

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

Installation Guide



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

Installation Guide



Note

Before using this information and the product it supports, read the information in “Notices” on page 195.

Edition notice

Note: This edition applies to version 8.2.1 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, 2015.

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

Figures

- | | | | | | |
|----|--|----|----|--|----|
| 1. | Stand-alone production server installation | 42 | 4. | Replacing the root CA and key signers for | |
| 2. | Replacing the root CA and key signers for | | | WebSphere Application Server in the truststore | |
| | with a new key size. | 48 | | with a new key size. | 72 |
| 3. | IBM Security Access Manager for Enterprise | | | | |
| | Single Sign-On in a two-node network | | | | |
| | deployment cluster example for high | | | | |
| | availability.. . . . | 65 | | | |

Contents

Figures iii

About this publication vii

Accessibility	vii
Technical training	vii
Support information	vii
Statement of Good Security Practices.	vii

Chapter 1. Installing the IMS Server. . . 1

IMS Server installation roadmap.	1
Server installation reusing existing middleware.	1
New server installation for stand-alone deployments (end-to-end)	3
New server installation on a clustered deployment (end-to-end)	9
Getting started	15
Preparing the database server	15
Preparing the WebSphere Application Server	19
Preparing the IBM HTTP Server	26
Preparing the directory servers	32
Installing the IMS Server with the IMS Server installer.	36
Setting up a stand-alone production server.	41
Creating and choosing stand-alone server profiles	43
Configuring the WebSphere Application Server	46
Configuring the IBM HTTP Server plug-in (stand-alone)	52
Configuring the IMS Server for a stand-alone deployment	58
Setting up a cluster (network deployment)	64
Creating and choosing profiles for network deployments	66
Configuring WebSphere Application Server for a cluster	76
Configuring the IBM HTTP Server plug-in (network deployment).	80
Configuring the IMS Server for a cluster.	85
Adding application servers to a cluster	92

Chapter 2. Installing AccessAgent and AccessStudio. 95

AccessAgent and AccessStudio installation roadmap	95
Preparing an installation package to install on multiple PCs	96
Remote software distribution methods	96
Silent installation configuration.	96
Preparing and installing a prepackaged Wallet.	96
Response file parameters (SetupHlp.ini)	98
Including support for additional languages	101
Installing the AccessAgent	102
Installing the AccessAgent	103
Installing the AccessAgent silently (command-line)	104
Installing the AccessAgent through Tivoli Endpoint Manager	105

Installing AccessAgent through Group Policy Object	105
Ways of setting the IMS Server location	106
Verifying files and registry entries	107
Verifying the ESSO Network Provider	107
Enabling single sign-on support in Mozilla Firefox Extended Support Release	108
Installing the AccessStudio	110
Installing the AccessStudio (Setup.exe)	110
Installing the AccessStudio (MSI package)	112
Installing the AccessStudio silently (command-line).	112

Chapter 3. Upgrading 115

IMS Server upgrade roadmap	115
Upgrading IMS Server 8.2 for a stand-alone deployment	115
Upgrading IMS Server 8.2 for a network deployment (cluster)	116
Upgrading IMS Server 8.1 for a stand-alone deployment	118
Upgrading IMS Server 8.1 for a network deployment (cluster)	119
Upgrading IMS Server 8.0.1 for a stand-alone deployment	121
Upgrading IMS Server 8.0.1 for a network deployment (cluster)	125
Upgrading IMS Server 3.6 or 8.0	128
Upgrading to 8.2.1.	129
Installing the IMS Server with the installer for an upgrade	129
Upgrading configurations from 8.1 or 8.2 to 8.2.1	132
Upgrading configurations from 8.0.1 to 8.2.1	133
Configuring the SSL certificate after an upgrade	134
Upgrading the AccessAgent	135
Upgrading the AccessStudio	135
Verifying a successful upgrade	135
Migrating the IMS Server 8.2.1 to a new environment.	136

Chapter 4. Uninstalling 139

Uninstalling	139
Uninstalling the IMS Server	139
Uninstalling the AccessAgent	141
Uninstalling the AccessStudio	142
Reinstalling or reconfiguring the IMS Server	143
Cleaning up the IMS Server configuration on WebSphere Application Server.	143

Chapter 5. Planning worksheet 145

Chapter 6. Creating database schemas 157

Creating users manually. 158

Chapter 7. Other installation and configuration tasks 161

Configuring the IMS Server to use directory servers 161

 Configuring the IMS Server to use Active

 Directory servers 162

 Configuring the IMS Server to use LDAP servers 166

 Configuring a generic LDAP directory server other than Tivoli Directory Server 169

Backing up and restoring 169

 Backing up WebSphere Application Server profiles (**manageprofiles** command) 170

 Backing up the IMS Server configuration (Export Configuration Utility) 170

 Backing up the database in DB2 9.7 171

 Backing up the database in DB2 10.1 172

 Restoring the WebSphere Application Server profiles 173

 Restoring the database in DB2. 173

Stopping and starting components 174

 Stopping and starting the IBM HTTP Server on Windows. 174

 Starting the WebSphere Application Server on Windows. 176

 Stopping the WebSphere Application Server on Windows. 178

 Stopping and starting the IMS Server applications 180

Deploying IMS Server on WebSphere Application Server manually 180

 Enabling application security in WebSphere Application Server 181

 Installing the Native Library Invoker resource adapter 182

 Setting up the command-line tool environment 182

 Installing the IMS Server EAR files manually 183

 Installing the IMS Server EAR files (command-line) 184

 Resynchronizing the nodes 184

Installing the web server plug-in for WebSphere

Application Server manually 185

Creating the database in SQL Server manually 187

Basic commands for managing WebSphere

Application Server profiles 188

Ways of resolving hosts and IP addresses 188

Renewing the SSL Certificate used by the IBM HTTP Server 189

Adding the IMS Root CA to the truststore. 190

Adding the directory server SSL certificate to WebSphere Application Server. 191

Retrieving the IBM HTTP Server administrator name and password 192

Uninstalling the TAM E-SSO IMS application from WebSphere Application Server. 192

Uninstalling the ISAMESSOIMS and ISAMESSOIMSConfig applications from

WebSphere Application Server. 193

Notices 195

Glossary 199

A 199

B 200

C 200

D 201

E 202

F 202

G 202

H 202

I. 203

J. 203

K 203

L 203

M 203

N 204

O 204

P 204

R 205

S 205

T 207

U 207

V 207

W 208

Index 209

About this publication

IBM Security Access Manager for Enterprise Single Sign-On Installation Guide provides detailed procedures on installation, upgrade, or uninstallation of IBM® Security Access Manager for Enterprise Single Sign-On.

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*.

Technical training

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

Support information

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

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

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

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

Statement of Good Security Practices

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

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

Chapter 1. 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.

IMS Server installation roadmap

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 on a stand-alone server, or in a clustered environment.

Note: To upgrade from an earlier version of IMS Server, see “IMS Server upgrade roadmap” on page 115.

Before you begin

Before you install the server, complete the following tasks:

1. Plan and prepare for your deployment. Determine the requirements, deployment scenarios, accounts, and security requirements.
See “Planning for deployment” in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.
2. Ensure that you have the Administrator privileges to complete the installation.
3. Use the following roadmaps to determine the best approach to install the server in your environment:
 - “Server installation reusing existing middleware”
 - “New server installation for stand-alone deployments (end-to-end)” on page 3
 - “New server installation on a clustered deployment (end-to-end)” on page 9

Server installation reusing existing middleware

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

	Procedure	Reference
1	<p>Review the middleware requirements to ensure that the existing middleware meets the requirements.</p> <p>With existing WebSphere Application Server 7.0 deployments, you must install the WebSphere Web 2.0 and Mobile feature pack if it is not already installed.</p>	<p>See “Hardware and software requirements” in the <i>IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide</i></p> <p>“Installing the IBM WebSphere Application Server Web 2.0 and Mobile feature pack” on page 25</p>

	Procedure	Reference
2	Configure the WebSphere® Application Server.	<p>For stand-alone deployments:</p> <ul style="list-style-type: none"> • “Creating and choosing stand-alone server profiles” on page 43 • “Configuring the WebSphere Application Server” on page 46 <p>For network deployments:</p> <ul style="list-style-type: none"> • “Creating and choosing profiles for network deployments” on page 66 • “Configuring WebSphere Application Server for a cluster” on page 76 <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 46 • “Verifying the Windows service for WebSphere Application Server” on page 47 • “Re-creating the root CA for WebSphere Application Server 7.0 (stand-alone)” on page 47 <p>WebSphere Application Server Version 7.0 documentation</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp <p>WebSphere Application Server Version 8.5 documentation</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v8r5/index.jsp
3	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 191
4	Configure the IBM HTTP Server.	<ul style="list-style-type: none"> • “Configuring the IBM HTTP Server plug-in (stand-alone)” on page 52 • “Configuring the IBM HTTP Server plug-in (network deployment)” on page 80
5	Deploy the IMS Server applications on the WebSphere Application Server.	“Installing the IMS Server with the IMS Server installer” on page 36
6	Verify the IMS Server deployment on the WebSphere Application Server.	“Verifying the IMS Server deployment on the WebSphere Application Server” on page 39
7	For WebSphere Application Server, Version 8.5 only: Configure the IMS Server deployment with the Sun Reference Implementation 1.2 implementation.	“Configuring the JSF implementation” on page 39
8	For WebSphere Application Server, Version 7.0 only: Add the JAX-RS shared library.	“Adding the JAX-RS shared library” on page 40
9	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 58 • “Configuring the IMS Server to use directory servers” on page 161 • (Network deployment) “Overriding session management for the ISAMESSOIMS” on page 90
10	Provision the IMS Server administrator.	“Provisioning the IMS Server administrator” on page 61

	Procedure	Reference
11	Update the ISAMESSOIMS module mapping to forward connection requests.	"Updating the ISAMESSOIMS module mapping for connection request forwarding" on page 62
12	Verify the IMS Server configuration.	"Verifying the IMS Server configuration" on page 63

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

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

	Procedure	Reference
1	<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 Version 9.7 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>IBM DB2 Version 10.1 documentation</p> <ul style="list-style-type: none"> • http://pic.dhe.ibm.com/infocenter/db2luw/v10r1/index.jsp <p>Microsoft SQL Server 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 Database 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
2	<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 32 <p>Microsoft Active Directory 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>

	Procedure	Reference
3	<p>Prepare the WebSphere Application Server.</p> <p>For WebSphere Application Server Version 7.0:</p> <ul style="list-style-type: none"> • Install WebSphere Application Server. • Install the WebSphere Update Installer. • Install the WebSphere Application Server fix pack. • Install the WebSphere Application Server 7.0 Web 2.0 and Mobile feature pack. <p>For WebSphere Application Server Version 8.5:</p> <ul style="list-style-type: none"> • Install the IBM Installation Manager. • Install WebSphere Application Server with fix pack 2. 	<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"> • “Installing WebSphere Application Server, Version 7.0” on page 22 • “Installing the WebSphere Update Installer” on page 23 • “Installing WebSphere Application Server, Version 7.0 fix packs” on page 24 • “Installing the IBM WebSphere Application Server Web 2.0 and Mobile feature pack” on page 25 • “Installing the IBM Installation Manager” on page 19 • “Installing WebSphere Application Server, Version 8.5” on page 20 <p>WebSphere Application Server Version 7.0 documentation</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp <p>WebSphere Application Server Version 8.5 documentation</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v8r5/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
4	<p>Prepare the IBM HTTP Server:</p> <p>For IBM HTTP Server Version 7.0:</p> <ul style="list-style-type: none"> • Install IBM HTTP Server. • Install the IBM HTTP Server fix pack by using the WebSphere Application Server Update Installer. <p>For IBM HTTP Server Version 8.5:</p> <ul style="list-style-type: none"> • Install IBM HTTP Server with fix pack 2 by using the IBM Installation Manager. 	<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"> • “Installing the IBM HTTP Server Version 7.0” on page 28 • “Installing the IBM HTTP Server Version 7.0 fix packs” on page 30 • “Installing the IBM HTTP Server Version 8.5” on page 26 <p>IBM HTTP Server Version 7.0 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/tihs/tihs_installihs.html <p>IBM HTTP Server Version 8.5 documentation</p> <ul style="list-style-type: none"> • http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/topic/com.ibm.websphere.ihs.doc/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>
5	<p>Create a stand-alone WebSphere Application Server profile.</p> <p>Important: For WebSphere Application Server, Version 8.5, the profile directory path must not contain any spaces.</p>	<p>“Creating and choosing stand-alone server profiles” on page 43</p>

	Procedure	Reference
6	<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 Java heap size. • Verify the Windows service for WebSphere Application Server. • Optional: Re-create 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 46 • “Verifying the Windows service for WebSphere Application Server” on page 47 • “Re-creating the root CA for WebSphere Application Server 7.0 (stand-alone)” on page 47 <p>WebSphere Application Server Version 7.0 documentation</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp <p>WebSphere Application Server Version 8.5 documentation</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v8r5/index.jsp
7	<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 191</p>
8	<p>Configure the IBM HTTP Server:</p> <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: Re-create the SSL certificate for the 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 (stand-alone)” on page 52 • “Enabling SSL directives on the IBM HTTP Server” on page 55 • “Increasing the SSL certificate key size for the IBM HTTP Server” on page 56 <p>IBM HTTP Server Version 7.0 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>IBM HTTP Server Version 8.5 documentation</p> <ul style="list-style-type: none"> • http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/topic/com.ibm.websphere.ihs.doc/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>
9	<p>Install the IMS Server on WebSphere Application Server.</p>	<p>“Installing the IMS Server with the IMS Server installer” on page 36</p>

	Procedure	Reference
10	Verify the IMS Server deployment on the WebSphere Application Server.	"Verifying the IMS Server deployment on the WebSphere Application Server" on page 39
11	For WebSphere Application Server, Version 7.0 only: Add the JAX-RS shared library.	"Adding the JAX-RS shared library" on page 40
12	For WebSphere Application Server, Version 8.5 only: Configure the IMS Server deployment with the Sun Reference Implementation 1.2 implementation.	"Configuring the JSF implementation" on page 39
13	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 58 • "Configuring the IMS Server to use directory servers" on page 161
14	Provision the IMS Server administrator.	"Provisioning the IMS Server administrator" on page 61
15	Update the ISAMESS0IMS module mapping to forward connection requests.	"Updating the ISAMESS0IMS module mapping for connection request forwarding" on page 62
16	Verify the IMS Server configuration.	"Verifying the IMS Server configuration" on page 63

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

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

	Procedure	Reference
1	<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 Version 9.7 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>IBM DB2 Version 10.1 documentation</p> <ul style="list-style-type: none">• http://pic.dhe.ibm.com/infocenter/db2luw/v10r1/index.jsp <p>Microsoft SQL Server 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 Database 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
2	<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 32 <p>Microsoft Active Directory 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
3	<p>On Host A, prepare the WebSphere Application Server:</p> <p>For WebSphere Application Server Version 7.0:</p> <ul style="list-style-type: none"> • Install WebSphere Application Server. • Install the WebSphere Update Installer. • Install the WebSphere Application Server fix pack. • Install the WebSphere Application Server Web 2.0 and Mobile feature pack. <p>For WebSphere Application Server Version 8.5:</p> <ul style="list-style-type: none"> • Install the IBM Installation Manager. • Install WebSphere Application Server with fix pack 2. <p>On Host B, prepare the WebSphere Application Server:</p> <p>For WebSphere Application Server Version 7.0:</p> <ul style="list-style-type: none"> • Install WebSphere Application Server. • Install the WebSphere Update Installer. • Install the WebSphere Application Server fix pack. • Install the WebSphere Application Server Web 2.0 and Mobile feature pack. <p>For WebSphere Application Server Version 8.5:</p> <ul style="list-style-type: none"> • Install the IBM Installation Manager. • Install WebSphere Application Server with fix pack 2. 	<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"> • “Setting up a cluster (network deployment)” on page 64 • “Installing WebSphere Application Server, Version 7.0” on page 22 • “Installing the WebSphere Update Installer” on page 23 • “Installing WebSphere Application Server, Version 7.0 fix packs” on page 24 • “Installing the IBM WebSphere Application Server Web 2.0 and Mobile feature pack” on page 25 • “Installing the IBM Installation Manager” on page 19 • “Installing WebSphere Application Server, Version 8.5” on page 20 <p>WebSphere Application Server Version 7.0 documentation</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp <p>WebSphere Application Server Version 8.5 documentation</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v8r5/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>
4	Optional: Re-create the 1024 bit root CA if your deployment requires a larger 2048 bit key size.	

	Procedure	Reference
5	<p>Prepare the IBM HTTP Server:</p> <p>For IBM HTTP Server Version 7.0:</p> <ul style="list-style-type: none"> • Install IBM HTTP Server. • Install the IBM HTTP Server fix pack by using the WebSphere Application Server Update Installer. <p>For IBM HTTP Server Version 8.5:</p> <ul style="list-style-type: none"> • Install IBM HTTP Server with fix pack 2 by using the IBM Installation Manager. <p>Important: Ensure that the required subcomponents, such as the Java SDK, Web Server Plug-in, and WebSphere Customization Toolbox, and interim fixes are installed.</p>	<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"> • “Installing the IBM HTTP Server Version 7.0” on page 28 • “Installing the IBM HTTP Server Version 7.0 fix packs” on page 30 • “Installing the IBM HTTP Server Version 8.5” on page 26 <p>IBM HTTP Server Version 7.0 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>IBM HTTP Server Version 8.5 documentation</p> <ul style="list-style-type: none"> • http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/topic/com.ibm.websphere.ihs.doc/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>
6	<p>For the WebSphere Application Server, create the deployment manager and nodes:</p> <p>Important: For WebSphere Application Server, Version 8.5, the profile directory path must not contain any spaces.</p> <ol style="list-style-type: none"> 1. On Host A, create a deployment manager profile and custom profile. <p>Note: Before you federate the custom profile on the deployment manager, ensure that there is a two-way name resolution between the deployment manager and custom nodes.</p> <ol style="list-style-type: none"> 2. On Host B, create a custom profile. 	<ul style="list-style-type: none"> • “Ways of resolving hosts and IP addresses” on page 188 • “Creating and choosing profiles for network deployments” on page 66

	Procedure	Reference
7	<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"> • For WebSphere Application Server 7.0: • “Configuring WebSphere Application Server for a cluster” on page 76 • “Defining a cluster” on page 76 • “Configuring the heap size for the deployment manager” on page 77 • “Configuring the heap size for the application server” on page 46 • “Creating a Windows service for the node agent” on page 78 <p>WebSphere Application Server Version 7.0 documentation</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp <p>WebSphere Application Server Version 8.5 documentation</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v8r5/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>
8	<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 191</p>

	Procedure	Reference
9	<p>Configure the IBM HTTP Server:</p> <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: Re-create the SSL certificate for the 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 (network deployment)” on page 80 • “Enabling SSL directives on the IBM HTTP Server” on page 82 • “Increasing the SSL certificate key size for the IBM HTTP Server” on page 83 <p>IBM HTTP Server Version 7.0 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>IBM HTTP Server Version 8.5 documentation</p> <ul style="list-style-type: none"> • http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/topic/com.ibm.websphere.ihs.doc/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>
10	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.
11	Install the IMS Server on WebSphere Application Server.	“Installing the IMS Server with the IMS Server installer” on page 36
12	Verify the IMS Server deployment on the WebSphere Application Server.	“Verifying the IMS Server deployment on the WebSphere Application Server” on page 39
13	For WebSphere Application Server, Version 7.0 only: Add the JAX-RS shared library.	“Adding the JAX-RS shared library” on page 40
14	For WebSphere Application Server, Version 8.5 only: Configure the IMS Server deployment with the Sun Reference Implementation 1.2 implementation.	“Configuring the JSF implementation” on page 39
15	Configure the IMS Server.	<ul style="list-style-type: none"> • “Configuring the IMS Server with the IMS Configuration Wizard (network deployment)” on page 85 • “Configuring the IMS Server to use directory servers” on page 161
16	Provision the IMS Server administrator.	“Provisioning the IMS Server administrator” on page 88
17	Update the ISAMESS0IMS module mapping to forward connection requests.	“Updating the ISAMESS0IMS module mapping for connection request forwarding” on page 89

	Procedure	Reference
18	Configure session management for ISAMESS0IMS.	"Overriding session management for the ISAMESS0IMS" on page 90
19	Verify the IMS Server configuration.	"Verifying the IMS Server configuration" on page 91
20	Optional: Add additional application servers to a cluster.	
21	Optional: Deploy ISAMESS0IMS on additional nodes in a network deployment.	

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 Chapter 5, "Planning worksheet," on page 145:

- 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 17.

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 18.

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 that is 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.

Follow the instructions in the DB2 documentation:

- Version 9.7 documentation: <http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=/com.ibm.db2.udb.doc/welcome.htm>.
- Version 10.1 documentation: <http://pic.dhe.ibm.com/infocenter/db2luw/v10r1/index.jsp?topic=%2Fcom.ibm.db2.luw.welcome.doc%2Fdoc%2Fwelcome.html>.

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

Record the values that are used in the planning worksheet. See Chapter 5, “Planning worksheet,” on page 145.

Procedure

1. Obtain a DB2 database system installation package from IBM.
2. Install the DB2 database server as described in the DB2 database server documentation.
3. Apply the latest fix packs. To download the latest fix packs, go to www.ibm.com/support/docview.wss?uid=swg27007053.

What to do next

Create a database in DB2.

Creating the database with IBM DB2:

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

Procedure

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

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

where the following parameters are defined:

Default buffer pool and table space page size

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

Code set

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

Territory

Specify **US** as the territory.

For example:

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

Results

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

What to do next

You can install and configure WebSphere Application Server.

- Version 8.5: “Installing WebSphere Application Server, Version 8.5” on page 20.
- Version 7.0: “Installing WebSphere Application Server, Version 7.0” on page 22.

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.

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 database server, see “Creating the database in SQL Server manually” on page 187.

Preparing the WebSphere Application Server

The IMS Server is implemented as a WebSphere Application Server application. You must install and configure the WebSphere Application Server before you install the IMS Server.

The following versions of WebSphere Application Server are supported:

- WebSphere Application Server Version 7.0 with fix pack 29 and later.
- WebSphere Application Server Version 8.5 with fix pack 2.

Note: The installation steps for WebSphere Application Server Versions 7.0 and 8.5 vary. Thus, it is important to identify the version of the application server that you want to install.

Preparing the WebSphere Application Server, Version 8.5

Prepare the WebSphere Application Server Version 8.5 with the latest fix packs for all the required components.

For WebSphere software, Version 8.5, you must install Fix Pack 2 for WebSphere Application Server and the Java SDK.

Installing the IBM Installation Manager:

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

Before you begin

- To avoid problems, download and use the latest version of the Installation Manager found on the support page.
- 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*.
- Review the prerequisites before installing the Installation Manager.

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

About this task

IBM Installation Manager is a single installation program that can use remote or local software flat-file repositories to install, modify, or update new WebSphere Application Server products. It determines and shows available

packages—including products, fix packs, interim fixes, and so on—checks prerequisites and interdependencies, and installs the selected packages.

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

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

For more information on using Installation Manager, read the IBM Installation Manager Version 1.6 Information Center.

Procedure

1. Take one of the following options:
 - Access the IBM WebSphere Application Server Network Deployment, Version 8.5 media for your operating system.
 - Extract the files from the archive file that you downloaded from Passport Advantage®. For example: CI6XDML.zip

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

2. Navigate to the location containing the Installation Manager installation files.
3. Run the administrative installation program for the Installation Manager `install.exe`.
4. Ensure that the Installation Manager package is selected, and click **Next**.
5. Follow the instructions in the installation wizard, and click **Next** until you reach the summary information.
6. Verify the information, and click **Install**. When the installation process is complete, a message confirms the success of the process.
7. Add the product repository for WebSphere Application Server Version 8.5 and the supplements, such as IBM HTTP Server and plug-ins to your Installation Manager preferences.
 - a. From the IBM Installation Manager, click **File > Preferences**.
 - b. Select **Repositories**.
 - c. Click **Add Repository**.
 - d. Specify the location of the WebSphere Application Server repository files, `<somepath>repository.config`. For example: `E:\WAS_ND_V8.5\repository.config`
 - e. Click **OK**.
 - f. Click **Add Repository**.
 - g. Specify the location of the WebSphere Application Server supplements. For example: `E:\WAS_V85_SUPPL\repository.config`
 - h. Click **OK**.

What to do next

Install WebSphere Application Server, Version 8.5

Installing WebSphere Application Server, Version 8.5:

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

Before you begin

- Ensure that you have installed the IBM Installation Manager and that you have configured the product repository. See “Installing the IBM Installation Manager” on page 19.
- Read the WebSphere Application Server documentation.
- Ensure that you have Administrator privileges.
- Ensure that your system meets the requirements. See Hardware and software requirements.
- Ensure that all required operating system fix packs are in place. For more information about tuning operating systems for the WebSphere Application Server, see the WebSphere Application Server documentation and search for tuning operating systems.

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

About this task

Record the values that are used in the planning worksheet. See Chapter 5, “Planning worksheet,” on page 145.

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

Procedure

1. Start the IBM Installation Manager. For example, click **Start > All Programs > IBM Installation Manager > IBM Installation Manager**.
2. Ensure that you have configured the product repository. For more information, see “Installing the IBM Installation Manager” on page 19.
3. Click **Install**. A list of available packages to install are displayed.
4. Select the following package:
 - **IBM WebSphere Application Server Network Deployment**
5. Click **Check for Other Versions, Fixes, and Extensions** to display the WebSphere Application Server Version 8.5.0.2.

Tip: Ensure that the **Show all versions** check box is selected to display all available versions.

6. Select the following package:
 - **IBM WebSphere Application Server Network Deployment**
 - **Version 8.5.0.2**

CAUTION:

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

7. Click **Next**.
8. Select the following fix and click **Next**:
 - For x86 Windows operating systems: 8.5.0.0-WS-WASJavaSDK-WinX32-IFPM91292 8.5.0.20130723_1400
 - For x64 Windows operating systems: 8.5.0.0-WS-WASJavaSDK-WinX64-IFPM91292 8.5.0.20130723_1359

9. Follow the instructions in the Installation Manager, and click **Next** until you reach the summary information.
10. Review the installation summary and verify that the package for **IBM WebSphere Application Server Network Deployment Version 8.5.0.2** is selected. Select the appropriate package according to your operating system.
11. Click **Install**. When the installation process is complete, a message confirms the success of the process.
12. Click **Finish**.

What to do next

Install the IBM HTTP Server Version 8.5.

Preparing the WebSphere Application Server, Version 7.0

Prepare the WebSphere Application Server Version 7.0 with the latest fix packs for all the required components.

For WebSphere software, Version 7.0 you must install at least Fix Pack 29 for WebSphere Application Server and the Java SDK subcomponent.

Installing WebSphere Application Server, Version 7.0:

Install and configure the WebSphere Application Server before the IMS Server installation.

Before you begin

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

For more information about installing the WebSphere Application Server, see the WebSphere Application Server Version 7.0 documentation and search for installing WebSphere Application Server.

About this task

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

Record the values that are used in the planning worksheet. See Chapter 5, “Planning worksheet,” on page 145.

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. Take one of the following actions:
 - Access the IBM WebSphere Application Server Network Deployment, Version 7.0 media for your operating system.
 - Extract the files from the archive file that you downloaded from Passport Advantage. For example: C1G2JML.zip

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

2. Run the WebSphere installation program `launchpad.exe`.
3. Click **Launch the installation wizard for WebSphere Application Server Network Deployment**.
4. Follow the instructions in the installation wizard until you reach the **Installation Directory** page.
5. In the **Installation Directory** page, accept the default installation directory or change the value. 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**.

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.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*.
- Review the prerequisites before installing the Update Installer.

For the detailed instructions, see the WebSphere Application Server documentation and search for installing the Update Installer.

About this task

The IBM 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: 7.0.0.29-WS-UPDI-WinAMD64
2. Browse to the extracted UpdateInstaller directory.
3. Run install.exe to start the Installation Wizard for the Update Installer.
4. Follow the instructions in the installation wizard.
5. Before you finish the installation, clear the **Launch IBM Update Installer for WebSphere software on exit** check box.
6. Click **Finish**.

What to do next

Apply the latest fix packs for WebSphere Application Server.

Installing WebSphere Application Server, Version 7.0 fix packs:

You must apply the latest WebSphere Application Server Version 7.0 fix pack before you run the IMS Server installation program.

Before you begin

- If you already have an installed WebSphere Application Server Version 7.0, ensure that you are using the required level of fix packs.
To determine the minimum fix pack to apply to WebSphere Application Server Version 7.0, see the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.
- If you are reusing an existing WebSphere Application Server Version 7.0 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.

- Download the latest IBM Update Installer from the IBM Support and Downloads website: <http://www.ibm.com/support/docview.wss?uid=swg24020448>.

About this task

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.

Note: For WebSphere Application Server Version 7.0, use fix pack 29 or later.

Procedure

1. Download the latest fix packs.
 - a. Access the WebSphere Application Server support site at <http://www.ibm.com/software/webservers/appserv/was/support/>.
 - b. Click the **Downloads** link.
 - c. Follow the links and instructions on the page to determine the fix packs to download.
 - d. Downloading fix packs for other WebSphere Application Server components. For example:
 - **<architecture> AMD/Intel AppServer**
 - **<architecture> AMD/Intel IBM HTTP Server**
 - **<architecture> AMD/Intel Java SDK**
 - e. Optional: Copy the downloaded fix packs to the <updi_home>\maintenance directory. For example: copy 7.0.0-WS-WAS-WinX64-FP0000029.pak to C:\Program Files\IBM\WebSphere\UpdateInstaller\maintenance.
2. Start the IBM Update Installer. (**Start > All Programs > IBM WebSphere > Update Installer for Websphere V7.0 Software > Update Installer**)
3. In the Product Selection page, select the WebSphere installation directory, and click **Next**. For example: C:\Program Files\IBM\WebSphere\AppServer.
4. Select **Install Maintenance Package** and click **Next**.
5. In the directory path, specify the location of the maintenance or fix pack.
6. Select the WebSphere Application Server fix packs. Select the WebSphere Application Server and SDK components.
7. Click **Next**.
8. After the prerequisites checker completes successfully, click **Next**.

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

You must install the Web 2.0 and Mobile feature pack on the WebSphere Application Server Version 7.0.

Before you begin

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

About this task

This task is relevant to WebSphere Application Server Version 7.0 only.

Procedure

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

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.

The following versions of IBM HTTP Server are supported:

- IBM HTTP Server Version 7.0 fix pack 29 and later.
- IBM HTTP Server Version 8.5 fix pack 2.

For more information about 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*.

Note: The installation steps for IBM HTTP Server Versions 7.0 and 8.5 vary. Thus it is important to identify the version of the web server that you want to install.

Installing the IBM HTTP Server Version 8.5

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

Before you begin

- Ensure that you have installed the IBM Installation Manager and that you have configured the product repository. See “Installing the IBM Installation Manager” on page 19.
- Ensure that you have the supplemental images in the repository.
- 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 you have Administrator privileges.
- Ensure that there is no service listening to port 80, 443 and 8008.
- This guide provides instructions about preparing the IBM HTTP Server. For detailed and up-to-date installation instructions, see the IBM HTTP Server documentation. In the WebSphere Application Server version 8.5 product documentation, search for Installing IBM HTTP Server using the GUI.
- IBM HTTP Server and web server plug-ins, Version 8.5, require the Microsoft Visual C++ 2008 Redistributable Package. For installations on x86 computers, install the x86 version of the Microsoft Visual C++ 2008 Redistributable Package. For installation on x64 computers, install both the x86 and x64 version of the Microsoft Visual C++ 2008 Redistributable Package. Go to the Microsoft website and search for Microsoft Visual C++ 2008 Redistributable x64 x86.

About this task

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

Record any values that you use in the planning worksheet. See Chapter 5, “Planning worksheet,” on page 145.

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 Chapter 5, “Planning worksheet,” on page 145.

Procedure

1. Start the IBM Installation Manager. For example, click **Start > All Programs > IBM Installation Manager > IBM Installation Manager**.
2. Ensure that you have configured the product repository. For more information, see “Installing the IBM Installation Manager” on page 19.
3. Click **Install**. A list of available packages to install are displayed.
4. Select the following packages:
 - **IBM HTTP Server for WebSphere Application Server**
 - **Web Server Plug-ins for IBM WebSphere Application Server**
 - **WebSphere Customization Toolbox**

CAUTION:

Selecting a package other than the ones that are listed earlier can produce undesirable results.

5. Click **Check for Other Versions, Fixes, and Extensions**.

Tip: Ensure that the **Show all versions** check box is selected to display all available versions.

6. Select the following packages:
 - **IBM HTTP Server for WebSphere Application Server**
 - **Version 8.5.0.2**
 - **Web Server Plug-ins for IBM WebSphere Application Server**
 - **Version 8.5.0.2**
 - **WebSphere Customization Toolbox**
 - **Version 8.5.0.2**

CAUTION:

Selecting a package other than the ones that are listed earlier can produce undesirable results.

7. Click **Next**.
8. Under **WebSphere Customization Toolbox 8.5.0.2**, ensure that **Web Server Plug-ins Configuration Tool** is selected.
9. Follow the instructions in the Installation Manager and in the following steps.
10. In the **Web Server Configuration** panel, complete the following steps and click **Next**:
 - a. Verify that the **HTTP Port** is 80.
 - b. Verify that **Run IBM HTTP Server as a Windows Service** is selected.

- c. Select **Log on as a local system account**.
- d. In the **Startup type** list, select **Automatic**.
- 11. Review the installation summary.
- 12. Click **Install** to start the installation. When the installation process is complete, a message confirms the success of the process.
- 13. Click **Finish**.

What to do next

- 1. Start the IBM HTTP Server service.
 - Click **Start > All Programs > IBM HTTP Server <version> > Start HTTP Server**.
- 2. Verify that you can access the web server from a web browser. For example:
 - To access the web server on the local computer, type `http://localhost` or `http://mywebsvr1`.
Where
`mywebsvr1` is your computer name.
 - To access the web server remotely, when a name server is available to resolve host names, type `http://<fully_qualified_host_name>`. For example:
`http://mywebsvr1.example.com`.

Installing the IBM HTTP Server Version 7.0

IBM HTTP Server Version 7.0 must be installed on the server where the IBM HTTP Server plug-in component is installed.

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

About this task

Use the IBM HTTP Server Version 7.0 installation media that is provided with IBM Security Access Manager for Enterprise Single Sign-On to ensure that you are using the correct version.

Record any values that you use in the planning worksheet. See Chapter 5, “Planning worksheet,” on page 145.

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 Chapter 5, “Planning worksheet,” on page 145.

Procedure

1. Take one of the following actions:
 - Access the WebSphere Application Server media for your operating system.
 - Extract the files from the supplementary archive file that you downloaded from Passport Advantage. For example: C1G2KML.zip

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

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

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

HTTP Port

80

HTTP Administration Port

8008

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

Note: If your multiserver deployment plan requires you to set up another web server, you must specify a unique web server definition name for each web server. For example: webserver2.

- c. For **Host name or IP address for the Application Server**, specify the name of the application server. For example: appsvr1.example.com.
 - d. Click **Next**.
8. Review the installation summary.
 9. Click **Next** to start the IBM HTTP Server installation.
 10. Click **Finish**.
 11. Start the IBM HTTP Server and Admin Server service.

- a. Click **Start > All Programs > IBM HTTP Server V7.0 > Start Admin Server**.
 - b. Click **Start > All Programs > IBM HTTP Server V7.0 > Start HTTP Server**.
12. Verify that you can access the web server from a web browser. For example:
- To access the web server on the local computer, type `http://localhost` or `http://mywebsvr1`.
Where
`mywebsvr1` is your computer name.
 - To access the web server remotely, when a name server is available to resolve host names, type `http://<fully_qualified_host_name>`. For example: `http://mywebsvr1.example.com`.

What to do next

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

Installing the IBM HTTP Server Version 7.0 fix packs

Apply the latest fix packs for the IBM HTTP Server.

Before you begin

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

About this task

If you have more than one IBM HTTP Server Version 7.0 in your deployment, install the fix pack on each web server.

Procedure

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

- g. Select the target update and click **Next**.
- h. On the **Installation Summary** screen, click **Next**.
- 5. Start the IBM HTTP Server. Click **Start > All Programs > IBM HTTP Server V7.0 > Start HTTP Server**.
- 6. Start the Admin Server. Click **Start > All Programs > IBM HTTP Server V7.0 > Start Admin Server**.

What to do next

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

Installing the IBM HTTP Server Version 7.0 plug-in fix pack

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

Before you begin

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

Procedure

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

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 IBM Security Access Manager for Enterprise Single Sign-On can communicate with it. 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 that are 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 following documentation:

- WebSphere Application Server Version 7.0 documentation: <http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp>.
- WebSphere Application Server Version 8.5 documentation: <http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/index.jsp>.

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 that you need in the Planning worksheet. See Chapter 5, "Planning worksheet," on page 145.

- IBM Security Access Manager for Enterprise Single Sign-On works with LDAP 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.

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. Enable SSL in the Active Directory so that clients can 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 IBM Security 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 IBM Security 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 IBM Security Identity Manager Active Directory Adapter, consult the IBM Security Identity Manager adapter documentation.

Use the IBM Security 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 requires SSL to be enabled for password reset in AccessAssistant and Web Workplace.

If there is no SSL connection, an instance of IBM Security Identity Manager Active Directory Adapter is required. See “Preparing the Active Directory Adapter” on page 34.

2. 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 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 that are 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.isamessoIm.s.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.isamessoIm.sConfig.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 ESS0\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 180.
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:\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:\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:\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:\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” on page 39.

If there are any IMS Server installation errors, resolve them before you configure the IMS Server. Check the <ims_home>/ISAM_ESS0_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. The ISAMESSOIMSConfig starts up with the deployment manager and the ISAMESSOIMS starts with the cluster.

What to do next

After you verify that the IMS Server WebSphere applications are deployed, configure the ISAMESSOIMSConfig application to use the JavaServer Faces implementation.

- “Configuring the JSF implementation”
- “Configuring the IMS Server for a new installation with the IMS Configuration Wizard (stand-alone)” on page 58
- “Configuring the IMS Server with the IMS Configuration Wizard (network deployment)” on page 85

Configuring the JSF implementation

Before you configure the IMS Server on the WebSphere Application Server Version 8.5, you must configure the IMS Server deployment to use the Sun Reference Implementation 1.2.

Before you begin

Install the IMS Server.

About this task

Use the following steps in the WebSphere Application Server Administrative Console to configure the JSF implementation of the ISAMESSOIMSConfig and ISAMESSOIMS applications.

Procedure

1. In the administrative console, click **Applications > Application Types > WebSphere Enterprise Applications**.
2. Repeat the following steps for ISAMESSOIMSConfig and ISAMESSOIMS.
 - a. Select the application.
 - b. Under **Web Module Properties**, click **JSP and JSF Options**.
 - c. For **JSF Implementation**, select **SunRI1.2**.
 - d. Save the changes to the master configuration.
 - e. Restart the WebSphere Application Server profile.

For clustered deployments, synchronize and restart the cluster.

What to do next

After you select the JSF implementation for the ISAMESSOIMSConfig and ISAMESSOIMS applications, configure the IMS Server with the IMS Configuration Wizard.

Adding the JAX-RS shared library

Define a container-wide shared library in WebSphere Application Server that can be used by the deployed ISAMESSOIMS application.

Before you begin

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

About this task

Perform this task on the WebSphere Application Server.

Note: This task is relevant to WebSphere Application Server Version 7.0 only.

For clustered deployments, perform this task on the deployment manager.

Procedure

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

```
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/commons-codec.jar  
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/commons-lang.jar  
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/httpclient.jar  
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/httpcore.jar  
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/ibm-wink-jaxrs.jar  
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/jcl-over-slf4j.jar
```

```

${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/jsr311-api.jar
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/slf4j-api.jar
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/slf4j-jdk14.jar
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/jackson/jackson-core-asl.jar
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/jackson/jackson-jaxrs.jar
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/jackson/jackson-mapper-asl.jar
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/jackson/jackson-xc.jar
${was_install_root}/web2mobilefep_1.1/optionalLibraries/jaxrs_1.X/webdav/wink-jaxrs-webdav.jar

```

where

`${was_install_root}` is a WebSphere environment variable to the location of the WebSphere Application Server directory. For example: C:\Program Files\IBM\WebSphere\AppServer.

7. Click **OK**.
8. Click **Save**.
9. Map the **ISAMESSOIMS** application to the shared library.
 - a. In the navigation pane, click **Applications > Application Types > WebSphere enterprise applications**.
 - b. In the **Enterprise Applications** page, click **ISAMESSOIMS**.
 - c. In the **Configuration** page, under **References**, click **Shared library references**.
 - d. Select **ISAMESSOIMS**.
 - e. Click **Reference shared libraries**.
 - f. In the **Available** list, select the **jaxrslib** library.
 - g. Move the **jaxrslib** library to the **Selected** list by clicking **>>**.
 - h. Click **OK** twice.
10. Save the changes to WebSphere Application Server.
11. For clustered deployments, synchronize all the nodes.
12. Restart the **ISAMESSOIMS** application.
 - a. In the navigation pane, browse to **Applications > Application Types > WebSphere Enterprise Applications**.
 - b. Select **ISAMESSOIMS**.
 - c. Click **Stop**.
 - d. Click **Start**.

The **ISAMESSOIMS** application is restarted.

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.

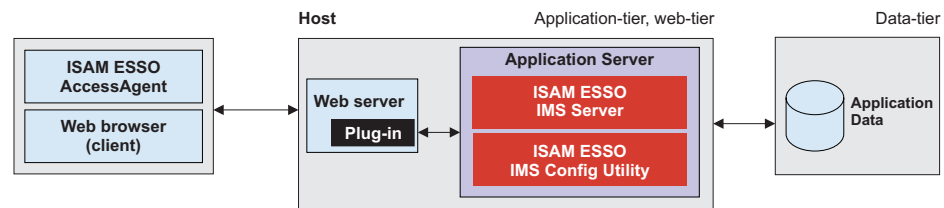


Figure 1. Stand-alone production server installation

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*.

Roadmap

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 the WebSphere Application Server.
3. Prepare the IBM HTTP Server.
4. Prepare the directory server.
5. Optional: Install IBM Tivoli Common Reporting or the IBM Cognos® Business Intelligence reporting components.

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.

IBM Tivoli Common Reporting or IBM Cognos Business Intelligence reporting components

Install IBM Tivoli Common Reporting or IBM Cognos Business Intelligence reporting components if you want to create IBM Security Access Manager for Enterprise Single Sign-On reports. See the *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide*.

Note: IBM Tivoli Common Reporting is currently supported, but is being deprecated. As a best practice, use the IBM Cognos reporting framework for the report generation.

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 stand-alone server profiles

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.

Important: For WebSphere Application Server Version 8.5, the profile directory path must not contain any spaces.

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 the following method:

- “Creating stand-alone profiles (Profile Management tool)”

Creating stand-alone profiles (Profile Management tool)

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

Before you begin

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

About this task

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

Procedure

1. Open the Profile Management Tool. For example:

WebSphere Application Server Version 7.0

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

WebSphere Application Server Version 8.5

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

2. On the **Welcome to the Profile Management Tool** panel, review the information.
3. Click **Launch Profile Management Tool**.
4. On the **Profiles** panel, click **Create** to create a profile.
5. On the **Environment Selection** panel, click **Application server**.
6. Click **Next**.
7. On the **Profile Creation Options** panel, choose the profile creation process.

For WebSphere Application Server Version 7.0:

- a. Click **Typical profile creation**.
- b. Click **Next**.
- c. 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.

- d. Click **Next**.

For WebSphere Application Server Version 8.5:

- a. Click **Advanced profile creation** and click **Next**.
- b. Clear the **Deploy the default application** check box and click **Next**.
- c. On the **Profile name and location** panel, specify a name for the profile and the directory path for the profile directory.

Important: The profile directory path must not contain any spaces.

For example:

- An invalid path: c:\Program Files\IBM\WebSphere\AppServer\AppSrv01
 - A valid path: c:\was\profiles\AppSrv01
- d. 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.

e. Click **Next**.

8. For the succeeding panels, keep the default values and click **Next** until you reach the **Profile Creation Summary** panel.

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.

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

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

For WebSphere Application Server Version 7.0:

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

For WebSphere Application Server Version 8.5:

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

12. 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**.
- For WebSphere Application Server Version 7.0, click **Start > All Programs > IBM WebSphere > Application Server <version> > Profiles > <profile_name> > Administrative console**.
- For WebSphere Application Server Version 8.5, click **Start > All Programs > IBM WebSphere > IBM WebSphere Application Server > Profiles > <profile_name> > Administrative console**.
- In a web browser, go to `https://<was_hostname>:<admin_ssl_port>/ibm/console`. For example: `https://localhost:9043/ibm/console`.

Configuring the WebSphere Application Server

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

1. Secure the WebSphere Application Server deployment.
 - Optional: (For WebSphere Application Server, Version 7.0 only) Re-create 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.
2. Configure the JVM heap size memory.
3. Verify the Windows services for WebSphere Application Server.

Configuring the heap size for the application server

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

Before you begin

Before you modify the Java heap size, ensure that the host has enough physical memory to support a JVM of 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, search for *Java virtual machine settings heap tuning* in the following documentation:

- WebSphere Application Server Version 7.0 documentation: <http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp>
- WebSphere Application Server Version 8.5 documentation: <http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/index.jsp>

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 is displayed in the list of services: IBM WebSphere Application Server <version> - <node_name>
For example:
 - IBM WebSphere Application Server v7.0 - *ibm-svr1Node01*
 - IBM WebSphere Application Server v8.5 - *ibm-svr1Node01*

Results

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

Re-creating 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 keystore. The certificates secure internal WebSphere Application Server communications.

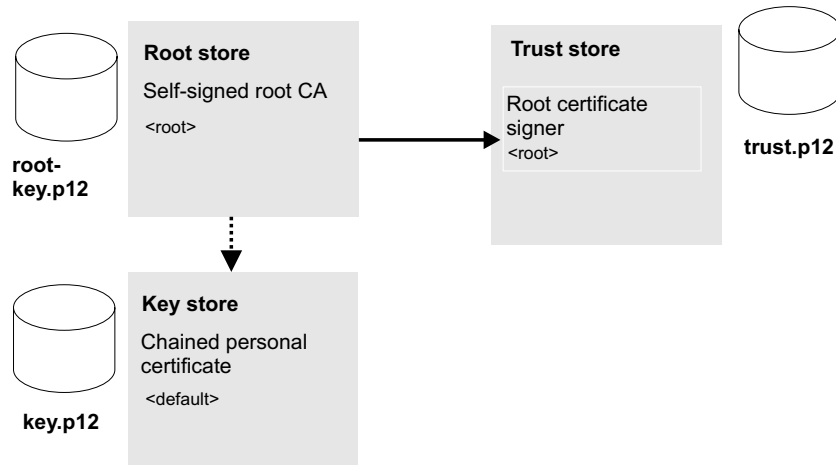


Figure 2. Replacing the root CA and key signers for WebSphere Application Server in the truststore with a new key size.

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 to step 8 on page 49.
2. Create a 2048 bit chained personal certificate in the keystore, and replace the existing version. See step 10 on page 50.
3. Export the personal certificate to the truststore. See step 11 on page 50.
4. Use the **ikeyman** utility to add the root CA to the truststore. See step 12 on page 51.

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

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

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

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

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

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

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

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

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

- a. In the **Personal Certificates** page, select the personal certificate check box. For example: default2.
- b. Click **Export**.
- c. In **Key store password**, enter the key store password For example: WebAS.

Note: The default key store password is documented in the WebSphere Application Server product documentation.

- 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 Chapter 5, “Planning worksheet,” on page 145

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

Deploy the IBM HTTP Server plug-in and configure connection requests to forward connections over Secure 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. To check whether a port is already in use, use a utility like **netstat**. For example: **netstat -na -p tcp -o**.
- If there are other applications listening to port 80, shut down the applications before you install the IBM HTTP Server.
- Ensure that the following software is started:
 - IBM HTTP Server
 - IBM HTTP Server Administration Server
 - WebSphere Application Server
- Review the planning worksheet for the configuration settings. See Chapter 5, “Planning worksheet,” on page 145.

About this task

Configuring IBM HTTP Server is a three-stage process.

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

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

Procedure

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

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

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

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 re-create 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\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 55 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.

Increasing the SSL certificate key size for the IBM HTTP Server

You can re-create 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 “Re-creating the root CA for WebSphere Application Server 7.0 (stand-alone)” on page 47
- For WebSphere Application Server in a cluster, see “Re-creating the root CA for WebSphere Application Server 7.0 on the deployment manager before creating member nodes” on page 71

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, complete 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: `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**.

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 ISAMESS0IMS 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

- If you are using the WebSphere Application Server Version 8.5, configure the JavaServer Faces implementation.
- Ensure that the WebSphere Application Server is started.
- Ensure that the IMS Server applications have the following status:
 - ISAMESS0IMSConfig is started.
 - ISAMESS0IMS is stopped.
- Prepare the directory server.
- Prepare the database server.
- Review the planning worksheet for sample values. See Chapter 5, “Planning worksheet,” on page 145.

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.

Note: For WebSphere Application Server Version 7.0, use fix pack 29 or later. For WebSphere Application Server Version 8.5, use fix pack 2.

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 Chapter 6, "Creating database schemas," on page 157.

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 that 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: imsdbs.

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 re-created 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 Chapter 5, “Planning worksheet,” on page 145.

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 is already 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 that is 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. (Network deployment) Restart the deployment manager node. (Stand-alone deployment) Restart the application server.

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. See "Configuring the IMS Server to use directory servers" in the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

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:

- ISAMESS0IMS
- IBM HTTP Server
- Cluster

About this task

You must map the ISAMESS0IMS application to the web-tier and application-tier hosts after installing the IMS Server with the IMS Server installer. You must update the ISAMESS0IMS 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 ISAMESS0IMS.
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, cluster or application server in your deployment.

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

6. Click **Apply**.
7. Click **OK**.
8. In the **Messages** box, click **Save**.
9. Do a full synchronization of the nodes. See “Resynchronizing the nodes” on page 184.

Results

The IMS Server application URLs connection requests are now forwarded correctly by the IBM HTTP Server to the ISAMESS0IMS 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:

- ISAMESS0IMS
- ISAMESS0IMSConfig
- 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 that you provisioned. For example: `imsadmin`.
 - c. Click **Setup assistant**.
 - d. You can review the instructions to configure authentication factors later. 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 complete 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.

Setting up a cluster (network deployment)

With cluster, you can 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.

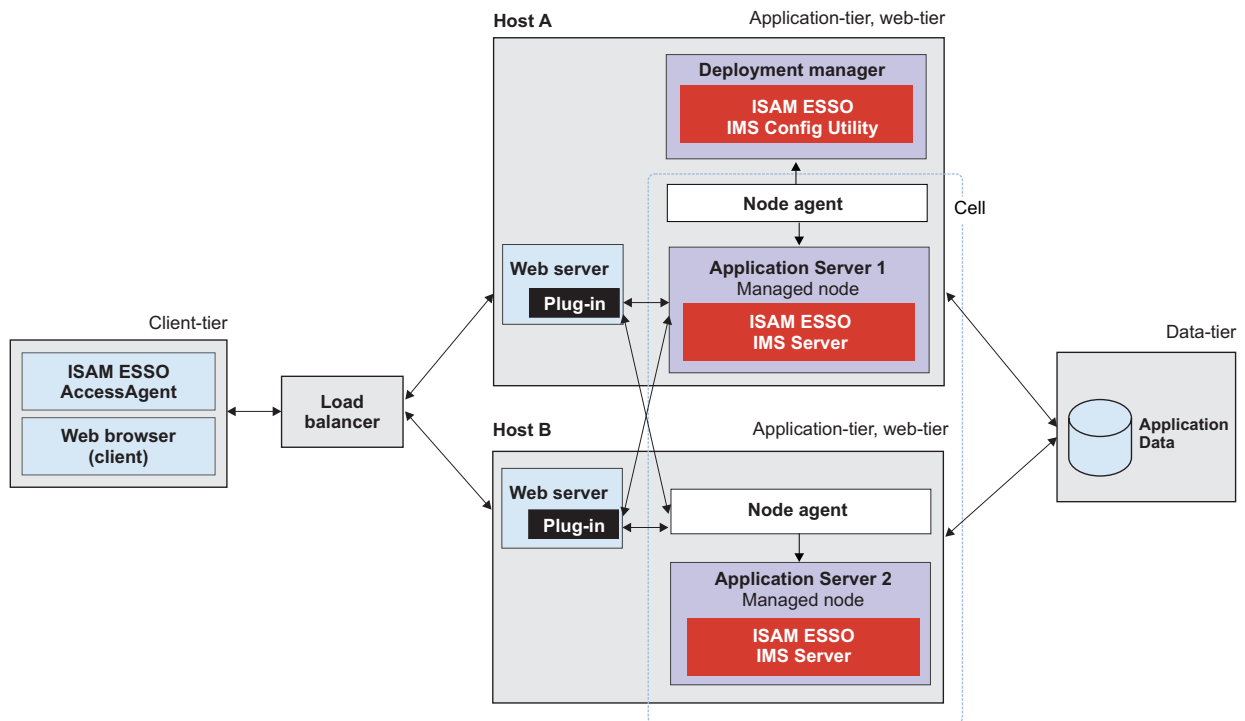


Figure 3. IBM Security Access Manager for Enterprise Single Sign-On in a two-node network deployment cluster example for high availability.

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*.

Roadmap

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 the WebSphere Application Server.
4. Prepare the IBM HTTP Server.
5. Optional: Install IBM Tivoli Common Reporting or the IBM Cognos Business Intelligence reporting components.

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.

IBM Tivoli Common Reporting or IBM Cognos Business Intelligence reporting components

Install IBM Tivoli Common Reporting or IBM Cognos Business Intelligence reporting components if you want to create IBM Security Access Manager for Enterprise Single Sign-On reports. See the *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide*.

Note: IBM Tivoli Common Reporting is currently supported, but is being deprecated. As a best practice, use the IBM Cognos reporting framework for the report generation.

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, you can use the graphical Profile Management Tool.

For WebSphere Application Server, Version 8.5, the profile directory path must not contain spaces in the folder names. This requirement is valid for deployment manager, application servers, and custom node profiles.

For a network deployment environment, complete the following steps:

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

Note: Only if your deployment plan requires security certificates with a larger key size, be sure to re-create 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.

WebSphere Application Server Profiles	When to use
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 whether a port is already in use. Changing the default ports is typically done by an experienced WebSphere Application Server administrator.

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

Deployment manager profiles

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

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

Important:

- 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)

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

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 file.

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 the following WebSphere Application Server documentation:

- Version 7.0 documentation: <http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp>
- Version 8.5 documentation: <http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/index.jsp>

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 you create 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.

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 that are created by the profile management tool.

For example, on a host that is 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 complete 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 188.

Procedure

1. Open the Profile Management Tool. For example:

WebSphere Application Server Version 7.0

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

WebSphere Application Server Version 8.5

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

2. 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 **Advanced profile creation**.
 - h. Click **Next**.
 - i. On the **Profile name and location** page, specify a name for the profile and the directory path for the profile directory.

Important: For WebSphere Application Server Version 8.5, the profile directory path must not contain any spaces.

- j. Click **Next**.
- k. In the **Administrative Security** page, ensure that the **Enable administrative security** check box is selected.
- l. 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.

- m. Click **Next**.
- n. Review the settings in the **Profile Creation Summary** page. Alternatively, you can record the values in the Chapter 5, "Planning worksheet," on page 145. For example:
 - Location (C:\WAS\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)
- o. Click **Create**. The deployment manager profile creation process starts.
- p. Ensure the **Launch the First Steps console** check box is selected.
- q. Click **Finish**. The WebSphere Application Server - First Steps window is displayed.
- r. 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.

- s. Verify that you can access the administrative console. For example: browse to `https://localhost:9043/ibm/console`.
- t. Close the output window and browser.
- 3. Optional: (For deployments with 2048 bits root CA certificate requirements only) Re-create the root CA on the deployment manager node. See “Re-creating the root CA for WebSphere Application Server 7.0 on the deployment manager before creating member nodes” on page 71.

Note: If you must increase the root CA key size to 2048 bits for a higher security deployment, re-create 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 **Advanced profile creation**.
 - f. Click **Next**.
 - g. On the **Profile name and location** page, specify a name for the profile and the directory path for the profile directory.

Important: For WebSphere Application Server Version 8.5, the profile directory path must not contain any spaces.

- h. 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.

- i. Click **Next**.
- j. Review the profile creation summary. Alternatively, record the values in the Planning Worksheet.
 - Profile name (default: Custom01)
 - Location (C:\WAS\profiles\Custom01)
- k. Click **Create** to start the profile creation.
- l. Clear the **Launch the First steps console** check box.
- m. 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.

Re-creating 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.

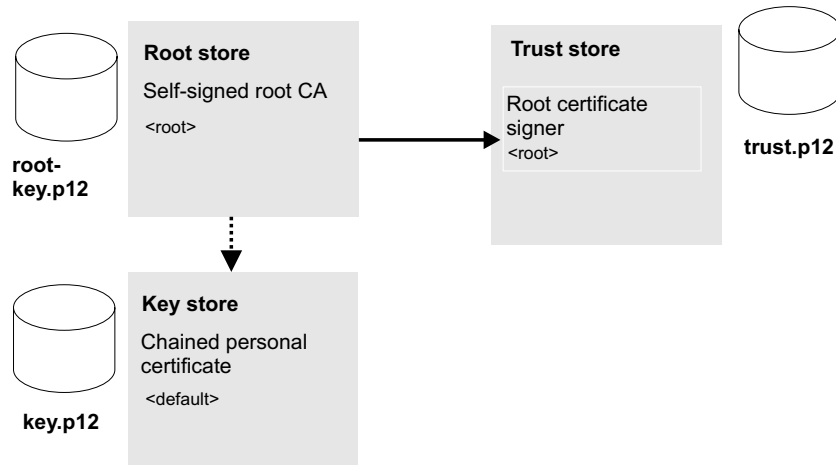


Figure 4. Replacing the root CA and key signers for WebSphere Application Server in the truststore with a new key size.

The process involves the following steps:

1. 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 73.
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 74 to step 11 on page 75.
3. Use the **ikeyman** utility to add the extracted root CA to the truststore. See step 12 on page 75.

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 product documentation on replacing a certificate for details:

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

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

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

- c. From the **Key size** list, select **2048**.
 - d. In the **Common name** field, enter the fully qualified domain name of the computer where the WebSphere Application Server is installed. For example: ibm-svr1.example.com.
 - e. In the **Validity period** field, enter the validity period of the certificate. For example: A root certificate is typically used for 7300 days, which is approximately 20 years.
 - f. Optional: Complete the certificate with optional identification details.
 - g. Click **OK**.
 - h. Click **Save**.
8. Replace the temporary root certificate with the new 2048 bit root that you retain.
 - a. In the **Personal Certificates** page, select the check box for the temporary root certificate: root2.
 - b. Click **Replace**.
 - c. From the **Replace with** list, choose the new 2048 root certificate you created: root.
 - d. Select **Delete old certificate after replacement**.
 - e. Ensure that the **Delete old signer** check box is not selected.

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

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

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

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

- c. In **Certificate file name**, enter the fully qualified path to the certificate to be extracted. For example: C:\root2048.cer
 - d. Verify **Data type** is **Base64-encoded ASCII data**
 - e. Click **OK**.
10. Create a chained personal certificate in the default cell keystore: **CellDefaultKeystore**.
- a. In the **Key stores and certificates** page, click **CellDefaultKeyStore**.
 - b. In **Additional Properties**, click **Personal certificates**.
 - c. Click the **default** certificate. The distinguished name for the default certificate in the **CellDefaultKeystore** must be in the following form:
CN=<CN>,OU=<OU>,O=<Organization>,C=<Country> For example:
CN=ibmsvr1.example.com, OU=Root Certificate, OU=ibmsvr1Cell01,
OU=ibmsvr1CellManager01, O=IBM, C=US .
 - d. Click **Back**.
 - e. Click **Create > Chained certificate**.
 - f. In the **Alias** field, enter a new personal certificate alias. For example: default2.
 - g. In the **Root certificate used to sign the certificate** field, select the alias **root**. This root certificate is the new 2048 bit root certificate.
 - h. In the **Key size** field, select **2048**.
 - i. In the **Common name** field, enter the fully qualified domain name of the computer where the WebSphere Application Server is installed.
 - j. In the **Validity period** field, enter the validity period of the certificate. For example: a typical default value for a personal certificate is 365 days.
 - k. Required: In the **Organization** field, specify the organization portion of the distinguished name.
- Important:** You must 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:** You must 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 product documentation.

- 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 66.

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 and click **Next**.
 - e. In the **Member name** field, type a name for the first member of the cluster. For example, `server1`.

- f. In **Select Node**, choose the node that you want to add to the cluster.
- g. Verify **Create the member using an application server template** is set to **default** and click **Next**. You added a member of the node to the cluster.
- h. Do one of the following steps:
 - If you have no other cluster members to add, click **Next**.
 - If you have additional cluster members to add:
 - 1) Type the `<server_member_name>`. For example, `server01`.
 - 2) Select the correct node.
 - 3) Click **Add member**.
 - 4) Specify additional cluster members before you click **Next**.
- i. Click **Finish**. You created a cluster and added members to the clusters.
- j. In the **Messages** box, click **Save**. The cluster status indicates that the cluster is not started.

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 that is 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, search for *Java virtual machine settings heap tuning* in the following documentation:

- WebSphere Application Server Version 7.0 documentation: <http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp>
- WebSphere Application Server Version 8.5 documentation: <http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/index.jsp>

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 (network deployment)

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

Before you begin

- Ensure that the following software is started:
 - IBM HTTP Server
 - IBM HTTP Server Administration Server
 - Deployment manager
 - Node agent on the managed node
- Review the planning worksheet for the configuration settings. See Chapter 5, “Planning worksheet,” on page 145.

About this task

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

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

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

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

Procedure

1. Run the web server plug-in configuration script.
 - a. On the IBM HTTP Server host, from `<ihs_home>\Plugins\bin`, copy the `configure<web_server_definition_name>.bat` file. For example: `configurewebserver1.bat`
 - b. On the deployment manager, paste the `configure<web_server_definition_name>.bat` file to the `<was_home>\bin` folder. For example: `C:\Program Files\IBM\WebSphere\AppServer\bin`
 - c. Open the command prompt.
 - d. Browse to `<was_home>\bin`.
 - e. Run the following command (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 p0ssw0rd`
 - f. Close the command prompt after the command completes with the following line:

Configuration save is complete.

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

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 re-create 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: *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**.
4. Required: If you have multiple web servers, repeat steps 1 on page 80 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 that are 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 82 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.

Increasing the SSL certificate key size for the IBM HTTP Server

You can re-create 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 “Re-creating the root CA for WebSphere Application Server 7.0 (stand-alone)” on page 47

- For WebSphere Application Server in a cluster, see “Re-creating the root CA for WebSphere Application Server 7.0 on the deployment manager before creating member nodes” on page 71

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, complete 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: *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**.
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. Configure session management.
7. 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 Chapter 6, “Creating database schemas,” on page 157.

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 that 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 re-created 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 Chapter 5, “Planning worksheet,” on page 145.

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 is already 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 that is 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 ISAMESS0IMSConfig. (Network deployment) Restart the deployment manager node. (Stand-alone deployment) Restart the application server.

Results

You 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 ISAMESS0IMSConfig 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, cluster or application server in your deployment.

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

6. Click **Apply**.
7. Click **OK**.
8. In the **Messages** box, click **Save**.
9. Do a full synchronization of the nodes. See “Resynchronizing the nodes” on page 184.

Results

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

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 whether 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 that you provisioned. For example: `imsadmin`.
 - c. Click **Setup assistant**.
 - d. You can review the instructions to configure authentication factors later. 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 complete 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 ISAMESOIMS application on the node.

In a network deployment	Deploy
On the deployment manager node.	<ul style="list-style-type: none"> • ISAMESSOIMS • ISAMESSOIMSConfig
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.

Chapter 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.

AccessAgent and AccessStudio installation roadmap

The AccessAgent and AccessStudio installation roadmap lists the high-level tasks that 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 AccessAgent and AccessStudio. See the corresponding reference link for the detailed procedures.

	Procedure	Reference
1	Optional: To enforce two-factor authentication, you must install the required third-party drivers and SDK.	For detailed and up-to-date installation instructions, see the appropriate product documentation.
2	Install AccessAgent on all employee client workstations and Citrix/Terminal Server that require single sign-on services. For enterprise deployments, you can deploy AccessAgent on Windows workstations through a software deployment solution. For example: Tivoli Endpoint Manager, Active Directory Group Policy Object (AD GPO), or Tivoli Provisioning Manager.	"Installing the AccessAgent" on page 102
3	This task is for Administrators only. Install the Microsoft .NET Framework Version 2.0 Redistributable package before you install AccessStudio.	Go to the Microsoft website at www.microsoft.com and search for ".NET Framework 2.0 download".
4	This task is for Administrators only. To manage single sign-on profiles, install AccessStudio on an Administrator workstation. To prepare your applications for single sign-on, use AccessStudio to create and upload AccessProfiles for supported authentication services and applications.	"Installing the AccessStudio" on page 110
5	Verify the files and registry entries to ensure that the installation is successful.	"Verifying files and registry entries" on page 107

Preparing an installation package to install on multiple PCs

Before you distribute the packages on multiple workstations, you can customize and pre-configure specific deployment attributes for each client.

You can customize the installers to do a remote deployment of AccessAgent and AccessStudio on multiple computers.

You can customize the deployment package attributes by:

- “Preparing and installing a prepackaged Wallet.”
- “Setting the IMS Server location manually (response file)” on page 106.

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 98.
- “Ways of setting the IMS Server location” on page 106.

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), Tivoli Endpoint Manager, and application provisioning software like Tivoli Provisioning Manager.

To distribute the client software on multiple workstations with:

- Tivoli Endpoint Manager: See the *IBM Security Access Manager for Enterprise Single Sign-On Tivoli Endpoint Manager Integration Guide*.
- Active Directory Group Policy Object: See the Microsoft website at <http://www.microsoft.com> and search for Group Policy install software remotely.
- Application provisioning software: See your vendor provided documentation.

Silent installation configuration

You can customize the default behavior of the AccessAgent installation by specifying parameters in the SetupHlp.ini file.

Administrators can use the SetupHlp.ini file to 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 98.

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.

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.

Note: Ensure that there is no previous version of AccessAgent installed.

- b. Ensure that the AccessAgent connects to the production IMS Server.

The AccessAgent client downloads the system data from the IMS Server. The System Wallet is created.

2. Copy the generated Wallet file to the AccessAgent installer.

On the staging workstation, copy the Wallet files from:	To the AccessAgent 8.2.1 installer:
<code><AccessAgent install path>\Cryptoboxes\Wallets</code> For example: <code>C:\Program Files\IBM\ISAM ESS0\Cryptoboxes\Wallets</code>	<code><AccessAgent installer location>\<aa version number>\<aa package guid>\Config\Cryptoboxes\Wallets</code> You must create the Cryptoboxes\Wallets folders manually. For example: For 32-bit <code>c:\<AccessAgent installer location>\aa-<version number>\{9713108D-08D5-474E-92A3-09CD7B63DB34}\Config\Cryptoboxes\Wallets</code> For 64-bit <code>c:\<AccessAgent installer location>\aa-<version number>_x64\{E72C4028-45BB-4EE6-8563-3066EEB39A84}\Config\Cryptoboxes\Wallets</code>

3. Install the new AccessAgent installation program on all other client computers.

Note: If the target computer has earlier versions of AccessAgent, the prepackaged Wallet is not applied. The Wallet from the earlier installation is copied to the new installation.

Important: If you are installing a pre-packaged Wallet on a computer that was previously registered on the IMS Server, re-apply the Machine Policy Template after installation. Alternatively, delete the machine entry from AccessAdmin.

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 ESS0\AA	Specify installation directories.
FirstSyncMaxRetries	Default: 1	Specify the number of attempts if the first synchronization fails during installation.
FirstSyncRetryIntervalMins	Default: 1	Time interval, which is specified in minutes, between each attempt during installation.

Option Name	Value	Description
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>Specify 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)	Specify whether to trigger a computer restart after setup.
RebootConfirmationEnabled	1 0 (default: 1)	Specify 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)	Specify whether to prompt user to insert USB Key, if a USB Key is not already inserted during installation time.
ImsConfigurationEnabled	1 0 (default: 1)	Specify whether to configure the default IMS Server settings and install certificates from the IMS Server during setup.
ImsConfigurationPromptEnabled	1 0 (default: 0)	Specify 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)	Specify whether to suppress all prompts and write to a log. Required for AD GPO installation.
EncentuateNetworkProviderEnabled	1 0 (default: 0)	Specify whether to enable Encentuate Network Provider during an AccessAgent installation.
EncentuateCredentialProviderEnabled	1 0 (default: 1)	Specify whether to install the IBM Security Access Manager for Enterprise Single Sign-On Credential Provider for Windows 7.

Option Name	Value	Description
ConsoleAppSupportEnabled	1 0 (default: 0)	Specify 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> in the <i><AccessAgent installation directory></i> after installation.
ResetBioAPIPermissions	1 0 (default: 0)	Specify whether to reset BioAPI Permissions.
DisableWin7CAD	1 0 (default: 1)	If set to 0, there are no changes to the DisableCAD policy. If set to 1, the DisableCAD policy is set to 1. When the DisableCAD policy is set to 1, the secure prompt screen (Ctrl-Alt-Del) is not displayed.
RemoveWallet	1 0 (default: Not defined)	Specify whether to remove Wallet during uninstallation. For uninstalling silently, set RemoveWallet=1 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
CitrixVirtualChannelConnectorMode	0 1 2 3 4 (default: Not defined)	AccessAgent Citrix Virtual Channel Connector mode configuration <ul style="list-style-type: none"> Set to 0 if you do not want to enable the Virtual Channel Connector. Set to 1 if you want to enable the Virtual Channel Connector on the client computer. Set to 2 if you want to enable the Virtual Channel Connector from the server and run AccessAgent in standard mode. Set to 3 if you want to enable the Virtual Channel Connector from the server and run AccessAgent in lightweight mode. Set to 4 if you want to enable the Virtual Channel Connector from the server and run AccessAgent in enforced lightweight mode.

Option Name	Value	Description
ICAClientInstallDir	<Citrix ICA Client installation directory>	Specify the installation directory for the Citrix ICA Client. This is required for the client Citrix Virtual Channel Connector.

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. This port is used to download IMS Server certificates only.
ImsDownloadProtocolDefault	default: http://	Default download protocol to download IMS Server certificates.

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)	Specify 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.

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 AccessStudio.msi file.

Use the Active Directory Group Policy Object options to apply language transforms. The AccessStudio component is 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

Locale Description	Language Transform	LCID	RFC1766 short string
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

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 for your IMS Server setup, 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 that forwards the connection request to the IMS 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. 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 "Known issues and solutions" in 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”
- “Installing the AccessAgent silently (command-line)” on page 104
- “Installing AccessAgent through Group Policy Object” on page 105
- “Verifying files and registry entries” on page 107
- “Verifying the ESSO Network Provider” on page 107
- “Enabling single sign-on support in Mozilla Firefox Extended Support Release” on page 108

Installing the AccessAgent

Use the Setup.exe file to install the complete AccessAgent package on the user computer.

Before you begin

- Note the product description or name that is listed on the Passport Advantage “Find downloads & media” page.
- Ensure that you have Administrator privileges.
- If you want single sign-on support for applications accessed through Mozilla Firefox, see “Enabling single sign-on support in Mozilla Firefox Extended Support Release” on page 108.

About this task

The Setup.exe file automatically installs the following software dependencies during the AccessAgent installation:

- MSXML 4.0 SP3
- MSXML 6.0 SP1
- Microsoft Visual C++ 2008 SP1

Procedure

1. Double-click Setup.exe from the AccessAgent installer package to start the InstallShield Wizard.
2. Select the product package level based on your license and click **Next**.
 - 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. Select **I accept the terms in the license agreement** and click **Next**.
4. In the Server field, enter the IMS Server name and click **Next**. The default port setting is 80. The installation directory is displayed. By default, AccessAgent is installed in C:\Program Files\IBM\ISAM ESSO\AA.

Note: To select a different location, click **Change** and select another folder.

If you specify an installation path that is too long, the path might display in a truncated form. However, this truncated form does not affect the actual installation location.

5. Click **Install**.
6. Click **Finish**. You are prompted to restart the computer.

7. Click **Yes**.

Results

There is a notification that the installation completed.

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 silently (command-line)

To do a silent installation, use the **/silent** parameter with the **Setup.exe** command.

Procedure

1. Open the SetupHlp.ini response file from the <AccessAgent install package path>\<AccessAgent install path>\Config directory. For example:
32-bit aa-8.2.1.0100\{9713108D-08D5-474E-92A3-09CD7B63DB34}\Config
64-bit aa-8.2.1.0100_x64\{E72C4028-45BB-4EE6-8563-3066EEB39A84}\Config
2. In the SetupHlp.ini response file, specify the following required parameters for a silent installation:

InstallTypeGPO

Verify that the value for the **InstallTypeGPO** parameter is 1.

ImConfigurationPromptEnabled

Verify that the value for the **ImConfigurationPromptEnabled** parameter is 1. The default value is 0.

Note: If the **ImConfigurationPromptEnabled** value is set to 1, the installation is not silent. The IMS Server configuration prompt is displayed even when you include the **/silent** parameter. Parameters in the response file always take precedence over any parameters in the command-line interface.

PriceLevel

Specify the product edition that you licensed with the **PriceLevel** parameter. For example: Suite or Standard.

ImServerName

Specify the IMS Server location. For example: IMSServerName = IMSServer.example.com.

3. Save the file.
4. Open the command prompt window.
5. In the command prompt window, type the **Setup.exe /silent /language:LCID** command.

Where:

Setup.exe

Installs AccessAgent.

/silent

Specifies a silent installation.

/language:LCID

Specifies that the installation run in a specific language. For a list of language Locale IDs (LCID), go to the Microsoft website at www.microsoft.com and search for Locale IDs assigned by Microsoft. If you specify a language ID that is not supported by the installation, the parameter is ignored.

Results

You installed AccessAgent silently as a background process. By default, the installation process created a log file in `%temp%\AAInstaller.log`.

Installing the AccessAgent through Tivoli Endpoint Manager

IBM Security Access Manager for Enterprise Single Sign-On integrates with IBM Tivoli Endpoint Manager 8.2 for the automatic deployment of AccessAgent on client computers.

For more information, see "Fixlet for AccessAgent installation or upgrade" in the *IBM Security Access Manager for Enterprise Single Sign-On Tivoli Endpoint Manager Integration Guide*.

Installing AccessAgent through Group Policy Object

For large AccessAgent deployments, you can install AccessAgent on multiple workstations through Microsoft Active Directory Group Policy Object.

About this task

For more information about the startup script, go to the Microsoft website at <http://www.microsoft.com> and search for Assign computer startup scripts GPO.

Procedure

1. In the SetupHlp.ini response file, specify the following required parameters:

InstallTypeGPO

Verify that the value for the **InstallTypeGPO** parameter is 1.

ImConfigurationPromptEnabled

Verify that the value for the **ImConfigurationPromptEnabled** parameter is 1.

PriceLevel

Specify the product edition that you licensed with the **PriceLevel** parameter. For example: Suite or Standard.

ImServerName

Specify the IMS Server location. For example: `IMSServerName = IMSServer.example.com`.

2. Put your AccessAgent installer package in a shared folder where all target client computers can access.
3. Navigate to **Group Policy Object > Computer Configuration > Windows Settings > Scripts > Startup**
4. Run the following installation batch script.

```
echo AA Suite Installation starts on %DATE% at %TIME% > %temp%\AASuiteInstall.log
<AccessAgent installer package>\setup.exe /silent
echo AA Suite Installation ends on %DATE% at %TIME% >> %temp%\AASuiteInstall.log
```

Ways of setting the IMS Server location

There are different 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 in C:\Program Files\IBM\ISAM ESSO\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 (response file)"
- "Setting the IMS Server location manually (menu shortcut)"

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 = <ISAM ESSO 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 name. For example: imssvr.example.com
3. Specify the HTTP port number. For example: 80
4. Click **OK** to finish.
5. Restart the computer.

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 ESSO\AA. The following subfolders and files are created after you install AccessAgent and AccessStudio.

- C:\Program Files\IBM\ISAM ESSO\AA\AccessAgent
- C:\Program Files\IBM\ISAM ESSO\AA\ECSS\AccessStudio
- C:\Program Files\IBM\ISAM ESSO\AA\Cryptoboxes
- C:\Program Files\IBM\ISAM ESSO\AA\Data
- C:\Program Files\IBM\ISAM ESSO\AA\ECSS
- C:\Program Files\IBM\ISAM ESSO\AA\ECSS\Firefox_ext
- C:\Program Files\IBM\ISAM ESSO\AA\ECSS\Firefox_xpcom
- C:\Program Files\IBM\ISAM ESSO\AA\GSKit
- C:\Program Files\IBM\ISAM ESSO\AA\License
- C:\Program Files\IBM\ISAM ESSO\AA\ECSS\JavaSupport
- C:\Program Files\IBM\ISAM ESSO\AA\Logs
- C:\Program Files\IBM\ISAM ESSO\AA\ECSS\SimpleToStateSupport
- C:\Program Files\IBM\ISAM ESSO\AA\TSSDK

AccessAgent and AccessStudio registry entries

AccessAgent and AccessStudio registry entries are stored in the [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO] key. Default registry values are automatically populated upon installation.

- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\AccessStudio]
- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\ECSS]
- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\ECSS\DeploymentOptions]
- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\ECSS\Temp]
- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\DeploymentOptions]
- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\IMSService\DefaultIMSSettings]
- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\IMSService\GlobalIMSSettings]
- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\AccessAgent\Integration]
- [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\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 that are 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 in the product installation directory.

Enabling single sign-on support in Mozilla Firefox Extended Support Release

To enable single sign-on and automation for web applications that are accessed through Mozilla Firefox Extended Support Release, you must download and install the AccessAgent extension for Mozilla Firefox Extended Support Release.

AccessAgent is not yet installed

You can enable the single sign-on support in Mozilla Firefox Extended Support Release even if AccessAgent is not yet installed.

Before you begin

Download the AccessAgent extension for Mozilla Firefox Extended Support Release from the IBM Security Access Manager for Enterprise Single Sign-On Support for Mozilla Firefox Extended Support Release technote at <http://www.ibm.com/support/docview.wss?uid=swg21660003>.

Ensure that you:

- Use Mozilla Firefox Extended Support Release.
- Have Administrator privileges.

About this task

Do this task only if you already installed Mozilla Firefox Extended Support Release but AccessAgent is not yet installed.

Procedure

1. Extract the downloaded ESS0Firefox<version>Extension.zip file to any folder. For example, C:\temp\.
2. Run the InstallFirefoxExt.vbs script from the command line with Administrator privileges.
3. Install AccessAgent. See "Installing the AccessAgent" in the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.
4. Start the Mozilla Firefox Extended Support Release browser. You might be prompted to enable the AccessAgent extension.

Results

The script automatically creates the following registry entry in the these locations:

Type	String (REG_SZ)
Key	For 32-bit [HKEY_LOCAL_MACHINE\SOFTWARE\ Mozilla\Firefox\extensions] For 64-bit [HKEY_LOCAL_MACHINE\SOFTWARE\ Wow6432Node\Mozilla\Firefox\ Extensions]
Name	isamesso@ibm.com
Value	<AA installation path>\ECSS\ Firefox17Extension

What to do next

Verify that the IBM Security Access Manager for Enterprise Single Sign-On Mozilla Firefox extension file is displayed and enabled in **Mozilla Firefox > Tools > Add-ons > Extensions**.

For troubleshooting issues, see the log file in the AccessAgent installation folder. For example: C:\Program Files\IBM\ISAM ESS0\AA\logs\AAInstaller.log.

AccessAgent is installed

You can enable the single sign-on support in Mozilla Firefox Extended Support Release after you installed AccessAgent.

Before you begin

Download the AccessAgent extension for Mozilla Firefox Extended Support Release from the IBM Security Access Manager for Enterprise Single Sign-On Support for Mozilla Firefox Extended Support Release technote at <http://www.ibm.com/support/docview.wss?uid=swg21660003>.

Ensure that you:

- Use Mozilla Firefox Extended Support Release.
- Have Administrator privileges.

About this task

Do this task only if you already installed AccessAgent.

Procedure

1. Extract the downloaded ESS0Firefox<version>Extension.zip file to any folder. For example, C:\temp\.
2. Run the InstallFirefoxExt.vbs script from the command line with Administrator privileges.
3. Start the Mozilla Firefox Extended Support Release browser. You might be prompted to enable the AccessAgent extension.

Results

The script automatically creates the following registry entry in the these locations:

Type	String (REG_SZ)
Key	For 32-bit [HKEY_LOCAL_MACHINE\SOFTWARE\ Mozilla\Firefox\extensions] For 64-bit [HKEY_LOCAL_MACHINE\SOFTWARE\ Wow6432Node\Mozilla\Firefox\ Extensions]
Name	isamesso@ibm.com
Value	<AA installation path>\ECSS\ Firefox<version>Extension

What to do next

Verify that the IBM Security Access Manager for Enterprise Single Sign-On Mozilla Firefox extension file is displayed and enabled in **Mozilla Firefox > Tools > Add-ons > Extensions**.

For troubleshooting issues, see the log file in the AccessAgent installation folder. For example: C:\Program Files\IBM\ISAM ESS0\AA\logs\AAInstaller.log.

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 112
- “Installing the AccessStudio silently (command-line)” on page 112

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 that is 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 package level based on your license and click **Next**.
 - 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.
5. 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.
6. Click **Next**.
7. Select **I accept the terms in the license agreement**.
8. 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.
9. Click **Next**. AccessStudio is installed successfully.
10. 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”.

- “Configuring the IMS Server for a cluster” on page 85.
- Ensure that you have Administrator privileges.

Note: To customize the .msi deployment package, see “Preparing an installation package to install on multiple PCs” on page 96.

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 is normally 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 in Administrator mode.
2. In the command prompt window, type the **msiexec** command with the following parameters (use without line breaks).

```
msiexec /i "<path>\ISAM  
ESS0 AccessStudio.msi" /quiet TRANSFORMS=<Installation  
language pack> PRICE_LEVEL=<License  
type>
```

Where:

/i "<path>\ISAM ESS0 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="<Installation language pack>"

Specifies the language pack to use for the installation.

Use TRANSFORMS="1033.mst" to install AccessStudio using the English language pack.

This is an optional parameter. If you do not include the **TRANSFORMS** parameter, the default language is U.S. English.

To apply a different language transform (.mst file) to the package, see "Including support for additional languages" on page 101.

PRICE_LEVEL="<License type>"

Specifies the licensed edition of AccessStudio. This is a required parameter.

To install the Standard edition, type "Standard". To install the Suite edition, type "Suite".

For example: If you want to install AccessStudio in English with Standard License, use the following command:

```
msiexec /i "<path>\ISAM ESS0 AccessStudio.msi" /quiet  
TRANSFORMS="1033.mst" PRICE_LEVEL="Standard"
```

Results

You installed AccessStudio silently as a background process. By default, the installation process created a log file in `c:\AAInstaller.log`.

Chapter 3. Upgrading

You can upgrade IBM Security Access Manager for Enterprise Single Sign-On from an earlier version.

IMS Server upgrade roadmap

The IMS Server upgrade roadmap contains the corresponding procedures for each upgrade scenario. Select the roadmap applicable to your IMS Server deployment.

Important: The provisioning API does not work after you upgrade from IMS Server version 3.6, 8.0, or 8.0.1. You must install the Native Library Invoker resource adapter on a 32-bit WebSphere Application Server, which is running the provisioning API service. See “Installing the Native Library Invoker resource adapter” on page 182. The functionality of the Native Library Invoker resource adapter that is required by the provisioning API works only on a 32-bit WebSphere Application Server.

The following sections are the roadmaps for upgrading the IMS Server:

- “Upgrading IMS Server 8.0.1 for a stand-alone deployment” on page 121
- “Upgrading IMS Server 8.0.1 for a network deployment (cluster)” on page 125
- “Upgrading IMS Server 8.1 for a stand-alone deployment” on page 118
- “Upgrading IMS Server 8.1 for a network deployment (cluster)” on page 119
- “Upgrading IMS Server 3.6 or 8.0” on page 128

Upgrading IMS Server 8.2 for a stand-alone deployment

Use the IMS Server upgrade roadmap for a better understanding of the topics and procedures that you must follow to complete the upgrade to a stand-alone IMS Server version 8.2.1.

	Procedure	Reference
1	Make sure that IMS Server 8.2 is installed and it works.	
2	Stop the ISAMESSOIMS and ISAMESSOIMSConfig applications in the WebSphere Application Server.	“Stopping and starting the IMS Server applications” on page 180
3	Uninstall the ISAMESSOIMS and ISAMESSOIMSConfig applications from the WebSphere Application Server administrative console. Note: Do this task so that you can back up the WebSphere Application Server profile.	“Uninstalling the ISAMESSOIMS and ISAMESSOIMSConfig applications from WebSphere Application Server” on page 193
4	Stop the stand-alone profile where IMS Server is installed.	“Stopping the WebSphere Application Server on Windows” on page 178
5	Stop the IBM HTTP Server.	“Stopping and starting the IBM HTTP Server on Windows” on page 174

	Procedure	Reference
6	Install the fix packs for WebSphere Application Server, IBM HTTP Server, IBM HTTP Server plug-ins and Java SDK. Note: For WebSphere Application Server Version 7.0, use fix pack 29 or later. For WebSphere Application Server Version 8.5, use fix pack 2 only.	<ul style="list-style-type: none"> • “Installing WebSphere Application Server, Version 7.0 fix packs” on page 24 • “Installing WebSphere Application Server, Version 8.5” on page 20 • “Installing the IBM HTTP Server Version 8.5” on page 26
7	Back up: <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 170 • “Backing up the database in DB2 9.7” on page 171 • “Backing up the database in DB2 10.1” on page 172
8	Start the WebSphere Application Server stand-alone profile.	“Starting the WebSphere Application Server on Windows” on page 176
9	Install and deploy the IMS Server applications in the WebSphere Application Server.	“Installing the IMS Server with the installer for an upgrade” on page 129
10	Verify the IMS Server deployment on the WebSphere Application Server.	“Verifying the IMS Server deployment on the WebSphere Application Server” on page 39
11	Install the latest IMS Server fix pack. Note: Download the latest fixes and updates for IMS Server from Fix Central.	IMS Server fix pack Readme, which is included in the fix pack package.
12	Upgrade the IMS Server settings.	“Upgrading configurations from 8.1 or 8.2 to 8.2.1” on page 132
13	Restart the WebSphere Application Server.	“Stopping the WebSphere Application Server on Windows” on page 178 “Starting the WebSphere Application Server on Windows” on page 176
14	Update the ISAMESSOIMS module mapping to forward connection requests.	“Updating the ISAMESSOIMS module mapping for connection request forwarding” on page 62
15	Restart the ISAMESSOIMS application.	“Stopping and starting the IMS Server applications” on page 180
16	Verify whether the upgrade is successful.	“Verifying a successful upgrade” on page 135

To upgrade the AccessAgent clients to 8.2.1, see “Upgrading the AccessAgent” on page 135.

To upgrade the AccessStudio clients to 8.2.1, see “Upgrading the AccessStudio” on page 135.

Upgrading IMS Server 8.2 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 8.2.1.

	Procedure	Reference
1	Make sure that IMS Server 8.2 is installed and it works.	
2	Stop the ISAMESSOIMS and ISAMESSOIMSConfig applications in the WebSphere Application Server.	"Stopping and starting the IMS Server applications" on page 180
3	Uninstall the ISAMESSOIMS and ISAMESSOIMSConfig applications from the WebSphere Application Server administrative console. Note: Do this task so that you can back up the WebSphere Application Server profile.	"Uninstalling the ISAMESSOIMS and ISAMESSOIMSConfig applications from WebSphere Application Server" on page 193
4	Stop the custom nodes and deployment manager.	"Stopping the WebSphere Application Server on Windows" on page 178
5	Stop the IBM HTTP Server.	"Stopping and starting the IBM HTTP Server on Windows" on page 174
6	Install the fix packs for WebSphere Application Server, IBM HTTP Server, IBM HTTP Server plug-ins and Java SDK. Note: For WebSphere Application Server Version 7.0, use fix pack 29 or later. For WebSphere Application Server Version 8.5, use fix pack 2 only.	<ul style="list-style-type: none"> • "Installing WebSphere Application Server, Version 7.0 fix packs" on page 24 • "Installing WebSphere Application Server, Version 8.5" on page 20 • "Installing the IBM HTTP Server Version 8.5" on page 26
7	Back up the IMS Server and its database: <ul style="list-style-type: none"> • Back up your WebSphere Application Server deployment manager 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 170 • "Backing up the database in DB2 9.7" on page 171 • "Backing up the database in DB2 10.1" on page 172
8	Start the WebSphere Application Server deployment manager.	"Starting the WebSphere Application Server on Windows" on page 176
9	Configure the Java heap size for the deployment manager.	"Configuring the heap size for the deployment manager" on page 77
10	Install the IMS Server on the deployment manager.	"Installing the IMS Server with the installer for an upgrade" on page 129
11	Verify the IMS Server deployment on the WebSphere Application Server.	"Verifying the IMS Server deployment on the WebSphere Application Server" on page 39
12	Verify that the node agents are stopped.	"Stopping the WebSphere Application Server on Windows" on page 178
13	Install the latest IMS Server fix pack. Note: Download the latest fixes and updates for IMS Server from Fix Central.	IMS Server fix pack Readme, which is included in the fix pack package.
14	Upgrade the IMS Server settings.	"Upgrading configurations from 8.1 or 8.2 to 8.2.1" on page 132
15	Restart the deployment manager.	"Stopping the WebSphere Application Server on Windows" on page 178 "Starting the WebSphere Application Server on Windows" on page 176

	Procedure	Reference
16	Update the ISAMESSOIMS module mapping to forward connection requests.	"Updating the ISAMESSOIMS module mapping for connection request forwarding" on page 62
17	Override session management for ISAMESSOIMS.	"Overriding session management for the ISAMESSOIMS" on page 90
18	Start the nodes.	"Starting the WebSphere Application Server on Windows" on page 176
19	Synchronize the nodes.	"Resynchronizing the nodes" on page 184
20	Start the cluster.	"Starting the WebSphere Application Server on Windows" on page 176
21	Verify whether the upgrade is successful.	"Verifying a successful upgrade" on page 135

Upgrading IMS Server 8.1 for a stand-alone deployment

Use the IMS Server upgrade roadmap for a better understanding of the topics and procedures that you must follow to complete the upgrade to a stand-alone IMS Server version 8.2.1.

	Procedure	Reference
1	Make sure that IMS Server 8.1 is installed and it works.	
2	Stop the TAM E-SSO IMS Server application in the WebSphere Application Server.	"Stopping and starting the IMS Server applications" on page 180
3	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.	"Uninstalling the TAM E-SSO IMS application from WebSphere Application Server" on page 192
4	Stop the stand-alone profile where IMS Server is installed.	"Stopping the WebSphere Application Server on Windows" on page 178
5	Stop the IBM HTTP Server.	"Stopping and starting the IBM HTTP Server on Windows" on page 174
6	Install the fix packs for WebSphere Application Server, IBM HTTP Server, IBM HTTP Server plug-ins and Java SDK. Note: For WebSphere Application Server Version 7.0, use fix pack 29 or later. For WebSphere Application Server Version 8.5, use fix pack 2 only.	<ul style="list-style-type: none"> • "Installing WebSphere Application Server, Version 7.0 fix packs" on page 24 • "Installing WebSphere Application Server, Version 8.5" on page 20 • "Installing the IBM HTTP Server Version 8.5" on page 26
7	Back up: <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 170 • "Backing up the database in DB2 9.7" on page 171

	Procedure	Reference
8	Start the WebSphere Application Server stand-alone profile.	"Starting the WebSphere Application Server on Windows" on page 176
9	Install and deploy the IMS Server applications in the WebSphere Application Server.	"Installing the IMS Server with the installer for an upgrade" on page 129
10	Verify the IMS Server deployment on the WebSphere Application Server.	"Verifying the IMS Server deployment on the WebSphere Application Server" on page 39
11	Install the latest IMS Server fix pack. Note: Download the latest fixes and updates for IMS Server from Fix Central.	IMS Server fix pack Readme, which is included in the fix pack package.
12	Upgrade the IMS Server settings.	"Upgrading configurations from 8.1 or 8.2 to 8.2.1" on page 132
13	Restart the WebSphere Application Server.	"Stopping the WebSphere Application Server on Windows" on page 178 "Starting the WebSphere Application Server on Windows" on page 176
14	Update the ISAMESSOIMS module mapping to forward connection requests.	"Updating the ISAMESSOIMS module mapping for connection request forwarding" on page 62
15	Restart the ISAMESSOIMS application.	"Stopping and starting the IMS Server applications" on page 180
16	Verify whether the upgrade is successful.	"Verifying a successful upgrade" on page 135

To upgrade the AccessAgent clients to 8.2.1, see "Upgrading the AccessAgent" on page 135.

To upgrade the AccessStudio clients to 8.2.1, see "Upgrading the AccessStudio" on page 135.

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 8.2.1.

	Procedure	Reference
1	Make sure that IMS Server 8.1 is installed and it works.	
2	Stop the TAM E-SSO IMS Server application in the WebSphere Application Server.	"Stopping and starting the IMS Server applications" on page 180
3	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.	"Uninstalling the TAM E-SSO IMS application from WebSphere Application Server" on page 192
4	Stop the custom nodes and deployment manager.	"Stopping the WebSphere Application Server on Windows" on page 178

	Procedure	Reference
5	Stop the IBM HTTP Server.	"Stopping and starting the IBM HTTP Server on Windows" on page 174
6	Install the fix packs for WebSphere Application Server, IBM HTTP Server, IBM HTTP Server plug-ins and Java SDK. Note: For WebSphere Application Server Version 7.0, use fix pack 29 or later. For WebSphere Application Server Version 8.5, use fix pack 2 only.	<ul style="list-style-type: none"> • "Installing WebSphere Application Server, Version 7.0 fix packs" on page 24 • "Installing WebSphere Application Server, Version 8.5" on page 20 • "Installing the IBM HTTP Server Version 8.5" on page 26
7	Back up the IMS Server and its database: <ul style="list-style-type: none"> • Back up your WebSphere Application Server deployment manager profile with the manageprofiles command. • Back up the IMS Server database. Note: To back up other supported databases, see your database documentation. 	"Backing up WebSphere Application Server profiles (manageprofiles command)" on page 170 "Backing up the database in DB2 9.7" on page 171
8	Start the WebSphere Application Server deployment manager.	"Starting the WebSphere Application Server on Windows" on page 176
9	Configure the Java heap size for the deployment manager.	"Configuring the heap size for the deployment manager" on page 77
10	Install the IMS Server on the deployment manager.	"Installing the IMS Server with the installer for an upgrade" on page 129
11	Verify the IMS Server deployment on the WebSphere Application Server.	"Verifying the IMS Server deployment on the WebSphere Application Server" on page 39
12	Verify that the node agents are stopped.	"Stopping the WebSphere Application Server on Windows" on page 178
13	Install the latest IMS Server fix pack. Note: Download the latest fixes and updates for IMS Server from Fix Central.	IMS Server fix pack Readme, which is included in the fix pack package.
14	Upgrade the IMS Server settings.	"Upgrading configurations from 8.1 or 8.2 to 8.2.1" on page 132
15	Restart the deployment manager.	"Stopping the WebSphere Application Server on Windows" on page 178 "Starting the WebSphere Application Server on Windows" on page 176
16	Update the ISAMESSOIMS module mapping to forward connection requests.	"Updating the ISAMESSOIMS module mapping for connection request forwarding" on page 62
17	Override session management for ISAMESSOIMS.	"Overriding session management for the ISAMESSOIMS" on page 90
18	Start the nodes.	"Starting the WebSphere Application Server on Windows" on page 176
19	Synchronize the nodes.	"Resynchronizing the nodes" on page 184
20	Start the cluster.	"Starting the WebSphere Application Server on Windows" on page 176
21	Verify whether the upgrade is successful.	"Verifying a successful upgrade" on page 135

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 8.2.1 involves the installation and configuration of other middleware. Use the IMS Server upgrade roadmap for a better understanding of the topics and procedures that you must follow to complete the upgrade to version 8.2.1.

	Procedure	Reference
1	Make sure that IMS Server 8.0.1 is installed and it works.	
2	Before you begin the upgrade: 1. Stop the IMS Server 8.0.1. 2. In the Windows Services Management Console, set the IMS Server 8.0.1 Windows server service Startup type to Manual .	
3	Back up the 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.	"Backing up the database in DB2 9.7" on page 171

	Procedure	Reference
4	<p>Prepare the WebSphere Application Server:</p> <ul style="list-style-type: none"> For WebSphere Application Server Version 7.0: <ul style="list-style-type: none"> Install WebSphere Application Server. Install the WebSphere Update Installer. Install the WebSphere Application Server fix pack. Install the WebSphere Application Server SDK. <p>Note: Use WebSphere Application Server Version 7.0 fix pack 29 or later.</p> <ul style="list-style-type: none"> For WebSphere Application Server Version 8.5: <ul style="list-style-type: none"> Install the IBM Installation Manager. Install WebSphere Application Server. <p>Note: Ensure that you are using WebSphere Application Server Version 8.5 fix pack 2.</p>	<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"> “Installing WebSphere Application Server, Version 7.0” on page 22 “Installing the WebSphere Update Installer” on page 23 “Installing WebSphere Application Server, Version 7.0 fix packs” on page 24 “Installing the IBM Installation Manager” on page 19 “Installing WebSphere Application Server, Version 8.5” on page 20 <p>WebSphere Application Server Version 7.0 documentation</p> <ul style="list-style-type: none"> http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp <p>WebSphere Application Server Version 8.5 documentation</p> <ul style="list-style-type: none"> http://publib.boulder.ibm.com/infocenter/wasinfo/v8r5/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>

	Procedure	Reference
5	<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. (Only applicable to IBM HTTP Server Version 7.0.) • Install the IBM HTTP Server Plug-in and SDK. 	<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"> • “Installing the IBM HTTP Server Version 7.0” on page 28 • “Installing the IBM HTTP Server Version 7.0 fix packs” on page 30 • “Installing the IBM HTTP Server Version 8.5” on page 26 <p>IBM HTTP Server Version 7.0 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>IBM HTTP Server Version 8.5 documentation</p> <ul style="list-style-type: none"> • http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/topic/com.ibm.websphere.ihs.doc/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>
6	<p>Create a stand-alone WebSphere Application Server profile.</p> <p>Note: Ensure that the WebSphere Application Server stand-alone profile is started.</p>	<p>“Creating stand-alone profiles (Profile Management tool)” on page 43</p>
7	<p>Configure the WebSphere Application Server.</p> <ul style="list-style-type: none"> • Configure the Java heap size memory. • Verify the Windows service. 	<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 46 • “Verifying the Windows service for WebSphere Application Server” on page 47 <p>WebSphere Application Server Version 7.0 documentation</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp <p>WebSphere Application Server Version 8.5 documentation</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v8r5/index.jsp

	Procedure	Reference
8	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 (stand-alone)” on page 52 • “Enabling SSL directives on the IBM HTTP Server” on page 55 IBM HTTP Server Version 7.0 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 IBM HTTP Server Version 8.5 documentation <ul style="list-style-type: none"> • http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/topic/com.ibm.websphere.ihs.doc/ihs/tihs_installihs.html 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.
9	Install the IMS Server on the WebSphere Application Server.	“Installing the IMS Server with the installer for an upgrade” on page 129
10	Verify the IMS Server deployment on the WebSphere Application Server.	“Verifying the IMS Server deployment on the WebSphere Application Server” on page 39
11	Upgrade the IMS Server settings.	“Upgrading configurations from 8.0.1 to 8.2.1” on page 133
12	Restart the WebSphere Application Server.	“Stopping the WebSphere Application Server on Windows” on page 178 “Starting the WebSphere Application Server on Windows” on page 176
13	Update the ISAMESSOIMS module mapping to forward connection requests.	“Updating the ISAMESSOIMS module mapping for connection request forwarding” on page 62
14	Configure the IBM HTTP Server to use the old IMS Server SSL certificate.	“Configuring the SSL certificate after an upgrade” on page 134
15	Restart the WebSphere Application Server.	For sample steps, see: <ul style="list-style-type: none"> • “Starting the WebSphere Application Server on Windows” on page 176 • “Stopping the WebSphere Application Server on Windows” on page 178
16	Verify whether the upgrade is successful.	“Verifying a successful upgrade” on page 135

To upgrade the AccessAgent clients to 8.2.1, see “Upgrading the AccessAgent” on page 135.

To upgrade the AccessStudio clients to 8.2.1, see “Upgrading the AccessStudio” on page 135.

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 for a better understanding of the topics and procedures that you must follow to complete the upgrade to version 8.2.1.

	Procedure	Reference
1	Make sure that IMS Server 8.0.1 is installed and it works.	
2	Before you begin the upgrade: 1. Stop the IMS Server 8.0.1. 2. In the Windows Services Management Console, set the IMS Server 8.0.1 Windows server service Startup type to Manual .	
3	Back up the 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.	“Backing up the database in DB2 9.7” on page 171

	Procedure	Reference
4	<p>Prepare the WebSphere Application Server:</p> <ul style="list-style-type: none"> For WebSphere Application Server Version 7.0: <ul style="list-style-type: none"> Install WebSphere Application Server. Install the WebSphere Update Installer. Install the WebSphere Application Server fix pack. Install the WebSphere Application Server SDK. <p>Note: Use WebSphere Application Server Version 7.0 fix pack 29 or later.</p> <ul style="list-style-type: none"> For WebSphere Application Server Version 8.5: <ul style="list-style-type: none"> Install the IBM Installation Manager. Install WebSphere Application Server. <p>Note: Ensure that you are using WebSphere Application Server Version 8.5 fix pack 2.</p>	<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"> “Installing WebSphere Application Server, Version 7.0” on page 22 “Installing the WebSphere Update Installer” on page 23 “Installing WebSphere Application Server, Version 7.0 fix packs” on page 24 “Installing the IBM Installation Manager” on page 19 “Installing WebSphere Application Server, Version 8.5” on page 20 <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>

	Procedure	Reference
5	<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. (Only applicable to IBM HTTP Server Version 7.0.) • Install the IBM HTTP Server Plug-in and SDK. 	<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"> • “Installing the IBM HTTP Server Version 7.0” on page 28 • “Installing the IBM HTTP Server Version 7.0 fix packs” on page 30 • “Installing the IBM HTTP Server Version 8.5” on page 26 <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>
6	<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. 	<p>“Creating network deployment profiles (Profile Management Tool)” on page 68</p> <p>“Starting the WebSphere Application Server on Windows” on page 176</p>
7	Configure the WebSphere Application Server for a cluster.	“Defining a cluster” on page 76
8	<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 77 • “Configuring the heap size for the application server” on page 46 • “Adding the directory server SSL certificate to WebSphere Application Server” on page 191 <p>WebSphere Application Server documentation:</p> <ul style="list-style-type: none"> • http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp

	Procedure	Reference
9	<p>Configure the IBM HTTP 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>Note: Repeat this task for each web server.</p>	<p>For sample instructions, see the following topics:</p> <ul style="list-style-type: none"> • “Enabling SSL directives on the IBM HTTP Server” on page 55 • “Configuring the IBM HTTP Server plug-in (network deployment)” on page 80 <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
10	Install the IMS Server on the deployment manager.	“Installing the IMS Server with the installer for an upgrade” on page 129
11	Verify the IMS Server deployment on the WebSphere Application Server.	“Verifying the IMS Server deployment on the WebSphere Application Server” on page 39
12	Verify that the node agents are stopped.	“Stopping the WebSphere Application Server on Windows” on page 178
13	Upgrade the IMS Server settings.	“Upgrading configurations from 8.0.1 to 8.2.1” on page 133
14	Restart the deployment manager.	<p>“Stopping the WebSphere Application Server on Windows” on page 178</p> <p>“Starting the WebSphere Application Server on Windows” on page 176</p>
15	Update the ISAMESSOIMS module mapping to forward connection requests.	“Updating the ISAMESSOIMS module mapping for connection request forwarding” on page 62
16	Override session management for ISAMESSOIMS.	“Overriding session management for the ISAMESSOIMS” on page 90
17	Configure the IBM HTTP Server to use the old IMS Server SSL certificate.	“Configuring the SSL certificate after an upgrade” on page 134
18	<p>Restart the WebSphere Application Server:</p> <ol style="list-style-type: none"> 1. Restart the deployment manager. 2. Start the nodes. 3. Fully resynchronize the nodes. 4. Start the cluster. 	<p>For sample steps, see:</p> <ul style="list-style-type: none"> • “Stopping the WebSphere Application Server on Windows” on page 178 • “Starting the WebSphere Application Server on Windows” on page 176 • “Resynchronizing the nodes” on page 184
19	Verify whether the upgrade is successful.	“Verifying a successful upgrade” on page 135

Upgrading IMS Server 3.6 or 8.0

You can upgrade IMS Server version 3.6 or 8.0 to IMS Server version 8.2.1.

About this task

If you upgraded from IMS Server version 3.6 or version 8.0, contact IBM Services for information about upgrading to version 8.2.1.

Procedure

1. Upgrade IMS Server 3.6 or 8.0 to 8.2.
See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* in the IBM Security Access Manager for Enterprise Single Sign-On 8.2 product documentation.
2. Upgrade IMS Server 8.2 to 8.2.1.
See “Upgrading IMS Server 8.2 for a stand-alone deployment” on page 115 or “Upgrading IMS Server 8.2 for a network deployment (cluster)” on page 116.

Upgrading to 8.2.1

To upgrade your current IBM Security Access Manager for Enterprise Single Sign-On version to version 8.2.1, upgrade the individual product components.

For an overview and considerations when upgrading to 8.2.1, see “Planning for an upgrade” in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

To complete 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 “IMS Server upgrade roadmap” on page 115.
- For the AccessAgent upgrade, see “Upgrading the AccessAgent” on page 135.
- For the AccessStudio upgrade, see “Upgrading the AccessStudio” on page 135.

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

- Stop the IMS Server and then back up the database.
- For IMS Server 8.0.1, stop the IMS Server service.
- For IMS Server 8.1, stop the TAM E-SSO IMS Server application.

Note:

- If you do not uninstall the TAM E-SSO IMS Server application, the IMS Server installer removes earlier versions of the TAM E-SSO IMS Server application and installs the new IMS Server.
- Uninstall the TAM E-SSO IMS Server application from the WebSphere administrative console.

Important: Do not run the IMS Server uninstaller.

- For IMS Server 8.2, stop the ISAMESSOIMS and ISAMESSOIMSConfig applications.
- 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.isamessoIm.s.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.isamessoIm.sConfig.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 package level based on your license and click **Next**.
 - 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.
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. Specify a new directory to install IMS Server 8.2.1. By default, IMS Server is installed in C:\Program Files\IBM\ISAM ESS0\IMS Server. Do not overwrite the IMS Server 8.2.
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 180.
11. Click **Yes** to specify that WebSphere Application Server security is enabled and then 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.
12. 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: 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.

- 13. 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.

- 14. Click **Next**. The **Pre-installation Summary** page is displayed.
- 15. Click **Install**.
- 16. 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 39.

Upgrading configurations from 8.1 or 8.2 to 8.2.1

Run the IMS Configuration Wizard to upgrade the IMS Server settings.

Before you begin

- Ensure that the IMS Server 8.2.1 is installed.
- Ensure that ISAMESS0IMSConfig is started.
- For WebSphere Application Server Stand-alone, ensure that the servers are stopped.
- For WebSphere Application Server Network Deployment, ensure that the cluster and node agents are 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 161.

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 roadmap:

- “Upgrading IMS Server 8.1 for a stand-alone deployment” on page 118.
- “Upgrading IMS Server 8.1 for a network deployment (cluster)” on page 119.

Upgrading configurations from 8.0.1 to 8.2.1

Run the IMS Configuration Wizard to upgrade the IMS Server settings.

Before you begin

- Ensure that the IMS Server 8.2.1 is installed.
- Ensure that ISAMESS0IMSConfig is started.
- For WebSphere Application Server Stand-alone, ensure that the servers are stopped.
- For WebSphere Application Server Network Deployment, ensure that the cluster and node agents are 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. Open the IMS Configuration Wizard.

For example: <https://localhost:9043/front>

The **Upgrade Configuration Wizard** page is displayed.

3. In **Server Set Up**, select **Upgrade from an earlier version 8.0.1**.

4. Click **Begin**.

5. In **Enter data source information**, the configuration values for the data source are pre-filled. Accept the default values if there are no changes.

6. Click **Next**.

7. In the **Old Configuration** page, specify the installation path of the old IMS Server. For example: `C:\Encentuate\IMSServer8.0.1.0.10`.

8. Click **Next**.

9. 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 that is used by the IBM HTTP Server.
- The typical default port number is 443.

10. 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 161.

11. In **Confirm Settings**, review the settings.
12. 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 roadmap:

- “Upgrading IMS Server 8.0.1 for a stand-alone deployment” on page 121.
- “Upgrading IMS Server 8.0.1 for a network deployment (cluster)” on page 125.

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 8.2.1 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 190.
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 8.2.1.

During the upgrade, you can use an AccessAgent installer with your prepackaged Wallet. Note that after the upgrade, AccessAgent continues to use your old Wallet.

To upgrade AccessAgent to 8.2.1:

1. Make sure that AccessAgent 8.x is installed and working properly.
2. Install AccessAgent 8.2.1. See “Installing the AccessAgent” on page 102.
When you upgrade, the AccessAgent 8.2.1 installer automatically uninstalls the existing AccessAgent. The new version is typically installed in
`<%PROGRAMFILES%>\IBM\ISAM ESS0\AA`.

Important: Upgrading from AccessAgent 8.1 (x86) on a 64-bit platform to AccessAgent 8.2.1 (x64) is not supported.

To upgrade, you must manually uninstall AccessAgent 8.1 (x86) and install AccessAgent 8.2.1 (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 8.0.1, 8.1 or 8.2.

To upgrade the AccessStudio to 8.2.1:

1. Uninstall the existing AccessStudio 8.x.
2. Install AccessStudio 8.2.1.

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 Chapter 5, “Planning worksheet,” on page 145 to reflect configuration or password changes.

Migrating the IMS Server 8.2.1 to a new environment

You can install or upgrade the IMS Server to version 8.2.1 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 8.2.1 is installed and that it works.

About this task

Migration from one IMS Server 8.2.1 host (<host A>) to another instance of a host (<host B>) applies to both installed or upgraded deployments of IMS Server 8.2.1

Where:

<host A>

Specifies the source host with a working IMS Server 8.2.1 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 8.2.1 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 8.2.1 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 36.
4. On *<host B>*, import the upgraded IMS Server configuration that you previously exported from *<host A>*. For more information, see the first step of this procedure.

Chapter 4. Uninstalling

Uninstalling IBM Security Access Manager for Enterprise Single Sign-On is dependent on the component you are planning to remove.

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 141
- “Uninstalling the AccessStudio” on page 142

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>
```

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 profile is restarted.
- On a network deployment, all of the nodes are synchronized and the deployment manager profile is restarted.

Note: Even if the command-line tool shows that the cleanup process is complete, the WebSphere Application Server might still be in the process of restarting.

2. Launch the software removal utility.
 - On Windows Server 2003, select **Start > Control Panel > Add or Remove Programs > ISAM ESSO IMS Server > Remove**.
 - On Windows Server 2008, or Windows 7, 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\<Server01Node01Cell01>\nodes\
<Server01Node01>\trust.p12
 - For WebSphere Application Server Network Deployment,
<was_home>\profiles\
<Dmgr_profilename>\config\cells\
<Server01Cell01>\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\<Server01Node01Cell01>\nodes\
<Server01Node01>\key.p12
 - For WebSphere Application Server Network Deployment,
<was_home>\profiles\
<Dmgr_profilename>\config\cells\
<Server01Cell01>\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 following documentation:
 - WebSphere Application Server Version 7.0 documentation:
<http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp>
 - WebSphere Application Server Version 8.5 documentation:
<http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/index.jsp>
 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 that is 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:
 - **All Programs > ISAM ESSO AccessAgent > Uninstall ISAM ESSO AccessAgent.**
 - **Control Panel > Add or Remove Programs > ISAM ESSO AccessAgent > Remove.**
 - **Control Panel > Programs and Features > ISAM ESSO AccessAgent > Remove.**

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 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.
 - Select **Start > All Programs > ISAM ESSO AccessStudio > Uninstall ISAM ESSO AccessStudio**.
 - On Windows XP, select **Start > Control Panel > Add or Remove Programs > ISAM ESSO AccessStudio > Remove**.
 - On Windows Server 2008 or Windows 7, 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.

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 that is 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 profile is restarted.
- On a network deployment, all of the nodes are synchronized and the deployment manager profile is restarted.

Note: Even if the command-line tool shows that the cleanup 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 139.

Chapter 5. 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 that are used throughout the guide and the corresponding default values. In some cases, the variable name matches the name of an environment variable that is set in the operating system. For example, %TEMP% represents the environment variable %TEMP% for Windows.

Note: When you install 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 (x86)
<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 Version 7.0	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 Note: If you are creating WebSphere Application Server Version 8.5 profiles for the IMS Server, do not specify a profile path that includes spaces in the path name.

Path variable	Component	Default directory (x86)
<%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 that are 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 that are used throughout the guide. The values vary depending on whether you are using WebSphere Application Server stand-alone or WebSphere Application Server Network Deployment.

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: <code>https://<was_hostname>:<admin_ssl_port>/ibm/console</code> If you are using WebSphere Application Server Network Deployment: <code>https://<dmgr_hostname>:<admin_ssl_port>/ibm/console</code> 	<code>https://localhost:9043/ibm/console</code> or <code>http://localhost:9060/ibm/console</code>

Description	Format	Example value
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>
AccessAdmin	<ul style="list-style-type: none"> If you are using a load balancer: <i>https:// <loadbalancer_hostname>:<ihs_ssl_port>/admin</i> If you are not using a load balancer: <i>https://<ims_hostname>:<ihs_ssl_port>/admin</i> If webserver is configured properly: <i>https://<ims_hostname>/admin</i> 	<ul style="list-style-type: none"> <i>https://imsserver:9443/admin</i> <i>https://imsserver/admin</i>
AccessAssistant	<ul style="list-style-type: none"> If you are using a load balancer: <i>https:// <loadbalancer_hostname>:<ihs_ssl_port>/aawwp</i> If you are not using a load balancer: <i>https://<ims_hostname>:<ihs_ssl_port>/aawwp</i> If webserver is configured properly: <i>https://<ims_hostname>/aawwp</i> 	<ul style="list-style-type: none"> <i>https://imsserver:9443/aawwp</i> <i>https://imsserver/aawwp</i>
Web Workplace	<ul style="list-style-type: none"> If you are using a load balancer: <i>https:// <loadbalancer_hostname>:<ihs_ssl_port>/aawwp?isWwp=true</i> If you are not using a load balancer: <i>https://<ims_hostname>:<ihs_ssl_port>/aawwp?isWwp=true</i> 	<i>https://imsserver:9443/aawwp?isWwp=true</i>

Users, profile names, and groups

The following table contains some of the users and groups that are created during the installation.

Variable	Description	Example value
<profile name>	WebSphere Application Server profile name. The profile name is defined when creating profiles for WebSphere Application Server with the manageprofiles command-line tool or graphical Profile Management tool.	<ul style="list-style-type: none"> If you are using WebSphere Application Server stand-alone: <AppSrv_profilenam> If you are using WebSphere Application Server Network Deployment: <ul style="list-style-type: none"> Deployment manager: <Dmgr_profilenam> Node <Custom_profilenam>
<WAS Admin user ID>	WebSphere administrator ID created during the installation of WebSphere Application Server.	wasadmin
<IHS Admin user ID>	HTTP Server administrator user ID created during the installation of the IBM HTTP Server.	ihsadmin
<DB2 Admin user ID>	DB2 administrator service user ID for Microsoft Windows created during the installation of IBM DB2.	db2admin
<IMS Admin user ID>	IBM Security Access Manager for Enterprise Single Sign-On administrator. User ID created during installation of the IMS Server for administration of IBM Security Access Manager for Enterprise Single Sign-On.	imsadmin
<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

Installing IBM DB2

The following table contains values that you specify when installing a database server.

Parameter	Default Or Example Value
Installation file	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
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 specify to create the IMS Server database.

Parameter	Default Or Example 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 specify, if you are creating a separate database user for IBM Security Access Manager for Enterprise Single Sign-On.

Parameter	Default Or Example Value
DB2 user	imsdb2admin
Administrative privileges	<ul style="list-style-type: none">• Connect to database• Create tables• Create packages

Installing IBM Installation Manager for WebSphere software installation

The following table contains the values that you specify when you install the IBM Installation Manager.

Parameter	Default Or Example Value
Installation file (administrative installation)	install.exe
Installation directory	C:\Program Files\IBM\InstallationManager
Local repository path	C:\repositories\product_name\local-repositories

Installing WebSphere Application Server

The following table contains the values that you specify when installing the WebSphere Application Server.

Parameter	Default Or Example Value
Installation directory	<was_home>
WebSphere Application Server Environment	(None) Note: Profiles are created only with the Profile Management tool or command-line interface after the WebSphere fix packs are applied. You can create the following profiles: For WebSphere Application Server stand-alone product deployments <ul style="list-style-type: none">• Application server For WebSphere Application Server Network Deployment (cluster) <ul style="list-style-type: none">• Deployment Manager• Custom Note: If you are creating WebSphere Application Server Version 8.5 profiles for the IMS Server, do not specify a profile path that includes spaces in the path name.
Enable Administrative Security	Yes
WebSphere Administration user name	wasadmin
Deployment Manager profile name	<Dmgr_profilename>

Parameter	Default Or Example Value
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 specify when you install the IBM Update Installer for WebSphere Software Installation.

Parameter	Default Or Example Value
Installation file	install.exe
Installation directory	C:\Program Files\IBM\WebSphere\ UpdateInstaller

Installing the latest WebSphere Application Server Version 7.0 fix pack

The following table contains the values that you specify when installing the latest WebSphere Application Server Version 7.0 fix pack.

Parameter	Default Or Example 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 specify when you install the IBM HTTP Server.

Parameter	Default Or Example Value
Installation directory	<ihs_home>
IBM HTTP Server HTTP Port	80
IBM HTTP Server HTTP Administration Port	8008
Run IBM HTTP Server as a Windows Service	Yes
Run IBM HTTP Administration as a Windows Service	Yes
Log on as a local system account	Yes

Parameter	Default Or Example Value
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	IMS821.samesso.ibm.com (example)

Installing the latest IBM HTTP Server Version 7.0 fix pack

The following table contains the values that you specify when you install the latest IBM HTTP Server Version 7.0 fix pack.

Parameter	Default Or Example 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 specify when configuring the IBM HTTP Server to work with the WebSphere Application Server.

Parameter	Default Or Example Value
Windows batch file	configure<webserver1>.bat
Original Location	<ihs_home>\Plugins\bin
Target Location	<was_home>\bin
com.ibm.SOAP.requestTimeoutproperty	6000
<i>Remote Web server management</i>	
Port	8008
User name	ihsadmin
Password	
Use SSL	No

Parameter	Default Or Example Value
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_plug-in.log • <ims_home>\ISAM_E-SSO_IMS_Server_InstallLog.log
Log level	Error

Installing IMS Server

The following table contains the values that you specify when you install the IMS Server.

Parameter	Default Or Example Value
Installation file	imsinstaller_8.2.1.0.x.exe
Installation folder	<ims_home>
Deploy IMS Server to WebSphere Application Server	<ul style="list-style-type: none"> • Yes - automatically deploys the IMS Server EAR file to WebSphere Application Server • No - you must manually deploy the IMS Server 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>\

Parameter	Default Or Example Value
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: <code><was_home>\profiles\ <AppSrv_profilename>\config\cells\ <Server01Cell01>\nodes\ <Server01Node01>\</code> If you are using WebSphere Application Server Network Deployment <code><was_home>\profiles\ <Dmgr_profilename>\config\cells\ <Server01Cell01>\</code>
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
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 specify when configuring the IMS Server.

Parameter	Default Or Example Value
JDBC provider name	ISAM ESSO JDBC Provider
Data source name	ISAM ESSO IMS Server Data Source

Parameter	Default Or Example Value
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>	
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 specify when configuring the enterprise directory.

Parameter	Default Or Example 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)

Chapter 6. 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: imsdbsr

Important: Specify the SQL Server logon account that you created in step 4 on page 187 on “Creating the database in SQL Server manually” on page 187.

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 that 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 run the following SQL statement.**

Note: Before running 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;
```

Chapter 7. 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:

- “Installing the IBM WebSphere Application Server Web 2.0 and Mobile feature pack” on page 25
- “Adding the JAX-RS shared library” on page 40
- “Configuring the IMS Server to use directory servers”
- “Backing up and restoring” on page 169
- “Stopping and starting components” on page 174
- “Deploying IMS Server on WebSphere Application Server manually” on page 180
- “Installing the web server plug-in for WebSphere Application Server manually” on page 185
- “Creating the database in SQL Server manually” on page 187
- “Enabling application security in WebSphere Application Server” on page 181
- “Basic commands for managing WebSphere Application Server profiles” on page 188
- “Ways of resolving hosts and IP addresses” on page 188
- “Renewing the SSL Certificate used by the IBM HTTP Server” on page 189
- “Adding the IMS Root CA to the truststore” on page 190
- “Adding the directory server SSL certificate to WebSphere Application Server” on page 191
- “Retrieving the IBM HTTP Server administrator name and password” on page 192
- “Uninstalling the TAM E-SSO IMS application from WebSphere Application Server” on page 192

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 IBM Security 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 Chapter 5, “Planning worksheet,” on page 145.

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 58.

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 domain name of the repository host. The NetBIOS domain 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 domain 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 domain 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>Connect using</p> <p>You can select only Domain controller host name / FQDN.</p> <p>Domain controller FQDN 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>Domain DNS name Specify the domain name of the Active Directory server that is connected to the IMS Server. For example: team.example.com</p> <p>Domain NetBIOS name Specify the NetBIOS domain name. The NetBIOS domain 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 domain 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 domain name. <p>Port Specify the port number. For example: the default is 389 (without SSL) or 636 (with SSL).</p> <p>Bind user name Specify the user name of the lookup user. For example: administrator.</p> <p>Password Enter the password for the lookup user.</p> <p>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>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> <p>Failover domain controllers</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>

Option	Parameters
If you are using SSL	<p>Connect using</p> <p>If you are using SSL, you can connect to the server by 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 by 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 domain name. The NetBIOS domain 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 domain 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 domain 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, which are 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 by 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 32.
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 stand-alone deployments, continue with step 18 on page 61 in “Configuring the IMS Server for a new installation with the IMS Configuration Wizard (stand-alone)” on page 58
- For network deployments, continue with step 18 on page 61 in “Configuring the IMS Server with the IMS Configuration Wizard (network deployment)” on page 85

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 Chapter 5, “Planning worksheet,” on page 145.

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 58.

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, which are 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, which are 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 stand-alone deployments, see “Configuring the IMS Server for a new installation with the IMS Configuration Wizard (stand-alone)” on page 58.
- For network deployments, see “Configuring the IMS Server with the IMS Configuration Wizard (network deployment)” on page 85.

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 166.

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 that 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 178.
- (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 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 8.2.1.

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 9.7

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.

Backing up the database in DB2 10.1

Back up the database in DB2 before you perform an upgrade, or after a successful server installation.

Before you begin

You must have SYSADM, SYSCTRL, or SYSMAINT authority.

Databases must be cataloged. Use **DB2 LIST DATABASE DIRECTORY** in the command line to view the cataloged database in the current instance.

Procedure

1. Click **Program files > IBM DB2 > Command Line Processor**.
2. Disconnect all applications and users from the database.
 - To get a list of all database connections for the current instance, use the **db2 LIST APPLICATIONS** command.
The command returns the following message if all applications are disconnected:**SQL1611W No data was returned by the Database System Monitor. SQLSTATE=00000.**
 - To disconnect all applications and users, use the **db2 FORCE APPLICATION ALL** command.
3. Backup your database using the **BACKUP DATABASE** command. Use the following parameters:
 - Database alias: **database_alias**
 - User name: **username**
 - Password: **password**
 - Directory to create backup files: **backup-dir**

For more information, see <http://pic.dhe.ibm.com/infocenter/db2luw/v10r1/index.jsp?topic=%2Fcom.ibm.db2.luw.qb.upgrade.doc%2Fdoc%2Ft0007139.html>

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 -backupFile <backup_file_location>**. For example
manageprofiles -restoreProfile -backupFile c:\backup\AppSrv01yymmdd.zip
The **manageprofiles** command-line tool always restores to the same path from which the profile was backed up.
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 that 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: When running command-line tools on Windows 7 and Windows Server 2008 operating systems with Windows User Account Control (UAC) enabled, certain operations require Administrator privileges. Examples of these operations are those involving Windows Services.

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. To run these command-line tools from a command prompt, do these steps:

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.
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 product documentation 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 product documentation. 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 Version 7.0 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 stand-alone WebSphere Application Server Version 8.5 configuration:

Stop the stand-alone server

Click **Start > All Programs > IBM WebSphere > IBM Websphere Application Server > <AppSrv01 profile> > Stop the server.**

- Stopping a clustered (network deployment) WebSphere Application Server Version 7.0 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**.

- Stopping a clustered (network deployment) WebSphere Application Server Version 8.5 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 > IBM Websphere Application Server > <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 8.2 and 8.2.1:

- Restart **ISAMESSOIMS** to restart AccessAdmin, AccessAssistant and Web Workplace.
- Restart **ISAMESSOIMSConfig** to restart the IMS Configuration Wizard and IMS Configuration Utility.

For IMS Server 8.1, restart **TAM E-SSO IMS Server**.

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:

For IMS Server 8.2 or 8.2.1

- **ISAMESSOIMS**
- **ISAMESSOIMSConfig**

For IMS Server 8.1

TAM E-SSO IMS Server

5. Click **Stop**.
6. Select the check box corresponding to the application.
7. 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 that are required to complete the installation. See Chapter 5, "Planning worksheet," on page 145.

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 183.

Network deployment

- a. Deploy ISAMESS0IMSConfig on deployment manager by using the command line. See “Installing the IMS Server EAR files (command-line)” on page 184.
 - b. Deploy ISAMESS0IMS to the cluster by using the Integrated Solutions Console. See “Installing the IMS Server EAR files manually” on page 183.
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 not required.

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 184.

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 ISAMESS0IMSConfig on a cluster, use the command-line tool.

Installing the IMS Server EAR files (command-line)

IMS Server has two EAR files, ISAMESS0IMS and ISAMESS0IMSConfig. 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 ISAMESS0IMSConfig before ISAMESS0IMS. 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 ESS0\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 ISAMESS0IMS 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: imsdbs
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: imsdbsr
 - 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: imsdbsr
 - 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.
 - 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: imsdbsr
 - 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: imsdbsr

- 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>
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 following WebSphere Application Server documentation:

- WebSphere Application Server Version 7.0 documentation: <http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp>
- WebSphere Application Server Version 8.5 documentation: <http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/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 that you configure on the DNS server must also match the host name that is 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 that is 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 that is 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
192.0.2.0	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 on page 190.
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 on page 190 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 Server** 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.

Uninstalling the ISAMESSOIMS and ISAMESSOIMSConfig applications from WebSphere Application Server

Uninstall the ISAMESSOIMS and ISAMESSOIMSConfig applications 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 **ISAMESSOIMS** and **ISAMESSOIMSConfig** applications.
5. Click **Uninstall**.
6. Click **Save**.

Results

You successfully removed the **ISAMESSOIMS** and **ISAMESSOIMSConfig** applications from the 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 character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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.

Privacy Policy Considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering uses other technologies that collect each user's user name, password or other personally identifiable information for purposes of session management, authentication, single sign-on configuration or other usage tracking or functional purposes. These technologies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at <http://www.ibm.com/privacy> and IBM’s Online Privacy Statement at <http://www.ibm.com/privacy/details/us/en> sections entitled “Cookies, Web Beacons and Other Technologies” and “Software Products and Software-as-a Service”.

Glossary

This glossary includes terms and definitions for IBM Security Access Manager for Enterprise Single Sign-On.

The following cross-references are used in this glossary:

- See refers you from a term to a preferred synonym, or from an acronym or abbreviation to the defined full form.
- See also refers you to a related or contrasting term.

To view glossaries for other IBM products, go to www.ibm.com/software/globalization/terminology (opens in new window).

A

account 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.

account data bag

A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item

The user credentials required for logon.

account data item template

A template that defines the properties of an account data item.

account data template

A template that defines the format of account data to be stored for credentials captured using a specific AccessProfile.

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 credential

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 radio frequency identification (active RFID)

A second authentication factor and presence detector. See also radio frequency identification.

active RFID

See active radio frequency identification.

AD See Active Directory.

administrator

A person responsible for administrative tasks such as access authorization and content management. Administrators can also grant levels of authority to users.

API See application programming interface.

application

A system that provides the user interface for reading or entering the authentication credentials.

application policy

A collection of policies and attributes governing access to applications.

application programming interface (API)

An interface that allows an application program that is written in a high-level language to use specific data or functions of the operating system or another program.

audit A process that logs the user, Administrator, and Helpdesk activities.

authentication factor

The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication

factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service

A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization code

An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

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.

B

base distinguished name

A name that indicates the starting point for searches in the directory server.

base image

A template for a virtual desktop.

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.

biometrics

The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

C

CA See certificate authority.

CAPI See cryptographic application programming interface.

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

CCOW

See Clinical Context Object Workgroup.

cell

A group of managed processes that are federated to the same deployment manager and can include high-availability core groups.

certificate

In computer security, a digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)

A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate.

CLI See command-line interface.

Clinical Context Object Workgroup (CCOW)

A vendor independent standard, for the interchange of information between clinical applications in the healthcare industry.

cluster

A group of application servers that collaborate for the purposes of workload balancing and failover.

command-line interface (CLI)

A computer interface in which the input and output are text based.

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.

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.

CSN See Card Serial Number.

CSP See cryptographic service provider.

D

dashboard

An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

database server

A software program that uses a database manager to provide database services to other software programs or computers.

data source

The means by which an application accesses data from a database.

deployment manager

A server that manages and configures operations for a logical group or cell of other servers.

deployment manager profile

A WebSphere Application Server runtime environment that manages 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. See also provision.

desktop pool

A collection of virtual desktops of similar

configuration intended to be used by a designated group of users.

directory

A file that contains the names and controlling information for objects or other directories.

directory service

A directory of names, profile information, and machine 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, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

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.

disaster recovery site

A secondary location for the production environment in case of a disaster.

distinguished name (DN)

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.

DLL See dynamic link library.

DN See distinguished name.

DNS See domain name server.

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.

E

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.

ESSO See enterprise single sign-on.

event code

A code that represents a specific event that is tracked and logged into the audit log tables.

F

failover

An automatic operation that switches to a redundant or standby system or node 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.

FIPS See Federal Information Processing Standard.

fix pack

A cumulative collection of fixes that is released between scheduled refresh packs, manufacturing refreshes, or releases. A fix pack updates the system to a specific maintenance level.

FQDN

See fully qualified domain name.

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`. See also host name.

G

GINA See graphical identification and authentication.

GPO See group policy object.

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.

H

HA See high availability.

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`. See also fully qualified domain name, IP address.

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.

I

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. See also host name.

J

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).

JMX See Java Management Extensions.

JRE See Java runtime environment.

JVM See Java virtual machine.

K

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. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

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 Terminal or Citrix Server and improves the single sign-on startup duration.

linked clone

A copy of a virtual machine that shares virtual disks with the parent virtual machine in an ongoing manner.

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.

M

managed node

A node that is federated to a deployment manager and contains a node agent and can contain managed servers. See also node.

mobile authentication

An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

N

network deployment

The deployment of an IMS Server on a WebSphere Application Server cluster.

node A logical group of managed servers. See also managed node.

node agent

An administrative agent that manages all application servers on a node and represents the node in the management cell.

O

one-time password (OTP)

A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

OTP See one-time password.

OTP token

A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

P

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 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.

PIN See personal identification number.

pinnable state

A state from an AccessProfile widget that

can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

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 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.

provision

To provide, deploy, and track a service, component, application, or resource. See also deprovision.

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.

Public Key Cryptography Standards (PKCS)

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

An 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.

R**radio frequency identification (RFID)**

An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS

See remote authentication dial-in user service.

random password

An arbitrarily generated password used to increase authentication security between clients and servers.

RDP See remote desktop protocol.

registry

A repository that contains access and configuration information for users, systems, and software.

registry hive

In Windows systems, the structure of the data stored in the registry.

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.

RFID See radio frequency identification.

root CA

See root certificate authority.

root certificate authority (root CA)

The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

S

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 that is used for issuing and exchanging 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.

serial ID service provider interface

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 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 the device as a second factor in AccessAgent.

signature

In profiling, unique identification information for any application, window, or field.

sign-on automation

A technology that works with application user interfaces to automate the sign-on process for users.

sign up

To request a resource.

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.

single sign-on (SSO)

An authentication process in which a user can access more than one system or application by entering a single user ID and password.

smart card

An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

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.

SMTP See Simple Mail Transfer Protocol.

snapshot

A captured state, data, and hardware configuration of a running virtual machine.

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. See also web service.

SPI See service provider interface.

SSL See Secure Sockets Layer.

SSL VPN

See Secure Sockets Layer virtual private network.

SSO See single sign-on.

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, using its own administrative console.

strong authentication

A solution that uses multifactor 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.

STS See Security Token Service.

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.

T**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.

terminal type (tty)

A generic device driver for a text display. A tty typically performs input and output on a character-by-character basis.

thin client

A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

transparent screen lock

An 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 a window on the desktop.

trust service chain

A chain of modules that operate in different modes such as validate, map, and issue truststore.

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. See also keystore.

tty See terminal type.

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.

U**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

The process of removing a 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.

V

VB See Visual Basic.

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 desktop

A user interface in a virtualized environment, stored on a remote server.

virtual desktop infrastructure

An infrastructure that consists of desktop operating systems hosted within virtual machines on a centralized server.

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.

VMM See Virtual Member Manager.

VPN See virtual private network.

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. See also SOAP.

WS-Trust

A web services security specification that defines a framework for trust models to establish trust between web services.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching

The process during single sign-on for an application whereby 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.

wallet manager

The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web server

A software program that is capable of servicing Hypertext Transfer Protocol (HTTP) requests.

Index

Numerics

- 1024 bits certificates 56, 83
- 2048 bits certificates 56, 83

A

- AAInstallDir parameter 98
- AboutThisProfile.txt file 43, 66
- AccessAgent
 - Citrix Server 95
 - files 107
 - installation path 98
 - installation road map 95
 - interactive installation 103
 - prerequisites 102
 - registry entries 107
 - server connection 106
 - silent installation 96
 - Terminal Server 95
 - uninstallation 141
 - upgrade 135
- accessibility vii
- AccessStudio
 - custom installers 110
 - files 107
 - installation road map 95
 - registry entries 107
 - silent installation 96
 - uninstallation 142
 - upgrade 135
- Active Directory
 - See Microsoft Active Directory
- adapters 34
- addresses 188
- application server profiles
 - network deployment 66
 - stand-alone 43

B

- base distinguished name
 - Active Directory 162
 - LDAP 167
- base profile 43
- BAT files
 - cleanImsConfig.bat file 143
 - deployIsamesso.bat file 184
 - deployIsamessoConfig.bat file 184
 - manageprofiles.bat file 188
 - setupCmdLine.bat file 182
- bind distinguished name
 - Active Directory 162
 - LDAP 167
- BIO-key 182
- biometric, installation 182

C

- Certificate Authority
 - See root CA
- certificates
 - 1024 bits 56, 83
 - 2048 bits 56, 83
- Citrix Servers 95, 99
- cleanImsConfig.bat file 143
- clusters
 - clusters 76
 - configuration 76
 - description 65
 - members 92
 - profiles 66
 - start 176
- cn attribute 168
- com.ibm.tamesso.ims-delhi.j2c.adapters.win32.rar file 182
- command-line environment
 - middleware 174
- CONF files
 - httpd.conf file 55, 82
- configuration
 - enterprise directory servers 161
 - IBM HTTP Server plug-in 80
 - IMS Server with IMS Configuration Wizard 58
 - WebSphere Application Server
 - clusters 76
 - WebSphere Application Server stand-alone 46
- connections 188
- Console Hook Loader 100
- ConsoleAppSupportEnabled
 - parameter 100
- custom profile 66

D

- database
 - collation 187
 - schema 187
- databases
 - back up 171, 172
 - DB2 16, 17
 - installation 16
 - Microsoft SQL Server 18
 - Oracle Database 17
 - preparation 15
 - restore 173
- DB2 15
 - database creation 17
 - installation 16
 - preparation 16
 - schema creation 157
 - users 158
- deployIsamesso.bat file 184
- deployIsamessoConfig.bat file 184
- deployment manager profile 66
 - maximum heap size 77

- deployment manager profile (*continued*)
 - start 176
- directory servers
 - See enterprise directories
- DisableWin7CAD parameter 100
- distinguished name (DN) 168
- DLL files
 - engina.dll 99
 - EnNetworkProvider.dll file 107
 - MSGina.dll 98
 - nwgina.dll 99
- DNS (Domain Name System) 163, 188
- Domain Name System (DNS) 163

E

- EAR files 58, 180
 - command-line 184
 - ISAMESOIMS 36
 - ISAMESOIMSConfig 36
 - manual deployment 183
- education vii
- EncentuateCredentialProviderEnabled
 - parameter 99
- EncentuateNetworkProviderEnabled
 - parameter 99
- engina.dll file 99
- EnginaConflictPromptEnabled
 - parameter 99
- EnginaEnabled parameter 99
- EnNetworkProvider.dll file 107
- Enterprise Archive (EAR) 58
- enterprise directories
 - description 161
 - generic LDAP Server 169
 - LDAP 35, 161, 167
 - lookup user 162, 167
 - Microsoft Active Directory 34, 161, 162
 - preparation 32
 - SSL 191
 - Tivoli Directory Server 35, 167
- ESSO Network Provider
 - verification 107
- Export Configuration Utility 171

F

- FirstSyncMaxRetries parameter 98
- FirstSyncRetryIntervalMins
 - parameter 98
- fix packs
 - IBM HTTP Server 30
 - IBM HTTP Server plug-in 31
 - WebSphere Application Server 24
 - WebSphere Update Installer 23

G

GinaWhiteList parameter 99
glossary 199

H

heap size 77
 deployment manager profile 46, 78
 performance 46, 78
high availability
 clusters 65
host names
 hostname command 188
 name resolution 188
 variables 146
hostname command 188
hosts file 188
httpd.conf file 55, 82, 185

I

IBM
 Software Support vii
 Support Assistant vii
IBM HTTP Server 55, 58, 82
 Administrator credentials 192
 fix packs 30
 installation 26, 28
 plug-in 31
 start 174
 stop 174
 verification 192
 WebSphere plug-in 52, 80, 185
IBM Installation Manager 19
IBM Security Identity Manager Active
 Directory Adapter 162
 installation 34
ikeyman utility 47, 71
IMS Configuration Wizard 58
IMS Root CA 190
IMS Server
 application mapping 62, 89
 configuration 58, 132
 database schemas 157
 description 15
 installation 1
 EAR files (command-line) 184
 EAR files manually 183
 network deployment 85
 upgrades 129
 with installers 36
 installation road map 1
 ISAMESSOIMS 58
 ISAMESSOIMSConfig 58
 manual deployment 180
 migration 136
 provisioning 61, 88
 reinstallation 143
 session management override 90
 stand-alone 58
 start 180
 stop 180
 target server
 menu shortcut 106
 response file 106
 uninstallation 139

IMS Server (*continued*)
 upgrade 1, 85, 129, 133
 upgrade 3.6 or 8.0 129
 upgrade road map 115
 verification
 configurations 63, 91
 WebSphere Application Server
 deployments 39
IMSAddressPromptEnabled
 parameter 101
ImsConfigurationEnabled parameter 99
ImsConfigurationPromptEnabled
 parameter 99, 104
ImsDownloadPortDefault parameter 101
ImsDownloadProtocolDefault
 parameter 101
ImsSecurePortDefault parameter 101
ImsServerName parameter 101
INI files
 SetupHlp.ini file 98
installation
 AccessAgent 102, 104
 AccessStudio 110, 112
 IBM DB2 16
 IBM HTTP Server 28
 IMS Server 36, 180
 prepackaged Wallet 96
 WebSphere Application Server 22
InstallTypeGpo parameter 99
IP addresses 189
ISAM ESSO AccessStudio.msi file 112,
 142
ISAMESSOIMS 58
 addition of nodes 92
 server mapping 62, 89
ISAMESSOIMSConfig 58

J

Java Naming and Directory Interface
 (JNDI) 182
Java Virtual Machine (JVM) 46, 78
java.lang.OutOfMemoryError event 77
JAX-RS 40
jaxrslib library 40
JNDI (Java Naming and Directory
 Interface) 182
JVM (Java Virtual Machine)
 performance 46, 78
JVMInstallationDirectories
 parameter 100

K

KDB files
 plugin-key.kdb file 55, 82
key.p12 file 154
keystore 47, 71
keystore location 36
keytool command 47, 71

L

language
 transforms 101
LCID (Locale ID) 101

LDAP (Lightweight Directory Access
 Protocol)
 certificates for WebSphere Application
 Server 191
 Data Interchange Format (LDIF) 35
 LDIF (LDAP Data Interchange
 Format) 35
 LDIF files 35
 preparation 32
 SSL-enabled 191
 Tivoli Directory Server 32
Lightweight Directory Access Protocol
 (LDAP)
 See LDAP
load balancer 58, 85, 102
Locale ID (LCID) 101
log parameter 104, 112
logs
 file location 43, 66
 server installation 58
lookup user
 LDAP servers 167
 Microsoft Active Directory 162

M

machine.wlt file 96
mail attribute 168
manageprofiles command 170, 171
manageprofiles.bat file 188
Microsoft Active Directory 34
 Application Mode (ADAM) 35
 Group Policy Object (AD GPO) 99,
 101
 IBM Security Identity Manager Active
 Directory Adapter 34
 Lightweight Directory Services (AD
 LDS) 35
 NetBIOS 34
 preparation 32
Microsoft SQL Server
 databases 18, 187
 requirements 15
 schemas 157
migration, IMS Server 136
Mozilla Firefox 103
MSGina.dll 99
MSI files 104, 112
 ISAM ESSO AccessStudio.msi
 file 112, 142
 large-scale deployments 96
msiexec command 104, 112
MST files 101
multi-language 101

N

Native Library Invoker (NLI) 182
nbstat command 188
NetBIOS
 description 188
 LDAP configuration 167
 Microsoft Active Directory
 configuration 162
netstat command 36, 43, 66
NLI resource adapter 182

- node agent
 - service creation 79
 - start the service 176
 - stop the service 176
- nodes
 - managed members 66
 - start 79
 - synchronization 185
- nslookup command 188
- nwgina.dll 99

O

- OldJVMInstallationDirectories
 - parameter 100
- Oracle Database
 - preparation 15, 17
 - schemas 157
- override session management 90

P

- packages, installation 96
- password reset 162
- password synchronization 162
- paths 145
- performance
 - heap size 46, 78
- planning worksheet
 - directories 145
 - host names 146
 - ports 146
 - profile names 147
 - URLs 146
 - users 147
- plug-in-cfg.xml file 185
- plugin-key.kdb file 55, 82
- port numbers
 - availability 36
 - network deployment 66
 - planning worksheet 146
 - stand-alone deployment 43
- prepackaged Wallets 96
- PriceLevel parameter 99
- problem-determination vii
- profiles
 - backup 170, 171
 - delete 188
 - deployment manager 66, 68
 - export 170
 - import 170
 - IMS Server
 - back up 171
 - restore 170
 - interactive 68
 - lists of 188
 - managed nodes, create 66
 - network deployment 66
 - restore 171
 - stand-alone 43
 - WebSphere Application Server
 - back up 170
 - restore 173
- publications
 - statement of good security practices vii

Q

- quiet parameter 104, 112, 113

R

- RAR files
 - com.ibm.tamesso.ims-delhi.j2c.adapters.win32.rar 182
- RebootConfirmationEnabled
 - parameter 99
- RebootEnabled parameter 99
- reinstallation
 - IMS Server 143
- RemoveWallet parameter 100
- ResetBioAPIPermission parameter 100
- resolution, URL addresses 188
- response file 98, 104, 112
- root CA 58
 - configuration 85
 - deployment manager 71
 - security 47
 - upgrade configurations
 - from 8.0.1 to 8.2.1 133
 - from 8.1 or 8.2 to 8.2.1 132

S

- scenarios
 - clustered 9
 - middleware reuse 1
 - stand-alone 3
- Secure Sockets Layer (SSL)
 - See SSL
- services
 - configuration WebSphere Application Server 46
 - start 174
 - stop 174
 - verification 47
- services.msc command 47
- session management, override 90
- setupCmdLine.bat file 182
- SetupHlp.ini file 98
- shared libraries 40
- silent
 - See also unattended installation
 - response file parameters 98
 - uninstallation 142
- SOAP 36
- SQL scripts 157
- SQL_Latin1_General_CP1_CS_AS
 - collation 187
- SSL
 - See also root CA
 - Active Directory 164, 191
 - after upgrade 134
 - certificate renewal 189
 - chained certificates 52, 80
 - directory server certificates 191
 - IBM HTTP Server 55, 82
 - LDAP servers 168, 191
 - two-way configuration 36
- stand-alone
 - description 42, 43
 - profiles 43
- startManager command 176, 185

- startNode command 79, 176
- startServer command 30, 176, 185
- stopManager command 178, 185
- stopNode command 178
- stopServer command 24, 178, 185
- synchronization
 - nodes 185
 - password 162

T

- TAM E-SSO IMS Server application
 - uninstallation 192, 193
- Terminal Servers 95, 99
- Tivoli Directory Server 167
 - description 32
 - preparation 35
- training vii
- transforms
 - language 101
 - parameter 113
- trust.p12 file 153
- truststore
 - location 36
 - root CA 71
 - stand-alone 47
- TXT files
 - AboutThisProfile.txt file 43, 66

U

- UAC (User Account Control) 174
- unattended
 - See also silent
 - response file parameters 98
 - uninstallation 142
- uninstallation 139
 - AccessStudio 142
 - AccessStudio silently 142
 - description 139
 - earlier versions 192, 193
 - IMS Server 139
- Update Installer 23
- upgrades 115
 - AccessAgent 129, 135
 - AccessStudio 129
 - IMS Server 129
 - from 3.6 or 8.0 129
 - from 8.0.1 121, 125
 - from 8.1 115, 117, 118, 119
 - port numbers
 - SOAP 129
 - verification 136
 - virtual appliance 129
- UsbKeyPromptEnabled parameter 99
- User Account Control (UAC) 174
- user name attribute 168

V

- Virtual Member Manager component
 - configuration 32, 161
 - directory servers 32

W

- Wallets 96
 - prepackaged 96, 98
 - removal 98
- WalletTypeSupported parameter 101
- WAS_PROFILE_HOME variable 182
- web server
 - See also* IBM HTTP Server
 - preparation 28
- WebSphere Application Server
 - application mapping 62, 89
 - application security 181
 - configuration 46
 - configuration clean up 143
 - installation 21, 22
 - fix packs 24
 - web server plug-in 185
 - WebSphere Update Installer 23
 - profile restoration 173
 - services verification 47
 - SSL certificates 191
- wizards
 - IMS Configuration Wizard 58
- WLT files
 - machine.wlt file 96

X

- XML files
 - plug-in-cfg.xml file 185



Printed in USA