that is defined for each domain. You can specify the fully qualified host name with or without the domain extension. Examples:
	`pdmgr`
	`pdmgr.example.com`

Policy server SSL port	Specifies the port number on which the policy server listens for SSL requests. The default port number is **7135**.
Domain	Specifies the name of the Security Access Manager default domain, which is also known as the *management domain*. This domain is created when the policy server is configured. The default domain enforces security policies for authentication, authorization, and access control. Any security policy that is implemented in a domain affects only those objects in that domain. Users with authority to perform tasks in one domain do not necessarily have authority to perform those tasks in other domains. The default value is **Default**, which indicates the management domain.
On systems other than Windows, you can enable SSL connections between this Security Access Manager runtime system and the LDAP server. If selected, you are prompted for the next values:	
Non-SSL port *	Specifies the port number on which the LDAP server listens. The default port number is **389**.
Port number *	Specifies the port number on which the LDAP server listens for SSL requests. The default port number is **636**.
Key file with full path *	Specifies the fully qualified path where the existing SSL client key file is located or, if the **Create SSL key file** check box is selected, where the newly created SSL key file is located. The key file holds the client-side certificates that are used in SSL communication. The file extension is always `.kdb`. Copy the SSL key file to any directory on your local system. This key file must be obtained (copied) from the LDAP server.

Table 22. Security Access Manager Runtime configuration options: LDAP (continued). * indicates a required option.

Configuration option	Description
Key file password	Specifies the existing password that is associated with the specified SSL key file. The client key file password was set when the key file was first created. Change this password by using the **gsk8capicmd** utility (which is part of GSKit 8) or the **ikeyman** utility (which is available with IBM Java). If changed, remember this password.
Certificate label	Specifies the label for the SSL client certificate. This label is valid only when SSL is used and when the LDAP server is configured to require client authentication. For example: `PDLDAP`. Use a certificate label to distinguish between multiple certificates within the SSL key file, or when a certificate other than the default certificate in the key file is used. Otherwise, leave this field blank.
Create SSL key file	Select the check box to create an SSL key file. The key file holds the client-side certificates that are used in SSL communication. The **pdconfig** utility uses IBM Global Security Kit (GSKit) to generate the certificate and the SSL key file. Default: enabled (The check box is selected).
Enable FIPS or NIST SP800-131 or Suite B	You can configure Security Access Manager to comply with various security standards. To enable the configuration, set the `[ssl] ssl-compliance` value in `pd.conf` after you configure the runtime but before you configure the policy server. The **pdconfig** utility creates all the keys and certificates by using algorithms appropriate for the configured compliance type. By setting the `[ssl] ssl-compliance` value, the IBM Tivoli Directory Server client is configured to use the appropriate secure communications protocol for the compliance type selected. **Note:** All run times must set their `[ssl] ssl-compliance` configurations to match because run times cannot be mixed. Default: `[ssl] ssl-compliance='none'`. This value means that no compliance is enabled.

Security Access Manager Runtime: Active Directory

Table 23 lists options that are prompted during configuration of the Security Access Manager Runtime package with an Active Directory registry.

Table 23. Security Access Manager Runtime configuration options: Active Directory. * indicates a required option.

Configuration option	Description
Registry	Specifies the type of registry server to be set up for Security Access Manager. Select **Active Directory**.

Table 23. Security Access Manager Runtime configuration options: Active Directory (continued). * indicates a required option.

Configuration option	Description
Configure to Multiple Active Directory domains	Select the check box to configure multiple Active Directory domains. If not selected, Security Access Manager is configured to a single domain. An example of multiple Microsoft Active Directory domain is a Security Access Manager single domain with multiple Microsoft Active Directory domains. When configured for multiple Microsoft Active Directory domains, the command line displays the Security Access Manager administrator ID (the default is **sec_master**) as **secmaster@***domain_name* Default: not enabled (Security Access Manager is configured to a single domain.)
Active Directory host name *	Specifies the Active Directory domain controller server name. For example: `adserver.example.com`
Active Directory domain	Specifies the Active Directory domain name. If configured to multiple domains, the name displays automatically. For example: `dc=tivoli,dc=com`
Enable encrypted connections	Specifies whether encryption communication to Microsoft Active Directory should be used. When the check box is selected, Kerberos is used in the Microsoft Active Directory Service Interface (ADSI) to encrypt data in the connection to the Microsoft Active Directory server. This setting is equivalent to enabling an SSL connection in a system environment that uses the LDAP client to communicate with the Active Directory server. The default value is not enabled (Security Access Manager is not configured for encryption.).
Specify the location of the Security Access Manager Policy Server. If you select **Security Access Manager Policy Server is installed on another machine**, you are prompted for the host name and listening port values:	

Table 23. Security Access Manager Runtime configuration options: Active Directory (continued). * indicates a required option.

Configuration option	Description

Host name	Specifies the host name or IP address of the Security Access Manager policy server (`pdmgrd`).
	
	The policy server manages the policy database (sometimes known as *master authorization database*), updates the database replicas whenever a change is made to the master database, and replicates the policy information throughout the domains. The policy server also maintains location information about other resource managers that are operating in the domain.
	
	There must be at least one policy server that is defined for each domain.
	
	You can specify the fully qualified host name with or without the domain extension. You can specify the fully qualified host name with or without the domain extension. Examples:
	`pdmgr`
	`pdmgr.example.com`

Listening port	Specifies the port number on which the Security Access Manager policy server listens for SSL requests. The default port number is **7135**.
On systems where LDAP client is used to communicate with the Active Directory Server, you can enable SSL connections between the LDAP client and the Active Directory server. If Enable encrypted connections is selected, you are prompted for the next four values:	
Port number	Specifies the port number on which the registry server listens for SSL requests. The default port number is **636**.
Key file with full path	Specifies the fully qualified path where the existing SSL client key file is located or, if the **Create SSL key file** check box is selected, where you want the newly created SSL key file to be located. The key file holds the client-side certificates that are used in SSL communication. The file extension is always `.kdb.` This key file must be obtained by using the **gsk8capicmd** utility (which is part of GSKit 8) or the **ikeyman** utility (which is available with IBM Java) and the Active Directory server CA certificate. If the SSL key file is created automatically by the **pdconfig** utility, the full path and key file name is either `C:\Program Files\IBM\LDAP\`*`version`*`\lib\am_key.kdb` or any path and SSL key file name that you choose. If you enable SSL by using an existing SSL key file, manually copy the SSL key file to any directory on your local system. This key file must be obtained (copied) from the LDAP server.

Table 23. Security Access Manager Runtime configuration options: Active Directory (continued). * indicates a required option.

Configuration option	Description
Certificate label	Specifies the label for the SSL client certificate. This label is valid only when SSL is being used and when the LDAP server is configured to require client authentication. For example: `PDLDAP`. Use a certificate label to distinguish between multiple certificates within the SSL key file or when you use a certificate other than the default certificate in the key file. Otherwise, leave this field blank.
Key file password	Specifies the existing password that is associated with the specified SSL key file. The client key file password was set when the key file was first created. Change this password by using the **gsk8capicmd** utility (which is part of GSKit 8) or the **ikeyman** utility (which is available with IBM Java). If changed, remember this password.
Active Directory Administrator ID	Specifies the identifier for the administrator account of the Microsoft Active Directory domain. This administrator ID was created when the Microsoft Active Directory domain was created. This administrator ID should be added to the groups of Administrators, Domain Administrators, enterprise Administrators, and schema Administrators. Note that this administrator user account is for a Microsoft Active Directory user only, and not for a Security Access Manager user.
Active Directory Administrator Password	Specifies the password for the Microsoft Active Directory domain administrator ID. This administrator password was created when you created your Microsoft Active Directory administrator account.
Enable the use of email address as user ID	Enables the use of an email address as the `userPrincipalname` user ID.
Global Catalog server host name (Active Directory LDAP mode only)	Specifies the Active Directory host name for the Global Catalog Server.
Global Catalog server port (Active Directory LDAP mode only)	Specifies the Active Directory Global Catalog port. For non-SSL enablement, the default is 3268. For SSL enablement, the default is 3269.

Table 23. Security Access Manager Runtime configuration options: Active Directory (continued). * indicates a required option.

Configuration option	Description
Security Access Manager data location distinguished name	Specifies the distinguished name that is used by Microsoft Active Directory to indicate where you want to store Security Access Manager data. The default value is the input value for Active Directory Domain. For example: `dc=tivoli,dc=com` If Security Access Manager is configured by using multiple Active Directory domains, this value is automatically set to the value of the Active Directory primary domain. Note that this field is only prompted for input when the check box is not selected for **Configure to Multiple Active Directory Domains**.
Enable Tivoli Common Directory for logging	Select to enable Tivoli Common Directory. Tivoli Common Directory is a central location on systems that run Tivoli software for storing files, such as trace and message logs.
Directory Name (for Tivoli Common Directory)	Specifies the fully qualified path for the Tivoli Common Directory. • If the location of the Tivoli Common Directory is already established on the system by the installation of another Tivoli application, the directory location displays in the field and cannot be modified. • If the location of the Tivoli Common Directory was not previously established on the system, you can specify its location. If Tivoli Common Directory is enabled and the directory location was not previously established, the default common directory names are: • Windows: `C:\Program Files\ibm\tivoli\common` • AIX, Linux, or Solaris: `/var/ibm/tivoli/common` Beneath the Tivoli Common Directory, each product stores its information in a product-specific subdirectory. Each product-specific directory is named with a three-character identifier. For example, for IBM Security Access Manager for Web: *`tivoli_common_dir`*`/HPD` See the *IBM Security Access Manager for Web Troubleshooting Guide* for a complete list of three-character identifiers. If Tivoli Common Directory is not enabled, Security Access Manager will write its message and trace log data to the following location: • Windows: `C:\Program Files\Tivoli\Policy Director\log` • AIX, Linux, or Solaris: `/var/PolicyDirector/log`

Table 23. Security Access Manager Runtime configuration options: Active Directory (continued). * indicates a required option.

Configuration option	Description
Directory name	Specifies the log directory for the first software product installed. The first time that you configure Tivoli Common Directory, you can specify the directory where you want the log files to be located. Afterward, you can configure the software to use this directory.
Enable FIPS or NIST SP800-131 or Suite B	You can configure Security Access Manager to comply with security standards. To enable the configuration, set the `[ssl] ssl-compliance` value in `pd.conf` after you configure the runtime but before you configure the policy server. The **pdconfig** utility creates all the keys and certificates by using algorithms appropriate for the configured compliance type. By setting the `[ssl] ssl-compliance` value, the IBM Tivoli Directory Server client is configured to use the appropriate secure communications protocol for the compliance type selected. **Note:** All runtimes must set their `[ssl] ssl-compliance` configurations to match because runtimes cannot be mixed. Default: `[ssl] ssl-compliance='none'`. This value means that no compliance is enabled.

If you are using Active Directory as your registry, an `activedir.conf` file is created in the following directory:

%PD_INSTALL_DIR%`\etc`

where *PD_INSTALL_DIR* is the directory where Security Access Manager is installed and `C:\Program Files\Tivoli\Policy Director` is the default Windows directory.

Security Access Manager Attribute Retrieval Service

Table 24 lists options prompted for during configuration of the Security Access Manager Attribute Retrieval Service package.

Table 24. Security Access Manager Attribute Retrieval Service. * indicates a required option.

Configuration option	Description
Node Name	Specifies the WebSphere node name that is used for administration. This name must be unique within its group of nodes (cell). The host name is the DNS name or IP address of your local system.
Local Host Name	Specifies the fully qualified name of the host system on which the Security Access Manager Attribute Retrieval Service will be located.
Local Admin ID	Specifies the administrator ID with which you are logged on. (On AIX, Linux, or Solaris, this ID is **root**; on Windows, this is **Administrator**).

Table 24. Security Access Manager Attribute Retrieval Service (continued). * indicates a required option.

Configuration option	Description
Local Admin Password	Specifies the password of the local administrator.

Security Access Manager Authorization Server

Table 25 lists options prompted for during configuration of the Security Access Manager Authorization Server package.

Note: Configure the Security Access Manager Runtime package before you configure the Security Access Manager Authorization Server package.

Table 25. Security Access Manager Authorization Server configuration options. * indicates a required option.

Configuration option	Description
Domain	Specifies the domain name. The default value is **Default**, which indicates the management domain.
Policy server host name	Specifies the host name that is used by the policy server to contact this server. The default value is the host name of the local system.
Policy server port	Specifies the port number on which the policy server listens for requests. The default port number is **7135**.
Security Access Manager administrator (or Administrator ID for domain Default)	Specifies the identifier for the Security Access Manager administrator of the management domain. The default administrator ID is **sec_master**.
Password	Specifies the password for the Security Access Manager administrator ID.
Instance name	Specifies the authorization server instance name. The default authorization server instance name is always empty. Enter a unique name to configure each additional authorization server. Instance names can contain the following characters: 'a'-'z', '0'-'9', '-', and '_' (without the single quotation mark ' character.) An instance name cannot begin with a hyphen ('-') character.
Local host name	Specifies the fully qualified name of the host system on which the authorization server will be located.
Administration request port	Specifies the administration request port. The default port is **7137**.
Authorization request port	Specifies the authorization request port number. The default port number is **7136**.

IBM Security Access Manager Runtime for Java

Table 26 lists options prompted for during configuration of the IBM Security Access Manager Runtime for Java package.

Table 26. IBM Security Access Manager Runtime for Java configuration options. * indicates a required option.

Configuration option	Description
Configuration type	To configure IBM Security Access Manager Runtime for Java for use within the current Java Runtime Environment (JRE), select a configuration type: **Full**: Select if you are configuring Web Portal Manager or enabling Java applications to manage and use Security Access Manager security. **Stand-alone**: Select if you are a developer using Runtime for Java classes. You are not prompted for policy server information.

Full path of the Java Runtime Environment to configure for Security Access Manager	Specifies the path to IBM Java Runtime provided with Security Access Manager. For example:
	`/opt/ibm/java-x86_64-60/jre`
	
	If you are installing a Web Portal Manager system, ensure that you specify the Java Runtime Environment that is installed with IBM WebSphere Application Server. For example:
	`/usr/WebSphere/AppServer/java/jre`

Host name of the Security Access Manager policy server machine	Specifies the fully qualified host name of the policy server. For example: `pdmgr.example.com`
Port number of the Security Access Manager policy server machine	Specifies the port number on which the policy server listens for SSL requests. The default port number is **7135**.
Security Access Manager Policy Server domain information	null
Enable Tivoli Common Directory for logging	Select to enable Tivoli Common Directory. Tivoli Common Directory is a central location on systems that run Tivoli software for storing files, such as trace and message logs.

Table 26. IBM Security Access Manager Runtime for Java configuration options (continued). * indicates a required option.

Configuration option	Description
Directory name	Specifies the fully qualified path for the Tivoli Common Directory. • If the location of the Tivoli Common Directory is already established on the system by the installation of another Tivoli application, the directory location displays in the field and cannot be modified. • If the location of the Tivoli Common Directory is not already established on the system, you can specify its location. If Tivoli Common Directory is enabled and the directory location is not already established, the default common directory name is: • Windows: `C:\Program Files\ibm\tivoli\common` • AIX, Linux, or Solaris: `/var/ibm/tivoli/common` Beneath the Tivoli Common Directory, each Tivoli product stores its information in a product-specific subdirectory. Each product-specific directory is named with a three-character identifier. For example, for IBM Security Access Manager for Web: *`tivoli_common_dir`*`/HPD` See the *IBM Security Access Manager for Web Troubleshooting Guide* for a complete list of three-character identifiers. If Tivoli Common Directory is not enabled, Security Access Manager writes its message and trace log data to the following location: • Windows: `C:\Program Files\Tivoli\Policy Director\log` • AIX, Linux, or Solaris: `/var/PolicyDirector/log`

Security Access Manager Plug-in for Web Servers on AIX, Linux, or Solaris

Table 27 lists configuration options for the plug-in for Web Servers on AIX, Linux, or Solaris platforms.

Table 27. Plug-in for Web Servers on AIX, Linux, or Solaris. * indicates a required option.

Configuration option	Description
Full path name to the directory containing the Web server configuration file	Specifies the default installation path of the Web server. Accept this path or enter a new one.

Table 27. Plug-in for Web Servers on AIX, Linux, or Solaris (continued). * indicates a required option.

Configuration option	Description
Which virtual hosts are to be protected	Specifies the menu choice number or you can enter **x** to exit. You have three options: • If you want only one virtual host protected by the plug-in, enter the number that relates to the virtual host in the displayed list. • To secure more than one virtual host, enter values that relate to the positions of the virtual hosts in the displayed list. Separate the entered numbers by spaces. • Enter `all` to have the plug-in protect all the known virtual hosts on the server.
Security Access Manager administrative user ID	Specifies the identifier for the Security Access Manager administrator of the management domain. The default administrator ID is **sec_master**. For Active Directory Multiple Domain, this is **sec_master@***domain_name*.
Security Access Manager administrative user ID password	Specifies the password for the Security Access Manager administrator ID.
Port number on which to listen for authorization policy updates	An authorization update is the transfer of policy information delta packets from the authorization policy server during the application operation. Enter the port number to listen for authorization updates or accept the default value of **7237**.
For LDAP registries on AIX, Linux, or Solaris only, you are prompted whether to enable SSL communication.	
Enable SSL communication between the Security Access Manager Plug-in for Web Servers authorization server and the LDAP server	Enabling SSL is not necessary in environments where the Web server and registry server are located in the same secure network. If you can be sure of the integrity and security of data sent between the Web server and your registry, choosing not to use SSL improves network bandwidth by removing the security overhead.
If you enable SSL between the Security Access Manager Plug-in for Web Servers authorization server and the LDAP server, you are prompted for the next four values:	
Location of the LDAP SSL client key file	Specifies where you want the client key file to be placed. The default location is `/usr/ldap/lib/ldapkey.kdb`. **Note:** When Security Access Manager Plug-in for Web servers is installed on the same machine as the policy server and configured with SSL to LDAP, the LDAP client file cannot be shared.AIX, Linux, or Solaris file permissions are essential for protecting files from unauthorized access. The LDAP client key file can be shared if the permissions allow Plug-in users access to the file.

Table 27. Plug-in for Web Servers on AIX, Linux, or Solaris (continued). * indicates a required option.

Configuration option	Description
SSL client certificate label	Specifies the label in the client LDAP key database file of the client certificate to be sent to the server. This label is required only if the server is configured to require client authentication during SSL establishment or if you want to use a non-default certificate in your key file. Typically, the LDAP server requires only server-side certificates that were specified during creation of the client `.kdb` file. If the SSL client key file label is not required, leave this field blank.
LDAP SSL client key file password	Specifies the existing password that is associated with the specified SSL key file. The client key file password was set when the key file was first created. Change this password by using the **gsk8capicmd** utility (which is part of GSKit 8) or the **ikeyman** utility (which is available with IBM Java). If changed, remember this password.
LDAP server SSL port number *	Specifies the port number on which the LDAP server listens for SSL requests. The default port number is **636**.

Security Access Manager Plug-in for Web Servers on Windows

Table 28 lists configuration options for the plug-in for Web Servers on Windows platforms.

Table 28. Plug-in for Web Servers on Windows. * indicates a required option.

Configuration option	Description
Which virtual hosts are to be protected	Specifies a list of virtual hosts that are to be protected. Select from the list to indicate which virtual hosts that you want to protect.
Security Access Manager administrative user ID *	Specifies the identifier for the Security Access Manager administrator of the management domain. The default administrator ID is **sec_master**. For Active Directory Multiple Domain, this value is **sec_master**@*domain_name*.
Security Access Manager administrative user ID password *	Specifies the password for the Security Access Manager administrator ID.
Port number on which to listen for authorization policy updates *	Specifies the port number to listen for authorization updates. n authorization update is the transfer of policy information delta packets from the authorization policy server during the application operation. The default value is **7237**.

Security Access Manager Policy Server

The following table lists configuration options for the policy server.

Note:

1. You are prompted to configure the Security Access Manager Runtime package before you configure the Security Access Manager Policy Server package.
2. If you reconfigure the Security Access Manager policy server, you must also reconfigure Security Access Manager Runtime or IBM Security Access Manager Runtime for Java to use the certificates for the new policy server.
3. The policy server is not supported on AIX, Linux, Solaris platforms for Active Directory registry server.

Table 29. Security Access Manager Policy Server configuration options. * indicates a required option.

Configuration option	Description
Security Access Manager administrator ID *	Specifies the identifier for the Security Access Manager administrator of the management domain. The default administrator ID is **sec_master**. For Active Directory Multiple Domain, this value is **sec_master@***domain_name*.
Security Access Manager administrator password *	Specifies the password for the Security Access Manager administrator ID.
Confirm password *	Specify the Security Access Manager administrative ID password again for confirmation.
Policy server SSL port *	Specifies the port number on which the policy server listens for SSL requests. The default port number is **7135**.
SSL certificate lifecycle *	Specifies the number of days that the SSL certificate file is valid. The default number of days is **365**.
SSL connection timeout *	Specifies the duration (in seconds) that an SSL connection waits for a response before timing out. The default number of seconds is **7200**.
Enable FIPS or NIST SP800-131 or Suite B	You can configure Security Access Manager to comply with various security standards. To enable the configuration, set the `[ssl] ssl-compliance` value in `pd.conf` after you configure the runtime but before you configure the policy server. The **`pdconfig`** utility creates all the keys and certificates by using algorithms appropriate for the configured compliance type. By setting the `[ssl] ssl-compliance` value, the IBM Tivoli Directory Server client is configured to use the appropriate secure communications protocol for the compliance type selected. **Note:** All runtimes must set their `[ssl] ssl-compliance` configurations to match because runtimes cannot be mixed. Default: `[ssl] ssl-compliance='none'`. This value means that no compliance is enabled.
Management domain name	The name of the management domain. The initial administrative domain that is created when the policy server is configured is the management domain. The management domain name must be unique within the LDAP server. The name must be an alphanumeric string up to 64 characters long and is not case-sensitive. The default is **Default**.

Table 29. Security Access Manager Policy Server configuration options (continued). * indicates a required option.

Configuration option	Description
LDAP management domain location DN	The distinguished name of the location within the LDAP server where to store the Security Access Manager metadata. By default, the management domain information is stored in its own suffix with the format secAuthority=*management_domain_name*. Whether the distinguished name is specified or the default is used, the location must exist in the LDAP server.

Security Access Manager Policy Proxy Server

Table 30 lists options prompted for during configuration of the Security Access Manager Policy Proxy Server package.

Note: Configure the Security Access Manager Runtime package before you configure the Security Access Manager Policy Proxy Server package.

Table 30. Security Access Manager Policy Proxy Server configuration options. * indicates a required option.

Configuration option	Description
Policy server host name *	Specifies the fully qualified host name of the policy server. For example: `pdmgr.example.com`
Policy server port *	Specifies the port number on which the policy server listens for requests. The default port number is **7135**.
Administrator ID *	Specifies the identifier for the Security Access Manager administrator of the management domain. The default administrator ID is **sec_master**. For Active Directory Multiple Domain, this value is **sec_master@***domain_name*.
Password *	Specifies the password for the Security Access Manager administrator ID.
Local host name *	Specifies the fully qualified name of the host system where the policy proxy server is to be located. For example: `pdproxy.example.com`
Administration request port *	Specifies the administration request port. The default port is **7139**.
Proxy request port *	Specifies the proxy request port. The default port is **7138**.

Security Access Manager Web Portal Manager

Table 31 lists options prompted for during configuration of the Security Access Manager Web Portal Manager package.

Table 31. Security Access Manager Web Portal Manager configuration options. * indicates a required option.

Configuration option	Description
Full path * (IBM WebSphere Application Server installation directory)	Specifies the existing IBM WebSphere Application Server installation directory. Type the existing fully qualified path location for one of the following types of IBM WebSphere Application Servers: • If clustering, specify the information for the existing IBM WebSphere Application Server Network Deployment. • If a single server, specify the information for the existing IBM WebSphere Application Server Default: `C:\Program Files\IBM\WebSphere\AppServer`
Host name * (IBM WebSphere Application Server)	Specifies the host name or IP address for one of the following types of IBM WebSphere Application Servers: • If clustering, specify the information for the existing IBM WebSphere Application Server Network Deployment. • If a single server, specify the information for the existing IBM WebSphere Application Server For example: `was01`
Port * (IBM WebSphere Application Server)	Specifies the port number, on which the IBM WebSphere Application Server listens for SOAP administration requests, for one of the following types of IBM WebSphere Application Servers: • If clustering, specify the information for the existing IBM WebSphere Application Server Network Deployment. • If a single server, specify the information for the existing IBM WebSphere Application Server Use the default port number, which is server-dependent. The default IBM WebSphere Application Server port number is **8880**. **Note:** Change this value only if the server is already configured to use a different port number. This process does not attempt to set this value for the server.
Enable SSL with the IBM WebSphere Application Server	Select the check for Secure Sockets Layer (SSL) communication to the existing IBM WebSphere Application Server. Default: not enabled (The check box is not selected.)

Table 31. Security Access Manager Web Portal Manager configuration options (continued). ***** indicates a required option.

Configuration option	Description
IBM WebSphere Application Server administrator ID *	Specifies the identifier for an administrator account for the existing IBM WebSphere Application Server. All administrator IDs must follow the IBM WebSphere Application Server naming policy.
IBM WebSphere Application Server administrator password *	Specifies the password for the specified existing IBM WebSphere Application Server administrator ID. This administrator password was created when you created the IBM WebSphere Application Server administrator account.
SSL truststore file with full path *	Specifies the fully qualified path where the existing truststore file is located. Use the truststore file to handle server-side certificates that are used in SSL communication. The truststore file verifies the certificate that is presented by the server. The signer of the SSL certificate must be recognized as a trusted certificate authority (CA). To specify the SSL client key file, type the fully qualified path and file name for the truststore file or browse and choose an existing truststore file.
SSL truststore file password	Specifies the existing password that protects the truststore file if a secure connection with the IBM WebSphere Application Server is being used. The truststore file password was set when the truststore file was first created.
SSL key file with full path	Specifies the fully qualified path where the existing key file is located. The key file holds the client-side certificates that are used in SSL communication. To specify the SSL client key file, type the fully qualified path and file name for the key file or browse and choose an existing key file.
SSL key file password	Specifies the existing password that is associated with the specified client key file. The key file password was set when the key file was first created.
Clusters *	Select an existing cluster where Web Portal Manager is to be deployed from the list displayed. You must select at least one cluster or application server. For example: `WPM_Cluster`
Application servers *	Select an existing application server from the list that is displayed where Web Portal Manager is to be deployed. You must select at least one application server or cluster. For example: `WebSphere:cell-was01Cell01,node=was01Node01,server==server1`
Web servers	Select an existing Web server from the list that is displayed where Web Portal Manager is to be deployed. For example: `WPM_WebServer`

Table 31. Security Access Manager Web Portal Manager configuration options (continued). * indicates a required option.

Configuration option	Description
Host name * (Security Access Manager policy server or policy proxy server)	Specifies the host name or IP address of the Security Access Manager policy server or policy proxy server. The policy server manages the policy database (sometimes referred as the *master authorization database*), updates the database replicas whenever a change is made to the master database, and replicates the policy information throughout the domains. The policy server also maintains location information about other resource managers that are operating in the domain. There must be at least one policy server that is defined for each domain. For example: `WPM_PolServer`
Port * (Security Access Manager policy server or policy proxy server)	Specifies the port number on which the Security Access Manager policy server or policy proxy server listens for SSL requests. Use the default port number value, which is server-dependent. The default port number for the policy server is **7135**. The default port number for the policy proxy server is **7138**.
Is Security Access Manager authorization server configured?	Select the check box to configure the Security Access Manager authorization server. Default: not enabled (The check box is not selected.)
Host name *	Specifies the existing fully qualified host name or IP address to configure the Security Access Manager authorization server to be used by Web Portal Manager. For example: `WPM_AuthServer`
Port *	Specifies the port number on which the Security Access Manager authorization server listens for SSL requests. Use the default port number value, which is server-dependent. The default port number for the authorization server is **7136**.
Administrator ID *	Specifies the identifier for an existing administrator account for the specified Security Access Manager domain. The default Security Access Manager administrator ID is **sec_master**.
Administrator password *	Specifies the password that is associated with the specified Security Access Manager administrator ID. This administrator password was created when you created the administrator account.

Table 31. Security Access Manager Web Portal Manager configuration options (continued). ***** indicates a required option.

Configuration option	Description
Domain *	Specifies the name of the domain. The domain must exist. Any security policy that is implemented in a domain affects only those objects in that domain. Users with authority to perform tasks in one domain do not necessarily have the authority to perform those tasks in other domains. The default domain name is **Default**, which indicates the management domain.

Security Access Manager WebSEAL

Table 32 lists options prompted for during configuration of the Security Access Manager WebSEAL package.

Note: Configure the Security Access Manager Runtime package before you configure the Security Access Manager WebSEAL package.

Table 32. Security Access Manager WebSEAL configuration options. ***** indicates a required option.

Configuration option	Description
WebSEAL instance name *	Specifies the fully qualified host name that is used by the policy server to contact the WebSEAL server.
Use logical network interface	Specifies to use a logical network interface. If **yes**, you are prompted for the IP address of the logical network interface.
WebSEAL host name *	Specifies the host name of the WebSEAL server.
WebSEAL listening port *	Specifies the port number on which the WebSEAL server listens for requests. The default port number is **7234**.
Administrator ID *	Specifies the identifier for the Security Access Manager administrator of the management domain. The default administrator ID is **sec_master**.
Administrator password *	Specifies the password for the Security Access Manager administrator ID.
Allow HTTP access (y/n)	Specifies whether to enable HTTP access. If selected, you must specify the HTTP port number. HTTP access is enabled by default.
HTTP port [80]	Specifies the HTTP port. The default port number is **80**. If there is a conflict with the port, configuration detects the conflict and incrementally increases the port number.
Allow secure HTTPS access (y/n)	Specifies whether to enable HTTPS access. If selected, you must specify the HTTPS port number. HTTPS access is enabled by default.

Table 32. Security Access Manager WebSEAL configuration options (continued). * indicates a required option.

Configuration option	Description
HTTPS port [443]	Specifies the HTTPS port. The default port number is **443**. If there is a conflict with the port, configuration detects the conflict and incrementally increases the port number choice.
Web document root directory [opt/pdweb/www-default/docs]	Default directories are as follows: • AIX, Linux, and Solaris: `/opt/pdweb/www-default/docs` • Windows: `C:\Progam Files\Tivoli\ PolicyDirector \PDWeb\www-default\docs`
Enable SSL with the registry server	Specifies whether to enable encrypted Secure Sockets Layer (SSL) connections with an LDAP server. **Note:** You must first configure the LDAP server for SSL access. Default: enabled (check box is selected)
Key file with full path	Specifies the fully qualified path where the SSL client key database file is on the runtime system. This key file must be obtained from the LDAP server. Any file extension can be used, but the file extension is normally `.kdb`. Use the SSL key file to handle certificates that are used in SSL communication. The signer of the SSL certificate must be recognized as a trusted certificate authority in the client key database.
Key file password	Specifies the existing password that is associated with the specified SSL key file. The client key file password was set when the key file was first created. Change this password by using the **gsk8capicmd** utility (which is part of GSKit 8) or the **ikeyman** utility (which is available with IBM Java). If changed, remember this password.

Table 32. Security Access Manager WebSEAL configuration options (continued). * indicates a required option.

Configuration option	Description
Certificate label	Specifies the SSL certificate label of the client certificate in the SSL key database that is sent to the registry server if the registry server is configured to perform both server and client authorization during SSL establishment. This label is only valid when SSL is used and when the registry server is configured to require client authorization. Typically, the registry server requires only server-side certificates that are specified during creation of the client `.kdb` file. The certificate label is an alphanumeric, case-sensitive string that you choose. String values should be characters that are part of the local code set. For example: `PDLDAP` This field requires that you type any character. Because you do not need to set up client-side certificate authentication, the character that you specify is ignored.
SSL port	Specifies the port number on which the LDAP server listens for SSL requests. A valid port number is any positive number that is allowed by TCP/IP and that is not currently being used by another application.

Appendix E. Language support installation

Security Access Manager is translated into several languages. The translations for these languages are provided as language support packages for each product component. To use the product components in a language other than English, you must install the language support package for that component.

Use these instructions to install the language support package if you are using the command-line installation method or the script installation method to install Security Access Manager components.

If you are using the Launchpad installation methods to install Security Access Manager components, the language support package is installed automatically and you do not need to complete these instructions.

Before you continue with the installation, ensure that you review all language support topics in the support knowledge website.

Language support overview

Security Access Manager software is translated into the following languages:

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

Note:

1. Only the panels in Web Portal Manager support the Hebrew language; messages and online help display in English.

The translations for these languages are provided as language support packages for the product. To obtain language support for Security Access Manager, you must install the language support package for that product. Each language is a separately installable product installation image.

- If you use native installation utilities to install Security Access Manager, you must install the language package *after* you install Security Access Manager

components but *before* you configure them. If you do not install the language support package, the associated product displays all text in English.
- If you are installing Security Access Manager Session Management Server or Session Management Command Line on Windows, you must install the language pack *after* you install the Session Management component.

If language support for a product is installed and you upgrade the product, you must also install the corresponding language support product, if one exists. See the upgrade documentation for the specific product to determine whether language support is required. If you do not install the language support after you upgrade, the associated product might display some fields and messages in English.

Installing language support packages for Security Access Manager

Enable language support for Security Access Manager by installing one or more language support packages.

Before you begin

Attention: When you install the Security Access Manager language packs, if a DBCS language is used for the installation, set the operating system locale to match the language that the installation program uses.

Procedure

1. Log on as **root** or as an Administrative user.
2. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. Ensure that IBM Java Runtime provided with Security Access Manager is installed for your particular operating system. For instructions, see one of the following procedures:
   - "AIX: Installing IBM Java Runtime" on page 31.
   - "Linux: Installing IBM Java Runtime" on page 32.
   - "Solaris: Installing IBM Java Runtime" on page 33.
   - "Windows: Installing IBM Java Runtime" on page 34.
4. Depending on the Security Access Manager component that you want to install, run one or more of the following setup scripts.
   - To install with a wizard:
     a. Ensure that the IBM Java Runtime is available in the command execution path (or prefix the command with the JRE directory).
     b. Run the following command:

        ```
        java -jar language_package.jar
        ```

        where *language_package.jar* is the name of the language package to install:

        carslp.jar
        Installs language packages for Common Auditing and Reporting Service.

        pdjrte_lp_setup.jar
        Installs language packages for IBM Security Access Manager Runtime for Java.

        pdrte_lp_setup.jar
        Installs language packages for Security Access Manager Runtime.

pdweb_lp_setup.jar
Installs language packages for Security Access Manager WebSEAL.

pdwbpi_lp_setup.jar
Installs language packages for Security Access Manager Plug-in for Web Servers.

pdwebrte_lp_setup.jar
Installs language packages for Security Access Manager Web Security Runtime.

smslp.jar
Installs language packages for Security Access Manager Session Management Server and Security Access Manager Session Management Command Line.

c. Click **Next** to begin installation. The Software License Agreement window is displayed.
d. To accept the license agreement, select the **I accept** check box to accept the terms.
e. Click **Next**. A dialog shows a list of the languages.
f. Select the language packages that you want to install.
g. Click **Next**. A dialog shows the location and features of the languages that you selected.
h. To accept the languages selected, click **Next**. The installation wizard validates that sufficient disk space is available.
i. To install the languages that you selected, click **Next**.
j. After installation for the Security Access Manager language pack completes successfully, click **Finish** to close the wizard.

- To install in console mode:
  a. Ensure that the IBM Java Runtime is available in the command execution path (or prefix the command with the JRE directory).
  b. Run the following command:

```
java -jar language_package.jar -console
```

where *language_package.jar* is the name of the language package to install:

carslp.jar
Installs language packages for Common Auditing and Reporting Service.

pdjrte_lp_setup.jar
Installs language packages for IBM Security Access Manager Runtime for Java.

pdrte_lp_setup.jar
Installs language packages for Security Access Manager Runtime.

pdweb_lp_setup.jar
Installs language packages for Security Access Manager WebSEAL.

pdwbpi_lp_setup.jar
Installs language packages for Security Access Manager Plug-in for Web Servers.

pdwebrte_lp_setup.jar
Installs language packages for Security Access Manager Web Security Runtime.

smslp.jar
Installs language packages for Security Access Manager Session Management Server and Security Access Manager Session Management Command Line.

c. Complete the prompts presented to install the language packages.

- To install silently using a response file:

Note: The silent installation method is not supported on Linux systems.

a. Create a response file.

On AIX or Solaris:

1) Open a text editor and create a file with a `.rsp` extension.
2) In the file, specify the information specific to your installation. Use this sample as a guide:

```
##########################################
# Auto-accept the license
# Note: By setting this to true you are accepting the terms
# and conditions of the license.
-G licenseAccepted=true
#
# Select languages to install by setting the feature to true.
# Set to false if you do not want to install a language.
#
-P arLangfeature.active=true
-P csLangfeature.active=true
-P deLangfeature.active=true
-P esLangfeature.active=true
-P frLangfeature.active=true
-P huLangfeature.active=true
-P itLangfeature.active=true
-P jaLangfeature.active=true
-P koLangfeature.active=true
-P plLangfeature.active=true
-P pt_BRLangfeature.active=true
-P ruLangfeature.active=true
-P zh_CNLangfeature.active=true
-P zh_TWLangfeature.active=true
```

Note: Ensure that the following line is included in the response file:

```
-G licenseAccepted=true
```

3) Save the file.

On Windows:

1) On the installation media, locate the sample response file named `\bin\isamLangPack.rsp`.
2) Edit the file with a text editor and use the instructions in the file to specify the information specific to your installation.
3) Ensure that the following line is included in the response file:

```
-G licenseAccepted=true
```

4) Save the file.

b. Ensure that the IBM Java Runtime is available in the command execution path (or prefix the command with the JRE directory).

c. Run the following command:

```
java -jar language_package.jar -silent -options response_file.rsp
```

where *language_package.jar* is the name of the language package to install:

carslp.jar
Installs language packages for Common Auditing and Reporting Service.

pdjrte_lp_setup.jar
Installs language packages for IBM Security Access Manager Runtime for Java.

pdrte_lp_setup.jar
Installs language packages for Security Access Manager Runtime.

pdweb_lp_setup.jar
Installs language packages for Security Access Manager WebSEAL.

pdwbpi_lp_setup.jar
Installs language packages for Security Access Manager Plug-in for Web Servers.

pdwebrte_lp_setup.jar
Installs language packages for Security Access Manager Web Security Runtime.

smslp.jar
Installs language packages for Security Access Manager Session Management Server and Security Access Manager Session Management Command Line.

and where *response_file.*.rsp is the path and file name of the response file you created in the first step.

Installing language support packages for IBM Tivoli Directory Server

In addition to installing language packages for Security Access Manager software, you must install language packages for the user registry, such as the IBM Tivoli Directory Server.

These language packages are provided on the Security Access Manager product media for the supported platforms.

The IBM Tivoli Directory Server requires that at least one language pack is installed on all AIX, Linux, or Solaris systems for the IBM Tivoli Directory Server client and administrative utilities to operate correctly. To determine whether a language pack is installed, see "LANG variable on AIX, Linux, or Solaris systems" on page 344.

After you install the Tivoli Directory Server language pack, you must install the fix pack for the language pack. The fix pack image is included in the Security Access Manager media in the `imagepath/platform/tdsV6.3FP/LangPack` directory. See the readme file in the `LangPack` directory for installation instructions.

After you install the Tivoli Directory Server language packages, you must install the IBM DB2 language packs.

Use the language pack installation instructions in the IBM Tivoli Directory Server Information Center:http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml

Attention: When you install the IBM Tivoli Directory Server product, or its language packs, or the Security Access Manager language packs, if a DBCS language is used for the installation, set the operating system locale to match the language that the installation program uses.

Locale environment variables

As with most current operating systems, localized behavior is obtained by specifying the wanted locale. For Security Access Manager software, you set the **LANG** environment variable to the wanted locale name as specified by POSIX, X/Open, or other open systems standards.

Note: If you are in a Windows environment, you can alternatively modify the language setting in the **Regional Settings** of the **Control Panel**.

If you specify the **LANG** environment variable and modify the regional settings, the **LANG** environment variable overrides this regional setting.

As specified by open systems standards, other environment variables override **LANG** for some or all locale categories. These variables include the following choices:

- **LC_COLLATE**
- **LC_CTYPE**
- **LC_MONETARY**
- **LC_NUMERIC**
- **LC_TIME**
- **LC_MESSAGES**
- **LC_ALL**

If any of the previous variables are set, you must remove their setting for the **LANG** variable to have full effect.

LANG variable on AIX, Linux, or Solaris systems

Most AIX, Linux, and Solaris systems use the **LANG** variable to specify the wanted locale. Different AIX, Linux, and Solaris operating systems, however, require different locale names to specify the same language. Be sure to use a value for **LANG** that is supported by the AIX, Linux, or Solaris operating system that you are using.

To obtain the locale names for your AIX, Linux, or Solaris system, enter the following command:

```
locale –a
```

The IBM Tivoli Directory Server requires that at least one language pack is installed on all AIX, Linux, and Solaris systems for the IBM Tivoli Directory Server client and administrative utilities (for example, **idscfgdb** or **db2dif**) to operate correctly. To verify that you have a language package that is installed for your AIX, Linux, or Solaris system, enter the following command:

```
locale
```

If you loaded a language package (for example **bos.loc.iso.en_us**), the output of the **locale** command would be:

```
LANG=en_US
LC_COLLATE="en_US"
LC_CTYPE="en_US"
LC_MONETARY="en_US"
LC_NUMERIC="en_US"
LC_TIME="en_US"
LC_MESSAGES="en_US"
LC_ALL=
```

If no language packages are installed, the output would be:

```
LANG=en_US
LC_COLLATE="C"
LC_CTYPE="C"
LC_MONETARY="C"
LC_NUMERIC="C"
LC_TIME="C"
LC_MESSAGES="C"
LC_ALL=
```

LANG variable on Windows systems

Most operating systems do not use the **LANG** environment variable. Security Access Manager software, however, can use **LANG** to determine the wanted language. To do so, set the **LANG** environment variable to the canonical locale name based on the ISO language or territory codes without a code set suffix. For example:

- **fr** is the locale for standard French
- **ja** is the locale for Japanese
- **pt_BR** is the locale for Brazilian Portuguese
- **C** is the locale for English in C locale

Using locale variants

Although Security Access Manager software currently provides only one translated version for each language, you can use a preferred locale variant, and Security Access Manager finds the corresponding language translation. For example, Security Access Manager provides one translation for French, but each of the following locale settings finds the appropriate translation:

- **fr** is the locale name for standard French
- **fr_FR** is the locale name for French in France
- **fr_CA** is the locale name for French in Canada
- **fr_CH** is the locale name for French in Switzerland

Message catalogs

Message catalogs are typically installed in a `msg` subdirectory and each of these message catalogs is installed under a language-specific subdirectory. For example, the Security Access Manager base components use the following directories:

- On AIX, Linux, or Solaris systems:

  `/opt/PolicyDirector/nls/msg/`*locale*

- On Windows systems:
  install_dir/nls/msg/*locale*

Other Security Access Manager components use similar directories for their message catalogs.

Security Access Manager recognizes variations in AIX, Linux, or Solaris locale names and is usually able to map the specified value to the appropriate message catalog.

The **NLSPATH** environment variable finds the appropriate message catalog directory, as specified by open systems standards. For example, if the message catalogs are in /opt/PolicyDirector/nls/msg, the **NLSPATH** variable is set to the following value:

```
/opt/PolicyDirector/nls/msg/%L/%N.cat:/opt/PolicyDirector/nls/msg/%L/%N
```

Note: For Windows, use a semicolon (**;**) instead of a (**:**) as the separator. For example:

```
C:\Program Files\PolicyDirector\nls\msg\%L\%N.cat;C:\Program
Files\PolicyDirector\nls\msg\%L\%N
```

The **%L** directive is expanded to the message catalog directory that most closely matches the current user language selection, and **%N.cat** expands to the wanted message catalog.

If a message catalog is not found for the wanted language, the English **C** message catalogs are used.

For example, suppose that you specify the AIX locale for German in Switzerland as follows:

```
LANG=De_CH.IBM-850
```

The **%L** directive is expanded in the following order to locate the specified locale:

1. **de_CH**
2. **de**
3. **C**

Because Security Access Manager does not provide a German in Switzerland language package, **de_CH** is not found. If the Security Access Manager German language package is installed, **de** is used. Otherwise, the default locale **C** is used, causing text to be displayed in English.

Text encoding (code set) support

Different operating systems often encode text in different ways. For example, Windows systems use **SJIS** (code page 932) for Japanese text, but AIX, Linux, or Solaris systems often use **eucJP**.

In addition, multiple locales can be provided for the same language so that different code sets can be used for the same language on the same machine. Providing multiple locales for the same language can cause problems when text is moved from system to system or between different locale environments.

Security Access Manager addresses these problems by using Unicode and UTF-8 (the multibyte form of Unicode) as the internal canonical representation for text.

Message catalogs are encoded by using UTF-8, and the text is converted to the locale encoding before it is presented to the user. In this way, the same French message catalog files can be used to support a variety of Latin 1 code sets, such as ISO8859-1, Microsoft 1252, IBM PC 850, and IBM MVS™ 1047.

UTF-8 is also used to achieve text interoperability. For example, Common Object Request Broker Architecture (CORBA) strings are transmitted as UTF-8. This enables remote management within a heterogeneous network in which local text encoding can vary. For example, Japanese file names can be manipulated on Japanese PC endpoints from a desktop that runs in the AIX, Linux, or Solaris Japanese EUC locale.

Text interoperability across the secure domain is also achieved by storing strings as UTF-8 within the Tivoli object database. Strings are converted to the local encoding for viewing and manipulation by applications that are running on different operating system code sets.

Location of code set files

Interoperability across your secure domain depends on code set files, which are used to complete UTF-8 conversion and other types of encoding-specific text processing. These files are installed in the following directories:

- On AIX, Linux, or Solaris systems:

  `/opt/PolicyDirector/nls/TIS`
- On Windows systems:

  install_dir`\nls\TIS`

Uninstalling Security Access Manager language support packages

Use the following procedure to uninstall Security Access Manager language support packages.

Before you begin

Unconfigure all Security Access Manager components before uninstalling language packs. See Appendix K, “Uninstallation,” on page 405.

Procedure

1. Change to the uninstall directory for the package you want to uninstall:
   - On AIX, Linux, or Solaris systems:

     Web Security Runtime
     `/AMWebRTELP/lp_uninst`

     Plug-in for Web Servers
     `/PDWpiLP/lp_uninst`

     Runtime
     `/opt/PolicyDirector/PDBLP/lp_uninst`

     Runtime for Java
     `/opt/PolicyDirector/PDJrtLP/lp_uninst`

Session Management Server and Session Management Command Line
/opt/pdsms/SMSLP/lp_uninst

WebSEAL
/opt/pdweb/PDWebLP/lp_uninst

- On Windows systems:

Web Security Runtime
c:\Program Files\Tivoli\PDWebRTE\AMWebRTELP\lp_uninst

Plug-in for Web Servers
c:\Program Files\Tivoli\PDWebPI\PDWpiLP/lp_uninst

Runtime
c:\Program Files\Tivoli\Policy Director/PDBLP/lp_uninst

Runtime for Java
c:\Program Files\Tivoli\Policy Director\PDJrtLP/lp_uninst

Session Management Server and Session Management Command Line
c:\Program Files\Tivoli\PDSMS\SMSLP\lp_uninst

WebSEAL
c:\Program Files\Tivoli\PDWeb/PDWebLP/lp_uninst

2. To uninstall the language support packages, enter one of the following commands:
   - On AIX, Linux, or Solaris systems:
     jre_path/java -jar *package*
   - On Windows systems:
     jre_path\java -jar *package*

   where *jre_path* is the path where the Java file is located and *package* is one of the following choices:

   Note: If the Java file is in the path, you do not have to specify *jre_path*.

   cars_lp_uninstall.jar
   Specifies the location of the language packages for Common Auditing and Reporting Service.

   pdrte_lp_uninstall.jar
   Specifies the location of the language packages for Security Access Manager Runtime.

   pdjrte_lp_uninstall.jar
   Specifies the language package for IBM Security Access Manager Runtime for Java.

   pdsms_lp_uninstall.jar
   Specifies the language package for Security Access Manager Session Management Server and Security Access Manager Session Management Command Line.

   pdwbpi_lp_uninstall.jar
   Specifies the language package for Plug-in for Web Servers.

   pdweb_lp_uninstall.jar
   Specifies the language package for Security Access Manager WebSEAL.

   pdwebrte_lp_uninstall.jar
   Specifies the language package for Security Access Manager Web Security Runtime.

Note: If a message is displayed that states a properties file exists for a language and asks if you want to remove the file, click **Yes to All**. Proceed with the uninstallation. If the uninstallation completion text lists any errors related to removing files, look in the installation directories to verify that the files have been removed. If the files still exist, delete them.

Appendix F. Password management

Use the `pdconf` utility to obfuscate or delete passwords that are stored in a configuration file.

Passwords that are used during the automated configuration are written and stored in an options file. You can obfuscate these passwords at any time. You can also delete these passwords from an options file after you complete configuration.

To manage configuration passwords in options files, see the following activities:

Table 33. Automated configuration password tasks

Goal	Task
Obfuscate a password on AIX, Linux, or Solaris	"Obfuscating passwords on AIX, Linux, or Solaris" on page 352
Obfuscate a password on Windows	"Obfuscating passwords on Windows" on page 353
Delete a password on AIX, Linux, or Solaris	"Deleting a stored password on AIX, Linux, and Solaris" on page 354
Delete a password on Windows	"Deleting a stored password on Windows" on page 355

About configuration option files

An *options* file contains variables, such as passwords. The automated configuration script uses the contents in the options file to facilitate an unattended configuration.

By default, the values in the options file are empty. Before you use the automated configuration script, complete the options file template with required passwords.

- On Windows, the `configure_isam.conf` options file stores configuration passwords.
- On AIX, Linux, or Solaris, each component has a default configuration options file, called

  `configure_`*`component`*`.options.template`

  where *component* is an installed component.

  See "Obfuscating passwords on AIX, Linux, or Solaris" on page 352 for a table of file names for AIX, Linux, and Solaris systems.

Best practices for securing configuration passwords

The configuration options file used by the automated configuration script stores passwords in clear text by default. Optionally, you can obfuscate those passwords. See "Obfuscating passwords on AIX, Linux, or Solaris" on page 352 or "Obfuscating passwords on Windows" on page 353

Obfuscated passwords return in clear text, however, when you specify the `pdconf` options `getstanza` or `getentry`.

To lessen security concerns about stored passwords, you can delete the entry that contains the password from the configuration options file. See “Deleting a stored password on AIX, Linux, and Solaris” on page 354 or “Deleting a stored password on Windows” on page 355.

Obfuscating passwords on AIX, Linux, or Solaris

Use the `pdconf` utility to obfuscate passwords that are in configuration options files on AIX, Linux, or Solaris.

Before you begin

You must modify the default options template file with passwords for the automated configuration script to complete unattended configuration. See the automated configuration instructions for the component you are installing:

- “Automating the configuration of a policy server” on page 119
- “Automating the configuration of an authorization server” on page 131
- “Automating the configuration of a runtime for Java system” on page 154
- “Automating the configuration of a policy proxy server” on page 167
- “Automating the configuration of a runtime system” on page 179
- “Automating the configuration of Web Portal Manager” on page 202
- “Automating configuration of the Apache Server plug-in or IBM HTTP Server plug-in” on page 230
- “Automating configuration of a session management server” on page 287
- “Automating configuration of a session management command line” on page 301

About this task

The required passwords are displayed in the options file to facilitate unattended configurations.

You can use the `pdconf` utility to obfuscate any specified password. By default, `pdconf` is in the `/opt/PolicyDirector/sbin/` subdirectory.

Procedure

1. Locate the options file on your system. You must know its location to complete the following steps. The default location for the template files is:

   `/opt/PolicyDirector/example/config`

   The following table shows the default name of the AIX, Linux, or Solaris options template file for each component:

Table 34. Default component options template files on AIX, Linux, or Solaris

Component	Options file on AIX, Linux, or Solaris
Policy server	`configure_policysvr.options.template`
Authorization server	`configure_authzsvr.options.template`
Java system	`configure_javarte.options.template`
Policy proxy server	`configure_policysvproxy.options.template`
Runtime system	`configure_runtime.options.template`
Web Portal Manager	`configure_wpm.options.template`

Table 34. Default component options template files on AIX, Linux, or Solaris (continued)

Component	Options file on AIX, Linux, or Solaris
Attribute Retrieval Service	`configure_webars.options.template`
Plug-in for Web servers	`configure_webpi.options.template`
Session management server - configuration	`configure_sms.options.template`
Session management server - deployment	`deploy_sms.options.template`
WebSEAL	`configure_webseal.options.template`

2. Open the file and note the entry and password value that you want to obfuscate.
3. Run the following command:

   ```
   /opt/PolicyDirector/sbin/pdconf -f configure_component.options.template
   setentry -obfuscate config entry password
   ```

   Where:

   configure_*component*.**options.template**
   Is the options template file that stores the passwords for the automated configuration script. *component* is the Security Access Manager component. This file might be saved as a different name.

   -obfuscate
   Specifies not to store the value in clear text.

   config Is the stanza name to write the value.

   Note: This stanza name must be `config`.

   entry Is the key matching the environment variable in the template file. For example, `SECMASTERPWD`.

   password
   Is the password to obfuscate.

Obfuscating passwords on Windows

Use the `pdconf.exe` utility to obfuscate passwords that are in configuration options files on Windows.

Before you begin

You must modify the default options template file with passwords for the automated configuration script to complete unattended configuration. See the automated configuration instructions for the component you are installing:

- "Automating the configuration of a policy server" on page 119
- "Automating the configuration of an authorization server" on page 131
- "Automating the configuration of a runtime for Java system" on page 154
- "Automating the configuration of a policy proxy server" on page 167
- "Automating the configuration of a runtime system" on page 179
- "Automating the configuration of Web Portal Manager" on page 202
- "Automating configuration of the Internet Information Service plug-in" on page 232
- "Automating configuration of a session management server" on page 287

- "Automating configuration of a session management command line" on page 301

About this task

The required passwords are displayed in the options file to facilitate unattended configurations.

You can use the `pdconf` utility to obfuscate any specified password. By default, `pdconf` is in the `C:\Program Files\Tivoli\Policy Director\sbin\` subdirectory.

Procedure

1. Locate the options file on your system. You must know its location to complete the following steps. By default, these template files are installed in the following location:

   ```
   C:\Program Files\Tivoli\PolicyDirector\example\config
   ```

2. Open the `configure_isam.conf` file and note the entry and password value that you want to obfuscate.
3. Run the following command:

   ```
   C:\Program Files\Tivoli\Policy Director\sbin\pdconf -f configure_isam.conf
   setentry -obfuscate config entry password
   ```

   Where:

   configure_isam.conf
   Is the options template file that stores the passwords for the automated configuration script.

   -obfuscate
   Identifies that the value should not be stored in clear text.

   config Is the stanza name to write the value.

   Note: This stanza name must be `config`.

   entry Is the key matching the environment variable in the template file. For example, `SECMASTERPWD`.

   password
   Is the password to obfuscate.

Deleting a stored password on AIX, Linux, and Solaris

Use the `pdconf` utility to delete passwords that are stored in a configuration file on AIX, Linux, or Solaris.

Before you begin

You must modify the default options template file with passwords for the automated configuration script to complete unattended configuration. See any "Automating the configuration of a *component*" procedure for the component in the *IBM Security Access Manager for Web Installation Guide*.

About this task

The required passwords are displayed in the options file to facilitate unattended configurations.

Obfuscated passwords return in clear text when the pdconf option of getstanza or getentry is used.

To avoid exposure of a password, delete any password when you are done with the configuration script.

Procedure

1. Locate the options file on your system. You must know its location to complete the following steps. The default location for the options files is /opt/PolicyDirector/example/config.
2. Run the pdconf tool:

   path to pdconf tool/pdconf -f *path to options file/optionsfile* deleteentry *stanza entry*

   Where:

   path to pdconf tool
   Specifies the directory that contains the pdconf.exe tool. By default, this path is opt/PolicyDirector/sbin/pdconf.

   optionsfile
   Specifies the name of the configuration options file that contains the password. The default template options files for each component are called configure_*component*.options.template, but you might have renamed it.

   deleteentry
   Deletes the entry and value in the specified stanza in the options file.

   stanza Specifies the stanza name from which you want to delete the password.

   entry Specifies the entry of the specified configuration options file and stanza. For example, SECMASTERPWD.

Deleting a stored password on Windows

Use the pdconf utility to delete passwords that are stored in a configuration options file on Windows.

Before you begin

You must modify the default options template file with passwords for the automated configuration script to complete unattended configuration. See any "Automating the configuration of a *component*" procedure for the component in this *IBM Security Access Manager for Web Installation Guide*.

About this task

The required passwords are displayed in the options file to facilitate unattended configurations.

Obfuscated passwords return in clear text when the pdconf option of getstanza or getentry is used.

To avoid exposure of a password, delete any password when you are done with the configuration script.

Procedure

1. Locate the options file on your system. You must know its location to complete the following steps.

   The default location for the options files is: `C:\Program Files\Tivoli\Policy Director\examples\config\configure_isam.conf`.

2. Run the `pdconf` tool:

   path to pdconf tool`\pdconf -f "`*path to options file*`\configure_isam.conf" deleteentry` *stanza entry*

   Where:

   path to pdconf tool
   : Specifies the directory that contains the `pdconf.exe` tool. By default, this path is `C:\Program Files\Tivoli\Policy Director\sbin\pdconf`.

   "*path to options file**optionsfile*"
   : Specifies the path and name of the configuration options file containing the password. This must be in quotations if the path contains spaces. The options file is called `configure_isam.conf`.

   deleteentry
   : Deletes the entry and value in the specified stanza in the options file.

   stanza
   : Specifies the stanza name from which you want to delete the password.

   entry
   : Specifies the entry of the specified configuration options file and stanza. For example, `SECMASTERPWD`.

Appendix G. Standby policy server (AIX) setup

You can configure a standby server to take over policy server functions in the event of a system failure or unplanned outage.

When the policy server goes down, the standby policy server acts as the policy server until the primary policy server assumes its original role. In turn, the standby policy server reverts to a standby role. At any time, there is *only one* active policy server and *only one* shared copy of the policy databases.

Security Access Manager supports the use of one standby policy server on supported AIX platforms. In addition, deploying a standby policy server requires the installation and configuration of High Availability Cluster Multi-Processing (IBM PowerHA®, formerly HACMP) software, a clustering solution that is designed to provide high-availability access to business-critical data and application through component redundancy and application failover.

The PowerHA scenario is provided as a general guide to show you how to install and configure a PowerHA environment for standby policy server capability. After you set up your PowerHA environment, follow product-specific instructions about creating a standby policy server within a Security Access Manager secure domain. Scripts and examples are provided for your convenience.

For more information about installing and configuring PowerHA, see:

- IBM PowerHA SystemMirror 7.1: http://pic.dhe.ibm.com/infocenter/aix/v7r1/topic/com.ibm.aix.powerha.navigation/powerha_main.htm
- IBM PowerHA SystemMirror 6.1: http://pic.dhe.ibm.com/infocenter/aix/v6r1/topic/com.ibm.aix.powerha.navigation/powerha_main.htm
- IBM PowerHA for AIX Cookbook: http://www.redbooks.ibm.com/redbooks/pdfs/sg247739.pdf
- The PowerHA for AIX (formerly HACMP™) cheat sheet: http://www.ibm.com/developerworks/aix/library/au-hacmpcheatsheet/index.html

Rules

- You can create one primary policy server and one standby policy server.
- Both the primary and standby policy servers must be on separate AIX systems that are part of a High Availability Cluster Multi-Processing (PowerHA) environment.
- Each AIX system must have access to a shared disk array that is configured for data redundancy.
- The policy database and the configuration files that are used by the policy server must be on a shared disk array.
- The registry server, such as IBM Tivoli Directory Server, must be available and installed on a separate system.
- Back up any shared data or any shared policy database before you configure the primary and standby servers to the shared file system.

IBM PowerHA environment scenario

This scenario is just one example of how you might install and configure a PowerHA environment for standby policy server capability. In this example scenario, similar to other PowerHA environments that provide for standby policy server capability, you must configure the PowerHA environment for IP address takeover of the primary system's service IP address and for shared access to an external file system.

For complete details about how to configure and set up these environments, see the PowerHA documents included when you purchased your PowerHA product. If you have any service problems that involve PowerHA, contact IBM Support for these products.

This scenario provides instructions for setting up a policy server on each of two AIX systems. The host systems that are used throughout this scenario are as follows:

- `tucana` has a service IP address of `192.168.2.13`, a boot IP address of `192.168.2.79`, and a standby IP address, which must be on a different subnet from the service and boot IP addresses of `192.168.3.2`. These IP addresses require that two network adapters, such as Ethernet adapters, be available on `tucana`. Only two network adapters are needed because in a PowerHA environment the service IP address is activated and the boot IP address is deactivated *after* the PowerHA cluster is started on a PowerHA node.
- `perseus` has a service IP address of `192.168.2.14`, a boot IP address of `192.168.2.80`, and a standby IP address, which must be on a different subnet from the service and boot IP addresses of `192.168.3.3`. These IP addresses require that two network adapters, such as Ethernet adapters, be available on `perseus`.

Note: The service and boot IP addresses on *each* AIX system will use the *same* network adapter. The standby IP address on each AIX system will use the second network adapter.

The primary policy server will be installed and configured on the primary AIX system. The primary host system in this scenario is `tucana`.

The standby policy server will be installed and configured on the other remaining AIX system. The other host system is `perseus` in this scenario.

Install and Configure IBM PowerHA for AIX

Use the following scenario to set up a basic IBM PowerHA environment on IBM AIX.

Procedure

1. Install the AIX operating system by using the AIX installation CDs, including all `rsct` packages and the appropriate service pack.
2. Install the PowerHA software and the AIX operating system prerequisites that are needed. Use the instructions that came with the software.
3. Configure the PowerHA cluster.

What to do next

After the PowerHA cluster is set up, continue with "Creating a standby policy server environment."

Creating a standby policy server environment

You can create a standby policy server environment for use in the event of a failover in the primary policy server.

Procedure

1. On *both* the primary policy server and the standby policy server systems, create an **ivmgr** user ID, an **ivmgr** group ID, a **tivoli** user ID, and a **tivoli** group ID. Before you create these IDs, ensure that the `/etc/security/limits` file on each system has the same default settings (where the creation of user and group IDs are concerned). These settings ensure that the user and group IDs are created with the same characteristics on both systems.
   To create these IDs, complete one of the following actions:
   - Use the Smitty utility to ensure that *both* AIX systems use the same number for each ID. For example, both systems must have the same ID number for the **ivmgr** user ID. In addition, the ID numbers must be different for each of the four IDs.
   - Create a script similar to the sample shown in "Script: Setting UIDs for both the primary and standby systems" on page 363. Run this script to set UIDs for **ivmgr** > **tivoli** users and groups. For example, if this script was named **`setivug`**, the following command would create an **ivmgr** group with an ID of `250`, an **ivmgr** user with an ID of `251`, a **tivoli** group with an ID of `260`, and a **tivoli** user with an ID of `261`:

     ```
     ./setivug 250 251 260 261
     ```

     Note: Ensure that the four UID values are not in use on either system *before* you attempt to create them.
2. After you configure and start the PowerHA cluster on your two systems, create a directory, such as `/share`, in the shared file system, which is mountable on these systems. For example, create a `/share` directory on the shared external SSA-based storage tower. To do so, follow these steps:
   a. On the system with the primary policy server, create a `/share` directory in the shared file system. This shared directory, in the external SSA-based storage tower, will contain critical information that must be shared between the primary and standby policy servers.
   b. Create a `/share` subdirectory named `/PolicyDirector` (`/share/PolicyDirector`). Ensure that **ivmgr** is the owner and **ivmgr** is the group that is associated with *both* directories.
   c. Use Smitty HACMP menus to simulate an IP takeover scenario. To do so, stop cluster services on the primary policy server machine by using the **Stop Cluster Services** option. When the cluster shutdown completes on the primary policy server, the standby policy server takes over the service IP address of the primary policy server and is able to access the `/share` and `/share/PolicyDirector` directories within the shared file system.
   d. From the standby policy server system, issue the **`ls –l`** command to validate that both of these directories are associated with the **ivmgr** user and the **ivmgr** group.

e. Restart the cluster on the primary policy server. After the restart completes, the service IP address is restored to the primary policy server system and the shared file system is mounted on the primary policy server system.

3. ***On the primary policy server***, do the following steps:

a. Install and configure required Security Access Manager components. For instructions, see Chapter 6, "Setting up a policy server," on page 103. Figure 1 illustrates the location of key files after the primary policy server is installed and configured.

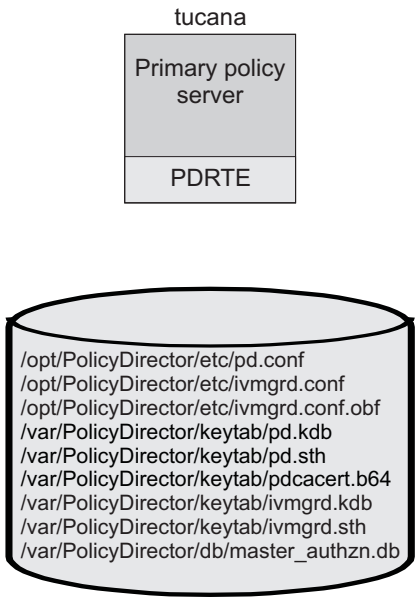

Figure 1. Primary policy server after initial configuration

b. Stop the primary policy server.

c. Edit the `/opt/PolicyDirector/etc/ivmgrd.conf` file and do the following steps:

1) Within the `[ssl]` stanza, change the value of the `ssl-io-inactivity-timeout` entry to `300`.

2) Within the `[configuration-database]` stanza, update the `file=` entry to indicate the fully qualified location of the `ivmgrd.conf.obf` file within the SHARED external file system. For example: `file=/share/PolicyDirector/etc/ivmgrd.conf.obf`

d. Edit the `/opt/PolicyDirector/pd.conf` file and change the host name of the primary policy server to match the host name of the service IP interface, which is configured in your PowerHA configuration for this system. In the example that is depicted in "Install and Configure IBM PowerHA for AIX" on page 358, this host name value was `tucana`.

e. After changes are saved to the configuration files, create a script similar to the sample shown in "Script: Linking files and directories on the primary system" on page 365. Run this script on the primary policy server to link required files and directories to the shared file system (`/share`).
Figure 2 on page 361 illustrates the location of key files after they are moved to the shared file system. Note that the standby policy server is not configured yet.

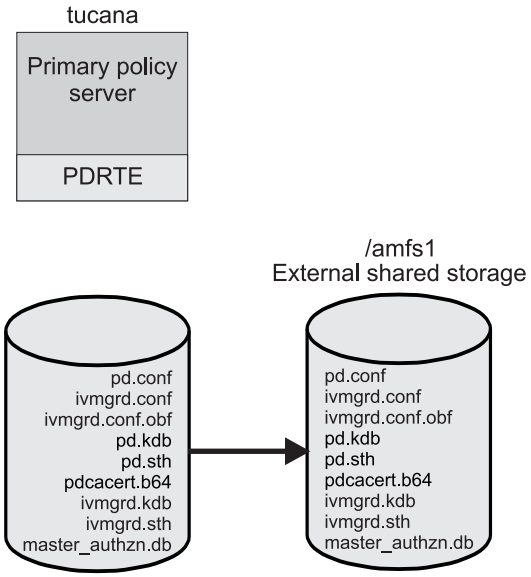

Figure 2. Primary policy server after you incorporate use of the shared file system

f. Restart the primary policy server.

g. Verify the directory structure, file location, soft links, and file permissions as shown on page "Example: Verifying the primary server directories, soft links, and permissions" on page 366.

4. ***On the standby policy server***, do the following steps:

   a. Install (*do not configure*) required Security Access Manager components by using a native installation utility, such as **`installp`**. For instructions, see "AIX: Installing the policy server" on page 107.

   b. Ensure that the PowerHA cluster is running on this system and validate that the shared external file system (`/share/PolicyDirector`) is accessible.

      This step is necessary so that the configuration process can access `.conf` files that are stored in the file system.

      For the standby policy server to access this shared external file system, the primary policy server must be shut down. To do so, use the Smitty HACMP menus to stop cluster services by selecting the **Stop Cluster Services** option on the primary policy server system.

      After the cluster is stopped on this system and after the PowerHA failover operation is completed (which should take no more than a minute), verify that the standby policy server system took over the service IP address of the primary policy server and that the shared file system is mounted on the standby policy server system.

   c. Configure the standby policy server, including the runtime, by using the **`pdconfig`** utility. For instructions, see "AIX: Installing the policy server" on page 107 and "AIX: Installing Security Access Manager Runtime" on page 170.

      Note: The primary policy server does not need to run to configure a standby policy server. However, the registry server that is used by the primary policy server must be available and running on a different system than the primary policy server system.
      During configuration, the **`pdconfig`** utility detects that a policy server configuration already exists. Respond `y` (Yes) to the following prompts: `A policy server is already configured to this LDAP server. A second`

policy server may be configured for migration or standby purposes ONLY! Would you like to configure a second policy server to this LDAP server (y/n) [No]? y Use this policy server for standby (y/n) [No]:y When prompted, type the "fully qualified" location of the ivmgrd.conf file (the existing policy server configuration file). For example, if the shared directory is /share, type the following :/share/PolicyDirector/ivmgrd.conf The **pdconfig** utility places a link to this file in the /opt/PolicyDirector/etc directory and modifies the ivmgrd.conf file to enable standby operation. **Note:** After successful configuration of the standby policy server, the standby policy server is *not* started. It will automatically start *only* after a failover condition is detected by the PowerHA software that is running on the standby policy server. Otherwise, serious errors and conflicts can occur if *both* the primary and the standby policy servers attempt to run in a concurrent manner.

d. Create a script similar to the sample shown in "Script: Linking from the AIX system files to the shared directory on the standby system" on page 367. Run this script to link from the AIX system files to the shared directory.

e. Verify the directory structure, file location, soft links, and file permissions as shown on page "Example: Verifying standby server directories, soft links and permissions" on page 369.

   Note: Because both systems share the directory, the contents of /share/PolicyDirector on the standby server must be identical to the contents shown for the primary server.

Results

Configuration of the primary and standby policy servers is now complete. Now, the PowerHA cluster is down on the primary policy server system and up on the standby policy server system.

Before you test the policy server failover capabilities, verify that the policy server executable is specified in the PowerHA configuration as an application server. To verify by using the SMITTY utility, select **Show Cluster Resources** from the PowerHA Cluster Resources panel to display the cluster resources.

To define an application server, select the **Add an Application Server** option from the PowerHA Define Application Servers panel. After this panel is selected, the start script (/usr/bin/pd_start start) and the stop script (/usr/bin/pd_start stop) for the policy server executable are specified.

Figure 3 on page 363 illustrates the location of key files after you use a native installation method to configure the standby policy server. Appropriate links to these key files within the shared system are also created.

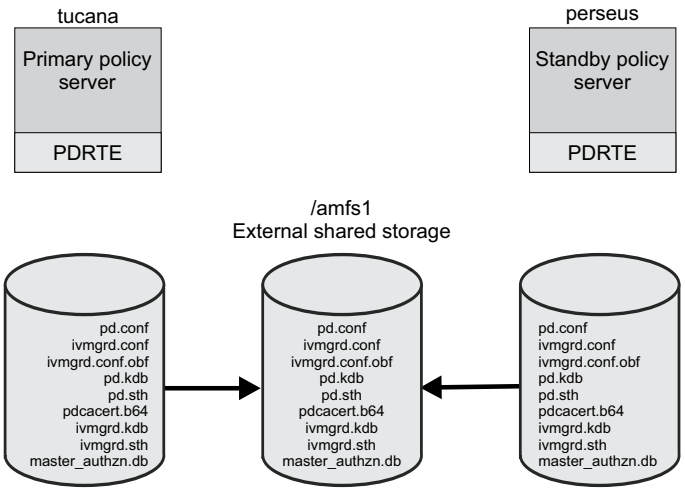

Figure 3. Completed primary/standby policy server environment

After the application server configuration is verified, it is now possible to fully activate the PowerHA primary or standby policy server configuration. To activate this configuration, the PowerHA cluster on the primary policy server system must be restarted. This action starts the primary policy server and put the standby policy server in standby mode.

Script: Setting UIDs for both the primary and standby systems

Use a script to set UIDs for **ivmgr** and **tivoli** users and groups on both the primary and standby policy server systems.

Use the following script as a guide.

```
#!/bin/ksh
#
# This script sets the uid values for the ivmgr user and the ivmgr group
# to values that are specified on the command line when this script is
# executed. In addition, this script defines the tivoli group uid and the
# tivoli user uid.
#
# The first parameter ($1) is the uid for the ivmgr group. The second parameter
# ($2) is the uid for the ivmgr user. The third parameter ($3) is the uid
# for the tivoli group. The fourth parameter ($4) is for the tivoli user uid.
# Before executing this script, insure that the four uid values ARE NOT already
# being used on either system.
#
# Due to the importance of these values, it is ABSOLUTELY necessary on the
# system which will run as the Standby Policy Server to set the ivmgr group
# uid and the ivmgr user uid to MATCH the corresponding settings for these
# entities on the system which is serving as the Primary Policy Server. Also,
# since the definition of the ivmgr user has membership in the tivoli group,
# then it is also necessary to create the tivoli group as well. Finally, since
# the tivoli group contains the tivoli user, then then tivoli user, with the
# appropriate uid, must be defined as well. These user/group settings insure
# consistency across the two policy servers allowing for each system to take
# over the role of the Primary Policy Server when it is appropriate.
# Otherwise, the Standby Policy Server will not run or will not even configure
# correctly if these values are not the same on BOTH systems.
#
# Note that this script, setivug, MUST be run BEFORE the Standby Policy Server
# is installed. As a matter of fact, it is recommended that this script be run
# BEFORE any Security Access Manager software is installed on either the Primary OR the
# Standby Policy server. In this way, all four of these ID's will be consistent
# across BOTH systems.
#
set -e
set -x
#
# Create the ivmgr and tivoli groups with the appropriate uids
#
mkgroup -'A' id="$1" ivmgr
mkgroup -'A' id="$3" tivoli
x() {
LIST=
SET_A=
for i in "$@"
do
if [ "$i" = "admin=true" ]
then
SET_A="-a"
continue
fi
LIST="$LIST \"$i\""
done
eval mkuser $SET_A $LIST
}
#
# Now define the ivmgr user uid to be a part of the staff, tivoli, and ivmgr groups.
# (Enter the following command on one continuous line.)
#
x id="$2" pgrp='staff' groups='staff,tivoli,ivmgr' home='/opt/PolicyDirector'
shell='/usr/bin/ksh' gecos='Policy Director Manager' ivmgr
#
# Now define the tivoli user uid to be a part of the staff and tivoli groups.
# (Enter the following command on one continuous line.)
#
x id="$4" pgrp='staff' groups='staff,tivoli' home='/home/tivoli' shell='/usr/bin/ksh'
gecos='Owner of Tivoli Common Files' tivoli
#
```

Script: Linking files and directories on the primary system

Use a script to link required files and directories on the primary policy server system.

Use the following script as a guide.

```
#!/bin/ksh
#

# Save a copy of the 3 files below under the .bkp extension
cp -p /opt/PolicyDirector/etc/pd.conf /opt/PolicyDirector/etc/pd.conf.bkp
cp -p /opt/PolicyDirector/etc/ivmgrd.conf /opt/PolicyDirector/etc/ivmgrd.conf.bkp
cp -p /opt/PolicyDirector/etc/ivmgrd.conf.obf /opt/PolicyDirector/etc/ivmgrd.conf.obf.bkp

# Move configuration files to shared directory on the external file system
mv /opt/PolicyDirector/etc/pd.conf /share/PolicyDirector
mv /opt/PolicyDirector/etc/ivmgrd.conf /share/PolicyDirector/ivmgrd.conf
mv /opt/PolicyDirector/etc/ivmgrd.conf.obf /share/PolicyDirector/ivmgrd.conf.obf

# Link the configuration files back to the original installation directory
# and change the ownership and group of these links to ivmgr.
ln -s /share/PolicyDirector/pd.conf /opt/PolicyDirector/etc
ln -s /share/PolicyDirector/ivmgrd.conf /opt/PolicyDirector/etc
ln -s /share/PolicyDirector/ivmgrd.conf.obf /opt/PolicyDirector/etc
chown -h ivmgr /share/PolicyDirector/files/ivmgrd.conf
chown -h ivmgr /share/PolicyDirector/files/ivmgrd.conf.obf
chown -h ivmgr /share/PolicyDirector/files/pd.conf
chgrp -h ivmgr /share/PolicyDirector/files/ivmgrd.conf
chgrp -h ivmgr /share/PolicyDirector/files/ivmgrd.conf.obf
chgrp -h ivmgr /share/PolicyDirector/files/pd.conf

# For the keytab, db and lock subdirectories, create a backup of these directories,
# move their contents to the shared external file system, and link the files in
# these directories back to the original installation directory.

cp -R -p /var/PolicyDirector/keytab /var/PolicyDirector/keytab_bkp
mv /var/PolicyDirector/keytab /share/PolicyDirector
ln -s /share/PolicyDirector/keytab /var/PolicyDirector

cp -R -p /var/PolicyDirector/db /var/PolicyDirector/db_bkp
mv /var/PolicyDirector/db /share/PolicyDirector
ln -s /share/PolicyDirector/db /var/PolicyDirector

cp -R -p /var/PolicyDirector/lock /var/PolicyDirector/lock_bkp
mv /var/PolicyDirector/lock /share/PolicyDirector
ln -s /share/PolicyDirector/lock /var/PolicyDirector

# Change the ownership and group of these links to ivmgr.
chown -h ivmgr /share/PolicyDirector/files/db
chown -h ivmgr /share/PolicyDirector/files/keytab
chown -h ivmgr /share/PolicyDirector/files/lock
chgrp -h ivmgr /share/PolicyDirector/files/db
chgrp -h ivmgr /share/PolicyDirector/files/keytab
chgrp -h ivmgr /share/PolicyDirector/files/lock
```

Example: Verifying the primary server directories, soft links, and permissions

Use the following example to verify the directories, links, and permissions.

In the /opt/PolicyDirector/etc **directory:**

```
==> ls -l
total 3714
-rw-r-----1 ivmgrivmgr1682440 Oct 10 11:48 AccessManagerBaseAutoTraceDatabaseFile.obfuscated
-rw-r--r--1 ivmgrivmgr2703 Oct 14 13:16 activedir_ldap.conf
-rw-r-----1 ivmgrivmgr2703 Jul 14 14:21 activedir_ldap.conf.template
-rw-r-----1 ivmgrivmgr18195 Jul7 10:46 additional_licenses.txt
drw-rw----2 ivmgrivmgr512 Dec 31 1969blades
-rw-r-----1 ivmgrivmgr5890 Jan 24 2003config
-rw-r-----1 ivmgrivmgr114 Oct 10 11:48 ffdc
lrwxrwxrwx1 ivmgrivmgr36 Oct 15 13:45 ivmgrd.conf -> /amfs1/PolicyDirector/ivmgrd.conf
-rw-r-----1 ivmgrivmgr16949 Oct 14 13:19 ivmgrd.conf.bkp
lrwxrwxrwx1 ivmgrivmgr40 Oct 15 13:45 ivmgrd.conf.obf -> /amfs1/PolicyDirector/ivmgrd.conf.obf
-rw-r-----1 ivmgrivmgr64 Oct 14 13:19 ivmgrd.conf.obf.bkp
-rw-r-----1 ivmgrivmgr16731 Oct 10 11:29 ivmgrd.conf.template
-rw-r--r--1 ivmgrivmgr2319 Oct 14 13:18 ldap.conf
-rw-r-----1 ivmgrivmgr2187 Oct 10 11:21 ldap.conf.template
-rw-r--r--1 ivmgrivmgr36544 Sep 29 12:45 novschema.def
-rw-r--r--1 ivmgrivmgr26260 Sep 29 12:45 nsschema.def
lrwxrwxrwx1 ivmgrivmgr32 Oct 15 13:45 pd.conf -> /amfs1/PolicyDirector/pd.conf
-rw-r--r--1 ivmgrivmgr3736 Oct 14 13:20 pd.conf.bkp
-rw-r-----1 ivmgrivmgr3645 Oct 10 11:29 pd.conf.template
-rw-r-----1 ivmgrivmgr5576 Oct 10 10:05 pdbackup.lst
-rw-r-----1 ivmgrivmgr7448 Oct 10 10:05 pdinfo.lst
-rw-r--r--1 ivmgrivmgr5354 Oct 14 13:19 pdmgrd_routing
-rw-r--r--1 ivmgrivmgr5255 Oct 10 11:36 pdmgrd_routing.template
-rw-r--r--1 ivmgrivmgr1492 Oct 14 12:49 pdversion.dat
-rw-r--r--1 ivmgrivmgr1492 Aug 18 11:37 pdversion.dat.template
-rw-r-----1 ivmgrivmgr1466 Jan 24 2003product
-rw-r--r--1 ivmgrivmgr5827 Oct 14 13:16 routing
-rw-r--r--1 ivmgrivmgr5674 Oct 10 11:36 routing.template
-rw-r--r--1 ivmgrivmgr14035 Sep 29 12:45 secschema.def
-rw-r--r--1 ivmgrivmgr11236 Jan 24 2003secschema390.def
-rw-r--r--1 ivmgrivmgr1 Oct 14 12:49 startup
-rw-r--r--1 ivmgrivmgr1 Jun 24 10:48 startup.template
-rw-r--r--1 ivmgrivmgr1233 Jan 24 2003upgrade3.7_ibm_schema.def
-rw-r--r--1 ivmgrivmgr1938 Jan 24 2003upgrade3.7_ibm_schema390.def
-rw-r--r--1 ivmgrivmgr1744 Jan 24 2003upgrade3.7_netscape_schema.def
```

In the /var/PolicyDirector **directory:**

```
==> ls -Rl
total 7
drwxrwxr-x2 ivmgrivmgr512 Dec 31 1969audit
lrwxrwxrwx1 ivmgrivmgr27 Oct 15 13:45 db -> /amfs1/PolicyDirector/db
drwxrwxr-x2 ivmgrivmgr512 Oct 14 13:19 db_bkp
lrwxrwxrwx1 ivmgrivmgr31 Oct 16 15:48 keytab -> /amfs1/PolicyDirector/keytab
drwxr-xr-x2 ivmgrivmgr512 Oct 16 15:42 keytab_bkp
lrwxrwxrwx1 ivmgrivmgr29 Oct 15 13:45 lock -> /amfs1/PolicyDirector/lock
drwxr-x---2 ivmgrivmgr512 Dec 31 1969lock_bkp
drwxrwxrwx3 ivmgrivmgr512 Oct 16 13:40 log
drwxrwxr-x2 ivmgrivmgr512 Dec 31 1969pdbackup
drwxr-x---2 ivmgrivmgr512 Oct 14 12:49 pdmgrd
./audit:
total 0

./db_bkp:
total 1056
-rw-------1 ivmgrivmgr540672 Oct 15 13:45 master_authzn.db

./keytab_bkp:
total 35
-rw-------1 ivmgrivmgr10080 Oct 14 13:19 ivmgrd.kdb
-rw-------1 ivmgrivmgr129 Oct 14 13:18 ivmgrd.sth
-rw-rw-rw-1 rootsystem5080 Oct 14 13:19 pd.kdb
-rw-rw-rw-1 rootsystem129 Oct 14 13:19 pd.sth
-rw-------1 rootsystem1070 Oct 14 13:18 pdcacert.b64

./lock_bkp:
total 0
```

In the SHARED directory, /share/PolicyDirector**, on the external file system:**

```
==> ls -Rl
total 80
drwxrwxr-x2 ivmgrivmgr512 Oct 14 13:19 db
-rw-r-----1 ivmgrivmgr16950 Oct 16 13:32 ivmgrd.conf
-rw-r-----1 ivmgrivmgr64 Oct 16 13:32 ivmgrd.conf.obf
drwxr-xr-x2 ivmgrivmgr512 Oct 16 15:42 keytab
drwxr-x---2 ivmgrivmgr512 Dec 31 1969lock
-rw-r--r--1 ivmgrivmgr3736 Oct 14 13:20 pd.conf

./db:
total 1056
-rw-------1 ivmgrivmgr540672 Oct 16 16:18 master_authzn.db

./keytab:
total 64
-rw-------1 ivmgrivmgr10080 Oct 14 13:19 ivmgrd.kdb
-rw-------1 ivmgrivmgr129 Oct 14 13:18 ivmgrd.sth
-rw-rw-rw-1 rootsystem5080 Oct 14 13:19 pd.kdb
-rw-rw-rw-1 rootsystem129 Oct 14 13:19 pd.sth
-rw-------1 rootsystem1070 Oct 14 13:18 pdcacert.b64

./lock:
total 0
```

Script: Linking from the AIX system files to the shared directory on the standby system

Use a script to link from the AIX system files to the shared directory on the standby policy server system.

Use the following script example as a guide.

```
#!/bin/ksh
#

# The Standby Policy Server must use the same configuration files as the
# Primary Policy Server. For this reason, the following links must be created
# in order for the Standby Policy Server to function correctly.
#
# Note the Security Access Manager configuration software will automatically create
# a link to the ivmgrd.conf file that is stored in the shared external file system.

# Backup pd.conf to pd.bkp and link to pd.conf in the shared external file system
mv /opt/PolicyDirector/etc/pd.conf /opt/PolicyDirector/etc/pd.conf.bkp
ln -s /share/PolicyDirector/pd.conf /opt/PolicyDirector/etc

# Backup keytab, db and lock directories and link the keytab, db, and lock
# directories to their corresponding files in the shared external file system.

mv /var/PolicyDirector/keytab /var/PolicyDirector/keytab_bkp
ln -s /share/PolicyDirector/keytab /var/PolicyDirector

mv /var/PolicyDirector/db /var/PolicyDirector/db_bkp
ln -s /share/PolicyDirector/db /var/PolicyDirector

mv /var/PolicyDirector/lock /var/PolicyDirector/lock_bkp
ln -s /share/PolicyDirector/lock /var/PolicyDirector

# Change the group and ownership of the five links above to ivmgr.
chown -h ivmgr /share/PolicyDirector/files/etc/pd.conf
chown -h ivmgr /share/PolicyDirector/files/db
chown -h ivmgr /share/PolicyDirector/files/keytab
chown -h ivmgr /share/PolicyDirector/files/lock
chgrp -h ivmgr /share/PolicyDirector/files/pd.conf
chgrp -h ivmgr /share/PolicyDirector/files/db
chgrp -h ivmgr /share/PolicyDirector/files/keytab
chgrp -h ivmgr /share/PolicyDirector/files/lock
```

Example: Verifying standby server directories, soft links and permissions

Use the following example to verify the directories, links, and permissions.

In the /opt/PolicyDirector/etc **directory:**

```
==> ls -l
total 3668
-rw-r----- 1 ivmgr ivmgr 1682440 Oct 10 11:48 AccessManagerBaseAutoTraceDatabaseFile.obfuscated
-rw-r--r-- 1 ivmgr ivmgr2703 Oct 16 13:26 activedir_ldap.conf
-rw-r----- 1 ivmgr ivmgr2703 Jul 14 14:21 activedir_ldap.conf.template
-rw-r----- 1 ivmgr ivmgr18195 Jul 07 10:46 additional_licenses.txt
drw-rw---- 2 ivmgr ivmgr512 Dec 31 1969blades
-rw-r----- 1 ivmgr ivmgr5890 Jan 24 2003config
-rw-r----- 1 ivmgr ivmgr114 Oct 10 11:48 ffdc
lrwxrwxrwx 1 rootsystem36 Oct 16 13:32 ivmgrd.conf -> /amfs1/PolicyDirector/ivmgrd.conf
lrwxrwxrwx 1 rootsystem40 Oct 16 13:32 ivmgrd.conf.obf -> /amfs1/PolicyDirector/ivmgrd.conf.obf
-rw-r----- 1 ivmgr ivmgr16731 Oct 10 11:29 ivmgrd.conf.template
-rw-r--r-- 1 ivmgr ivmgr2319 Oct 16 13:31 ldap.conf
-rw-r----- 1 ivmgr ivmgr2187 Oct 10 11:21 ldap.conf.template
-rw-r--r-- 1 ivmgr ivmgr36544 Sep 29 12:45 novschema.def
-rw-r--r-- 1 ivmgr ivmgr26260 Sep 29 12:45 nsschema.def
lrwxrwxrwx 1 ivmgr ivmgr32 Oct 16 13:36 pd.conf -> /amfs1/PolicyDirector/pd.conf
-rw-r--r-- 1 ivmgr ivmgr3741 Oct 16 13:32 pd.conf.bkp
-rw-r----- 1 ivmgr ivmgr3645 Oct 10 11:29 pd.conf.template
-rw-r----- 1 ivmgr ivmgr5576 Oct 10 10:05 pdbackup.lst
-rw-r----- 1 ivmgr ivmgr7448 Oct 10 10:05 pdinfo.lst
-rw-r--r-- 1 ivmgr ivmgr5255 Oct 10 11:36 pdmgrd_routing.template
-rw-r--r-- 1 ivmgr ivmgr1492 Oct 16 13:27 pdversion.dat
-rw-r--r-- 1 ivmgr ivmgr1492 Aug 18 11:37 pdversion.dat.template
-rw-r----- 1 ivmgr ivmgr1466 Jan 24 2003product
-rw-r--r-- 1 ivmgr ivmgr5810 Oct 16 13:27 routing
-rw-r--r-- 1 ivmgr ivmgr5674 Oct 10 11:36 routing.template
-rw-r--r-- 1 ivmgr ivmgr14035 Sep 29 12:45 secschema.def
-rw-r--r-- 1 ivmgr ivmgr11236 Jan 24 2003secschema390.def
-rw-r--r-- 1 ivmgr ivmgr1 Oct 16 13:27 startup
-rw-r--r-- 1 ivmgr ivmgr1 Jun 24 10:48 startup.template
-rw-r--r-- 1 ivmgr ivmgr1233 Jan 24 2003upgrade3.7_ibm_schema.def
-rw-r--r-- 1 ivmgr ivmgr1938 Jan 24 2003upgrade3.7_ibm_schema390.def
-rw-r--r-- 1 ivmgr ivmgr1744 Jan 24 2003upgrade3.7_netscape_schema.def
```

In the /var/PolicyDirector **directory:**

```
==> ls -Rl
total 7
drwxrwxr-x2 ivmgrivmgr512 Dec 31 1969audit
lrwxrwxrwx1 ivmgrivmgr27 Oct 16 13:36 db -> /amfs1/PolicyDirector/db
drwxrwxr-x2 ivmgrivmgr512 Dec 31 1969db_bkp
lrwxrwxrwx1 ivmgrivmgr31 Oct 16 13:36 keytab -> /amfs1/PolicyDirector/keytab
drwxrwxrwx2 ivmgrivmgr512 Dec 31 1969keytab_bkp
lrwxrwxrwx1 ivmgrivmgr29 Oct 16 13:36 lock -> /amfs1/PolicyDirector/lock
drwxr-x---2 ivmgrivmgr512 Dec 31 1969lock_bkp
drwxrwxrwx2 ivmgrivmgr512 Dec 31 1969log
drwxrwxr-x2 ivmgrivmgr512 Dec 31 1969pdbackup
drwxr-x---2 ivmgrivmgr512 Oct 16 13:24 pdmgrd
./audit:
total 0

./db_bkp:
total 0

./keytab_bkp:
total 0

./lock_bkp:
total 0
```

High availability management

The following tasks ensure that you correctly followed the initial Security Access Manager configuration procedures for setting up HACMP Security Access Manager primary and standby servers.

Verify the policy server setup for high availability

To verify that the installation and configuration procedures were correctly followed, ensure that the following primary tasks are completed:

- Make sure that you set up the required soft links from the active primary server to the standby server.
- Make sure that you modified the appropriate configuration options in the `ivmgrd.conf` and `pd.conf` configuration files on both the primary and standby policy servers. These configuration files must have the same default settings for the following required user and group IDs:
  - The **ivmgr** user ID
  - The **tivoli** user ID
  - The **ivmgr** group ID
  - The **tivoli** group ID
- Ensure that you copy files from the local AIX file system for the primary server and the standby server to the shared file system. Ensure that the shared file system is on a common directory and that each user and group has the necessary access permissions.

If any of these items are incorrectly set, return to the procedure for setting up a standby policy server. See Appendix G, “Standby policy server (AIX) setup,” on page 357.

Review log files

You can monitor the transition process of the primary policy to the standby server by examining the `hacmp.log` file to verify that all HACMP and PowerHA failover operations occurred.

The procedure for reviewing HACMP and PowerHA logs can be found in the HACMP and PowerHA documentation. The `hacmp.log` log file is found in the `/tmp` directory.

If a read or write operation error occurred during the policy server failover, you can review the primary policy server log files. The location of the Security Access Manager log files depends on whether Tivoli Common Directory is used. See the *IBM Security Access Manager for Web Troubleshooting Guide* for information about these log files and the XML log file viewer.

Appendix H. Setup for a standby policy server with IBM Tivoli System Automation for Multiplatforms

You can configure a standby server to take over policy server functions during a system failure or unplanned outage.

When the policy server goes down, the standby policy server acts as the primary policy server until the primary policy server assumes its original role. In turn, the standby policy server reverts to a standby role. At any time, there is only one active policy server and only one shared copy of the policy databases.

Security Access Manager supports one standby policy server on supported AIX, Linux, or Windows platforms. In addition, deploying a standby policy server requires a network load balancer and IBM Tivoli System Automation for Multiplatforms.

This scenario is provided as a general guide. It describes how to install and configure a Tivoli System Automation for Multiplatforms environment for standby policy server capability.

Note: If you configure a standby policy server on AIX, you might want to use the scenario in Appendix G, “Standby policy server (AIX) setup,” on page 357.

Scenario components

This standby policy scenario uses a runtime server, an LDAP server and a load balancer, a primary server, and a standby server. IBM Tivoli System Automation for Multiplatforms is used on both the primary server and the standby server. It provides high availability and policy-based automation functionality for the environment.

The following graphic depicts the arrangement of these components:

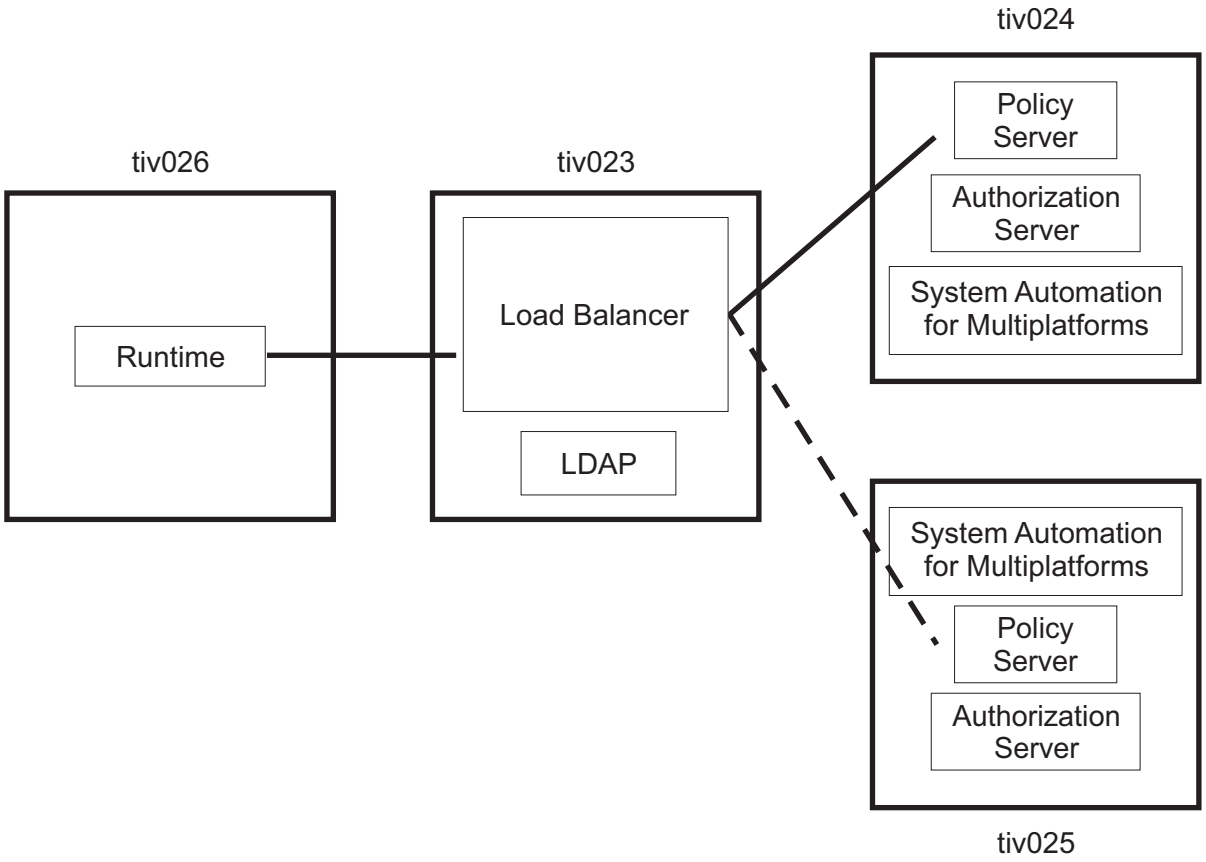

Table 35. Scenario components that use IBM Tivoli System Automation for Multiplatforms

Name	Use
tiv023	LDAP and Load Balancer for fail-over
tiv024	Primary policy server, with IBM Tivoli System Automation Application Manager
tiv025	Standby policy server, with IBM Tivoli System Automation Application Manager
tiv026	Runtime and LDAP client server **Note:** The runtime component in this scenario can be any Security Access Manager component that requires access to the policy server. For example, you can replace the runtime server that is shown in the scenario with a WebSEAL server.

The solid line is the normal path to the primary Security Access Manager system. The broken line is the failover path to the backup system.

Preinstallation requirements

This high availability environment has specific software requirements.

Ensure that the following software is available for your installation:

- A supported LDAP server, such as IBM Tivoli Directory Server
- IBM Security Access Manager
- Load Balancer for fail-over
- IBM Tivoli System Automation for Multiplatforms

Complete the preinstallation setup for each server. See Chapter 4, “Prerequisite installation and configuration roadmap,” on page 27.

LDAP and Load Balancer requirements

This scenario requires the installation of LDAP and load balancer (for fail-over) software. In these instructions, the LDAP server is installed on the same server where the runtime server is installed. However, you can install them on separate servers.

For information about the prerequisites for the user registry, see Chapter 5, “User registry server installation and configuration,” on page 51.

Primary server requirements

The primary server requires a Security Access Manager policy server and authorization server and IBM Tivoli System Automation for Multiplatforms.

Policy server and authorization server

For prerequisite information, see “Security Access Manager base systems” on page 12.

Tivoli System Automation for Multiplatforms

For prerequisite information, see http://www.ibm.com/software/tivoli/products/sys-auto-linux/platforms.html

Standby server requirements

The standby server requires a Security Access Manager policy server and authorization server and IBM Tivoli System Automation for Multiplatforms.

Policy server and authorization server

For prerequisite information, see “Security Access Manager base systems” on page 12.

Tivoli System Automation for Multiplatforms

For prerequisite information, see http://www.ibm.com/software/tivoli/products/sys-auto-linux/platforms.html

Runtime server requirements

The runtime server requires the Security Access Manager runtime component. The runtime component in this scenario can be any Security Access Manager component that requires access to the policy server. For example, you can replace the runtime server that is shown in the scenario with a WebSEAL server.

Runtime

For prerequisite information, see “Security Access Manager base systems” on page 12.

LDAP client

For prerequisite information, see Chapter 5, “User registry server installation and configuration,” on page 51.

Installing the LDAP and the load balancer

To begin your deployment, install LDAP and the load balancer software on the server to provide failover between primary and secondary Policy servers.

Before you begin

Make sure that your environment meets the requirements that are described in “LDAP and Load Balancer requirements” on page 375.

Procedure

1. Install LDAP. Use the instructions in Chapter 5, “User registry server installation and configuration,” on page 51. During the installation, ensure that you keep the default values in the following fields:
   - **Encryption seed**
   - **Non-SSL port**
   - **SSL port**
   - **SSL key file with full path**
   - **Certificate label**
2. Install the load balancer software. For instructions on installing the load balancer, use the documentation that came with the product.

What to do next

Continue with “Installing the primary server.”

Installing the primary server

The initial setup of the primary server includes installing Security Access Manager policy server and authorization server. In a subsequent task, you install IBM Tivoli System Automation for Multiplatforms on this server.

Before you begin

Make sure that your environment meets the requirements that are described in “Primary server requirements” on page 375.

Procedure

1. Install the LDAP client. See “IBM Tivoli Directory Server client installation” on page 42.
2. Install the Global Security Kit. See “IBM Global Security Kit (GSKit) installation” on page 34.
3. Install the IBM Security Access Manager License, if not already installed. For instructions, see “IBM Security Access Manager License installation” on page 37.
4. Install the IBM Security Utilities. See “IBM Security Utilities installation” on page 39.

5. Install the runtime component. See Chapter 11, “Setting up a runtime system,” on page 169
6. Install the policy server. See Chapter 6, “Setting up a policy server,” on page 103
7. Install the authorization server. See Chapter 7, “Authorization server setup,” on page 121
8. Configure only the runtime and policy servers to use the LDAP you previously installed. See Chapter 11, “Setting up a runtime system,” on page 169 and Chapter 6, “Setting up a policy server,” on page 103.
9. Create any Security Access Manager domains that are required in addition to the Security Manager default management domain. Use the **pdadmin domain create** command. See the *IBM Security Access Manager for Web Command Reference*.
10. Clone the primary policy server by creating a backup. Use the **pdbackup** command. See the *IBM Security Access Manager for Web Command Reference*. A `.tar` file is created for AIX and Linux systems. For example, `pdbackup.tiv024.tar`. A `.dar` file is created for Windows systems.
11. Configure an authorization server for the Security Access Manager management domain. See Chapter 7, “Authorization server setup,” on page 121.
12. If you create additional Security Access Manager domains, configure additional authorization server instances, one for each domain. Consider using instance names for these domains that are easily recognizable. For example, consider using the domain name that the instance is being configured for.

What to do next

Continue with “Installing the standby server.”

Installing the standby server

Setting up the standby server includes several tasks. You must install Security Access Manager on the server, clone the primary server, restore the clone onto the standby server, and configure a unique authorization server on the standby server. In a subsequent task, you also install IBM Tivoli System Automation for Multiplatforms on this server.

Before you begin

Complete the requirements that are described in “Primary server requirements” on page 375.

Procedure

1. Install the LDAP client. See “IBM Tivoli Directory Server client installation” on page 42.
2. Install the Global Security Kit. See “IBM Global Security Kit (GSKit) installation” on page 34.
3. Install the IBM Security Access Manager License, if not already installed. For instructions, see “IBM Security Access Manager License installation” on page 37.
4. Install the IBM Security Utilities. See “IBM Security Utilities installation” on page 39.

5. Install the runtime component. See Chapter 11, “Setting up a runtime system,” on page 169.
6. Install the policy server. See Chapter 6, “Setting up a policy server,” on page 103.
7. Install the authorization server. See Chapter 7, “Authorization server setup,” on page 121
8. Configure *only* the runtime (pdrte) on the standby server. See Chapter 6, “Setting up a policy server,” on page 103
9. Copy the backup of the primary server to the standby server.
   a. Copy the `.tar` file from the primary server onto the standby server in a temporary directory.
   b. Restore the backup onto the standby server by using the `restore` action with the **pdbackup** command. For example, on AIX or Linux type:

      ```
      pdbackup -action restore -file /tmp/pdbackup.tiv024.tar
      ```

      For example, on Windows type:

      ```
      pdbackup -action restore -file %TEMP%pdbackup.tiv024.dar
      ```
10. Display the policy server files. For example, on AIX and Linux from the `/var/PolicyDirector/db` directory, type:

    ```
    ls -l
    ```

    You can expect results similar to this example:

    ```
    -rw------- 1 ivmgr ivmgr 540672 Oct 19 10:38 master_authzn.db
    ```

    If you created additional domains, you can also expect results similar to the following example:

    ```
    -rw------- 1 ivmgr ivmgr 540672 Oct 19 10:38 domain2.db
    -rw------- 1 ivmgr ivmgr 540672 Oct 19 10:38 domain3.db
    ```
11. Check the configuration status of the servers on the standby server. For example, on AIX or Linux directory, type:

    ```
    pdconfig
    ```

    When prompted, select **3. Display Configuration Status**. You can expect results similar to this example:

    ```
    Security Access Manager Runtime Yes
    Security Access Manager Policy Server Yes
    Security Access Manager Authorization Server No
    ```
12. Configure unique authorization servers on the standby server.
    a. Configure an authorization server for the Security Access Manager management domain.
    b. If you created additional Security Access Manager domains, configure additional authorization server instances, one for each domain. Consider using instance names for these domains that are easily recognizable. For example, consider using the domain name that the instance is being configured for.
13. Verify that the configuration was successful by running the **server list** command. See the *IBM Security Access Manager for Web Command Reference* for details. Both the primary server and standby server are in the list that is displayed by the command. Only one policy server is listed.

What to do next

Continue with "Verifying Security Access Manager servers."

Verifying Security Access Manager servers

Before you continue with the remaining setup tasks, ensure that the installation and configuration of the Security Access Manager servers are correct. Then, update some of the replicated settings so that they point to the appropriate servers.

About this task

The policy and authorization servers on both the primary and standby servers are using the same policy database. Therefore, updates from either server are replicated across the policy databases and must be accessible from both the servers. This task verifies that accessibility.

Note: On Microsoft Windows systems, use the Services window from the Control Panel to start and stop the server processes manually. From the Services window, change the Startup type from Automatic to Manual for the Security Access Manager Auto-Start Service.

The files that you work with in this task are in the following locations by default.

AIX, Linux, and Solaris:

```
/opt/PolicyDirector/etc/pd.conf
/opt/PolicyDirector/etc/ivmgrd.conf
```

Windows:

```
C:\Program Files\Tivoli\Policy Director\etc\pd.conf
C:\Program Files\Tivoli\Policy Director\etc\imgmrd.conf
```

Replace the path information in the examples of this task with the appropriate path for your environment.

Procedure

1. Create an ACL on the primary server:
   a. Make sure that the policy server and authorization server on the primary server are started. For example, on AIX or Linux, type:

      ```
      pd_start start
      ```

      To ensure that they are started, type `pd_start status`.
   b. Create an ACL by using the **`pdadmin acl create`** command. For example, on AIX or Linux, type:

      ```
      pdadmin -a sec_master -p passw0rd
      pdadmin sec_master> acl create testacl
      pdadmin sec_master> acl show testacl
      ```

      The result is similar to the following example:

      ```
      ACL Name: testacl
      Description:
      Entries:
      User sec_master TcmdbsvaBRl
      ```
   c. Stop the policy server and the authorization server. For example, on AIX or Linux, type:

      ```
      pd_start stop
      ```

2. Check the replication on the standby server:
   a. Stop the authorization server on the standby server. For example, type:

      ```
      pd_start stop
      ```

   b. Change the master-host in the `pd.conf` file to comment out the entries for the policy server and add an entry for the standby server. Edit the `pd.conf` file to read as follows, where tiv024 is the primary server and tiv025 is the standby server:

      ```
      # Hostname of the server.
      # This parameter is set by the bassslcfg utility.
      #master-host = <Server host name>
      #master-host = tiv024
      master-host = tiv025
      ```

   c. In the same file, stop the authorization server from starting. Change the following setting:

      ```
      [pdrte]
      boot-start-ivacld=no
      ```

      If you configured additional authorization servers, stop them also:

      ```
      [pdrte]
      boot-start-domain2-ivacld=no
      boot-start-domain3-ivacld=no
      ```

   d. Change the database-path in the `ivmgrd.conf` file. Edit the `ivmgrd.conf` as follows.

      Note: On Windows, replace `/var/PolicyDirector/db/` with the appropriate directory.

      ```
      # Database file
      #database-path=/var/PolicyDirector/db/master_authzn.db
      database-path=/var/PolicyDirector/db/ivacld.db
      ```

      If you created additional domains, update their database-path entries to the corresponding authorization server database files:

      ```
      [domain=domain2]
      #database-path=/var/PolicyDirector/db/domain2.db
      database-path=/var/PolicyDirector/db/domain2-ivacld.db
      [domain=domain3]
      #database-path=/var/PolicyDirector/db/domain3.db
      database-path=/var/PolicyDirector/db/domain3-ivacld.db
      ```

   e. Start the policy server but *do not* start the authorization servers. For example, on AIX or Linux, type:

      ```
      pd_start start
      ```

      Note: The **pd_start start** command can be used here because in an earlier step, the command was prevented from starting the authorization servers.

   f. On the standby server (tiv025 in this example), log in to **pdadmin** and check for the ACL that was created on the primary server. For example, on AIX or Linux, type:

      ```
      pdadmin -a sec_master -p passw0rd
      pdadmin sec_master> acl list
      ```

      Locate the name of the ACL that you added on the primary server, such as `testacl`.
3. On the standby server, update the ACL.

a. On the primary server, change the master-host in the `pd.conf` file. Open the `pd.conf` file in an editor. Then, edit the file to read as follows, where tiv024 is the primary server and tiv025 is the standby server:

```
# Hostname of the server.
# This parameter is set by the bassslcfg utility.
#master-host = <Server host name>
#master-host = tiv024
master-host = tiv025
```

b. In the same file, stop the policy server from starting. Change the following setting:

```
[pdrte]
boot-start-ivmgrd=no
```

c. Change the master-host in the `ivacld.conf` file. Edit the `ivacld.conf` as follows, where tiv024 is the primary server and tiv025 is the standby server:

```
# Hostname of the server.
# This parameter is set by the svrsslcfg utility.
#master-host = <Server host name>
#master-host = tiv024
master-host = tiv025
```

d. Start the authorization servers but *do not* start the policy server. For example, on AIX or Linux, type:

```
pd_start start
```

Note: The **pd_start start** command can be used here because in the previous step, the command was prevented from starting the policy server. To ensure that it is started, type `pd_start status`.

4. On the standby server, add a user to the ACL.

a. Show the ACL that you previously created. For example, type:

```
pdadmin -a sec_master -p passw0rd
pdadmin sec_master> acl show testacl
```

b. Create a user by using the **pdadmin user create** command and add the user to the previously created ACL. For example, type:

```
pdadmin sec_master> user create bobsm cn=bobsm,o=ibm,c=us
    Bob Smith passw0rd
pdadmin sec_master> user modify bobsm account-valid yes
pdadmin sec_master> acl modify testacl set user bobsm Tr
pdadmin sec_master> acl show testacl
```

The result is something similar to the following example:

```
ACL Name: testacl
Description:
Entries:
User sec_master TcmdbsvaBRl
User bobsm Tr
```

5. On the standby server, stop the policy server.

```
pd_start stop
```

6. On the primary server, stop the authorization server.

```
pd_start stop
```

7. On the primary server, change the policy server settings so that it points to the authorization server on the primary server.

a. Change the master-host in the `pd.conf` file to comment out the entries for the policy server and add an entry for the standby server. Edit the `pd.conf` as follows, where tiv024 is the primary server and tiv025 is the standby server:

```
# Hostname of the server.
# This parameter is set by the bassslcfg utility.
#master-host = <Server host name>
master-host = tiv024
```

b. In the same file, enable the policy server to start and stop the authorization server from starting. Change the following setting:

```
[pdrte]
boot-start-ivmgrd=yes
boot-start-ivacld=no
```

If you configured additional authorization servers, stop them also:

```
[pdrte]
boot-start-domain2-ivacld=no
boot-start-domain3-ivacld=no
```

c. Change the database-path in the `ivmgrd.conf` file. Edit the `ivmgrd.conf` file to read as follows.

Note: On Windows, replace `/var/PolicyDirector/db/` with the appropriate directory.

```
# Database file
#database-path=/var/PolicyDirector/db/master_authzn.db
database-path=/var/PolicyDirector/db/ivacld.db
```

If you created additional domains, update their database-path entries to the corresponding authorization server database files:

```
[domain=domain2]
#database-path=/var/PolicyDirector/db/domain2.db
database-path=/var/PolicyDirector/db/domain2-ivacld.db
[domain=domain3]
#database-path=/var/PolicyDirector/db/domain3.db
database-path=/var/PolicyDirector/db/domain3-ivacld.db
```

8. On the primary server, start the policy server.

```
pd_start start
```

9. On the primary server, log in to **pdadmin** and check for the ACL that was modified on the standby server. For example, type:

```
pdadmin -a sec_master -p passw0rd
pdadmin sec_master> acl show testacl
```

The result is something similar to the following example:

```
ACL Name: testacl
Description:
Entries:
User sec_master TcmdbsvaBRl
User bobsm Tr
```

The modification that is done to the ACL on the standby server is visible on the primary server.

10. Restore the initial configuration on the standby server.

a. Change the master-host in the `pd.conf` file to comment out the entries for the policy server and add an entry for the standby server. Edit the `pd.conf` file to read as follows, where tiv024 is the primary server and tiv025 is the standby server:

```
# Hostname of the server.
# This parameter is set by the bassslcfg utility.
#master-host = <Server host name>
master-host = tiv024
```

b. In the same file, stop the policy server from starting and enable the authorization server to start. Change the following setting:

```
[pdrte]
boot-start-ivmgrd=no
boot-start-ivacld=yes
```

If you configured additional authorization servers, enable them also:

```
[pdrte]
boot-start-domain2-ivacld=yes
boot-start-domain3-ivacld=yes
```

c. Start the authorization server, but *do not* start the policy server. For example, on AIX or Linux, type:

```
pd_start start
```

d. To ensure that it is started, type `pd_start status`.

e. Use **pdadmin** commands to ensure that the servers are working properly. For example, type:

```
pdadmin -a sec_master -p passw0rd
pdadmin sec_master> server list
```

Configuring the Load Balancer

The load balancer software must be configured to provide fail-over from the primary Policy server to the standby server when it detects the primary Policy server is not responding. The load balancer must not attempt to send requests to both policy servers simultaneously, but instead it should provide only fail-over support because only one Policy server is active at a time.

Installing and configuring the runtime server

The setup of the runtime server includes installing the LDAP client and the Security Access Manager runtime server.

About this task

Complete the requirements that are described in "Runtime server requirements" on page 375.

The file for this task in the following default location:

AIX, Linux, and Solaris:

```
/opt/PolicyDirector/etc/pd.conf
```

Windows:

```
C:\Program Files\Tivoli\Policy Director\etc\pd.conf
```

Replace the path information in the examples of this task with the appropriate path for your environment.

Procedure

1. Install the LDAP client. See "IBM Tivoli Directory Server client installation" on page 42.
2. Install the Global Security Kit. See "IBM Global Security Kit (GSKit) installation" on page 34.
3. Install the IBM Security Access Manager License, if not already installed. For instructions, see "IBM Security Access Manager License installation" on page 37.

4. Install the IBM Security Utilities. See "IBM Security Utilities installation" on page 39.
5. Install the runtime component. See Chapter 11, "Setting up a runtime system," on page 169.
6. Configure the runtime server to use the LDAP that you previously installed.
7. Verify request forwarding by the load balancer.
   a. Log in to **pdadmin** and verify that the primary and standby servers are listed. For example, type:

      ```
      pdadmin -a sec_master -p passw0rd
      pdadmin sec_master> server list
      ```

   b. On the runtime server, modify master-host in the `pd.conf` file to point to the cluster IP address. Edit the `pd.conf` file to read as follows, where tiv024 is the primary server and tiv026 is the runtime server.

      ```
      # Hostname of the server.
      # This parameter is set by the bassslcfg utility.
      #master-host = <Server host name>
      #master-host = <tiv024_ip_address>
      master-host = <ip_address_of_Edge_server_cluster>
      ```

   c. Log in to **pdadmin** and verify the change in the server list, ACL list, and ACL. For example, type:

      ```
      pdadmin -a sec_master -p passw0rd
      pdadmin sec_master> server list
      ```

   d. Verify that the primary and standby servers are listed. Then, type:

      ```
      pdadmin sec_master> acl list
      ```

   e. Verify that all ACLs (including the ACL that was created, called `testacl` in this example) are listed. Then, type:

      ```
      pdadmin sec_master> acl show testacl
      ```

   f. Verify that all users that are part of that ACL are listed.

What to do next

Continue with "Installing and configuring Tivoli System Automation for Multiplatforms."

Installing and configuring Tivoli System Automation for Multiplatforms

Install and configure IBM Tivoli System Automation for Multiplatforms on both the primary server and the standby server. IBM Tivoli System Automation for Multiplatforms provide high availability and policy-based automation functionality for the environment.

About this task

For details about installing and configuring Tivoli System Automation for Multiplatforms, use the installation instructions at http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.samp.doc_3.2.2/HALICG23.pdf.

The command examples use the following variables. Replace these variables with the names that are appropriate to your installation:

tiv024 The name of the primary server.

tiv025 The name of the standby server.

tiv023 The name of the LDAP and load balancer server.

mynetwork
A name that is used to represent your network.

Procedure

1. On both the primary server and the standby server, install Tivoli System Automation for Multiplatforms. Use the instructions in the Tivoli System Automation for Multiplatforms Information Center: http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.samp.doc_3.2.2/HALICG23.pdf
2. After the installation of the product, use the instructions to complete the configuration.
3. On the primary server, create a two-node cluster.

   Note: On Windows, run all commands from the IBM Tivoli System Automation Shell. To start the Shell, click **Start** > **All programs** > **SA for Multiplatforms** > **IBM Tivoli System Automation - Shell**.

   a. Run **preprpnode** with the names of both the primary and standby nodes. For example, type:

      ```
      preprpnode tiv024 tiv025
      ```

   b. Create a cluster and specify both the primary and standby nodes. Use a name that you choose. SA_DOMAIN is the name that is used in the example. For example, type:

      ```
      mkrpdomain SA_DOMAIN tiv024 tiv025
      ```

   c. Check to see whether the cluster is offline. Display the cluster information. For example, type:

      ```
      lsrpdomain SA_DOMAIN
      ```

   d. Bring the cluster online. For example, type:

      ```
      startrpdomain SA_DOMAIN
      ```

      Wait a few minutes for the cluster to come online. Run the **lsrpdomain SA_DOMAIN** command again until it is listed as Online.
4. Check the status of the cluster on the standby server. For example, on the standby server, type:

   ```
   lsrpdomain SA_DOMAIN
   ```

5. Set up the network tiebreaker on the primary server.

   a. List the available tiebreaker types. For example, type:

      ```
      lsrsrc -c IBM.TieBreaker AvailableTypes
      ```

   b. Create a tiebreaker. For example, type:

      ```
      mkrsrc IBM.TieBreaker Type="EXEC" Name="mynetwork"
      DeviceInfo='PATHNAME=/usr/sbin/rsct/bin/samtb_net Address=tiv023_ip_address
      Log=1' PostReserveWaitTime=30;
      ```

   c. Activate the tiebreaker. For example, type:

      ```
      chrsrc -c IBM.PeerNode OpQuorumTieBreaker="mynetwork"
      ```

   d. On the standby server, display the tiebreaker information. For example, on the standby server, type:

      ```
      lsrsrc IBM.TieBreaker
      ```

What to do next

Continue with “Enabling failover automation” on page 386.

Enabling failover automation

IBM Tivoli System Automation for Multiplatforms uses *application resources* to enable the automation of failover functions. An application resource is any piece of hardware or software you can be define to System Automation for Multiplatforms.

About this task

This deployment uses an application resource that you must create on the primary server. In addition, you must create scripts to start, stop, and monitor both the primary server and the standby server.

On Windows, run all commands in this task from the IBM Tivoli System Automation Shell. To start the Shell, click **Start** > **All programs** > **SA for Multiplatforms** > **IBM Tivoli System Automation - Shell**.

Procedure

1. Use the sample scripts in the following locations to create the necessary scripts for both the primary server and the standby server:
   - **For AIX, Linux, and Solaris:**
     - Primary: `/opt/PolicyDirector/example/primaryscripts`
     - Standby: `/opt/PolicyDirector/example/standbyscripts`
   - **For Windows:**
     - Primary: `C:\Program Files\Tivoli\Policy Director\example\primaryscripts`

       Standby: `C:\Program Files\Tivoli\Policy Director\example\standbyscripts`

   Create each of the following scripts on both the primary server and the standby server:

   polup The start script for bringing the resource online. Use the sample script in the following topics to create your own:
   - "Polup script for the primary server" on page 388
   - "Polup script for the standby server" on page 389

   poldown
   The stop script for taking the resource offline. Use the sample script in the following topics to create your own:
   - "Poldown script for the primary server" on page 391
   - "Poldown script for the standby server" on page 392

   polmon
   The script for monitoring the resource. Use the sample script in the following topics to create your own:
   - "Polmon script for the primary server" on page 394
   - "Polmon script for the standby server" on page 395
2. Place the scripts in the `/opt/PolicyDirector/etc` directory or `C:\Program Files\Tivoli\Policy Director/etc` on Windows.
3. Create a floating application resource on the primary server. A *floating resource* is a resource that can run on several nodes in the cluster but only on one node at a time.
   a. Create a text file called `pdmgrd-rs.def` in the `/opt/PolicyDirector/etc` directory or `C:\Program Files\Tivoli\Policy Director/etc` on Windows.

b. Include the following content and definitions in the file.

On AIX or Linux:

```
PersistentResourceAttributes:
Name="pdmgrd-rs"
StartCommand="/opt/PolicyDirector/etc/polup"
StopCommand="/opt/PolicyDirector/etc/poldown"
MonitorCommand="/opt/PolicyDirector/etc/polmon"
MonitorCommandPeriod=5
MonitorCommandTimeout=30
NodeNameList={'tiv024','tiv025'}
StartCommandTimeout=30
StopCommandTimeout=30
UserName="root"
ResourceType=1
```

On Windows:

```
PersistentResourceAttributes::
Name="pdmgrd-rs"
StartCommand="/dev/fs/C/Progra~1/Tivoli/Policy~1/etc/polup"
StopCommand="/dev/fs/C/Progra~1/Tivoli/Policy~1/etc/poldown"
MonitorCommand="/dev/fs/C/Progra~1/Tivoli/Policy~1/etc/polmon"
MonitorCommandPeriod=5
MonitorCommandTimeout=30
NodeNameList={'tiv024','tiv025'}
StartCommandTimeout=30
StopCommandTimeout=30
UserName="Administrator"
ResourceType=1
```

Note: ResourceType=1 specifies a floating resource; the resource can run on any node, but only one resource is up at a time.

c. Save the file.

d. Run the following command:

```
mkrsrc -f pdmgrd-rs.def IBM.Application
```

4. Create a resource group. For example, on AIX or Linux, type:

```
mkrg pdmgrd-rg
```

5. Add the application resource to the resource group. For example, on AIX or Linux, type:

```
addrgmgr -g pdmgrd-rg IBM.Application:pdmgrd-rs
```

6. Bring the resource online. For example, on AIX or Linux, type:

```
chrg -o online pdmgrd-rg
```

7. Test the failover automation:

a. Stop the primary server. The pdmgrd on the standby server starts automatically.

b. Use the **lssam** command on the standby server. If the failover is working, the primary server (pdmgrd) is listed as offline and the standby server (pdmgrd) is online.

c. Try a **pdadmin** command on the runtime server to ensure that the pdadmin function is working.

d. Next, stop the standby server. The pdmgrd on the primary server starts automatically.

e. Try a **pdadmin** command on the runtime server again to ensure that the pdadmin function is working.

f. If these tests complete successfully, automation is working. If these tests do not complete successfully, review the previous steps and your configuration until you determine the error.

Polup script for the primary server

Use this sample script to create a script that starts the primary server.

AIX or Linux script

```
#!/bin/sh

#
# Set the hostname or IP address for the standby policy server
#
STANDBY_SERVER=<standby_policy_server>

#
# Add Security Access Manager CLI to PATH
#
PATH=$PATH:/opt/PolicyDirector/bin
PATH=$PATH:/opt/PolicyDirector/sbin
export PATH

#
# Stop authorization server
#
pd_start stop >/dev/null 2>&1
logger -i -t "POLUP" "Authorization server stopped"

#
# Change pd.conf
#
cd /opt/PolicyDirector/etc

pdconf -f pd.conf setentry manager master-host $STANDBY_SERVER
pdconf -f pd.conf setentry pdrte boot-start-ivmgrd yes
pdconf -f pd.conf setentry pdrte boot-start-ivacld no

#
# Add lines for additional authorization servers used for additional domains
#
#pdconf -f pd.conf setentry pdrte boot-start-domain2-ivacld no
#pdconf -f pd.conf setentry pdrte boot-start-domain3-ivacld no

logger -i -t "POLUP" "pd.conf modified: master-host set to $STANDBY_SERVER"

#
# Alias the loopback interface for the cluster IP address
#
ifconfig lo:1 <cluster_ip_address> netmask 255.255.255.255 up
logger -i -t "POLUP" "lo:1 interface UP"

#
# Start policy server
#
pd_start start >/dev/null 2>&1
logger -i -t "POLUP" "Policy server started"

exit 0
```

Windows script

```
#!/bin/sh

#
# Set the hostname for the primary policy server
#
PRIMARY_SERVER=tiv024

#
# Add Security Access Manager dll location to PATH
```

```
#
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/Policy~1/bin
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/Policy~1/sbin
export PATH

#
# Add IBM Security Utilities dll location to PATH
#
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/TivSecUtl/bin
export PATH

#
# Stop authorization server
#
net stop IVAcld >/dev/null 2>&1
logger -i -t "POLUP" "Authorization server stopped"

#
# Change pd.conf
#
cd /dev/fs/C/Progra~1/Tivoli/Policy~1/etc

pdconf.exe -f pd.conf setentry manager master-host $PRIMARY_SERVER
pdconf.exe -f pd.conf setentry pdrte boot-start-ivmgrd yes
pdconf.exe -f pd.conf setentry pdrte boot-start-ivacld no

#
# Add lines for additional authorization servers used for additional domains
#
#pdconf.exe -f pd.conf setentry pdrte boot-start-domain2-ivacld no
#pdconf.exe -f pd.conf setentry pdrte boot-start-domain3-ivacld no

logger -i -t "POLUP" "pd.conf modified: master-host set to $PRIMARY_SERVER"

#
# Start policy server
#
net start IVMgr >/dev/null 2>&1
logger -i -t "POLUP" "Policy server started"

exit 0
```

Polup script for the standby server

Use this sample script to create a script that starts the standby server.

AIX or Linux script

```
#!/bin/sh

#
# Set the hostname or IP address for the standby policy server
#
STANDBY_SERVER=<standby_policy_server>

#
# Add Security Access Manager CLI to PATH
#
PATH=$PATH:/opt/PolicyDirector/bin
PATH=$PATH:/opt/PolicyDirector/sbin
export PATH

#
# Stop authorization server
#
pd_start stop >/dev/null 2>&1
logger -i -t "POLUP" "Authorization server stopped"
```

```
#
# Change pd.conf
#
cd /opt/PolicyDirector/etc

pdconf -f pd.conf setentry manager master-host $STANDBY_SERVER
pdconf -f pd.conf setentry pdrte boot-start-ivmgrd yes
pdconf -f pd.conf setentry pdrte boot-start-ivacld no

#
# Add lines for additional authorization servers used for additional domains
#
#pdconf -f pd.conf setentry pdrte boot-start-domain2-ivacld no
#pdconf -f pd.conf setentry pdrte boot-start-domain3-ivacld no

logger -i -t "POLUP" "pd.conf modified: master-host set to $STANDBY_SERVER"

#
# Alias the loopback interface for the cluster IP address
#
ifconfig lo:1 <cluster_ip_address> netmask 255.255.255.255 up
logger -i -t "POLUP" "lo:1 interface UP"

#
# Start policy server
#
pd_start start >/dev/null 2>&1
logger -i -t "POLUP" "Policy server started"

exit 0
```

Windows script

```
#!/bin/sh

#
# Set the hostname for the standby policy server
#
STANDBY_SERVER=tiv025

#
# Add Security Access Manager dll location to PATH
#
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/Policy~1/bin
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/Policy~1/sbin
export PATH

#
# Add IBM Security Utilities dll location to PATH
#
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/TivSecUtl/bin
export PATH

#
# Stop authorization server
#
net stop IVAcld >/dev/null 2>&1
logger -i -t "POLUP" "Authorization server stopped"

#
# Change pd.conf
#
cd /dev/fs/C/Progra~1/Tivoli/Policy~1/etc

pdconf.exe -f pd.conf setentry manager master-host $STANDBY_SERVER
pdconf.exe -f pd.conf setentry pdrte boot-start-ivmgrd yes
```

```
pdconf.exe -f pd.conf setentry pdrte boot-start-ivacld no

#
# Add lines for additional authorization servers used for additional domains
#
#pdconf.exe -f pd.conf setentry pdrte boot-start-domain2-ivacld no
#pdconf.exe -f pd.conf setentry pdrte boot-start-domain3-ivacld no

logger -i -t "POLUP" "pd.conf modified: master-host set to $STANDBY_SERVER"

#
# Start policy server
#
net start IVMgr >/dev/null 2>&1
logger -i -t "POLUP" "Policy server started"

exit 0
```

Poldown script for the primary server

Use this sample script to create a script that stops the primary server.

AIX or Linux script

```
#!/bin/sh

#
# Set the hostname or IP address for the primary policy server
#
PRIMARY_SERVER=<primary_policy_server>

#
# Add Security Access Manager CLI to PATH
#
PATH=$PATH:/opt/PolicyDirector/bin
PATH=$PATH:/opt/PolicyDirector/sbin
export PATH

#
# Stop policy server
#
pd_start stop >/dev/null 2>&1
logger -i -t "POLDOWN" "Policy server stopped"

#
# Change pd.conf
#
cd /opt/PolicyDirector/etc

pdconf -f pd.conf setentry manager master-host $PRIMARY_SERVER
pdconf -f pd.conf setentry pdrte boot-start-ivmgrd no
pdconf -f pd.conf setentry pdrte boot-start-ivacld yes

#
# Add lines for additional authorization servers used for additional domains
#
#pdconf -f pd.conf setentry pdrte boot-start-domain2-ivacld yes
#pdconf -f pd.conf setentry pdrte boot-start-domain3-ivacld yes

logger -i -t "POLDOWN" "pd.conf modified: master-host set to $PRIMARY_SERVER"

#
# Unalias the loopback interface
#
ifconfig lo:1 down
logger -i -t "POLDOWN" "lo:1 interface DOWN"
```

```
#
# Start authorization server
#
pd_start start >/dev/null 2>&1
logger -i -t "POLDOWN" "Authorization server started"

exit 0
```

Windows script

```
#!/bin/sh

#
# Set the hostname for the standby policy server
#
STANDBY_SERVER=tiv025

#
# Add Security Access Manager dll location to PATH
#
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/Policy~1/bin
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/Policy~1/sbin
export PATH

#
# Add IBM Security Utilities dll location to PATH
#
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/TivSecUtl/bin
export PATH

#
# Stop policy server
#
net stop IVMgr >/dev/null 2>&1
logger -i -t "POLDOWN" "Policy server stopped"

#
# Change pd.conf
#
cd /dev/fs/C/Progra~1/Tivoli/Policy~1/etc

pdconf.exe -f pd.conf setentry manager master-host $STANDBY_SERVER
pdconf.exe -f pd.conf setentry pdrte boot-start-ivmgrd no
pdconf.exe -f pd.conf setentry pdrte boot-start-ivacld yes

#
# Add lines for additional authorization servers used for additional domains
#
#pdconf.exe -f pd.conf setentry pdrte boot-start-domain2-ivacld yes
#pdconf.exe -f pd.conf setentry pdrte boot-start-domain3-ivacld yes

logger -i -t "POLDOWN" "pd.conf modified: master-host set to $STANDBY_SERVER"

#
# Start authorization server
#
net start IVAcld >/dev/null 2>&1
logger -i -t "POLDOWN" "Authorization server started"

exit 0
```

Poldown script for the standby server

Use this sample script to create a script that stops the standby server.

AIX or Linux script

```
#!/bin/sh

#
# Set the hostname or IP address for the primary policy server
#
PRIMARY_SERVER=<primary_policy_server>

#
# Add Security Access Manager CLI to PATH
#
PATH=$PATH:/opt/PolicyDirector/bin
PATH=$PATH:/opt/PolicyDirector/sbin
export PATH

#
# Stop policy server
#
pd_start stop >/dev/null 2>&1
logger -i -t "POLDOWN" "Policy server stopped"

#
# Change pd.conf
#
cd /opt/PolicyDirector/etc

pdconf -f pd.conf setentry manager master-host $PRIMARY_SERVER
pdconf -f pd.conf setentry pdrte boot-start-ivmgrd no
pdconf -f pd.conf setentry pdrte boot-start-ivacld yes

#
# Add lines for additional authorization servers used for additional domains
#
#pdconf -f pd.conf setentry pdrte boot-start-domain2-ivacld yes
#pdconf -f pd.conf setentry pdrte boot-start-domain3-ivacld yes

logger -i -t "POLDOWN" "pd.conf modified: master-host set to $PRIMARY_SERVER"

#
# Unalias the loopback interface
#
ifconfig lo:1 down
logger -i -t "POLDOWN" "lo:1 interface DOWN"

#
# Start authorization server
#
pd_start start >/dev/null 2>&1
logger -i -t "POLDOWN" "Authorization server started"

exit 0
```

Windows script

```
#!/bin/sh

#
# Set the hostname for the primary policy server
#
PRIMARY_SERVER=tiv024

#
# Add Security Access Manager dll location to PATH
#
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/Policy~1/bin
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/Policy~1/sbin
export PATH
```

```
#
# Add IBM Security Utilities dll location to PATH
#
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/TivSecUtl/bin
export PATH

#
# Stop policy server
#
net stop IVMgr >/dev/null 2>&1
logger -i -t "POLDOWN" "Policy server stopped"

#
# Change pd.conf
#
cd /dev/fs/C/Progra~1/Tivoli/Policy~1/etc

pdconf.exe -f pd.conf setentry manager master-host $PRIMARY_SERVER
pdconf.exe -f pd.conf setentry pdrte boot-start-ivmgrd no
pdconf.exe -f pd.conf setentry pdrte boot-start-ivacld yes

#
# Add lines for additional authorization servers used for additional domains
#
#pdconf.exe -f pd.conf setentry pdrte boot-start-domain2-ivacld yes
#pdconf.exe -f pd.conf setentry pdrte boot-start-domain3-ivacld yes

logger -i -t "POLDOWN" "pd.conf modified: master-host set to $PRIMARY_SERVER"

#
# Start authorization server
#
net start IVAcld >/dev/null 2>&1
logger -i -t "POLDOWN" "Authorization server started"

exit 0
```

Polmon script for the primary server

Use this sample script to create a script that monitors the primary server.

AIX or Linux script

```
#!/bin/sh

OPSTATE_ONLINE=1
OPSTATE_OFFLINE=2

ps -ef | grep -v "grep" | grep "pdmgrd" >/dev/null
if [ $? == 0 ]
then
    RC=${OPSTATE_ONLINE}
else
    RC=${OPSTATE_OFFLINE}
fi

exit $RC
```

Windows script

```
#!/bin/sh

OPSTATE_ONLINE=1
OPSTATE_OFFLINE=2

ps -e | grep -v "grep" | grep "pdmgrd" >/dev/null
```

```
if [ $? == 0 ]
then
    RC=${OPSTATE_ONLINE}
else
    RC=${OPSTATE_OFFLINE}
fi

exit $RC
```

Polmon script for the standby server

Use this sample script to create a script that monitors the standby server.

AIX or Linux script

```
#!/bin/sh

OPSTATE_ONLINE=1
OPSTATE_OFFLINE=2

ps -ef | grep -v "grep" | grep "pdmgrd" >/dev/null
if [ $? == 0 ]
then
    RC=${OPSTATE_ONLINE}
else
    RC=${OPSTATE_OFFLINE}
fi

exit $RC
```

Windows script

```
#!/bin/sh

OPSTATE_ONLINE=1
OPSTATE_OFFLINE=2

ps -e | grep -v "grep" | grep "pdmgrd" >/dev/null
if [ $? == 0 ]
then
    RC=${OPSTATE_ONLINE}
else
    RC=${OPSTATE_OFFLINE}
fi

exit $RC
```

Appendix I. Tivoli Directory Server proxy environment setup

A Tivoli Directory Server proxy is a special type of IBM Tivoli Directory Server that provides request routing, load balancing, fail over, distributed authentication and support for distributed/membership groups and partitioning of containers.

Attention: IBM Security Access Manager customers who want to use the Tivoli Directory Server proxy server must purchase a separate Tivoli Directory Server entitlement. The version of Tivoli Directory Server that is part of the Security Access Manager package does not allow IBM Security Access Manager customer-use of the Tivoli Directory Server proxy server.

If you have the appropriate entitlement, use the proxy server instructions in the *IBM Tivoli Directory Server Administration Guide* to set up the proxy server: http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/admin_gd.htm.

Then, return to this document for instructions about setting up the proxy server to work with IBM Security Access Manager.

Security Access Manager stores its metadata within a required suffix called `secAuthority=Default`. Metadata includes information that is used to track user and group status information specific to Security Access Manager. When using a proxy, the `secAuthority=Default` object itself cannot be modified by using the proxy because the object at a proxy partition split point cannot be modified through the proxy. Therefore, Security Access Manager cannot be configured directly through the proxy because Security Access Manager must modify the `secAuthority=Default` object during configuration.

In a proxy environment, the administrator should decide on which back-end server the `secAuthority=Default` subtree will be hosted and set up that back-end server and the proxy partition information to reflect that topology. This example configures `Server A` to host the `secAuthority=Default` subtree.

Data under a proxy partition split point (for example, `o=ibm,c=us`) is hashed to determine which back-end server has the subtree. In this example, `Proxy` is configured to hash RDN values immediately after `o=ibm,c=us` among two servers. This also means the RDN values more than 1 away from `o=ibm,c=us` will map to the same server as values immediately after `o=ibm,c=us`. For this reason, it is usually more advantageous to configure the proxy with a single partition for the `secAuthority=Default` suffix.

If you want to distribute the Security Access Manager metadata within the `secAuthority=Default` suffix among multiple back-end servers, it is best to split the partition below the `cn=Users,secAuthority=Default` container. Entries are made on behalf of each user defined, below the `cn=Users,secAuthority=Default` container and therefore splitting this user information can help distribute the data more evenly across the back-end servers. This example will not distribute the data but instead maintain the entire `secAuthority=Default` subtree within `Server A`.

Adding the Security Access Manager suffix to the proxy

For the proxy to work with Security Access Manager, you must configure the `secAuthority=Default` suffix.

Procedure

1. Log in to `Server A` as the local LDAP administrator (for example `cn=root`).
2. Select **Server administration** > → > **Manage server properties**. Select the Suffixes property.
3. In the **Suffix DN** field, type `secAuthority=Default`.
4. Click **Add**.
5. When you are finished, click **Apply** to save your changes without exiting, or click **OK** to apply your changes and exit.
6. The suffix will not be available until the server is restarted. In the navigation pane, select **Server administration** and then select **Start/stop/restart server**.
7. Ensure the **Start/restart in configuration only mode** check box is *not* selected.
8. Click **Restart**.
9. After a message is displayed that the restart request was sent, go to **Server administration** and check the status of the server. Wait until the server restarts successfully and is running before you continue.
10. Log in to `Proxy` as the local LDAP administrator (for example `cn=root`).
11. From the navigation pane, expand **Proxy administration**.
12. On the Proxy administration page, click **Manage proxy properties**.
13. In the **Suffix DN** field, type `secAuthority=Default`.
14. Click **Add**.
15. Click **OK** to save your changes and return to the Introduction window.
16. From the navigation pane, click **Proxy administration** and then click **Manage partition bases**.
17. From the **Manage partition bases** menu, click **Add**.
18. In the **Split Name** field, type: `Split 1`
19. In the **Partition base DN** field, type: `secAuthority=Default`
20. In the **Number of partitions** field, type: `1`
21. In the **Partition bases** table, select the **secAuthority=Default** radio button.
22. Click **View servers** and then verify that `secAuthority=Default` is displayed in the **Partition base DN** field.
23. In the **Back-end directory servers for partition base** table, click **Add**.
24. From the **Add Back-end directory server** menu, click **Back-end directory server** > → > **Server A**.
25. Ensure that `1` is displayed in the **Partition index** field.
26. Click **OK**.
27. When you are finished, click **Close**.
28. Restart `Proxy` for the changes to take effect.

Configuring Security Access Manager to use the proxy

After the Tivoli Directory Server proxy server and back-end servers are configured with the Directory Information Tree (DIT) partitioning setup, you can configureSecurity Access Manager to use the proxy. The proxy server provides a unified view of the directory and shields the LDAP application (Security Access Manager for example) from having to be aware of the DIT partitioning.

When configured to use the Tivoli Directory Server proxy server, Security Access Manager is only aware of the proxy and performs all operations through the proxy, as if it represented the entire DIT namespace.

To provide failover support, multiple Tivoli Directory Server proxy servers can also be configured. See the *IBM Tivoli Directory Server: Administration Guide* for information about configuring multiple Tivoli Directory Server proxy servers to provide failover support. When configuring multiple proxy servers to provide failover support, Security Access Manager should be configured to treat each of the proxy servers as a directory server replica. The example scenario described here, assumes a single proxy.

Because Security Access Manager cannot be configured directly to the Tivoli Directory Server proxy server, Security Access Manager must first be configured to the back-end server that hosts the `secAuthority=Default` subtree. When configuring the Security Access Manager Runtime component for use with this back-end server, select **LDAP** as the registry type. When the **pdconfig** utility requests the **LDAP hostname**, type the host name and **LDAP port number** of `Server A` (the back-end server that hosts the `secAuthority=Default` subtree); do not type the host name of the Tivoli Directory Server proxy server (`Proxy`).

Configure SSL information for setting up an SSL connection with `Server A`, if SSL is to be used. When using SSL, `Proxy` needs to be configured with a server certificate that is generated by the same certificate authority (CA) that was used to create the server certificate for `Server A`. Specify the LDAP DN (for example `cn=root`) and the LDAP administrator password for `Server A`. After the Security Access Manager policy server is configured successfully to the back-end server (`Server A`), you can then retarget the Security Access Manager policy server system to the Tivoli Directory Server proxy server. Exit the **pdconfig** utility.

Redirecting the policy server to the proxy

To retarget the Security Access Manager policy server system to the proxy, stop the policy server by using the **pd_start stop** command on AIX, Linux, or Solaris or by using Windows Services. Edit the policy server `ldap.conf` and `pd.conf` configuration files by using the **pdadmin config** command.

Procedure

1. Start the **pdadmin** utility.
2. Log in to the local system with the **login –l** command.
3. After locally logged in, change the value of the host and port in the configuration files to specify the host name and port of the Tivoli Directory Server proxy server with the following commands:
   For AIX, Linux, or Solaris:

```
config modify keyvalue set /opt/PolicyDirector/etc/ldap.conf ldap host proxy_hostname
config modify keyvalue set /opt/PolicyDirector/etc/ldap.conf ldap port proxy_port
config modify keyvalue set /opt/PolicyDirector/etc/pd.conf pdrte user-reg-server proxy_hostname
config modify keyvalue set /opt/PolicyDirector/etc/pd.conf pdrte user-reg-host proxy_hostname
config modify keyvalue set /opt/PolicyDirector/etc/pd.conf pdrte user-reg-hostport proxy_port
```

For Windows: **Note:** This example assumes that Security Access Manager is installed to the default location. Change the following commands to match the installation location for your system if necessary.

```
config modify keyvalue set "c:\Program Files\Tivoli\Policy Director\etc\ldap.conf"
   ldap host proxy_hostname
config modify keyvalue set "c:\Program Files\Tivoli\Policy Director\etc\ldap.conf"
   ldap port proxy_port
config modify keyvalue set "c:\Program Files\Tivoli\Policy Director\etc\pd.conf"
  pdrte user-reg-server proxy_hostname
config modify keyvalue set "c:\Program Files\Tivoli\Policy Director\etc\pd.conf"
  pdrte user-reg-host proxy_hostname
config modify keyvalue set "c:\Program Files\Tivoli\Policy Director\etc\pd.conf"
  pdrte user-reg-hostport proxy_port
```

where:

proxy_hostname
The host name of the Tivoli Directory Server proxy server.

proxy_port
The port number of the Tivoli Directory Server proxy server.

4. After the configuration files are modified, the policy server can be restarted using the **pd_start start** utility for AIX, Linux, or Solaris or using Windows Services.

Results

For more information about these commands and utilities, see the *IBM Security Access Manager for Web Command Reference*.

Setting access controls for the proxy

As stated earlier, access control lists (ACLs) cannot be managed from the Tivoli Directory Server proxy server. When a proxy server is used, it is the back-end server that enforces access control. The LDAP administrator is responsible to ensure that the proper ACLs are created on each of the back-end servers if the ACLs exist on the top-level object of the partition split point.

About this task

Security Access Manager must have proper access control to allow it to manage users and groups within the suffixes where user and group definitions are maintained. To set the necessary ACLs on the back-end servers to allow Security Access Manager to manage the partition suffixes, use the Security Access Manager **ivrgy_tool** utility with the **add-acls** parameter.

Procedure

1. Run the **ivrgy_tool** utility from any system where the Security Access Manager Runtime component is installed, for example the system where the policy server is installed.
2. To apply the proper ACLs on each of the back-end servers, run the following command:

```
ivrgy_tool -h backend_host -p backend_port -D ldap_admin_DN \
-w ldap_admin_pwd -d [-Z] [-K ssl_keyfile] [-P ssl_keyfile_pwd] \
[-N label] add-acls domain
```

For more information about the **ivrgy_tool** utility, see the *IBM Security Access Manager for Web Command Reference*.

Results

The policy server is the only Security Access Manager component that must be retargeted to the Tivoli Directory Server proxy server as described in "Configuring Security Access Manager to use the proxy" on page 399. Other Security Access Manager components, such as the authorization server or WebSEAL, do not need to be retargeted.

After the policy server has been configured, other Security Access Manager components can be configured normally.

When configuring Security Access Manager Runtime for other components, the Tivoli Directory Server proxy server host name and port should be specified for the LDAP host name. It is not necessary to indicate any of the back-end servers.

Unconfiguring Security Access Manager from the proxy

Before the policy server can be unconfigured, it must be retargeted back to the back-end server that hosts the `secAuthority=Default` subtree. Before you attempt to retarget and unconfigure the policy server, ensure that all other Security Access Manager components are unconfigured and stopped.

About this task

All Security Access Manager components *other than* the policy server can be unconfigured normally when the environment is set up as with the Tivoli Directory Server proxy server (as described in "Configuring Security Access Manager to use the proxy" on page 399).

After all Security Access Manager components are unconfigured, the policy server can be retargeted to the back-end server that is hosting the `secAuthority=Default` subtree.

To retarget the policy server system to the back-end server, stop the policy server using the **pd_start stop** command on AIX, Linux, or Solaris or using Windows Services. Edit the policy server `ldap.conf` and `pd.conf` configuration files using the **pdadmin config** command.

Procedure

1. Start the **pdadmin** command.
2. Log in to the local system with the **login –l** command.
3. Change the value of the host and port in the configuration files to specify the host name and port of the back-end server that hosts the `secAuthority=Default` subtree (`Server A` in this example):

   For AIX, Linux, or Solaris

   ```
   config modify keyvalue set /opt/PolicyDirector/etc/ldap.conf
      \ldap host serverA_hostname
   config modify keyvalue set /opt/PolicyDirector/etc/ldap.conf
     \ldap port serverA_port
   config modify keyvalue set /opt/PolicyDirector/etc/pd.conf
     \pdrte user-reg-server serverA_hostname
   ```

```
config modify keyvalue set /opt/PolicyDirector/etc/pd.conf
  \pdrte user-reg-host serverA_hostname
config modify keyvalue set /opt/PolicyDirector/etc/pd.conf
  \pdrte user-reg-hostport serverA_port
```

For Windows

This example assumes that Security Access Manager is installed to the default location. Change the following commands to match the installation location for your system if necessary:

```
config modify keyvalue set "c:\Program Files\Tivoli\Policy Director\etc\ldap.conf"
  ldap host serverA_hostname
config modify keyvalue set "c:\Program Files\Tivoli\Policy Director\etc\ldap.conf"
  ldap port serverA_port
config modify keyvalue set "c:\Program Files\Tivoli\Policy Director\etc\pd.conf"
  pdrte user-reg-server serverA_hostname
config modify keyvalue set "c:\Program Files\Tivoli\Policy Director\etc\pd.conf"
  pdrte user-reg-host serverA_hostname
config modify keyvalue set "c:\Program Files\Tivoli\Policy Director\etc\pd.conf"
  pdrte user-reg-hostport serverA_port
```

where:

serverA_hostname
: The host name of the back-end server.

serverA_port
: The port number of the back-end server.

4. After the configuration files are modified, the policy server can be restarted using the **pd_start start** utility for AIX, Linux, or Solaris or using Windows Services.
5. After the policy server is successfully restarted, it can be unconfigured normally using the **pdconfig** utility.

Results

For more information about these commands and utilities, see the *IBM Security Access Manager for Web: Command Reference*.

Appendix J. Security Access Manager registry adapter for WebSphere federated repositories

The Security Access Manager registry adapter for WebSphere federated repositories uses the Security Access Manager Registry Direct Java API to perform registry-related operations.

The adapter:

- Is a virtual member manager (VMM) adapter. For detailed information about VMM, see the Virtual member manager documentation in the IBM WebSphere Application Server information center: http://www.ibm.com/software/webservers/appserv/was/library/.
- Supports a single Security Access Manager domain. However, the Security Access Manager supports multiple secure domains support when configured with the LDAP registry.
- Supports the Security Access Manager registries supported by the Registry Direct Java API.

Appendix K. Uninstallation

Uninstalling Security Access Manager is a three-part process.

You must unconfigure components, remove Security Access Manager packages, and then restart the system.

Attention: Do not unconfigure the Security Access Manager Runtime component unless all Security Access Manager applications installed on the system, such as WebSEAL and other Web server plug-ins, already are unconfigured. Otherwise, the Security Access Manager application is left in an unusable state.

Unconfigure and remove the policy server system last.

Unconfiguring Security Access Manager components

Before you remove Security Access Manager packages, you must ensure that the component is unconfigured (if needed).

Procedure

1. On AIX, Linux or Solaris, log on as **root**. On Windows, log on as a user with Windows administrator privileges.
2. To start the configuration utility, enter the following command:

   ```
   pdconfig
   ```

   Note: On Windows system, you also can select **Start → Programs → IBM Security Access Manager → Configuration**.
   The Security Access Manager Setup Menu is displayed.
3. Unconfigure components in the following order:
   a. Security Access Manager Attribute Retrieval Service
   b. Security Access Manager session management command-line interface, or Security Access Manager session management service
   c. Security Access Manager Web Portal Manager, Access Manager WebSEAL, or Security Access Manager Plug-in for Web Servers
   d. Security Access Manager Authorization Server instances
   e. Security Access Manager Policy Proxy Server, standby Security Access Manager Policy Server
   f. Security Access Manager Policy Server
   g. Security Access Manager Runtime and Security Access Manager Runtime for Java

   To unconfigure a component on AIX, Linux, or Solaris, type the number of the menu item for the Security Access Manager component. To unconfigure a component on Windows, select a component and then click **Unconfigure**. Repeat this procedure for each package that you want to unconfigure.

   Note:

   a. If you are using an LDAP user registry and are unconfiguring a policy server or policy proxy server, you are prompted for the distinguished name (**cn=root**) and password of the LDAP Administrator.

b. When you unconfigure the policy server:
   - You are warned that configuration and authorization information for all Security Access Manager servers and applications that are installed in the management domain will be removed. Enter **y** to proceed.
   - You are prompted whether you want to permanently remove domain information from the registry. Enter **y** to remove all domain information, including user and group information. Enter **n** to remove domain information but retain user and group information so that the domain can be re-created later if needed.

c. If you have either the Security Access Manager Runtime for Java or Web Portal Manager installed, but *not* the Security Access Manager Runtime, use the **pdjrtecfg** utility in the/opt/PolicyDirector/sbin/ path to unconfigure Security Access Manager Runtime for Java. Type:

   ```
   /opt/PolicyDirector/sbin/pdjrtecfg -action unconfig -interactive
   ```

   Use the **amwpmcfg** utility in the /opt/PolicyDirector/sbin/ path to unconfigure Security Access Manager Web Portal Manager. Type:

   ```
   /opt/PolicyDirector/sbin/amwpmcfg -action unconfig -interactive
   ```

Unconfiguring IBM Tivoli Directory Server

Unconfiguring IBM Tivoli Directory Server involves unconfiguring the database from the directory server instance and removing the directory server instance.

Back up your directory and any existing schema files before you start this procedure.

Unconfiguring the database

You can unconfigure the database that is associated with a directory server instance by using either the Configuration Tool or the command line.

Using the Configuration Tool

Use the Configuration Tool to unconfigure the database that is associated with a directory server instance.

Procedure

1. On AIX, Linux, or Solaris systems, log on as **root**. On Windows systems, log on with a user ID that is a member of the Administrators group.
2. Start the Configuration Tool by entering the following command:`idsxcfg`
3. Click **Unconfigure Database** in the navigation pane.
4. In the **Unconfigure Database** window, select one of the following options:

   Unconfigure database
   Removes information about the database from the configuration file for the directory server instance. However, the database and its data are left intact. This makes the database inaccessible to the directory server instance but does not destroy any data in the database.

   Unconfigure and destroy database
   Deletes the database and its contents and removes information about the database from the configuration file for the directory server instance.

5. Click **Unconfigure**.
6. Click **Yes** to confirm the operation.

Using the command line

Use the **idsucfgdb** command to unconfigure a database for a directory server instance.

By default, **idsucfgdb** unconfigures the database from the `ibmslapd.conf` file but does not delete the database. You can optionally specify to delete the database also.

Note: On AIX, Linux, or Solaris systems, log on as **root**. On Windows systems, log on with a user ID that is a member of the Administrators group.

For example:

- To unconfigure the database for directory server instance `my_instance`, enter the command:

  ```
  idsucfgdb -n -I my_instance
  ```

  Note: The -n option specifies not to prompt the user for confirmation before unconfiguring
- To unconfigure and delete the database for directory server instance `my_instance`, enter the command:

  ```
  idsucfgdb –r –n -I myinstance
  ```

  Note:

  1. The `-n` option specifies not to prompt the user for confirmation before unconfiguring
  2. The `-r` option specifies deletion of the database

See the *IBM Tivoli Directory Server Command Reference* for detailed information about the **idsucfgdb** command.

Deleting a directory server instance

You can delete a directory server instance and its associated database instance by using either the Instance Administration Tool or the command line.

Using the Instance Administration Tool

Use the Instance Administration Tool to delete a directory server instance, and optionally, its associated database instance.

Procedure

1. On AIX, Linux, or Solaris systems, log on as **root**. On Windows systems, log on with a user ID that is a member of the Administrators group.
2. Stop the directory instance, if it is running.
3. Start the Instance Administration Tool, if it is not already running.
   - On AIX, Linux, Solaris, or Windows systems, enter the following command:`idsxinst`
   - On Windows systems, you also can click **Start** > **Programs** > **IBM Tivoli Directory Server** > **Instance Administration Tool**.
4. In the **IBM Tivoli Directory Server Instance Administration Tool** window, select the instance to delete and click **Delete...**.
5. In the **Delete directory server instance** window, select one of the following options:

Delete directory server instance only
To remove the directory server instance but leave the database instance intact.

Delete directory server instance and destroy associated database instance
To remove both the directory server instance and the database instance.

6. Click **Delete**. Messages are displayed in the Task Messages pane as the operation is performed.
7. Click **Close** after the operation completes to close the window and return to the main window of the Instance Administration Tool.
8. When you finish using the Instance Administration Tool, click **Close** to exit the tool.

Using the command line

Use the **idsidrop** command to delete a directory server instance.

Procedure

1. On AIX, Linux, or Solaris systems, log on as **root**. On Windows systems, log on with a user ID that is a member of the Administrators group.
2. Stop the directory instance to be removed.
3. Enter the command to delete the instance. Provide the appropriate options for the command.

   Examples:

   - To remove the directory server instance but retain the associated database instance:

     ```
     idsidrop -I <instance_name>
     ```

   - To remove a directory server instance and destroy the associated database instance:

     ```
     idsidrop -I <instance_name> -r
     ```

   - To unconfigure the associated database instance without removing a directory server instance:

     ```
     idsidrop -I <instance_name>
     -R
     ```

Results

See the *IBM Tivoli Directory Server Command Reference* for information about the **idsidrop** command.

Removing packages

Uninstalling Security Access Manager is a three-part process. You must unconfigure components, remove Security Access Manager packages, and then restart the system.

Uninstalling IBM Tivoli Directory Server

After you unconfigure IBM Tivoli Directory Server, you can uninstall it.

Before you begin

The appropriate method for uninstalling IBM Tivoli Directory Server depends on the method you used to install Tivoli Directory Server. Use the following table to choose the correct method for uninstalling.

Table 36. Methods for uninstalling Tivoli Directory Server

Method used to install Tivoli Directory Server	Method to uninstall Tivoli Directory Server
Tivoli Directory Server installation wizard "Installing IBM Tivoli Directory Server with the Tivoli Directory Server installation wizard" on page 58	Use the following procedure, which uses a graphical user interface like the installation wizard.
Script file	Use the method for your platform: • "AIX: Removing packages" • "Linux: Removing packages" on page 411 • "Solaris: Removing packages" on page 413 • "Windows: Removing packages" on page 415
Launchpad "Installing Tivoli Directory Server with the Launchpad (Windows only)" on page 67	Use either the following procedure or "Windows: Removing packages" on page 415.

Procedure

1. Open a command prompt.
2. Change to the `_uninst` directory.

   Windows

   ldap_home`\_uninst`

   where *ldap_home* is the location where Tivoli Directory Server is installed.

   AIX and Solaris

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

   Linux

   `/opt/IBM/ldap/V6.3/_uninst`
3. Run the uninstall command:

   Windows

   `uninstall_tds.exe`

   AIX, Linux, or Solaris

   `./uninstall_tds.bin`

AIX: Removing packages

Remove packages on AIX to uninstall Security Access Manager.

Before you begin

Before you remove packages, stop any running Security Access Manager services and applications.

Procedure

1. Ensure that the components are unconfigured (if necessary). Follow the instructions in "Unconfiguring Security Access Manager components" on page 405.

2. Enter the following command: `installp -u -g` *packages*
   where *packages* specifies one or more of the following. **Note:** Use the **–g** option only if you want dependent software for the specified package removed.

AIX Certificate and SSL Base Runtime Acme Toolkit IBM Global Security Kit (GSKit)	GSKit8.gsksslб4.ppc.rte GSKit8.gskcrypt64.ppc.rte
IBM Tivoli Directory Server Web Administration Tool (No SSL)	idsldap.webadmin63
IBM Tivoli Directory Server Web Administration Tool (SSL)	idsldap.webadmin_max_crypto63
IBM Tivoli Directory Server client	idsldap.cltbase63 idsldap.clt64bit63 idsldap.clt_max_crypto64bit63 idsldap.cltjava63
IBM Tivoli Directory Server	idsldap.srv64bit63 idsldap.srvproxy64bit63 idsldap.srv_max_crypto64bit63 idsldap.srv_max_cryptoproxy64bit63 idsldap.msg63.en_US
Security Access Manager Application Development Kit	PD.AuthADK
Security Access Manager Attribute Retrieval Service	PDWeb.ARS
Security Access Manager Authorization Server	PD.Acld
Security Access Manager License	PD.lic
Security Access Manager Plug-in for IBM HTTP Server	PD.WPIIHS
Security Access Manager Plug-in for Web Servers	PD.WPI
Security Access Manager Policy Proxy Server	PD.MgrPrxy
Security Access Manager Policy Server	PD.Mgr
Security Access Manager Runtime	PD.RTE
IBM Security Access Manager Runtime for Java	PDJ.rte
Security Access Manager Session Management Command Line	PD.SMSCLI
Security Access Manager Session Management Server	PD.SMS
Security Access Manager Web Portal Manager	PD.WPM
Security Access Manager Web Security ADK	PDWeb.ADK
Security Access Manager Web Security Runtime	PDWeb.RTE
Security Access Manager WebSEAL	PDWeb.Web
Security Utilities	TivSec.Utl

3. After you remove the packages, restart the system.

Removing DB2

Use this task to remove DB2 on an AIX system.

Procedure

1. Log in as user with `root` authority.
2. Change to the following directory:
   db2_install_dir`/install`

   where *db2_install_dir* is the directory where DB2 is installed.
3. Run the following command:
   `./db2_deinstall -a`

Removing WebSphere Application Server, IBM HTTP Server, or the plug-in for Web servers

To remove WebSphere Application Server and associated WebSphere software, such as IBM HTTP Server, or the plug-in for Web servers from an AIX system, see the instructions in the WebSphere Application Server information center.

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/welcome_nd.html

Linux: Removing packages

Remove packages on Linux to uninstall Security Access Manager.

Before you begin

Before you remove packages, stop any running Security Access Manager services and applications.

Procedure

1. Ensure that you have unconfigured components. Follow instructions in "Unconfiguring Security Access Manager components" on page 405.
2. Enter the following command: `rpm -e` *packages*
   where *packages* specifies one or more of the following component packages:

IBM Global Security Kit (GSKit)	`gskcrypt64-8.0.14.26` `gskssl64-8.0.14.26`
IBM Tivoli Directory Server Web Administration Tool	`idsldap-webadmin63-6.3.0-17`

IBM Tivoli Directory Server client	`idsldap-clt64bit63-6.3.0-17`
	`idsldap-cltbase63-6.3.0-17`
	`idsldap-cljava63-6.3.0-17`

IBM Tivoli Directory Server (64-bit server and 64-bit proxy server packages)	`idsldap-srv64bit63-6.3.0-17` `idsldap-srvproxy64bit63-6.3.0-17`
IBM Tivoli Directory Server English messages	`idsldap-msg63-en-6.3.0-17`
Security Access Manager Application Development Kit	`PDAuthADK-PD-7.0.0-0`

Security Access Manager Attribute Retrieval Service (Linux on System z and Linux on x86-64 only)	PDWebARS-PD-7.0.0-0
Security Access Manager Authorization ServerPDAcld-PD-7.0.0-0	
Security Access Manager License	PDlic-PD-7.0.0-0
Security Access Manager Plug-in for Apache Web Server (Linux on System z only)	PDWPI-Apache-7.0.0-0
Security Access Manager Plug-in for IBM HTTP Server (Linux on x86-64 and Linux on System z)	PDWPI-IHS-7.0.0-0
Security Access Manager Plug-in for Web Servers (Linux on System z and Linux on x86-64)	PDWPI-PD-7.0.0-0
Security Access Manager Policy Proxy Server	PDMgrPrxy-PD-7.0.0-0
Security Access Manager Policy Server	PDMgr-PD-7.0.0-0
Security Access Manager Runtime	PDRTE-PD-7.0.0-0
IBM Security Access Manager Runtime for Java	PDJrte-PD-7.0.0-0
Security Access Manager Session Management Command Line (Linux on System z only)	PDSMS-CLI-7.0.0-0
Security Access Manager Session Management Server (Linux on System z only)	PDSMS-PD-7.0.0-0
Security Access Manager Web Portal Manager	PDWPM-PD-7.0.0-0
Security Access Manager Web Security ADK (Linux on System z and Linux on x86-64 only)	PDWebADK-PD-7.0.0-0
Security Access Manager Web Security Runtime (Linux on System z and Linux on x86-64 only)	PDWebRTE-PD-7.0.0-0
Security Access Manager WebSEAL (Linux on System z and Linux on x86-64 only)	PDWeb-PD-7.0.0-0
Security Utilities	TivSecUtl-TivSec-7.0.0-0

3. After you remove the packages, restart the system.

Results

Note: Not all of the packages that are listed are available for each type of Linux .

Removing DB2

Use this task to remove DB2 on an Linux system.

Procedure

1. Log in as user with `root` authority.
2. Change to the following directory:
   db2_install_dir`/install`
   where *db2_install_dir* is the directory where DB2 is installed.
3. Run the following command:
   `./db2_deinstall -a`

Removing WebSphere Application Server, IBM HTTP Server, or the plug-in for Web servers

To remove WebSphere Application Server and associated WebSphere software, such as IBM HTTP Server, or the plug-in for Web servers from a Linux system, see the instructions in the WebSphere Application Server information center.

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/welcome_nd.html

Solaris: Removing packages

Remove packages on Solaris to uninstall Security Access Manager.

Before you begin

Before you remove packages, stop any running Security Access Manager services and applications.

Procedure

1. Ensure that the components are unconfigured. To unconfigure components, follow the instructions in "Unconfiguring Security Access Manager components" on page 405.
2. To remove a package, enter the following command: `pkgrm` *packages*
   where *packages* specifies one of the following component packages:

IBM Global Security Kit (GSKit)	`gsk8cry64` `gsk8ssl64`
IBM Tivoli Directory Server Web Administration Tool	`IDSlweb63`

IBM Tivoli Directory Server client	`idsldap.cltbase63`
	`idsldap.clt64bit63`
	`idsldap.cltjava63`

IBM Tivoli Directory Server (64-bit server and 64-bit proxy server packages)	`IDSl64s63` `IDSl64p63`
IBM Tivoli Directory Server English messages	`IDSlen63`
Security Access Manager Application Development Kit	`PDAuthADK`
Security Access Manager Attribute Retrieval Service	`PDWebARS`
Security Access Manager Authorization Server	`PDAcld`
Security Access Manager License	`PDlic`

Security Access Manager Plug-in for Apache Web Server	`PDWPIapa`
Security Access Manager Plug-in for IBM HTTP Server	`PDWPIihs`
Security Access Manager Plug-in for Web Servers	`PDWPI`
Security Access Manager Policy Proxy Server	`PDMgrPrxy`
Security Access Manager Policy Server	`PDMgr`
Security Access Manager Runtime	`PDRTE`
IBM Security Access Manager Runtime for Java	`PDJrte`
Security Access Manager Session Management Command Line	`PDSMSCLI`
Security Access Manager Session Management Server	`PDSMS`
Security Access Manager Web Portal Manager	`PDWPM`
Security Access Manager Web Security ADK	`PDWebADK`
Access Manager Web Security Runtime	`PDWebRTE`
Security Access Manager WebSEAL	`PDWeb`
Security Utilities	`TivSecUtl`

3. When prompted to confirm the removal of these components, enter **y**. A prompt is displayed indicating that the pre-removal script is being run. Each file is listed as it is removed.
4. After you remove the packages, restart the system.

Removing DB2

Use this task to remove DB2 from a Solaris system.

Procedure

1. Log in as user with `root` authority.
2. Change to the following directory:
   db2_install_dir`/install`

   where *db2_install_dir* is the directory where DB2 is installed.
3. Run the following command:
   `./db2_deinstall -a`

Removing WebSphere Application Server, IBM HTTP Server, or the plug-in for Web servers

To remove WebSphere Application Server and associated WebSphere software, such as IBM HTTP Server, or the plug-in for Web servers from a Solaris system, see the instructions in the WebSphere Application Server information center.

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/welcome_nd.html

Windows: Removing packages

Remove packages on Solaris to uninstall Security Access Manager.

Before you begin

Before removing packages, stop any running Security Access Manager services and applications.

Procedure

1. Log on as a user with Windows administrator privileges.
2. Select **Start → Control Panel** and then click **Programs and Features**.
3. Select one of the installed components and then click **Remove**. You can select to uninstall the following Security Access Manager packages:
   - IBM Tivoli Directory Server
   - DB2 Enterprise Server Edition
   - Security Access Manager Application Developer Kit
   - Security Access Manager Attribute Retrieval Service
   - Security Access Manager Authorization Server
   - Security Access Manager License
   - Security Access Manager for Plug-in for Internet Information Services
   - Security Access Manager Plug-in for Web Servers
   - Security Access Manager Policy Proxy Server
   - Security Access Manager Policy Server
   - Security Access Manager Session Management Command Line
   - Security Access Manager Session Management Server
   - Security Access Manager Runtime
   - IBM Security Access Manager Runtime for Java
   - Security Access Manager Web Portal Manager
   - Security Access Manager Web Security ADK
   - Security Access Manager Web Security Runtime
   - Security Access Manager WebSEAL
   - Security Utilities
   - GSKit8 SSL 64-bit
4. Select another component from the list or click **OK** to exit the program.
5. When you are done, restart the system.

Removing WebSphere Application Server, IBM HTTP Server, or the plug-in for Web servers

To remove WebSphere Application Server and associated WebSphere software, such as IBM HTTP Server, or the plug-in for Web servers from a Windows system, see the instructions in the WebSphere Application Server information center.

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/welcome_nd.html

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 (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.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

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

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 www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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

Cell Broadband Engine and Cell/B.E. are trademarks of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Index

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Printed in USA

GC23-6502-03