

IBM® Security Access Manager for Enterprise Single
Sign-On
Version 8.2

Installation Guide



IBM® Security Access Manager for Enterprise Single
Sign-On
Version 8.2

Installation Guide



Note

Before using this information and the product it supports, read the information in "Notices" on page 211.

Edition notice

Note: This edition applies to version 8.2 of IBM Security Access Manager for Enterprise Single Sign-On, (product number 5724-V67) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2002, 2012.

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

Figures

1. Stand-alone installation with a virtual appliance 39
2. Stand-alone production server installation 51
3. Replacing the root CA and key signers for WebSphere Application Server in the truststore with a new key size. 57
4. IBM Security Access Manager for Enterprise Single Sign-On in a two-node network deployment cluster example for high availability.. . . . 75
5. Replacing the root CA and key signers for WebSphere Application Server in the truststore with a new key size. 84

Contents

Figures	iii
--------------------------	------------

About this publication	ix
Intended audience	ix
What this publication contains	ix
Publications	x
IBM Security Access Manager for Enterprise Single Sign-On library	x
Accessing terminology online	xii
Accessing publications online	xii
Ordering publications	xii
Accessibility	xiii
Tivoli technical training	xiii
Tivoli user groups	xiii
Support information	xiii
Conventions used in this publication	xiii
Typeface conventions	xiv
Operating system-dependent variables and paths	xiv

Part 1. Installing the IMS Server . . . 1

Chapter 1. IMS Server installation road map 3

Server installation by using a virtual appliance	4
Server installation reusing existing middleware	5
New server installation for stand-alone deployments (end-to-end)	6
New server installation on a clustered deployment (end-to-end)	10

Chapter 2. Getting started 15

Preparing the database server	15
Preparing a database server with DB2	16
Preparing a database server with Oracle	19
Preparing a database server with SQL Server	19
Preparing the WebSphere Application Server	20
Installing the WebSphere update installer	22
Installing WebSphere Application Server fix packs	23
Preparing the IBM HTTP Server	24
Installing the IBM HTTP Server fix packs	27
Installing the IBM HTTP Server plug-in fix pack	28
Preparing the directory servers	29
Preparing an Active Directory server	31
Preparing Active Directory Lightweight Directory Services on Windows	32
Preparing the Tivoli Directory Server	32
Installing Tivoli Common Reporting	33
Installing the IMS Server with the IMS Server installer	33
Verifying the IMS Server deployment on the WebSphere Application Server	36

Chapter 3. Setting up a server with a virtual appliance 39

Preparing the virtual appliance DVD	41
Deploying the virtual appliance on VMware ESXi	42
Activating and configuring the virtual appliance	43
Virtual appliance replication for high availability	48

Chapter 4. Setting up a stand-alone production server 51

Creating and choosing profiles for stand-alone server deployments	52
Creating stand-alone profiles (Profile Management tool) for x86 architectures	53
Creating stand-alone profiles (command-line) for x86 or x64 architectures	54
Configuring the WebSphere Application Server	55
Configuring the heap size for the application server	56
Verifying the Windows service for WebSphere Application Server	56
Recreating the root CA for WebSphere Application Server 7.0 (stand-alone)	57
Configuring the IBM HTTP Server plug-in and securing the connection (stand-alone)	61
Enabling SSL directives on the IBM HTTP Server	64
Recreating the SSL certificate for the IBM HTTP Server	66
Configuring the IMS Server for a stand-alone deployment	67
Configuring the IMS Server for a new installation with the IMS Configuration Wizard (stand-alone)	68
Provisioning the IMS Server administrator	71
Updating the ISAMESSOIMS module mapping for connection request forwarding	72
Verifying the IMS Server configuration	73

Chapter 5. Setting up a cluster (network deployment) 75

Creating and choosing profiles for network deployments	76
Creating network deployment profiles (Profile Management Tool) for x86 architectures	78
Creating profiles for network deployments (command-line) for x86 or x64 architectures	81
Recreating the root CA for WebSphere Application Server 7.0 on the deployment manager before creating member nodes	83
Configuring WebSphere Application Server for a cluster	88
Defining a cluster	88
Configuring the heap size for the deployment manager	89
Configuring the heap size for the application server	90

Creating a Windows service for the node agent	90
Configuring the IBM HTTP Server plug-in and securing the connection (network deployment)	92
Enabling SSL directives on the IBM HTTP Server	94
Recreating the SSL certificate for the IBM HTTP Server	95
Configuring the IMS Server for a cluster	97
Configuring the IMS Server with the IMS Configuration Wizard (network deployment)	97
Provisioning the IMS Server administrator	100
Updating the ISAMESSOIMS module mapping for connection request forwarding	101
Disabling auto start for ISAMESSOIMS	102
Overriding session management for the ISAMESSOIMS	103
Verifying the IMS Server configuration	104
Adding application servers to a cluster	105

Part 2. Installing AccessAgent and AccessStudio 107

Chapter 6. AccessAgent and AccessStudio installation road map. . 109

Chapter 7. Installing the AccessAgent 111

Installing the AccessAgent (Setup.exe)	111
Installing the AccessAgent (MSI package)	112
Installing the AccessAgent silently (command-line)	113
Verifying files and registry entries	115
Verifying the ESSO Network Provider	116

Chapter 8. Installing the AccessStudio 117

Installing the AccessStudio (Setup.exe)	117
Installing the AccessStudio (MSI package)	118
Installing the AccessStudio silently (command-line)	119

Chapter 9. Preparing an installation package to install on multiple PCs . . 121

Preparing and installing a prepackaged Wallet	122
Response file parameters (SetupHlp.ini)	123
Setting the AccessAgent installation path	126
Including support for additional languages	126
Ways of setting the IMS Server location	127
Setting the IMS Server location manually (response file)	128
Setting the IMS Server location manually (menu shortcut)	128
Setting the IMS Server location manually (command-line)	128
Setting the IMS Server location manually (registry)	128

Part 3. Upgrading. 129

Chapter 10. IMS Server upgrade road map 131

Upgrading IMS Server 8.0.1 for a stand-alone deployment	131
---	-----

Upgrading IMS Server 8.0.1 for a network deployment (cluster)	134
Upgrading IMS Server 8.1 for a stand-alone deployment	137
Upgrading IMS Server 8.1 for a network deployment (cluster)	138
Upgrading IMS Server 3.6 or 8.0	139

Chapter 11. Upgrading to 8.2. 141

Installing the IMS Server with the installer for an upgrade	141
Upgrading configurations from 8.1 to 8.2	144
Upgrading configurations from 8.0.1 to 8.2	144
Configuring the SSL certificate after an upgrade	145
Upgrading the AccessAgent	146
Upgrading the AccessStudio	147
Verifying a successful upgrade	147

Chapter 12. Migrating the IMS Server 8.2 from one host to another. 149

Part 4. Uninstalling 151

Chapter 13. Uninstalling. 153

Uninstalling the IMS Server	153
Uninstalling the AccessAgent	155
Uninstalling the AccessAgent silently (unattended)	156
Uninstalling the AccessStudio	156
Uninstalling the AccessStudio silently (unattended)	157

Chapter 14. Reinstalling or reconfiguring the IMS Server. 159

Cleaning up the IMS Server configuration on WebSphere Application Server	159
--	-----

Part 5. Appendixes 161

Appendix A. Planning worksheet . . . 163

Appendix B. Creating database schemas 175

Creating users manually	176
-------------------------	-----

Appendix C. Other installation and configuration tasks 179

Configuring the IMS Server to use directory servers	179
Configuring the IMS Server to use Active Directory servers	180
Configuring the IMS Server to use LDAP servers	184
Configuring a generic LDAP directory server other than Tivoli Directory Server	187
Backing up and restoring	188

Backing up WebSphere Application Server profiles (manageprofiles command)	188	Installing the IMS Server EAR files (command-line)	201
Backing up the IMS Server configuration (Export Configuration Utility)	189	Resynchronizing the nodes	201
Backing up the database in DB2	189	Installing the web server plug-in for WebSphere Application Server manually	202
Restoring the WebSphere Application Server profiles	190	Creating the database in SQL Server manually	203
Restoring the database in DB2	191	Basic commands for managing WebSphere Application Server profiles	204
Stopping and starting components	191	Ways of resolving hosts and IP addresses	205
Stopping and starting the IBM HTTP Server on Windows	192	Renewing the SSL Certificate used by the IBM HTTP Server	206
Starting the WebSphere Application Server on Windows	193	Adding the IMS Root CA to the truststore	207
Stopping the WebSphere Application Server on Windows	195	Adding the directory server SSL certificate to WebSphere Application Server	208
Stopping and starting the IMS Server applications	197	Retrieving the IBM HTTP Server administrator name and password	209
Deploying IMS Server on WebSphere Application Server manually	197	Uninstalling the TAM E-SSO IMS application from WebSphere Application Server	209
Enabling application security in WebSphere Application Server	198		
Installing the Native Library Invoker resource adapter	198	Notices	211
Setting up the command-line tool environment	199	Glossary	215
Installing the IMS Server EAR files manually	200	Index	223

About this publication

IBM® Security Access Manager for Enterprise Single Sign-On automates access to corporate information, strengthens security, and enforces compliance at the enterprise endpoints. With IBM Security Access Manager for Enterprise Single Sign-On, enterprises can efficiently manage business risks, achieve regulatory compliance, decrease IT costs, and increase user efficiency.

Intended audience

This publication is for system administrators who must install and configure the main IBM Security Access Manager for Enterprise Single Sign-On components:

- Server component (IMS Server)
- Client component (AccessAgent)
- Application profiling component (AccessStudio)

Readers must be familiar with the following topics:

- Implementation of single sign-on requirements
- Security concepts and authentication management
- Types of installation and deployment scenarios
- IBM WebSphere® Application Server

What this publication contains

This publication contains the following sections:

- Chapter 1, “IMS Server installation road map,” on page 3
Provides an overview of the instructions for installing the IMS Server in various scenarios.
- Chapter 2, “Getting started,” on page 15
Provides instructions of how to install the IMS Server and prepare the necessary prerequisites.
- Chapter 3, “Setting up a server with a virtual appliance,” on page 39
Provides instructions for installing and configuring the IMS Server with a virtual appliance.
- Chapter 4, “Setting up a stand-alone production server,” on page 51
Provides instructions for installing and configuring the server component in a stand-alone server deployment.
- Chapter 5, “Setting up a cluster (network deployment),” on page 75
Provides instructions on how to install and configure the server component in a clustered deployment.
- Chapter 6, “AccessAgent and AccessStudio installation road map,” on page 109
Provides an overview of installing AccessAgent and AccessStudio.
- Chapter 7, “Installing the AccessAgent,” on page 111
Provides an overview of installing AccessAgent.
- Chapter 8, “Installing the AccessStudio,” on page 117
Provides an overview of installing AccessStudio.

- Chapter 9, “Preparing an installation package to install on multiple PCs,” on page 121
Provides instructions on packaging the client installers for silent deployments or push-based installations.
- Chapter 10, “IMS Server upgrade road map,” on page 131
Provides an overview of instructions for upgrading from earlier versions of the product.
- Chapter 11, “Upgrading to 8.2,” on page 141
Provides instructions for upgrading from earlier versions of the product.
- Chapter 12, “Migrating the IMS Server 8.2 from one host to another,” on page 149
Provides an overview of the instructions for migrating an upgraded IMS Server configuration by exporting.
- Chapter 13, “Uninstalling,” on page 153
Provides instructions for uninstalling IBM Security Access Manager for Enterprise Single Sign-On.
- Chapter 14, “Reinstalling or reconfiguring the IMS Server,” on page 159
Provides instructions for reinstalling or reconfiguring the IMS Server.
- Appendix A, “Planning worksheet,” on page 163
Provides the default values you can use during the installation and configuration of the IBM Security Access Manager for Enterprise Single Sign-On.
- Appendix B, “Creating database schemas,” on page 175
Describes how to create the database schema manually.
- Appendix C, “Other installation and configuration tasks,” on page 179
Provides additional deployment instructions such as stopping and starting the server, or deploying the IMS Server manually on an application server.

Publications

This section lists publications in the IBM Security Access Manager for Enterprise Single Sign-On library. The section also describes how to access Tivoli® publications online and how to order Tivoli publications.

IBM Security Access Manager for Enterprise Single Sign-On library

The following documents are available in the IBM Security Access Manager for Enterprise Single Sign-On library:

- *IBM Security Access Manager for Enterprise Single Sign-On Quick Start Guide*, CF38DML
Read this guide for a quick start on the main installation and configuration tasks to deploy and use IBM Security Access Manager for Enterprise Single Sign-On.
- *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*, SC23995203
Read this guide before you do any installation or configuration tasks. This guide helps you to plan your deployment and prepare your environment. It provides an overview of the product features and components, the required installation and configuration, and the different deployment scenarios. It also describes how to achieve high availability and disaster recovery.
- *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*, GI11930901

Read this guide for the detailed procedures on installation, upgrade, or uninstallation of IBM Security Access Manager for Enterprise Single Sign-On.

This guide helps you to install the different product components and their required middleware, and also do the initial configurations required to complete the product deployment. It covers procedures for using virtual appliance, WebSphere Application Server Base editions, and Network Deployment.

- *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*, GC23969201

Read this guide if you want to configure the IMS Server settings, the AccessAgent user interface, and its behavior.

- *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide*, SC23995103

This guide is intended for the Administrators. It covers the different Administrator tasks. This guide provides procedures for creating and assigning policy templates, editing policy values, generating logs and reports, and backing up the IMS Server and its database. Use this guide together with the IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide.

- *IBM Security Access Manager for Enterprise Single Sign-On Help Desk Guide*, SC23995303

This guide is intended for Help desk officers. The guide helps Help desk officers to manage queries and requests from users usually about their authentication factors. Use this guide together with the IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide.

- *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide*, SC23969401

Read this guide for the detailed descriptions of the different user, machine, and system policies that Administrators can configure in AccessAdmin. Use this guide along with the IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide.

- *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide*, GC23969301

Read this guide if you have any issues with regards to installation, upgrade, and product usage. This guide covers the known issues and limitations of the product. It helps you determine the symptoms and workaround for the problem. It also provides information about fixes, knowledge bases, and support.

- *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide*, SC23995603

Read this guide if you want to create or edit profiles. This guide provides procedures for creating and editing standard and advanced AccessProfiles for different application types. It also covers information about managing authentication services and application objects, and information about other functions and features of AccessStudio.

- *IBM Security Access Manager for Enterprise Single Sign-On Provisioning Integration Guide*, SC23995703

Read this guide for information about the different Java™ and SOAP API for provisioning. It also covers procedures for installing and configuring the Provisioning Agent.

- *IBM Security Access Manager for Enterprise Single Sign-On Web API for Credential Management Guide*, SC14764600

Read this guide if you want to install and configure the Web API for credential management.

- *IBM Security Access Manager for Enterprise Single Sign-On Lightweight AccessAgent mode on Terminal Server SDK Guide, SC14765700*
Read this guide for the details on how to develop a virtual channel connector that integrates AccessAgent with Terminal Services applications.
- *IBM Security Access Manager for Enterprise Single Sign-On Serial ID SPI Guide, SC14762600*
IBM Security Access Manager for Enterprise Single Sign-On has a Service Provider Interface (SPI) for devices that contain serial numbers, such as RFID. See this guide to know how to integrate any device with serial numbers and use it as a second authentication factor with AccessAgent.
- *IBM Security Access Manager for Enterprise Single Sign-On Context Management Integration Guide, SC23995403*
Read this guide if you want to install and configure the Context Management solution.
- *IBM Security Access Manager for Enterprise Single Sign-On User Guide, SC23995003*
This guide is intended for the end users. This guide provides instructions for using AccessAgent and Web Workplace.
- *IBM Security Access Manager for Enterprise Single Sign-On Error Message Reference Guide, GC14762400*
This guide describes all the informational, warning, and error messages associated with IBM Security Access Manager for Enterprise Single Sign-On.

Accessing terminology online

The IBM Terminology Web site consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology Web site at the following Web address:

<http://www.ibm.com/software/globalization/terminology>

Accessing publications online

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli Information Center Web site at <http://www.ibm.com/tivoli/documentation>.

Note: If you print PDF documents on other than letter-sized paper, set the option in the **File > Print** window that allows Adobe Reader to print letter-sized pages on your local paper.

Ordering publications

You can order many Tivoli publications online at <http://www.elink.ibm.com/publications/servlet/pbi.wss>.

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order Tivoli publications. To locate the telephone number of your local representative, perform the following steps:

1. Go to <http://www.elink.ibm.com/publications/servlet/pbi.wss>.
2. Select your country from the list and click **Go**.

3. Click **About this site** in the main panel to see an information page that includes the telephone number of your local representative.

Accessibility

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

For additional information, see "Accessibility features" in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

Tivoli technical training

For Tivoli technical training information, see the following IBM Tivoli Education Web site at <http://www.ibm.com/software/tivoli/education>.

Tivoli user groups

Tivoli user groups are independent, user-run membership organizations that provide Tivoli users with information to assist them in the implementation of Tivoli Software solutions. Through these groups, members can share information and learn from the knowledge and experience of other Tivoli users. Tivoli user groups include the following members and groups:

- 23,000+ members
- 144+ groups

Access the link for the Tivoli Users Group at www.tivoli-ug.org.

Support information

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

Online

Go to the IBM Software Support site at <http://www.ibm.com/software/support/probsub.html> and follow the instructions.

IBM Support Assistant

The IBM Support Assistant is a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. The IBM Support Assistant provides quick access to support-related information and serviceability tools for problem determination. To install the IBM Support Assistant software, go to <http://www.ibm.com/software/support/isa>.

Troubleshooting Guide

For more information about resolving problems, see the *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide*.

Conventions used in this publication

This publication uses several conventions for special terms and actions, operating system-dependent commands and paths, and margin graphics.

Typeface conventions

This publication uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets) and labels (such as **Tip:** and **Operating system considerations:**)
- Keywords and parameters in text

Italic

- Citations (examples: titles of publications, diskettes, and CDs)
- Words defined in text (example: a nonswitched line is called a *point-to-point line*)
- Emphasis of words and letters (words as words example: "Use the word *that* to introduce a restrictive clause."; letters as letters example: "The LUN address must start with the letter *L*.")
- New terms in text (except in a definition list): a *view* is a frame in a workspace that contains data.
- Variables and values you must provide: ... where *myname* represents....

Monospace

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Operating system-dependent variables and paths

This publication uses the UNIX convention for specifying environment variables and for directory notation.

When using the Windows command line, replace *\$variable* with *% variable%* for environment variables and replace each forward slash (/) with a backslash (\) in directory paths. The names of environment variables are not always the same in the Windows and UNIX environments. For example, *%TEMP%* in Windows environments is equivalent to *\$TMPDIR* in UNIX environments.

Note: You can use the UNIX conventions if you are using the bash shell on a Windows system.

Part 1. Installing the IMS Server

Installing the IMS Server for IBM Security Access Manager for Enterprise Single Sign-On depends on the type of server deployment, the available middleware, and the availability requirements.

Chapter 1. IMS Server installation road map

You can install the IMS Server for a new installation or upgrade an existing server from a previous version of the product. You can deploy the server as a virtual appliance, on a stand-alone server, or in a clustered environment.

Note: To upgrade from an earlier version of IMS Server, see Chapter 10, “IMS Server upgrade road map,” on page 131.

Before you begin

Before installing the server, complete the following tasks:

1. Plan and prepare for your deployment. Determine the requirements, deployment scenarios, accounts, and security requirements.
See “Deployment planning” in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.
2. Ensure that you have the administrator privileges to perform the installation.
3. Use the following road maps to determine the best approach to install the server in your environment:
 - “Server installation by using a virtual appliance” on page 4
 - “Server installation reusing existing middleware” on page 5
 - “New server installation for stand-alone deployments (end-to-end)” on page 6
 - “New server installation on a clustered deployment (end-to-end)” on page 10

Server installation by using a virtual appliance

Use the road map as a reference for an IMS Server virtual appliance deployment.

Procedure	Reference
<p>Prepare the database server. You can:</p> <ul style="list-style-type: none"> • Install a new database server or use an existing database server. • Use an IBM DB2®, Microsoft SQL Server, or Oracle Database. 	<ul style="list-style-type: none"> • For the supported database servers and versions, see “Hardware and software requirements” in the <i>IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide</i>. • “Preparing the database server” on page 15. <p>IBM DB2 documentation:</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=/com.ibm.db2.udb.doc/welcome.htm <p>Microsoft documentation:</p> <ul style="list-style-type: none"> • Go to the Microsoft website at http://www.microsoft.com and locate the documentation for your product. <p>Oracle documentation:</p> <ul style="list-style-type: none"> • Go to the Oracle website at http://www.oracle.com and locate the documentation for your product. <p>Note: This guide provides information about configuring databases for the IMS Server. For the detailed and up-to-date installation instructions, see the database product documentation.</p>
<p>Prepare the directory server. You can:</p> <ul style="list-style-type: none"> • Install a new directory server or use an existing directory server. • Use an Active Directory server or an LDAP server. 	<ul style="list-style-type: none"> • For the supported directory servers and versions, see “Hardware and software requirements” in the <i>IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide</i>. • “Preparing the directory servers” on page 29 • For Active Directory installation, see http://technet.microsoft.com/en-us/library/cc758107(v=WS.10).aspx <p>Note: This guide provides instructions about configuring directory servers. For detailed and up-to-date installation instructions, see the directory server product documentation.</p>
<p>Deploy the virtual appliance on VMware ESXi.</p>	<p>“Deploying the virtual appliance on VMware ESXi” on page 42</p>
<p>Activate and configure the virtual appliance.</p>	<p>“Activating and configuring the virtual appliance” on page 43</p>
<p>If your directory server connections use SSL, add the directory server certificates to WebSphere Application Server.</p>	<p>“Adding the directory server SSL certificate to WebSphere Application Server” on page 208</p>

Procedure	Reference
Provision the IMS Server administrator.	"Provisioning the IMS Server administrator" on page 71
Verify the IMS Server configuration.	"Verifying the IMS Server configuration" on page 73

Server installation reusing existing middleware

If you have an existing installation with the required middleware, you can reuse existing middleware.

Procedure	Reference
Configure the WebSphere Application Server.	<p>For stand-alone deployments:</p> <ul style="list-style-type: none"> "Creating and choosing profiles for stand-alone server deployments" on page 52 "Configuring the WebSphere Application Server" on page 55 <p>For network deployments:</p> <ul style="list-style-type: none"> "Creating and choosing profiles for network deployments" on page 76 "Configuring WebSphere Application Server for a cluster" on page 88
If your directory server connections use SSL, add the directory server certificates to WebSphere Application Server.	"Adding the directory server SSL certificate to WebSphere Application Server" on page 208
Configure the IBM HTTP Server.	<ul style="list-style-type: none"> "Configuring the IBM HTTP Server plug-in and securing the connection (stand-alone)" on page 61 "Configuring the IBM HTTP Server plug-in and securing the connection (network deployment)" on page 92
Deploy the IMS Server applications on the WebSphere Application Server.	"Installing the IMS Server with the IMS Server installer" on page 33
Verify the IMS Server deployment on the WebSphere Application Server.	"Verifying the IMS Server deployment on the WebSphere Application Server" on page 36
Configure the IMS Server.	<ul style="list-style-type: none"> "Configuring the IMS Server for a new installation with the IMS Configuration Wizard (stand-alone)" on page 68 "Configuring the IMS Server to use directory servers" on page 179 (Network deployment) "Overriding session management for the ISAMESSOIMS" on page 103
Provision the IMS Server administrator.	"Provisioning the IMS Server administrator" on page 71
Update the ISAMESSOIMS module mapping to forward connection requests.	"Updating the ISAMESSOIMS module mapping for connection request forwarding" on page 72

Procedure	Reference
Verify the IMS Server configuration.	"Verifying the IMS Server configuration" on page 73

New server installation for stand-alone deployments (end-to-end)

Use the roadmap as a reference to install a stand-alone server.

Procedure	Reference
<p>Prepare the database server. You can:</p> <ul style="list-style-type: none"> • Install a new database server or use an existing database server. • Use an IBM DB2, Microsoft SQL Server, or Oracle Database. 	<p>For the supported database servers and versions, see "Hardware and software requirements" in the <i>IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide</i>.</p> <p>For sample instructions, see the following topics:</p> <ul style="list-style-type: none"> • "Preparing the database server" on page 15 <p>IBM DB2 documentation:</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=/com.ibm.db2.udb.doc/welcome.htm <p>Microsoft documentation:</p> <ul style="list-style-type: none"> • Go to the Microsoft website at http://www.microsoft.com and locate the documentation for your product. <p>Oracle documentation:</p> <ul style="list-style-type: none"> • Go to the Oracle website at http://www.oracle.com and locate the documentation for your product. <p>Note: This guide provides information about configuring databases for the IMS Server. For the detailed and up-to-date installation instructions, see the database product documentation.</p>

Procedure	Reference
<p>Prepare the directory server. You can:</p> <ul style="list-style-type: none"> • Install a new directory server or use an existing directory server. • Use single or multiple directory servers. 	<p>For the supported directory servers and versions, see “Hardware and software requirements” in the <i>IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide</i>.</p> <p>For sample instructions, see the following topics:</p> <ul style="list-style-type: none"> • “Preparing the directory servers” on page 29 <p>Microsoft documentation:</p> <ul style="list-style-type: none"> • Go to the Microsoft website at http://www.microsoft.com and locate the documentation for your product. <p>Note: This guide provides instructions about configuring directory servers. For detailed and up-to-date installation instructions, see the directory server product documentation.</p>
<p>Prepare the WebSphere Application Server:</p> <ul style="list-style-type: none"> • Install WebSphere Application Server. • Install the WebSphere update installer. • Install the WebSphere Application Server fix pack. 	<p>For the supported WebSphere Application Server versions, see “Hardware and software requirements” in the <i>IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide</i>.</p> <p>For sample instructions, see the following topics:</p> <ul style="list-style-type: none"> • “Preparing the WebSphere Application Server” on page 20 • “Installing the WebSphere update installer” on page 22 • “Installing WebSphere Application Server fix packs” on page 23 <p>WebSphere Application Server documentation:</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp <p>Note: This guide provides instructions about preparing the WebSphere Application Server for the IMS Server. For detailed and up-to-date installation instructions, see the WebSphere Application Server documentation.</p>

Procedure	Reference
<p>Prepare the IBM HTTP Server:</p> <ul style="list-style-type: none"> • Install the IBM HTTP Server. • Install the IBM HTTP Server fix pack by using the WebSphere Application Server Update Installer. 	<p>For the supported IBM HTTP Server versions, see “Hardware and software requirements” in the <i>IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide</i>.</p> <p>For sample instructions, see the following topics:</p> <ul style="list-style-type: none"> • “Preparing the IBM HTTP Server” on page 24 • “Installing the IBM HTTP Server fix packs” on page 27 <p>IBM HTTP Server documentation:</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/ihs/ihs/tihs_installihs.html <p>Note: This guide provides instructions about preparing the IBM HTTP Server. For detailed and up-to-date installation instructions, see the IBM HTTP Server documentation.</p>
<p>Create a stand-alone WebSphere Application Server profile.</p>	<p>“Creating and choosing profiles for stand-alone server deployments” on page 52</p>
<p>Configure the WebSphere Application Server. These tasks secure the deployment and tune the Java Virtual Machine (JVM) performance.</p> <ul style="list-style-type: none"> • Configure the JVM heap size. • Verify the Windows service for WebSphere Application Server. • Optional: Recreate the 1024 bit root CA if your deployment requires a larger 2048 bit key size. 	<p>For sample instructions, see the following topics:</p> <ul style="list-style-type: none"> • “Configuring the heap size for the application server” on page 56 • “Verifying the Windows service for WebSphere Application Server” on page 56 • “Recreating the root CA for WebSphere Application Server 7.0 (stand-alone)” on page 57 <p>WebSphere Application Server documentation:</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp
<p>If your directory server connections use SSL, add the directory server certificates to WebSphere Application Server.</p>	<p>“Adding the directory server SSL certificate to WebSphere Application Server” on page 208</p>

Procedure	Reference
Configure the IBM HTTP Server: <ul style="list-style-type: none"> • Configure the IBM HTTP Server plug-in and secure the connection. • Enable Secure Socket Layer (SSL) directives on the IBM HTTP Server. • Optional: Recreate the SSL certificate for the IBM HTTP Server. 	For sample instructions, see the following topics: <ul style="list-style-type: none"> • “Configuring the IBM HTTP Server plug-in and securing the connection (stand-alone)” on page 61 • “Enabling SSL directives on the IBM HTTP Server” on page 64 • “Recreating the SSL certificate for the IBM HTTP Server” on page 66 IBM HTTP Server documentation: <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/ihs/ihs/tihs_installihs.html <p>Note: This guide provides instructions about preparing the IBM HTTP Server. For detailed and up-to-date installation instructions, see the IBM HTTP Server documentation.</p>
Install the IMS Server on WebSphere Application Server.	“Installing the IMS Server with the IMS Server installer” on page 33
Verify the IMS Server deployment on the WebSphere Application Server.	“Verifying the IMS Server deployment on the WebSphere Application Server” on page 36
Configure the IMS Server.	<ul style="list-style-type: none"> • “Configuring the IMS Server for a new installation with the IMS Configuration Wizard (stand-alone)” on page 68 • “Configuring the IMS Server to use directory servers” on page 179
Provision the IMS Server administrator.	“Provisioning the IMS Server administrator” on page 71
Update the ISAMESSOIMS module mapping to forward connection requests.	“Updating the ISAMESSOIMS module mapping for connection request forwarding” on page 72
Verify the IMS Server configuration.	“Verifying the IMS Server configuration” on page 73

New server installation on a clustered deployment (end-to-end)

Use the road map as a reference to install the server on a clustered environment.

Procedure	Reference
<p>Prepare the database server. You can:</p> <ul style="list-style-type: none"> • Install a new database server or use an existing database server. • Use an IBM DB2, Microsoft SQL Server, or Oracle Database. 	<p>For the supported database servers and versions, see “Hardware and software requirements” in the <i>IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide</i>.</p> <p>For sample instructions, see the following topics:</p> <ul style="list-style-type: none"> • “Preparing the database server” on page 15 <p>IBM DB2 documentation:</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=/com.ibm.db2.udb.doc/welcome.htm <p>Microsoft documentation:</p> <ul style="list-style-type: none"> • Go to the Microsoft website at http://www.microsoft.com and locate the documentation for your product. <p>Oracle documentation:</p> <ul style="list-style-type: none"> • Go to the Oracle website at http://www.oracle.com and locate the documentation for your product. <p>Note: This guide provides information about configuring databases for the IMS Server. For the detailed and up-to-date installation instructions, see the database product documentation.</p>
<p>Prepare the directory server. You can:</p> <ul style="list-style-type: none"> • Install a new directory server or use an existing directory server. • Use multiple directory servers or a single directory server. 	<p>For the supported directory servers and versions, see “Hardware and software requirements” in the <i>IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide</i>.</p> <p>For sample instructions, see the following topics:</p> <ul style="list-style-type: none"> • “Preparing the directory servers” on page 29 <p>Microsoft documentation:</p> <ul style="list-style-type: none"> • http://technet.microsoft.com/en-us/library/cc758107(v=WS.10).aspx <p>Note: This guide provides instructions about configuring directory servers. For detailed and up-to-date installation instructions, see the directory server product documentation.</p>

Procedure	Reference
<p>On Host A, prepare the WebSphere Application Server:</p> <ul style="list-style-type: none"> • Install the WebSphere Application Server. • Install the WebSphere update installer. • Install the WebSphere Application Server fix pack. <p>On Host B, prepare the WebSphere Application Server:</p> <ul style="list-style-type: none"> • Install the WebSphere Application Server. • Install the WebSphere update installer. • Install the WebSphere Application Server fix pack. 	<p>For the supported WebSphere Application Server versions, see “Hardware and software requirements” in the <i>IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide</i>.</p> <p>For sample instructions, see the following topics:</p> <ul style="list-style-type: none"> • Chapter 5, “Setting up a cluster (network deployment),” on page 75 • “Preparing the WebSphere Application Server” on page 20 • “Installing the WebSphere update installer” on page 22 • “Installing WebSphere Application Server fix packs” on page 23 <p>WebSphere Application Server documentation:</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp <p>Note: This guide provides instructions about preparing the WebSphere Application Server for the IMS Server. For detailed and up-to-date installation instructions, see the WebSphere Application Server documentation.</p>
<p>Optional: Recreate the 1024 bit root CA if your deployment requires a larger 2048 bit key size.</p>	
<p>Prepare the IBM HTTP Server:</p> <ul style="list-style-type: none"> • Install the IBM HTTP Server. • Install the IBM HTTP Server fix pack by using the WebSphere Application Server Update Installer. 	<p>For the supported IBM HTTP Server versions, see “Hardware and software requirements” in the <i>IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide</i>.</p> <p>For sample instructions, see the following topics:</p> <ul style="list-style-type: none"> • “Preparing the IBM HTTP Server” on page 24 • “Installing the IBM HTTP Server fix packs” on page 27 <p>IBM HTTP Server documentation:</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/ihs/ihs/tihs_installihs.html <p>Note: This guide provides instructions about preparing the IBM HTTP Server. For detailed and up-to-date installation instructions, see the IBM HTTP Server documentation.</p>

Procedure	Reference
<p>For the WebSphere Application Server, create the deployment manager and nodes:</p> <ol style="list-style-type: none"> On Host A, create a deployment manager profile and custom profile. Note: Before you federate the custom profile on the deployment manager, ensure that there is two way name resolution between the deployment manager and custom nodes. On Host B, create a custom profile. 	<ul style="list-style-type: none"> “Ways of resolving hosts and IP addresses” on page 205 “Creating and choosing profiles for network deployments” on page 76
<p>Configure the WebSphere Application Server:</p> <ul style="list-style-type: none"> Create a cluster definition and add members to the cluster. Configure the Java heap size for the deployment manager. Configure the Java heap size for the WebSphere Application Server. Create a Windows service for the node agent. 	<p>For sample instructions, see the following topics:</p> <ul style="list-style-type: none"> “Configuring WebSphere Application Server for a cluster” on page 88 “Defining a cluster” on page 88 “Configuring the heap size for the deployment manager” on page 89 “Configuring the heap size for the application server” on page 56 “Creating a Windows service for the node agent” on page 90 <p>WebSphere Application Server documentation:</p> <ul style="list-style-type: none"> http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp <p>Note: This guide provides instructions about preparing the WebSphere Application Server for the IMS Server. For detailed and up-to-date installation instructions, see the WebSphere Application Server documentation.</p>
<p>If your directory server connections use SSL, add the directory server certificates to WebSphere Application Server.</p>	<p>“Adding the directory server SSL certificate to WebSphere Application Server” on page 208</p>

Procedure	Reference
Configure the IBM HTTP Server: <ul style="list-style-type: none"> • Configure the IBM HTTP Server plug-in and secure the connection. • Enable Secure Socket Layer (SSL) directives on IBM HTTP Server. • Optional: Recreate the SSL certificate for IBM HTTP Server. 	For sample instructions, see the following topics: <ul style="list-style-type: none"> • “Configuring the IBM HTTP Server plug-in and securing the connection (network deployment)” on page 92 • “Enabling SSL directives on the IBM HTTP Server” on page 94 • “Recreating the SSL certificate for the IBM HTTP Server” on page 95 IBM HTTP Server documentation: <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/ihs/ihs/tihs_installihs.html <p>Note: This guide provides instructions about preparing the IBM HTTP Server. For detailed and up-to-date installation instructions, see the IBM HTTP Server documentation.</p>
If you use a load balancer, ensure that the load balancer is configured to route requests to the web servers you set up.	Check the product documentation from your vendor.
Install the IMS Server.	“Installing the IMS Server with the IMS Server installer” on page 33
Verify the IMS Server deployment on the WebSphere Application Server.	“Verifying the IMS Server deployment on the WebSphere Application Server” on page 36
Configure the IMS Server.	<ul style="list-style-type: none"> • “Configuring the IMS Server with the IMS Configuration Wizard (network deployment)” on page 97 • “Configuring the IMS Server to use directory servers” on page 179
Provision the IMS Server administrator.	“Provisioning the IMS Server administrator” on page 100
Update the ISAMESSOIMS module mapping to forward connection requests.	“Updating the ISAMESSOIMS module mapping for connection request forwarding” on page 101
Disable auto start for the cluster.	“Disabling auto start for ISAMESSOIMS” on page 102
Configure session management for ISAMESSOIMS.	“Overriding session management for the ISAMESSOIMS” on page 103
Verify the IMS Server configuration.	“Verifying the IMS Server configuration” on page 104
Optional: Add additional application servers to a cluster.	
Optional: Deploy ISAMESSOIMS on additional nodes in a network deployment.	

Chapter 2. Getting started

Prepare the middleware before you install and configure the IMS Server component for IBM Security Access Manager for Enterprise Single Sign-On.

Note: Some of the procedures include examples, references, or sample values for both network deployments and stand-alone deployments. Choose only the examples that are most appropriate for your environment.

To learn more about stand-alone or clustered scenarios (network deployments), see the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

Preparing the database server

You must prepare a database server to store user and Wallet credentials for single sign-on.

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

You can use an IBM DB2, Microsoft SQL Server, or Oracle Database. For the supported database servers and versions, see “Hardware and software requirements” in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

Tip: You can record the following values in Appendix A, “Planning worksheet,” on page 163:

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

To prepare the IMS Server database with:

IBM DB2

You must create a database before you start the IMS Server installation. See “Preparing a database server with DB2” on page 16.

Oracle database server

You must provide the schema owner username and password. See “Preparing a database server with Oracle” on page 19.

Microsoft SQL Server

You must provide the SQL Server administrator username and password.

You can use the IMS Configuration Wizard to automatically create the IMS Server database.

Alternatively, you can manually create the database and specify its details when you install the IMS Server. See “Preparing a database server with SQL Server” on page 19.

Preparing a database server with DB2

To use DB2 as your database server, you must install it and create a database before you install IBM Security Access Manager for Enterprise Single Sign-On. The DB2 database server stores Wallets and user credentials.

Installing IBM DB2

If you do not have a supported database server installed for IBM Security Access Manager for Enterprise Single Sign-On, then you can install IBM DB2.

Before you begin

- For the supported database servers and versions, see “Hardware and software requirements” in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.
- Ensure that your system meets the installation, memory, and disk requirements.
- Ensure that you have administrator privileges.

About this task

This guide provides information about configuring databases for the IMS Server. For the detailed and up-to-date installation instructions, see the database product documentation. See <http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=/com.ibm.db2.udb.doc/welcome.htm>.

Use the DB2 installation media provided with IBM Security Access Manager for Enterprise Single Sign-On to ensure that you are using the correct version.

Record the values used in the planning worksheet. See Appendix A, “Planning worksheet,” on page 163.

Procedure

1. Take one of the following actions:
 - If you have a DVD, insert it into the DVD drive.
 - If you use the default DB2 Workgroup Server Edition installation images for Windows, extract the files to a temporary directory where you want to install DB2. For example, the installation images you can use are:
 - DB2_97_limited_CD_Win_x86.exe for Windows x86
 - DB2_97_limited_CD_Win_x86-64.exe for Windows x64
- Note:** The DB2 Version 9.7 Workgroup Server Edition extracts installation files to a WSER directory. DB2 Version 9.7 Enterprise Server Edition extracts to an ESE directory.
2. Start the DB2 Setup Launchpad by clicking `setup.exe`. For example:
`c:\images\wser\image\setup.exe`
 3. Click the **Install a product** link.
 4. In the DB2 Workgroup Server Edition Version 9.7 section, click **Install New**.
 5. Install DB2 with the following parameters.
 - a. In the **Select the installation type** panel, select **Typical**.
 - b. Click **Next**.
 - c. In the **Select the installation, response file creation or both** panel, select **Install DB2 Workgroup Server Edition on this computer**.
 - d. Click **Next**.

- e. In the **Select the installation folder** panel, accept the default values. For example C:\Program Files\IBM\SQLLIB
 - f. Click **Next**.
 - g. In the **Set user information for the DB2 Administration Server** panel, specify the db2admin username and password. You can specify a local user or a domain account.

Note: The DB2 installation program automatically creates the db2admin administration server user account. If you select a domain account, the logged on administrator account must have privileges to add users on the domain.
 - h. In the **Configure DB2 instances** panel, accept the default values.
 - i. Click **Next**.
 - j. In the **Prepare the DB2 tools catalog** panel, click **Next**.
 - k. In the **Set up notifications** panel, clear the **Set up your DB2 server to send notifications** check box.
 - l. Click **Next**.
 - m. In the **Enable operating system security for DB2 objects** panel, verify that the **Enable operating system security** check box is selected.

Note: The default option creates the groups DB2ADMNS and DB2USERS on the local computer.
 - n. Click **Next**.
 - o. Review the final configuration settings.
 - p. Click **Install**.
6. When installation completes, click **Finish**.
 7. Close the **DB2 First Steps** window.
 8. Verify that the db2admin account is created.
 - On the local computer:
 - a. Click **Start > Administrative Tools > Computer Management**.
 - b. In the navigation tree, expand and select **Local Users and Groups**.
 - c. Select **Users**.
 - On a Windows domain controller:
 - a. Click **Start > Administrative Tools > Active Directory Users and Computers**.
 - b. Expand the domain group.
 - c. Click **Users**.

Results

You successfully installed a database server with IBM DB2 for the IBM Security Access Manager for Enterprise Single Sign-On installation.

What to do next

You can create and configure a database for IBM Security Access Manager for Enterprise Single Sign-On on DB2.

Creating the DB2 database

For IBM DB2, you must create the database for IBM Security Access Manager for Enterprise Single Sign-On.

Procedure

1. Click **Start > All Programs > IBM DB2 > Profile instance name (default) > General Administration Tools > Control Center**.
2. If the **Control Center View** dialog box is displayed, click **Advanced**.
3. Click **OK**.
4. In the Control Center tree pane, expand and select **All Databases**.
5. Right-click **All Databases**.
6. Select **Create Database > Standard**.
7. Enter the following DB2 configuration parameters:

Database name

Specify a name for the database. For example: `imsdb`.

Default path

Use the default value or specify an alternative path to store the database. For example: the default is `c:\`.

Default buffer pool and table space page size

Change the default value of **4K** to **8K**.

Important: You must specify the buffer pool and page size as **8 K**.

8. Click **Next**.
9. In the **Specify where to store your data** panel, accept the default values.
10. Click **Next**.
11. In the **Specify the locale for this database** panel, specify the following options:

Country/Region

Use the **Default** option.

Territory

Type **US**. Default is **US**.

Code set

Select **UTF-8** code set.

Important: You must specify a UTF-8 code set.

12. Click **Next**.
13. Review the summary of configuration parameters used to create the database.
14. Click **Finish**.
15. After the database is created, click **Close**.
16. Verify that the database is created successfully. In the Control Center tree pane, expand **All Databases**. The database you created for IBM Security Access Manager for Enterprise Single Sign-On is displayed.

Results

You created a database for IBM Security Access Manager for Enterprise Single Sign-On.

What to do next

You can install and configure WebSphere Application Server. See “Preparing the WebSphere Application Server” on page 20.

Preparing a database server with Oracle

Install the Oracle database server and configure it based on the IMS Server database server requirements and settings.

Installation

For the supported databases and versions, see “Hardware and software requirements” in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

This guide provides information about configuring databases for the IMS Server. For the detailed and up-to-date installation instructions, see the database product documentation.

1. Prepare the Oracle installation media.
2. Install and configure the Oracle database server.
3. Install the latest service packs for the Oracle database server.

Important: WebSphere Application Server fix packs 15 and 17 might have connectivity problems with Oracle. See this site for more details: <http://www-01.ibm.com/support/docview.wss?uid=swg21497098>.

As workaround, install the interim fix before running the IMS configuration wizard. See <http://www-01.ibm.com/support/docview.wss?uid=swg24029891> for more details.

Database requirements and settings

Oracle automatically creates the database.

Ensure that you comply with these requirements and settings:

Oracle database requirements

- You must have a database instance name.
- Set database character to **Unicode (AL32UTF8)**.
- Set national character to **UTF8 - Unicode 3.0 UTF-8 Universal character set, CESU-8 compliant, or AL16UTF16 - Unicode UTF-16 Universal character set**.

Database user requirements

- Set default tablespace to **USERS**.
- Set temporary tablespace to **TEMP**.
- Assign user with a **Connect and Resource** role.
- Assign user with the following privileges:
 - **Create Procedure**
 - **Create Session**
 - **Create Table**
 - **Create View**

Preparing a database server with SQL Server

Install the Microsoft SQL Server and configure it based on the IMS Server database server requirements and settings.

Installation

For the supported database servers and versions, see “Hardware and software requirements” in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

For detailed and up-to-date installation instructions, see the respective product documentation.

1. Prepare the SQL Server installation media.
2. Install Microsoft SQL Server.
3. Install the latest security service packs for Microsoft SQL Server.

Database requirements and settings

Use the IMS Server configuration wizard to automatically create an IMS Server database.

Alternatively, you can manually create the database and specify its details when you install the IMS Server.

Ensure that you comply with these database requirements and settings:

Database requirements

- You must have a System Administrator (SA) user name and password.
- Set collation name to **SQL_Latin1_General_CP1_CS_AS**.
- Disable **Enforce password policy**.
- Set default database as the name of the database you created.

Database user requirements

- You must have a database user logon name.
- Use the logon name for your database user name, and schema name.
- Set database role ownership to **db_owner**.
- Run the SQL scripts with a database user privilege.

For information about creating the IMS Server database on a Microsoft SQL Server 2005 or 2008 database server, see “Creating the database in SQL Server manually” on page 203.

Preparing the WebSphere Application Server

The IMS Server application runs on the WebSphere Application Server. Install and configure the WebSphere Application Server before the IMS Server installation.

Before you begin

- Read the WebSphere Application Server installation guide. You must have WebSphere Application Server implementation and administration skills.
- Ensure that you have administrator privileges.
- For the supported WebSphere Application Server versions, see “Hardware and software requirements” in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.
- Ensure that your system meets the requirements.
- Windows Server 2008 R2 is a new operating system that WebSphere Application Server 7.0 supports. When installing WebSphere Application Server on Windows

Server 2008 R2 platforms, the prerequisites check can fail. To resolve the issue, see <http://www-01.ibm.com/support/docview.wss?uid=swg21306830>.

About this task

For detailed and up-to-date installation instructions, see the respective product documentation. See <http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp>.

Use the WebSphere Application Server Network Deployment installation media provided with the product to ensure that you are using the correct version.

Record the values used in the planning worksheet. See Appendix A, “Planning worksheet,” on page 163.

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

Note: If the WebSphere Application Server is already deployed, you must ensure that you have the required fix packs. See the section on preparing required fix packs in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

Procedure

1. Access the IBM WebSphere Application Server Network Deployment Version 7.0 CD for your operating system. You can also extract the files from the archive file that you downloaded from Passport Advantage®. For example: C1G2GML.zip.

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

2. Run the WebSphere installation program `launchpad.exe`.
3. Click **Launch the installation wizard for WebSphere Application Server Network Deployment**.
4. Follow the instructions in the installation wizard until you reach the **Installation Directory** page.
5. In the **Installation Directory** page, accept the default installation directory or change the value. For example: the default installation location is `c:\Program Files\IBM\WebSphere\AppServer`.
6. In the **WebSphere Application Server Environments** page, choose **None**. You create required profiles manually through the profile management tool.

Note: A warning is displayed if you do not create the profile at this stage.

7. When prompted, click **Yes** to proceed with the installation without creating any profiles.
8. In the **Repository for Centralized Installation Managers** page, click **Next**.
9. Follow the rest of the instructions in the installation wizard.
10. When you see the **Installation Results** page, clear the **Create a new WebSphere Application Server profile using the Profile Management Tool** check box.
11. Click **Finish**.

Results

You installed the WebSphere Application Server.

What to do next

Install the WebSphere update installer to apply the latest WebSphere Application Server fix packs.

Installing the WebSphere update installer

Install the WebSphere update installer to apply maintenance fix packs.

Before you begin

- To avoid problems, download and use the latest version of the Update Installer found on the support page. See <http://www-01.ibm.com/support/docview.wss?uid=swg24020448>.
- Ensure that your system meets the requirements. See “Hardware and software requirements” in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

About this task

For the detailed instructions, see the WebSphere Application Server documentation. See http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/ihs/ihs/tihs_installihs.html.

Review the prerequisites before installing the update installer.

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

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

Procedure

1. Copy and extract the update installer compressed file to a writable disk.
For example:
 - 7.0.0.13-WS-UPDI-WinIA32 for Microsoft Windows x86 platforms.
 - 7.0.0.13-WS-UPDI-WinAMD64 for Microsoft Windows x64 platforms.
2. Browse to the extracted UpdateInstaller directory.
3. Use the installation wizard to install the Update Installer. Run `install.exe`. The Installation Wizard for the Update Installer is displayed.
4. Follow the instructions in the installation wizard until you reach the installation directory page.
5. Review the installation directory or accept the defaults. The default installation directory is `C:\Program Files\IBM\WebSphere\UpdateInstaller`.
6. Click **Next**.
7. Review the summary.
8. Click **Next**.
9. Before you finish the installation, clear the **Launch IBM Update Installer for WebSphere software on exit** check box.

10. Click **Finish**.

What to do next

Use the update installer to apply the latest fix packs for WebSphere Application Server.

Installing WebSphere Application Server fix packs

Fix packs are software maintenance updates that include reliability and performance enhancements. You must apply the latest WebSphere Application Server fix pack before you run the IMS Server installation program.

Before you begin

- If you already have an installed WebSphere Application Server, ensure that you are using the required level of fix packs.

To determine the minimum fix pack to apply to WebSphere Application Server, see the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

- If you are reusing an existing WebSphere Application Server with existing profiles, stop any WebSphere Application Server profiles that might be running.

In a command prompt, type `<was_home>\profiles\<profile_name>\bin\stopServer.bat <server_name>`. For example: `C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\bin\stopServer.bat server1`.

Note: Skip this step if you are following the default instructions for a new installation and if you have not created WebSphere Application Server profiles yet.

- If you are using IBM Update Installer Version 7.0.0.0, update it to at least Fix Pack 1 (7.0.0.1) or later. Alternatively, download the latest IBM Update Installer from the IBM Support and Downloads website: <http://www-01.ibm.com/support/docview.wss?uid=swg24020448>.

About this task

This guide provides instructions about preparing the WebSphere Application Server for the IMS Server. For detailed and up-to-date installation instructions, see the WebSphere Application Server documentation. See <http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp>.

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

Important: WebSphere Application Server fix packs 15 and 17 might have connectivity problems with Oracle. See <http://www-01.ibm.com/support/docview.wss?uid=swg21497098> for more details.

As a workaround, install the interim fix before running the IMS configuration wizard. See <http://www-01.ibm.com/support/docview.wss?uid=swg24029891> for more details.

Procedure

1. Access the WebSphere Application Server support site to locate the latest fix packs: <http://www.ibm.com/software/webservers/appserv/was/support/>. The Support overview page for WebSphere Application Server is displayed.

Note: To locate the latest fix pack downloads:

- a. Click the **Downloads** link.
- b. Follow the links and instructions on the page to determine the fix packs to download.

See the following considerations when downloading fix packs for WebSphere Application Server:

- When downloading fix packs for WebSphere Application Server, be sure to download fix packs for other WebSphere Application Server components. For example:
 - *<architecture>* **AMD/Intel AppServer**
 - *<architecture>* **AMD/Intel IBM HTTP Server**
 - *<architecture>* **AMD/Intel Java SDK**
 - Optional: After the download completes, you can copy the downloaded fix pack to the *<updi_home>*\maintenance directory. For example: copy 7.0.0-WAS-WAS-WinX32-FP0000013.pak to C:\Program Files\IBM\WebSphere\UpdateInstaller\maintenance.
2. Apply the fix pack. For example: 7.0.0-WAS-WAS-WinX32-FP0000013.pak
 - a. Start the IBM Update Installer. (**Start > All Programs > IBM WebSphere > Update Installer for Websphere V7.0 Software > Update Installer**)
 - b. Follow the instructions in the installer.
 - 1) In the Product Selection page, select the WebSphere installation directory. For example: the default is C:\Program Files\IBM\WebSphere\AppServer.
 - 2) Click **Next**.
 - 3) Select **Install Maintenance Package**.
 - 4) Click **Next**.
 - 5) In the directory path, specify the location of the maintenance or fix pack.
 - 6) Select the WebSphere Application Server fix pack.
 - 7) Click **Next**.
 - 8) After the prerequisites checker completes successfully, click **Next** to apply the fix pack.

Results

You applied the latest fix pack to the WebSphere Application Server.

Related information:

 <http://www-01.ibm.com/support/docview.wss?uid=swg21497098>

 <http://www-01.ibm.com/support/docview.wss?uid=swg24029891>

Preparing the IBM HTTP Server

Install the web server on a separate server or on the WebSphere Application Server. The web server routes requests from client computers to the WebSphere Application Server or nodes in a cluster.

Before you begin

- For the supported IBM HTTP Server versions, see “Hardware and software requirements” in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

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

About this task

This guide provides instructions about preparing the IBM HTTP Server. For detailed and up-to-date installation instructions, see the IBM HTTP Server documentation. See the information about installing the IBM HTTP Server in the WebSphere Application Server Information Center: <http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp>.

Use the IBM HTTP Server installation media provided with IBM Security Access Manager for Enterprise Single Sign-On to ensure that you are using the correct version.

Record any values you use in the planning worksheet. See Appendix A, “Planning worksheet,” on page 163.

Multiserver installations: If you are installing a cluster of HTTP servers for high availability, use a load balancer to distribute requests to servers in the cluster. When you use a load balancer, remember to record the IP address or target host name of the load balancer in the Appendix A, “Planning worksheet,” on page 163.

Procedure

1. Insert the WebSphere CD or extract the WebSphere supplementary files (C1G2HML.zip for 32-bit) and browse to the /IHS directory. For example: C:\Images\C1G2HML\IHS.

Note: The package number is different for the 64-bit version.

2. Run install.exe.
3. Follow the instructions in the installation wizard to continue.
4. In the **Installation Location** panel, accept the default product installation location or specify your own values.
5. Click **Next**.
6. In the **Port Values Assignment** panel, verify the following default values:

HTTP Port

80

HTTP Administration Port

8008

7. In the **Windows Service Definition** panel, complete the following steps:
 - a. Verify that **Run IBM HTTP Server as a Windows service** is selected.
 - b. Verify that **Run IBM HTTP Administration as a Windows service** is selected.
 - c. Select the **Log on as a local system account** check box.
 - d. In the **User Name** field, specify a local system account. For example: administrator.
 - e. In the **Startup type** list, select **Automatic**.
8. In the **HTTP Administration Server Authentication** panel, complete the following steps:

- a. Select the **Create a user ID for IBM HTTP Server administration server authentication** check box.
 - b. Specify the HTTP administrator account and password. For example: `ihsadmin`.
9. Click **Next**.
10. In the **IBM HTTP Server Plug-in for WebSphere Application Server** panel, complete the following steps:
- a. Ensure the **Install the IBM HTTP Server Plug-in for IBM WebSphere Application Server** check box is selected.

Note: In an environment, where you have multiple deployment manager profiles, you can install the IBM HTTP Server plug-in separately. If you decide to install the plug-in manually at a later stage, clear the check box. See “Installing the web server plug-in for WebSphere Application Server manually” on page 202. If you have only one deployment manager profile, you can leave the option selected.
 - b. Click **Next** to start the web server plug-in installation.
 - c. In **Web server definition**, change or verify the default web server definition name. For example, you can use the default name `webserver1`.

Note: If your multiserver deployment plan requires you to set up another web server, you must specify a unique web server definition name for each web server. For example: `webserver2`.
 - d. For **Host name or IP address for the Application Server**, specify the name of the application server. For example: `appsvr1.example.com`.
 - e. Click **Next**.
11. Review the installation summary.
- Tip:** You can update the Planning Worksheet with the necessary values.
12. Click **Next** to start the IBM HTTP Server installation.
13. Click **Finish**.
14. Start the IBM HTTP Server and Admin Server service.
- a. Click **Start > All Programs > IBM HTTP Server V7.0 > Start Admin Server**.
 - b. Click **Start > All Programs > IBM HTTP Server V7.0 > Start HTTP Server**.
15. Verify that you can access the web server from a web browser. For example:
- To access the web server on the local computer, type `http://localhost` or `http://mywebsvr1`.
Where
`mywebsvr1` is your computer name.
 - To access the web server remotely, when a name server is available to resolve host names, type `http://<fully_qualified_host_name>`. For example `http://mywebsvr1.example.com`.

What to do next

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

Installing the IBM HTTP Server fix packs

Apply the latest fix packs for the IBM HTTP Server. This fix pack updates the base installation to the latest fix pack level.

Before you begin

- Ensure that the WebSphere Application Server Update Installer is installed.
- Download the fix packs.

About this task

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

Procedure

1. Optional: Copy the fix pack you downloaded to the <was_home>/UpdateInstaller/maintenance. For example:
 - 7.0.0-WS-IHS-WinX32-FP00000xx.pak for Windows x86 platforms.
 - 7.0.0-WS-IHS-WinX64-FP00000xx.pak for Windows x64 platforms.
2. Stop the IBM HTTP Server. Click **Start > All Programs > IBM HTTP Server V7.0 > Stop HTTP Server**.
3. Stop the Admin Server. Click **Start > All Programs > IBM HTTP Server V7.0 > Stop Admin Server**.
4. Install the fix pack.
 - a. Launch the update installer wizard. Click **Start > All Programs > IBM WebSphere > Update Installer for WebSphere V7.0 Software > Update Installer**.
 - b. Click **Next**.
 - c. From the **Product Selection** panel, select the IBM HTTP Server installation directory.
 - Important:** Be sure to select the IBM HTTP Server installation directory. For example: C:\Program Files\IBM\HTTPServer.
 - d. Click **Next**.
 - e. From the **Maintenance Operation Selection** panel, select **Install maintenance package**.
 - f. Click **Next**.
 - g. In the **Maintenance Package Directory Selection** page, browse to the <updi_home>\maintenance directory or the path where you copied the fix pack to. The default value is C:\Program Files\IBM\WebSphere\UpdateInstaller\maintenance.
 - h. Click **Next**.
 - i. From the **Available Maintenance Package to Install** panel, click **Select Recommended Updates**, and select the target update.
 - j. Click **Next**.
 - k. On the **Installation Summary** screen, click **Next**.
5. Start the IBM HTTP Server. Click **Start > All Programs > IBM HTTP Server V7.0 > Start HTTP Server**.
6. Start the Admin Server. Click **Start > All Programs > IBM HTTP Server V7.0 > Start Admin Server**.

Results

You applied the latest IBM HTTP Server fix pack on each web server.

What to do next

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

Installing the IBM HTTP Server plug-in fix pack

The latest WebSphere plug-in fix pack is required. Use the update installer to install the WebSphere plug-in fix pack. This task updates the base installation of the plug-in to the latest fix pack.

Before you begin

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

Procedure

1. Optional: Copy the fix pack file to the <updi_home>/maintenance directory. For example:
 - 7.0.0-WS-PLG-WinX32-FP0000013.pak for x86 Windows.
 - 7.0.0-WS-PLG-WinX64-FP0000013.pak for x64 Windows.
2. Stop the IBM HTTP Server. For example: Click **Start > All Programs > IBM HTTP Server V7.0 > Stop HTTP Server**.
3. Install the fix pack.
 - a. Start the update installer wizard. Click **Start > All Programs > IBM WebSphere > Update Installer For WebSphere v7.0 Software > Update Installer**.
 - b. Click **Next**.
 - c. From the **Product Selection** panel, select the IBM HTTP Server Plugins directory. For example <ihs_home>/Plugins directory.
 - d. Click **Next**.
 - e. From the **Maintenance Operation Selection** panel, select **Install maintenance package**.
 - f. Click **Next**.
 - g. In the **Maintenance Package Directory Selection** page, browse to the <updi_home>\maintenance directory or the path where you copied the fix pack. The default value is C:\Program Files\IBM\WebSphere\UpdateInstaller\maintenance.
 - h. Click **Next**.
 - i. From the **Available Maintenance Package to install** panel, click **Select Recommended Updates**.
 - j. Select the target update.
 - k. Click **Next**.
 - l. On the **Installation Summary** screen, click **Next**, to begin fix pack installation.
 - m. Click **Finish**.
4. Start the IBM HTTP Server. For example: Click **Start > All Programs > IBM HTTP Server V7.0 > Start HTTP Server**.

Results

You applied the fix pack for the IBM HTTP Server plug-in.

Preparing the directory servers

Install and set up the directory server so that it communicates with IBM Security Access Manager for Enterprise Single Sign-On. You can use a Microsoft Active Directory, Tivoli Directory Server, or an LDAP-compatible host as a directory server.

A directory service or user registry provides user authentication and access control. IBM Security Access Manager for Enterprise Single Sign-On can work with your existing supported directory server if you are already using a directory service to authenticate and manage user accounts in a repository.

Important: IBM Security Access Manager for Enterprise Single Sign-On does not specifically require an enterprise directory service to retrieve or to store user authentication details.

Integration with a directory server is not an installation prerequisite. IBM Security Access Manager for Enterprise Single Sign-On also operates in enterprise environments that choose not to use a directory service. For additional deployment considerations with a directory server, see the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

You can work in configurations with a single directory server or a federated repository. IBM Security Access Manager for Enterprise Single Sign-On uses the virtual member manager component in WebSphere Application Server to support authentication on directory servers.

Before combining multiple Active Directory servers or user registries, review the following considerations:

- Distinguished names must be unique for a collection of users or groups over all directory servers. For example: If `cn=imsadmin,dc=ibm` exists in *AD-LDAP1*, it must not exist in *AD-LDAP2*, and in *AD-LDAP3*.
- For LDAP only: The short name, for example `imsadmin`, must be unique for a realm over all registries.
- The base distinguished names for all registries used within a realm must not overlap. For example: If *AD-LDAP1* is `cn=users,dc=ibm`, *AD-LDAP2* must not be `dc=ibm`.

For more information about the virtual member manager component in WebSphere Application Server, see the information center: <http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.wim.doc/welcome.html>.

You can choose an enterprise directory before installing IBM Security Access Manager for Enterprise Single Sign-On.

For complete instructions on preparing and setting up an existing directory server, see your vendor supplied documentation for the directory server.

If you decide to use a directory server, see the following deployment notes:

- Prepare to provide the required directory server host name, domain name, port number, required lookup user, bind distinguished names, and base distinguished names.

You must provide the values when you choose to configure the IMS Server with a directory server. You can update the values you need in the Planning worksheet. See Appendix A, “Planning worksheet,” on page 163.

- IBM Security Access Manager for Enterprise Single Sign-On works with both LDAP v3 compatible directory servers like IBM Tivoli Directory Server or an Active Directory.
- To support password resets with AccessAssistant or Web Workplace:
 - On an Active Directory with non-SSL connections, you must install the Tivoli Identity Manager Active Directory Adapter on the same domain.
 - On an Active Directory with an SSL connection, no further directory server configurations are required.
 - Prepare a directory user with administrative privileges. You can also prepare a designated directory user account with password reset privileges on the directory server.
- If you are preparing for a virtual appliance deployment, do not add the `<VA non-root user ID>` in the directory server. The `<VA non-root user ID>` credential must not exist in the directory server.

Supported directory servers

To display a list of supported directory servers for WebSphere Application Server 7.0:

1. Browse to <http://www-01.ibm.com/support/docview.wss?rs=180&uid=swg27012369>.
2. Select your target operating system. For example: **Windows**.
3. Locate the **LDAP Server using Federated Repository Configuration** section to view the list of supported directory servers.

Directory server resources

The following resources can help you prepare a supported directory server and enable security.

Tivoli Directory Server

- Overview and installation instructions
<http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.IBMDS.doc/install27.htm>
- Enabling SSL security instructions
<http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml>

Note: Enter Configuring IBM Tivoli Directory Server for SSL access in the search field.

Microsoft Active Directory

- Overview and installation instructions
Go to the Microsoft website at www.microsoft.com and search for “Active Directory installation overview”.
- Enabling SSL security instructions

Go to the Microsoft website at www.microsoft.com and search for “Active Directory SSL enabling”.

Preparing an Active Directory server

Install and set up the directory server so that Active Directory communicates with IBM Security Access Manager for Enterprise Single Sign-On.

You can prepare an Active Directory server if you plan to use Active Directory as a directory server. For considerations on using a directory server with IBM Security Access Manager for Enterprise Single Sign-On, see the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

SSL is required to set up and change passwords programmatically during sign-on and user creation in Active Directory. Enabling SSL in Active Directory lets clients communicate securely with the Active Directory servers.

Important: If you plan to use password resets in AccessAssistant or Web Workplace but not use Active Directory over SSL, install the Tivoli Identity Manager Active Directory Adapter. See “Preparing the Active Directory Adapter.”

1. Verify the deployment requirements for your Active Directory configuration.

To determine the Active Directory steps you must complete:

- If SSL is required but not yet enabled, see your vendor-specific documentation on enabling SSL for your version of Active Directory.
- If SSL is required and enabled, verify that the SSL port numbers are what you need.
- If SSL is not required in your deployment, see “Preparing the Active Directory Adapter.”

2. Optional: Create a lookup user in Active Directory for IBM Security Access Manager for Enterprise Single Sign-On directory lookups.

To support password resets in AccessAssistant and Web Workplace, you must prepare a directory user with password reset privileges.

Ensure that the user is:

- Active and not set to be disabled.
- Not set to expire.

Note: Avoid creating an administrative user with the same user name as the WebSphere administrator.

Preparing the Active Directory Adapter

Install the Tivoli Identity Manager Active Directory Adapter if you are using Active Directory without SSL and you plan to support password resets in AccessAssistant and Web Workplace.

Before you begin

On the directory server, prepare a user account with domain administrator privileges. For example: *tadadmin*.

About this task

For detailed instructions on installing and configuring the Tivoli Identity Manager Active Directory Adapter, consult the Tivoli Identity Manager adapter documentation.

Use the Tivoli Identity Manager Active Directory Adapter to administer user accounts for IBM Security Access Manager for Enterprise Single Sign-On on an Active Directory domain. The Active Directory Adapter resides on the domain controller or a non-domain controller workstation.

IBM Security Access Manager for Enterprise Single Sign-On documentation does not include instructions on how to install, use, or configure the adapter with Active Directory.

Preparing Active Directory Lightweight Directory Services on Windows

If you plan to use Active Directory Lightweight Directory Services as a user registry, prepare Active Directory Lightweight Directory Services so that it communicates with IBM Security Access Manager for Enterprise Single Sign-On.

Active Directory Lightweight Directory Services (AD LDS), which was previously known as Active Directory Application Mode (ADAM) provides support for directory enabled applications. Use the following high-level steps to prepare AD LDS or ADAM. For considerations on using a directory server with IBM Security Access Manager for Enterprise Single Sign-On, see the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

1. Verify your deployment requirements for AD LDS or ADAM.

For complete documentation on configuring ADAM or AD LDS, go to the Microsoft website at www.microsoft.com and search for “Active Directory Lightweight Directory Services overview”.

Note: By default, Active Directory Lightweight Directory Services on Windows Server 2008 or ADAM on Windows Server 2003 requires SSL to be enabled for password reset in AccessAssistant and Web Workplace.

2. Optional: Create a designated IBM Security Access Manager for Enterprise Single Sign-On lookup user. For example: lookupusr.

To support password resets, you can create an administrative user or a designated user with password reset privileges. For example: myresetuser.

Ensure that the user account is:

- Active and not set to be disabled.
- Not set to expire.

Preparing the Tivoli Directory Server

If you plan to use IBM Tivoli Directory Server as an LDAP enterprise directory, you must prepare the server so that it communicates with IBM Security Access Manager for Enterprise Single Sign-On.

For considerations on using a directory server with IBM Security Access Manager for Enterprise Single Sign-On, see the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

1. Verify your Tivoli Directory Server configuration. For detailed instructions on retrieving information about your deployment, see the respective product documentation.

Note: A limitation in the Tivoli Directory Server is that users or groups must not contain a Turkish uppercase dotted I or lowercase dotted i in the DN. These characters prevent correct retrieval of that user or group.

2. Create the IBM Security Access Manager for Enterprise Single Sign-On lookup user.

Installing Tivoli Common Reporting

Install Tivoli Common Reporting if you want to create, customize, and manage reports. This task is optional.

IBM Security Access Manager for Enterprise Single Sign-On provides auditing capabilities for its components. If auditing is enabled, the software generates audit events and stores them in the database. You can use Tivoli Common Reporting to produce reports on the audit events even if the IMS Server is not running. Tivoli Common Reporting generates reports in HTML, PDF, Microsoft Excel, or Adobe PostScript format.

For installation instructions, see the IBM Tivoli Common Reporting Information Center at: http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc/tcr_welcome.htm.

For information about the reports included for IBM Security Access Manager for Enterprise Single Sign-On, see the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

Installing the IMS Server with the IMS Server installer

Install and deploy the IMS Server to WebSphere Application Server with the IMS Server installer.

Before you begin

- Review the preinstallation considerations. See "Planning for installation" in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.
- Complete the middleware installation and configuration:
 - Create the WebSphere Application Server profile (for stand-alone deployments) or deployment manager profile (for network deployments).
 - Make sure the WebSphere Application Server profile (for stand-alone deployments) or deployment manager profile (for network deployments) is started.
 - Prepare the directory server.
 - Prepare the database server.
 - Prepare the IBM HTTP Server.
 - For WebSphere Application Server stand-alone deployments:
 - Ensure that the server profile is started.
 - Review the WebSphere Application Server configuration for stand-alone deployments.
 - Review the IBM HTTP Server configuration.
 - For WebSphere Application Server Network Deployment:
 - Ensure that the deployment manager profile is started.
 - Review the WebSphere Application Server configuration for a cluster.
 - Review the IBM HTTP Server configuration.
- Review the planning worksheet for the different data required to complete the installation.

About this task

The IMS Server installation process deploys two applications on WebSphere Application Server:

Application name	EAR file name	Contains
ISAMESSOIMS	com.ibm.tamesso.ims-delhi.deploy.isamessoIms.ear	<ul style="list-style-type: none">• AccessAdmin• AccessAssistant and Web Workplace• Runtime web service for IMS Server
ISAMESSOIMSConfig	com.ibm.tamesso.ims-delhi.deploy.isamessoImsConfig.ear	<ul style="list-style-type: none">• IMS Configuration Wizard• IMS Configuration Utility

Procedure

1. Run `imsinstaller.exe` to start the IMS Server installation wizard.
2. Accept the default language or select another language.
3. Click **OK**.
4. Select the product for which you have a license to install.
 - IBM Security Access Manager for Enterprise Single Sign-On Standard
This package offers strong authentication, session management, and centralized logging, and reporting in addition to single sign-on.
 - IBM Security Access Manager for Enterprise Single Sign-On Suite
This package offers one time password support, AccessAgent plug-ins, Web single sign-on and remote access through Web Workplace, custom tracking, and IAM Integration in addition to the Standard package.
5. Click **Next**.
6. Select **I accept the terms in the license agreement**.
7. Click **Next**.
8. Accept the default installation directory or specify a new directory. By default, the IMS Server is installed in `C:\Program Files\IBM\ISAM ESSO\IMS Server`.
9. Click **Next**.
10. Select **Yes** to automatically deploy the IMS Server to the WebSphere Application Server.
 - To deploy the WebSphere Application Server manually, click **No**. See “Deploying IMS Server on WebSphere Application Server manually” on page 197.
11. Click **Yes** to specify that WebSphere Application Server security is enabled. If you click **No**, you must provide the SOAP port. The typical SOAP port for a:
 - Stand-alone deployment is 8880.
 - Network deployment (Deployment manager node) is 8879.

Note: Specify the correct application security details before you proceed. If the security validation for WebSphere Application Server fails, you entered the wrong information. In this case, you can restart the installer.
12. Click **Next**.
13. Configure the WebSphere Application Server administration security settings.

Note: If two-way secure sockets layer (SSL) is enabled for the WebSphere Application Server, the SSL Java keystore file and password are required.

- a. Specify the WebSphere administrative user name and password you provided during the profile creation. For example: wasadmin and password.
- b. Specify the SSL Trusted Java keystore file, trust.p12, and its location.

For example:

- **For WebSphere Application Server stand-alone:**

```
<was_home>\profiles\<AppSrv_profilename>\config\cells\  
<cell_name>\nodes\<node_name>\trust.p12
```

See the following example:

```
C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\  
config\cells\ibmusvr1Node01Cell\nodes\ibmusvr1Node01\trust.p12
```

- **For WebSphere Application Server Network Deployment:**

```
<was_home>\profiles\<Dmgr_profilename>\config\cells\<cell_name>\  
trust.p12
```

See the following example:

```
C:\Program Files\IBM\WebSphere\AppServer\Profiles\Dmgr01\config\  
cells\ibm-svr1Cell01\trust.p12
```

- c. Specify the SSL Trusted keystore password.

The default SSL Trusted keystore password is WebAS.

- d. Optional: Specify the SSL Java keystore file, key.p12, and its location.

For example:

- **For WebSphere Application Server stand-alone:**

```
<was_home>\profiles\<AppSrv_profilename>\config\cells\  
<cell_name>\nodes\<node_name>\key.p12
```

See the following example:

```
C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\  
config\cells\ibmusvr1Node01Cell\nodes\ibmusvr1Node01\key.p12
```

- **For WebSphere Application Server Network Deployment:**

```
<was_home>\profiles\<Dmgr_profilename>\config\cells\<cell_name>\  
key.p12
```

See the following example:

```
C:\Program Files\IBM\WebSphere\AppServer\Profiles\Dmgr01\config\  
cells\ibm-svr1Cell01\key.p12
```

Note: If you specify the SSL Java keystore file, you must specify the keystore password in **SSL keystore password**. See step e.

- e. If you specified the SSL Java keystore file, specify the SSL Java keystore password.

The default SSL Java keystore password is WebAS.

14. Accept the default WebSphere Application Server SOAP connector port or specify a different SOAP connector port.

Note: You can determine the correct port number in the following directory for each profile. For example:

```
Stand-alone : <was_home>/profiles/<AppSrv_profilename>/logs/  
AboutThisProfile.txt
```

Network deployment: <was_home>/profiles/<Dmgr_profilename>/logs/
AboutThisProfile.txt

For example:

- For WebSphere Application Server stand-alone, the default SOAP port for the application server is 8880.
- For WebSphere Application Server Network Deployment, the default SOAP port for the Deployment Manager is 8879.

15. Click **Next**.

16. Click **Install**.

17. In the **Installation Complete** window, click **Done**.

What to do next

Before you set up the IMS Server with the IMS Configuration Wizard, verify the IMS Server deployment on the WebSphere Application Server. See “Verifying the IMS Server deployment on the WebSphere Application Server.”

If there are any IMS Server installation errors, resolve them before you configure the IMS Server. Check the <ims_home>/ISAM_ESSO_IMS_Server_InstallLog.log file for critical IMS Server installation errors that must be addressed.

Verifying the IMS Server deployment on the WebSphere Application Server

Check the Integrated Solutions Console to determine whether the IMS Server is successfully deployed in WebSphere Application Server.

Before you begin

- (Network deployment) Ensure that the deployment manager is started.
- (Stand-alone) Ensure that the application server is started.
- Install the IMS Server.

Procedure

1. Select **Start > All Programs > IBM WebSphere > Application Server <version> > Profiles > <profile name> > Administrative console**.

Where <profile name> is:

- The deployment manager for a network deployment. For example: **Dmgr01**.
- The stand-alone application server instance. For example: **AppSrv01**.

2. Log on to the Integrated Solutions Console with the WebSphere administrator credentials. For example: wasadmin.
3. On the Integrated Solutions Console navigation pane, select **Applications > Application Types > WebSphere Enterprise Applications**.
4. Verify that the following IMS Server applications are on the list:

Application	Status
ISAMESSOIMS	Stopped.
ISAMESSOIMSConfig	Started.

Note: You can leave the ISAMESSOIMS application in a stopped state. However, if you restart the WebSphere Application Server host, the ISAMESSOIMSConfig and the ISAMESSOIMS modules start automatically.

What to do next

After you verify that the IMS Server WebSphere applications are deployed, configure the IMS Server with the IMS Configuration Wizard.

- “Configuring the IMS Server for a new installation with the IMS Configuration Wizard (stand-alone)” on page 68
- “Configuring the IMS Server with the IMS Configuration Wizard (network deployment)” on page 97

Chapter 3. Setting up a server with a virtual appliance

You can deploy a ready to run server virtual appliance on VMware ESX and ESXi for faster deployments. Deploy server virtual appliances in stand-alone or high availability configurations. Unlike installing the server product manually, a virtual appliance contains configured software prerequisites with the IMS Server in a single virtual image.

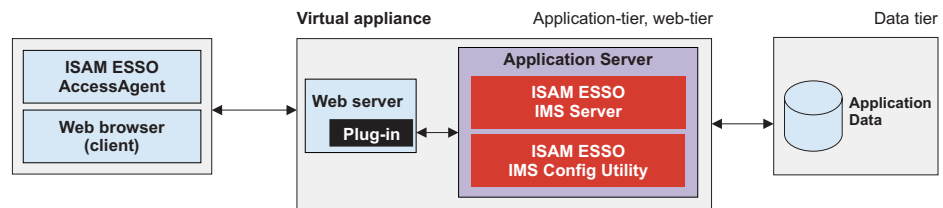


Figure 1. Stand-alone installation with a virtual appliance

For more information about planning and deployment considerations when you set up a server with a virtual appliance, see the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

Road map

The IBM Security Access Manager for Enterprise Single Sign-On virtual appliance is a self-contained virtual image. The virtual image contains SUSE Linux Enterprise Server, WebSphere Application Server Hypervisor Edition, Tivoli Common Reporting, IBM HTTP Server, and the IMS Server application.

Run the virtual image on VMware ESX or ESXi hypervisors. Before you install the virtual appliance, make sure that your virtualization platform meets the requirements. A virtual appliance deployment is easier to deploy because the operating system and applications are already installed and partially configured.

Complete the following tasks:

1. Prepare the database server.
2. Prepare the directory server.
3. Deploy the virtual appliance.
4. Activate and configure the virtual appliance.

The virtual appliance deploys a working IBM Security Access Manager for Enterprise Single Sign-On server enterprise application on a WebSphere Hypervisor. You can use the virtual appliance as a pilot or test system. A single virtual appliance can also act as a single production system for a small department.

For production or high availability environments, you can deploy additional virtual appliances as a replica. A virtual appliance replica refers to a set of virtual appliances which are configured the same way. To simplify the process of

replicating configurations with multiple virtual appliances, you can export the IMS Server configuration to a file. See “Virtual appliance replication for high availability” on page 48.

Note: If the IMS Server configurations change, you must use the *Export and Import configuration tool* to synchronize the configurations manually with other replicas. As the number of replicas increase, the overhead of synchronizing the IMS Server configuration increases. For the management of multiple IMS Server nodes, see the WebSphere Application Server Network Deployment (clustered) approach.

To learn more about high availability considerations for virtual appliances in a replicated configuration, see the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

For information about using the IMS Server *Export and Import configuration tool* to replicate configurations, see the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

What is included in the virtual appliance

The virtual appliance contains the following preinstalled components:

WebSphere Application Server

WebSphere Application Server Hypervisor Edition, provides a centralized application administration platform that extends the ability of a web server to handle web application requests. The IBM Security Access Manager for Enterprise Single Sign-On IMS Server component is a WebSphere application that uses the application server.

IBM HTTP Server

The IBM HTTP Server for WebSphere Application Server Hypervisor Edition is a dedicated HTTP server that is configured to work with the application server.

Tivoli Common Reporting

Tivoli Common Reporting is an optional reporting component that provides advanced report management functions.

IBM Security Access Manager for Enterprise Single Sign-On IMS Server

The IMS Server is a web application on WebSphere Application Server that administrators can use to configure identity management and single sign-on settings.

Note: The virtual appliance distribution includes a set of optional utilities for administering the virtual appliance. For more information, see the section on command-line tools in the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

What is not included in the virtual appliance

The virtual appliance does not include the following components.

Database server

Install the database server separately. However, the standard IBM Security Access Manager for Enterprise Single Sign-On non-virtual appliance software distribution includes a limited use edition of IBM DB2. You must install the database server on a separate server before you install the virtual appliance.

Directory server

If you are using an LDAP server, you can configure the virtual appliance to work with a new directory server or an existing server. For non-SSL Active Directory servers with password reset requirements with AccessAssistant or Web Workplace, install the Active Directory Adapter. You can install the adapter on the domain controller or on a separate host. Prepare the directory server on a separate host before you configure the virtual appliance.

Important: Fingerprint authentication is not supported on the virtual appliance.

Preparing a database server

You can either install or reuse an existing database server before installing the IMS Server because a database server is not included in the virtual appliance. See “Preparing the database server” on page 15.

Preparing directory servers

The virtual appliance does not include a directory server. If you plan to use a directory server to provide user authentication services, you can prepare a new directory server or reuse an existing directory server before installing the IMS Server. You can prepare a required lookup user with directory lookup privileges. See “Preparing the directory servers” on page 29.

IBM Security Access Manager for Enterprise Single Sign-On IMS Server and web server configuration

The image contains IBM HTTP Server for WebSphere Application Server Hypervisor Edition and web server plug-ins, which are installed and configured for the user. Most of the environment is pre-configured. Additional web server configuration is not required for basic operations.

You can stop and start the IBM HTTP Server, and the IBM Security Access Manager for Enterprise Single Sign-On server in the administrative console.

Preparing the virtual appliance DVD

If you obtained the IBM Security Access Manager for Enterprise Single Sign-On virtual appliance from a set of DVDs, you must combine and extract the files before you can deploy the virtual appliance.

Before you begin

Ensure that you have the virtual appliance DVD distribution.

Procedure

1. Copy the files from the 3 virtual appliance DVDs to the same folder on your local computer. The DVD of the IMS Server virtual appliance package consists of archived files that are split into multiple parts.
2. In a command prompt, navigate to the folder where you copied the files.
3. Combine the split archives into a single archive.

Type one of the following commands, without line breaks:

Windows

```
copy /b ISAMESSO_IMS_VA_<version>.zip.001+
ISAMESSO_IMS_VA_<version>.zip.002+
ISAMESSO_IMS_VA_<version>.zip.003 ISAMESSO_IMS_VA_<version>_FULL.zip
```

Linux

```
cat ISAMESSO_IMS_VA_<version>.zip.001+
ISAMESSO_IMS_VA_<version>.zip.002+
ISAMESSO_IMS_VA_<version>.zip.003 ISAMESSO_IMS_VA_<version>_FULL.zip
```

4. Extract the complete archive, ISAMESSO_IMS_VA_<version>_FULL.zip, to a location on the computer.

Windows

On Windows, you can use a third-party utility to extract the file: ISAMESSO_IMS_VA_<version>_FULL.zip.

Note: The Windows **unzip** command-line tool can fail.

Linux

In a command prompt, enter:

```
unzip -d <output_directory> ISAMESSO_IMS_VA_<version>_FULL.zip
```

where

<output_directory> is the location of the extracted files. For example: /home/<username>/va

5. Ensure that the following extracted files exist in the extracted location. These files have the OVF, MF, and VMDK file type extensions.
 - ISAMESSO_IMS_VA_<version>-disk1.vmdk
 - ISAMESSO_IMS_VA_<version>-disk2.vmdk
 - ISAMESSO_IMS_VA_<version>-disk3.vmdk
 - ISAMESSO_IMS_VA_<version>-disk4.vmdk
 - ISAMESSO_IMS_VA_<version>.mf
 - ISAMESSO_IMS_VA_<version>.ovf

Results

You successfully extracted the virtual appliance files.

Deploying the virtual appliance on VMware ESXi

Start the IBM Security Access Manager for Enterprise Single Sign-On server virtual image and use the VMware ESXi hypervisor to configure the operating system and the product.

Before you begin

- Ensure that the VMware vSphere Client is installed on the computer.
- Ensure that you have an account to log on to the VMware ESXi host with privileges to create and deploy virtual machines.
- Prepare the IMS Server virtual appliance DVD or download the images from Passport Advantage (<http://www.ibm.com/software/howtobuy/passportadvantage/>).
- If you are using the virtual appliance DVD, you must combine and extract the files from the DVD.

About this task

Use the **Deploy OVF Wizard** from the vSphere Client to deploy the IBM Security Access Manager for Enterprise Single Sign-On virtual appliance on a virtual machine. The vSphere Client is the client application that lets you start and run virtual machines on the VMware ESXi hypervisor.

Procedure

1. Take one of the following actions:
 - If you have the DVD distribution, copy the prepared files to a single location on your computer. To prepare or combine the files from a DVD distribution, see “Preparing the virtual appliance DVD” on page 41.
 - If you have the downloaded source, extract and copy the files to a single location on your computer.

The extracted virtual appliance package consists of files with the OVF, MF, and VMDK file type extensions.

2. On Microsoft Windows, click **Start > All Programs > VMware > VMware vSphere Client**.
3. Log on to the **VMware vSphere Client**.
4. In the **VMware vSphere Client**, click **File > Deploy OVF Template**.
5. Click **Deploy from File** and choose the ISAMESSO_IMS_VA_<version>.ovf file.
6. Click **Next**.
7. Verify the template details and then click **Next**.
8. Specify a name for the virtual appliance in the ESXi inventory folder. For example: ISAMESSO_IMS_VA_82
9. Click **Next**.
10. Specify a location to store your virtual appliance files and then click **Next**.
11. Verify the installation summary; then click **Finish**. The deployment process starts uploading the virtual appliance to the VMware ESXi host.
12. Click **Close**.

Results

You deployed the IBM Security Access Manager for Enterprise Single Sign-On virtual appliance on the VMware ESXi hypervisor. The virtual appliance is ready to be activated.

What to do next

Complete the appropriate task:

- If you do not have a database server installed, you must install and configure a database server on a separate host before you activate the virtual appliance. See “Preparing the database server” on page 15.
- If you have a database server installed, activate and configure the virtual appliance. See “Activating and configuring the virtual appliance.”

Activating and configuring the virtual appliance

You can activate the virtual appliance and configure the IMS Server.

Before you begin

- Prepare the database server.
- Prepare the directory server.
- Ensure that you can provide the following information:

Type of information	Values
Network information	<ul style="list-style-type: none">• Host name• Domain name• (Static only) IP address• (Static only) Net mask• (Static only) Gateway address
Database information	<ul style="list-style-type: none">• Database for the IMS Server• Database host IP or address• Database administrator credentials
Enterprise directory or repository information	<ul style="list-style-type: none">• Repository fully qualified domain name• Repository domain name• Base distinguished name• Bind distinguished name

Note: There is no indication whether the virtual appliance IP address is duplicated in the network. An IP address conflict can occur and cause the IMS Server configuration to timeout.

Remember: To ensure that clients on a domain can connect to the IMS Server, you must add a DNS entry for the IP address of the virtual appliance. On the virtual appliance, ensure that there is a hosts entry for the domain controller.

About this task

Activate the virtual appliance and configure the credentials for two user accounts:

- Root user account: `root`.
- Non-root user account: `<VA non-root user ID>`. By default: `virtuser`.

The root user has administrator privileges. You use `<VA non-root user ID>` to log on to the guest operating system after the activation process completes. You also use the `<VA non-root user ID>` credential to configure the IMS Server.

The configuration process uses `<VA non-root user ID>` as the administrator credentials for:

- IBM HTTP Server
- WebSphere Application Server
- Tivoli Common Reporting
- IMS Server configuration

Important: If you use directory servers with the IMS Server, do not add `<VA non-root user ID>` to your directory servers. Ensure that the non-root user account does not exist in the directory server.

Note:

- The following tasks apply to configuring and activating the virtual appliance on vSphere Client.
- To navigate the startup console screens for the virtual appliance:
 - Press **Spacebar** to select an option.
 - Press **Enter** to confirm or apply your selection.
 - Press **Tab** to move the focus from one control to another on the page.

Procedure

1. In the vSphere Client, expand the **Virtual Appliance** node; then select the virtual appliance. For example: ISAMESSO_IMS_82.
2. Right-click the virtual appliance; then click **Power on**. The virtual appliance is powered on.
3. Open the console.

Tip: To open the console, on the toolbar, click the **Launch Virtual Machine Console** command.

4. Configure the primary and secondary language settings.
Although the operating system can support additional languages, the installation panels are available only in the languages supported by the WebSphere Application Server Hypervisor Edition.

Tip: To accept the default settings for the primary and secondary languages, press **F10**.

5. Read and accept all license statements and agreements. For example: operating system, VMware, and the IBM WebSphere Application Server.
6. In **Network Configuration**, specify a static or Dynamic Host Configuration Protocol (DHCP) network protocol.
 - If you specified **DHCP**; then enter the following values.

Host name

Specify the host name for the computer. For example: ibm-ss01.

Domain

Specify the domain. For example: example.com.

Net Mask

(Optional) Specify the subnet mask number. For example:
255.255.255.0

- If you specified **Static**; then enter the following values:

IP Address

Specify the static IP address of the computer on the network as assigned by your network administrator.

Net Mask

Specify the subnet mask number. For example: 255.255.255.0

Gateway Address

The IP address of a gateway router.

DNS

Specify the IP address of the primary DNS or name server to resolve network addresses.

Host Name

Specify the host name for the computer. For example: ibm-ss01

Domain

If the computer is part of a domain, specify the domain. For example: `example.com`.

7. Configure the credentials for root and the non-root user accounts.
 - a. Enter a new password for the root user.
 - b. Press **Enter**.
 - c. Type the root user password again.
 - d. Press **Enter**.
 - e. Accept the default non-root user ID or specify a new name. For example: `virtuser`
 - f. Press **Enter**.
 - g. Enter a new password for the non-root user credentials.
 - h. Press **Enter**.
 - i. Type the non-root user password again.

Note: You must provide the non-root user credentials to log on to the guest operating system when the activation process completes.

- j. Press **Enter**.
8. Configure the clock and time zone settings for the host. You can complete the following steps:
 - Press **Enter** to select a region.
 - Press **Tab** to move the focus forward between the panels on the page.
 - Set the time manually or set up the clock to synchronize with a Network Time Protocol (NTP) server.

The regional and clock settings are saved.

9. Select the IBM Security Access Manager for Enterprise Single Sign-On server license type, and press **Enter**.
 - To select IBM Security Access Manager for Enterprise Single Sign-On Standard, press **1**.

This package offers strong authentication, session management, centralized logging, and reporting in addition to single sign-on.
 - To select IBM Security Access Manager for Enterprise Single Sign-On Suite, press **2**.

In addition to the Standard package, this package offers one time password support, AccessAgent plug-ins, Web single sign-on, remote access through Web Workplace, custom tracking, and IAM Integration.
10. Review the IMS Server license agreement and press **Enter** to accept.
11. Optional: Install the Tivoli Common Reporting component.
 - a. In the **Install Tivoli Common Reporting for IMS** menu, select the **Install TCR** option.
 - b. Click **Next**.
 - c. Click **Yes** to confirm.
 - d. Accept the Tivoli Common Reporting license to complete the Tivoli Common Reporting component installation. The server activation process is started.

Note: The installation of Tivoli Common Reporting can take up to one hour.

After the activation process is complete, the logon screen is displayed.

12. In the guest operating system logon screen, log on with the <VA non-root user ID> credentials. For example: virtuser.
 - a. Type the <VA non-root user ID> credentials.
 - b. Specify the <VA non-root user ID> password.
13. Ensure that the network connection to the remote servers can be resolved from the virtual appliance. Test the following connections:
 - Database server
 - Directory server
14. Start the IBM Security Access Manager for Enterprise Single Sign-On IMS configuration wizard.
 - a. On the guest operating system desktop, select the **ISAM ESSO IMS Server Configuration** shortcut.
 - b. Press **Enter**.
 - c. On the security warning prompt, click **I Understand the Risks**.
 - d. Click **Add Exception**.
 - e. Click **Confirm Security Exception**.
15. If you want the database to be created automatically, select the **Create IMS Server database schema** check box.
16. Click **Next**.
17. If you are creating the IMS Server schema automatically, select the database type to create the schema on. For example: DB2.
18. Specify the appropriate options for your environment.

For Microsoft SQL Server

- a. In the **Create new database** page, select the **Create new database** check box.
- b. Click **Next**.

For DB2 and Oracle

Before you begin, ensure that you created the IBM Security Access Manager for Enterprise Single Sign-On database manually on the database server.

19. Specify the database connection configuration.

Host Name

Specify the computer that is hosting the database. For example: `ibm-db.example.com`.

Port

The default port for each database type is already specified. However, if you use custom port numbers for hosted database services, specify the port number.

Database Name

Specify the database name. For example: `imsdb`.

User Name

Specify a database user name with administrator privileges for creating and configuring the database. For example: `db2admin`.

User Password

Specify the database user name password.

20. Click **Next**.

21. When the **Enter IMS Server URL** page is displayed, specify the target URL. Client computers with AccessAgent use the target URL to connect to the IMS Server.
 - For a single-server installation, the virtual appliance host name is pre-filled. For example: `ibm1.example.com`
 - When using a load balancer, specify the fully qualified domain name of the load balancer.
22. Click **Next**.
23. Configure the enterprise directory.
24. Review the settings to be applied.
25. Click **Save** to start the IMS Server and database configuration.

Note: If Tivoli Common Reporting is installed, after the **IMS configured** page is displayed, the Tivoli Common Reporting configuration is started.

26. Restart the WebSphere Application Server after you complete the configuration. You can use the command shortcuts on the desktop to restart the WebSphere Application Server.

Results

You completed the virtual appliance activation and IMS Server configuration process. The IBM Security Access Manager for Enterprise Single Sign-On server is now activated, configured, and ready to use.

What to do next

Click the WebSphere administrative console shortcut on the desktop to open the administrative console. Log on with the non-root user name and password. See the following tasks:

- “Provisioning the IMS Server administrator” on page 71
- “Verifying the IMS Server configuration” on page 73

Virtual appliance replication for high availability

You can set up multiple virtual appliance replicas for a high availability virtual appliance deployment.

Before you begin

- You must have at least two virtual appliances. For example: `VA_1` and `VA_2`.

Where:

VA_1 Specifies a source host with an activated and configured instance of the IMS Server virtual appliance.

VA_2 Specifies the target replica with an activated instance of the IMS Server virtual appliance.

- Ensure that any remote servers in your deployment, such as directory servers or databases servers, can be resolved either by DNS or the hosts file.

About this task

You can achieve high availability by setting up two or more virtual appliance replicas with the *Export and Import configuration tool*. When using the virtual

appliance IMS Server in a replicated configuration, you must synchronize any IMS Server configuration changes manually between the servers.

When any of the following changes occur between VA_1 and VA_2:	You must do the following tasks:
<ul style="list-style-type: none"> • IMS Server configuration changes: 	<ol style="list-style-type: none"> 1. Export the IMS Server configuration from VA_1. 2. Import the changed IMS Server configuration again in VA_2.

The IMS Server configuration changes include:

- JDBC settings.
- IMS Server certificates. For example: IMS Server keys, certificates and the WebSphere Application Server root CA key.
- IBM HTTP Server certificates.
- Configuration files in the configuration repository: `<profile_root>/config/tamesso`.
- IMS Server SOAP service URL.
- Virtual Member Manager enterprise directory configurations.

The following elements are not exported by the IMS Server *Export and Import configuration tool*:

- Manual configuration changes to the profile: For example: heap size values, session management overrides.

With the *Export and Import configuration tool*, you can back up an existing working IMS Server configuration. Use the configuration you back up for additional IMS Server replicas that you want to deploy.

See the following considerations:

- The *Export and Import configuration tool* does not import Tivoli Common Reporting configurations. If you want to replicate the Tivoli Common Reporting configuration from VA_1 to VA_2, manually install and configure Tivoli Common Reporting in VA_2.
- The *Export and Import configuration tool* only exports IMS Server configurations. It does not import or export WebSphere Application Server specific configuration changes.

The following steps outline the tasks to set up a high availability virtual appliance deployment. Repeat the steps depending on the number of virtual appliance replicas you plan to set up.

For the detailed procedures on exporting and importing the IMS Server configuration, see the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

Procedure

1. Deploy the virtual appliance VA_1.
2. Activate and configure the virtual appliance VA_1.
3. Repeat the following steps for each replica:
 - a. Deploy the virtual appliance VA_2.

- b. Activate the virtual appliance *VA_2*.
 - c. Log on to *VA_2* with the non-root user account, *<VA non-root user ID>*. For example: *virtuser*.
 - d. From *VA_2*, log on to *VA_1* IMS Configuration Utility. For example:
https://VA_1:9043/webconf
 - e. Export the IMS Server configuration.
 - f. From *VA_2*, log on to *VA_2* IMS Configuration Utility. For example:
https://VA_2:9043/webconf.
 - g. Import the IMS Server configuration.
4. Set up the load balancer.
 5. If the IMS Server configuration is changed, export and import the configuration again.

Chapter 4. Setting up a stand-alone production server

Set up a stand-alone production environment when you do not need a robust clustered environment. A stand-alone production deployment is typically used by smaller to medium sized sites. A stand-alone server deployment can be deployed in demonstration or production configurations.

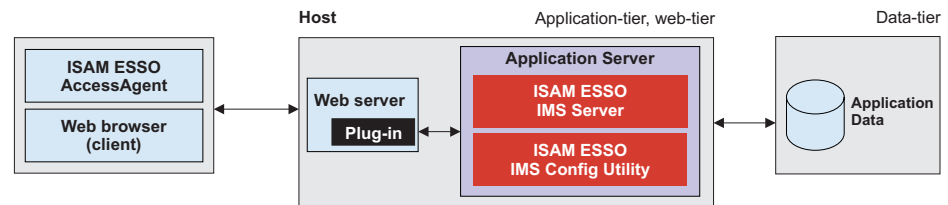


Figure 2. Stand-alone production server installation

For more information about planning and deployment considerations when setting up a stand-alone production server, see the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

Road map

These steps are only an example of how you can prepare a middleware environment for new installations. Install and prepare the following middleware before you run the IMS Server installation:

1. Prepare the database server.
2. Prepare WebSphere Application Server.
3. Prepare IBM HTTP Server.
4. Prepare the directory server.
5. Optional: Install the Tivoli Common Reporting component.

You must prepare the following middleware components for use with the IBM Security Access Manager for Enterprise Single Sign-On:

Database server

The database server hosts single sign-on user identities and Wallets. You can install a new instance of a database server or use an existing instance.

WebSphere Application Server

The WebSphere Application Server provides a centralized application administration platform that extends the ability of a web server to handle web application requests. The IBM Security Access Manager for Enterprise Single Sign-On IMS Server is a WebSphere application. To use an existing application server, you must install and configure it manually.

IBM HTTP Server

The IBM HTTP Server is a separate, dedicated web server that is configured to work with the application server.

Tivoli Common Reporting

Tivoli Common Reporting is an optional component. Tivoli Common Reporting is an integrated reporting solution that lets you link multiple reports across various Tivoli products and simplify report navigation and access.

Directory server

A directory server or LDAP repository authenticates a user and retrieves information about users and groups to perform security-related functions, including authentication and authorization. You can install a new instance of a directory server, or reuse an existing instance.

If you are reusing existing middleware that was previously deployed, apply the minimum supported fix packs before installing the IBM Security Access Manager for Enterprise Single Sign-On server.

Creating and choosing profiles for stand-alone server deployments

A WebSphere Application Server profile defines the runtime environment.

Using profiles, you can define different types of WebSphere Application Server environments on a single system without having to install multiple copies of the WebSphere Application Server.

For a single-server or stand-alone environment, create a stand-alone application server profile.

Note: There is no graphical Profile Management tool to create profiles for 64-bit platforms. Use the `manageprofiles` command. For 64-bit platforms, see “Creating stand-alone profiles (command-line) for x86 or x64 architectures” on page 54.

The port numbers and settings for each profile you create is always recorded in the `AboutThisProfile.txt` file. The file is stored in `<was_home>/profiles/<profile_name>/logs`. This file is helpful when you must determine the correct port number for a profile.

Stand-alone profiles

For single-server or stand-alone environments, use the stand-alone application server profile.

Important: The administrative user name that you supply for the WebSphere administrator must not exist on the directory server. For example, if the WebSphere administrator you provide is `wasadmin`, then the user `wasadmin` must not exist on the corporate enterprise directory. Avoid the use of “administrator” as the WebSphere Application Server administrator. Choose a user name that is least likely to conflict with your potential existing enterprise directory users.

To create a profile, use either of the following methods:

- “Creating stand-alone profiles (Profile Management tool) for x86 architectures” on page 53
- “Creating stand-alone profiles (command-line) for x86 or x64 architectures” on page 54

Creating stand-alone profiles (Profile Management tool) for x86 architectures

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

Before you begin

- Log on to the system as a user with administrator privileges.
- Prepare the WebSphere Application Server.
- Install the WebSphere Application Server fix packs.

About this task

For complete information about creating profiles, see the WebSphere Application Server documentation.

Procedure

1. Open the Profile Management Tool. For example: Click **Start > All Programs > IBM WebSphere > Application Server Network Deployment V7.0 > Profile Management Tool**.
2. On the **Welcome to the Profile Management Tool** panel, review the information.
3. Click **Launch Profile Management Tool**.
4. On the **Profiles** panel, click **Create** to create a profile.
5. On the **Environment Selection** panel, click **Application server**.
6. Click **Next**.
7. Click **Typical Profile Creation**.
8. Click **Next**.
9. Type the WebSphere administrator user name and password. For example: wasadmin.

Important: The administrative user name that you supply for the WebSphere administrator must not exist on any of the directory servers that you plan to configure. For example, if the WebSphere administrator you provide is wasadmin, then the user wasadmin must not exist on any of the enterprise directories. Avoid the use of “administrator” as the WebSphere Application Server administrator. Choose a user name that is least likely to conflict with your potential existing enterprise directory users.

10. Click **Next**.

Note: On the **Profile Creation Summary** page, you can record the server name, host name, and port numbers to be used. A Windows service is also created automatically for the server.

11. Click **Create** to start creating the server profile.
12. After the profile creation, ensure that the **Launch the First Steps console** check box is selected.
13. Click **Finish** to start the **First Steps** console.

Tip: If the wizard does not start automatically, click **All Programs > IBM WebSphere > Application Server Network Deployment V7.0 > Profiles > <AppSrv01> > First steps**.

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

```
ADMU3200I: Server launched. Waiting for initialization status.  
ADMU3000I: Server server1 open for e-business; process id is 236
```

Results

You created and verified that the stand-alone application server profile is working. The stand-alone server is running.

What to do next

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

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

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

Creating stand-alone profiles (command-line) for x86 or x64 architectures

Use the **manageprofiles** command to create profiles for stand-alone product deployments from the command line.

Before you begin

- Log on to the system as a user with administrator privileges.
- Prepare the WebSphere Application Server.
- Install the WebSphere Application Server fix packs.

About this task

For 64-bit WebSphere Application Server 7.0, use the **manageprofiles** command to create profiles because the Profile Management tool is not available for 64-bit systems.

The command-line parameters included in this task uses the same profile creation parameters to create the profiles in the Profile Management tool. The **manageprofiles** command is in the `<was_home>\bin` directory.

Procedure

- Open the command prompt.
- Use the **manageprofiles** command to create profiles for stand-alone product deployment.

See the following example (use without line-breaks, case-sensitive):

Command line with parameters (case-sensitive, use without line breaks)	Example with sample values
<pre><was_home>\bin\manageprofiles.bat -create -profileName <profile_name> -profilePath "<was_home>\profiles\<profile_directory>" -templatePath "<was_home>\profileTemplates\default" -enableAdminSecurity true -adminUserName <WAS Admin user ID> -adminPassword <password> -winserviceAccountType localsystem -winserviceCheck true -winserviceStartupType automatic -omitAction samplesInstallAndConfig</pre>	<pre>"c:\Program Files\IBM\WebSphere\AppServer\bin\ manageprofiles.bat" -create -profileName AppSrv01 -profilePath "c:\Program Files\IBM\WebSphere\AppServer\ profiles\AppSrv01" -templatePath "c:\Program Files\IBM\WebSphere\AppServer\profileTemplates\default" -enableAdminSecurity true -adminUserName wasadmin -adminPassword password -winserviceAccountType localsystem -winserviceCheck true -winserviceStartupType automatic -omitAction samplesInstallAndConfig</pre>

The example creates a stand-alone application server profile and excludes sample applications. The **winserviceCheck** creates a Windows service. If the host restarts, the Windows service runs under a local system user account and starts automatically.

- To verify the installation, start the First Steps wizard. For example: Click **Start > All Programs > IBM WebSphere > Application Server 7.0 > Profiles > profile_name > First steps**.

Results

You created a stand-alone application server profile for a stand-alone WebSphere Application Server deployment. You verified that the application server profile started successfully.

What to do next

You are ready to configure the WebSphere Application Server. See “Configuring the WebSphere Application Server.”

Configuring the WebSphere Application Server

You must configure the WebSphere Application Server stand-alone environment before you install the IMS Server.

About this task

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

Complete the following steps for both optional or required configurations before you install the IMS Server.

- Secure the WebSphere Application Server deployment.
 - Optional: Recreate the root CA key size.

If your deployment includes specific minimum key size or high security requirements, you can increase the default root CA key size from 1024 bits to 2048 bits.
- Configure the JVM heap size memory.
- Verify the Windows services for WebSphere Application Server.

Configuring the heap size for the application server

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

Before you begin

Before you modify the Java heap size, ensure that the host has enough physical memory to support a JVM of 3.0 GB without swapping. If the physical memory of the host system exceeds 3 GB, you can increase the maximum heap size. However, if the heap size is too large, the system does not have enough physical memory and starts allocating virtual memory to hold the data.

About this task

Adjust the Java heap size with the following guidelines before installing the IBM Security Access Manager for Enterprise Single Sign-On IMS Server component. To learn more, see the WebSphere Application Server information center (<https://www-01.ibm.com/software/webservers/appserv/was/library/v70/>) and search for *Java virtual machine settings heap tuning*.

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

Procedure

1. On the WebSphere Application Server host, where you are installing the IMS Server, log on to the administrative console. For example: `https://localhost:9043/ibm/console/`.
2. Navigate to the Java virtual machine settings.
 - a. Expand **Servers > Server Types** and select **WebSphere application servers**.
 - b. Click the name of your server. For example: **server1**.
 - c. Under the **Server Infrastructure** group, click to expand **Java and Process Management**.
 - d. Click **Process Definition**.
 - e. Under the **Additional Properties** group, click **Java Virtual Machine**.
3. Use the following settings (for a single server instance, 3 GB host):
 - **Initial Heap Size:** 1024
 - **Maximum Heap Size:** 1280
4. Click **OK**.
5. In the messages box, click **Save**.
6. Click **OK**.
7. In the messages box, click **Save**.
8. Restart the WebSphere Application Server.

Verifying the Windows service for WebSphere Application Server

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

Procedure

1. Open the Windows Services management console.
 - a. Click **Start > Run**.

- b. Type `services.msc`.
2. Verify that the service IBM WebSphere Application Server v7.0 - `<node_name>` is displayed in the list of services. For example: IBM WebSphere Application Server v7.0 - `ibm-svr1Node01`.

Results

You successfully verified that a Windows server service exists for the WebSphere Application Server process.

Recreating the root CA for WebSphere Application Server 7.0 (stand-alone)

The WebSphere Application Server root CA has a default 1024 bit key size. Change the root CA key size to a larger 2048 bit key size to offer an increased level of security. This task is optional.

Before you begin

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

About this task

This optional task applies only to new installations of the IMS Server. If you choose to change your root CA key size to 2048 bit, complete these steps before you run the IMS Configuration Wizard. The root CA certificate signs the default certificates in the key store. The certificates secure internal WebSphere Application Server communications.

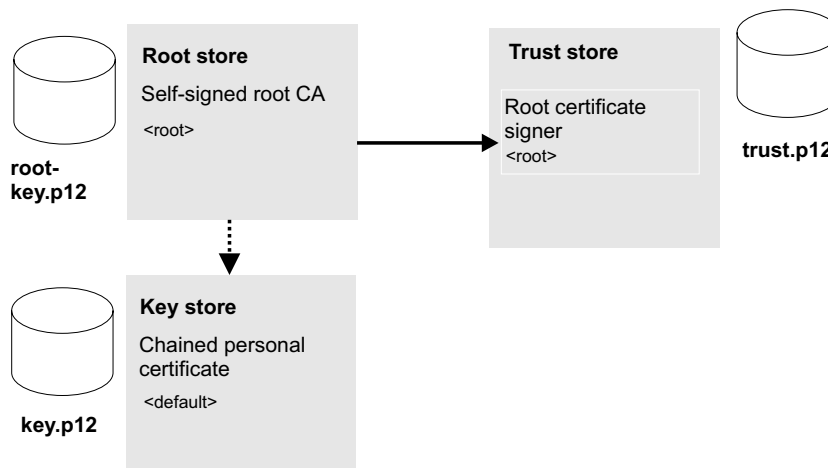


Figure 3. Replacing the root CA and key signers for WebSphere Application Server in the truststore with a new key size.

The process involves the following steps:

1. Create a 2048 bit self-signed root CA in the root store, replace the existing version, and extract it. See step 1 on page 58 to step 8 on page 59.
2. Create a 2048 bit chained personal certificate in the key store, and replace the existing version. See step 10 on page 59.
3. Export the personal certificate to the truststore. See step 11 on page 60.

4. Use the **ikeman** utility to add the root CA to the truststore. See step 12 on page 60.

Procedure

1. Select **Start > All Programs > IBM WebSphere > Application Server <version> > Profiles > <profile name> > Administrative console**.
2. Log on to the IBM Integrated Solutions Console.
3. On the Integrated Solutions Console navigation pane, select **Security > SSL certificate and key management**.
4. In **Related items**, click **Key stores and certificates**.
5. Create a temporary self-signed root CA in the default root store.
The temporary root certificate is used to replace the older root certificate. The temporary root certificate is then replaced with a new 2048 bit root certificate.
 - a. From the **Keystore usages** list, select **Root certificates keystore**.
 - b. Click **NodeDefaultRootStore**.
 - c. Under **Additional Properties**, click **Personal certificates**.
 - d. Click **Create > Self-signed Certificate**.
 - e. In **Alias**, enter a new alias name. For example: root2.
 - f. In the **Common name** field, enter the fully qualified domain name of the computer where the WebSphere Application Server is installed. For example: ibm-svr1.example.com.
 - g. Click **OK**.
 - h. Click **Save**.
6. Replace the old root CA with the new root CA: root2. Replace the old root with the temporary root2.
 - a. In the **Personal Certificates** page, select the check box for the older root certificate, root.
 - b. Click **Replace**.
 - c. From the **Replace with** list, choose the alias of the certificate you created.
 - d. Select **Delete old certificate after replacement**.
See the WebSphere Application Server information center on replacing a certificate for details:
http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/tsec_sslreplaceselfsigncert.html
 - e. Ensure that the **Delete old signer** check box is not selected.
 - f. Click **OK**.
 - g. Click **Save** to apply the changes to the master configuration.
7. Create the 2048 bit root CA. This root certificate is the 2048 bit certificate that you retain.
 - a. Click **Create > Self-signed Certificate**.
 - b. In **Alias**, enter root.

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

- e. In the **Validity period** field, enter the validity period of the certificate. For example: A root certificate is typically used for 7300 days, which is approximately 20 years.
 - f. Optional: Complete the certificate with optional identification details.
 - g. Click **OK**.
 - h. Click **Save** to apply the changes to the master configuration.
8. Replace the temporary root certificate with the new 2048 bit root certificate that you retain.
- a. In the **Personal Certificates** page, select the check box for the temporary root certificate, root2.
 - b. Click **Replace**.
 - c. From the **Replace with** list, choose the new 2048 root certificate you created, root.
 - d. Select **Delete old certificate after replacement**.
 - e. Ensure that the **Delete old signer** check box is not selected.

Important: Ensure that the **Delete old signer** check box is not selected.

- f. Click **OK**.
- g. Click **Save** to apply the changes to the master configuration.

You successfully replaced the original 1024 bit root certificate with a new 2048 bit root certificate.

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

Important: Before you begin, be sure to check that your host names are resolving correctly.

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

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

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

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

- l. Optional: Enter information in the rest of the optional fields.
- m. Click **OK**.
- n. Click **Save** to apply the changes to the master configuration.
- o. Replace the old default personal certificate with the new one.
 - 1) In the **Personal Certificates** page, select the **default** check box.
 - 2) Click **Replace**.
 - 3) From the **Replace with** list, choose the alias of the certificate you created. For example: default2.
 - 4) Select **Delete old certificate after replacement**.

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

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

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

- 11. Export the personal certificate to the keystore: <was_home>\profiles\
<profile_name>\etc\key.p12.
 - a. In the **Personal Certificates** page, select the personal certificate check box. For example: default2.
 - b. Click **Export**.
 - c. In **Key store password**, enter the key store password For example: WebAS.

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

- d. Select **Key store file**.
- e. In **Key store file**, specify the key store location. For example:
<was_home>\profiles\
<profile_name>\etc\key.p12.
- f. For **Type**, verify that the default **PKCS12** is selected.
- g. In **Key file password**, type the password. For example: WebAS.
- h. Click **OK**.

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

- 12. Use the IBM Key Management utility, *ikeyman*, to add the extracted root CA to the truststore.
 - a. Start the **ikeyman** utility. Locate the utility in <was_home>\profiles\
<profile_name>\bin\ikeyman.bat.
 - b. Open the truststore. Click **Key Database File > Open**. In **Key database type**, select **PKCS12**.
 - c. Click **Browse** to locate the truststore. You can locate the truststore in <was_home>\profiles\
<profile_name>\etc\trust.p12

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

The root CA is added to the truststore and saved.

13. Stop and start the server.

Results

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

What to do next

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

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

Be sure to update the Planning worksheet with the new aliases you used for the root and default certificate aliases. You must specify the aliases later when you choose to set up a new IMS Server in the IMS Configuration Wizard. See Appendix A, "Planning worksheet," on page 163

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

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

Before you begin

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

- Review the planning worksheet for the configuration settings. See Appendix A, “Planning worksheet,” on page 163.

About this task

Configuring IBM HTTP Server is a three-stage process.

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

Procedure

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

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

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

Tip: To learn more about each field, on the page, see the field descriptions in the **Help** pane.

For guidance, consider the following notes:

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

Tip: The Server name is not the web server host name.

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

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

- a. From `<ihs_home>\Plugins\bin`, on the IBM HTTP Server host, copy the `configure<web_server_definition_name>.bat` file. For example: `configurewebserver1.bat`.
- b. On the application server, paste the `configure<web_server_definition_name>.bat` file to the `<was_home>\bin` folder. For example: `C:\Program Files\IBM\WebSphere\AppServer\bin`

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

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

For example:

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

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

Configuration save is complete.

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

2. In the WebSphere administrative console, click **Servers > Server Types > Web servers**. Verify that the web server definition is displayed. For example: **webserver1**.
3. Grant remote server management rights to the WebSphere Application Server administrator by supplying the IBM HTTP Server administrator account.
 - a. In the administrator console, click **Servers > Server Types > Web servers**.
 - b. Click the **<Web_server_name>**. For example: **webserver1**.
 - c. In the **Additional Properties** section on the **Configuration** tab, click **Remote Web Server Management**.
 - d. Enter the IBM HTTP Server administration server authentication user ID and password. For example: **ihsadmin**.
 - e. Clear the **Use SSL** check box.
 - f. Click **OK**.
 - g. In the **Messages** box, click **Save**.
4. (Complete this step only if the IBM HTTP Server and WebSphere Application Server are not on the same computer; or if you are using a load balancer.) Set up the SSL certificates signed by the WebSphere Application Server certificate authority.

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

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

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

- g. In the **Common Name** field, you can enter one of the following names:
 - The fully qualified domain name of the computer where the IBM HTTP Server is installed. For example: `webserver1.example.com`.
 - The fully qualified host name of the load balancer if a load balancer is used.
- h. Optional: Enter the remaining optional information.
- i. Click **OK**.
- j. In the **Messages** box, click **Save**.
- k. If you have more than one IBM HTTP Server, for each IBM HTTP Server, repeat steps a to j.

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

5. Synchronize the WebSphere Application Server keystore with the IBM HTTP Server keystore.
 - a. On the IBM Integrated Solutions Console navigation pane, click **Servers > Server Types > Web servers**.
 - b. Click the `<Web server name>`. For example: `webserver1`.
 - c. In the **Additional Properties** section on the **Configuration** tab, click **Plug-in properties**.
 - d. Click **Copy to Web Server key store directory**.
 - e. Click **OK**.
 - f. In the **Messages** box, click **Save**.

Results

You defined a web server in the WebSphere Application Server configuration. The web server routes requests received from client workstations to the application server.

Enabling SSL directives on the IBM HTTP Server

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

About this task

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

Complete this procedure for every web server.

Procedure

1. On the IBM Integrated Solutions Console, click **Servers > Server Types > Web servers**.
2. Click the `<Web server name>`. For example: `webserver1`
3. In the **Additional Properties** section on the **Configuration** tab, click **Configuration File**.

If the configuration file fails to open, see the *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide*.

4. Add the following lines to the end of the configuration file:

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 0.0.0.0:443
## IPv6 support:
```



```
#Listen [::]:443
<VirtualHost *:443>
    SSLEnable
    SSLProtocolDisable SSLv2
SSLServerCert default
</VirtualHost>
KeyFile "<ihs_home>\Plugins\config\<web_server_definition>\plugin-key.kdb"
SSLDisable
```

where

default

Specifies the alias of the default SSL certificate.

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

- a. In the IBM Integrated Solutions Console navigation pane, click **Security > SSL certificate and key management**.
- b. Under **Related Items**, click **Key stores and certificates**.
- c. Click **CMSKeyStore**.
- d. Under **Additional Properties**, click **Personal certificates**.

<ihs_home>\Plugins\config\<web_server_definition>\plugin-key.kdb

Specifies the path to the plug-in key store file plugin-key.kdb.

For example: C:\Program Files\IBM\HTTPServer\Plugins\config\webserv1\plugin-key.kdb.

5. Click **Apply**.
6. Click **OK**.
7. Select **General Properties > Apply**.
8. In the **Messages** box, click **Save**.
9. Restart the IBM HTTP Server.
 - a. On the IBM Integrated Solutions Console, click **Servers > Server Types > Web servers**.
 - b. Select the check box of the corresponding web server. For example: webserv1.
 - c. Click **Stop**.
 - d. Select the check box for the web server again.
 - e. Click **Start**.
10. Verify that the SSL directives are enabled correctly. Type the following https address in a web browser. For example:
 - https://<ihs_host>

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

A web browser security prompt might display because you are accessing a page over the secure https protocol. Follow the instructions in the dialog box to accept the security certificate and continue to the page.

 - http://<ihs_host>

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

You can also verify that pages over non-https protocol are still accessible.

Tip: If the verification fails, check whether the custom variables you specified in step 4 on page 64 are added and replaced correctly. For additional troubleshooting tips, see the *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide*.

Results

You enabled SSL on the IBM HTTP Server. You also verified pages over the secure https protocol.

Recreating the SSL certificate for the IBM HTTP Server

You can recreate the SSL certificate to increase the SSL certificate key size for the IBM HTTP Server, from 1024 bits to 2048 bits. This task is optional.

Before you begin

Ensure that the WebSphere Application Server root CA is already upgraded to 2048 bits. See one of the following topics:

- For WebSphere Application Server in a stand-alone deployment, see “Recreating the root CA for WebSphere Application Server 7.0 (stand-alone)” on page 57
- For WebSphere Application Server in a cluster, see “Recreating the root CA for WebSphere Application Server 7.0 on the deployment manager before creating member nodes” on page 83

About this task

This task is optional and applicable only for new installations of the IMS Server. If you must upgrade the default SSL certificate for IBM HTTP Server to 2048 bits, complete this task before you install the IMS Server.

If you are using multiple web servers, perform the following steps on each **CMSKeyStore** in the administrative console.

Procedure

1. Select **Start > All Programs > IBM WebSphere > Application Server <version> > Profiles > <profile name> > Administrative console.**
2. Log on to the IBM Integrated Solutions Console.
3. On the Integrated Solutions Console navigation pane, select **Security > SSL certificate and key management.**
4. Under **Related items**, click **Key stores and certificates.**
5. Click **CMSKeyStore.**
6. Under **Additional Properties**, click **Personal certificates.**
7. Select the certificate named **default.**
8. Click **Delete.**
9. Click **Create > Chained Certificate.**
10. In the **Alias** field, enter a new alias name. For example: default.
11. From the **Root certificate used to sign the certificate** list, select the alias of the newly created Root CA. For example: root
12. From the **Key size** list, select **2048.**
13. In the **Common Name** field, use one of the following entries:
 - If you are not using a load balancer, specify the fully qualified name of the host where IBM HTTP Server is installed. For example: httpsvr1.example.com.
 - If you are using a load balancer, specify the fully qualified name of the load balancer.

Note: You must provide a **Common Name**.

14. In the **Validity period** field, enter the validity period of the certificate. For example: 365 days.
15. Optional: Enter the information in the following fields:
 - Organization
 - Organization Unit
 - Locality
 - State/Province
 - Zip Code
 - Country or Region
16. Click **OK**.
17. In the **Messages** box, click **Save**.
18. Synchronize the WebSphere Application Server keystore with the IBM HTTP Server keystore.
 - a. On the IBM Integrated Solutions Console navigation pane, click **Servers > Server Types > Web servers**.
 - b. Click the *<Web server name>*. For example: *webserv1*.
 - c. In the **Additional Properties** section on the **Configuration** tab, click **Plug-in properties**.
 - d. Click **Copy to Web Server key store directory**.
 - e. Click **OK**.
 - f. In the **Messages** box, click **Save**.
19. Resynchronize the nodes.
 - a. Click **System administration > Nodes**.
 - b. Select the check box for each corresponding node.
 - c. Click **Full Resynchronize**.
20. Restart the IBM HTTP Server.

Configuring the IMS Server for a stand-alone deployment

You can install the IMS Server by using the IMS Server installer or by deploying the IMS Server Enterprise Archive (EAR) files manually on WebSphere.

1. Review the release notes.
2. Extract and install the IMS Server. Choose one of the following methods:
 - Install the IMS Server interactively with the installer.
 - Deploy the IMS Server on WebSphere Application Server manually.
3. Verify the IMS Server deployment.
4. Set up and configure the IMS Server.
 - With the IMS Configuration Wizard, set up the data source, certificates, target URL, and directory services.
 - Provision an IMS Server administrator.

You can use the IMS Server administrator credentials to access and administer single sign-on resources.
5. Update the application mappings for the ISAMESSOIMS application.

Mapping ensures that all client connection requests from the web-tier or load balancer front end are forwarded correctly to the WebSphere Application Server and the IMS Server application.

6. Verify the IMS Server configuration.

Configuring the IMS Server for a new installation with the IMS Configuration Wizard (stand-alone)

Configure the IMS Server to complete the IMS Server installation.

Before you begin

- Ensure that the WebSphere Application Server is started.
- Ensure that the IMS Server applications have the following status:
 - ISAMESSOIMSConfig is started.
 - ISAMESSOIMS is stopped.
- Prepare the directory server.
- Prepare the database server.
- Review the planning worksheet for sample values. See Appendix A, “Planning worksheet,” on page 163.

About this task

To configure the IMS Server, the IMS Configuration Wizard helps you accomplish the following tasks:

1. Set up the data sources.
2. Update certificates.
3. Set up the IMS Server URL.
4. Configure the IMS Server for directory servers.

WebSphere Application Server fix packs 15 and 17 might have connectivity problems with Oracle. Install the interim fix before running the IMS Configuration Wizard. See <http://www-01.ibm.com/support/docview.wss?uid=swg24029891>

Procedure

1. Open the IMS Configuration Wizard. The URL is in the following form:
`https://<dmgr_hostname>:<admin_ssl_port>/front`
For example: `https://localhost:9043/front`.
2. To switch to another language in the IMS Configuration Wizard, choose your preferred language in the **Language** menu.
3. In the **Server Set Up** page, select **Set up a new IMS Server**.
4. Click **Begin**.
5. In **Enter data source information**, accept the default values or customize the fields for the data source.
6. Click **Next**.
7. To use the default option to create a database schema by using the IMS Configuration Wizard, ensure that the **Create IMS Server database schema** check box is selected.

Note: Alternatively, you can create the database schema manually. See Appendix B, “Creating database schemas,” on page 175.

8. Click **Next**.
9. Select the IMS Server database type.

Note: If you are using a Microsoft SQL Server database, you have the following choices:

- Default: Create a database with the configuration wizard. Select **Create new database**.
- Use an existing database. Clear the **Create new database** check box. Click **Next**.

10. Click **Next**.

11. In **Database Configuration - <database type>**, specify the connection information about the database type. Follow the instructions in the wizard to specify the database connection details. The database type you select might include a different set of fields. See the help descriptions on the page for guidance.

Tip: To see additional help for each item, move the cursor over each item. The following fields are specific to DB2. You can use the following descriptions for additional guidance:

Host Name

Specify the database host name. For example: mydbsvr.

Port

The database connection port number is pre-filled. Verify whether the default port value is correct.

For example:

- The default value for DB2 is 50000.
- The default value for SQL Server is 1433.
- The default value for Oracle is 1521.

Note: To determine the correct database connection port numbers, see your database vendor documentation on how to determine the correct values for your database server.

Database name

Specify the name of the database. For example: imsdB.

User name

Specify the database user you prepared. For example: db2admin.

User password

Specify the password for the database user.

12. Click **Next**.

13. In **Provide Root CA Details**, verify the default values.

Verify the keystore name, keystore password, and certificate alias of the Root CA used to sign the IMS Server intermediate CA.

Important: If you recreated or upgraded the key size for the root CA, the root CA alias name might change. Be sure to specify the correct alias. See the following descriptions for guidance:

Tip: Use the Planning Worksheet to verify the custom values you used. See Appendix A, "Planning worksheet," on page 163.

Keystore name

Specifies the name of the root key store. The root key store is a key

database that contains both public and private keys for secure communication. Typically, you can use the default value.

Keystore scope

Specifies the level at which the keystore is visible at the cell or node level. Typically, you can use the default value.

Keystore password

Specifies the password for the root certificate keystore. Typically, you can use the default value.

Root CA alias name

Accept the default value for the root alias unless the root CA alias has been modified.

14. Click **Next**. The certificate credentials for the keystore and root alias are verified.
15. In **Configure IMS Services URL**, specify the IBM HTTP Server or load balancer name and port number or accept the default values.

Note: The IBM HTTP Server or load balancer name:

- Is the fully qualified name of the IBM HTTP Server or load balancer that interfaces with the WebSphere Application Server.
- Must match the **CN** attribute of the SSL certificate used by the IBM HTTP Server.

16. Click **Next**.
17. Configure the IMS Server to work with a directory server.

Note:

- To configure directory servers later, be sure to complete the directory server setup before you use the IMS Configuration Utility.
- If you are planning to use a directory server, configure the IMS Server to work with a directory server before you provision an IMS Server administrator account.

18. Click **Next**.
19. Review the settings.
20. Click **Save**.
21. To complete the IMS Server configuration, do one of the following options:

Option	Description
If you configured enterprise directories:	(Network deployment) Restart the deployment manager node. (Stand-alone deployment) Restart the application server.
If you did not configure any enterprise directories:	Restart the ISAMESSOIMSConfig.

Results

You successfully set up the IMS Server.

What to do next

If you configured the enterprise directory, you can provision the IMS Server administrator account.

If you have not yet configured the enterprise directory, do it through the IMS Configuration Utility.

Provisioning the IMS Server administrator

For new installations, you can provision an administrator account for the IMS Server.

Before you begin

- Ensure that the deployment manager is started.
- Ensure that the ISAMESSOIMSConfig is started.
- Ensure that the cluster is stopped.
- Prepare the directory server.
 - If your deployment requires you to use a directory server with the IMS Server, configure the directory server first. See *Configure the IMS Server for directory servers*.
 - Ensure that the user names for the IMS Server administrator or the WebSphere administrator are unique and do not exist on the directory server where you are provisioning the account.
 - On the Active Directory or LDAP server, create an IMS Server administrator account. For example: `imsadmin`.
 - Start the directory server and ensure that it is available.

About this task

Considerations when provisioning an administrator:

When enterprise directories are not configured

The provisioned IMS Server administrator account is created and stored in the IMS Server database. When you log on with the IMS Server administrator credentials, the credentials are authenticated against the IMS Server database. This account in the database is also known as a base connector user account.

When enterprise directories are configured

The provisioned IMS Server administrator account is synchronized and authenticated with a similar account in the enterprise directory.

Procedure

1. In a browser, start the IMS Configuration Utility. For example: type `https://localhost:9043/webconf`.
2. Log on with the WebSphere administrator credentials.
3. In the Configuration Wizards area, click **Provision IMS Administrator**.
4. Type the credentials of a valid user for the IMS Server administrator you want to provision. For example: `imsadmin`.

If you are using a directory server, type the credentials for a valid enterprise directory user. If you did not create a specific IMS Server administrator, you can specify any existing user on the directory server.

Note: If there are multiple enterprise directories, select the domain where the user exists.

Results

You provisioned an IMS Server administrator account.

What to do next

Continue with additional IMS Server post-installation configuration. Update the application mappings for the ISAMESSOIMS application.

Updating the ISAMESSOIMS module mapping for connection request forwarding

Update the application mappings for ISAMESSOIMS to the web-tier and application-tier hosts with the new IMS Server application mappings.

Before you begin

Ensure that the following components and applications are started:

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

Ensure that the following components and applications are stopped:

- ISAMESSOIMS
- IBM HTTP Server
- Cluster

About this task

You must map the ISAMESSOIMS application to the web-tier and application-tier hosts after installing the IMS Server with the IMS Server installer. You must update the ISAMESSOIMS application mappings manually if you are adding additional nodes to a cluster.

Procedure

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

Tip: To select multiple servers, press the **Shift** key and click to select multiple web servers and application servers.

6. Click **Apply**.
7. Click **OK**.

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

Results

The IMS Server application URLs connection requests are now forwarded correctly by the IBM HTTP Server to the ISAMESSOIMS application.

Verifying the IMS Server configuration

Verify that the IMS Server installation and configuration are working.

Before you begin

Ensure that the following applications and components are started:

- ISAMESSOIMS
- ISAMESSOIMSConfig
- WebSphere Application Server
- IBM HTTP Server
- Database servers
- Directory servers

Procedure

1. Verify that you can access AccessAdmin.
 - a. In a browser, go to the AccessAdmin URL. For example:
 - `https://<ihs_host>/admin`
 - `https://<loadbalancer_host>/admin`
 - b. Log on to AccessAdmin with the IMS Server administrator account you provisioned. For example: `imsadmin`.
 - c. Click **Setup assistant**.
 - d. You can review the instructions to configure authentication factors at a later time. Close the browser. You successfully verified that you have access to AccessAdmin.
2. Verify that you can access Web Workplace.
 - a. In a browser, go to the Web Workplace URL. For example:
 - `https://<ihs_host>/aawwp?isWwp=true`
 - `https://<loadbalancer_host>/aawwp?isWwp=true`
 - b. Log on to Web Workplace with the IMS Server administrator account that you provisioned. For example: `imsadmin`.
3. Verify that you can access AccessAssistant.
 - a. In a browser, go to the AccessAssistant URL. For example:
 - `https://<ihs_host>/aawwp`
 - `https://<loadbalancer_host>/aawwp`
 - b. Log on to AccessAssistant with the IMS Server administrator account that you provisioned. For example: `imsadmin`.

Results

You successfully installed the IMS Server and ensured that it works. You also verified that the URL to access the administration components work.

What to do next

To perform additional server configurations specific to your deployment, such as adding authentication factors, see the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

You can now install the AccessAgent or AccessStudio clients on client workstations.

Tip: To save time and simplify access, bookmark the administrative URLs in your web browser.

Chapter 5. Setting up a cluster (network deployment)

Clusters enable you to scale your IBM Security Access Manager for Enterprise Single Sign-On configuration. Clusters enable enterprise applications to be highly available because requests are automatically routed to the running servers in the event of a failure. A clustered deployment is typically used in enterprise production environments.

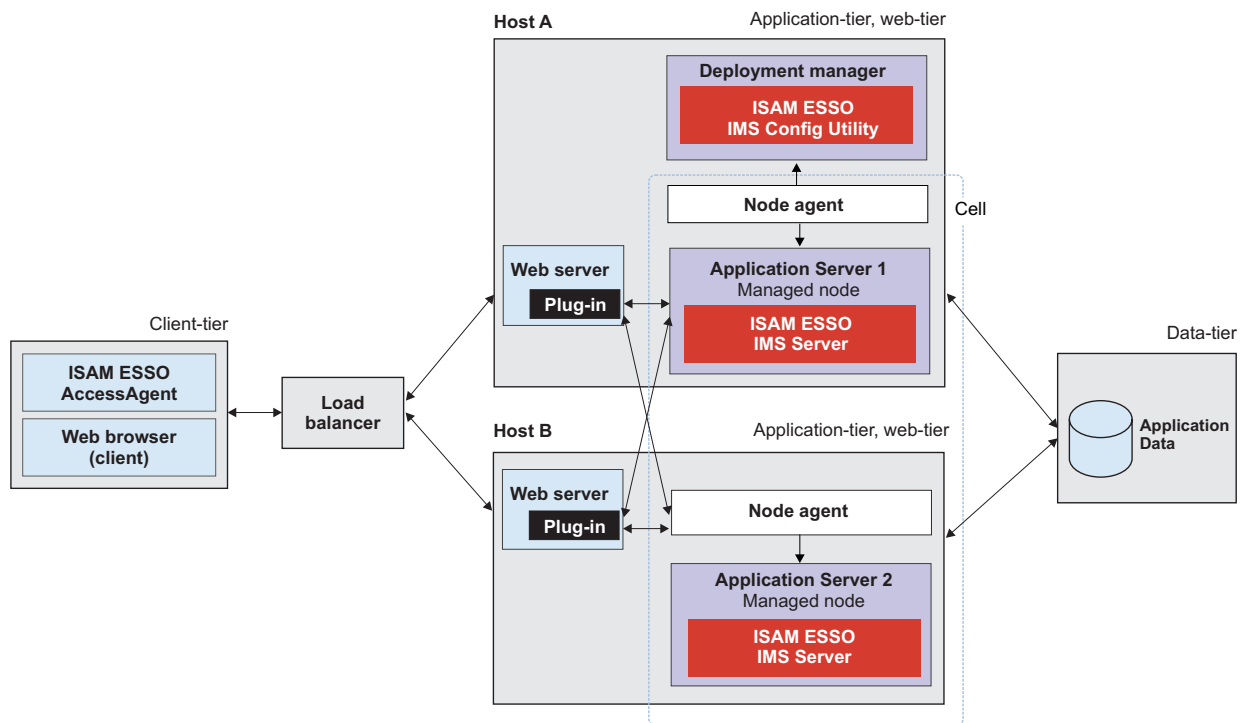


Figure 4. IBM Security Access Manager for Enterprise Single Sign-On in a two-node network deployment cluster example for high availability.

For more information about planning and deployment considerations when setting up a cluster, see the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

Road map

Install and prepare the following middleware before you run the IMS Server installation:

1. Prepare the database server.
2. Prepare the directory server.
3. Prepare WebSphere Application Server.
4. Prepare IBM HTTP Server.
5. Optional: Install the Tivoli Common Reporting component.

You must prepare the following middleware components for use with the IBM Security Access Manager for Enterprise Single Sign-On:

Database server

The database server hosts single sign-on user identities and Wallets. You can install a new instance of a database server or reuse an existing instance.

WebSphere Application Server

The WebSphere Application Server provides a centralized application administration platform that extends the ability of a web server to handle web application requests. The IBM Security Access Manager for Enterprise Single Sign-On IMS Server is a WebSphere application. To reuse an existing application server, you must install and configure it manually.

IBM HTTP Server

The IBM HTTP Server is a separate, dedicated web server that is configured to work with the application server.

Tivoli Common Reporting (optional)

Tivoli Common Reporting is an integrated reporting solution that lets you link multiple reports across various Tivoli products and simplify report navigation and access.

Directory server

A directory server or LDAP repository authenticates a user and retrieves information about users and groups to perform security-related functions, including authentication and authorization. You can install a new instance of a directory server or reuse an existing instance.

If you are reusing existing middleware that was previously deployed, apply the minimum supported fix packs before installing the IMS Server.

Creating and choosing profiles for network deployments

A WebSphere Application Server profile defines the runtime environment. High availability application-serving environments require multiple profiles to manage the complexity of the system.

By using profiles, you can define different types of WebSphere Application Server environments on a single system without having to install multiple copies of WebSphere Application Server. To create profiles for WebSphere Application Server 7.0, you can use the command line or the graphical Profile Management Tool.

Note: To create profiles for 64-bit WebSphere Application Server 7.0, you must use the command line. See “Creating profiles for network deployments (command-line) for x86 or x64 architectures” on page 81.

For a network deployment environment, complete the following steps:

1. Create a deployment manager profile before creating the other profiles.

Note: Only if your deployment plan requires security certificates with a larger key size, be sure to recreate the root certificate before you continue.

2. Create a custom profile for each managed node.

Create the following WebSphere Application Server profiles for a network deployment.

WebSphere Application Server Profiles	When to use
Deployment manager: <i>management</i> profile	For a network deployment environment, create this profile first.
Managed member nodes: <i>custom</i> profile	For a network deployment environment, create custom nodes. You can then use the administrative console to install the ISAMESSOIMS application to the cluster created with the custom nodes.

Note: If the server is newly installed on a computer that has no previous versions of the server, you can use the default values for the ports. Use a utility like **netstat** to check if a port is already in use. Changing the default ports is typically done by an experienced WebSphere Application Server administrator.

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

Deployment manager profiles

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

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

Important:

- Ensure that the administrative user name that you supply for the WebSphere administrator, does not exist on the directory servers that you plan to use for the IMS Server. For example, if the WebSphere administrator you provide is `wasadmin`, then the user `wasadmin` must not exist on the corporate enterprise directory.
- Do not provide a common user name like “administrator” as the WebSphere Application Server administrator.
- Choose a user name that is least likely to conflict with your potential enterprise directory users.

Custom profiles

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

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

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

Creating network deployment profiles (Profile Management Tool) for x86 architectures

Use the Profile Management Tool to create a deployment manager and custom profile for a network deployment for an x86 environment.

Before you begin

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

About this task

This guide provides instructions about preparing the WebSphere Application Server for the IMS Server. For detailed and up-to-date installation instructions, see the WebSphere Application Server documentation.

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

For a network deployment environment, complete the following steps:

- Create a deployment manager profile before creating the other profiles.
- Optional: Upgrade the root cert for the deployment manager from 1024 bit to 2048 bit.
- Create a custom profile for each node that you plan to add to the server cluster.

For systems with 64-bit WebSphere Application Server, the Profile Management Tool is not available. To create profiles for a 64-bit network deployment environment, use the command line. See “Creating profiles for network deployments (command-line) for x86 or x64 architectures” on page 81.

The profile creation process creates default copies of the WebSphere truststore and keystore. When you install the IMS Server component, you must specify the location of the WebSphere truststore and keystore. If you use the default files, you specify the file paths created by the profile management tool.

For example, on a host called `mySvr1`, the default truststore location for the deployment manager is:

```
<was_home>/profiles/<Dmgr_profilename>/config/cells/mySvr1Node01Cell/trust.p12
```

On the same host, the default keystore is:

```
<was_home>/profiles/<Dmgr_profilename>/config/cells/mySvr1Node01Cell/key.p12
```

Tip: To perform basic profile management tasks, such as deleting and listing profiles in WebSphere Application Server, see “Basic commands for managing WebSphere Application Server profiles” on page 204.

Procedure

1. Start the Profile Management Tool. Click **Start > All Programs > IBM WebSphere > Application Server Network Deployment V7.0 > Profile Management Tool**. The Profile Management Tool is displayed.
2. To create a deployment manager profile, do the following steps:
 - a. Click **Launch Profile Management Tool**.
 - b. Click **Create**.
 - c. In the **Environment selection** page, click **Management**.
 - d. Click **Next**.
 - e. In the **Server Type Selection** page, select **Deployment manager**.
 - f. Click **Next**.
 - g. In the **Profile Creation Options** page, select **Typical profile creation**.
 - h. Click **Next**.
 - i. In the **Administrative Security** page, ensure that the **Enable administrative security** check box is selected.
 - j. Specify a WebSphere user name and password. For example, wasadmin.

Important: The administrative user name that you supply for the WebSphere administrator must be unique and not exist on the directory server. For example: if the WebSphere administrator you provide is wasadmin, then the user wasadmin must not exist on the corporate enterprise directory.

- k. Click **Next**.
- l. Review the settings in the **Profile Creation Summary** page. Alternatively, you can record the values in the Appendix A, "Planning worksheet," on page 163. For example:
 - Location (Default is C:\Program Files\IBM\WebSphere\AppServer\profiles\Dmgr01)
 - Profile name (Default is Dmgr01)
 - Cell name
 - Node name
 - Host name
 - Administrative console port: (Default is 9060)
 - Administrative console secure port (Default is 9043)
 - Deployment manager bootstrap port (Default is 9809)
 - Deployment manager SOAP connector port (Default is 8879)
- m. Click **Create**. The deployment manager profile creation process starts.
- n. Ensure the **Launch the First Steps console** check box is selected.
- o. Click **Finish**. The WebSphere Application Server - First Steps window is displayed.
- p. Click the **Installation verification** link. The last two lines are displayed. The deployment manager is started.

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

- q. Verify that you can access the administrative console. For example: browse to `https://localhost:9043/ibm/console`.
- r. Close the output window and browser.

3. Optional: (For deployments with 2048 bits root CA certificate requirements only) Recreate the root CA on the deployment manager node. See “Recreating the root CA for WebSphere Application Server 7.0 on the deployment manager before creating member nodes” on page 83.

Note: If you must increase the root CA key size to 2048 bits for a higher security deployment, recreate the root CA on the deployment manager node before federating nodes.

4. For each WebSphere Application Server node that you want to federate to a deployment manager, do the following steps:
 - a. Click **Launch Profile Management Tool**. The Profile Management Tool is displayed.
 - b. Click **Create**.
 - c. In the **Environment selection** page, select **Custom profile**.
 - d. Click **Next**.
 - e. Click **Typical profile creation**.
 - f. Click **Next**.
 - g. In the **Federation** page, specify the connection values about the deployment manager host.

Note: See the planning worksheet for the values that apply to your environment.

Deployment manager host name or IP address:

Specify the fully qualified domain name of the deployment manager host. For example: appsvr1.example.com.

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

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

Deployment manager SOAP port number (default 8879)

Accept the default value or change to a different port number.

User name

Specify the deployment manager administrator user name. For example, wasadmin.

Password

Specify the deployment manager administrator password.

- h. Click **Next**.
- i. Review the profile creation summary. Alternatively, record the values in the Planning Worksheet.
 - Profile name (default: Custom01)
 - Location (default: C:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01)
- j. Click **Create** to start the profile creation.
- k. Clear the **Launch the First steps console** check box.
- l. Click **Finish**. If the federation fails, see the *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide*.

Results

You installed a deployment manager host and created custom server nodes for a WebSphere Application Server cluster.

What to do next

Configure the WebSphere Application Server.

Creating profiles for network deployments (command-line) for x86 or x64 architectures

Use the **manageprofiles** command to create profiles for a network deployment from the command line.

Before you begin

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

About this task

For 64-bit WebSphere Application Server 7.0, you must use the **manageprofiles** command to create profiles because the Profile Management Tool is not available for 64-bit systems.

The command-line parameters included with the following steps, uses the same profile creation parameters you might use when you create the profiles in the Profile Management Tool. The examples serve only as a guide. For complete information about creating profiles in WebSphere Application Server, see the WebSphere Application Server information center.

Important: For new network deployments, create a deployment manager profile first.

Procedure

1. Open the command prompt.
2. To create the deployment manager profile.
See the following example (use without line-breaks, case-sensitive):

Command line with parameters (case-sensitive, use without line breaks)	Example with sample values
<pre>"<was_home>\bin\manageprofiles.bat" -create -profileName <Dmgr01> -profilePath "<was_home>\profiles\<Dmgr01>" -templatePath "<was_home>\profileTemplates\management" -enableAdminSecurity true -adminUserName <WAS Admin user ID> -adminPassword <password> -winserviceAccountType localsystem -winserviceCheck true -winservicePassword <password> -winserviceStartupType automatic</pre>	<pre>"C:\Program Files\IBM\WebSphere\AppServer\bin\ manageprofiles.bat" -create -profileName Dmgr01 -profilePath "C:\Program Files\IBM\WebSphere\AppServer\ profiles\Dmgr01" -templatePath "C:\Program Files\IBM\WebSphere\AppServer\profileTemplates\management" -enableAdminSecurity true -adminUserName wasadmin -adminPassword <password> -winserviceAccountType localsystem -winserviceCheck true -winserviceStartupType automatic</pre>

Important: The administrative user name that you supply for the WebSphere administrator must not exist on the directory server. For example: if the WebSphere administrator you provide is wasadmin, then the user wasadmin must not exist on the corporate enterprise directory.

3. Verify that the profile is created.
 - a. Click **Start > All Programs > IBM WebSphere > Application Server Network Deployment 7.0 > Application Server > profiles > <Dmgr01> > First steps**.
 - b. Click the **Installation verification** link.
4. Optional: Recreate the root CA on the deployment manager node before creating member nodes. This optional step is only for deployments with specific 2048 bit key size requirements.
5. To create the custom profile for a managed node:

Note: Ensure that the deployment manager is started. Ensure that two way name resolution is enabled between the nodes and the deployment manager. See the following example (case-sensitive, use without line-breaks):

Command line with parameters (case-sensitive, use without line breaks)	Example with sample values
<pre>"<was_home>\bin\manageprofiles.bat" -create -profileName <Custom01> -profilePath "<was_home>\profiles\<Custom01>" -templatePath "<was_home>\profileTemplates\managed" -dmgrHost ibm-svr1.example.com -dmgrPort 8879 -dmgrAdminUserName <WAS Admin user ID> -dmgrAdminPassword <password></pre>	<pre>"C:\Program Files\IBM\WebSphere\AppServer\bin\ manageprofiles.bat" -create -profileName Custom01 -profilePath "C:\Program Files\IBM\WebSphere\AppServer\ profiles\Custom01" -templatePath "C:\Program Files\IBM\WebSphere\AppServer\profileTemplates\managed" -dmgrHost ibm-svr1.example.com -dmgrPort 8879 -dmgrAdminUserName wasadmin -dmgrAdminPassword <password></pre>

The example creates a custom profile and federates the custom node into the deployment manager node.

Remember: You can update the Appendix A, "Planning worksheet," on page 163 with the values of your created profile. If the federation fails, see the *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide*.

What to do next

Optional: If the installation is not verified, start the **First steps** tool to verify the installation.

1. Click **Start > All Programs > IBM WebSphere > Application Server Network Deployment 7.0 > Application Server > profiles > <Dmgr01> > First steps.**
2. Click **Installation verification.**

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

The WebSphere Application Server root CA has a default 1024 bit key size. Change the root CA key size to 2048 bit on the deployment manager node before you create any federated nodes. Use a 2048 bit key size to offer an increased level of security.

Before you begin

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

About this task

This task is optional. It applies only to:

- New installations of the IMS Server that must upgrade the default 1024 bit root certificate key size to 2048 bit.
- A new cluster where only the deployment manager node is created.
Custom WebSphere Application Server profiles or member nodes of the cluster are not yet created or federated.

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

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

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

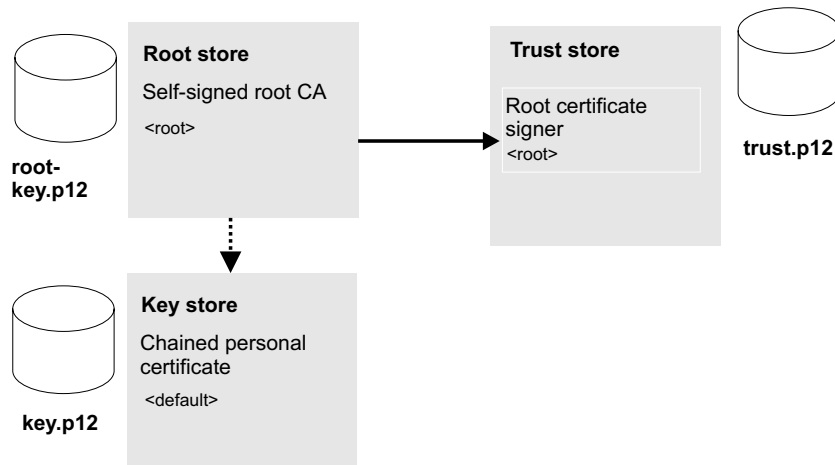


Figure 5. Replacing the root CA and key signers for WebSphere Application Server in the truststore with a new key size.

The process involves the following steps:

1. Replace the default 1024 bit root certificate with a new 2048 bit root certificate; then extract it. See step 1 to step 9 on page 85.
2. Create a 2048 bit chained personal certificate in the key store, replace the older version, and export the personal certificate to a keystore. See step 10 on page 86 to step 11 on page 87.
3. Use the **ikeman** utility to add the extracted root CA to the truststore. See step 12 on page 87.

Procedure

1. Select **Start > All Programs > IBM WebSphere > Application Server <version> > Profiles > <dmgr_profile_name> > Administrative console**.
2. Log on to the IBM Integrated Solutions Console.
3. On the Integrated Solutions Console navigation pane, select **Security > SSL certificate and key management**.
4. In **Related items**, click **Key stores and certificates**.
5. Create a temporary self-signed root CA in the default root store.
The temporary root certificate is used to replace the older root certificate. The temporary root certificate is then replaced with a new 2048 bit root certificate.
 - a. From the **Keystore usages** list, select **Root certificates keystore**.
 - b. Click **DmgrDefaultRootStore**.
 - c. Under **Additional Properties**, click **Personal certificates**.
 - d. Click **Create > Self-signed Certificate**.
 - e. In **Alias**, enter a new alias name. For example: root2.
 - f. In the **Common name** field, enter the fully qualified domain name of the computer where the WebSphere Application Server is installed. For example: ibm-svr1.example.com.
 - g. Click **OK**.
 - h. Click **Save**.
6. Replace the old root CA with the new root CA: root2. Replace the old root with the temporary root2.

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

Important: Be sure that the **Delete old signer** check box is not selected. See the WebSphere Application Server information center on replacing a certificate for details:

http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/tsec_sslreplaceselfsigncert.html

- e. Click **OK**.
 - f. Click **Save** to apply the changes to the master configuration.
7. Create the 2048 bit root CA. This root certificate is the 2048 bit certificate that you retain.
- a. Click **Create > Self-signed Certificate**.
 - b. In **Alias**, enter root.

Important: You must specify the alias name as root for this 2048 bit certificate.

- c. From the **Key size** list, select **2048**.
- d. In the **Common name** field, enter the fully qualified domain name of the computer where the WebSphere Application Server is installed. For example: `ibm-svr1.example.com`.
- e. In the **Validity period** field, enter the validity period of the certificate. For example: A root certificate is typically used for 7300 days, which is approximately 20 years.
- f. Optional: Complete the certificate with optional identification details.
- g. Click **OK**.
- h. Click **Save**.

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

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

- f. Click **OK**.
- g. Click **Save** to apply the changes to the master configuration.

You successfully replaced the original 1024 bit root certificate with a new 2048 bit root certificate.

9. Extract the new root CA to a file.
- a. In the **Personal Certificates** page, select **Root**.
 - b. Click **Extract**.

- c. In **Certificate file name**, enter the fully qualified path to the certificate to be extracted. For example: C:\root2048.cer
 - d. Verify **Data type** is **Base64-encoded ASCII data**
 - e. Click **OK**.
10. Create a chained personal certificate in the default cell keystore: **CellDefaultKeystore**.
- a. In the **Key stores and certificates** page, click **CellDefaultKeyStore**.
 - b. In **Additional Properties**, click **Personal certificates**.
 - c. Click the **default** certificate. The distinguished name for the default certificate in the **CellDefaultKeystore** must be in the following form:
CN=<CN>,OU=<OU>,O=<Organization>,C=<Country> For example:
CN=ibmsvr1.example.com, OU=Root Certificate, OU=ibmsvr1Cell01,
OU=ibmsvr1CellManager01, O=IBM, C=US .
 - d. Click **Back**.
 - e. Click **Create > Chained certificate**.
 - f. In the **Alias** field, enter a new personal certificate alias. For example: default2.
 - g. In the **Root certificate used to sign the certificate** field, select the alias **root**. This root certificate is the new 2048 bit root certificate.
 - h. In the **Key size** field, select **2048**.
 - i. In the **Common name** field, enter the fully qualified domain name of the computer where the WebSphere Application Server is installed.
 - j. In the **Validity period** field, enter the validity period of the certificate. For example: a typical default value for a personal certificate is 365 days.
 - k. Required: In the **Organization** field, specify the organization portion of the distinguished name.
- Important:** It is important that you specify the organization portion of the distinguished name.
- l. Required: In the **Country or region** field, specify the country portion of the distinguished name.
- Important:** It is important that you specify the country portion of the distinguished name.
- m. Optional: Enter additional certificate identification information in the optional fields.
 - n. Click **OK**.
 - o. Click **Save** to apply the changes to the master configuration.
 - p. Replace the old default personal certificate with the new one.
 - 1) In the **Personal Certificates** page, select the **default** check box.
 - 2) Click **Replace**.
 - 3) From the **Replace with** list, choose the alias of the certificate you created. For example: default2.
 - 4) Select **Delete old certificate after replacement**.
 - 5) Ensure that the **Delete old signer** check box is not selected.

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

 - 6) Click **OK**.

- 7) Click **Save** to apply changes to the master configuration.

Note: If the web browser alerts you that a certificate is revoked and a new certificate is available, click **Yes** to proceed. Follow instructions on the screen to accept any additional security prompts of the new security certificate.

11. Export the personal certificate to the keystore: For example:
<was_home>\profiles\<dmgr_profile_name>\etc\key.p12.
 - a. In the **Personal Certificates** page, select the personal certificate check box. For example, default2.
 - b. Click **Export**.
 - c. In **Key store password**, enter the key store password For example: WebAS.

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

- d. Select **Key store file**.
- e. In **Key store file**, specify the key store location. For example:
<was_home>\profiles\<dmgr_profile_name>\etc\key.p12
- f. For **Type**, verify that the default **PKCS12** is selected.
- g. In **Key file password**, type the password. For example: WebAS.
- h. Click **OK**.

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

12. Use the IBM Key Management utility, *ikeyman*, to add the extracted root CA to the deployment manager truststore.
 - a. Start the **ikeyman** utility.

You can locate the utility in the following location, for example:
<was_home>\profiles\<dmgr_profile>\bin\ikeyman.bat
 - b. Click **Key Database File > Open**.
 - c. In **Key database type**, select **PKCS12**.
 - d. Click **Browse** to locate the truststore. You can locate the truststore in
<was_home>\profiles\<Dmgr_profile>\etc\trust.p12.
 - e. Type the truststore password. For example: WebAS
 - f. Add the root CA you extracted to the truststore.
 - 1) In **Key database content** area, select **Signer Certificates**.
 - 2) Click **Add**.
 - 3) Specify the location of the extracted root CA. For example:
C:\root2048.cer
 - 4) Specify a label for the extracted root CA in the truststore. For example:
root2048_signer

The root CA is saved and added to the truststore.

13. Verify that the certificates are upgraded.
 - a. Log out of the administrator console and try logging in again.
 - b. When you see the security prompt in the web browser, view the certificate details.
 - c. Verify that the key size of the reissued certificate is 2048 bits.
14. Restart the deployment manager.

Results

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

What to do next

Continue with the process of creating custom profiles for the rest of the member nodes of a cluster in WebSphere Application Server. See “Creating and choosing profiles for network deployments” on page 76.

You can update the Planning worksheet with the aliases you used for the root and default certificate aliases. You must specify the aliases in the IMS Configuration Wizard.

Configuring WebSphere Application Server for a cluster

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

Before you begin

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

About this task

Configure WebSphere Application Server for a cluster before you install the IMS Server. Configuring WebSphere Application Server for a cluster involves the following tasks:

1. Define a WebSphere Application Server cluster.
2. Configure the heap size for the deployment manager.
3. Configure the heap size for WebSphere Application Server.
4. Create a Windows service for the node agent.

Defining a cluster

Create a cluster definition and add members to the cluster before you install the IMS Server.

Procedure

1. Open the administrative console and log on to the Deployment Manager with administrator privileges.
 - a. For example: in a web browser, type `https://localhost:9043/ibm/console`.
 - b. Log on with the WebSphere administrator account. For example: `wasadmin`
2. Define a new cluster.
 - a. Expand the **Servers** link, and select **Clusters > WebSphere application server clusters**.
 - b. Click **New**.
 - c. In the **Cluster name** field, enter a name for the cluster. For example: type `cluster1`.
 - d. Select the **Configure HTTP session memory-to-memory replication** check box.
 - e. Ensure the **Prefer local** check box is selected.

- f. Click **Next**.
- g. In the **Member name** field, type a name for the first member of the cluster. For example, server1.
- h. In **Select Node**, choose the node that you want to add to the cluster.
- i. Verify **Create the member using an application server template** is set to **default**.
- j. Click **Next**. You added a member of the node to the cluster.
- k. Do one of the following steps:
 - If you have no other cluster members to add, click **Next**.
 - If you have additional cluster members to add, type the name. Select the correct node. Click **Add member**. Specify additional cluster members before you click **Next**.
- l. Click **Finish**. You created a cluster and added members to the clusters.
- m. In the **Messages** box, click **Save**. The cluster status indicates that the cluster is not started.

Results

You prepared a WebSphere Application Server cluster and added member nodes. You can administer the cluster and nodes from the WebSphere administrative console.

What to do next

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

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

Configuring the heap size for the deployment manager

Update the memory heap size used by the deployment manager in a clustered deployment. Update the allocated memory to ensure that sufficient memory is available for the deployment manager. Sufficient memory is required when you must configure many Active Directory repositories for the IMS Server.

Before you begin

Before you modify the Java heap size, ensure that the host has enough physical memory to support a JVM of 3.0 GB without swapping. If the physical memory of the host system exceeds 3 GB, you can increase the maximum heap size. However, if the heap size is too large, the system does not have enough physical memory and starts allocating virtual memory to hold the data.

Procedure

1. In the navigation panel, click **System administration > Deployment manager > Java and Process Management > Process Definition**.
2. Under **Additional Properties**, click **Java Virtual Machine**.
3. In the **Initial heap size** field, type 512.
4. In the **Maximum heap size** field, type 1024.
5. Click **OK**.
6. In the **Messages** box, click **Save**.

7. Restart the deployment manager.

Configuring the heap size for the application server

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

Before you begin

Before you modify the Java heap size, ensure that the host has enough physical memory to support a JVM of 3.0 GB without swapping. If the physical memory of the host system exceeds 3 GB, you can increase the maximum heap size. However, if the heap size is too large, the system does not have enough physical memory and starts allocating virtual memory to hold the data.

About this task

Adjust the Java heap size with the following guidelines before installing the IBM Security Access Manager for Enterprise Single Sign-On IMS Server component. To learn more, see the WebSphere Application Server information center (<https://www-01.ibm.com/software/webservers/appserv/was/library/v70/>) and search for *Java virtual machine settings heap tuning*.

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

Procedure

1. On the WebSphere Application Server host, where you are installing the IMS Server, log on to the administrative console. For example: `https://localhost:9043/ibm/console/`.
2. Navigate to the Java virtual machine settings.
 - a. Expand **Servers > Server Types** and select **WebSphere application servers**.
 - b. Click the name of your server. For example: **server1**.
 - c. Under the **Server Infrastructure** group, click to expand **Java and Process Management**.
 - d. Click **Process Definition**.
 - e. Under the **Additional Properties** group, click **Java Virtual Machine**.
3. Use the following settings (for a single server instance, 3 GB host):
 - **Initial Heap Size:** 1024
 - **Maximum Heap Size:** 1280
4. Click **OK**.
5. In the messages box, click **Save**.
6. Click **OK**.
7. In the messages box, click **Save**.
8. Restart the WebSphere Application Server.

Creating a Windows service for the node agent

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

About this task

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

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

Procedure

1. Open a command prompt window.
2. Change the directory to `<was_home>\bin`. For example: type `cd c:\Program Files\IBM\WebSphere\AppServer\bin`
3. Type the following **WASService** command with the following parameters (case-sensitive, without the line breaks):

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

Where

<was_home>

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

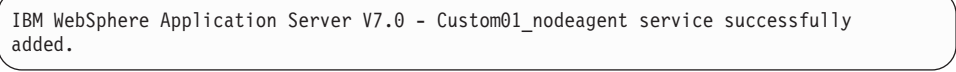
<profile_name>

Specifies the name of the custom node profile in Windows service. For example, `Custom01`.

Example (with sample values)

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

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



```
IBM WebSphere Application Server V7.0 - Custom01_nodeagent service successfully
added.
```

5. Close the command prompt.
6. Verify that the service is added to Windows services.
 - a. Click **Start > Run**. Type `services.msc`.
 - b. Verify that the node agent service is displayed. For example, `IBM WebSphere Application Server v7.0 - Custom01_nodeagent`.
7. Optional: If you have additional nodes, repeat this task for other nodes in your cluster. For example: `Custom02`.

Results

You added the node agent service to the list of Windows services.

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

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

Before you begin

- Ensure that the following software is started:
 - IBM HTTP Server
 - IBM HTTP Server Administration Server
 - Deployment manager
 - Node agent on the managed node
- Review the planning worksheet for the configuration settings. See Appendix A, “Planning worksheet,” on page 163.

About this task

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

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

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

Procedure

1. Run the web server plug-in configuration script.
 - a. On the IBM HTTP Server host, from `<ihs_home>\Plugins\bin`, copy the `configure<web_server_definition_name>.bat` file. For example: `configurewebserver1.bat`
 - b. On the deployment manager, paste the `configure<web_server_definition_name>.bat` file to the `<was_home>\bin` folder. For example: `C:\Program Files\IBM\WebSphere\AppServer\bin`
 - c. Open the command prompt.
 - d. Browse to `<was_home>\bin`.
 - e. Run the following command (without the line breaks):

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

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

Configuration save is complete.

Running the script plug-in added and configured a web server definition on the WebSphere administrative console (**Servers > Server types > Web servers**). For example, `websvr1`.

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

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

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

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

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

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

3. Synchronize the WebSphere Application Server keystore with the IBM HTTP Server keystore.
 - a. On the IBM Integrated Solutions Console navigation pane, click **Servers > Server Types > Web servers**.
 - b. Click the `<Web server name>`. For example: `websvr1`.
 - c. In the **Additional Properties** section on the **Configuration** tab, click **Plug-in properties**.
 - d. Click **Copy to Web Server key store directory**.
 - e. Click **OK**.
 - f. In the **Messages** box, click **Save**.
4. Required: If you have multiple web servers, repeat steps 1 on page 92 to 3.
5. Regenerate and propagate the web server plug-in configuration.

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

- a. Click **Servers > Server Types > Web Servers**.

- b. Select the web server from the list. For example: `webserver1`.
 - c. Click **Generate Plug-in**.
 - d. Select the web server from the list. For example: `webserver1`.
 - e. Click **Propagate Plug-in**.
6. Synchronize the nodes with the deployment manager.

Results

You defined a web server in the WebSphere Application Server configuration that can route requests received from client workstations to the application server.

Enabling SSL directives on the IBM HTTP Server

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

About this task

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

Complete this procedure for every web server.

Procedure

1. On the IBM Integrated Solutions Console, click **Servers > Server Types > Web servers**.
2. Click the `<Web server name>`. For example: `webserver1`
3. In the **Additional Properties** section on the **Configuration** tab, click **Configuration File**.

If the configuration file fails to open, see the *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide*.

4. Add the following lines to the end of the configuration file:

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

where

default

Specifies the alias of the default SSL certificate.

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

- a. In the IBM Integrated Solutions Console navigation pane, click **Security > SSL certificate and key management**.
- b. Under **Related Items**, click **Key stores and certificates**.
- c. Click **CMSKeyStore**.
- d. Under **Additional Properties**, click **Personal certificates**.

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

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

5. Click **Apply**.
6. Click **OK**.
7. Select **General Properties > Apply**.
8. In the **Messages** box, click **Save**.
9. Restart the IBM HTTP Server.
 - a. On the IBM Integrated Solutions Console, click **Servers > Server Types > Web servers**.
 - b. Select the check box of the corresponding web server. For example: webserver1.
 - c. Click **Stop**.
 - d. Select the check box for the web server again.
 - e. Click **Start**.
10. Verify that the SSL directives are enabled correctly. Type the following https address in a web browser. For example:
 - https://<ihs_host>
For example: https://mywebsvr.example.com.
A web browser security prompt might display because you are accessing a page over the secure https protocol. Follow the instructions in the dialog box to accept the security certificate and continue to the page.
 - http://<ihs_host>
For example: http://mywebsvr.example.com.
You can also verify that pages over non-https protocol are still accessible.

Tip: If the verification fails, check whether the custom variables you specified in step 4 on page 94 are added and replaced correctly. For additional troubleshooting tips, see the *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide*.

Results

You enabled SSL on the IBM HTTP Server. You also verified pages over the secure https protocol.

Recreating the SSL certificate for the IBM HTTP Server

You can recreate the SSL certificate to increase the SSL certificate key size for the IBM HTTP Server, from 1024 bits to 2048 bits. This task is optional.

Before you begin

Ensure that the WebSphere Application Server root CA is already upgraded to 2048 bits. See one of the following topics:

- For WebSphere Application Server in a stand-alone deployment, see “Recreating the root CA for WebSphere Application Server 7.0 (stand-alone)” on page 57
- For WebSphere Application Server in a cluster, see “Recreating the root CA for WebSphere Application Server 7.0 on the deployment manager before creating member nodes” on page 83

About this task

This task is optional and applicable only for new installations of the IMS Server. If you must upgrade the default SSL certificate for IBM HTTP Server to 2048 bits, complete this task before you install the IMS Server.

If you are using multiple web servers, perform the following steps on each **CMSKeyStore** in the administrative console.

Procedure

1. Select **Start > All Programs > IBM WebSphere > Application Server <version> > Profiles > <profile name> > Administrative console.**
2. Log on to the IBM Integrated Solutions Console.
3. On the Integrated Solutions Console navigation pane, select **Security > SSL certificate and key management.**
4. Under **Related items**, click **Key stores and certificates.**
5. Click **CMSKeyStore.**
6. Under **Additional Properties**, click **Personal certificates.**
7. Select the certificate named **default.**
8. Click **Delete.**
9. Click **Create > Chained Certificate.**
10. In the **Alias** field, enter a new alias name. For example: default.
11. From the **Root certificate used to sign the certificate** list, select the alias of the newly created Root CA. For example: root
12. From the **Key size** list, select **2048.**
13. In the **Common Name** field, use one of the following entries:
 - If you are not using a load balancer, specify the fully qualified name of the host where IBM HTTP Server is installed. For example: httpsvr1.example.com.
 - If you are using a load balancer, specify the fully qualified name of the load balancer.
14. In the **Validity period** field, enter the validity period of the certificate. For example: 365 days.
15. Optional: Enter the information in the following fields:
 - Organization
 - Organization Unit
 - Locality
 - State/Province
 - Zip Code
 - Country or Region
16. Click **OK.**
17. In the **Messages** box, click **Save.**
18. Synchronize the WebSphere Application Server keystore with the IBM HTTP Server keystore.
 - a. On the IBM Integrated Solutions Console navigation pane, click **Servers > Server Types > Web servers.**
 - b. Click the **<Web server name>**. For example: *websvr1*.

- c. In the **Additional Properties** section on the **Configuration** tab, click **Plug-in properties**.
 - d. Click **Copy to Web Server key store directory**.
 - e. Click **OK**.
 - f. In the **Messages** box, click **Save**.
19. Resynchronize the nodes.
 - a. Click **System administration > Nodes**.
 - b. Select the check box for each corresponding node.
 - c. Click **Full Resynchronize**.
 20. Restart the IBM HTTP Server.

Configuring the IMS Server for a cluster

You can install the IMS Server by using the IMS Server installer or by deploying the IMS Server Enterprise Archive (EAR) files manually on WebSphere.

1. Review the release notes.
2. Extract and install the IMS Server. Choose one of the following methods:
 - Install the IMS Server interactively with the IMS Server installer.
 - Deploy the IMS Server on WebSphere Application Server manually.
3. Verify the IMS Server deployment.
4. Set up and configure the IMS Server.
 - Configure the IMS Server with the IMS Configuration Wizard
Set up the data source, certificates, target URL, and directory services.
 - Provision an IMS Server administrator.
You can use the IMS Server administrator credentials to access and administer single sign-on resources.
5. Update the application mappings for the ISAMESSOIMS application.
Mapping ensures that all client connection requests from the web-tier or from the load balancer are forwarded correctly to the WebSphere Application Server and IMS Server application.
6. Disable auto start for the ISAMESSOIMS application on a cluster.
7. Configure session management.
8. Verify the configuration.

Configuring the IMS Server with the IMS Configuration Wizard (network deployment)

Complete the IMS Server installation with some initial required configuration.

Before you begin

- Prepare the directory server.
- Prepare the database server.
- Ensure that the cluster is stopped.
- Ensure that the managed nodes in the cluster are stopped.
- Ensure that the deployment manager is started.
- Ensure that the IMS Server application ISAMESSOIMSConfig is started.
- Review the planning worksheet for sample values.

About this task

To configure the IMS Server, the IMS Configuration Wizard helps you accomplish the following tasks:

- Set up the data source.
- Update certificates.
- Set up the IMS Server URL.
- Configure the IMS Server for enterprise directories.

Procedure

1. Open the IMS Configuration Wizard. The URL is in the following form:
https://<dmgr_hostname>:<admin_ssl_port>/front
For example: https://localhost:9043/front.
2. To switch to another language in the IMS Configuration Wizard, choose your preferred language in the **Language** menu.
3. In the **Server Set Up** page, select **Set up a new IMS Server**.
4. Click **Begin**.
5. In **Enter data source information**, accept the default values or customize the fields for the data source.
6. Click **Next**.
7. To use the default option to create a database schema by using the IMS Configuration Wizard, ensure that the **Create IMS Server database schema** check box is selected.

Note: Alternatively, you can create the database schema manually. See Appendix B, "Creating database schemas," on page 175.

8. Click **Next**.
9. Select the IMS Server database type.

Note: If you are using a Microsoft SQL Server database, you have the following choices:

- Default: Create a database with the configuration wizard. Select **Create new database**.
 - Use an existing database. Clear the **Create new database** check box. Click **Next**.
10. Click **Next**.
 11. In **Database Configuration - <database type>**, specify the connection information about the database type. Follow the instructions in the wizard to specify the database connection details. The database type you select might include a different set of fields. See the help descriptions on the page for guidance.

Tip: To see additional help for each item, move the cursor over each item. The following fields are specific to DB2. You can use the following descriptions for additional guidance:

Host Name

Specify the database host name. For example: mydbsvr.

Port

The database connection port number is pre-filled. Verify whether the default port value is correct.

For example:

- The default value for DB2 is 50000.
- The default value for SQL Server is 1433.
- The default value for Oracle is 1521.

Note: To determine the correct database connection port numbers, see your database vendor documentation on how to determine the correct values for your database server.

Database name

Specify the name of the database. For example: imsdB.

User name

Specify the database user you prepared. For example: db2admin.

User password

Specify the password for the database user.

12. Click **Next**.

13. In **Provide Root CA Details**, verify the default values.

Verify the keystore name, keystore password, and certificate alias of the Root CA used to sign the IMS Server intermediate CA.

Important: If you recreated or upgraded the key size for the root CA, the root CA alias name might change. Be sure to specify the correct alias. See the following descriptions for guidance:

Tip: Use the Planning Worksheet to verify the custom values you used. See Appendix A, “Planning worksheet,” on page 163.

Keystore name

Specifies the name of the root key store. The root key store is a key database that contains both public and private keys for secure communication. Typically, you can use the default value.

Keystore scope

Specifies the level at which the keystore is visible at the cell or node level. Typically, you can use the default value.

Keystore password

Specifies the password for the root certificate keystore. Typically, you can use the default value.

Root CA alias name

Accept the default value for the root alias unless the root CA alias has been modified.

14. Click **Next**. The certificate credentials for the keystore and root alias are verified.

15. In **Configure IMS Services URL**, specify the IBM HTTP Server or load balancer name and port number or accept the default values.

Note: The IBM HTTP Server or load balancer name:

- Is the fully qualified name of the IBM HTTP Server or load balancer that interfaces with the WebSphere Application Server.
- Must match the CN attribute of the SSL certificate used by the IBM HTTP Server.

16. Click **Next**.

17. Configure the IMS Server to work with a directory server.

Note:

- To configure directory servers later, be sure to complete the directory server setup before you use the IMS Configuration Utility.
- If you are planning to use a directory server, configure the IMS Server to work with a directory server before you provision an IMS Server administrator account.

18. Click **Next**.

19. Review the settings.

20. Click **Save**.

21. To complete the IMS Server configuration, do one of the following options:

Option	Description
If you configured enterprise directories:	(Network deployment) Restart the deployment manager node. (Stand-alone deployment) Restart the application server.
If you did not configure any enterprise directories:	Restart the ISAMESSOIMSConfig.

Results

You have successfully set up the IMS Server.

What to do next

You are ready to provision the IMS Server administrator account.

Provisioning the IMS Server administrator

For new installations, you can provision an administrator account for the IMS Server.

Before you begin

- Ensure that the deployment manager is started.
- Ensure that the ISAMESSOIMSConfig is started.
- Ensure that the cluster is stopped.
- Prepare the directory server.
 - If your deployment requires you to use a directory server with the IMS Server, configure the directory server first. See Configure the IMS Server for directory servers.
 - Ensure that the user names for the IMS Server administrator or the WebSphere administrator are unique and do not exist on the directory server where you are provisioning the account.
 - On the Active Directory or LDAP server, create an IMS Server administrator account. For example: `imsadmin`.
 - Start the directory server and ensure that it is available.

About this task

Considerations when provisioning an administrator:

When enterprise directories are not configured

The provisioned IMS Server administrator account is created and stored in the IMS Server database. When you log on with the IMS Server administrator credentials, the credentials are authenticated against the IMS Server database. This account in the database is also known as a base connector user account.

When enterprise directories are configured

The provisioned IMS Server administrator account is synchronized and authenticated with a similar account in the enterprise directory.

Procedure

1. In a browser, start the IMS Configuration Utility. For example: type `https://localhost:9043/webconf`.
2. Log on with the WebSphere administrator credentials.
3. In the Configuration Wizards area, click **Provision IMS Administrator**.
4. Type the credentials of a valid user for the IMS Server administrator you want to provision. For example: `imsadmin`.

If you are using a directory server, type the credentials for a valid enterprise directory user. If you did not create a specific IMS Server administrator, you can specify any existing user on the directory server.

Note: If there are multiple enterprise directories, select the domain where the user exists.

Results

You provisioned an IMS Server administrator account.

What to do next

Continue with additional IMS Server post-installation configuration. Update the application mappings for the ISAMESSOIMS application.

Updating the ISAMESSOIMS module mapping for connection request forwarding

Update the application mappings for ISAMESSOIMS to the web-tier and application-tier hosts with the new IMS Server application mappings.

Before you begin

Ensure that the following components and applications are started:

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

Ensure that the following components and applications are stopped:

- ISAMESSOIMS

- IBM HTTP Server
- Cluster

About this task

You must map the ISAMESSOIMS application to the web-tier and application-tier hosts after installing the IMS Server with the IMS Server installer. You must update the ISAMESSOIMS application mappings manually if you are adding additional nodes to a cluster.

Procedure

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

Tip: To select multiple servers, press the **Shift** key and click to select multiple web servers and application servers.

6. Click **Apply**.
7. Click **OK**.
8. In the **Messages** box, click **Save**.

Results

The IMS Server application URLs connection requests are now forwarded correctly by the IBM HTTP Server to the ISAMESSOIMS application.

Disabling auto start for ISAMESSOIMS

When the ISAMESSOIMS application is deployed on a cluster, you must disable the **Auto Start** option for the ISAMESSOIMS application.

Procedure

1. Log on to the WebSphere Application Server administrative console.
2. In the WebSphere Application Server administrative console navigation pane, click **Applications > Application types > WebSphere enterprise applications**.
3. Click the **ISAMESSOIMS** link.
4. Under **Detail Properties**, click **Target specific application status**.
5. Select the check box for the cluster. For example: cluster1
6. Click **Disable Auto Start**.
7. Click **OK**.
8. In the **Messages** box, click **Save**.

Results

You disabled the auto start option for the cluster.

Note: After disabling the autostart option, you must remember to start the ISAMESSOIMS application manually every time you restart the WebSphere Application Server.

Overriding session management for the ISAMESSOIMS

You must override session management to ensure that the ISAMESSOIMS application can override any inherited session management settings from the parent object.

Before you begin

Ensure that the ISAMESSOIMS mapping is updated.

About this task

ISAMESSOIMS is a web application. Session management provides a mechanism for ISAMESSOIMS, to hold the state of information for a user over a time for a series of web pages users interact with.

Procedure

1. In the WebSphere administrative console navigation pane, click **Applications > Application types > WebSphere enterprise applications**.
2. Click ISAMESSOIMS.
3. Under **Web Module Properties**, click **Session management**.
4. Under **General Properties**, select the **Override session management** check box.
5. Click **Apply**.
6. In the **Messages** box, click **Save**. The ISAMESSOIMS application is stopped.
7. Configure session management override for AccessAdmin.
 - a. In the **Enterprise Applications** page, click ISAMESSOIMS.
 - b. Under **Modules**, click **Manage Modules**.
 - c. Click the **ISAM ESSO IMS Server AccessAdmin <version number>** link.
 - d. Under **Additional Properties**, click **Session management**.
 - e. Select the **Override session management** check box.
 - f. Click **OK**.
 - g. Click **Save**.
8. Resynchronize the nodes.
 - a. Click **System administration > Nodes**.
 - b. Select the check box for each corresponding node.
 - c. Click **Full Resynchronize**.
9. Start the cluster.
 - a. Click **Servers > Clusters > WebSphere application server clusters**.
 - b. Select the check box for the cluster.
 - c. Click **Stop**.
 - d. Click **Start**.

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

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

Results

You started the following components:

- Cluster
- Managed member nodes
- ISAMESSOIMS application
- ISAMESSOIMSConfig application

Verifying the IMS Server configuration

Verify that the IMS Server installation and configuration are working.

Before you begin

Ensure that the following applications and components are started:

- ISAMESSOIMS
- ISAMESSOIMSConfig
- WebSphere Application Server
- IBM HTTP Server
- Database servers
- Directory servers

Procedure

1. Verify that you can access AccessAdmin.
 - a. In a browser, go to the AccessAdmin URL. For example:
 - `https://<ihs_host>/admin`
 - `https://<loadbalancer_host>/admin`
 - b. Log on to AccessAdmin with the IMS Server administrator account you provisioned. For example: `imsadmin`.
 - c. Click **Setup assistant**.
 - d. You can review the instructions to configure authentication factors at a later time. Close the browser. You successfully verified that you have access to AccessAdmin.
2. Verify that you can access Web Workplace.
 - a. In a browser, go to the Web Workplace URL. For example:
 - `https://<ihs_host>/aawwp?isWwp=true`
 - `https://<loadbalancer_host>/aawwp?isWwp=true`
 - b. Log on to Web Workplace with the IMS Server administrator account that you provisioned. For example: `imsadmin`.
3. Verify that you can access AccessAssistant.
 - a. In a browser, go to the AccessAssistant URL. For example:
 - `https://<ihs_host>/aawwp`
 - `https://<loadbalancer_host>/aawwp`
 - b. Log on to AccessAssistant with the IMS Server administrator account that you provisioned. For example: `imsadmin`.

Results

You successfully installed the IMS Server and ensured that it works. You also verified that the URL to access the administration components work.

What to do next

To perform additional server configurations specific to your deployment, such as adding authentication factors, see the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

You can now install the AccessAgent or AccessStudio clients on client workstations.

Tip: To save time and simplify access, bookmark the administrative URLs in your web browser.

Adding application servers to a cluster

You can add an additional IBM Security Access Manager for Enterprise Single Sign-On cluster member node to a WebSphere Application Server cluster.

About this task

Create a custom profile for the node. Then add the node to an existing WebSphere Application Server cluster. After adding the node, deploy the ISAMESSOIMS application on the node.

In a network deployment	Deploy
On the deployment manager node.	<ul style="list-style-type: none">ISAMESSOIMSISAMESSOIMSConfig
On each node of the cluster.	ISAMESSOIMS

Procedure

1. Create a custom profile with the WebSphere Application Server Profile Management tool or command-line tool.
2. In the WebSphere Application Server administrative console, add the newly created server to the WebSphere Application Server cluster.

Tip: When adding cluster members, in the console navigation tree, be sure to select the cluster and add members in the **Cluster members** page. For example: Click **Servers > Clusters > WebSphere application server clusters**. Select the cluster. Click **Cluster members**. Click **New**.

3. Optional: Create a Windows service for the additional node agent and server node.

Example (case-sensitive, use without line breaks):

```
wasservice -add Custom02_nodeagent -serverName nodeagent -profilePath
"C:\Program Files\IBM\WebSphere\AppServer\profiles\Custom02" -wasHome
"C:\Program Files\IBM\WebSphere\AppServer" -logRoot
"C:\Program Files\IBM\WebSphere\AppServer\profiles\Custom02\logs\nodeagent" -logFile
"C:\Program Files\IBM\WebSphere\AppServer\profiles\Custom02\logs\nodeagent\startServer.log"
-restart true
-startType automatic
```

4. Optional: Install the Native Library Invoker resource adapter on the new node.
5. Generate and propagate the web server plug-in.
6. Restart the IBM HTTP Server.
7. Deploy the ISAMESSOIMS application.

- a. On the Integrated Solutions Console navigation pane, select **Applications > Application Types > WebSphere Enterprise Applications**.
- b. Click ISAMESSOIMS.
- c. Under **Modules**, click **Manage Modules**.
- d. Select the check box for all the applications.
- e. In **Clusters and servers**, select the web server and cluster.
- f. Click **Apply**.
- g. Save the changes to the master configuration.
8. Resynchronize all the nodes.
9. Start the cluster.
10. Start the ISAMESSOIMS application.

Part 2. Installing AccessAgent and AccessStudio

To provide single sign-on for Windows workstations, install the AccessAgent client component. To extend single sign-on support for applications with AccessProfiles, install the AccessStudio.

Chapter 6. AccessAgent and AccessStudio installation road map

The AccessAgent and AccessStudio installation road map lists the high-level tasks you must complete to install and set up these client-side components.

Before you begin:

- Read the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*. This guide helps you to plan your deployment and prepare your environment.
- Ensure that you have administrator privileges.
- Install and configure the IMS Server.

Follow these tasks in this order when deploying the client-side components. See the corresponding reference link for the detailed procedures.

Procedure	Reference
Optional: If you want to enforce two-factor authentication, you must install the required third-party drivers and libraries.	<ul style="list-style-type: none"> • For detailed and up-to-date installation instructions, see the respective product documentation.
Install AccessAgent on all employee client workstations and Citrix/Terminal Server that require single sign-on services. <ul style="list-style-type: none"> • For enterprise deployments, you can deploy AccessAgent on Windows workstations through a software provisioning solution. For example: Tivoli Provisioning Manager or Active Directory Group Policy Object (AD GPO). 	<ul style="list-style-type: none"> • Chapter 7, “Installing the AccessAgent,” on page 111
(For Windows XP Professional only) Install the Microsoft .NET Framework Version 2.0 Redistributable package before you install AccessStudio.	<ul style="list-style-type: none"> • Go to the Microsoft website at www.microsoft.com and search for “.NET Framework 2.0 download”.
To manage single sign-on profiles, install AccessStudio on an Administrator workstation. <ul style="list-style-type: none"> • Use AccessStudio to create and upload AccessProfiles for supported authentication services and applications to provide single sign-on. 	<ul style="list-style-type: none"> • Chapter 8, “Installing the AccessStudio,” on page 117
Verify the files and registry entries to ensure that the installation is successful.	<ul style="list-style-type: none"> • “Verifying files and registry entries” on page 115

Chapter 7. Installing the AccessAgent

You can install the AccessAgent interactively or silently. The interactive installation method guides you through the installation. The silent installation option enables standardized, repeatable installations across many client computers.

Before you begin

If you are using a load balancer, provide the URL of the load balancer as your target URL for each AccessAgent deployment.

If you are not using a load balancer, provide the URL of the IBM HTTP Server. If you are using a remote web server, ensure that the web server URL is reachable.

Remember:

- In production deployments, do not install the AccessAgent client on the IMS Server host. You deploy AccessAgent separately on client workstations that require single sign-on.
- Antivirus software can interfere with AccessAgent or the IMS Server. For more information, see the *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide*.

For more information, see the following topics:

- System requirements. See “Hardware and software requirements” in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.
- “Installing the AccessAgent (Setup.exe)”
- “Installing the AccessAgent (MSI package)” on page 112
- “Installing the AccessAgent silently (command-line)” on page 113
- “Verifying files and registry entries” on page 115
- “Verifying the ESSO Network Provider” on page 116

Installing the AccessAgent (Setup.exe)

For individual deployments, use the Setup.exe file to install AccessAgent on the user computer.

Before you begin

- Note the product description or name listed on the Passport Advantage “Find downloads & media” page.
- Ensure that you have administrator privileges.
- Optional: Install Mozilla Firefox.

For single sign-on support in the Mozilla Firefox browser, you must always install Mozilla Firefox first before running the AccessAgent installer. If AccessAgent is installed on a computer without Mozilla Firefox, you cannot experience single sign-on in Mozilla Firefox when the browser is installed later.

About this task

When you use Setup.exe to install AccessAgent, you can select the preferred setup language. You can also specify the IMS Server name and port number during installation.

Procedure

1. Double-click setup.exe from the installation package.
2. Select the product for which you have a license to install.
 - IBM Security Access Manager for Enterprise Single Sign-On Standard
This package offers single sign-on, strong authentication, session management, centralized logging, and reporting.
 - IBM Security Access Manager for Enterprise Single Sign-On Suite
This package offers one time password support, AccessAgent plug-ins, Web single sign-on, and remote access through Web Workplace, custom tracking, and IAM Integration in addition to the Standard package.
3. Click **Next**.
4. Select **I accept the terms in the license agreement**.
5. Click **Next**. The installation directory is displayed. By default, AccessAgent is installed in C:\Program Files\IBM\ISAM ESS0\AA.

Note: To select a different location, click **Browse** and select another folder.

If you specify an installation path that is too long, the path might appear in a truncated form. However, this truncated form does not affect the actual installation location.

6. Click **Next**.
7. In the Server name field, enter the IMS Server name. The default port setting is 80.
8. Click **OK**. AccessAgent is configured successfully.
9. Click **Finish**. You are prompted to restart the computer.
10. Click **Yes**.

Results

You installed AccessAgent.

What to do next

After the computer restarts, and the logon screen is displayed, verify that you can sign in and log on. You can also verify the files and registry entries to ensure that the installation is successful.

Installing the AccessAgent (MSI package)

For large-scale deployments, use the MSI package to install the AccessAgent on several computers simultaneously.

Before you begin

- Ensure that you have administrator privileges.
- For single sign-on support in the Mozilla Firefox browser, you must always install Mozilla Firefox first before running the AccessAgent installer. If

AccessAgent is installed on a computer without Mozilla Firefox, you cannot experience single sign-on in Mozilla Firefox if the browser is installed later.

About this task

When you use the MSI package to install AccessAgent, the English language is used by default in the installation program and in the AccessAgent interface. To deploy AccessAgent in a different language, you can apply a language transform.

To predefine the IMS Server name, you can specify the IMS Server in the SetupHlp.ini file. See Chapter 9, "Preparing an installation package to install on multiple PCs," on page 121.

Procedure

1. Double-click ISAM ESS0 AccessAgent.msi from the installation package. You are prompted to confirm whether to run the file.
2. Click **Run**. The IBM Security Access Manager for Enterprise Single Sign-On AccessAgent installation program wizard starts.
3. Click **Next**.
4. Select **I accept the terms in the license agreement**.
5. Click **Next**. The installation directory displays. By default, AccessAgent is installed in C:\Program Files\IBM\ISAM ESS0\AA.

Note: To select a different location, click **Browse** and select another folder.

6. Click **Next**. AccessAgent is configured successfully.
7. Click **Finish**. You are prompted to restart the computer.
8. Click **Yes** to restart the computer. You must restart the computer before you can sign up for a single sign-on account or log on to the Wallet.
9. For Microsoft Windows Vista computers, do one of the following steps:
 - a. On Active Directory servers, if the **Interactive logon: Do not require Ctrl+Alt+Delete** security option is not enabled, you must enable it. AccessAgent automatically attempts to enable this security option during the installation unless a group policy permission denies the change from being applied.
 - b. If **Interactive logon: Do not require Ctrl+Alt+Delete** is not enabled, press **Ctrl+Alt+Delete** to open the AccessAgent logon screen.

Results

You installed AccessAgent successfully.

What to do next

After the computer restarts and when the logon screen is displayed, verify that you can sign in with a valid user account successfully on the IMS Server. You can also verify the files and registry entries to ensure that the installation is successful.

Installing the AccessAgent silently (command-line)

To do a silent installation, use the **/quiet** parameter with the **msiexec** command.

About this task

The **msiexec** command uses parameters to give the MSI-based installer some or all of the information that would normally be specified interactively in an installer. You can include parameters in the command-line interface to use a language transform and a response file.

If you specify a parameter that exists in both the command line and in the response file, the setting in the response file, `SetupHlp.ini` takes precedence.

Note: Including the response file, `SetupHlp.ini`, as a parameter is optional. In a default installation, the MSI-based installer locates the `SetupHlp.ini` response file automatically in the `\Config` directory.

Important: If you are using the **msiexec** command with the **/quiet** parameter, specify the IMS Server location value **ImsServerName** in the `SetupHlp.ini` response file.

Note: For more information about the **msiexec** command-line tool, go to the Microsoft website at www.microsoft.com and search for "msiexec command-line options".

Procedure

1. Open the `SetupHlp.ini` response file from the `\Config` directory.
2. In the `SetupHlp.ini` response file, specify the following required parameters for a silent installation:

ImsServerName

Specify the IMS Server location. For example: `mylb.example.com`. For more information, see "Setting the IMS Server location manually (response file)" on page 128.

PriceLevel

Specify the product edition that you licensed with the **PriceLevel** parameter. For example: `Suite`.

ImsConfigurationPromptEnabled

Verify that the value for the **ImsConfigurationPromptEnabled** parameter is 0. The default value is 0.

Note: If the **ImsConfigurationPromptEnabled** value is set to 1, the installation is not silent. The IMS Server configuration prompt is displayed even when you include the **/quiet** parameter. Parameters in the response file always take precedence over any parameters in the command-line interface.

3. On the **Start** menu, click **Run**.
4. In **Open**, type `cmd`.
5. In the command prompt window, type the **msiexec** command with the following parameters (use without line breaks). For example:

```
msiexec /i "<path>\ISAM ESS0 AccessAgent.msi" /quiet  
TRANSFORMS="1033.mst"
```

Where:

```
/i "<path>\ISAM ESS0 AccessAgent.msi"  
Installs AccessAgent by using the specified .msi.
```

/quiet

Specifies a silent installation.

TRANSFORMS="1033.mst"

Specifies that the installation is in U.S. English. To apply a different language transform (.mst file) to the package, see “Including support for additional languages” on page 126.

Results

You installed AccessAgent silently as a background process. By default, the installation process created a log file in *%temp%\AAInstaller.log*.

Verifying files and registry entries

After you install the AccessAgent and the AccessStudio, verify that all the program files and registry entries are successfully installed on your computer.

AccessAgent and AccessStudio program files

By default, the AccessAgent and AccessStudio program files are stored in C:\Program Files\IBM\ISAM ESS0\AA. The following subfolders and files are created after you install AccessAgent and AccessStudio.

- C:\Program Files\IBM\ISAM ESS0\AA
- C:\Program Files\IBM\ISAM ESS0\AA\ECSS\AccessStudio
- C:\Program Files\IBM\ISAM ESS0\AA\Cryptoboxes
- C:\Program Files\IBM\ISAM ESS0\AA\Data
- C:\Program Files\IBM\ISAM ESS0\AA\ECSS
- C:\Program Files\IBM\ISAM ESS0\AA\ECSS\Firefox_ext
- C:\Program Files\IBM\ISAM ESS0\AA\ECSS\Firefox_xpcom
- C:\Program Files\IBM\ISAM ESS0\AA\GSKit
- C:\Program Files\IBM\ISAM ESS0\AA\License
- C:\Program Files\IBM\ISAM ESS0\AA\ECSS\JavaSupport
- C:\Program Files\IBM\ISAM ESS0\AA\Logs
- C:\Program Files\IBM\ISAM ESS0\AA\ECSS\SimpleToStateSupport
- C:\Program Files\IBM\ISAM ESS0\AA\TSSDK

AccessAgent and AccessStudio registry entries

AccessAgent and AccessStudio registry entries are stored in the [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESS0] key. Default registry values are automatically populated upon installation.

- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESS0\AccessStudio]
- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESS0\ECSS]
- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESS0\ECSS\DeploymentOptions]
- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESS0\ECSS\Temp]
- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESS0\DeploymentOptions]
- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESS0\IMSService\DefaultIMSSettings]
- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESS0\IMSService\GlobalIMSSettings]
- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESS0\AccessAgent\Integration]
- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESS0\Internal]

- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\LastLogin]
- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\SOCIAccess]
- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\Temp]

Verifying the ESSO Network Provider

The ESSO Network Provider captures the user credentials entered in the Microsoft GINA. The ESSO Network Provider uses these credentials to log on the user to IBM Security Access Manager for Enterprise Single Sign-On. Ensure that the ESSO Network Provider works.

The ESSO Network Provider is installed and working if:

- There is a [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EnNetworkProvider].
- The registry key ProviderOrder in [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order] contains the value EnNetworkProvider. If it is not yet in the **Value data** field, add it.

Note: Do not include a comma if there are no preceding entries.

- The EnNetworkProvider.dll file is located in the product installation directory.

Chapter 8. Installing the AccessStudio

Install the AccessStudio on one computer or configure a silent deployment for multiple client computers.

See the following topics for more information:

- Requirements for AccessStudio. See “Hardware and software requirements” in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.
- “Installing the AccessStudio (Setup.exe)”
- “Installing the AccessStudio (MSI package)” on page 118
- “Installing the AccessStudio silently (command-line)” on page 119

Installing the AccessStudio (Setup.exe)

You can install the AccessStudio on designated client computers to create additional AccessProfiles. For individual deployments, use the Setup.exe file to install the AccessStudio on the user computer.

Before you begin

- Note the product description or name listed on the Passport Advantage "Find downloads & media" page.
- Ensure that you have administrator privileges.
- For Windows XP Professional only: Ensure that Microsoft .NET Framework Version 2.0 is installed.
To download, go to the Microsoft website at www.microsoft.com and search for “.NET Framework 2.0 download”.
- Install the AccessAgent.

About this task

When you use Setup.exe to install AccessStudio, you can select the preferred setup language.

Procedure

1. Double-click setup.exe from the installation package.
2. Select a language from the list. Product License Validation is displayed.
3. Click **OK**.
4. Select the product for which you have a license to install.
 - IBM Security Access Manager for Enterprise Single Sign-On Standard
This package offers strong authentication, session management and centralized logging and reporting in addition to single sign-on.
 - IBM Security Access Manager for Enterprise Single Sign-On Suite
This package offers one time password support, AccessAgent plug-ins, Web single sign-on, and remote access through Web Workplace, custom tracking and IAM Integration in addition to the Standard package.
5. Click **Next**.
6. Select **I accept the terms in the license agreement**.

7. Click **Next**. The installation directory is displayed.
 - For Windows 64-bit platforms, the default, AccessStudio installation directory is C:\Program Files (x86)\IBM\ISAM ESS0\AA\ECSS.
 - For Windows 32-bit platforms, the default, AccessStudio installation directory is C:\Program Files\IBM\ISAM ESS0\AA\ECSS\AccessStudio.

Note: To select a different location, click **Browse** and select another folder.

8. Click **Next**. AccessStudio is installed successfully.
9. Click **Finish**.

Results

You successfully installed AccessStudio.

What to do next

Verify that you can start AccessStudio, create, and deploy an AccessProfile on the IMS Server host. See *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide*.

Verify the files and registry entries for the AccessStudio.

Installing the AccessStudio (MSI package)

With the MSI package file, you can install the AccessStudio on designated client computers to create additional AccessProfiles. For large-scale deployments, use the MSI package to install AccessStudio on the several user computers simultaneously. Learn the prerequisites and procedure for installing the AccessStudio through the MSI package file.

Before you begin

- For Windows XP only: Ensure that Microsoft .NET Framework Version 2.0 is installed.

To download this software, go to the Microsoft website at www.microsoft.com and search for “.NET Framework 2.0 download”.
- Install the AccessAgent.
- Ensure that you have administrator privileges.

Note: To customize the .msi deployment package, see Chapter 9, “Preparing an installation package to install on multiple PCs,” on page 121.

Procedure

1. Double-click ISAM ESS0 AccessStudio.msi from the installation package. You are prompted to confirm whether to run the file.
2. Click **Run**. The IBM Security Access Manager for Enterprise Single Sign-On AccessStudio installation program wizard is started.
3. Select **I accept the terms in the license agreement**.
4. Click **Next**. AccessStudio is installed successfully.
5. Click **Finish**.

Results

You successfully installed AccessStudio.

What to do next

Verify that you can start AccessStudio, create, and deploy an AccessProfile on the IMS Server host. See *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide*.

Verify the files and registry entries for the AccessStudio.

Installing the AccessStudio silently (command-line)

To do a silent installation, use the **/quiet** parameter with the **msiexec** command. This means that you can install the AccessStudio on a computer without any interaction.

About this task

The **msiexec** command uses parameters to give the MSI-based installer some or all of the information that would normally be specified interactively in an installer. You can include parameters in the command-line interface to apply a specific language transform.

Note: For more information about the **msiexec** command-line tool, go to the Microsoft website at www.microsoft.com and search for the “msiexec command-line options”.

Procedure

1. Open the command prompt.
2. In the command prompt window, type the **msiexec** command with the following parameters (use without line breaks). For example:

```
msiexec /i "<path>\ISAM ESSO AccessStudio.msi" /quiet  
TRANSFORMS="1033.mst" PRICE_LEVEL="Standard"
```

Where:

/i "<path>\ISAM ESSO AccessStudio.msi"

Installs AccessStudio by using the specified .msi. This is a required parameter.

/quiet

Specifies a silent installation. This is a required parameter.

TRANSFORMS="1033.mst"

Specifies that the installation is in U.S. English. To apply a different language transform (.mst file) to the package, see “Including support for additional languages” on page 126. If you do not include the **TRANSFORMS** parameter, the default language is U.S. English. This is an optional parameter.

PRICE_LEVEL="Standard"

Specifies that the licensed edition of AccessStudio is the Standard edition. To install the Suite edition, type "Suite". This is a required parameter.

Results

You installed AccessStudio silently as a background process. By default, the installation process created a log file in `c:\AAInstaller.log`.

Chapter 9. Preparing an installation package to install on multiple PCs

You can customize the installers to do a remote or silent deployment of AccessAgent and AccessStudio on multiple computers.

Before you distribute the packages on multiple workstations, you can customize and preconfigure specific deployment attributes for each client.

You can customize the deployment package attributes by:

- “Setting the AccessAgent installation path” on page 126.
- “Preparing and installing a prepackaged Wallet” on page 122.
- “Including support for additional languages” on page 126.
- “Setting the IMS Server location manually (response file)” on page 128.

See the following topics for information about response file attributes and the different ways to specify the IMS Server location:

- “Response file parameters (SetupHlp.ini)” on page 123.
- “Ways of setting the IMS Server location” on page 127.

For additional AccessAgent features that you can tailor for your organization, see the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

Remote software distribution methods

You can do a push-installation of the AccessAgent and AccessStudio MSI packages on target Windows workstations. Typical software distribution systems include Microsoft Active Directory Group Policy Object (AD GPO) and application provisioning software like Tivoli Provisioning Manager.

To distribute the client software on multiple workstations with:

- Active Directory Group Policy Object: Go to the Microsoft website at <http://www.microsoft.com> and search for “Group Policy install software remotely”.
- Application provisioning software: See your vendor provided documentation.

Locale and language support

To apply the appropriate locale and language support during installation, use the included transforms (.mst file) with the .msi file before deploying.

IBM Security Access Manager for Enterprise Single Sign-On already includes language transforms for AccessAgent and AccessStudio.

The Windows Installer package uses transforms to add support for other languages. Typically, administrators can create transforms to restrict which features can be installed or customized by users.

Note: Transforms do not actually modify the source image. A transform is a file containing a series of modifications that are applied to the base MSI database, for example, ISAM ESS0 AccessAgent.msi or ISAM ESS0 AccessStudio.msi at installation time.

Silent installation configuration

You can customize the default behavior of the installation by specifying parameters in the SetupHlp.ini file. The SetupHlp.ini file also lets Windows administrators predefine the parameters that can be used by ISAM ESS0 AccessAgent.msi for a silent installation. By predefining the attributes, administrators can simplify large-scale client deployments and avoid possible deployment issues by specifying the correct host name connections. For more information, see “Response file parameters (SetupHlp.ini)” on page 123.

Preparing and installing a prepackaged Wallet

Before you install AccessAgent on multiple computers, you can prepackage a Wallet first. Prepackaging the Wallet can reduce the load on the IMS Server when new Wallets are downloaded simultaneously by clients in large-scale deployments.

Before you begin

- Prepare a client computer for installing the AccessAgent. This client computer is the staging workstation.
- Ensure that the IMS Server is installed and configured.

About this task

Configuring a prepackaged Wallet is useful for large-scale deployments of AccessAgent.

When AccessAgent is installed on a new workstation without cached Wallets on the computer, AccessAgent downloads a fresh system Wallet from the IMS Server.

By including a prepackaged Wallet, AccessAgent downloads only incremental updates from the IMS Server instead of downloading a fresh system Wallet.

Note: If the target machine has earlier versions of AccessAgent, the prepackaged Wallet is not applied. The Wallet from the earlier installation is copied to the new installation.

Procedure

1. Prepare the prepackaged Wallets on the staging workstation.
 - a. Install the AccessAgent on the client computer. This client computer is the staging workstation.
 - b. Ensure that the AccessAgent connects to the production IMS Server.
The AccessAgent client downloads the system data from the IMS Server.
The system Wallets are created.
2. Copy the generated Wallet file to the AccessAgent installer.

On the staging workstation, copy the Wallet files from:	To the AccessAgent 8.2 installer:
<p><AccessAgent install path>\Cryptoboxes\Wallets</p> <p>For example:</p> <p>C:\Program Files\IBM\ISAM ESSO\Cryptoboxes\Wallets</p>	<p><AccessAgent installer location>\<aa version number>\Config\Cryptoboxes\Wallets</p> <p>You must create the Cryptoboxes\Wallets folders manually.</p> <p>For example:</p> <p>c:\images\aa-<version number>\Config\Cryptoboxes\Wallets</p>

3. Install the new AccessAgent installation program on all other client computers.

Note: If the target machine has earlier versions of AccessAgent, the prepackaged Wallet is not applied. The Wallet from the earlier installation is copied to the new installation.

Results

You prepackaged a Wallet with the AccessAgent installation program.

Response file parameters (SetupHlp.ini)

You can specify the installed features, installation directories, target server, and single sign-on options in the Setuphlp.ini response file. Learn more about the contents of the Setuphlp.ini file

The options in SetupHlp.ini are divided into the following categories:

Setup time only options

This section contains a list of options that you cannot change after installation.

Setup time and runtime options that map to multiple registry values each

This section contains a list of options that you can change after installation by modifying registry values. Each option is mapped to several registry values.

Setup time and runtime options that map to one registry value each

This section contains a list of options that you can change after installation by modifying registry values. Each option is mapped to a registry value.

Dependency URLs

The installation program directs you to these URLs if the required installation components are missing. For the list of included URLs, check the response file in your installation package.

Setup time only options

This section contains a list of options that you cannot change after installation.

Option Name	Value	Description
AAInstallDir	AAInstallDir =C:\Program Files\IBM\ISAM ESSO\AA	Specify installation directories.

Option Name	Value	Description
FirstSyncMaxRetries	Default: 1	Specify the number of attempts if the first synchronization fails during installation.
FirstSyncRetryIntervalMins	Default: 1	Time interval, specified in minutes, between each attempt during installation.
GinaWhiteList	msgina, engina.dll, nwgina.dll	<p>List of GINAs that are currently supported by IBM Security Access Manager for Enterprise Single Sign-On.</p> <p>AccessAgent is not installed if you are using a GINA that is not in this list.</p> <p>During the installation, a prompt displays to determine whether you want to replace the GINA in this list.</p> <p>For a silent installation, you must configure the EnginaEnabled option.</p> <p>Note:</p> <ul style="list-style-type: none"> • If you want to use a GINA not included in this list, test the new GINA against AccessAgent. Then add the new .DLL file to this list. • Use a comma to separate the values.
EnginaEnabled	1 0 (default: 1)	<p>Whether to replace the current GINA with EnGINA.</p> <p>Note:</p> <ul style="list-style-type: none"> • For AccessAgent version 3.3.0.0 and later, the behavior of this option is consistent for workstations, Terminal Servers, and Citrix Servers. • For Citrix Servers, use option 0.
PriceLevel	Standard Suite	Specifies the product license level.
RebootEnabled	1 0 (default: 1)	Whether to trigger a computer reboot after setup.
RebootConfirmationEnabled	1 0 (default: 1)	Whether to confirm with the user before rebooting. Effective only if RebootEnabled=1.
EnginaConflictPromptEnabled	1 0 (default: 1)	If there is a GINA conflict, whether a prompt is displayed.
UsbKeyPromptEnabled	1 0 (default: 1)	Whether to prompt user to insert USB Key, if a USB Key is not already inserted during installation time.
ImsConfigurationEnabled	1 0 (default: 1)	Whether to configure the default IMS Server settings and install certificates from the IMS Server during setup.
ImsConfigurationPromptEnabled	1 0 (default: 0)	Whether to prompt the user for the default IMS Server entry, even if it is already correctly configured. Effective only if ImsConfigurationEnabled=1.
InstallTypeGpo	1 0 (default: 0)	Whether to suppress all prompts and write to a log. Required for AD GPO installation.
EncentuateNetworkProviderEnabled	1 0 (default: 0)	Whether to enable Encentuate Network Provider during an AccessAgent installation.
EncentuateCredentialProviderEnabled	1 0 (default: 1)	Whether to install the IBM Security Access Manager for Enterprise Single Sign-On Vista Credential Provider.

Option Name	Value	Description
ConsoleAppSupportEnabled	1 0 (default: 0)	Whether to enable IBM Security Access Manager for Enterprise Single Sign-On Console Hook Loader. Note: <ul style="list-style-type: none"> The Console Hook Loader is disabled by default. To enable console application support, set the value to 1. Alternatively, you can run <code>InstallConsoleSupport.vbs</code> located in the <code><AccessAgent installation directory></code> after installation.
ResetBioAPIPermissions	1 0 (default: 0)	Whether to reset BioAPI Permissions.
DisableWin7CAD	1 0 (default: 1)	Whether to disable Ctrl+Alt+Del in Windows Vista/Windows 7.
RemoveWallet	1 0 (default: Not defined)	Whether to remove Wallet during uninstallation. For uninstalling silently, set <code>RemoveWallet=1</code> if it is not configured.
JVMInstallationDirectories	<JVM Directory 1> <JVM Directory 2> <JVM Directory 3>	JVM directories for which to enable Java automatic sign-on support. Each directory must be separated by a vertical bar. There must be no space in between 2 JVM directories. For example: <ul style="list-style-type: none"> C:\Program Files\Java\jre1.5.0_11 C:\TAM E-SSO\j2re1.4.1 Specifically for JVM version 1.2 or later.
OldJVMInstallationDirectories	<JVM Directory 1> <JVM Directory 2> <JVM Directory 3>	JVM directories for which to enable Java automatic sign-on support. Each directory must be separated by a vertical bar. There must be no space in between 2 JVM directories. For example: <ul style="list-style-type: none"> C:\Program Files\Java\jre1.5.0_11 C:\TAM E-SSO\j2re1.4.1 Specifically for JVM version 1.1

Setup time and run time options that map to multiple registry values

This section contains a list of options that you can change after installation by modifying registry values. Each option is mapped to several registry values.

Option Name	Value	Description
ImsSecurePortDefault	default: 443	Default secure port number for the default IMS Server.
ImsDownloadPortDefault	default: 80	Default download port number for the default IMS Server.
ImsDownloadProtocolDefault	default: http://	Default download protocol for the default IMS Server.

Setup time and run time options that map to one registry value

This section contains a list of options that you cannot change after installation.

Option Name	Value	Description
WalletTypeSupported	0 1 2 (default: 0)	Supported Wallet types. <ul style="list-style-type: none">• 0 - IMS Server only• 1 - Non IMS Server only• 2 - Both IMS Server and non-IMS Server
ImsAddressPromptEnabled	1 0 (default: 0)	Whether to prompt up the user for an IMS Server address during signup, even if the IMS Server address specified in ImsServerName is correct.
ImsServerName	<SAM ESSO IMS Server>	Actual host name of the IMS Server.

Setting the AccessAgent installation path

You can set the installation path in the ISAM ESSO AccessAgent.msi file for silent installations. You do this task before the installation.

Before you begin

Ensure that you have the Orca MSI Database editor. The Orca editor is part of the Microsoft Windows Installer SDK.

About this task

The Orca database editor is a table-editing tool for editing .msi files.

Note: For more information about installing and using the Orca database editor, go to the Microsoft website at <http://www.microsoft.com> and search for “Orca editor”.

Procedure

1. Launch the Orca editor.
2. Open the ISAM ESSO AccessAgent.msi file.
3. Click the **Property** table.
4. Specify the value for **CONFIG_PARAMS_BASE_PATH**.

Including support for additional languages

You can include support for additional languages before you start the installation. To add language support, apply language transforms to the ISAM ESSO AccessAgent.msi file or to the ISAM ESSO AccessStudio.msi file.

Use the Active Directory Group Policy Object options to apply language transforms. The AccessAgent and AccessStudio components are supplied with transform files in each components folder for the installer.

Transforms have a file extension of .mst. Select the language transform (.mst) file based on the following locale ID or LCID values. The transform file uses the decimal form of the LCID.

Locale Description	Language Transform	LCID	RFC1766 short string
Arabic	1025.mst	0x0401	ar-sa
Brazilian Portuguese	1046.mst	0x0416	pt-br
Chinese - Simplified Chinese	2052.mst	0x0804	zh-cn
Chinese - Traditional Chinese	1028.mst	0x0404	zh-tw
Czech	1029.mst	0x0405	cs
Danish	1030.mst	0x0406	da
Dutch - Netherlands	1043.mst	0x0413	nl
English - United States	1033.mst	0x0409	en-us
Finnish	1035.mst	0x040b	fi
French - France	1036.mst	0x040c	fr
German - Germany	1031.mst	0x0407	de
Hebrew	1037.mst	0x040d	he
Hungarian	1038.mst	0x040e	hu
Italian - Italy	1040.mst	0x0410	it
Japanese	1041.mst	0x0411	ja
Korean	1042.mst	0x0412	ko
Polish	1045.mst	0x0415	po
Russian	1049.mst	0x0419	ru
Spanish - Spain	1034.mst	0x040a	es

Ways of setting the IMS Server location

There are four ways to set the IMS Server location manually for AccessAgent.

Verify the host connections to avoid common deployment problems between the AccessAgent client and the IMS Server. Use the **ping** command to ensure that the connections between hosts can be resolved.

Ensure that you complete the following tasks before you set the IMS Server location:

- IBM HTTP Server is configured and started.
- WebSphere Application Server is configured and started.
- IMS Server application on WebSphere Application Server is started.
- Database server is started.
- Directory server is started.

Important: When you change the IMS Server location, delete the **Cryptoboxes** folder located in C:\Program Files\IBM\ISAM ESS0\AA\ . Delete the folder to avoid mixing policies from different IMS Servers. You can also back up the folder before you delete it.

To set or change the IMS Server host for AccessAgent, choose one of the following methods:

- “Setting the IMS Server location manually (registry)” on page 128

- “Setting the IMS Server location manually (menu shortcut)”
- “Setting the IMS Server location manually (response file)”
- “Setting the IMS Server location manually (command-line)”

Setting the IMS Server location manually (response file)

To prepare AccessAgent for a silent installation, specify the IMS Server host in the SetupHlp.ini response file.

Procedure

1. Open the Config folder. For example: c:\Program Files\IBM\ISAM ESSO\
2. Double-click SetupHlp.ini to open the file.
3. Search for IMSServerName = <SAM E-SSO IMS Server>.
4. Replace <SAM E-SSO IMS Server> with the name of your IMS Server. For example: IMSServerName = IMSServer.example.com.
5. Save the file.
6. Restart the computer.

Setting the IMS Server location manually (menu shortcut)

Use the installed program shortcuts in the **Start** menu to set the IMS Server location for AccessAgent.

Procedure

1. Click **Start > All Programs > ISAM ESSO AccessAgent > Set IMS Server Location**.
2. Specify the IMS Server host. For example: imssvr.example.com
3. Click **OK** to finish.

Setting the IMS Server location manually (command-line)

Use the **SetupCertDlg** command to set the IMS Server host manually.

Procedure

1. Browse to the <aa_home> installation directory. For example: C:\Program Files\IBM\ISAM ESSO\AA
2. Run SetupCertDlg.exe

Setting the IMS Server location manually (registry)

Use the Registry Editor to set the IMS Server host. You specify the value in the **ImServerName** attribute in the Windows registry.

Procedure

1. Open the registry editor.
 - a. Select **Start > Run**.
 - b. Type regedit.
2. Locate the registry key HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\IMSService\DefaultIMSSettings.
3. In the **ImServerName** attribute, type the IMS Server host name. For example: imssvr.example.com.
4. Restart the computer.

Part 3. Upgrading

You can upgrade IBM Security Access Manager for Enterprise Single Sign-On from an earlier version.

Chapter 10. IMS Server upgrade road map

The IMS Server upgrade road map contains the corresponding procedures for each upgrade scenario. Select the road map applicable to your IMS Server deployment.

The following sections are the road maps for upgrading the IMS Server:

- “Upgrading IMS Server 8.0.1 for a stand-alone deployment”
- “Upgrading IMS Server 8.0.1 for a network deployment (cluster)” on page 134
- “Upgrading IMS Server 8.1 for a stand-alone deployment” on page 137
- “Upgrading IMS Server 8.1 for a network deployment (cluster)” on page 138
- “Upgrading IMS Server 3.6 or 8.0” on page 139

Note: If you are upgrading to IMS Server version 3.6 or version 8.0, contact IBM Services for information about upgrading to version 8.2.

Upgrading IMS Server 8.0.1 for a stand-alone deployment

Upgrading a stand-alone IMS Server version 8.0.1 to IMS Server version 8.2 involves the installation and configuration of other middleware. Use the IMS Server upgrade road map to avoid confusion on the topics and procedures that you must follow to complete the upgrade to version 8.2.

Procedure	Reference
Make sure that IMS Server 8.0.1 is installed and it works.	
Stop IMS Server 8.0.1 before you configure the middleware. In the Windows Services Management Console, be sure to set the IMS Server 8.0.1 Windows server service Startup type to Manual .	
Back up IMS Server and its database. <ul style="list-style-type: none">• Back up your IMS Server 8.0.1 installation folder.• Back up the IMS Server database.	Note: To back up other supported databases, see your database documentation. <ul style="list-style-type: none">• “Backing up the database in DB2” on page 189

Procedure	Reference
<p>Prepare the WebSphere Application Server:</p> <ul style="list-style-type: none"> • Install WebSphere Application Server. • Install the WebSphere update installer. • Install the WebSphere Application Server fix pack. 	<p>For the supported WebSphere Application Server versions, see “Hardware and software requirements” in the <i>IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide</i>.</p> <p>For sample instructions, see the following topics:</p> <ul style="list-style-type: none"> • “Preparing the WebSphere Application Server” on page 20 • “Installing the WebSphere update installer” on page 22 • “Installing WebSphere Application Server fix packs” on page 23 <p>WebSphere Application Server documentation:</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp <p>Important: This guide provides instructions about preparing the WebSphere Application Server for the IMS Server. For detailed and up-to-date installation instructions, see the WebSphere Application Server documentation.</p>
<p>Prepare the IBM HTTP Server:</p> <ul style="list-style-type: none"> • Install the IBM HTTP Server. • Install IBM HTTP Server fix pack by using the WebSphere Update Installer. 	<p>For the supported IBM HTTP Server versions, see “Hardware and software requirements” in the <i>IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide</i>.</p> <p>For sample instructions, see the following topics:</p> <ul style="list-style-type: none"> • “Preparing the IBM HTTP Server” on page 24 • “Installing the IBM HTTP Server fix packs” on page 27 <p>IBM HTTP Server documentation:</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/ihs/ihs/tihs_installihs.html <p>Important: This guide provides instructions about preparing the IBM HTTP Server. For detailed and up-to-date installation instructions, see the IBM HTTP Server documentation.</p>
<p>Create a stand-alone WebSphere Application Server profile.</p> <p>Note: Ensure that the WebSphere Application Server stand-alone profile is started.</p>	<ul style="list-style-type: none"> • “Creating stand-alone profiles (Profile Management tool) for x86 architectures” on page 53 • “Creating stand-alone profiles (command-line) for x86 or x64 architectures” on page 54

Procedure	Reference
Configure the WebSphere Application Server. <ul style="list-style-type: none"> • Configure the JVM heap size memory. • Verify the Windows service. 	For sample instructions, see the following topics: <ul style="list-style-type: none"> • “Configuring the heap size for the application server” on page 56 • “Verifying the Windows service for WebSphere Application Server” on page 56 WebSphere Application Server documentation: <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp
Configure the IBM HTTP Server: <ul style="list-style-type: none"> • Configure the IBM HTTP Server plug-in and secure the connection. • Enable SSL directives on IBM HTTP Server. 	For sample instructions, see the following topics: <ul style="list-style-type: none"> • “Configuring the IBM HTTP Server plug-in and securing the connection (stand-alone)” on page 61 • “Enabling SSL directives on the IBM HTTP Server” on page 64 IBM HTTP Server documentation: <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/ihs/ihs/tihs_installihs.html <p>Important: This guide provides instructions about preparing the IBM HTTP Server. For detailed and up-to-date installation instructions, see the IBM HTTP Server documentation.</p>
Install the IMS Server on the WebSphere Application Server.	“Installing the IMS Server with the installer for an upgrade” on page 141
Verify the IMS Server deployment on the WebSphere Application Server.	“Verifying the IMS Server deployment on the WebSphere Application Server” on page 36
Upgrade the IMS Server settings.	“Upgrading configurations from 8.0.1 to 8.2” on page 144
Restart the WebSphere Application Server.	<ul style="list-style-type: none"> • “Stopping the WebSphere Application Server on Windows” on page 195 • “Starting the WebSphere Application Server on Windows” on page 193
Update the ISAMESSOIMS module mapping to forward connection requests.	“Updating the ISAMESSOIMS module mapping for connection request forwarding” on page 72
Configure the IBM HTTP Server to use the old IMS Server SSL certificate.	“Configuring the SSL certificate after an upgrade” on page 145
Restart the WebSphere Application Server.	For example steps, see: <ul style="list-style-type: none"> • “Starting the WebSphere Application Server on Windows” on page 193 • “Stopping the WebSphere Application Server on Windows” on page 195

Procedure	Reference
Verify whether the upgrade is successful.	“Verifying a successful upgrade” on page 147

To upgrade the AccessAgent clients to 8.2, see “Upgrading the AccessAgent” on page 146.

To upgrade the AccessStudio clients to 8.2, see “Upgrading the AccessStudio” on page 147.

Upgrading IMS Server 8.0.1 for a network deployment (cluster)

Upgrading a clustered IMS Server version 8.0.1 to IMS Server version 8.2 involves the installation and configuration of other middleware. Use the IMS Server upgrade roadmap to avoid confusion on the topics and procedures that you must follow to complete the upgrade to version 8.2.

Procedure	Reference
Make sure IMS Server 8.0.1 is installed and it works.	
Before you begin the upgrade: 1. Stop the IMS Server 8.0.1. 2. Set the IMS Server Windows service Startup type to Manual .	
Back up the IMS Server and the database: <ul style="list-style-type: none"> • Back up your IMS Server 8.0.1 installation folder. • Back up the IMS Server database. 	<p>Note: To back up other supported databases, see your database documentation.</p> <p>For example:</p> <ul style="list-style-type: none"> • “Backing up the database in DB2” on page 189

Procedure	Reference
<p>Prepare the WebSphere Application Server:</p> <ul style="list-style-type: none"> • Install WebSphere Application Server. • Install the WebSphere update installer. • Install the WebSphere Application Server fix pack. 	<p>For the supported WebSphere Application Server versions, see “Hardware and software requirements” in the <i>IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide</i>.</p> <p>For sample instructions, see the following topics:</p> <ul style="list-style-type: none"> • “Preparing the WebSphere Application Server” on page 20 • “Installing the WebSphere update installer” on page 22 • “Installing WebSphere Application Server fix packs” on page 23 <p>WebSphere Application Server documentation:</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp <p>Important: This guide provides instructions about preparing the WebSphere Application Server for the IMS Server. For detailed and up-to-date installation instructions, see the WebSphere Application Server documentation.</p>
<p>Prepare the IBM HTTP Server:</p> <ul style="list-style-type: none"> • Install the IBM HTTP Server. • Install IBM HTTP Server fix pack by using the WebSphere Update Installer. 	<p>For the supported IBM HTTP Server versions, see “Hardware and software requirements” in the <i>IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide</i>.</p> <p>For sample instructions, see the following topics:</p> <ul style="list-style-type: none"> • “Preparing the IBM HTTP Server” on page 24 • “Installing the IBM HTTP Server fix packs” on page 27 <p>IBM HTTP Server documentation:</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/ihs/ihs/tihs_installihs.html <p>Important: This guide provides instructions about preparing the IBM HTTP Server. For detailed and up-to-date installation instructions, see the IBM HTTP Server documentation.</p>

Procedure	Reference
<ol style="list-style-type: none"> 1. Create the WebSphere Application Server deployment manager profile. 2. Start the WebSphere Application Server deployment manager. 3. Create custom node profiles. 	<ul style="list-style-type: none"> • “Creating network deployment profiles (Profile Management Tool) for x86 architectures” on page 78 • “Creating profiles for network deployments (command-line) for x86 or x64 architectures” on page 81 • “Starting the WebSphere Application Server on Windows” on page 193
Configure the WebSphere Application Server for a cluster.	• “Defining a cluster” on page 88
<p>Configure the WebSphere Application Server:</p> <ul style="list-style-type: none"> • Configure the Java heap size for the deployment manager. • Configure the Java heap size for the WebSphere Application Server. Repeat this task for each server. • For SSL directory server connections, add the SSL certificate to WebSphere Application Server. 	<p>For sample instructions, see the following topics:</p> <ul style="list-style-type: none"> • “Configuring the heap size for the deployment manager” on page 89 • “Configuring the heap size for the application server” on page 56 • “Adding the directory server SSL certificate to WebSphere Application Server” on page 208 <p>WebSphere Application Server documentation:</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp
<p>Configure the IBM HTTP Server. Repeat for each web server.</p> <ul style="list-style-type: none"> • Configure the IBM HTTP Server plug-in and secure the connection. • Enable SSL directives on IBM HTTP Server. 	<p>For sample instructions, see the following topics:</p> <ul style="list-style-type: none"> • “Configuring the IBM HTTP Server plug-in and securing the connection (stand-alone)” on page 61 • “Enabling SSL directives on the IBM HTTP Server” on page 64 <p>IBM HTTP Server documentation:</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/ihs/ihs/tihs_installihs.html
Install the IMS Server application in the WebSphere Application Server on the deployment manager.	“Installing the IMS Server with the installer for an upgrade” on page 141
Verify the IMS Server deployment on the WebSphere Application Server.	“Verifying the IMS Server deployment on the WebSphere Application Server” on page 36
Stop the node agents.	“Stopping the WebSphere Application Server on Windows” on page 195
Upgrade the IMS Server settings.	“Upgrading configurations from 8.0.1 to 8.2” on page 144
Restart the deployment manager.	<ul style="list-style-type: none"> • “Stopping the WebSphere Application Server on Windows” on page 195 • “Starting the WebSphere Application Server on Windows” on page 193

Procedure	Reference
Update the ISAMESSOIMS module mapping to forward connection requests.	"Updating the ISAMESSOIMS module mapping for connection request forwarding" on page 72
Disable auto start for the ISAMESSOIMS application.	"Disabling auto start for ISAMESSOIMS" on page 102
Override session management for ISAMESSOIMS.	"Overriding session management for the ISAMESSOIMS" on page 103
Configure the IBM HTTP Server to use the old IMS Server SSL certificate.	"Configuring the SSL certificate after an upgrade" on page 145
Restart the WebSphere Application Server: 1. Restart the deployment manager. 2. Start the nodes. 3. Fully resynchronize the nodes. 4. Start the cluster.	For example steps, see: <ul style="list-style-type: none"> • "Stopping the WebSphere Application Server on Windows" on page 195 • "Starting the WebSphere Application Server on Windows" on page 193 • "Resynchronizing the nodes" on page 201
Verify whether the upgrade is successful.	"Verifying a successful upgrade" on page 147

Upgrading IMS Server 8.1 for a stand-alone deployment

Use the IMS Server upgrade roadmap to avoid confusion on the topics and procedures that you must follow to complete the upgrade to a stand-alone IMS Server version 8.2.

Procedure	Reference
Make sure that IMS Server 8.1 is installed and it works.	
Stop the TAM E-SSO IMS Server application in the WebSphere Application Server.	
Uninstall the earlier version of IMS Server from WebSphere Application Server.	"Uninstalling the TAM E-SSO IMS application from WebSphere Application Server" on page 209
Stop the stand-alone profile where IMS Server is installed.	"Stopping the WebSphere Application Server on Windows" on page 195
Stop the IBM HTTP Server.	"Stopping and starting the IBM HTTP Server on Windows" on page 192
Back up the IMS Server and its database: <ul style="list-style-type: none"> • Back up your WebSphere Application Server profile with the manageprofiles command. • Back up the IMS Server database. 	<ul style="list-style-type: none"> • "Backing up WebSphere Application Server profiles (manageprofiles command)" on page 188 • "Backing up the database in DB2" on page 189
Start the WebSphere Application Server stand-alone profile.	"Starting the WebSphere Application Server on Windows" on page 193
Install and deploy the IMS Server applications in the WebSphere Application Server.	"Installing the IMS Server with the installer for an upgrade" on page 141
Verify the IMS Server deployment on the WebSphere Application Server.	"Verifying the IMS Server deployment on the WebSphere Application Server" on page 36

Procedure	Reference
Upgrade the IMS Server settings.	"Upgrading configurations from 8.1 to 8.2" on page 144
Restart the WebSphere Application Server.	<ul style="list-style-type: none"> "Stopping the WebSphere Application Server on Windows" on page 195 "Starting the WebSphere Application Server on Windows" on page 193
Update the ISAMESSOIMS module mapping to forward connection requests.	"Updating the ISAMESSOIMS module mapping for connection request forwarding" on page 72
Restart the WebSphere Application Server.	<ul style="list-style-type: none"> "Stopping the WebSphere Application Server on Windows" on page 195 "Starting the WebSphere Application Server on Windows" on page 193
Verify if the upgrade is successful.	"Verifying a successful upgrade" on page 147

To upgrade the AccessAgent clients to 8.2, see "Upgrading the AccessAgent" on page 146.

To upgrade the AccessStudio clients to 8.2, see "Upgrading the AccessStudio" on page 147.

Upgrading IMS Server 8.1 for a network deployment (cluster)

Use the IMS Server upgrade roadmap to identify the tasks to complete the upgrade to a clustered IMS Server version 8.2.

Make sure that IMS Server 8.1 is installed and it works.

Procedure	Reference
Stop the TAM E-SSO IMS Server application in the WebSphere Application Server.	
Uninstall the TAM E-SSO IMS Server application from the WebSphere Application Server administrative console. Note: Do this task so that you can back up the WebSphere Application Server profile.	<ul style="list-style-type: none"> "Uninstalling the TAM E-SSO IMS application from WebSphere Application Server" on page 209
Stop the network deployment profile where IMS Server is installed. <ol style="list-style-type: none"> 1. Stop the cluster. 2. Stop the nodes. 3. Stop the deployment manager. 	<ul style="list-style-type: none"> "Stopping the WebSphere Application Server on Windows" on page 195
Stop the IBM HTTP Server.	"Stopping and starting the IBM HTTP Server on Windows" on page 192

Procedure	Reference
Back up IMS Server and its database: <ul style="list-style-type: none"> • Back up your WebSphere Application Server profile with the manageprofiles command. • Back up the IMS Server database. Note: To back up other supported databases, see your database documentation. 	<ul style="list-style-type: none"> • “Backing up WebSphere Application Server profiles (manageprofiles command)” on page 188 • “Backing up the database in DB2” on page 189
Start the WebSphere Application Server deployment manager.	“Starting the WebSphere Application Server on Windows” on page 193
Configure the Java maximum heap size for the deployment manager.	“Configuring the heap size for the deployment manager” on page 89
Install the IMS Server on the deployment manager.	“Installing the IMS Server with the installer for an upgrade” on page 141
Verify the IMS Server deployment on the WebSphere Application Server.	“Verifying the IMS Server deployment on the WebSphere Application Server” on page 36
Stop the node agents.	“Stopping the WebSphere Application Server on Windows” on page 195
Upgrade the IMS Server settings.	“Upgrading configurations from 8.1 to 8.2” on page 144
Restart the deployment manager.	<ul style="list-style-type: none"> • “Stopping the WebSphere Application Server on Windows” on page 195 • “Starting the WebSphere Application Server on Windows” on page 193
Update the ISAMESSOIMS module mapping to forward connection requests.	“Updating the ISAMESSOIMS module mapping for connection request forwarding” on page 72
Disable auto start for the ISAMESSOIMS application.	“Disabling auto start for ISAMESSOIMS” on page 102
Override session management for ISAMESSOIMS.	“Overriding session management for the ISAMESSOIMS” on page 103
Synchronize the nodes.	“Resynchronizing the nodes” on page 201
Restart the cluster: <ol style="list-style-type: none"> 1. Stop the cluster. 2. Stop the nodes. 3. Start the nodes. 4. Start the cluster. 	For example steps, see: <ul style="list-style-type: none"> • “Stopping the WebSphere Application Server on Windows” on page 195 • “Starting the WebSphere Application Server on Windows” on page 193
Verify if the upgrade is successful.	“Verifying a successful upgrade” on page 147

Upgrading IMS Server 3.6 or 8.0

You can upgrade IMS Server version 3.6 or 8.0 to IMS Server version 8.2.

About this task

If you upgraded to IMS Server version 3.6 or version 8.0, contact IBM Services for information about upgrading to version 8.2.

Procedure

1. Upgrade IMS Server 3.6 or 8.0 to 8.0.1.

See *Upgrading an existing installation of IMS Server* at: http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.itamesso.doc_8.0.1/tasks/IMS_Installation_Upgrading_existing_IMSServer_installation.html

2. Upgrade IMS Server 8.0.1 to 8.2.

See one of the following sections to get started:

- “Upgrading IMS Server 8.0.1 for a stand-alone deployment” on page 131
- “Upgrading IMS Server 8.0.1 for a network deployment (cluster)” on page 134

Chapter 11. Upgrading to 8.2

To upgrade your current IBM Security Access Manager for Enterprise Single Sign-On version to version 8.2, upgrade the individual product components.

For an overview and considerations when upgrading to 8.2, see "Planning for an upgrade" in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

To perform an upgrade, do the following tasks in order:

1. Upgrade the IMS Server.
2. Upgrade the deployed AccessAgent clients.
3. Upgrade the deployed AccessStudio clients.

The upgrade procedure varies for each component and scenario.

- For the IMS Server upgrade, see Chapter 10, "IMS Server upgrade road map," on page 131.
- For the AccessAgent upgrade, see "Upgrading the AccessAgent" on page 146.
- For the AccessStudio upgrade, see "Upgrading the AccessStudio" on page 147.

Installing the IMS Server with the installer for an upgrade

Upgrade and deploy the IMS Server to WebSphere Application Server by using the IMS Server installer.

Before you begin

- Back up the database.
- For IMS Server 8.0.1, stop the IMS Server service.
- For IMS Server 8.1, stop the **tamesso** application.

Note:

- If you remove or do not back up the **tamesso** application, the IMS Server installer removes earlier versions of the **tamesso** application and installs the new IMS Server.
- Remove the **tamesso** application from the WebSphere administrative console. Do not run the IMS Server uninstaller.
- For IMS Server 8.0.1, complete the middleware installation.
- For WebSphere Application Server stand-alone deployments:
 - Ensure that the WebSphere Application Server is started.
 - Review the WebSphere Application Server configuration for stand-alone deployments.
 - Review the IBM HTTP Server configuration.
- For WebSphere Application Server Network Deployment:
 - Ensure that the deployment manager profile is started.
 - Review the WebSphere Application Server configuration for a cluster.
 - Review the IBM HTTP Server configuration.
- Review the planning worksheet for any required values to complete the installation.

About this task

The IMS Server installation process deploys two applications on the WebSphere Application Server:

Application name	EAR file name	Contains
ISAMESSOIMS	com.ibm.tamesso.ims-delhi.deploy.isamessoIms.ear	<ul style="list-style-type: none">• AccessAdmin• AccessAssistant and Web Workplace• Runtime web service for IMS Server
ISAMESSOIMSConfig	com.ibm.tamesso.ims-delhi.deploy.isamessoImsConfig.ear	<ul style="list-style-type: none">• IMS Configuration Wizard• IMS Configuration Utility

Procedure

1. Run `imsinstaller.exe`. The IMS Server installation program wizard starts.
2. Select a language from the list.
3. Click **OK**. **Product License Validation** is displayed.
4. Select the product for which you have a license to install.
 - IBM Security Access Manager for Enterprise Single Sign-On Standard
This package offers strong authentication, session management, centralized logging, and reporting in addition to single sign-on.
 - IBM Security Access Manager for Enterprise Single Sign-On Suite
This package offers one time password support, AccessAgent plug-ins, Web single sign-on and remote access through Web Workplace, custom tracking and IAM Integration in addition to the Standard package.
5. Click **Next**. **The software License Agreement** is displayed.
6. Select **I accept the terms in the license agreement**.
7. Click **Next**. The installation directory is displayed.
8. Accept the default installation directory or specify a new directory. By default, IMS Server is installed in `C:\Program Files\IBM\ISAM ESSO\IMS Server`.
9. Click **Next**.
10. Select **Yes** to automatically deploy the IMS Server to WebSphere Application Server.
 - To deploy WebSphere Application Server manually, click **No**. See “Deploying IMS Server on WebSphere Application Server manually” on page 197.
11. Click **Yes** to specify that WebSphere Application Server security is enabled.
12. Click **Next**. If you click **No**, you must provide the SOAP port.
For example:
 - For WebSphere Application Server stand-alone, the default SOAP port for the application server is 8880.
 - For WebSphere Application Server Network Deployment, the default SOAP port for the Deployment Manager is 8879.
13. Configure the WebSphere Application Server administration security settings.

Note: If two-way secure sockets layer (SSL) is enabled for the WebSphere Application Server, the SSL Java keystore file and password are required.

- a. Specify the WebSphere administrative user name and password. For example: use wasadmin and password.
- b. Specify the SSL Trusted Java keystore file, trust.p12, and its location.

For example:

- **For WebSphere Application Server stand-alone:**

```
<was_home>\profiles\<AppSrv_profilename>\config\cells\  
<cell_name>\nodes\<node_name>\trust.p12
```

See the following example:

```
C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\  
config\cells\ibmusvr1Node01Cell\nodes\ibmusvr1Node01\trust.p12
```

- **For WebSphere Application Server Network Deployment:**

```
<was_home>\profiles\<Dmgr_profilename>\config\cells\<cell_name>\  
trust.p12
```

See the following example:

```
C:\Program Files\IBM\WebSphere\AppServer\Profiles\Dmgr01\config\  
cells\ibm-svr1Cell01\trust.p12
```

- c. Specify the SSL Trusted keystore password.
The default SSL Trusted keystore password is WebAS.
- d. Optional: Specify the SSL Java keystore file, key.p12, and its location.

For example:

- **For WebSphere Application Server stand-alone:**

```
<was_home>\profiles\<AppSrv_profilename>\config\cells\  
<cell_name>\nodes\<node_name>\key.p12
```

See the following example:

```
C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\  
config\cells\ibmusvr1Node01Cell\nodes\ibmusvr1Node01\key.p12
```

- **For WebSphere Application Server Network Deployment:**

```
<was_home>\profiles\<Dmgr_profilename>\config\cells\<cell_name>\  
key.p12
```

See the following example:

```
C:\Program Files\IBM\WebSphere\AppServer\Profiles\Dmgr01\config\  
cells\ibm-svr1Cell01\key.p12
```

- e. Optional: Specify the SSL Java keystore password if you specified the SSL Java keystore file.

The default SSL Java keystore password is WebAS.

14. Accept the default WebSphere Application Server SOAP connector port, or specify a different SOAP connector port.

Note: You define the SOAP connector port when you create a WebSphere Application Server profile. You can determine the correct port number in the following directory for each profile.

For stand-alone deployment: <was_home>/profiles/<AppSrv_profilename>/logs/AboutThisProfile.txt

For a network deployment: <was_home>/profiles/<Dmgr_profilename>/logs/AboutThisProfile.txt

For example:

- For WebSphere Application Server stand-alone, the SOAP port for the application server is 8880.
- For WebSphere Application Server Network Deployment, the SOAP port for the Deployment Manager is 8879.

15. Click **Next**. The **Pre-installation Summary** page is displayed.

16. Click **Install**.

17. In the **Installation Complete** window, click **Done**.

What to do next

Before you set up the IMS Server with the IMS Configuration Wizard, verify the IMS Server deployment on the WebSphere Application Server. See “Verifying the IMS Server deployment on the WebSphere Application Server” on page 36.

Upgrading configurations from 8.1 to 8.2

Run the IMS Configuration Wizard to upgrade the IMS Server settings.

Before you begin

- Ensure that the IMS Server 8.2 is installed.
- Ensure that the ISAMESS0IMSConfig is started.
- Ensure that the node agent is stopped.
- Check the <ims_home>/ISAM_ESS0_IMS_Server_InstallLog.log file for critical errors that occurred during the IMS Server installation. If there are any errors, resolve them first before you configure the IMS Server.

Procedure

1. Open the IMS Configuration Wizard.

For example: <https://localhost:9043/front> The **Upgrade Configuration Wizard** page is displayed.

2. Click **Begin**.

Note: If there is any problem with the existing repository, it cannot be upgraded. You are redirected to the Enterprise Directory configuration page to address any values that are missing or wrong. For information about the directory server fields, see “Configuring the IMS Server to use directory servers” on page 179.

3. In **Confirm Settings**, review the settings.

4. Click **Save**. The **Data Source, Certificate Store, and Enterprise Directory Setup Complete** page is displayed.

What to do next

To continue with the upgrade, see the applicable road map:

- “Upgrading IMS Server 8.1 for a stand-alone deployment” on page 137.
- “Upgrading IMS Server 8.1 for a network deployment (cluster)” on page 138.

Upgrading configurations from 8.0.1 to 8.2

Run the IMS Configuration Wizard to upgrade the IMS Server settings.

Before you begin

- Install the IMS Server version 8.2.
- Ensure that the node agent is stopped.
- Ensure that the ISAMESSOIMSConfig is started.
- Check the <ims_home>/ISAM_ESSO_IMS_Server_InstallLog.log file for critical errors that occurred during the IMS Server installation. If there are any errors, resolve them first before you configure the IMS Server.

Procedure

1. Open the IMS Configuration Wizard.
For example: `https://localhost:9043/front`
The **Upgrade Configuration Wizard** page is displayed.
2. In **Server Set Up**, select **Upgrade from an earlier version 8.0.1**.
3. Click **Begin**.
4. In **Enter data source information**, the configuration values for the data source are pre-filled. Accept the default values if there are no changes.
5. Click **Next**.
6. In the **Old Configuration** page, specify the installation path of the old IMS Server. For example: `C:\Encentuate\IMSServer8.0.1.0.10`.
7. Click **Next**.
8. In **Configure IMS services URL**, specify the fully qualified web server name and HTTP Server name and port number.

Note:

- The IBM HTTP Server name is the fully qualified name of the IBM HTTP Server that interfaces with the WebSphere Application Server.
 - The IBM HTTP Server name must match the **CN** attribute of the SSL certificate used by the IBM HTTP Server.
 - The typical default port number is 443.
9. Click **Next**.

Note: If there are problems with the existing repository, it cannot be imported. You are redirected to the Enterprise Directory configuration page to correct any values that are missing or wrong. For information about the directory server fields, see “Configuring the IMS Server to use directory servers” on page 179.

10. In **Confirm Settings**, review the settings.
11. Click **Save**. After the settings are applied, the **Data Source, Certificate Store, and Enterprise Directory Setup Complete** page is displayed.

What to do next

To continue with the upgrade, see the applicable road map:

- “Upgrading IMS Server 8.0.1 for a stand-alone deployment” on page 131.
- “Upgrading IMS Server 8.0.1 for a network deployment (cluster)” on page 134.

Configuring the SSL certificate after an upgrade

Set the IBM HTTP Server to use the old IMS Server SSL certificate.

About this task

This task is only applicable for version 8.0.1 to 8.2 IMS Server upgrades.

Use the old IMS Server SSL certificate so that the existing AccessAgent continues to work with the upgraded IMS Server.

Procedure

1. Select **Start > All Programs > IBM WebSphere > Application Server <version> > Profiles > <profile name> > Administrative console.**
2. Log on to the IBM Integrated Solutions Console.
3. On the IBM Integrated Solutions Console navigation pane, click **Servers > Server Types > Web servers.**
4. Click the *<Web server name>*. For example: *webserver1*.
5. In the **Additional Properties** section on the **Configuration** tab, click **Plug-in properties.**
6. Click **Manage key and certificates.**
7. Under **Additional Properties**, click **Personal Certificates.**
8. Select the **default** certificate.
9. Click **Delete.**
10. Click **Save.**
11. Click **Import.**
12. Under **Managed Key Store**, select **TAMESSOIMSKeystore** from the **Key store** list.
13. Specify **changeit** as the keystore password.
14. Click **Get key store alias.**
15. From the **Certificate aliases to import** list, choose **imsscrert.**
16. Enter **default** in the **Imported certificate alias** field.
17. Click **OK.**
18. In the **Messages** box, click **Save.**
19. Select **Servers > Server types > Web servers.**
20. Click the appropriate *<Web server name>*. For example: *webserver1*.
21. In the **Additional Properties** section on the **Configuration** tab, click **Plug-in properties.**
22. Click **Copy to Web server key store directory.**
23. Click **Apply.**
24. In the **Messages** box, click **Save.**
25. Optional: Do this step only if the WebSphere Application Server uses a non-default trust store. See “Adding the IMS Root CA to the truststore” on page 207.
26. Restart the web server from the IBM Integrated Solutions Console.

Upgrading the AccessAgent

You can directly upgrade AccessAgent 8.x, or 8.x.x to version 8.2. You can also upgrade with a prepackaged AccessAgent installer.

Before you begin the upgrade, you can choose to prepare custom scripts that the installer runs before and after upgrading the AccessAgent:

- `BeforeUpgrade.vbs`: The installer runs this script before starting the AccessAgent upgrade.
- `AfterUpgrade.vbs`: The installer runs this script after the AccessAgent upgrade is complete.

Important:

- These custom scripts are optional.
- Save these scripts in the `<aa_installer>\config` folder.
- Save the scripts in those specified file names.

To upgrade with a prepackaged AccessAgent installer, see Chapter 9, “Preparing an installation package to install on multiple PCs,” on page 121.

To upgrade AccessAgent to 8.2:

1. Make sure that AccessAgent 8.x is installed and working properly.
2. Install AccessAgent 8.2. See Chapter 7, “Installing the AccessAgent,” on page 111.

When you upgrade, the AccessAgent 8.2 installer automatically uninstalls the existing AccessAgent. The new version is typically installed in `<%PROGRAMFILES%>\IBM\ISAM ESSO\AA`.

Important: Upgrading from AccessAgent 8.1 (x86) on a 64-bit platform to AccessAgent 8.2 (x64) is not supported.

To upgrade, you must manually uninstall AccessAgent 8.1 (x86) and install AccessAgent 8.2 (x64).

Note: When you uninstall AccessAgent 8.1 (x86), it removes the existing Wallets.

Upgrading the AccessStudio

Before you upgrade the AccessStudio, you must uninstall the existing version of AccessStudio 8.0, 8.0.1, or 8.1.

To upgrade the AccessStudio to 8.2:

1. Uninstall the existing AccessStudio 8.x.
2. Install AccessStudio 8.2.

Verifying a successful upgrade

After completing the upgrade, verify each server and client component to ensure that the upgrade is complete and that it works.

Before you begin

- For a stand-alone deployment, start the WebSphere Application Server.
- For a network deployment, start the WebSphere Application Server deployment manager.
- Upgrade the IMS Server.
- Upgrade the AccessAgent.
- Upgrade the AccessStudio.

Procedure

1. Verify the server upgrade.
 - Log on to AccessAdmin. Verify the version number, users, and settings of the upgraded server.
For example:
 - `https://<ihs_host>/admin`
 - `https://<loadbalancer_host>/admin`
2. Verify the upgraded client workstations and configuration.
 - a. On a client workstation, verify the version of the AccessAgent client.
You can also try to accomplish the following common client verification tasks:
 - Sign up a user
 - Log on a user
 - Lock and unlock a user
 - b. Verify that you can connect to the server.
 - c. If you are using AccessStudio, verify the version of the AccessStudio client.
 - d. If you are using second authentication factors such as smart cards or fingerprint readers, verify that the authentication devices continue to work.
 - e. For shared session workstations, verify that the shared session AccessAgent server components are upgraded.
3. Review the system installation logs for any important messages to ensure that any system upgrade issues are addressed or noted.
4. Review and update the Appendix A, “Planning worksheet,” on page 163 to reflect configuration or password changes.

Chapter 12. Migrating the IMS Server 8.2 from one host to another

You can install or upgrade the IMS Server to version 8.2 on one host and then migrate it to a new WebSphere Application Server instance.

Before you begin

- Prepare two host computers.
- On one of the hosts, ensure that IMS Server 8.2 is installed and that it works.

About this task

Migration from one IMS Server 8.2 host (<host A>) to another instance of a host (<host B>) applies to both installed or upgraded deployments of IMS Server 8.2

Where:

<host A>

Specifies the source host with a working IMS Server 8.2 configuration.

<host B>

Specifies the target host that you want to migrate to with the IMS Server configuration.

Procedure

1. On <host A>, export the IMS Server 8.2 configuration. See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.
2. On <host B>, prepare the required middleware. For example:
 - WebSphere Application Server
 - IBM HTTP Server

The middleware on <host B> can be prepared and configured the same way as <host A>.

3. On <host B>, install IMS Server 8.2 on the new WebSphere Application Server profile. Do not configure the IMS Server on <host B> after completing the installation. See “Installing the IMS Server with the IMS Server installer” on page 33.
4. On <host B>, import the upgraded IMS Server configuration you previously exported from <host A>. For more information, see the first step in this procedure.

Part 4. Uninstalling

Uninstalling IBM Security Access Manager for Enterprise Single Sign-On is dependent on the component you are planning to remove.

Chapter 13. Uninstalling

Uninstalling is the process of removing the installed server and client components from the computer.

To uninstall the product, you must uninstall the different product components.

See the following tasks:

- “Uninstalling the IMS Server”
- “Uninstalling the AccessAgent” on page 155
- “Uninstalling the AccessStudio” on page 156

Uninstalling the IMS Server

You can use the uninstall wizard to uninstall the IMS Server package from a single installation location.

Before you begin

Ensure that:

- You have administrator privileges.
- You have WebSphere Application Server administrator privileges.
- You set up the command-line tool environment correctly.

About this task

Uninstalling the product component does not remove all of the files and directories. You must do a file clean-up.

Note: If the uninstallation wizard is in either Arabic or Dutch languages, the IMS Server uninstallation stops. If uninstallation stops, uninstall IMS Server from the WebSphere Application Server administrative console (IBM Integrated Solutions Console) and delete the IMS Server installation folder from the computer.

Procedure

1. Clean up the IMS Server configuration on WebSphere Application Server.
 - a. Open the command prompt.
 - b. Type the following command:

```
<ims_home>\bin\cleanImConfig <was_admin> <password>
```

The command-line tool completes the configuration cleanup process on WebSphere Application Server.

- On a stand-alone deployment, the server is restarted.
 - On a network deployment, the deployment manager is restarted.
2. Launch the software removal utility.
 - On Windows XP or Windows Server 2003, select **Start > Control Panel > Add or Remove Programs > ISAM ESSO IMS Server > Remove**.
 - On Windows Server 2008, Windows 7 or Windows Vista, select **Start > Control Panel > Programs and Features > ISAM ESSO IMS Server > Remove**.

3. Click **Next**. You are prompted to confirm whether the WebSphere Application Server security is enabled.
4. Specify whether the WebSphere Application Server administration security is enabled.
 - If the WebSphere Application Server administration security is enabled:
 - a. Select **Yes**.
 - b. Click **Next**.
 - c. Proceed to specify the WebSphere Application Server administration security settings (5)
 - If the WebSphere Application Server administration security is not enabled:
 - a. Select **No**.
 - b. Click **Next**.
 - c. Proceed to specify the SOAP connections in step (6)
5. Specify the WebSphere Application Server administration security settings.

Note: The SSL Java keystore file and password are required only if two-way secure sockets layer (SSL) is enabled for the WebSphere Application Server.

- a. Specify the WebSphere administrative user name and password. For example: use wasadmin account name and password.
- b. Specify the SSL Trusted Java keystore file, trust.p12 and its location.
For example:
 - For WebSphere Application Server stand-alone, <was_home>\profiles\
<AppSrv_profilename>\config\cells\
<Server01Node01Cell101>\nodes\
<Server01Node01>\trust.p12
 - For WebSphere Application Server Network Deployment,
<was_home>\profiles\
<Dmgr_profilename>\config\cells\
<Server01Cell101>\trust.p12
- c. Specify the SSL Trusted keystore password.
The default SSL Trusted keystore password is WebAS.
- d. Specify the SSL Java keystore file, key.p12 and its location.
For example:
 - For WebSphere Application Server stand-alone, <was_home>\profiles\
<AppSrv_profilename>\config\cells\
<Server01Node01Cell101>\nodes\
<Server01Node01>\key.p12
 - For WebSphere Application Server Network Deployment,
<was_home>\profiles\
<Dmgr_profilename>\config\cells\
<Server01Cell101>\key.p12
- e. Specify the SSL Java keystore password.
The default SSL Java keystore password is WebAS.
6. Specify the WebSphere Application Server SOAP connector port.

Note:

- The SOAP connector port is specified during the creation of your WebSphere Application Server custom profile. For example:
 - For WebSphere Application Server stand-alone, the typical SOAP Port for the Application Server is 8880.
 - For WebSphere Application Server Network Deployment, the typical SOAP Port for the Deployment Manager is 8879.

- Verify the recorded value in the following directory <was_home>/profiles/<profile>/logs/AboutThisProfile.txt
7. Click **Next**.
 8. Click **Uninstall**.
 9. In the **Uninstallation Complete** window, click **Done**.
 10. Clean up the WebSphere Application Server profile. To delete the WebSphere Application Server profile, see the WebSphere Application Server information center at: http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.express.doc/info/exp/ae/tpro_removeprofile.html.
 11. Do a file clean-up.
 - a. Delete the <ims_home> directory.
 - b. Delete the <was_home> directory.
 12. Delete the IMS Server database.

To delete or to back up the database, see the database documentation provided with your database product.

Uninstalling the AccessAgent

Use the Windows **Control Panel** or **Start menu** shortcut to uninstall the AccessAgent from the computer.

Before you begin

Ensure that you have administrator privileges.

About this task

You can uninstall AccessAgent either directly from the Windows Start menu shortcuts or through the **Control Panel**.

Procedure

1. Choose one of the following methods to launch the software removal utility:
 - (Start menu) Select **Start > All Programs > ISAM ESSO AccessAgent > Uninstall ISAM ESSO AccessAgent**.
 - On Windows XP or Windows Server 2003, select **Start > Control Panel > Add or Remove Programs > ISAM ESSO AccessAgent > Remove**.
 - On Windows 7, Windows Server 2008 or Windows Vista, select **Start > Control Panel > Programs and Features > ISAM ESSO AccessAgent > Remove**.
2. You are prompted to confirm whether you want to uninstall the product.
 2. Click **Yes**. AccessAgent is uninstalled from the computer.

Note:

If you uninstall AccessAgent x64 from Windows 7 x64, the following message is displayed:

The setup must update files or services that cannot be updated while the system is running. If you choose to continue, a reboot will be required to complete the setup.

What to do next

Verify that the installation directory for AccessAgent is removed.

Uninstalling the AccessAgent silently (unattended)

Use the **msiexec** command with the **/uninstall** parameter and **/quiet** switch for an unattended removal of the AccessAgent.

Before you begin

- Ensure that you have administrator privileges.
- Ensure that you have the ISAM ESSO AccessAgent.msi installer.
- Verify any required response file parameters or considerations.

The response file, SetupHlp.ini, is in `<aa_path>\Config`.

`<aa_path>` is the location of the AccessAgent MSI-based installer.

- You can choose to keep or remove any Wallets with the **RemoveWallet** parameter.

Note: If the **RemoveWallet** parameter is not defined in a silent uninstall, the Wallet is retained by default.

Procedure

1. Open the command prompt.
2. Type:

```
msiexec /uninstall "<aa_path>\ISAM ESSO AccessAgent.msi" /quiet
```

The AccessAgent user is not logged off or removed from the system until the workstation is rebooted.

Results

You uninstalled the AccessAgent.

What to do next

Verify that the installation directory for AccessAgent is removed.

Uninstalling the AccessStudio

Use the **Control Panel** or the Windows **Start menu** shortcut to uninstall the AccessStudio from the computer.

Before you begin

Ensure that you have administrator privileges.

About this task

You can uninstall AccessStudio either directly from **ISAM ESSO AccessStudio** or through the **Control Panel**.

Procedure

1. Launch the software removal utility.

- (Start menu) Select **Start > All Programs > ISAM ESSO AccessStudio > Uninstall ISAM ESSO AccessStudio**.
- On Windows XP or Windows Server 2003, select **Start > Control Panel > Add or Remove Programs > ISAM ESSO AccessStudio > Remove**.
- On Windows 7, Windows Server 2008 or Windows Vista, select **Start > Control Panel > Programs and Features > ISAM ESSO AccessStudio > Remove**.

You are prompted to confirm whether you want to uninstall the product.

2. Click **Yes**. AccessStudio is uninstalled from the computer.

What to do next

Verify that the installation directory for AccessStudio is removed.

Uninstalling the AccessStudio silently (unattended)

Use the `msiexec` command with the `/uninstall` parameter and `/quiet` switch for an unattended removal of the AccessStudio.

Before you begin

- Ensure that you have administrator privileges.
- Ensure that you have the ISAM ESSO AccessStudio.msi installer.

Procedure

1. Open the command prompt.
2. Type:

```
msiexec /uninstall "<as_path>\ISAM ESSO AccessStudio.msi" /quiet
```

Where:

`<as_path>` is the location of the AccessStudio MSI-based installer.

Results

You removed AccessStudio successfully.

What to do next

Verify that the installation directory for AccessStudio is removed.

Chapter 14. Reinstalling or reconfiguring the IMS Server

To reinstall or reconfigure the IMS Server after an installation or configuration failure, you must first clean up the IMS Server configuration on WebSphere Application Server.

About this task

If the IMS Server configuration fails, you can clean up the existing server configuration on WebSphere Application Server and attempt to reinstall the IMS Server. Alternatively, you can clean up the configuration and then uninstall the IMS Server.

Procedure

- To reconfigure the IMS Server:
 1. Clean up the IMS Server configuration.
 2. Optional: If the database schema is modified, you can reuse the database or prepare another database.
To delete a database, see the documentation for your database product.
 3. Start the IMS Configuration Wizard to reconfigure the server.
- To reinstall the IMS Server:
 1. Clean up the IMS Server configuration on WebSphere Application Server.
 2. Uninstall the IMS Server.
 3. Install and configure the IMS Server.
 - a. Install the IMS Server with the IMS Server installer.
 - b. Verify the IMS Server deployment on the WebSphere Application Server.
 - c. Configure the IMS Server.

Cleaning up the IMS Server configuration on WebSphere Application Server

You can use the **cleanImConfig** command-line tool to clean up the IMS Server configuration on WebSphere Application Server. After the configuration cleanup, you can configure the IMS Server again with the IMS Configuration Wizard.

Before you begin

- Ensure that you have WebSphere Application Server administrator privileges.
- Ensure that the command-line tool environment is set up correctly.
- (Network deployment) Stop the cluster.
- (Network deployment) Ensure that the node agents are started.

About this task

The command-line tool removes the IMS Server JDBC settings, IMS keystore, any directory server, and database settings that the IMS Server configuration process creates. For more information about the command-line tool, see the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

For network deployments, run the **cleanImsConfig** command on the deployment manager node.

Important: The **cleanImsConfig** command-line tool does not delete any databases from the database server. To delete or to back up the database, see the database documentation provided with your database product.

Procedure

1. Open the command prompt.
2. Browse to the <ims_home>\bin directory. For example, type:
cd <ims_home>\bin
3. Type the following command:

```
cleanImsConfig <was_admin> <password>
```

During the configuration cleanup process on WebSphere Application Server, the command-line tool completes the following tasks asynchronously:

- On a stand-alone deployment, the server is restarted.
- On a network deployment, the deployment manager is restarted.

Note: Even if the command-line tool shows that the clean up process is complete, the WebSphere Application Server might still be in the process of restarting.

4. Delete the IMS Server database.

What to do next

If you are uninstalling the IMS Server, run the IMS Server uninstaller program. See “Uninstalling the IMS Server” on page 153.

Part 5. Appendixes

Appendix A. Planning worksheet

Use the planning worksheet as a reference for the default and sample values during the installation and configuration of the IBM Security Access Manager for Enterprise Single Sign-On server and other required software.

Installation directories and other paths

The following table contains the different path variables used throughout the guide and the corresponding default values. In some cases, the variable name matches the name of an environment variable that is set in the operating system. For example, %TEMP% represents the environment variable %TEMP% for Windows.

Note: When installing the IBM Security Access Manager for Enterprise Single Sign-On on Windows systems, the default directory is typically the system program files directory <system drive>\Program Files\IBM\, where the system drive is typically a C: drive. However, you can specify that IBM Security Access Manager for Enterprise Single Sign-On is installed on a disk drive other than the C: drive.

Path variable	Component	Default directory
<aa_home>	AccessAgent	C:\Program Files\IBM\ISAM ESSO\AA
<as_home>	AccessStudio	C:\Program Files\IBM\ISAM ESSO\AA\ECSS\AccessStudio
<db_home>	DB2	C:\Program Files\IBM\SQLLIB
<ihs_home>	IBM HTTP Server	C:\Program Files\IBM\HTTPServer
<ims_home>	IBM Security Access Manager for Enterprise Single Sign-On IMS Server	C:\Program Files\IBM\ISAM ESSO\IMS Server
<jvm_home>	Java Virtual Machine	C:\Program Files\Java\jre1.5.0_11
<updi_home>	IBM Update Installer for WebSphere Application Server	C:\Program Files\IBM\WebSphere\UpdateInstaller
<was_home>	WebSphere Application Server	C:\Program Files\IBM\WebSphere\AppServer
<was_dmgr_home>	WebSphere Application Server Network Deployment deployment manager profile	C:\Program Files\IBM\WebSphere\AppServer\profiles\Dmgr01
<%TEMP%>	Windows directory for temporary files	When logged on as Administrator, C:\Documents and Settings\Administrator\Local Settings\Temp
<%PROGRAMFILES%>	Windows directory for installed programs	C:\Program Files

Host names and ports

The following table contains the different variable host names and port numbers used throughout the guide.

Variable	Description
<was_hostname>	Name of the host where the WebSphere Application Server is installed.
<dmgr_hostname>	Name of the host where the WebSphere Application Server Network Deployment Manager is installed.
<ihs_hostname>	Name of the host where the IBM HTTP Server is installed.
<loadbalancer_hostname>	Name of the host where the load balancer is installed.
<ims_hostname>	Name of the host where the IMS Server is installed.
<ihs_ssl_port>	IBM HTTP Server SSL port number.
<admin_ssl_port>	Administrative console secure port number.

URLs and addresses

The following table contains the different URLs and addresses used throughout the guide. The values vary depending on whether you are using WebSphere Application Server stand-alone or WebSphere Application Server Network Deployment.

Description	Format	Example value
Integrated Solutions Console (WebSphere Application Server administrative console)	<ul style="list-style-type: none"> If you are using WebSphere Application Server stand-alone: <i>https://<was_hostname>:<admin_ssl_port>/ibm/console</i> If you are using WebSphere Application Server Network Deployment: <i>https://<dmgr_hostname>:<admin_ssl_port>/ibm/console</i> 	<p><i>https://localhost:9043/ibm/console</i></p> <p>or</p> <p><i>http://localhost:9060/ibm/console</i></p>
IMS Configuration Wizard	<ul style="list-style-type: none"> If you are using WebSphere Application Server stand-alone: <i>https://<was_hostname>:<admin_ssl_port>/front</i> If you are using WebSphere Application Server Network Deployment: <i>https://<dmgr_hostname>:<admin_ssl_port>/front</i> 	<i>https://localhost:9043/front</i>
IMS Configuration Utility	<ul style="list-style-type: none"> If you are using WebSphere Application Server stand-alone: <i>https://<was_hostname>:<admin_ssl_port>/webconf</i> If you are using WebSphere Application Server Network Deployment: <i>https://<dmgr_hostname>:<admin_ssl_port>/webconf</i> 	<i>https://localhost:9043/webconf</i>

Description	Format	Example value
AccessAdmin	<ul style="list-style-type: none"> If you are using a load balancer: <code>https:// <loadbalancer_hostname>:<ihs_ssl_port>/ admin</code> If you are not using a load balancer: <code>https://<ihs_hostname>:<ihs_ssl_port>/admin</code> If webserver is configured properly: <code>https://ihs_hostname>/admin</code> 	<ul style="list-style-type: none"> <code>https://imsserver:9443/admin</code> <code>https://imsserver/admin</code>
AccessAssistant	<ul style="list-style-type: none"> If you are using a load balancer: <code>https:// <loadbalancer_hostname>:<ihs_ssl_port>/ aawwp</code> If you are not using a load balancer: <code>https://<ihs_hostname>:<ihs_ssl_port>/aawwp</code> 	<code>https://imsserver:9443/aawwp</code>
Web Workplace	<ul style="list-style-type: none"> If you are using a load balancer: <code>https:// <loadbalancer_hostname>:<ihs_ssl_port>/ aawwp?isWwp=true</code> If you are not using a load balancer: <code>https://<ihs_hostname>:<ihs_ssl_port>/ aawwp?isWwp=true</code> 	<code>https://imsserver:9443/aawwp?isWwp=true</code>

Users, profile names, and groups

The following table contains some of the users and groups created during the installation.

Variable	Description	Example value
<profile name>	<p>WebSphere Application Server profile name.</p> <p>The profile name is defined when creating profiles for WebSphere Application Server with the <code>manageprofiles</code> command-line tool or graphical Profile Management tool.</p>	<ul style="list-style-type: none"> If you are using WebSphere Application Server stand-alone: <code><AppSrv_profilename></code> If you are using WebSphere Application Server Network Deployment: <ul style="list-style-type: none"> Deployment manager: <code><Dmgr_profilename></code> Node <code><Custom_profilename></code>
<WAS Admin user ID>	WebSphere administrator ID created during the installation of WebSphere Application Server.	<code>wasadmin</code>
<IHS Admin user ID>	HTTP Server administrator user ID created during the installation of the IBM HTTP Server.	<code>ihsadmin</code>

Variable	Description	Example value
<DB2 Admin user ID>	DB2 administrator service user ID for Microsoft Windows created during the installation of IBM DB2.	db2admin
<IMS Admin user ID>	IBM Security Access Manager for Enterprise Single Sign-On administrator. User ID created during installation of the IMS Server for administration of IBM Security Access Manager for Enterprise Single Sign-On.	imsadmin
<TIMAD Admin user ID>	(Only for Active Directory enterprise directories) User ID created for use with the Tivoli Identity Manager Active Directory Adapter. Not required for LDAP directories.	tadadmin
<LDAP Admin or lookup user ID>	Sample LDAP user ID created for use by the IMS Server with LDAP V3 compatible directory servers.	ldapadmin lookupusr
<VA non-root user ID>	General user account for virtual appliance deployments. Created during virtual appliance activation and deployment.	virtuser
<VA root user ID>	Root user account for virtual appliance deployments. Used to log on to virtual appliance during boot up.	root

Installing IBM DB2

The following table contains values that you must specify when installing a database server.

Parameter	Default Value
Installation file	Workgroup Server Edition (limited use) <ul style="list-style-type: none"> • DB2_97_limited_CD_Win_x86.exe • DB2_97_limited_CD_Win_x86-64.exe Enterprise Server Edition <ul style="list-style-type: none"> • DB2_ESE_V97_Win_x86.exe • DB2_ESE_V97_Win_x86-64.exe Note: The installation files might vary according to the version and edition of DB2.
Installation directory	C:\Program Files\IBM\SQLLIB
<i>User information for the DB2 Administration Server</i>	
Domain	None - use local user account
User name	db2admin

Parameter	Default Value
Password	
DB2 instance	Create the default DB2 instance
Partitioning option for the default DB2 instance	Single partition instance
DB2 tools catalog	None
Set up your DB2 Server to send notifications	No
Enable operating system security	Yes
<i>DB2 administrators group</i>	
Domain	None
Group Name	DB2ADMNS Note: This value is an example. You can specify your own value.
<i>DB2 users group</i>	
Domain	None
Group Name	DB2USERS Note: This value is an example. You can specify your own value.
Port number	50000

Creating the IMS Server database

The following table contains the values that you must specify to create the IMS Server database.

Parameter	Default Value
Database name	imsdb Note: This value is an example. You can specify your own value.
Default path	C:\
Alias	imsdb Note: This value is an example. You can specify your own value.
Comment	DB for IMS Note: This value is an example. You can specify your own value.
Let DB2 manage my storage (automatic storage)	Yes
Default buffer pool and table space page size	8K
Use the database path as a storage path	Yes
Code set	UTF-8
Collating sequence	
Region	Default

Creating a DB2 user manually

The following table contains the values that you must specify, if you are creating a separate database user for IBM Security Access Manager for Enterprise Single Sign-On.

Parameter	Default Value
DB2 user	imsdb2admin

Parameter	Default Value
Administrative privileges	<ul style="list-style-type: none"> • Connect to database • Create tables • Create packages

Installing WebSphere Application Server

The following table contains the values that you must specify when installing the WebSphere Application Server.

Parameter	Default Value
Installation file	llaunchpad.exe
Installation directory	<was_home>
WebSphere Application Server Environment	(None) Note: Profiles are created only with the Profile Management tool or command-line interface <i>after</i> the WebSphere fix packs are applied. You can create the following profiles: For WebSphere Application Server stand-alone product deployments <ul style="list-style-type: none"> • Application server For WebSphere Application Server Network Deployment (cluster) <ul style="list-style-type: none"> • Deployment Manager • Custom
Enable Administrative Security	Yes
WebSphere Administration user name	wasadmin
Deployment Manager profile name	<Dmgr_profilename>
Custom profile name (node)	<Custom_profilename>
Application server profile name	<AppSrv_profilename>
Cell name	<Server01Node01Cell01>
Deployment Manager node name	<Server01Cell01>
Application server node name	<Server01Node01>
HTTP server installation location	<ihs_home>
HTTP port	80
HTTP admin server port	8080

Installing IBM Update Installer for WebSphere software installation

The following table contains the values that you must specify when installing the IBM Update Installer for WebSphere Software Installation.

Parameter	Default Value
Installation file	install.exe
Installation directory	C:\Program Files\IBM\WebSphere\UpdateInstaller

Installing the latest WebSphere Application Server fix pack

The following table contains the values that you must specify when installing the latest WebSphere Application Server fix pack.

Parameter	Default Value
Installation file	<ul style="list-style-type: none"> • 7.0.0-WS-WAS-WinX32-FP000000X.pak • 7.0.0-WS-WAS-WinX64-FP000000X.pak
Installation directory	<was_home>
Maintenance Operation Selection	Install maintenance package
Maintenance package directory path	<updi_home>\maintenance

Installing IBM HTTP Server

The following table contains the values that you must specify when installing the IBM HTTP Server.

Parameter	Default Value
Installation file	launchpad.exe
Installation directory	<ihs_home>
IBM HTTP Server HTTP Port	80
IBM HTTP Server HTTP Administration Port	8008
Run IBM HTTP Server as a Windows Service	Yes
Run IBM HTTP Administration as a Windows Service	Yes
Log on as a local system account	Yes
Log on as a specified user account	No
User name	Administrator Note: This value is an example. You can specify your own value.
Password	
Startup type	Automatic
Create a user ID for IBM HTTP Server administration server authentication	Yes
IBM HTTP Server administration server authentication user ID	ihsadmin Note: WebSphere Application Server account for administering IBM HTTP Server and the IBM HTTP Server plug-in.
IBM HTTP Server administration server authentication password	
Install IBM HTTP Server Plug-in for IBM WebSphere Application Server	Yes
Web server definition	<webserver1>
Host name or IP address for the Application Server	IMS82.samesso.ibm.com

Installing the latest IBM HTTP Server fix pack

The following table contains the values that you must specify when installing the latest IBM HTTP Server fix pack.

Parameter	Default Value
Installation file	<ul style="list-style-type: none"> 7.0.0-WS-IHS-WinX32-FP000000X.pak 7.0.0-WS-IHS-WinX64-FP000000X.pak
Installation directory	<ihs_home>
Maintenance Operation Selection	Install maintenance package
Maintenance package directory path	<was_home>\UpdateInstaller\maintenance

Configuring the IBM HTTP Server

The following table contains the values that you must specify when configuring the IBM HTTP Server to work with the WebSphere Application Server.

Parameter	Default Value
Windows batch file	configure<webserver1>.bat
Original Location	<ihs_home>\Plugins\bin
Target Location	<was_home>\bin
com.ibm.SOAP.requestTimeoutproperty	6000
<i>Remote Web server management</i>	
Port	8008
User name	ihsadmin
Password	
Use SSL	No
Refresh configuration interval	60 seconds
Plug-in configuration file name	plugin-cfg.xml
Plug-in keystore file name	plugin-key.kdb
Plug-in configuration directory and file name	<ihs_home>\Plugins\config\<webserver1>\plugin-cfg.xml
Plug-in keystore directory and file name	<ihs_home>\Plugins\config\<webserver1>\plugin-key.kdb
Automatically generate the plug-in configuration file	Yes
Automatically propagate the plug-in configuration file	Yes
Log file name	<ul style="list-style-type: none"> <ihs_home>\Plugins\logs\<webserver1>\http_plugin.log <ims_home>\ISAM_E-SSO_IMS_Server_InstallLog.log
Log level	Error

Installing IMS Server

The following table contains the values that you must specify when installing the IMS Server.

Parameter	Default Value
Installation file	imsinstaller_8.2.0.0.x.exe
Installation folder	<ims_home>
Deploy IMS Server to WebSphere Application Server	<ul style="list-style-type: none"> • Yes - automatically deploys the IMS EAR file to WebSphere Application Server • No - you must manually deploy the IMS EAR file to WebSphere Application Server
WebSphere Application Server Administration Security enabled	Yes
Administrative user name	wasadmin Note: This value must be the same value as the WebSphere Application Server Administrator Server user name.
Administrative password	
SSL Trusted Java key store file	trust.p12
SSL Trusted Java key store file location	<ul style="list-style-type: none"> • If you are using WebSphere Application Server stand-alone: <was_home>\profiles\ <AppSrv_profilename>\config\cells\ <Server01Cell01>\nodes\ <Server01Node01>\ • If you are using WebSphere Application Server Network Deployment <was_home>\profiles\ <Dmgr_profilename>\config\cells\ <Server01Cell01>\
SSL Trusted Java key store password	WebAS
SSL Java key store file	key.p12
SSL Java key store file location	<ul style="list-style-type: none"> • If you are using WebSphere Application Server stand-alone: <was_home>\profiles\ <AppSrv_profilename>\config\cells\ <Server01Cell01>\nodes\ <Server01Node01>\ • If you are using WebSphere Application Server Network Deployment <was_home>\profiles\ <Dmgr_profilename>\config\cells\ <Server01Cell01>\
SSL Java key store password	WebAS
WebSphere Application Server SOAP connector port	<ul style="list-style-type: none"> • For WebSphere Application Server stand-alone: 8880 • For WebSphere Application Server Network Deployment (deployment manager): 8879

Parameter	Default Value
SOAP connector port number location	<ul style="list-style-type: none"> If you are using WebSphere Application Server stand-alone: <code><was_home>\profiles\ <AppSrv_profilename>\logs\ AboutThisProfile.txt</code> If you are using WebSphere Application Server Network Deployment <code><was_home>\profiles\ <Dmgr_profilename>\logs\ AboutThisProfile.txt</code>
IMS Server URL	<p>Example: <code>https://localhost:9043/front</code></p> <ul style="list-style-type: none"> If you are using WebSphere Application Server stand-alone: <code>https://<was_hostname>:<admin_ssl_port>/front</code> If you are using WebSphere Application Server Network Deployment: <code>https://<dmgr_hostname>:<admin_ssl_port>/front</code>

Configuring the IMS Server

The following table contains the values that you must specify when configuring the IMS Server.

Parameter	Default Value
JDBC provider name	ISAM ESS0 JDBC Provider
Data source name	ISAM ESS0 IMS Server Data Source
JNDI name	jdbc/ims Note: The JNDI name is not editable.
J2C authentication data alias	imsauthdata
Create IMS Server database schema	Yes
Choose Database Type	<ul style="list-style-type: none"> IBM DB2 Server Microsoft SQL Server Oracle Server
<i>Database Configuration - <database type></i>	
Host Name	
Instance Note: For Microsoft SQL Server only.	
Port	<ul style="list-style-type: none"> For IBM DB2 Server: 50000 For Microsoft SQL Server: 1433 For Oracle Server: 1521
Database Name Note: For IBM DB2 only.	
SID Note: For Oracle Server only.	
User Name	db2admin
User Password	
<i>Provide Root CA Details</i>	

Parameter	Default Value
Keystore name	CellDefaultKeyStore
Keystore password	
Root CA alias name	root
Fully qualified web server name	web1.example.com
<i>IMS Services URL</i>	
HTTPS port number	443

Configuring enterprise directory (LDAP or Active Directory)

The following table contains the values that you must specify when configuring the enterprise directory.

Parameter	Default value
Host name	ldapsvr.example.com
Bind distinguished name	<ul style="list-style-type: none"> • For Active Directory: cn=lookupusr, cn=users, dc=team, dc=example, dc=com • For LDAP: cn=lookupusr, ou=users, o=example, c=us
Base distinguished name	<ul style="list-style-type: none"> • For Active Directory: cn=users, dc=team, dc=example, dc=com • For LDAP: ou=users, o=example, c=us
Domain	team.example.com
Port	389 (without SSL) 636 (with SSL)

Appendix B. Creating database schemas

You must specify a database schema when configuring the IMS Server data source and certificate.

When configuring the IMS Server, you can choose your own database schema or have the configuration wizard create the database schema. If you want to use your own database schema, run the correct SQL scripts for your supported database server.

- If you want to use your own database schema, create the database schema before you start the configuration of the IMS Server data source and certificate.
- The delimiter for:
 - IBM DB2: `initPL.sql` script is `!`.
 - Oracle: `initPL.sql` and `logPL.sql` scripts, is `/`.
 - All databases: the delimiter is `;`.

If IBM DB2 Server is the IMS Server database:

1. Browse to `<IMS Server installation directory>\com.ibm.tamesso.ims-delhi.build.boot\src\database\data\sql\db2\create-schema`.
2. Run these scripts in the following order:
 - a. `init.sql`
 - b. `log.sql`
 - c. `initPL.sql`
3. Browse to `<IMS Server installation directory>\com.ibm.tamesso.ims-delhi.build.root\src\database\data\sql\common\initialize-prod`.
4. Run `boot.sql`.
5. Browse to `<IMS Server installation directory>\com.ibm.tamesso.ims-delhi.build.boot\src\database\data\sql\db2\create-schema`.
6. Run `view.sql`.

If Microsoft SQL Server is the IMS Server database:

1. Log on to SQL Server Management Studio. For example: `imsdbusr`

Important: Specify the SQL Server logon account that you created in 4 on page 204 on “Creating the database in SQL Server manually” on page 203.

2. Complete the following steps for each of the scripts:

Run each of the following SQL scripts in order:	Do:
<ol style="list-style-type: none"> 1. <ims_home>\com.ibm.tamesso.ims-delhi.build.boot\src\database\data\sql\sqlserver\create-schema\init.sql 2. <ims_home>\com.ibm.tamesso.ims-delhi.build.boot\src\database\data\sql\sqlserver\create-schema\log.sql 3. <ims_home>\com.ibm.tamesso.ims-delhi.build.boot\src\database\data\sql\common\initialize-prod\boot.sql 4. <ims_home>\com.ibm.tamesso.ims-delhi.build.boot\src\database\data\sql\sqlserver\create-schema\view.sql 	<p>To run the SQL script:</p> <ol style="list-style-type: none"> 1. Open the SQL script. 2. Click the Query Options command. 3. Set the batch separator to “;”, without the quotes. 4. Click OK. 5. Click Execute.

3. Verify the tables:
 - a. Expand **<IMS Server database_name> > Tables**.
 - b. Ensure that the table names include the SQL Server logon name as a prefix. For example: imsdbsr.<table name>

If Oracle Database is the IMS Server database:

1. Browse to *<IMS Server installation directory>*\com.ibm.tamesso.ims-delhi.build.boot\src\database\data\sql\oracle\create-schema.
2. Run these scripts in the following order:
 - a. init.sql
 - b. log.sql
 - c. initPL.sql
 - d. logPL.sql
3. Browse to *<IMS Server installation directory>*\com.ibm.tamesso.ims-delhi.build.boot\src\database\data\sql\common\initialize-prod.
4. Run boot.sql.
5. Browse to *<IMS Server installation directory>*\com.ibm.tamesso.ims-delhi.build.boot\src\database\data\sql\oracle\create-schema.
6. Run view.sql.

Creating users manually

You can create and designate a DB2 user in IBM DB2 that the IMS Server can use to connect to the database. This task is optional.

Before you begin

Log on to the database server with administrator privileges.

About this task

This task is optional.

The DB2 user account you create must have privileges to connect to the database, create tables, and create packages. A common user name is db2admin, but you can assign any user name as long as the account has administrative access. Avoid changing the user name after creating it.

Procedure

1. Create an operating system user with administrative privileges (member of the local administrators group). For example: *imsdb2admin*.
2. Use one of the following methods to create and assign DB2 privileges to the user:
 - **Use the DB2 Control Center:**
 - a. Open DB2 Control Center.
 - b. If the Control Center View is displayed, select **Advanced**.
 - c. Click **OK**.
 - d. In Object View, expand the object tree for the IMS Server database that you are authorizing a user to use. Expand the object tree until you find the **User and Group Objects** folder.
 - e. Click **User and Group Objects**.
 - f. Right-click **DB Users**.
 - g. Click **Add**.
 - h. In **Users**, specify the user account that was created in step 1. For example: *imsdb2admin*.
 - i. In the **Authorities** field, select the following check boxes:
 - **Connect to database**
 - **Create tables**
 - **Create packages**
 - j. Click **OK**.
 - **Use the DB2 command line processor to execute the following SQL statement.**

Note: Before executing the SQL statement, replace the variables in the SQL statement with your values.

```
connect to <ims database>;
grant createtab,bindadd,connect on database to user <DB2 user>;
connect reset;
```

For example: The following SQL statement grants the necessary privileges for the database *imsdb* to the user *imsdb2admin*:

```
connect to imsdb;
grant createtab,bindadd,connect on database to user imsdb2admin;
connect reset;
```

Appendix C. Other installation and configuration tasks

Depending on the deployment, you might perform additional installation and configuration tasks for IBM Security Access Manager for Enterprise Single Sign-On.

See the following topics:

- “Configuring the IMS Server to use directory servers”
- “Backing up and restoring” on page 188
- “Stopping and starting components” on page 191
- “Deploying IMS Server on WebSphere Application Server manually” on page 197
- “Installing the web server plug-in for WebSphere Application Server manually” on page 202
- “Creating the database in SQL Server manually” on page 203
- “Enabling application security in WebSphere Application Server” on page 198
- “Basic commands for managing WebSphere Application Server profiles” on page 204
- “Ways of resolving hosts and IP addresses” on page 205
- “Renewing the SSL Certificate used by the IBM HTTP Server” on page 206
- “Adding the IMS Root CA to the truststore” on page 207
- “Adding the directory server SSL certificate to WebSphere Application Server” on page 208
- “Retrieving the IBM HTTP Server administrator name and password” on page 209
- “Uninstalling the TAM E-SSO IMS application from WebSphere Application Server” on page 209

Configuring the IMS Server to use directory servers

You can configure the IMS Server to use either an LDAP server or multiple Active Directory servers. You can configure directory servers either through the IMS Configuration Wizard or the IMS Configuration Utility.

Use the IMS Configuration Wizard to set up the IMS Server for the first time in a new installation. The IMS Configuration Wizard includes steps for setting up the IMS Server to use directory servers. Use the IMS Configuration Utility to set up the IMS Server to use directory servers later.

After configuring the directory server, restart the WebSphere Application Server immediately to apply the configuration changes. If you configure the web server definition and the directory server before restarting the WebSphere Application Server, the configuration is not saved.

Ensure that the directory server repositories are running to connect to these repositories. If one or more of the configured repositories are unreachable, you cannot authenticate or stop the WebSphere Application Server.

If the problem persists, it is because of a security feature of virtual member manager. The virtual member manager always checks all repositories before

authenticating the user. For more information about the solution, see <http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.wim.doc/UnableToAuthenticateWhenRepositoryIsDown.html>.

Configuring the IMS Server to use Active Directory servers

Add prepared Active Directory servers so that the IMS Server can look up user account information for authorization. You can add multiple Active Directory servers.

Before you begin

You can provide self-service password reset in AccessAssistant and Web Workplace under the following conditions for your Active Directory connection:

- **Not using SSL:** Ensure that the Tivoli Identity Manager Active Directory Adapter is installed and running on the directory server or on a separate host. Be ready to provide the credentials for an administrative user or a designated user with password reset privileges. For example: myresetusr.
- **Using SSL:** Be ready to provide the credentials for an administrative user or a designated user with password reset privileges. For example: myresetusr.

Note: You are not required to install Tivoli Identity Manager Active Directory Adapter.

For SSL connections, add the directory server SSL certificates to the WebSphere Application Server.

You must prepare the following enterprise directory information:

- Domain controller FQDN. For example: adserver.team.example.com
- Domain DNS name. For example: team.example.com.
- Credentials for the directory lookup user. For example: lookupusr.
- Base distinguished name. For example: cn=users,dc=team,dc=example,dc=com
- Optional: For password resets in AccessAssistant and Web Workplace, you need the credentials for a directory user with password reset privileges. For example: myresetusr.

If you are using the planning worksheet, see the Appendix A, “Planning worksheet,” on page 163.

About this task

If you are in the middle of configuring the IMS Server with the IMS Configuration Wizard complete these steps, then continue with the procedures in “Configuring the IMS Server for a new installation with the IMS Configuration Wizard (stand-alone)” on page 68.

Procedure

1. Click **Add new repository**.
2. Select the enterprise directory type.
 - a. Select **Active Directory**.
 - b. Click **Next**.
3. For Active Directory servers, complete the following steps:
 - a. Specify whether to enable password synchronization.

Password synchronization is available only for Active Directory servers. When password synchronization is enabled, the IBM Security Access Manager for Enterprise Single Sign-On password is synchronized with Active Directory.

When you change the password, the software changes it on every Active Directory host on which the user has an account. If the password is reset out-of-band, the IBM Security Access Manager for Enterprise Single Sign-On password is resynchronized at the next online logon.

See the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide* for more details about Active Directory password synchronization.

- b. Specify the repository connection details.

Tip: To see additional help for each item, move the cursor over each item.

Domain controller FQDN

Specify the fully qualified domain name of the domain controller .
For example: adserver.team.example.com

Domain DNS Name

Specify the domain name of the server where the IMS Server connects. For example: team.example.com.

Note: This attribute is not the fully qualified name of the DNS. It is the "domain" of the server.

Domain NetBIOS Name

Specify the NetBIOS computer name of the repository host. The NetBIOS computer name is typically the same as the repository host name of the same domain. For example: mydirsvr.

Note:

- The NetBIOS name is not validated by the IMS Server. You must provide the correct name.
- To determine the correct NetBIOS computer name, go to the Microsoft website at www.microsoft.com and search for "nbtstat". See instructions on how to use **nbtstat** to determine the NetBIOS computer name with the **nbtstat** command.

Port The default port number is 389 without SSL. The default port number with SSL is 636.

Note: To enable password resets in a non-SSL environment, use the Tivoli Identity Manager Active Directory Adapter. In an SSL environment, you are not required to install the Tivoli Identity Manager Active Directory Adapter.

Bind user name

Specify the user name of the lookup user. For example: lookupusr.

Password

Enter the password for the lookup user.

4. Click **Next**.
5. To view or customize additional repository details, click **Open advanced settings**.
6. Specify whether you are using a Secure Socket Layer (SSL) connection.

Option	Parameters
If you are not using SSL	<p data-bbox="480 237 643 264">Connect using</p> <p data-bbox="574 281 1219 308">You can select only Domain controller host name / FQDN.</p> <p data-bbox="480 338 764 365">Domain controller FQDN</p> <p data-bbox="574 369 1406 451">Specify the fully qualified domain name of the domain controller. For example: adserver.team.example.com where team.example.com is the domain name server.</p> <p data-bbox="480 485 699 512">Domain DNS name</p> <p data-bbox="574 516 1395 573">Specify the domain name of the Active Directory server that is connected to the IMS Server. For example: team.example.com</p> <p data-bbox="480 602 745 630">Domain NetBIOS name</p> <p data-bbox="574 634 1414 716">Specify the NetBIOS computer name. The NetBIOS computer name is typically the same as the host name of the computer in the same domain. For example: mydirsvr</p> <p data-bbox="574 720 638 747">Note:</p> <ul data-bbox="574 751 1414 909" style="list-style-type: none"> <li data-bbox="574 751 1390 808">• The NetBIOS name is not validated by the IMS Server. You must provide the correct name. <li data-bbox="574 821 1414 909">• To determine the correct NetBIOS computer name, go to the Microsoft website at www.microsoft.com and search for “nbtstat”. See instructions on how to use nbtstat to determine the NetBIOS computer name. <p data-bbox="480 982 1414 1039">Port Specify the port number. For example: the default is 389 (without SSL) or 636 (with SSL).</p> <p data-bbox="480 1071 1341 1127">Bind user name Specify the user name of the lookup user. For example: administrator.</p> <p data-bbox="480 1157 1005 1213">Password Enter the password for the lookup user.</p> <p data-bbox="480 1245 1403 1388">Base distinguished name At least one base distinguished name is required. The base distinguished name indicates the starting point for searches in this directory server. For authorization purposes, this field is case sensitive by default. Match the case in your directory server.</p> <p data-bbox="574 1404 1325 1520">For example: For a user with a DN of <code>cn=lookupusr,cn=users,dc=team,dc=example,dc=com</code>, specify the base distinguished name with any of the following options: <code>cn=users,dc=team,dc=example,dc=com</code> or <code>dc=team,dc=example,dc=com</code>.</p> <p data-bbox="480 1551 1414 1753">Failover domain controllers Use a failover domain controller for replicated Active Directory servers in a high availability configuration. Specify the host name or the fully qualified domain name, and the port number of the secondary domain controller. The secondary domain controller is used when the primary domain controller fails.</p>

Option	Parameters
If you are using SSL	<p>Connect using</p> <p>If you are using SSL, you can connect to the server using a Domain DNS name or a Domain controller host name / FQDN. If you are using a domain name server to resolve host names or IP addresses, select Domain DNS name.</p> <p>If you select Domain controller host name / FQDN, the Domain controller host name / FQDN is displayed.</p> <p>Domain controller host name / FQDN</p> <p>If you choose to connect using Domain controller host name / FQDN, the domain controller host name or fully qualified domain name is displayed.</p> <p>Domain DNS name</p> <p>The domain name of the Active Directory server that is connected to the IMS Server is displayed. For example: team.example.com</p> <p>Domain NetBIOS name</p> <p>Specify the NetBIOS computer name. The NetBIOS computer name is typically the same as the host name of the computer in the same domain. For example: mydirsvr</p> <p>Note:</p> <ul style="list-style-type: none"> • The NetBIOS name is not validated by the IMS Server. You must provide the correct name. • To determine the correct NetBIOS computer name, go to the Microsoft website at www.microsoft.com and search for “nbtstat”. See instructions on how to use nbtstat to determine the NetBIOS computer name. <p>Bind distinguished name</p> <p>Enter the distinguished name (DN) for the lookup user. The distinguished name is the name that uniquely identifies an entry in the directory. The directory user must be authorized to perform directory lookups. A DN is made up of attribute=value pairs, separated by commas. For example: cn=lookupusr,cn=users,dc=team,dc=example,dc=com</p> <p>Password</p> <p>Enter the password for the lookup user.</p> <p>Base distinguished name</p> <p>At least one base distinguished name is required. The base distinguished name indicates the starting point for searches in this directory server. For authorization purposes, this field is case sensitive by default. Match the case in your directory server.</p> <p>For example: For a user with a DN of cn=lookupusr,cn=users,dc=team,dc=example,dc=com, specify the base distinguished name with any of the following options: cn=users,dc=team,dc=example,dc=com or dc=team,dc=example,dc=com.</p>

Option	Parameters
	<p>Failover domain controllers</p> <p>This field is displayed only if you choose a connection using Domain controller host name / FQDN.</p> <p>Use a failover domain controller for replicated Active Directory servers in a high availability configuration.</p> <p>Specify the host name or the fully qualified domain name, and the port number of the secondary domain controller. The secondary domain controller is used when the primary domain controller fails.</p>

7. If password synchronization is enabled:
 - a. You can choose to enable **AccessAssistant/Web Workplace password reset**.
If you choose to enable this feature, users can reset their passwords in AccessAssistant or Web Workplace.
 - b. If you enabled **AccessAssistant/Web Workplace password reset**, enter the user credentials of a directory user with password reset privileges, host name, and port number.
For non-SSL Active Directory connections, the host name and port number are the details of the Tivoli Identity Manager Active Directory Adapter.
When specifying the user credentials, specify the credentials for an administrative directory user or a designated directory user with password reset privileges for the directory server. For example: myresetusr.

Note: See “Preparing the directory servers” on page 29.
8. Click **Next**.
9. Restart the WebSphere Application Server.
 - a. Stop the WebSphere Application Server (for stand-alone deployments) or the deployment manager (for network deployments).
 - b. Start the WebSphere Application Server (for stand-alone deployments) or the deployment manager (for network deployments).

What to do next

If configuring the enterprise directory is part of your new IMS Server installation, see the following sections:

- For virtual appliance deployments, see “Activating and configuring the virtual appliance” on page 43.
- For stand-alone deployments, continue with step 18 on page 70 in “Configuring the IMS Server for a new installation with the IMS Configuration Wizard (stand-alone)” on page 68
- For network deployments, continue with step 18 on page 70 in “Configuring the IMS Server with the IMS Configuration Wizard (network deployment)” on page 97

Configuring the IMS Server to use LDAP servers

You can add prepared LDAP servers such as Tivoli Directory Server, so that the IMS Server can look up the directory server for credential authorization. You can add one LDAP server.

Before you begin

Prepare to provide the following enterprise directory information:

- Credentials for the directory lookup user. For example: lookupusr.
- Bind distinguished name. For example: cn=lookupusr,ou=users,o=example,c=us.
- Base distinguished name. For example: ou=users,o=example,c=us.

When you configure directory servers for a new IMS Server installation, ensure that you log on to the IMS Configuration Wizard.

If you are using the planning worksheet, see the Appendix A, “Planning worksheet,” on page 163.

For SSL directory server connections, you must add the SSL certificate to the WebSphere Application Server.

About this task

If you are in the middle of configuring the IMS Server with the IMS Configuration Wizard, complete these steps; then continue with the procedures in “Configuring the IMS Server for a new installation with the IMS Configuration Wizard (stand-alone)” on page 68.

Procedure

1. Click **Add new repository**.
2. Select the enterprise directory type.
 - a. If you are using LDAP servers, select **LDAP**.
 - b. Click **Next**.
3. For the LDAP server, specify the following details:
 - a. Specify the repository details.

Tip: To see additional help for each item, move the cursor over each item.

Domain controller host name / FQDN

Specify the host name or the fully qualified domain name of the LDAP server. For example: mydirsvr

Port Specify the port number. For example: the default is 389 (without SSL) or 636 (with SSL).

Remember: If your deployment uses non-default port numbers or you are connecting to the repository over SSL, be sure to specify the correct port number.

Bind distinguished name

Shows the distinguished name for the lookup user. The distinguished name is the name that uniquely identifies an entry in the directory. The lookup user must be authorized to perform directory lookups on the server.

A DN is made up of attribute=value pairs, separated by commas. For example: cn=lookupusr,ou=users,o=example,c=us.

Password

Enter the password for the lookup user.

4. To customize additional repository details, click **Advanced**.

Use SSL

Specify whether you are using a secure socket layer (SSL) connection.

Domain controller host name / FQDN

Specify the domain controller fully qualified domain name. For example: mydirsvr.

Port Specify the port number. For example: The default port is **389** (without SSL) or **636** (with SSL).

Bind distinguished name

Enter the distinguished name (DN) for the lookup user. The distinguished name is the name that uniquely identifies an entry in the directory.

A DN is made up of attribute=value pairs, separated by commas. For example: cn=lookupusr,ou=users,o=example,c=us.

Password

Enter the password for the lookup user.

User name attributes

Specify a valid enterprise directory user name attribute that users provide as their user names for authentication. Other attributes can also be used for the user name. For example: if you specify the mail attribute, users must enter their email addresses for their user names.

To use different user name attributes (for example, badge number, email address or an employee number), provide the custom attributes properties instead.

For LDAP, the default is cn.

Base distinguished name

At least one base distinguished name is required. The base distinguished name indicates the starting point for searches in this LDAP directory server. For authorization purposes, this field is case-sensitive by default. Match the case in your directory server.

For example: For a user with DN of cn=lookupusr,ou=users,o=example,c=us, specify the base distinguished name with the following option: ou=users,o=example,c=us.

Failover domain controllers

Use a failover domain controller to ensure the LDAP server high availability.

Specify the host name or the fully qualified domain name, and the port number of the secondary domain controller. The secondary domain controller is used when the primary domain controller fails.

5. Click **Next**.
6. Restart the WebSphere Application Server.
 - a. Stop the WebSphere Application Server (for stand-alone deployments) or the deployment manager (for network deployments).
 - b. Start the WebSphere Application Server (for stand-alone deployments) or the deployment manager (for network deployments).

Results

You added and configured directory server connections for the IMS Server. The IMS Server verifies user credentials against the directory servers you specified.

What to do next

If you are using a directory server other than IBM Tivoli Directory Server, there are additional configuration steps. See “Configuring a generic LDAP directory server other than Tivoli Directory Server.”

Ensure that you restart the WebSphere Application Server to apply the directory server configuration changes.

To continue configuring the IMS Server with the IMS Configuration Wizard.

- For virtual appliance deployments, see “Activating and configuring the virtual appliance” on page 43.
- For stand-alone deployments, see “Configuring the IMS Server for a new installation with the IMS Configuration Wizard (stand-alone)” on page 68.
- For network deployments, see “Configuring the IMS Server with the IMS Configuration Wizard (network deployment)” on page 97.

Configuring a generic LDAP directory server other than Tivoli Directory Server

If you are configuring an LDAP directory server other than Tivoli Directory Server, you must specify the directory type; then restart the application server.

Before you begin

Complete the LDAP directory server configuration for the IMS Server. Complete the directory server configuration by using the IMS Configuration Utility or the IMS Configuration Wizard. See “Configuring the IMS Server to use LDAP servers” on page 184.

Procedure

1. Set the LDAP directory type.
 - a. Log on to the WebSphere administrative console.
 - b. In the administrative console, click **Security > Global security**.
 - c. Under **User account repository**, in the **Available realm definitions** list, verify that **Federated repositories** is selected.
 - d. Click **Configure**
 - e. Under **Related Items**, click **Manage repositories**.
 - f. Click the LDAP server you configured.
 - g. In **Directory type**, select the correct directory type. For example: IBM Lotus® Domino®.
 - h. Click **Apply**.
2. Restart the WebSphere Application Server.

Backing up and restoring

You must back up your server configuration and database before you begin a server upgrade. You can also back up your deployment as a routine procedure in your disaster recovery plan.

Use the **manageprofiles** command-line tool to back up WebSphere Application Server profiles.

Remember: To ensure that you can use known server backups to restore necessary server systems quickly in the event of a disaster:

- Validate and verify server backups periodically.
- Always test and maintain changes to any additional internal recovery procedures.

Backing up WebSphere Application Server profiles (manageprofiles command)

You can back up your WebSphere Application Server profiles with the **manageprofiles** command before you upgrade a server or for routine system backups in disaster recovery procedures.

Before you begin

Ensure that the following components are stopped:

- WebSphere Application Server. See “Stopping the WebSphere Application Server on Windows” on page 195.
- (Network deployment) Node agent
- (Network deployment) Deployment manager
- IBM HTTP Server

Procedure

1. Open the command prompt.
2. Browse to the `<was_home>\bin` directory. For example, type:

```
cd <was_home>\bin
```

For example:

```
cd c:\Program Files\IBM\WebSphere\AppServer\bin
```

3. Use the WebSphere Application Server **manageprofiles** command with the **backupProfile** parameter.

```
manageprofiles.bat -backupProfile -profileName <profile_name>  
-backupFile <backupFile_name>
```

For example:

Stand-alone

```
manageprofiles.bat -backupProfile -profileName AppSrv01  
-backupFile c:\backup\AppSrv01ymmdd.zip
```

Network deployment

```
manageprofiles.bat -backupProfile -profileName Dmgr01 -backupFile  
c:\backup\Dmgr01ymmdd.zip
```

Backing up the IMS Server configuration (Export Configuration Utility)

You can back up or export the IMS Server configuration to a file with the Export Configuration Utility.

Before you begin

Ensure that the following servers are active and responding to requests:

- Database servers
- Directory servers

About this task

The Export Configuration Utility is available only in IBM Security Access Manager for Enterprise Single Sign-On version 8.2.

The IMS Server includes a built-in server configuration backup utility.

You can use the Export Configuration Utility to replicate server configurations or to back up IMS Server 8.2.

To use the Export Configuration Utility to back up the server profile configuration, see the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

Backing up the database in DB2

Back up the database in DB2 before you perform an upgrade, or after a successful server installation.

Before you begin

Ensure that the following servers are stopped:

- WebSphere Application Server
- Nodes
- Deployment manager
- IBM HTTP Server

Procedure

1. Start the DB2 Control Center.
2. Right-click the IMS Server database to back up. For example: Right-click `imsdb`.
3. Select **Backup**.
4. Click **Next**.
5. In **Media Type**, select **File System**.
6. Click **Add**.
7. Specify the path to store the backup files.
8. Click **OK**.
9. Click **Next**.
10. In the **Choose your backup options** page, click **Next**.
11. In the **Specify performance options for the backup** page, click **Next**.

12. Select **Run now without saving task history**.
13. Click **Next**.
14. Review the summary.
15. Click **Finish**.

Results

You backed up the database.

What to do next

Start the IBM HTTP Server, and the WebSphere Application Server.

If you are performing the database backup before an upgrade process, see the upgrade procedures. Check whether you must stop the servers before you proceed with the upgrade.

Restoring the WebSphere Application Server profiles

Restore the WebSphere Application Server profiles from a backup if you must recover from a previously backed up working WebSphere Application Server profile.

Before you begin

Ensure that the following servers are stopped:

- WebSphere Application Server
- Node agents
- IBM HTTP Server

Be sure that the `<was_home>/profiles` directory does not contain a similar folder name as the profile to be restored. If a duplicate exists, you can delete the profile with the **manageprofiles** command or move the folder to another location.

Procedure

1. In a command prompt, browse to the `<was_home>\bin` directory. Type `cd <was_home>\bin`.
For example: `cd c:\Program Files\IBM\WebSphere\AppServer\bin`
2. Restore the profile. Type **manageprofiles -restoreProfile -backup <backup_file_location>**. For example
manageprofiles -restoreProfile -backup c:\backup\AppSrv01ymmdd.zip The **manageprofiles** command-line tool always restores to the same path the profile was backed up from.
3. Verify that the profile is restored. Browse to the `<was_home>\profiles` directory.
For example: `<was_home>\profiles\AppSrv01`. If the profile is restored successfully, a folder for the restored profile is displayed.

Results

You restored the WebSphere Application Server profile.

If you are performing this task as part of a server restoration procedure, do not start the profile. Determine whether you must restore the database first.

Restoring the database in DB2

You can restore the database in DB2 to recover from a previous database backup.

Before you begin

Stop the IBM HTTP Server.

Procedure

1. Start the DB2 Control Center.
2. Right-click the database to restore.
3. Select the **Restore to an existing database**.
4. Click **Next**.
5. In **Available back up images**, select the backup you made.
6. Click the right arrow button.
7. Click **Next**.
8. In **Set non-automatic storage containers for redirected restore** page, click **Next**.
9. In **Choose your restore options** page, click **Next**.
10. In **Select performance options for the restore**, click **Next**.
11. Select **Run now without saving task history**.
12. Click **Next**.
13. Review the summary.
14. Click **Finish**. The database restore process begins.

Results

You restored the database.

What to do next

If you are completing this task as part of a server recovery procedure, you can start the database, IBM HTTP Server, and the WebSphere Application Server.

To start the WebSphere Application Server for a network deployment:

1. Start the deployment manager.
2. Start the node agents.
3. Start the cluster.

Stopping and starting components

Start or stop the IBM Security Access Manager for Enterprise Single Sign-On server, WebSphere Application Server, cluster, or IBM HTTP Server to complete installation, upgrade, or configuration tasks.

Important: Considerations running command-line tools on Windows Vista, Windows 7 and Windows Server 2008 operating systems with Windows User Account Control (UAC) enabled: Certain operations (such as those involving Windows Services) require Administrator privileges.

To ensure that the following command-line tools have sufficient privileges, run them with elevated administrator authority on systems that have the Windows

User Account Control (UAC) and with the **Run all administrators in Admin Approval Mode** policy enabled. When you run these command-line tools from a command prompt, run them from a command prompt window that is launched by performing the following actions:

1. Right-click a command prompt shortcut.
2. Click **Run As Administrator**.
An operating-system dialog box is displayed.
3. Click **Continue** to proceed.

Stopping and starting the IBM HTTP Server on Windows

You can stop and start the IBM HTTP Server service in Windows with the WebSphere administrative console, Start menu, or the command line.

Before you begin

Ensure that the IBM HTTP Server Administration Service is started.

About this task

In a clustered deployment, if you have multiple remote web servers to manage or restart from a single location, you can use the WebSphere administrative console. Typically, you must stop the IBM HTTP Server before you apply fix packs or apply IBM HTTP Server configuration changes.

Procedure

- **To start and stop the IBM HTTP Server from the Windows Start menu:**

Option	Description
Start IBM HTTP Server	Click Start > All Programs > IBM HTTP Server V7.0 > Start HTTP Server .
Stop IBM HTTP Server	Click Start > All Programs > IBM HTTP Server V7.0 > Stop HTTP Server .

- **To start and stop the IBM HTTP Server from the WebSphere administrative console:**

Note: If the web server is not displayed in the administrative console, be sure that you configured the IBM HTTP Server. Configuring the IBM HTTP Server, creates the web server definition in the WebSphere administrative console.

Option	Description
Start IBM HTTP Server	<ol style="list-style-type: none"> 1. Start the WebSphere administrative console and log on with WebSphere administrator privileges. 2. Click Servers > Server Types > Web servers. 3. Select the check box next to each web server. For example: webserver1. 4. Click Start.

Option	Description
Stop IBM HTTP Server	<ol style="list-style-type: none"> 1. Start the WebSphere administrative console and log on with WebSphere administrator privileges. 2. Click Servers > Server Types > Web servers. 3. Select the check box next to each web server. For example: webserver1. 4. Click Stop.

- **To start and stop the IBM HTTP Server Administration service:**

See the following examples:

Start the IBM HTTP Server Administration service

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

Stop the IBM HTTP Server Administration service

Click **Start > All Programs > IBM HTTP Server V7.0 > Stop Admin Server**.

Note: Some procedures such as applying IBM HTTP Server fix packs might require you to stop the HTTP Server Administration service as a prerequisite.

Results

You restarted the IBM HTTP Server.

Example

Command-line alternatives (Windows)

Stop HTTP Server service

```
net stop "IBM HTTP Server 7.0"
```

Stop HTTP Administration Server service

```
net stop "IBM HTTP Administration 7.0"
```

Start HTTP Server service

```
net start "IBM HTTP Server 7.0"
```

Start HTTP Administration service

```
net start "IBM HTTP Administration 7.0"
```

What to do next

To verify the status of the IBM HTTP Server in the services management console.

On the web server host, run the services management console.

Verify the status indicators for the services, IBM HTTP Server 7.0 and IBM HTTP Administration 7.0.

Starting the WebSphere Application Server on Windows

Start the WebSphere Application Server on a network deployment cluster or stand-alone Windows environment after a shutdown or reboot.

About this task

If you must restart a WebSphere Application Server application, you must stop the application first before restarting. If you have multiple nodes in a cluster, you must start the node agent service on each node individually.

WebSphere Application Server includes command-line tools such as **startServer.bat**, **startNode.bat**, and **startManager.bat** as alternatives for starting servers, node agents, or the deployment manager node.

You might be prompted to supply additional WebSphere Application Server administrator credentials as arguments when using these administrative commands. You can check the WebSphere Application Server information center for help on using command-line tools with security turned on.

Note: If a service was created for the WebSphere Application Server and node agent, the WebSphere Application Server and node agent service is started automatically after the host is restarted.

Procedure

- To start WebSphere Application Server in a stand-alone configuration:

Start the stand-alone server environment

Click **Start > All Programs > IBM WebSphere > Application Server Network Deployment V7.0 > <AppSrv01 profile> > Start the server.**

- To start WebSphere Application Server in a clustered configuration:

Start the deployment manager

Click **Start > All Programs > IBM WebSphere > Application Server Network Deployment V7.0 > <Dmgr01 profile> > Start the deployment manager.**

Start the node agent

```
<was_home>\profiles\Custom01\bin\startNode.bat
```

Note: If the node agent is stopped, you cannot use the WebSphere Application Server administrator console to start the node agent. Starting the node agent is accomplished by using the **startNode** command.

Start the cluster

1. Log on to the WebSphere administrative console. For example: <https://localhost:9043/ibm/console>.
2. In the console navigation tree, click **Servers > Server Types > WebSphere application server clusters**.
3. Select the check box for the cluster that is not started. For example: cluster1.
4. Click **Start**.

Results

You started the WebSphere Application Server.

Examples

See the following examples of additional ways of starting the node agent:

- Start the node agent by using the WebSphere **startNode.bat** command.

In a command prompt type `<was_home>\profiles\Custom01\bin\startNode`

- Start the node agent Windows service (command-line)
 1. Click **Start > Run**. Type `cmd`.
 2. In the command prompt, type `net start "IBM WebSphere Application Server V7.0 - <node agent service name>"` and press **Enter**.

For example: `net start "IBM WebSphere Application Server V7.0 - Custom01_nodeagent"`.

The screen ends with the following lines:

```
The IBM WebSphere Application Server V7.0 - Custom01_nodeagent service was started successfully.
```

- Start the node agent (Windows Services management console).
 1. Click **Start > Run**.
 2. Type `services.msc`.
 3. Select the IBM WebSphere Application Server node agent service. For example: **IBM WebSphere Application Server V7.0 - Custom01_nodeagent**.
 4. Click **Start**.

Note: If there is no node agent service available, you did not create a Windows service for the node agent.

What to do next

(Stand-alone) Verify that the stand-alone server is started. Log on to the WebSphere administrative console.

(Network deployment) Verify that the cluster, node agent, and deployment manager nodes are started. Log on to the WebSphere administrative console to determine the status of each component.

Stopping the WebSphere Application Server on Windows

You can stop the nodes in a network deployment or stand-alone server. You must stop middleware, for example, after applying administrator changes or before you apply fix packs.

About this task

Stopping the server might be necessary when you perform a new server installation, component configuration, or upgrade.

Note: After WebSphere administrative security is turned on, you must supply additional WebSphere Application Server administrator credentials as arguments when using the WebSphere Application Server command-line tools **stopNode.bat**, **stopManager.bat** commands. For help on using command-line tools with security turned on, see the WebSphere Application Server information center. The following examples use standard Windows shortcuts and the WebSphere administrative console to achieve the same results.

Procedure

- Stopping a stand-alone WebSphere Application Server configuration:

Stop the stand-alone server

Click **Start > All Programs > IBM WebSphere > Application Server Network Deployment V7.0 > <AppSrv01 profile> > Stop the server.**

- Stopping a clustered (network deployment) WebSphere Application Server configuration:

Stop the cluster

Log on to the WebSphere Application Server administrator console. For example: `https://localhost:9043/ibm/console`.

In the console navigation tree, click **Servers > Server Types > WebSphere application server clusters.**

Select the check box for the cluster.

Click **Stop.**

Stop the node agent

Log on to the WebSphere Application Server administrator console. For example: `https://localhost:9043/ibm/console`.

In the console navigation tree, click **Servers > System administration > Node agents.**

Select the **nodeagent** check box.

Click **Stop.**

Stop the deployment manager

Click **Start > All Programs > IBM WebSphere > Application Server Network Deployment V7.0 > <Dmgr01 profile> > Stop the deployment manager.**

Results

You stopped WebSphere Application Server in a cluster or a stand-alone environment.

Examples

See the following alternatives for stopping the node agent.

- Stop the node agent by using the WebSphere **stopNode.bat** command.
In a command prompt type `<was_home>\profiles\Custom01\bin\stopNode -user <was_admin> -password <was_admin_password>`
- Stop the node agent service (Services management console)
Click **Start > Run.**
Type `services.msc`.
Select the IBM WebSphere Application Server node agent service. For example: **IBM WebSphere Application Server V7.0 - Custom01_nodeagent.**
Click **Stop.**
- Stop the node agent service (command-line)
In the command prompt, type `net stop "IBM WebSphere Application Server V7.0 - <node agent service name>"`.
Press **Enter.**
For example: `net stop "IBM WebSphere Application Server V7.0 - Custom01_nodeagent"`.

The screen ends with the following line:

```
The IBM WebSphere Application Server V7.0 - Custom01_nodeagent service was stopped successfully.
```

Stopping and starting the IMS Server applications

Learn how to restart the IMS Server applications with the Integrated Solutions Console.

About this task

- For IMS Server applications such as AccessAdmin, AccessAssistant and Web Workplace, restart ISAMESSOIMS.
- For IMS Server applications such as IMS Configuration Wizard and IMS Configuration Utility, restart ISAMESSOIMSConfig.

Procedure

1. Select **Start** > **All Programs** > **IBM WebSphere** > **Application Server <version>** > **Profiles** > **<profile name>** > **Administrative console**.
2. Log on to the Integrated Solutions Console.
3. On the Integrated Solutions Console navigation pane, select **Applications** > **Application Types** > **WebSphere Enterprise Applications**.
4. Select the following check boxes:
 - ISAMESSOIMS
 - ISAMESSOIMSConfig
5. Click **Stop**.
6. (For network deployments only), do a full resynchronization of the nodes. See “Resynchronizing the nodes” on page 201.
7. Select the following check boxes:
 - ISAMESSOIMS
 - ISAMESSOIMSConfig
8. Click **Start**.

Deploying IMS Server on WebSphere Application Server manually

You can deploy IMS Server manually if you did not deploy the IMS Server on WebSphere Application Server. You can also do this task if the installer was not able to deploy any one of the IMS Server EAR files.

Before you begin

- Prepare the WebSphere Application Server.
- Enable application security in WebSphere Application Server.
- Review the planning worksheet for the different data required to complete the installation. See Appendix A, “Planning worksheet,” on page 163.

Procedure

1. Copy the isamesso folder from <ims_home> to the following directories:

Stand-alone deployment

<was_home>\profiles\<AppSrv_profilename>\config

Network deployment

<was_home>\profiles\<Dmgr_profilename>\config

2. Optional: Install the Native Library Invoker resource adapter.
3. Set up the command-line tool environment.
4. Deploy the IMS Server EAR files on WebSphere Application Server.

Stand-alone deployment

Deploy ISAMESS0IMS and ISAMESS0IMSConfig on the application server.

See “Installing the IMS Server EAR files manually” on page 200.

Network deployment

- a. Deploy ISAMESS0IMSConfig on deployment manager by using the command line. See “Installing the IMS Server EAR files (command-line)” on page 201.
 - b. Deploy ISAMESS0IMS to the cluster by using the Integrated Solutions Console. See “Installing the IMS Server EAR files manually” on page 200.
5. For WebSphere Application Server Network Deployment, perform a full resynchronization of the nodes.

Enabling application security in WebSphere Application Server

You must enable application security if you deploy the IMS Server EAR files manually to an existing IBM WebSphere Application Server. If you are installing the IMS Server with the installer, the process of enabling application security is automated, and you do not need to do this.

About this task

If application security is not enabled, the setup application cannot enable form-based security in the IMS Configuration Utility.

Procedure

1. Select **Start > All Programs > IBM WebSphere > Application Server <version> > Profiles > <profile name> > Administrative console**.
2. Log on to the Integrated Solutions Console.
3. On the Integrated Solutions Console navigation pane, select **Security > Global security**.
4. On the **Global security** page, select **Enable application security**.
5. Click **Apply**.
6. Click **Save**.

Results

You enabled WebSphere Application Server application security.

Note: After application security is enabled, provide WebSphere administrative privileges as arguments when you stop the server or nodes from the command line.

Installing the Native Library Invoker resource adapter

If you want to have biometric support, install the Native Library Invoker (NLI) resource adapter on every node in the WebSphere Application Server cluster.

About this task

The IMS Server installer does not deploy the Native Library Invoker resource adapter automatically to WebSphere Application Server. If you need BIO-key support for fingerprint or biometric verification systems, you must manually install this resource adapter on every node in the WebSphere cluster. After you install the adapter, specify the JNDI key for the resource adapter so that the adapter can be accessed.

Procedure

1. Select **Start > All Programs > IBM WebSphere > Application Server <version> > Profiles > <profile name> > Administrative console.**
2. Log on to the Integrated Solutions Console.
3. On the Integrated Solutions Console navigation pane, select **Resources > Resource Adapters > Resource adapters.**
4. Click **Install RAR.** The **Install RAR File** page is displayed.
5. Under **Scope**, select the node on which the NLI RAR file is to be installed.
6. Under **Path**, select **Local file system** and then provide the full path to the `com.ibm.tamesso.ims-delhi.j2c.adapters.win32.rar` file in `<ims_home>`.
7. Click **Next.** The General Properties of the new resource adapter is displayed.
8. Keep the default values. Click **OK.**
9. In the **Messages**, click **Save.**
10. Add the JNDI key for the NLI resource adapter to the connection factory.
 - a. Click **ISAM E-SSO IMS Server Native Library Invoker J2C Resource.** The General Properties of the new resource adapter is displayed.
 - b. Under **Additional Properties**, click **J2C connection factories.**
 - c. Click **New.** The General Properties of the connection factory is displayed.
 - d. Enter `TAMESSO_NLI_J2C_ConnFactory` in the **Name** field.
 - e. Enter `tamesso/nli/j2c/shared` in the **JNDI name** field.
 - f. Retain the default values for the rest of the fields.
 - g. Click **OK.**
 - h. In the **Messages** box at the top of the page, click **Save.**
11. Restart the WebSphere Application Server.

Setting up the command-line tool environment

The setup command-line tool defines the environment variables for the command line and scripts to run successfully.

Procedure

1. Open the IMS Server installation bin directory. For example: `C:\Program Files\IBM\ISAM ESSO\IMS Server\bin.`
2. Open `setupCmdLine.bat` with a text editor.
3. Change the value for the `SET WAS_PROFILE_HOME` variable.
 - For Stand-alone deployments: Change the value to the WebSphere Application Server profile root folder. For example: `C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01.`
 - For Network deployments: Change the value to the WebSphere Application Server deployment manager profile root folder. For example: `C:\Program Files\IBM\WebSphere\AppServer\profiles\Dmgr01.`

4. Save the file.

Installing the IMS Server EAR files manually

IMS Server has two EAR files, ISAMESS0IMS and ISAMESS0IMSConfig. Learn how to manually install the IMS Server EAR files on a WebSphere Application Server stand-alone deployment.

Before you begin

- Review the planning worksheet for the data required to complete the installation.
- Enable application security on WebSphere Application Server.

About this task

Use this procedure for either of these scenarios:

- Deploy ISAMESS0IMSConfig and ISAMESS0IMS for WebSphere Application Server stand-alone deployments.
- Deploy ISAMESS0IMS for WebSphere Application Server Network Deployment.

Important: You must deploy ISAMESS0IMSConfig for WebSphere Application Server Network Deployment by using the command-line only. See “Installing the IMS Server EAR files (command-line)” on page 201.

Deploy ISAMESS0IMSConfig before ISAMESS0IMS. The EAR files are stopped by default when you deploy these files manually.

Procedure

1. Start the administrative console. Select **Start > All Programs > IBM WebSphere > Application Server<version> > Profiles > <profile name> > Administrative console**.
2. Log on to the Integrated Solutions Console.
3. On the Integrated Solutions Console navigation pane, click **Applications > Application Types > WebSphere enterprise applications**.
4. Click **Install**.
5. Under **Path**, click **Browse**. The com.ibm.tamesso.ims-delhi.deploy.isamessoIm.s.ear file is located by default in C:\Program Files\IBM\ISAM ESS0\IMS Server\.
6. Click **Next**. The Preparing for the application installation page is displayed.
7. Select **Fast Path - Prompt only when additional information is required**.
8. Click **Next**. The **Install New Application** page is displayed.
9. Retain the default values under **Select installation options**.
10. Click **Next**.
11. Select all modules.
12. Specify the target clusters and web servers in the **Clusters and servers** field. The web server is selected by default.
13. Click **Apply**.
14. Click **Next**.
15. Click **Finish**.
16. Click **Save**.

What to do next

To deploy ISAMESSOIMSConfig on a cluster, use the command-line tool.

Installing the IMS Server EAR files (command-line)

IMS Server has two EAR files, ISAMESSOIMS and ISAMESSOIMSConfig. Learn how to manually install the IMS Server EAR files on WebSphere Application Server Network Deployment.

Before you begin

- Review the planning worksheet for the data required to complete the installation.
- Enable application security in WebSphere Application Server.
- Set up the command-line tool environment.

About this task

Deploy ISAMESSOIMSConfig before ISAMESSOIMS. The EAR files are stopped by default when you deploy these files manually.

Procedure

1. On the **Start** menu, click **Run**.
2. In **Open**, type `cmd`.
3. In the command prompt window, browse to the `<ims_home>\bin` directory. For example: `C:\Program Files\IBM\ISAM ESSO\IMS Server\bin`.
4. If you are using WebSphere Application Server stand-alone:
 - a. Run `deployIsamessoConfig.bat`. For example:
deployIsamessoConfig.bat *<WAS Admin user ID>* *<password>*
 - b. Run `deployIsamesso.bat`. For example:
deployIsamesso.bat *<WAS Admin user ID>* *<password>*
5. If you are using WebSphere Application Server network deployment:
 - a. Run `deployIsamessoConfig.bat`. For example:
deployIsamessoConfig.bat *<WAS Admin user ID>* *<password>*

What to do next

Update the ISAMESSOIMS module mapping.

Resynchronizing the nodes

Resource resynchronization is required whenever an IMS Server application creates a resource such as data source and certificates. This task is also required when there are changes in the enterprise directory. In a WebSphere Application Server Network Deployment, all resources are created first in the deployment manager where the IMS Server is installed.

Before you begin

- Ensure that the nodes are started.

Procedure

1. Select **Start** > **All Programs** > **IBM WebSphere** > **Application Server** *<version>* > **Profiles** > *<profile name>* > **Administrative console**.

2. Log on to the Integrated Solutions Console.
3. On the Integrated Solutions Console navigation pane, select **System administration > Nodes**.
4. Select the check box for the node where the IMS Server is installed.
5. Click **Full Resynchronize**.

Installing the web server plug-in for WebSphere Application Server manually

Install the WebSphere plug-in where the web server host exists. You must install the web server plug-in for WebSphere Application Server manually if you skipped the plug-in installation during the IBM HTTP Server installation. You can skip the plug-in installation if the plug-in is already installed with IBM HTTP Server.

Procedure

1. On the host where you installed IBM HTTP Server, log on as the administrator.
2. In the location where you extracted the WebSphere Application Server supplementary disk (C1G2HML), browse to the plug-in directory. For example: c:\images\C1G2HML\plug-in
3. Click **install.exe**.
4. On the **Welcome** panel, clear the **Installation road map: Overview and installation scenarios** check box.
5. Click **Next**.
6. Accept the license agreement.
7. Click **Next**.
8. After the system prerequisites check completes successfully, click **Next**.
9. From the plug-in selection panel, select the web server plug-in then click **Next**. For example: **IBM HTTP Server V7**.
10. From the installation scenario, click **WebSphere Application Server machine (local)**.

If the Application Server and the web server are on the same host
Click **WebSphere Application Server machine (local)**.

If the Application Server and the web server are not on the same host
Click **Web server machine (remote)**.

11. In the installation directory panel, accept the default values. For example: <ihs_home>\Plugins
12. Click **Next**.
13. (If the WebSphere Application Server is local) Complete the following steps:
 - a. Select the WebSphere Application Server. For example: C:\Program Files\IBM\WebSphere\AppServer.
 - b. Click **Next**.
 - c. Follow the instructions in the wizard to complete the plug-in installation for a local WebSphere Application Server.
14. (If the WebSphere Application Server is remote) From the web server configuration panel, specify the following values:

Select the existing IBM HTTP Server httpd.conf file

Browse to the location of the httpd.conf file; the default is <ihs_home>/conf/httpd.conf

Specify the Web server port

The default is port 80.

Clicking **Next** might produce a warning message that indicates the selected IBM HTTP Server already contains plug-in entries. If you proceed, this new configuration file is updated with a new `plug-in-cfg.xml` file. You can click **OK** to proceed.

15. From the web server definition panel, specify a unique web server definition name. For example: the default value is `webserver1`. For example: If you are installing the plug-in for a second HTTP Server, the value is `webserver2`.
 - a. Accept the default web server plug-in configuration file name (`plug-in-cfg.xml`) and location.
 - b. Click **Next** to acknowledge the manual configuration steps.
 - c. When the installation completes, click **Next**.
16. Restart the WebSphere Application Server. On the application server host, type the following commands in a command prompt.

For stand-alone product deployments (without a deployment manager node) To restart the application server:

```
<was_home>\profiles\AppSrv01\bin\stopServer.bat server1  
<was_home>\profiles\AppSrv01\bin\startServer.bat server1
```

For network deployments

To restart the deployment manager:

```
<was_home>\profiles\Dmgr01\bin\stopManager.bat  
<was_home>\profiles\Dmgr01\bin\startManager.bat
```

Note: If WebSphere Application Server is in a remote location, this step is completed by logging on to the WebSphere Application Server deployment manager host.

Results

You installed the WebSphere plug-in for IBM HTTP Server. You restarted the IBM HTTP Server, and Admin Server services.

What to do next

You are ready to apply the latest WebSphere plug-in fix pack for IBM HTTP Server.

Creating the database in SQL Server manually

When you create the IMS Server database in Microsoft SQL Server 2005 and 2008 manually, you must specify the correct attributes for the logon name, user and collation.

Procedure

1. Log on to the SQL Server Management Studio with `sa` credentials.
2. Create a database.
 - a. In the **Object Explorer** panel, right-click **Databases**.
 - b. Click **New Database**.
 - c. In the **Database Name** field, provide the database name. For example: `imsdb`
3. Set the collation.

- a. In the **Select a Page** panel, click **Options**.
- b. From the **Collation** list, select the collation **SQL_Latin1_General_CP1_CS_AS**.
- c. Click **OK**.
4. Create a SQL Server logon. For example: imsdbusr
 - a. In the **Object Explorer** panel, expand **Security > Logins**.
 - b. Select **Logins**, right-click **New Login**, and select **SQL Server authentication**.
 - c. Enter a logon name. For example: imsdbusr
 - d. Enter the password twice.
 - e. Clear the **Enforce password policy** check box.
 - f. For **Default Database**, select the database you created in step 2 on page 203.
 - g. Click **OK**.
5. Create a user.
 - a. In the **Object Explorer** panel, expand **Databases > <dbname> > Security > Users**.
 - b. Select **Users**.
 - c. Right-click **Users** and select **New User**.
 - d. In each of the following fields, type the same name that you specified in step 4 :
 - **User name**
 - **Login name**
 - **Default schema**
 For example: imsdbusr
 - e. In the **Database role membership** panel, select db_owner.
 - f. Click **OK**.
6. Add the schema.
 - a. In the **Object Explorer** panel, expand **Databases > <dbname> > Security > Schemas**.
 - b. Click **New Schema**.
 - c. Type the name you specified in step 4, for each of the following fields:
 - **Schema name**
 - **Schema owner**
 For example: imsdbusr
 - d. Click **OK**.
7. Close SQL Server Management Studio.

Basic commands for managing WebSphere Application Server profiles

You can use basic command-line tools to list, validate, and delete WebSphere Application Server profiles.

The following case-sensitive commands can be useful for managing profiles in WebSphere Application Server:

Task	Command
Delete a profile	<was_home>/bin/manageprofiles.bat -delete -profileName <i>profile name</i>

Task	Command
Refresh the registry (for example, after deleting a profile)	<was_home>/bin/manageprofiles.bat -validateandupdateregistry
List existing profiles	<was_home>/bin/manageprofiles.bat -listProfiles

For information about the complete list of WebSphere Application Server commands for managing profiles, see the WebSphere Application Server 7.0 information center: <http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp>.

Search for managing profiles using commands.

For information about the provided command-line tools for IBM Security Access Manager for Enterprise Single Sign-On, see the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

Ways of resolving hosts and IP addresses

You can use a hosts file or a domain name server to resolve host names and IP addresses on a stand-alone or distributed deployment.

Resolving host names with a DNS server

If you are using a name server or DNS server to resolve host names, the host name must be configured on the DNS server. The host name you configure on the DNS server must also match the host name configured in the operating system.

1. To check the host name on the operating system, in a command prompt, type:

```
hostname
```

For example: If the computer is `ibm1`, the system displays the following result:

```
ibm1
```

2. Verify the computer name information:
 - a. Right-click **My Computer**.
 - b. Click **Properties**.
 - c. Click the **Computer Name** tab.
 - d. Verify that the **Full computer name** field displays the fully qualified domain name of the computer. For example `ibm1.example.com`

Note: To view the NetBIOS name for the local computer, click **Change**, then click **More**. Alternatively, in a command prompt, type `nbtstat -n`.

3. Check the host name configured on the DNS server. Run the following command:

```
nslookup host_name
```

Where `host_name` is the host name.

The `nslookup` command returns the fully qualified domain name configured on the DNS server. For example: `ibm1.example.com`.

4. Check that the host is responding. You can run the following command:

```
ping host_name
```

Where `host_name` is the host name.

Note: In some environments, the **ping** command might fail if the computer is configured to ignore ping requests. Check with your network administrator for alternative ways, if the problem persists.

Resolving host names with a hosts file

Domain names or IP addresses on a local computer can be resolved by adding entries in the local hosts file on a computer. Entries in the local hosts file have the added advantage that the system can run the application server, even when disconnected from the network. If you are using a hosts file to resolve IP addresses, the file must be configured correctly.

The location of the hosts file for:

Windows

`SystemDrive:\Windows\System32\Drivers\etc\`

Linux `/etc/hosts`

The file must include the following information:

- The IP address, fully qualified domain name, and the host name of the computer.
- The IP address 127.0.0.1, the fully qualified domain name localhost.localdomain, and the host name localhost.

For example: for a computer with a host name `ibm1`, the hosts file might contain the following entries:

#IP address	Fully Qualified Domain Name	Short Name
102.54.11.38	ibm1.example.com	ibm1
127.0.0.1	localhost.localdomain	localhost

Renewing the SSL Certificate used by the IBM HTTP Server

If a personal certificate is compromised or is about to expire, renew the certificate.

About this task

The default expiration of a certificate is one year. Renewing a certificate re-creates all the information from the original certificate except the expiration date and key pair. The renewed certificate contains a new expiration date, and a public or private key pair. If the certificate for signing the chained certificate is not in the root keystore; then use the default root certificate to renew the certificate.

Procedure

1. Select **Start > All Programs > IBM WebSphere > Application Server <version> > Profiles > <profile name> > Administrative console**.
2. Log on to the IBM Integrated Solutions Console.
3. On the IBM Integrated Solutions Console navigation pane, click **Servers > Server Types > Web servers**.
4. Click the `<Web server name>`.
5. In the **Additional Properties** section on the **Configuration** tab, click **Plug-in properties**.
6. Under **Repository copy of Web server plug-in files**, click **Manage keys and certificates**.
7. Under the **Additional properties** list, click **Personal certificates**.

8. Select **default**.
9. Click **Renew**.
10. Click **Save** directly to the master configuration.
11. Click the **Plug-in properties** link.
12. Under **Repository copy of Web server plug-in files**, click **Copy to Web server key store directory**.
13. For WebSphere Application Server network deployment:
 - a. Propagate the web server plug-in configuration.
 - b. Resynchronize the nodes with the deployment manager.
14. Restart the IBM HTTP Server.

Adding the IMS Root CA to the truststore

If the WebSphere Application Server uses a non-default truststore, you must add the IMS Root CA to the truststore.

Procedure

1. Extract the certificate:
 - a. In the IBM Integrated Solutions Console navigation pane, click **Security > SSL certificate and key management**.
 - b. On the **SSL certificate and key management** page, under **Related Items**, select **Key stores and certificates**.
 - c. Click **TAMESSOIMSKeystore** from the table.
 - d. From the **TAMESSOIMSKeystore** page, under **Additional Properties**, click **Personal certificates**.
 - e. Select **<imsrootca>** from the table.
 - f. Click **Extract**.
2. In the **Certificate file name** field, specify the appropriate file path.
3. Choose **Base64-encoded ASCII data** from the **Data type** list.
4. Click **OK**.
5. In the IBM Integrated Solutions Console, click **Security > SSL certificate and key management**.
6. On the **SSL certificate, and key management** page, under **Related Items**, select **Key stores and certificates**.
7. Click the truststore.

For a WebSphere Application Server stand-alone deployment
Click **NodeDefaultTrustStore**.

For a WebSphere Application Server Network Deployment
Click **CellDefaultTrustStore** and all **NodeDefaultTrustStore**.

8. Under **Additional Properties**, click **Signer certificates**.
9. Click **Add**.
10. Enter **<imsrootca>** in the **Alias** field.
11. In the **File name** field, specify the file path from where you extracted the certificate in, as specified in the step 2.
12. Choose **Base64-encoded ASCII data** from the **Data type** list.
13. Click **OK**.
14. In the **Messages** box, click **Save**.
15. Delete the extracted certificate in step 2 from the file system.

Adding the directory server SSL certificate to WebSphere Application Server

If the directory server connection is SSL enabled, you must add the certificates from the directory server to WebSphere Application Server. Retrieving the certificate ensures that you can establish a connection between the directory server and WebSphere Application Server. Ensure that the SSL connection is successful before you configure the IMS Server for directory servers.

Before you begin

- Prepare the directory server.
- Configure the directory server for SSL. For more information, see the directory server documentation.
- Start the directory server.
- Prepare the WebSphere Application Server.
- Start the WebSphere Application Server.
- Ensure that the host names between the computers can be resolved.
- Ensure that you can log on with WebSphere Application Server administrator privileges.

About this task

This task applies only to directory servers with SSL enabled.

Procedure

1. Log on to the WebSphere Application Server administrator console.
2. In the navigation panel, click **Security > SSL certificate and key management**.
3. Under **Related Items**, click **Key stores and certificates**.
4. Open the truststore.

For stand-alone deployments

Click **NodeDefaultTrustStore**.

For network deployments

Click **CellDefaultTrustStore**.

5. Under **Additional Properties**, click **Signer Certificates**.
6. Click **Retrieve from port**.
7. Specify the following fields:
 - Host** Type the host name, IP or fully qualified domain name of the directory server.
 - Port** Type the SSL port number for the directory server. The typical SSL port number is 636.
 - Alias** Type the certificate alias name to reference the signer in the configuration. For example: myldap1
8. Click **Retrieve signer information**. Information about the SSL signer information is displayed.
9. Click **OK**.
10. In the **Messages** box, click **Save**.
11. For network deployment, resynchronize the nodes.

Retrieving the IBM HTTP Server administrator name and password

If you cannot remember the IBM HTTP Server administrator credentials, see the `admin.passwd` file. You can also reset the password with the `htpasswd` utility.

To retrieve the IBM HTTP Server administrator name:

1. Browse to the `<ihs_home>\conf` directory. For example: `C:\Program Files\IBM\HTTPServer\conf`
2. Open the `admin.passwd` file.

To reset the password:

1. Open the command-line tool.
2. Navigate to `<ihs_home>\conf`.
3. Enter "`<ihs_home>\bin\htpasswd.exe admin.passwd <webserver admin name>`".

Uninstalling the TAM E-SSO IMS application from WebSphere Application Server

Uninstall the TAM E-SSO IMS Server 8.1 application in the Integrated Solutions Console before you start an upgrade.

Procedure

1. Select **Start > All Programs > IBM WebSphere > Application Server <version> > Profiles > <profile name> > Administrative console**.
2. Log on to the Integrated Solutions Console.
3. On the Integrated Solutions Console navigation pane, select **Applications > Application Types > WebSphere Enterprise Applications**.
4. Select the **TAM E-SSO IMS** check box.
5. Click **Uninstall**.
6. Click **Save**.

Results

You successfully removed the TAM E-SSO IMS Server 8.1 application from WebSphere Application Server.

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.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

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

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

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

Licensees of this program who wish to have information about it 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.

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.



Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Glossary

AccessAdmin. A web-based management console that Administrators and Helpdesk officers use to administer the IMS Server and to manage users and policies.

AccessAgent plug-in. A piece of script, written in VBscript or Javascript, that is embedded within an AccessProfile to perform custom checking of conditions or to execute custom actions. It is used for extending the capability of an AccessProfile beyond the built-in triggers and actions.

AccessAgent. The client software that manages the identity of the user, authenticates the user, and automates single sign-on and sign-off.

AccessAssistant. The web-based interface that helps users to reset their passwords and retrieve their application credentials.

AccessProfile widget / widget. An independent AccessProfile that consists of pinnable states, which can be used to build another AccessProfile.

AccessProfiles. AccessAgent uses these XML specifications to identify application screens that it can perform single sign-on and automation.

AccessStudio. An application used by Administrators for creating and maintaining AccessProfiles.

Account data bag. A data structure that holds user credentials in memory while single sign-on is performed on an application.

Account data item template. A template that defines the properties of an account data item.

Account data item. The user credentials required for logon.

Account data template. A template that defines the format of account data to be stored for credentials captured by using a specific AccessProfile.

Account data. The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

Action. In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD). A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credentials. The Active Directory user name and password.

Active Directory password synchronization. An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

Active RFID (ARFID). ARFID is both a second authentication factor and a presence detector. It can detect the presence of a user and AccessAgent can be configured to perform specific actions. In previous releases, it is called Active Proximity Badge.

ActiveCode. Short-lived authentication codes that are generated and verified by IBM Security Access Manager for Enterprise Single Sign-On. There are two types of ActiveCodes: Mobile ActiveCodes and Predictive ActiveCodes.

Mobile ActiveCodes are generated by IBM Security Access Manager for Enterprise Single Sign-On and dispatched to the mobile phone or email account of the user. Predictive ActiveCodes, or One Time Passwords, are generated from OTP tokens when a user presses its button.

Combined with alternative channels or devices, ActiveCodes provide effective second-factor authentication.

Administrator. A person responsible for administrative tasks such as access authorization and content management. Administrators can also grant levels of authority to users.

Application policies. A collection of policies and attributes governing access to applications.

Application programming interface (API). An interface that allows an application program written in a high-level language to use specific data or functions of the operating system or another program.

Application. One or more computer programs or software components that provide a function in direct support of a specific business process or processes. In AccessStudio, it is the system that provides the user interface for reading or entering the authentication credentials.

Audit. A process that logs the user, Administrator, and Helpdesk activities.

Authentication factor. The different devices, biometrics, or secrets required as credentials for validating digital identities. Examples of authentication

factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

Authentication service. In IBM Security Access Manager for Enterprise Single Sign-On, a service that verifies the validity of an account against their own user store or against a corporate directory. Identifies the authentication service associated with a screen. Account data saved under a particular authentication service is retrieved and auto-filled for the logon screen that is defined. Account data captured from the logon screen defined is saved under this authentication service.

Authorization code. An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass with AccessAgent, AccessAssistant, and Web Workplace.

Auto-capture. A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

Automatic sign-on. A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

Base distinguished name. A name that indicates the starting point for searches in the directory server.

Bidirectional language. A language that uses a script, such as Arabic and Hebrew, whose general flow of text proceeds horizontally from right to left, but numbers, English, and other left-to-right language text are written from left to right.

Bind distinguished name. A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also *Distinguished name*.

Biometrics. The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

Card Serial Number (CSN). A unique data item that identifies a hybrid smart card. It has no relation to the certificates installed in the smart card

Cell. In WebSphere Application Server, a cell is a virtual unit that consists of a deployment manager and one or more nodes.

Certificate authority (CA). A trusted organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate.

IMS Server Certificate. Used in IBM Security Access Manager for Enterprise Single Sign-On. The IMS Server Certificate allows clients to identify and authenticate an IMS Server.

Client AccessAgent. AccessAgent installed and running on the client machine.

Client workstation, client machine, client computers. Computers where AccessAgent installed.

Clinical Context Object Workgroup (CCOW). A vendor independent standard, for the interchange of information between clinical applications in the healthcare industry.

Clustering. In WebSphere Application Server, clustering is the ability to group application servers.

Clusters. A group of application servers that collaborate for the purposes of workload balancing and failover.

Command line interface. A computer interface in which the input command is a string of text characters.

Credentials. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

Cryptographic application programming interface (CAPI). An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP). A feature of the i5/OS® operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

Data source. The means by which an application accesses data from a database.

Database (DB) server. A software program that uses a database manager to provide database services to software programs or computers.

DB2. A family of IBM licensed programs for relational database management.

Deployment manager profiles. A WebSphere Application Server runtime environment that manages operations for a logical group, or cell, of other servers.

Deployment manager. A server that manages and configures operations for a logical group or cell of other servers.

Deprovision. To remove a service or component. For example, to deprovision an account means to delete an account from a resource.

Desktop application. Application that runs in a desktop.

Desktop Manager. Manages concurrent user desktops on a single workstation

Direct auth-info. In profiling, direct auth-info is a direct reference to an existing authentication service.

Directory service. A directory of names, profile information, and computer addresses of every user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, or an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

Directory. A file that contains the names and controlling information for objects or other directories.

Disaster recovery site. A secondary location for the production environment in case of a disaster.

Disaster recovery. The process of restoring a database, system, policies after a partial or complete site failure that was caused by a catastrophic event such as an earthquake or fire. Typically, disaster recovery requires a full backup at another location.

Distinguished name. The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region.

Distributed IMS Server. The IMS Servers are deployed in multiple geographical locations.

Domain name server (DNS). A server program that supplies name-to-address conversion by mapping domain names to IP addresses.

Dynamic link library (DLL). A file containing executable code and data bound to a program at load time or run time, rather than during linking. The code and data in a DLL can be shared by several applications simultaneously.

Enterprise directory. A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

Enterprise Single Sign-On (ESSO). A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

Enterprise user name. The user name of a user account in the enterprise directory.

ESSO audit logs. A log file that contains a record of system events and responses. ESSO audit logs are stored in the IMS Database.

ESSO Credential Provider. Previously known as the Encentuate Credential Provider (EnCredentialProvider), this is the IBM Security Access Manager for Enterprise Single Sign-On GINA for Windows Vista and Windows 7.

ESSO credentials. The ISAM ESSO user name and password.

ESSO GINA. Previously known as the Encentuate GINA (EnGINA). IBM Security Access Manager for Enterprise Single Sign-On GINA provides a user interface that is integrated with authentication factors and provide password resets and second factor bypass options.

ESSO Network Provider. Previously known as the Encentuate Network Provider (EnNetworkProvider). An AccessAgent module that captures the Active Directory server credentials and uses these credentials to automatically log on the users to their Wallet.

ESSO password. The password that secures access to the user Wallet.

Event code. A code that represents a specific event that is tracked and logged into the audit log tables.

Failover. An automatic operation that switches to a redundant or standby system in the event of a software, hardware, or network interruption.

Fast user switching. A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS). A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

Fix pack. A cumulative collection of fixes that is made available between scheduled refresh packs, manufacturing refreshes, or releases. It is intended to allow customers to move to a specific maintenance level.

Fully qualified domain name (FQDN). In Internet communications, the name of a host system that

includes all of the subnames of the domain name. An example of a fully qualified domain name is rchland.vnet.ibm.com.

Graphical Identification and Authentication (GINA).

A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

Group Policy Object (GPO). A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

High availability (HA). The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

Host name. In Internet communication, the name given to a computer. The host name might be a fully qualified domain name such as mycomputer.city.company.com, or it might be a specific subname such as mycomputer.

Hot key. A key sequence used to shift operations between different applications or between different functions of an application.

Hybrid smart card. An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

IBM HTTP server. A web server. IBM offers a web server, called the IBM HTTP Server, that accepts requests from clients and forward to the application server.

IMS Bridge. A module embedded in third-party applications and systems to call to IMS APIs for provisioning and other purposes.

IMS Configuration Utility. A utility of the IMS Server that allows Administrators to manage lower-level configuration settings for the IMS Server.

IMS Configuration wizard. Administrators use the wizard to configure the IMS Server during installation.

IMS Connector. A module that connects IMS to external systems to dispatch a mobile active code to a messaging gateway.

IMS data source. A WebSphere Application Server configuration object that defines the location and parameters for accessing the IMS database.

IMS Database. The relational database where the IMS Server stores all ESSO system, machine, and user data and audit logs.

IMS Root CA. The root certificate authority that signs certificates for securing traffic between AccessAgent and IMS Server.

IMS Server. An integrated management system for ISAM ESSO that provides a central point of secure access administration for an enterprise. It enables centralized management of user identities, AccessProfiles, authentication policies, provides loss management, certificate management, and audit management for the enterprise.

Indirect auth-info. In profiling, indirect auth-info is an indirect reference to an existing authentication service.

Interactive graphical mode. A series of panels that prompts for information to complete the installation.

IP address. A unique address for a device or logical unit on a network that uses the Internet Protocol standard.

Java Management Extensions (JMX). A means of doing management of and through Java technology. JMX is a universal, open extension of the Java programming language for management that can be deployed across all industries, wherever management is needed.

Java runtime environment (JRE). A subset of a Java developer kit that contains the core executable programs and files that constitute the standard Java platform. The JRE includes the Java virtual machine (JVM), core classes, and supporting files.

Java virtual machine (JVM). A software implementation of a processor that runs compiled Java code (applets and applications).

Keystore. In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted, or public, keys.

Lightweight Directory Access Protocol (LDAP). An open protocol that uses TCP/IP to provide access to directories that support an X.500 model. An LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

Lightweight mode. A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

Load balancing. The monitoring of application servers and management of the workload on servers. If one server exceeds its workload, requests are forwarded to another server with more capacity.

Lookup user. A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

Main AccessProfile. The AccessProfile that contains one or more AccessProfile widgets

Managed node. A node that is federated to a deployment manager and contains a node agent and can contain managed servers.

Microsoft Cryptographic application programming interface (CAPI). An interface specification from Microsoft for modules that provide cryptographic functionality and that allow access to smart cards.

Mobile ActiveCode (MAC). A one-time password that is used by users for two-factor authentication in Web Workplace, AccessAssistant, and other applications. This OTP is randomly generated and dispatched to user through SMS or email.

Mobile authentication. An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

Network deployment. Also known as a clustered deployment. A type of deployment where the IMS Server is deployed on a WebSphere Application Server cluster.

Node agent. An administrative agent that manages all application servers on a node and represents the node in the management cell.

Nodes. A logical group of managed servers.

One-Time Password (OTP). A one-use password generated for an authentication event, sometimes communicated between the client and the server through a secure channel.

OTP token. A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets.

Password aging. A security feature by which the superuser can specify how often users must change their passwords.

Password complexity policy. A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

Personal applications. Windows and web-based applications where AccessAgent can store and enter credentials.

Some examples of personal applications are web-based mail sites such as Company Mail, Internet banking sites, online shopping sites, chat, or instant messaging programs.

Personal desktop. The desktop is not shared with any other users.

Personal Identification Number (PIN). In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

Pinnable state. A state from the AccessProfile widget that is declared as 'Can be pinned in another AccessProfile'.

Pinned state. A pinnable state that is attached to a state in the main AccessProfile.

Policy template. A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

Portal. A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

Presence detector. A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

Primary authentication factor. The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

Private desktop. Under this desktop scheme, users have their own Windows desktops in a workstation. When a previous user return to the workstation and unlocks it, AccessAgent switches to the desktop session of the previous user and resumes the last task.

Private key. In computer security, the secret half of a cryptographic key pair that is used with a public key algorithm. The private key is known only to its owner. Private keys are typically used to digitally sign data and to decrypt data that has been encrypted with the corresponding public key.

Provisioning API. An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

Provisioning bridge. An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

Provisioning system. A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

Provision. To provide, deploy, and track a service, component, application, or resource.

Public Key Cryptography Standards. A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Published application. Application installed on Citrix XenApp server that can be accessed from Citrix ICA Clients.

Published desktop. A Citrix XenApp feature where users have remote access to a full Windows desktop from any device, anywhere, at any time.

Radio Frequency Identification (RFID). An automatic identification and data capture technology that identifies unique items and transmits data using radio waves.

Random password. An arbitrarily generated password used to increase authentication security between clients and servers.

Registry hive. In Windows systems, the structure of the data stored in the registry.

Registry. A repository that contains access and configuration information for users, systems, and software.

Remote Authentication Dial-In User Service (RADIUS). An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP). A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

Replication. The process of maintaining a defined set of data in more than one location. Replication involves copying designated changes for one location (a source) to another (a target) and synchronizing the data in both locations.

Revoke. To remove a privilege or an authority from an authorization identifier.

Root certificate authority (CA). The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

Scope. A reference to the applicability of a policy, at the system, user, or machine level.

Secret question. A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

Secure Remote Access. The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Sockets Layer (SSL). A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

Secure Sockets Layer virtual private network (SSL VPN). A form of VPN that can be used with a standard web browser.

Security Token Service (STS). A web service used for issuing and exchanging of security tokens.

Security trust service chain. A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

Self-service features. Features in IBM Security Access Manager for Enterprise Single Sign-On which users can use to perform basic tasks such as resetting passwords and secrets with minimal assistance from Help desk or your Administrator.

Serial ID Service Provider Interface (SPI). A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

Serial number. A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On Keys, which is unique to each Key and cannot be changed.

Server AccessAgent. AccessAgent deployed on a Microsoft Windows Terminal Server or a Citrix server.

Server locator. A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

Service Provider Interface (SPI). An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

Session management. Management of user session on private desktops and shared desktops.

Shared desktop. A desktop configuration where multiple users share a generic Windows desktop.

Shared workstation. A workstation shared among users.

Sign up. To request a resource.

sign-on automation. A technology that works with application user interfaces to automate the sign-on process for users.

sign-on information. Information required to provide access to users to any secure application. This information can include user names, passwords, domain information, and certificates.

Signature. In profiling, unique identification information for any application, window, or field.

Silent mode. A method for installing or uninstalling a product component from the command line with no GUI display. When using silent mode, you specify the data required by the installation or uninstallation program directly on the command line or in a file (called an option file or response file).

Simple Mail Transfer Protocol (SMTP). An Internet application protocol for transferring mail among users of the Internet.

Simple Object Access Protocol (SOAP). A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

Single sign-on. An authentication process in which a user can access more than one system or application by entering a single user ID and password.

Smart card middleware. Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

Smart card. An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

Stand-alone deployment. A deployment where the IMS Server is deployed on an independent WebSphere Application Server profile.

Stand-alone server. A fully operational server that is managed independently of all other servers, and it uses its own administrative console.

Strong authentication. A solution that uses multi-factor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

Strong digital identity. An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

System modal message. A system dialog box that is typically used to display important messages. When a system modal message is displayed, nothing else can be selected on the screen until the message is closed.

Terminal emulator. A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal

Thin client. A client machine that has little or no installed software. It has access to applications and desktop sessions that is running on network servers that are connected to it. A thin client machine is an alternative to a full-function client such as a workstation.

Tivoli Common Reporting tool. A reporting component that you can use to create, customize, and manage reports.

Tivoli Identity Manager adapter. An intermediary software component that allows IBM Security Access Manager for Enterprise Single Sign-On to communicate with Tivoli Identity Manager.

Transparent screen lock. A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Trigger. In profiling, an event that causes transitions between states in a states engine, such as, the loading of a web page or the appearance of window on the desktop.

Trust service chain. A chain of modules operating in different modes. For example: validate, map and issue.

Truststore. In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys.

TTY (terminal type). A generic device driver for a text display. A tty typically performs input and output on a character-by-character basis.

Two-factor authentication. The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

Uniform resource identifier. A compact string of characters for identifying an abstract or physical resource.

User credential. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

User deprovisioning. Removing the user account from IBM Security Access Manager for Enterprise Single Sign-On.

User provisioning. The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

Virtual appliance. A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

Virtual channel connector. A connector that is used in a terminal services environment. The virtual channel connector establishes a virtual communication channel to manage the remote sessions between the Client AccessAgent component and the Server AccessAgent.

Virtual Member Manager (VMM). A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

Virtual Private Network (VPN). An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure.

Visual Basic (VB). An event-driven programming language and integrated development environment (IDE) from Microsoft.

Wallet caching. When performing single sign-on for an application, AccessAgent retrieves the logon credentials from the user credential Wallet. The user credential Wallet is downloaded on the user machine and stored securely on the IMS Server. So users can access their Wallet even when they log on to IBM Security Access Manager for Enterprise Single Sign-On from a different machine later.

Wallet manager. The IBM Security Access Manager for Enterprise Single Sign-On GUI component that users can use to manage application credentials in the personal identity Wallet.

Wallet Password. A password that secures access to the Wallet.

Wallet. A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

Web server. A software program that is capable of servicing Hypertext Transfer Protocol (HTTP) requests.

Web service. A self-contained, self-describing modular application that can be published, discovered, and invoked over a network using standard network protocols. Typically, XML is used to tag the data, SOAP is used to transfer the data, WSDL is used for describing the services available, and UDDI is used for listing what services are available.

Web Workplace. A web-based interface that users can log on to enterprise web applications by clicking links without entering the passwords for individual applications. This interface can be integrated with the existing portal or SSL VPN of the customer.

WebSphere Administrative console. A graphical administrative Java application client that makes method calls to resource beans in the administrative server to access or modify a resource within the domain.

WebSphere Application Server profile. The WebSphere Application Server administrator user name and profile. Defines the runtime environment.

WebSphere Application Server. Software that runs on a web server and that can deploy, integrate, execute, and manage e-business applications.

Windows logon screen, Windows logon UI mode. The screen where users enter their user name and password to log on to the Windows desktop.

Windows native fast user switching. A Windows XP feature which allows users to quickly switch between user accounts.

Windows Terminal Services. A Microsoft Windows component that users use to access applications and data on a remote computer over a network.

WS-Trust. A web services security specification that defines a framework for trust models to establish trust between web services.

Index

Numerics

- 1024 bits certificates 66, 95
- 2048 bits certificates 66, 95

A

- AAInstallDir parameter 123
- AboutThisProfile.txt file 52, 76
- AccessAgent
 - Citrix Server 109
 - installation
 - path 126
 - road map 109
 - installation path 123
 - installing interactively 111
 - MSI-based installation 112
 - prerequisites 111
 - setting server connection 127
 - silent installation 121
 - Terminal Server 109
 - uninstalling 155
 - upgrading 146
 - verifying files 115
 - verifying registry entries 115
- accessibility xiii
- AccessStudio
 - installation road map 109
 - packaging custom installers 117
 - silent installation 121
 - uninstalling 156
 - upgrading 147
 - verifying files 115
 - verifying registry entries 115
- addresses 205
- application server profiles
 - network deployment 76
 - stand-alone 52
- Auto Start option
 - clusters 102

B

- base distinguished name
 - Active Directory 180
 - LDAP 185
- base profile 52
- BAT files
 - cleanImsConfig.bat file 159
 - deployIsamesso.bat file 201
 - deployIsamessoConfig.bat file 201
 - manageprofiles.bat file 204
 - setupCmdLine.bat file 199
- bind distinguished name
 - Active Directory 180
 - LDAP 185
- BIO-key 199
- biometric, installing 199
- books
 - See* publications

C

- cat command 42
- Certificate Authority
 - See* root CA
- certificates
 - 1024 bits 66, 95
 - 2048 bits 66, 95
- Citrix Servers 109, 124
- cleanImsConfig.bat file 159
- clusters
 - adding members 105
 - Auto Start option 102
 - configuring WebSphere Application Server 88
 - creating profiles 76
 - defining 88
 - description 75
 - starting 194
- cn attribute 186
- com.ibm.tamesso.ims-delhi.j2c.adapters.win32.rar file 199
- command-line environment
 - stopping and starting middleware 191
- CONF files
 - httpd.conf file 64, 94
- configuration
 - enterprise directory servers 179
 - IBM HTTP Server plug-in 92
 - IMS Server with IMS Configuration Wizard 68
 - WebSphere Application Server
 - clusters 88
 - WebSphere Application Server stand-alone 55
- connections 205
- Console Hook Loader 125
- ConsoleAppSupportEnabled parameter 125
- conventions
 - typeface xiv
- copy command 42
- custom profile 76

D

- database
 - collation 203
 - schema 203
- databases
 - backing up 189
 - DB2 16, 18
 - installing 16
 - Microsoft SQL Server 20
 - Oracle Database 19
 - preparing 15
 - restoring 191
 - virtual appliance 41
- DB2 15
 - database creation 18

- DB2 (*continued*)
 - installing 16
 - preparing 16
 - schema creation 175
 - users, creating 176
- deployIsamesso.bat file 201
- deployIsamessoConfig.bat file 201
- deployment manager profile 76
 - maximum heap size 89
 - starting 194
- DHCP (Dynamic Host Configuration Protocol) 44
- directory names, notation xiv
- directory servers
 - See* enterprise directories
- DisableWin7CAD parameter 125
- distinguished name (DN) 186
- DLL files
 - engina.dll 124
 - EnNetworkProvider.dll file 116
 - MSGina.dll 123
 - nwgina.dll 124
- DNS (Domain Name System) 181, 205
- Domain Name System (DNS) 181
- Dynamic Host Configuration Protocol (DHCP) 44

E

- EAR files 67, 197
 - deploying manually 200
 - installing command-line 201
 - ISAMESSOIMS 33
 - ISAMESSOIMSConfig 33
- education
 - See* Tivoli technical training
- EncentuateCredentialProviderEnabled parameter 124
- EncentuateNetworkProviderEnabled parameter 124
- engina.dll file 124
- EnginaConflictPromptEnabled parameter 124
- EnginaEnabled parameter 124
- EnNetworkProvider.dll file 116
- Enterprise Archive (EAR) 67
- enterprise directories
 - description 179
 - enabling SSL 208
 - generic LDAP Server
 - configuring 187
 - LDAP 32, 179, 185
 - lookup user 180, 185
 - Microsoft Active Directory
 - configuring 179, 180
 - preparing 31
 - preparing 29
 - Tivoli Directory Server
 - configuring 185
 - preparing 32
 - virtual appliance 41

environment variables, notation xiv
ESSO Network Provider
 verifying 116
Export Configuration Utility 189

F

FirstSyncMaxRetries parameter 124
FirstSyncRetryIntervalMins
 parameter 124
fix packs
 IBM HTTP Server 27
 IBM HTTP Server plug-in 28
 WebSphere Application Server 23
 WebSphere Update Installer 22

G

GinaWhiteList parameter 124

H

heap size 89
 deployment manager profile 56, 90
 performance 56, 90
high availability
 clusters 75
 virtual appliance 48
host names
 hostname command 205
 resolving 205
 variables 164
hostname command 205
hosts file 205
httpd.conf file 64, 94, 202

I

IBM HTTP Server 64, 68, 94
 fix packs, installing 27
 installing 24
 plug-in, installing 28
 retrieving administrator
 credentials 209
 starting 192
 stopping 192
 verifying 209
 WebSphere plug-in 61, 92, 202
ikeyman utility 57, 83
IMS Configuration Wizard 68
IMS Root CA 207
IMS Server
 configuring with IMS Configuration
 Wizard 68, 144
 creating database schemas 175
 deploying manually 197
 description 15
 installation road map 3
 installing 3
 EAR files (command-line) 201
 EAR files manually 200
 network deployment 97
 upgrades 141
 with installers 33
 installing stand-alone 67

IMS Server (*continued*)
 ISAMESSOIMS 68
 ISAMESSOIMSConfig 68
 mapping applications 72, 101
 migrating 149
 overriding session management 103
 provisioning 71, 100
 reinstalling 159
 starting 197
 stopping 197
 target server
 command-line 128
 menu shortcut 128
 registry 128
 response file 128
 uninstalling 153
 upgrade road map 131
 upgrading 3, 141
 network deployment 97
 upgrading 3.6 or 8.0 139
 upgrading 8.0.1 to 8.2 145
 verifying
 configurations 73, 104
 WebSphere Application Server
 deployments 36
IMSAddressPromptEnabled
 parameter 126
ImsConfigurationEnabled parameter 124
ImsConfigurationPromptEnabled
 parameter 114, 124
ImsDownloadPortDefault parameter 125
ImsDownloadProtocolDefault
 parameter 125
ImsSecurePortDefault parameter 125
ImsServerName parameter 126
INI files
 SetupHlp.ini file 123
installation
 AccessAgent 111, 114
 AccessStudio 117, 119
 IBM DB2 16
 IBM HTTP Server 24
 IMS Server 33, 197
 prepackaged Wallet 122
 virtual appliance 39
 WebSphere Application Server 20
InstallTypeGpo parameter 124
IP addresses 206
ISAM ESSO AccessAgent.msi file 156
ISAM ESSO AccessStudio.msi file 118,
 157
ISAMESSOIMS 68
 adding nodes 105
 mapping to servers 72, 101
ISAMESSOIMSConfig 68

J

Java Naming and Directory Interface
(JNDI) 199
Java Virtual Machine (JVM) 56, 90
 java.lang.OutOfMemoryError event 89
JNDI (Java Naming and Directory
 Interface) 199
JVM (Java Virtual Machine)
 performance 56, 90

JVMInstallationDirectories
 parameter 125

K

KDB files
 plugin-key.kdb file 64, 94
key.p12 file 171
keystore 57, 83
keystore location 33
keytool command 57, 83

L

language
 transforms 126
LCID 126
LDAP
 adding certificates to WebSphere
 Application Server 208
 SSL-enabled 208
LDAP (Lightweight Directory Access
 Protocol)
 preparing 29
 Tivoli Directory Server 29
LDAP Data Interchange Format
(LDIF) 32
LDIF (LDAP Data Interchange
 Format) 32
LDIF files 32
Lightweight Directory Access Protocol
(LDAP) 29
load balancer 68, 97, 111
log parameter 114, 119
logs
 file location 52, 76
 server installation 68
lookup user
 LDAP servers 185
 Microsoft Active Directory 180

M

machine.wlt file 122
mail attribute 186
manageprofiles command 54, 81, 188,
 189
manageprofiles.bat file 204
manuals
 See publications
Microsoft Active Directory 31
 preparing 29
 Tivoli Identity Manager Active
 Directory Adapter 31
Microsoft Active Directory Application
 Mode (ADAM) 32
Microsoft Active Directory Group Policy
 Object (AD GPO) 126
Microsoft Active Directory Lightweight
 Directory Services (AD LDS) 32
Microsoft AD GPO (Active Directory
 Group Policy Object) 124, 126
Microsoft AD LDS (Active Directory
 Lightweight Directory Services) 32
Microsoft ADAM (Active Directory
 Application Mode) 32

- Microsoft SQL Server
 - creating database 203
 - creating schemas 175
 - preparing
 - database servers 20
 - preparing databases
 - databases 15
- migration, IMS Server 149
- Mozilla Firefox 111, 112
- MSGina.dll 124
- MSI files 112, 114, 119
 - ISAM ESSO AccessAgent.msi file 156
 - ISAM ESSO AccessStudio.msi file 118, 157
 - packaging, for large-scale deployments 121
- msiexec command 114, 119
- MST files 126
- multi-language 126

N

- Native Library Invoker (NLI) 199
- nbtstat command 205
- NetBIOS
 - description 205
 - LDAP configuration 185
 - Microsoft Active Directory configuration 180
- netstat command 33, 52, 76
- Network Time Protocol (NTP) 46
- NLI resource adapter 199
- node agent
 - creating the service 91
 - starting the service 194
 - stopping the service 194
- nodes
 - managed member 76
 - starting 91
 - synchronizing 201
- non-root user 44
 - description 166
- notation
 - environment variables xiv
 - path names xiv
 - typeface xiv
- nslookup command 205
- NTP (Network Time Protocol) 46
- nwgina.dll 124

O

- OldJVMInstallationDirectories
 - parameter 125
- online publications
 - accessing xii
- Oracle Database
 - creating schemas 175
 - preparing 15, 19
- Orca database editor 126
- ordering publications xii
- override session management 103
- OVF files 42

P

- packages, installation 121
- passwords
 - resetting 180
 - synchronizing 180
- path names, notation xiv
- paths
 - planning 163
- performance
 - heap size 56, 90
- planning worksheet
 - directories 163
 - host names 164
 - ports 164
 - profile names 165
 - URLs 164
 - users 165
- plug-in-cfg.xml file 202
- plugin-key.kdb file 64, 94
- port numbers
 - availability 33
 - network deployment 76
 - planning worksheet 164
 - stand-alone deployment 52
- prepackaged Wallet 122
- PriceLevel parameter 124
- profiles
 - backing up 188, 189
 - command-line, creating 54, 81
 - creating interactively 78
 - custom 81
 - deleting 204
 - deployment manager 76, 78
 - exporting 188
 - importing 188
 - IMS Server
 - backing up 189
 - restoring 188
 - listing 204
 - managed nodes, creating 76
 - manageprofiles command 54, 81
 - network deployment 76
 - restoring 189
 - stand-alone 52, 53
 - WebSphere Application Server
 - backing up 188
 - restoring 190
- publications x
 - accessing online xii
 - ordering xii

Q

- quiet parameter 114, 119

R

- RAR files
 - com.ibm.tamesso.ims-delhi.j2c.adapters.win32.rar 199
- RebootConfirmationEnabled
 - parameter 124
- RebootEnabled parameter 124
- reinstalling
 - IMS Server 159
- RemoveWallet parameter 125

- ResetBioAPIPermission parameter 125
- resolution, URL addresses 205
- response file 114, 119, 123
- root CA 68
 - configuring IMS Server 97
 - recreating 57, 83
 - upgrading configurations
 - from 8.0.1 to 8.2 145
 - from 8.1 to 8.2 144
- root user 44
 - description 166

S

- scenarios
 - clustered 10
 - reusing existing middleware 5
 - stand-alone 6
 - virtual appliance 4
- Secure Sockets Layer (SSL)
 - See SSL
- services
 - configuring WebSphere Application Server 55
 - starting 191
 - stopping 191
 - verifying 56
- services.msc command 56
- session management, override 103
- SetupCertDlg command 128
- setupCmdLine.bat file 199
- SetupHlp.ini file 123
- silent
 - See also unattended installation
 - install 112
 - response file parameters 123
 - uninstall 156, 157
- SOAP 33
- split archives 42
- SQL scripts 175
- SQL_Latin1_General_CP1_CS_AS
 - collation 203
- SSL
 - See also root CA
 - Active Directory 182, 208
 - adding directory server certificates 208
 - after upgrading 146
 - chained certificate 61, 92
 - IBM HTTP Server 64, 94
 - LDAP servers 186, 208
 - renewing certificates 206
 - two-way configuration 33
- stand-alone
 - creating profiles 53
 - description 51, 52
- startManager command 194, 202
- startNode command 91, 194
- startServer command 27, 194, 202
- static 44
- stopManager command 195, 202
- stopNode command 195
- stopServer command 23, 195, 202
- synchronization
 - nodes 201
 - password 180

T

- TAM E-SSO IMS Server application
 - uninstalling 209
- Terminal Server 109
- Terminal Servers 124
- Tivoli Common Reporting
 - installing 33
- Tivoli Directory Server 185
 - description 29
 - preparing 32
- Tivoli Identity Manager Active Directory Adapter 180
 - installing 31
- Tivoli Information Center xii
- Tivoli technical training xiii
- Tivoli user groups xiii
- training, Tivoli technical xiii
- transforms parameter 114, 119
- transforms, language 126
- trust.p12 file 171
- truststore
 - creating root CA, before member nodes 83
 - location 33
 - recreating for stand-alone 57
- TXT files
 - AboutThisProfile.txt file 52, 76
- typeface conventions xiv

U

- UAC (User Account Control) 191
- unattended
 - See also* silent
 - response file parameters 123
 - uninstall 156, 157
- uninstall 153
 - AccessAgent silently 156
 - AccessStudio 156
 - AccessStudio silently 157
 - description 153
 - earlier versions 209
 - IMS Server 153
- Update Installer 22
- upgrades 131
 - AccessAgent 141, 146
 - AccessStudio 141
 - IMS Server 141
 - from 3.6 or 8.0 139
 - from 8.0.1 131, 134
 - from 8.1 137, 138
 - port numbers
 - SOAP 141
 - verifying 147
 - virtual appliance 141
- UsbKeyPromptEnabled parameter 124
- User Account Control (UAC) 191
- user groups, Tivoli xiii
- user name attribute 186

V

- variables, notation for xiv
- virtual appliance
 - deploying 42

- virtual appliances
 - activating 44
 - exporting configurations 48
 - high availability 48
 - importing configurations 48
- Virtual Member Manager component
 - configuring directory servers 29
 - configuring IMS Server 179
 - preparing directory servers 29
- VMDK files 42
- VMware 39, 42
- VMware ESXi 42
- vSphere Client 42

W

- Wallets 122
 - preparing prepackaged 122
 - removing prepackaged 123
- WalletTypeSupported parameter 126
- WAS_PROFILE_HOME variable 199
- web server
 - See also* IBM HTTP Server
 - preparing 24
- WebSphere Application Server
 - adding SSL certificates 208
 - cleaning up 159
 - configuring 55
 - enabling application security 198
 - installing 20
 - fix packs 23
 - web server plug-in 202
 - WebSphere Update Installer 22
 - mapping applications 72, 101
 - restoring profiles 190
 - SSL 208
 - verifying services 56
- Windows Installer 112
- wizards
 - IMS Configuration Wizard 68
- WLT files
 - machine.wlt file 122

X

- XML files
 - plug-in-cfg.xml file 202



Printed in USA

GI11-9309-01

