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

# *Configuration Guide*

GC23-9692-01

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

# *Configuration Guide*

GC23-9692-01

**Note**
Before using this information and the product it supports, read the information in "Notices" on page 123.

**Edition notice**

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

# Contents

# About this publication

The IBM® Security Access Manager for Enterprise Single Sign-On provides sign-on and sign-off automation, authentication management, and user tracking to provide a seamless path to a strong digital identity. The *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* provides information about configuring the different components of the product.

## Intended audience

This publication is for Administrators who set up the main components of IBM Security Access Manager for Enterprise Single Sign-On after completing the necessary installations.

Administrators configure the following components:

- IMS Server
- AccessAgent
- Authentication factors such as:
  - Passwords
  - Secrets
  - ARFID
  - RFID
  - Fingerprint readers (BIO-key, DigitalPersona, UPEK)
  - Smart cards

## What this publication contains

This publication contains the following sections:

- Chapter 1, "Configuring the IMS Server," on page 1

  Covers the different configurable settings and utilities in the IMS Configuration Utility. You can provision an IMS Server administrator, register an authentication service, configure the enterprise directory, data source, and user authentication.
- Chapter 2, "Backing up and recovering the IMS Server, WebSphere Application Server profiles, and database," on page 45

  Provides information on how to back up the database for recovery when data loss occurs.
- Chapter 3, "Configuring AccessAgent," on page 49

  Provides instructions for configuring AccessAgent user interface and behavior. You can choose not to enable the ESSO GINA and change the AccessAgent banner.
- Chapter 4, "Configuring Citrix and Terminal Servers," on page 61

  Provides instructions for configuring the Citrix and Terminal Server and how to implement the AccessAgent lightweight mode.
- Chapter 5, "Configuring a strong authentication setup," on page 65

  Provides instructions for installing and configuring ARFID and biometric readers, as well as configuring smart card middleware support.
- Chapter 6, "Configuring a secure deployment," on page 87

Provides instructions for protecting your deployment against potential security risks.

- Appendix A, “Logging on to AccessAdmin,” on page 91

  Describes how to access and log on to AccessAdmin.
- Appendix B, “Setting up policy templates,” on page 93

  Provides instructions on how you can automatically set up policy templates, depending on the needs of your organization.
- Appendix C, “Automatically assigning User Policy Templates to new users,” on page 95

  Provides instructions on how you can configure user attributes and map them to user policy templates in AccessAdmin.
- Appendix D, “Excluding machine attributes,” on page 97

  Provides steps on how you can manage machine attributes with the IMS Server.
- Appendix E, “Configuring JMX support,” on page 99

  Describes how you can use Java Management Extensions to monitor the IMS server beans.
- Appendix F, “Planning worksheet,” on page 101

  Provides the default and sample values for the installation and configuration of the IBM Security Access Manager for Enterprise Single Sign-On.
- Appendix G, “Command-line interface reference,” on page 113

  Covers the different command-lines that you can use for IMS Server configuration.

## Publications

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

### IBM Security Access Manager for Enterprise Single Sign-On library

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

- *IBM Security Access Manager for Enterprise Single Sign-On Quick Start Guide*, CF38DML

  Read this guide for a quick start on the main installation and configuration tasks to deploy and use IBM Security Access Manager for Enterprise Single Sign-On.
- *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*, SC23995203

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

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

  This guide helps you to install the different product components and their required middleware, and also do the initial configurations required to complete

the product deployment. It covers procedures for using virtual appliance, WebSphere® Application Server Base editions, and Network Deployment.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- *IBM Security Access Manager for Enterprise Single Sign-On Lightweight AccessAgent mode on Terminal Server SDK Guide*, SC14765700

  Read this guide for the details on how to develop a virtual channel connector that integrates AccessAgent with Terminal Services applications.

- *IBM Security Access Manager for Enterprise Single Sign-On Serial ID SPI Guide*, SC14762600

  IBM Security Access Manager for Enterprise Single Sign-On has a Service Provider Interface (SPI) for devices that contain serial numbers, such as RFID. See this guide to know how to integrate any device with serial numbers and use it as a second authentication factor with AccessAgent.
- *IBM Security Access Manager for Enterprise Single Sign-On Context Management Integration Guide*, SC23995403

  Read this guide if you want to install and configure the Context Management solution.
- *IBM Security Access Manager for Enterprise Single Sign-On User Guide*, SC23995003

  This guide is intended for the end users. This guide provides instructions for using AccessAgent and Web Workplace.
- *IBM Security Access Manager for Enterprise Single Sign-On Error Message Reference Guide*, GC14762400

  This guide describes all the informational, warning, and error messages associated with IBM Security Access Manager for Enterprise Single Sign-On.

## Accessing terminology online

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

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

## Accessing publications online

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

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

## Ordering publications

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

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

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

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

1. Go to http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss.
2. Select your country from the list and click **Go**.
3. Click **About this site** in the main panel to see an information page that includes the telephone number of your local representative.

## Accessibility

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

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

## Tivoli technical training

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

## Tivoli user groups

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

- 23,000+ members
- 144+ groups

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

## Support information

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

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

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

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

## Conventions used in this publication

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

## Typeface conventions

This publication uses the following typeface conventions:

**Bold**

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

*Italic*

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

**`Monospace`**

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

## Operating system-dependent variables and paths

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

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

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

# Chapter 1. Configuring the IMS Server

The IMS Server centrally manages users, authentication factors, credential Wallets, AccessProfiles, audit logs, and policies.

This section focuses on configuring the IMS Server through the IMS Configuration Utility. IMS Server configuration with the IMS Configuration wizard is covered in the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.

See the following topics for more information.



## Accessing the IMS Configuration Utility

When you install the IMS Server, it deploys an application that contains an IMS Configuration Utility. The IMS Configuration Utility is a web-based interface for configuring the different IMS Server settings.

### Procedure

1. Enter the following addresses in your browser. The address varies depending on the type of deployment.
   - If you are using WebSphere Application Server Base: `https://<was_hostname>:<admin_ssl_port>/ webconf`.
   - If you are using WebSphere Application Server Network Deployment: `https://<dmgr_hostname>:<admin_ssl_port>/ webconf`.
   - For example, `https://localhost:9043/webconf`
2. Select the preferred language from the **Language** list.
3. Enter your WebSphere logon credentials.
4. Click **Log on**.

## Provisioning IMS Server Administrators

Provisioning an IMS Server Administrator creates and stores the Administrator account in the IMS Server database.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Under **Configuration Wizards**, click **Provision IMS Administrator**.
3. At **Choose Credentials**, enter the user name, password, and domain of a valid enterprise directory user.
4. Click **Next**.
5. Review the configuration summary.
6. Click **Finish**.

# Basic settings

You can configure the basic settings in the IMS Configuration Utility. Basic settings include authentication services, enterprise directories, biometric support, and ActiveCode deployment.

See the following topics for more information.

- "Adding an authentication service"
- Configuring the IMS Server to use directory servers
- "Enabling biometric support" on page 10
- "Configuring ActiveCode deployment" on page 10

## Adding an authentication service

An authentication service defines how user credentials are submitted to the application. Multiple applications can use the same authentication service.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Select **Basic settings** > **Authentication services** from the IMS Configuration Utility navigation panel.
3. Click **Add new service**.

   **Note:** You can also create Authentication services in AccessStudio. However, you can create connectors for the authentication services only with the IMS Configuration Utility.
4. Complete the following fields:

| Option | Description |
|---|---|
| **Authentication service ID** | Enter a unique identifier for the authentication service. |
| **Authentication service name** | Enter the name of the authentication service from the Wallet Manager.<br>**Note:** You can store the authentication service display name in multiple languages, depending on the language specified by the user during logon. |
| **Description** | Enter a short description of the authentication service.<br>**Note:** You can store the authentication service description in multiple languages, depending on the language specified by the user during logon. |
| **Account data template ID** | Select an account data template ID from the drop-down list.<br><br>The template ID defines the structure of the account data to be captured for the authentication service.<br><br>For example, `adt_ciuser_cspwd` means that the selected account data template captures a user name that is not case sensitive and a case sensitive password. |

| Option | Description |
| --- | --- |
| **Authentication service groups** | Select the group for the authentication service from the drop-down list and click **Add**. |
| **Server locators to be used during injection** | Enter the name of the server alias during auto-fill and click **Add**. |
| **Server locators to be used during capture** | Enter the name of the server alias during capture and click **Add**. |

5. Edit any of the configuration keys in the form, except for the **Authentication Service ID**.
6. Click **Add**.

# Configuring the IMS Server to use directory servers

You can configure the IMS Server to use either an LDAP server or multiple Active Directory servers. You can configure directory servers either through the IMS Configuration Wizard or the IMS Configuration Utility.

Use the IMS Configuration Wizard to set up the IMS Server for the first time in a new installation. The IMS Configuration Wizard includes steps for setting up the IMS Server to use directory servers. Use the IMS Configuration Utility to set up the IMS Server to use directory servers later.

After configuring the directory server, restart the WebSphere Application Server immediately to apply the configuration changes. If you configure the web server definition and the directory server before restarting the WebSphere Application Server, the configuration is not saved.

Ensure that the directory server repositories are running to connect to these repositories. If one or more of the configured repositories are unreachable, you cannot authenticate or stop the WebSphere Application Server.

If the problem persists, it is because of a security feature of virtual member manager. The virtual member manager always checks all repositories before authenticating the user. For more information about the solution, see http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.wim.doc/UnableToAuthenticateWhenRepositoryIsDown.html.

## Configuring the IMS Server to use Active Directory servers

Add prepared Active Directory servers so that the IMS Server can look up user account information for authorization. You can add multiple Active Directory servers.

### Before you begin

You can provide self-service password reset in AccessAssistant and Web Workplace under the following conditions for your Active Directory connection:

- **Not using SSL:** Ensure that the Tivoli Identity Manager Active Directory Adapter is installed and running on the directory server or on a separate host.

  Be ready to provide the credentials for an administrative user or a designated user with password reset privileges. For example: `myresetusr`.
- **Using SSL:** Be ready to provide the credentials for an administrative user or a designated user with password reset privileges. For example: `myresetusr`.

**Note:** You are not required to install Tivoli Identity Manager Active Directory Adapter.

For LDAP enabled SSL connections, you must add the directory server SSL certificates to the WebSphere Application Server. See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.

You must prepare the following enterprise directory information:

- Domain controller FQDN. For example: `adserver.team.example.com`
- Domain DNS name. For example: `team.example.com`.
- Credentials for the directory lookup user. For example: `lookupusr`.
- Base distinguished name. For example: `cn=users,dc=team,dc=example,dc=com`
- Optional: For password resets in AccessAssistant and Web Workplace, you need the credentials for a directory user with password reset privileges. For example: `myresetusr`.

If you are using the planning worksheet, see the Appendix F, "Planning worksheet," on page 101.

## Procedure

1. Log on to the IMS Configuration Utility.
2. In the IMS Configuration Utility navigation pane, under **Basic Settings**, click **Enterprise Directories**.
3. Click **Add new repository**.
4. Select the enterprise directory type.
   a. Select **Active Directory**.
   b. Click **Next**.
5. For Active Directory servers, complete the following steps:
   a. Specify whether to enable password synchronization.

      Password synchronization is available only for Active Directory servers.

      When password synchronization is enabled, the IBM Security Access Manager for Enterprise Single Sign-On password is synchronized with Active Directory.

      When you change the password, the software changes it on every Active Directory host on which the user has an account. If the password is reset out-of-band, the IBM Security Access Manager for Enterprise Single Sign-On password is resynchronized at the next online logon.

      See the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide* for more details about Active Directory password synchronization.
   b. Specify the repository connection details.

      **Tip:** To see additional help for each item, move the cursor over each item.

      **Domain controller FQDN**
      Specify the fully qualified domain name of the domain controller . For example: `adserver.team.example.com`

      **Domain DNS Name**
      Specify the domain name of the server where the IMS Server connects. For example: `team.example.com`.

**Note:** This attribute is not the fully qualified name of the DNS. It is the "domain" of the server.

**Domain NetBIOS Name**
Specify the NetBIOS computer name of the repository host. The NetBIOS computer name is typically the same as the repository host name of the same domain. For example: `mydirsvr`.

**Note:**

- The NetBIOS name is not validated by the IMS Server. You must provide the correct name.
- To determine the correct NetBIOS computer name, go to the Microsoft website at www.microsoft.com and search for "nbtstat". See instructions on how to use **nbtstat** to determine the NetBIOS computer name with the **nbtstat** command.

**Port** The default port number is `389` without SSL. The default port number with SSL is `636`.

**Note:** To enable password resets in a non-SSL environment, use the Tivoli Identity Manager Active Directory Adapter. In an SSL environment, you are not required to install the Tivoli Identity Manager Active Directory Adapter.

**Bind user name**
Specify the user name of the lookup user. For example: `lookupusr`.

**Password**
Enter the password for the lookup user.

6. Click **Next**.
7. To view or customize additional repository details, click **Open advanced settings**.
8. Specify whether you are using a Secure Socket Layer (SSL) connection.

| Option | Parameters |
|---|---|
| If you are not using SSL | **Connect using**<br>You can select only **Domain controller host name / FQDN**.<br><br>**Domain controller FQDN**<br>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.<br><br>**Domain DNS name**<br>Specify the domain name of the Active Directory server that is connected to the IMS Server. For example: `team.example.com` |

| Option | Parameters |
| --- | --- |
| | **Domain NetBIOS name**<br>Specify the NetBIOS computer name. The NetBIOS computer name is typically the same as the host name of the computer in the same domain. For example: `mydirsvr`<br>**Note:**<br>• The NetBIOS name is not validated by the IMS Server. You must provide the correct name.<br>• To determine the correct NetBIOS computer name, go to the Microsoft website at www.microsoft.com and search for "nbtstat". See instructions on how to use **nbtstat** to determine the NetBIOS computer name.<br><br>**Port** Specify the port number. For example: the default is **389** (without SSL) or **636** (with SSL).<br><br>**Bind user name**<br>Specify the user name of the lookup user. For example: `administrator`.<br><br>**Password**<br>Enter the password for the lookup user.<br><br>**Base distinguished name**<br>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.<br>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`.<br><br>**Failover domain controllers**<br>Use a failover domain controller for replicated Active Directory servers in a high availability configuration.<br>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. |
| If you are using SSL | **Connect using**<br>If you are using SSL, you can connect to the server using a **Domain DNS name** or a **Domain controller host name / FQDN**. If you are using a domain name server to resolve host names or IP addresses, select **Domain DNS name**.<br>If you select **Domain controller host name / FQDN**, the **Domain controller host name / FQDN** is displayed.<br><br>**Domain controller host name / FQDN**<br>If you choose to connect using **Domain controller host name / FQDN**, the domain controller host name or fully qualified domain name is displayed.<br><br>**Domain DNS name**<br>The domain name of the Active Directory server that is connected to the IMS Server is displayed. For example: `team.example.com` |

| Option | Parameters |
| --- | --- |
| | **Domain NetBIOS name**<br>Specify the NetBIOS computer name. The NetBIOS computer name is typically the same as the host name of the computer in the same domain. For example: `mydirsvr`<br>**Note:**<br>• The NetBIOS name is not validated by the IMS Server. You must provide the correct name.<br>• To determine the correct NetBIOS computer name, go to the Microsoft website at www.microsoft.com and search for "nbtstat". See instructions on how to use **nbtstat** to determine the NetBIOS computer name.<br><br>**Bind distinguished name**<br>Enter the distinguished name (DN) for the lookup user. The distinguished name is the name that uniquely identifies an entry in the directory. The directory user must be authorized to perform directory lookups. A DN is made up of attribute=value pairs, separated by commas. For example: `cn=lookupusr,cn=users,dc=team,dc=example,dc=com`<br><br>**Password**<br>Enter the password for the lookup user.<br><br>**Base distinguished name**<br>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.<br><br>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`.<br><br>**Failover domain controllers**<br><br>This field is displayed only if you choose a connection using **Domain controller host name / FQDN**.<br><br>Use a failover domain controller for replicated Active Directory servers in a high availability configuration.<br><br>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. |

9. 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`.

10. Click **Next**.
11. 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).

## 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`.

If you are using the planning worksheet, see the Appendix F, "Planning worksheet," on page 101.

### Procedure

1. Log on to the IMS Configuration Utility.
2. In the IMS Configuration Utility navigation pane, under **Basic Settings**, click **Enterprise Directories**.
3. Click **Add new repository**.
4. Select the enterprise directory type.
    a. If you are using LDAP servers, select **LDAP**.
    b. Click **Next**.
5. For the LDAP server, specify the following details:
    a. Specify the repository details.

    **Tip:** To see additional help for each item, move the cursor over each item.

    **Domain controller host name / FQDN**
    Specify the host name or the fully qualified domain name of the LDAP server. For example: `mydirsvr`

    **Port** Specify the port number. For example: the default is `389` (without SSL) or `636` (with SSL).

    **Remember:** If your deployment uses non-default port numbers or you are connecting to the repository over SSL, be sure to specify the correct port number.

    **Bind distinguished name**
    Shows the distinguished name for the lookup user. The distinguished name is the name that uniquely identifies an entry in the directory. The lookup user must be authorized to perform directory lookups on the server.

    A DN is made up of `attribute=value` pairs, separated by commas. For example: `cn=lookupusr,ou=users,o=example,c=us`.

**Password**
Enter the password for the lookup user.

6. To customize additional repository details, click **Advanced**.

   **Use SSL**
   Specify whether you are using a secure socket layer (SSL) connection.

   **Domain controller host name / FQDN**
   Specify the domain controller fully qualified domain name. For example: `mydirsvr`.

   **Port** Specify the port number. For example: The default port is **389** (without SSL) or **636** (with SSL).

   **Bind distinguished name**
   Enter the distinguished name (DN) for the lookup user. The distinguished name is the name that uniquely identifies an entry in the directory.

   A DN is made up of attribute=value pairs, separated by commas. For example: `cn=lookupusr,ou=users,o=example,c=us`.

   **Password**
   Enter the password for the lookup user.

   **User name attributes**
   Specify a valid enterprise directory user name attribute that users provide as their user names for authentication. Other attributes can also be used for the user name. For example: if you specify the `mail` attribute, users must enter their email addresses for their user names.

   To use different user name attributes (for example, badge number, email address or an employee number), provide the custom attributes properties instead.

   For LDAP, the default is `cn`.

   **Base distinguished name**
   At least one base distinguished name is required. The base distinguished name indicates the starting point for searches in this LDAP directory server. For authorization purposes, this field is case-sensitive by default. Match the case in your directory server.

   For example: For a user with DN of `cn=lookupusr,ou=users,o=example,c=us`, specify the base distinguished name with the following option: `ou=users,o=example,c=us`.

   **Failover domain controllers**

   Use a failover domain controller to ensure the LDAP server high availability.

   Specify the host name or the fully qualified domain name, and the port number of the secondary domain controller. The secondary domain controller is used when the primary domain controller fails.

7. Click **Next**.
8. 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.

## Testing the enterprise directory connector

You can test the enterprise directory connection to verify the enterprise directory configuration.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Select **Basic settings** > **Enterprise directories** from the IMS Configuration Utility navigation panel.
3. In the **Enable password synchronization** option, select **Yes** or **No**.
4. Click **Update**.

## Verifying user information

Use the diagnostic tool so that you can verify user information.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Select **Basic settings** > **Enterprise directories** from the IMS Configuration Utility navigation panel.
3. Click **Diagnostic test**.
4. Under **Verify user**, type in the username and password.
5. In **Repository Alias**, select the correct repository.
6. Click **Verify user**.

# Enabling biometric support

IBM Security Access Manager for Enterprise Single Sign-On supports fingerprint authentication. Users can authenticate themselves by scanning their fingerprints on a fingerprint reader. To implement fingerprint authentication, you must enable biometric support in the IMS Server.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Select **Basic settings** > **Biometric support**.
3. In the **Enable biometrics support** field, select **True** or **False**.
4. Click **Update**.

# Configuring ActiveCode deployment

ActiveCode is a second-factor authentication mechanism to authenticate users when their desktop has no connection to the IMS Server. You can edit the different ActiveCode settings such as its validity period, verification attempts, and assigned messaging connector.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Select **Basic Settings** > **ActiveCode deployment** from the IMS Configuration Utility navigation panel.
3. Complete the following fields:

| Option | Description |
| --- | --- |
| **Maximum number of ActiveCode verification attempts** | Enter the maximum number of Mobile ActiveCode entries that are not correct before the account gets locked. |
| **ActiveCode account reset-lockout time, in seconds** | Enter the waiting time before a locked Mobile ActiveCode is reset (in milliseconds). Enter a number. |
| **Mobile ActiveCode validity period, in seconds** | Enter the period when a Mobile ActiveCode is available for use. |
| **Allowed ActiveCode client IPs** | Specify the IP address of the MAC-enabled application, which connects to the MAC Service Module of the IMS Server.<br>**Note:** IBM Security Access Manager for Enterprise Single Sign-On 8.2 supports Internet Protocol version 6 (IPv6). |
| **Enable SSL for ActiveCode client** | Specify whether SSL access is required for the client requesting or verifying Mobile ActiveCode calls.<br><br>Select **Yes** from the list to enable SSL.<br><br>Select **No** from the list if you are using RADIUS. |
| **ActiveCode access password** | Enter the password between the client and server for making Mobile ActiveCode calls. |
| **OTP look-ahead number** | Enter the number of times an OTP or a One Time Password generates in sequence from the seed for verification. |
| **OTP no-synchronization window** | Specify the window size in which the OTP seeds are not synchronized. |
| **OTP token reset window** | Enter the number of OTPs to check when resetting OTP tokens. |
| **IP-application name bindings** | Use to search the application name from the IP of the caller. Each entry uses the format `IP:authentication service`. Enter an IP-application name, and then click **Add**.<br><br>To remove an IP-application name, click the **Remove** button next to the corresponding IP-application name. |
| **NASID-application name bindings** | Use to search the application name from the Network Access Server or NAS ID of the caller.<br><br>Each entry uses the format `IP:authentication service`.<br><br>Enter an NASID-application name, and click **Add**.<br><br>To remove an NASID-application name, click the **Remove** button next to the corresponding NASID-application name. |

| Option | Description |
| --- | --- |
| **Application binding for MAC/OTP accounts** | Specify the application binding properties. An application binding maps an application username to an enterprise ID.<br><br>The values are:<br>• **explicit**: the logon ID cannot be the same as enterprise ID and users can use MAC<br>• **implicit**: the logon ID is the enterprise ID |
| **Use MAC-only registration of users** | Specify whether non-AccessAgent, MAC-only user-registration is supported. |
| **Allow Mobile ActiveCodes to be application-specific** | Specify whether MACs are application-specific or are valid across applications. |
| **The ActiveDirectory attribute to be displayed for MAC-only registration of users** | Enter an Active Directory attribute, which is shown when searching for users in the User registration page. |
| **Send out Mobile ActiveCodes in uppercase** | Specify whether MACs are sent out in uppercase or lowercase.<br><br>The values are:<br>• **True** - MACs are sent out in uppercase<br>• **False** - MACs are sent out in lowercase |
| **Search filter used for MAC-only registration of users UI** | Specify the comma-separated search filter, which is used for searching users on the User registration page.<br><br>Specify Name Value pairs in a comma-separated list, such as:<br><br>`sAMAccountName=*,objectClass=user`. |
| **Default messaging connector** | Specify the default messaging connector. |
| **Authentication mechanisms for Stage 1** | Specify the acceptable user inputs for stage 1 (authentication request) of a RADIUS Challenge-Response.<br><br>It is an ordered list of one or more of the following values:<br>• **ENC_PWD_OR_APP_PWD**: password or application password<br>• **MAC**: Mobile ActiveCode<br>• **AA_OTP**: OTP generated by AccessAgent<br>• **BYPASS**: ActiveCode bypass (for example, authorization code + password)<br>• **OATH**: OTP generated by an OATH token |

| Option | Description |
| --- | --- |
| **Authentication mechanisms for Stage 2** | Specify the acceptable user inputs for stage 2 (response to challenge) of a RADIUS Challenge-Response.<br><br>If the user is already authenticated by using MAC or OTP in stage 1, the stage 2 authentication is skipped.<br><br>It is an ordered list of one or more of the values in **Authentication mechanisms for Stage 1**. |
| **Enterprise Directory attributes to be matched before MAC/OTP request/verification** | Specify the Enterprise Directory attribute to check for MAC/OTP request/verification. This attribute indicates whether the user can use MAC/OTP. If there is no such attribute, leave this setting empty.<br><br>Limitations:<br>• Only one attribute can be specified.<br>• If set to **true**, performance is degraded, as each OTP/MAC request or verification calls the Enterprise Directory.<br>• To support fetching of multi-valued attributes (for example, **memberOf**), use the ADSI connector to configure the Enterprise Directory |
| **Values of the Enterprise Directory attribute to be matched before MAC/OTP request/verification** | Specify the list of values for the Enterprise Directory attribute. If the Enterprise Directory attribute of the user matches any of the values in this list, the user can use MAC/OTP.<br><br>Both single and multi-valued attributes are supported. For multi-valued attributes such as **memberOf**), the user can use MAC/OTP. However, one of the values must match any of the values in the list.<br><br>For the **memberOf** attribute, the values are the Distinguished Names (DN).<br><br>For example: `cn=Domain Users`, `dc=IBM`, and `dc=com`. |
| **ActiveCode-enabled authentication services** | Specify the list of values for the ActiveCode-enabled authenticated services from the list. |

4. Click **Update**.

   See the **Character set**, **ActiveCode length** and **algorithm binding** parameters, which are set during deployment and cannot be modified. You can view only the parameters in the IMS Configuration Utility.

   ```
   YZ23456789ABCDEFGHJKLMNPQRSTUVWX,6,AES
   WXYZ23456789ABCDEFGHJKLMNPQRSTUV,8,AES
   1234567890,8,AES
   JKLMNPQRSTUVWXYZ23456789ABCDEFGH,6,MCA
   ```

XYZ23456789ABCDEFGHJKLMNPQRSTUVW,6,TRIPLEDES

VWXYZ23456789ABCDEFGHJKLMNPQRSTU,8,TRIPLEDES

The parameter used for MAC is JKLMNPQRSTUVWXYZ23456789ABCDEFGH,6,MCA.

# Advanced settings

You can configure advanced settings in the IMS Configuration Utility. The advanced settings are for the AccessAdmin, IMS Server, data source, message connectors, IMS Bridges, and user authentication.

See the following topics for more information.


- "Setting AccessAdmin"
- "Setting the IMS Server" on page 21
- "Setting the data source" on page 25
- "Setting message connectors" on page 28
- "Setting the IMS bridge" on page 32
- "Configuring user authentication" on page 34


## Setting AccessAdmin

AccessAdmin is a web-based management console that Administrators and Help desk officers use to manage users and policies on an IMS Server. You can edit the AccessAdmin user interface, help files URL, session, user attributes, computer attributes, and feedback email.

### Configuring the AccessAdmin user interface

Use the IMS Configuration Utility to edit the information displayed in the AccessAdmin interface.

#### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **AccessAdmin** > **User interface**.
3. Complete the following fields:

| Option | Description |
|---|---|
| **IBM Security Access Manager for Enterprise Single Sign-On default locale** | Select the preferred locale from the **Language** list.<br>**Note:**<br>1. The IMS Server uses the selected locale during the following scenarios:<br>• A new HTTP session is established.<br>• There is no cookie that stores the selected locale.<br>• The default locale setting of the browser is not supported in the list of available IBM Security Access Manager for Enterprise Single Sign-On locales.<br>2. AccessAgent (versions older than 8.1) also uses this locale.<br>However, AccessAgent can read only text policies in one locale. The locale must be set before you modify the configurable text policy or authentication service. |

| Option | Description |
| --- | --- |
| **Key type attribute** | Enter the attribute that provides information about the type of key being used.<br><br>The entry must match an SID attribute in the **IMSAttributeName** table in the database. For example:`tokenType`. |
| **User service log display period, in days** | Enter the number of days that the user service logs are displayed. The default value is `10` days. |
| **User service log display events** | Enter which user service events to display in the IMS Server user interface. |
| **User activity log display period, in days** | Enter the number of days that the user logs are displayed. The default value is `10` days. |
| **User activity log display events** | Specify which user events to display in the IMS Server user interface.<br><br>The event codes are in hexadecimal and correspond to the codes declared in **IBM.ims.common.EventCode**. |
| **User admin log display events** | Enter which Help desk events to display in the IMS Server user interface.<br><br>The event codes are in hexadecimal and correspond to the codes declared in **IBM.ims.common.EventCode**. |
| **User admin log display period, in days** | Enter the number of days Help desk logs are displayed. The default is `10` days. |
| **User admin log searchable events** | Enter which events are searchable on the IMS Server user interface.<br><br>The value is a comma-separated list of the event codes in Hexadecimal format. |
| **User admin log favorite searches file location** | Specify the location of the file that contains the user admin log favorite searches. |
| **Number of results per page shown for user admin log** | Enter the number of log entries to show per page for the User Admin Log page. |
| **Amount of system log information kept in memory, in KB** | Enter the amount (in KB) of system logs to keep in memory.<br><br>These logs are displayed on the status page of AccessAdmin. |
| **Policy assignment attribute** | Enter the attribute based on whose value the policy templates are applied to users during registration. |
| **Enable delete user button** | Specify whether the delete user option is available on AccessAdmin. Select a value from the drop-down list.<br>• **true** - enables the delete user button<br>• **false** - does not enable the delete user button |

| Option | Description |
| --- | --- |
| **Authorization code expiration** | Shows the different expiry times possible for authorization code expiry on AccessAdmin.<br><br>Each value is made from a number and a letter. The letter can be from the set {h, d, w, m} corresponding to {hour, day, week, month}.<br><br>The number represents how many hours/days/weeks/months (For example: 1d is one day, 2w is two weeks).<br><br>Enter an expiry time and then click **Add**.<br><br>To remove an expiry time, click the **Remove** button next to the expiry time. |
| **Length of the authorization code, in characters** | Enter the character length of the authorization code. Enter a number between 1 and 32 (inclusive). |
| **Validity of the authorization code, in days** | Specify the validity period of an authorization code. The validity period is specified in number of days. |
| **Non-searchable attribute display types** | Specify display types that are not searchable on AccessAdmin.<br><br>Enter a display type and then click **Add**.<br><br>To remove a display type, click the **Remove** button next to the display type. |
| **Number of entries per page** | Enter the number of entries to display on an AccessAdmin page. |
| **Choice for number of users to be displayed per page** | Select the number of users to be displayed per page from the drop-down list. |
| **Non-certificate authentication access types** | Enter the access types for non-certificate authentication.<br><br>Enter an access type and then click **Add**.<br><br>To remove an access type, click the **Remove** button next to the access type. |
| **Attributes used on the user interface** | Enter the attributes that AccessAdmin uses with display names and display types.<br><br>Enter an attribute and then click **Add**.<br><br>To remove an attribute, click the **Remove** button. |
| **Searchable LDAP attributes** | Enter the LDAP attributes that supports the IMS Server queries.<br><br>The format is **[LDAP Attribute]:[Display Name]:[Display Order]**. Enter an attribute, and then click **Add**.<br><br>To remove an attribute, click the **Remove** button. |

| Option | Description |
|---|---|
| **Policy display configuration file location** | Enter the name of the file that determines the policies and in what order to display them on the AccessAdmin UI. |
| **Custom user interface policies** | List the policies with custom user interfaces.<br><br>The value is in the format of a comma-separated policy ID and class name. For example: `pid_bind, IBM.ims.ui.component.Binder`.<br><br>Enter a policy and click **Add**.<br><br>To remove a policy, click the **Remove** button next to the policy. |
| **Custom user interface attributes** | Enter the attributes with custom user interfaces.<br><br>The value is in the format of a comma-separated attribute name and class name. For example, `gsmNumber, IBM.ims.ui.component.GsmNumber`.<br><br>Enter an attribute and click **Add**.<br><br>To remove an attribute, click the **Remove** button next to the attribute. |

4. The following parameters are set during deployment and cannot be modified. You can view only the parameters in the IMS Configuration Utility.

| Option | Description |
|---|---|
| **Default LDAP connector to be used for lookup** | Use this connector for attributes based on user interface searches. |

5. Click **Update**.

## Changing the help files URL

Use the IMS Configuration Utility to change the help file link inAccessAdmin.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **AccessAdmin** > **Help files URL**.
3. Complete the following field:

| Option | Description |
|---|---|
| **AccessAdmin help files URL** | The default URL is *http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itamesso.doc/ic-homepage.html*. |

4. Click **Update**.

## Enabling form-based logon

Use the IMS Configuration Utility if you want to enable form-based logon to AccessAdmin.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **AccessAdmin** > **Login**.
3. Complete the following field:

| Option | Description |
|---|---|
| **Allow form-based login to AccessAdmin from remote machine** | This option sets whether to use form-based logon to AccessAdmin from a remote computer where the IMS Server is installed.<br><br>If set to **false**, user can log on only from an AccessAgent session. |

4. Click **Update**.

## Configuring AccessAdmin session settings

Use the IMS Configuration Utility so that you can manage the session settings for AccessAdmin. The session settings include whether to check the client IP address, session inactivity, and forced session timeout.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **AccessAdmin** > **Session**.
3. Complete the following fields:

| Option | Description |
|---|---|
| **Check client IP address** | Specify whether to check the IP address of the client during session validation.<br><br>This option restricts a session to the created IP address.<br><br>Select a value. The default value is **false**.<br>• **true** - checks the IP address of the client<br>• **false** - does not check the IP address of the client |
| **Check session inactivity** | Specify whether sessions are timed out because of inactivity.<br><br>Select a value. The default value is **true**.<br>• **true** - session times out after a period of inactivity.<br>• **false** - session does not time out. |
| **Session inactivity timeout, in minutes** | Enter the inactivity timeout in minutes.<br><br>The default value is 15 minutes. |
| **Check forced session timeout** | Specify whether to force the client to log on again after a fixed time.<br><br>Select a value. The default value is **false**.<br>• **true** - client is forced to log on after a period of inactivity<br>• **false** - session does not time out. |

| Option | Description |
| --- | --- |
| **Forced session timeout, in minutes** | Enter the forced timeout in minutes.<br><br>The default value is one day (1440 minutes). |

4. Click **Update**.

## Specifying attributes for IMS user roles

Use the IMS Configuration Utility to specify the attributes that are used during role assignment. For example, you can specify the enterprise directory ID to be assigned the Administrator role.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **AccessAdmin** > **User attributes**.
3. Complete the following fields:

| Option | Description |
| --- | --- |
| **Initial IMS Admin ISAM ESSO user names** | Enter the enterprise IDs to be automatically promoted to the Administrator role when they are registered.<br><br>Enter an enterprise ID and then click **Add**.<br><br>To remove an enterprise ID, click the **Remove** button next to the enterprise ID. |
| **Role assignment attribute name** | Enter the name of an Active Directory attribute used as a criterion for the IMS Server role assignment. |
| **Role assignment attribute value** | Specify the key of role assignment mapping (an AD attribute value). Multiple values are separated by a semicolon (;). |
| **Desired IMS role** | Specify the value of role assignment mapping (a valid IMS Server role). |
| **Automatically assign all policy templates and users to new Help desk user"** | Specify whether to automatically assign all existing users and policy templates to any newly created Help desk user. |

4. The following parameters are set during deployment and cannot be modified. You can view only the parameters in the IMS Configuration Utility.

| Option | Description |
| --- | --- |
| **Default IMS user role** | Upon registration, the role of the user is set to **1** (unbound user).<br><br>There must be a matching entry in the `IMSRole` table of the database under `roleID`. |
| **Bound IMS user role** | After a successful registration of the user, the role of the user is set to **2** (user).<br><br>Multiple entries can be specified for multiple roles.<br><br>There must be a matching entry in the `IMSRole` table of the database under `roleID`. |

| Option | Description |
|---|---|
| **Revoked IMS user role** | Specify the role of the user after revocation. |
| **Enterprise binding attribute** | Specify the enterprise bind attribute to create on successful binding.<br><br>This option must match one of the **attrName** fields in **IMSAttributeName** table. |
| **Software key allowed** | Specify whether software keys can be used. |

5. Click **Update**.

## Specifying machine attributes

You can assign machine policy templates to different groups of computers based on the LDAP attribute of the computer object in the enterprise directory. Use the IMS Configuration Utility to set the machine attribute and LDAP filter.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **AccessAdmin** > **Machine attributes**.
3. Complete the following fields:

| Option | Description |
|---|---|
| **Machine attributes to be fetched from Active Directory** | Enter the computer attribute and click **Add**. To remove the attribute, click **Remove**. |
| **LDAP search filter for searching machine attributes** | Enter the LDAP filter used as criterion for searching computer attributes. |

4. Click **Update**.

## Setting feedback email settings

Use the IMS Configuration Utility so that you can specify the details of the SMTP server and the email address where users can send email to.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **AccessAdmin** > **Feedback email**.
3. Complete the following fields:

| Option | Description |
|---|---|
| **SMTP server URL** | Enter the URL of the SMTP server to use to send emails. |
| **SMTP server user name** | Enter the user name to authenticate to the SMTP mail server.<br><br>This option must be a valid user name on the SMTP mail server. |
| **SMTP server password** | Enter the corresponding password for the user name authenticating to the mail server. |
| **Feedback e-mail address** | Specify the email address to receive feedback from readers |

| Option | Description |
| --- | --- |
| **IMS e-mail address** | Specify the email address to display in the **from** field for emails sent from the IMS Server. |

4. Click **Update**.

# Setting the IMS Server

You can edit the settings for the IMS Server logging, event handling, CRL republication, and authorization code generation settings.

## Enabling log-signing

If you want to enable log-signing in the IMS Server, you can add specific types of logs that you want to view like user activity and system activity. Use the IMS Configuration Utility to enable log-signing in the IMS Server.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **IMS Server** > **Logging** > **Log-signing**.
3. In the **Enable log signing** field, select a table from the drop-down list. The field contains a list of tables for which the logs are hashed and signed. The available tables are:
   - logSystemManagementActivity
   - logUserAdminActivity
   - logUserService
   - logUserActivity

   To remove a table from the list, click the **Remove** button next to the table name.
4. Click **Add**.
5. Click **Update**.

## Configuring syslog settings

Use the IMS Configuration Utility to configure IBM Security Access Manager for Enterprise Single Sign-On to forward its audit log records to any external SysLog server. For example, Microsoft Operations Manager. Enable syslog and define its parameters.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **IMS Server** > **Logging** > **Syslog**.
3. Complete the following fields:

| Option | Description |
| --- | --- |
| **Enable syslog** | Specify the list of tables where the logs are stored in the syslog server.<br><br>The available tables are:<br>• logSystemManagementActivity<br>• logSystemOps<br>• logUserAdminActivity<br>• logUserService<br>• logUserActivity<br><br>Select a table and then click **Add**.<br><br>To remove a table from the list, click the **Remove** button next to the table name. |
| **Syslog server port** | Enter the port number at which the syslog daemon is listening. |
| **Syslog server hostname** | Enter the hostname of the syslog server. |
| **Syslog logging facility** | Enter the integer value of the facility used for logging to the syslog server. |
| **Syslog field-separator** | Enter the field separator character used for separating name and value pairs in a log entry. For example, "\n" (Line feed). |

4. Click **Update**.

## Configuring the log server information

Use the IMS Configuration Utility to specify the type of log server used by the IMS Server. The log server types are **rdb** and **syslog**.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **IMS Server** > **Logging** > **Log server information**.
3. Complete the following field:

| Option | Description |
| --- | --- |
| **Log server types** | Specify the type of log server used as the IMS Server log data store. |

4. Click **Add**.
5. Click **Update**.

## Configuring the certificate and keystore settings

Use the IMS Configuration Utility to edit the IMS Server certificate and keystore settings. You can edit settings such as validity period, RSA keypair in size, and alias for IMS soft CA.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **IMS Server** > **IMS Crypto System** > **Certificate/keystore**.
3. Complete the following fields:

| Option | Description |
|---|---|
| **Certificate validity period, in months** | Enter the number of months that the issued certificates are valid. |
| **RSA keypair size in bits** | Enter the size of the RSA keypairs used in the IMS Server.<br><br>The keypairs are used for IMS Server CA and user certificates. |
| **Alias for IMS Soft CA in the keystore** | Enter the alias specified in the IMS Server keystore for the IMS Server CA. |

4. Click **Update**.

## Viewing the symmetric crypto

Use the IMS Configuration Utility to view the transformation string for symmetric crypto.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **IMS Server** > **IMS Crypto System** > **Symmetric Crypto**.
3. View the information in the following field:

| Option | Description |
|---|---|
| **The transformation string for symmetric crypto** | Displays the transformation encryption key. |

## Configuring the events system settings

Use the IMS Configuration Utility to configure the event handling settings such as whether to handle events immediately or not and how often the IMS Server checks for events.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **IMS Server** > **Events system**.
3. Complete the following fields:

| Option | Description |
|---|---|
| **Handle events immediately** | Specify whether the event system handles events immediately.<br><br>If this option is set to **True**, then the sleep interval is ignored. |
| **Events handler sleep interval** | Specify how often the Event Controller checks for events.<br><br>This option is used only if `IBM.events.HandleImmediately` is set to **false**. |

4. The following parameters are set during deployment and cannot be modified. You can view only the parameters in the IMS Configuration Utility.

| Option | Description |
| --- | --- |
| **Events system configuration file location** | Displays the location of the file that contains Events systems configuration. |

5. Click **Update**.

## Viewing the IMS Server startup settings

Use the IMS Configuration Utility to view the IMS Server startup settings. These settings cannot be modified.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **IMS Server** > **Startup**.
3. View the information in the following fields:

| Option | Description |
| --- | --- |
| **IMS Server startup health check tasks** | A list of health checking tasks that runs when IMS Server starts. |
| **IMS Server startup file location** | The file needed by the IMS Server to start. |

## Configuring miscellaneous settings of the IMS Server

Use the IMS Configuration Utility to configure the miscellaneous settings of the IMS Server such as application binding tasks, download service timeout, and maximum thread size in download service.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **IMS Server** > **Miscellanous**.
3. Complete the following fields:

| Option | Description |
| --- | --- |
| **Application binding tasks** | Enter the class names of the tasks performed when application binding occurs. |
| **Machine attributes to exclude from the IMS Server** | Machine attributes which are not updated or saved by the IMS Server.<br><br>For more information, see Appendix D, “Excluding machine attributes,” on page 97. |
| **Download service timeout, in seconds** | The maximum time in seconds before a connection times out. |
| **Maximum thread size in download service** | The maximum number of threads in the download service. |

4. Click **Update**.

## Specifying the IMS Server and LDAP attribute names

Use the IMS Configuration Utility to specify the IMS Server and LDAP attribute names.

### Procedure

1. Log on to the IMS Configuration Utility.

2. Navigate to **Advanced Settings** > **IMS Server** > **IMS and LDAP user association**.
3. Complete the following field:

| Option | Description |
|---|---|
| **Matchers classes** | Enter the qualified class names of the matchers in the order that they associated to an IMS Server user and an LDAP user. |
| **LDAP attribute name** | Enter the name of the LDAP attribute that associates an IMS Server and an LDAP user. For example, `sAMAccountName`. |
| **IMS attribute name** | Enter the name of the IMS Server attribute that associates an IMS Server user and an LDAP user. For example, `Enterprise Logon`. |

4. Click **Update**.

### Specifying self-service authentication code generation settings

Use the IMS Configuration Utility to set your preferences for the IMS Server user attributes. The IMS user attributes include phone number, secret for self-service, and IMS connector for SMS gateway.

#### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **IMS Server** > **Self-service authentication code generation**.
3. Complete the following fields:

| Option | Description |
|---|---|
| **Self-service request handler** | Enter the qualified class name that implements the **`AuthCodeRequestHandler`** interface.<br><br>This handler must be specified if the self-service feature is enabled. |
| **IMS user attribute - phone number** | Enter the name of the IMS Server user attribute that stores the phone numbers of the users (for example, **`gsmNumber`**). |
| **IMS user attribute - secret for self-service** | Enter the name of the IMS Server user attribute that is used as a secret for authorization code requests. |
| **IMS connector for SMS gateway** | Enter the name of one IMS Server connector that communicates with an SMS gateway.<br><br>This configuration is required if IMS Server delivers authorization codes through SMS. |

4. Click **Update**.

## Setting the data source

The IMS Server stores all user and system data in a relational database. Configure the data source settings to allow the IMS Server to communicate to your database server.

## Specifying the general data source settings

You can specify the settings for the data source. Use the IMS Configuration Utility to set the general data source settings such as database type, datastore IDs, data object types, and maximum records returned by the database.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **Data Source** > **General Data Source**.
3. Complete the following fields:

| Option | Description |
|---|---|
| **Database type** | Specify the type of database (for example, DB2, MS SQL Server, Oracle). |
| **Datastore IDs** | Each value of **ds.do_type** must have a corresponding value. It defines the data source parameters used for the associated **ds.do_type**.<br><br>The associated group of parameters have the ID in its name. For example `ds.ims.rdb.*`. If any **ds.do_type** share the same data source ID, the two groups of DOs share the same connection pool. |
| **Data object types** | Specify the qualified class name of a class that contains the types of a logical group of DOs. There can be multiple values for this tag.<br><br>Each value identifies a logical group of DO, each of which can use a different connection pool (such as different data source). |
| **Max records returned by database** | Specify the maximum number of results to be shown on the IMS Server user interface when a search is performed. The default value is `25`. |

4. View the following fields:

| Option | Description |
|---|---|
| **Default data object type** | Displays the default **ds.do_type** if :<br>• no value is specified during a request for a connection<br>• data source parameters for other ds.do_types are not found<br><br>**Note:** *ds* stands for data store and *do* is a data object. |
| **Path to data source configuration file for IMS Server** | Displays the configuration file path for IMS. |
| **Path to data source configuration file for IMS Configuration Utility** | Displays the configuration file path for IMS Configuration Utility. |

5. Click **Update**.

## Specifying the IMS data source settings

Use the IMS Configuration Utility to specify the IMS database settings such as URI, schema, name, username, and password.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **Data Source** > **IMS data source**.
3. Complete the following fields:

| Option | Description |
|---|---|
| **IMS database URI** | Specify the Uniform Resource Identifier (URI) of the RDB server. |
| **IMS database schema** | Specify the schema of the database tables for **do_type**. |
| **IMS database name** | Enter the name of the IMS Server database. |
| **IMS database user name** | Enter the user name used to log on to the database. |
| **IMS database password** | Enter the corresponding password for the user name used to log on to the database. When run for the first time, it is replaced by a fixed string with the encrypted value written in the ciphertext section. |

4. View the following field:

| Option | Description |
|---|---|
| **IMS Server JDBC driver** | Displays the JDBC driver being used. |

5. Click **Update**.

## Specifying the IMS Server log data source settings

Use the IMS Configuration Utility to specify the IMS Server log database settings such as URI, schema, name, user name, and password.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **Data Source** > **Log data source**.
3. Complete the following fields:

| Option | Description |
|---|---|
| **IMS log database URI** | Specify the Uniform Resource Identifier (URI) of the RDB server. |
| **IMS log database schema** | Specify the schema of the database tables for **do_type**. |
| **IMS log database name** | Enter the name of the IMS Server log database. |
| **IMS log database user name** | Enter the user name used to log on to the log database. |
| **IMS log database password** | Enter the corresponding password for the user name used to log on to the database. |

| Option | Description |
|---|---|
| **Maximum log connection-pool wait in milliseconds** | Enter the waiting time (in milliseconds) for an **ims_log** connection before declaring that no connections are available. |
| **Maximum log connection-pool size** | Enter the maximum size of the log connection pool. |

4. View the following field:

| Option | Description |
|---|---|
| **IMS Server log JDBC driver** | The fully-qualified classname of the JDBC driver. |

5. Click **Update**.

# Setting message connectors

The IMS Server uses different messaging connectors –- SMPP, SMTP, and Web-based SMS connectors. The IMS Server uses these messaging connectors to send out the one-time password or ActiveCode to the user. Select which message connector to use and configure its basic and advanced settings.

## Configuring the SMPP messaging connector settings

Use the IMS Configuration Utility to edit the basic and advanced settings for SMPP messaging connector. The basic settings include the message connector name, address attribute name, SMPP server IP address, SMPP port number, sender address, SMPP system ID, and SMPP system password. The advanced settings include the enterprise directory address attribute details.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **Message connectors**.
3. In **Add configuration group**, select **SMPP Messaging Connector** from the drop-down list.
4. Click **Configure**.
5. Under **Basic configuration keys**, complete the following fields:

| Option | Description |
|---|---|
| **Message Connector Name** | Enter the display name of the Web-based SMS connector. |
| **Address Attribute Name** | Enter a name for the address attribute. This attribute is used as the target address for sending messages. For example, for an SMS message connector, the attribute is `gsmNumber`, which specifies the phone number of the user. |
| **SMPP server IP address** | Enter the IP address of the SMPP server. **Note:** IBM Security Access Manager for Enterprise Single Sign-On 8.2 supports Internet Protocol version 6 (IPv6). |
| **SMPP port number** | Specify the TCP/IP port on the SMPP server connecting to the gateway. |

| Option | Description |
|---|---|
| **Sender address** | Specify the default sender address to apply to outbound messages. |
| **SMPP system ID** | Specify the user name for the gateway to use when connecting to the SMPP server. |
| **SMPP system password** | Specify the password for the gateway to use when connecting to the SMPP server. |
| **Keep-alive timeout, in milliseconds** | Specify how long a network connection waits for a new request before closing. |
| **Bind timeout, in milliseconds** | Specify the maximum number of seconds that a client spends attempting to bind to the domain. |

6. Under **Advanced configuration keys**, complete the following fields:

| Option | Description |
|---|---|
| **Fetch the address attribute from Enterprise Directory** | Specify whether the address attribute used by this messaging connector is fetched from the Enterprise Directory.<br>• If set to **false**, the address attribute (specified by Address Attribute Name) is fetched from the IMS Server database.<br>• If set to **true**, performance degraded as each MAC issuance calls the Enterprise Directory.<br>To support fetching of multi-valued attributes (for example, **memberOf**), use the ADSI connector to configure the Enterprise Directory. |
| **Enterprise directory address attribute** | Specify the name of the attribute to look up from the Enterprise Directory (AD or LDAP server).<br>Set this field only if **Fetch the address attribute from Enterprise Directory** is set to **True**.<br>If this attribute specifies a phone number, it is in the format "CountryCode-AreaCode-PhoneNumber". Use the format "CountryCode-AreaCode-PhoneNumber". For example: `1-650-4136800` and `65--64735110`. |

7. Click **Add**.

## Configuring the SMTP messaging connector settings

Use the IMS Configuration Utility to edit the basic and advanced SMTP messaging connector settings. The basic settings include the message connector name, address attribute name, SMTP server URI, SMTP from address, and SMTP from friendly name. The advanced settings include the SMTP port number, SMTP user name, SMTP password, and enterprise directory address attribute.

## Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **Message connectors**.
3. In **Add Configuration Group**, select **SMTP Messaging Connector** from the drop-down list.
4. Click **Configure**.
5. Under **Basic configuration keys**, complete the following fields:

| Option | Description |
|---|---|
| **Message connector name** | Enter the display name of the Web-based SMS connector. |
| **Address attribute name** | Enter a name to describe the address attribute. |
| **SMTP server URI** | Enter the URI of the SMTP Server (for example, `mail.mycompany.com`). |
| **SMTP from address** | Enter the address from which electronic mails are sent. |
| **SMTP from friendly name** | Enter a friendly name used in place of the email address. |

6. Under **Advanced configuration keys**, complete the following fields:

| Option | Description |
|---|---|
| **SMTP port number** | Enter an SMTP server port number. |
| **SMTP user name** | Enter the user name which is used for SMTP authentication. |
| **SMTP user password** | Enter the password used for SMTP authentication. |
| **Fetch the address attribute from Enterprise Directory** | Specify whether the address attribute used by this messaging connector is fetched from the Enterprise Directory.<br>• If set to **false**, the address attribute (specified by Address Attribute Name) is fetched from the IMS Server database.<br>• If set to **true**, performance is degraded as each MAC issuance calls the Enterprise Directory.<br>To support fetching of multi-valued attributes (for example, **`memberOf`**), the ADSI connector is used for configuring the Enterprise Directory. |
| **Enterprise directory address attribute** | Specify the name of the attribute to look up from the Enterprise Directory (AD or LDAP server).<br>Set this attribute only if **Fetch the address attribute from Enterprise Directory** is set to **true**.<br>If this attribute specifies a phone number, it is in the format "CountryCode-AreaCode-PhoneNumber", for example, `1-650-4136800`, `65-64735110`. |

7. Click **Add**.

## Configuring the Web-based SMS connector settings

Use the IMS Configuration Utility to edit the basic and advanced Web-based SMS connector settings. The basic settings include the message connector name, address attribute name, GSM code to gateway mappings, default SMS gateway, phone number field name, message field name, and other field names. The advanced settings include enterprise directory address attribute, HTTP retry count, and HTTP timeout in milliseconds.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Select **Advanced Settings** > **Message Connectors**.
3. In **Add Configuration Group**, select **Web-based SMS Connector** from the drop-down list.
4. Click **Configure**.
5. Under **Basic configuration keys**, complete the following fields:

| Option | Description |
|---|---|
| **Message Connector Name** | Enter the display name of the Web-based SMS connector. |
| **Address Attribute Name** | Enter a name to describe the address attribute. |
| **GSM Code to gateway mappings** | Enter the mappings of GSM codes to the corresponding gateway IP address or host name (for example, `65,127.0.0.1`). |
| **Default SMS gateway** | Enter the SMS gateway IP address or host name used if the current GSM code does not match any of the GSM codes with the gateway mappings. |
| **Phone number field name** | Enter the name of the phone number field on the target Web-form that sends the SMS. |
| **Message field name** | Enter the name of the message field on the target Web-form that sends the SMS. |
| **Other field names** | Enter the comma-separated name-value mappings of other fields sent to the target Web-form. For example: `group,executive`. |

6. Under **Advanced configuration keys**, complete the following fields:

| Option | Description |
| --- | --- |
| **Fetch the address attribute from Enterprise Directory** | Specify whether the address attribute used by this messaging connector is fetched from the Enterprise Directory.<br>• If set to **False**, the address attribute (specified by Address Attribute Name) is fetched from the IMS Server database.<br>• If set to **True**, performance is degraded as each MAC issuance calls the Enterprise Directory.<br>To support fetching of multi-valued attributes (for example, **memberOf**), the ADSI connector is used for configuring the Enterprise Directory. |
| **Enterprise directory address attribute** | Specify the name of the attribute to looked up in the Enterprise Directory (AD or LDAP server).<br>Set this attribute only if **Fetch the address attribute from Enterprise Directory** is set to **true**.<br>If this attribute specifies a phone number, it is in the format "CountryCode-AreaCode-PhoneNumber", for example, `1-650-4136800`, `65-64735110`. |
| **HTTP retry count** | Specify the number of times to attempt an HTTP connection when the connection fails on the first try. |
| **HTTP timeout, in milliseconds** | Specify the amount of time, in milliseconds, to wait for a server response.<br>If you have a slow network connection, increase the value of this option. |

7. Click **Add**.

# Setting the IMS bridge

The IMS Server interfaces with other applications through message connectors and IMS Server provisioning bridges. Configure the IMS bridges settings to do user provisioning.

## Adding IMS Bridge user names

Use the IMS Configuration Utility to add IMS Bridge user names. An IMS Bridge is a module embedded in third-party applications and systems that call IMS APIs for provisioning purposes.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **IMS Bridges** > **Startup**.
3. Complete the following field:

| Option | Description |
| --- | --- |
| **IMS Bridge user names** | Enter the names for authenticating the IMS Bridge. |

4. Click **Add** to add the new IMS Bridge user name.
5. Click **Update**.

## Configuring the IMS Handler-IMS Bridge settings

Use the IMS Configuration Utility to configure your IMS Handler-IMS Bridge settings such as password, IP addresses, and types.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **IMS Bridges** > **ImsHandler - IMS Bridge**.
3. Complete the following fields:

| Option | Description |
| --- | --- |
| **IMS Bridge password** | Enter the password that authenticates the IMS Bridge. |
| **IMS Bridge IP addresses** | Enter the IP addresses from which the IMS Bridge can access the IMS Server.<br>**Note:** IBM Security Access Manager for Enterprise Single Sign-On 8.2 supports Internet Protocol version 6 (IPv6).<br><br>Click **Add** to add the new IMS Server IP address. |
| **IMS Bridge type** | Enter the role to be assigned to the IMS Bridge when it logs on. |

4. Click **Add** to add the new IMS Bridge IP address.
5. Click **Update**.

## Configuring the IMS Bridge settings

Use the IMS Configuration Utility to configure your IMS Bridge settings such as name, password, IP address, and type.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **IMS Bridges** > **Add Configuration Group**.
3. Select **IMS Bridge** from the drop-down list.
4. Click **Configure**.
5. Complete the following fields:

| Option | Description |
| --- | --- |
| **Name** | Enter the name that authenticates the IMS Bridge. |
| **IMS Bridge password** | Enter the password that authenticates the IMS Bridge. |

| Option | Description |
| --- | --- |
| **IMS Bridge IP addresses** | Enter the IP addresses from which the IMS Bridge can access the IMS Server.<br>**Note:** IBM Security Access Manager for Enterprise Single Sign-On 8.2 supports Internet Protocol version 6 (IPv6). |
| **IMS Bridge type** | Enter the role to be assigned to the IMS Bridge when it logs on. |

6. Click **Add**.

# Configuring user authentication

IBM Security Access Manager for Enterprise Single Sign-On manages user authentication. Configure the settings that affect how the user is authenticated, by password authentication, use of non-certificate authentication, authorization code, biometric support, RADIUS authentication, and others.

## Configuring logon settings

Use the IMS Configuration Utility to edit logon settings for user authentication. The logon settings include downloadable software keys, maximum online logon attempts, and backup software key characters sets.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **AccessAdmin** > **User authentication** > **Logon**.
3. Complete the following fields:

| Option | Description |
| --- | --- |
| **Downloadable software keys** | Specify whether to enable a system-wide policy so that users can create downloadable software keys. |
| **Allow non-certificate authentication by default** | Specify whether all users can access non-certificate based authentication by default.<br><br>If there is no user-based access control policy for non-certificate based authentication, this system-wide policy is enforced. If this key is not specified, users cannot access by default.<br><br>The IMS Server Administrator then grants permissions to each user. |
| **Max consecutive failed non-certificate online logon attempts** | Enter the maximum number of consecutive failures before the user is locked out. User cannot log on to the IMS Server with non-certificate based authentication. |
| **The number of days a Backup key activation request code is valid after generation** | Specify the number of days that an Activation Request Code is valid after generation. |

| Option | Description |
| --- | --- |
| **Backup software key character sets** | Add or remove the Character sets that can be supported by the IMS Server.<br><br>Specify one of the following values:<br>• Form character_set<br>• N2<br>• Character_set<br>• D2<br><br>Your choice depends on whether the deployment uses AccessAgent, which has different BSK Secrets on every computer. |

Example value: `Z3467ALEQHJKRWXY,CHARSET_D2`.

**Note:** All character sets are positionally unambiguous.

4. Click **Update**.

## Enabling password authentication

Use the IMS Configuration Utility to set your password authentication preference.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **AccessAdmin** > **User authentication** > **Password**.
3. Complete the following field:

| Option | Description |
| --- | --- |
| **Password authentication enabled** | Specify whether password authentication is enabled by the IMS Server. |

4. Click **Update**.

## Enabling biometrics and authorization codes

Use the IMS Configuration Utility to enable authorization codes and biometrics for user authentication.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **AccessAdmin** > **User authentication** > **Authorization code**.
3. Complete the following fields:

| Option | Description |
| --- | --- |
| **Authorization code enable** | Specify whether authorization code authentication is enabled by the IMS Server. |
| **Enable biometrics support** | Specify whether to enable or not enable biometrics support. |

4. The following parameters are set during deployment and cannot be modified. You can view the parameters only by using the IMS Configuration Utility.

| Option | Description |
| --- | --- |
| **IMS AccessAgent shared secret for biometrics implementation.** | This value is a secret shared between the IMS Server and AccessAgent.<br><br>This value is required for the biometrics implementation. |
| **Biometrics vendor ID to its implementation class binding** | This key specifies a set of bindings between the biometrics vendors supported by the IMS Server and the classes that implement the vendor-specific algorithms. |

5. Click **Update**.

## Configuring startup settings of the RADIUS server

Use the IMS Configuration Utility to specify the startup settings for the RADIUS or Remote Authentication Dial In User Service server. The settings include enable RADIUS module, RADIUS Server IP, UDP Port listening for authentication requests, clients of the RADIUS server, and authentication realms for unregistered users.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **AccessAdmin** > **User authentication** > **RADIUS server**.
3. Complete the following fields:

| Option | Description |
| --- | --- |
| **Enable RADIUS module** | Specify whether to enable the RADIUS module. |
| **RADIUS Server IP** | Enter the IP address of the RADIUS server. |
| **UDP port listening for authentication requests** | Specify the port that the server listens on for RADIUS Authentication requests.<br><br>The default value is 1812. |
| **UDP port listening for accounting requests** | Specify the port that the server listens on for RADIUS Accounting requests.<br><br>The default value is 1813. |
| **Maximum service queue for the Radius server** | Specify the maximum service queue before the system regards the RADIUS server as unavailable. |
| **Remove domain component from RADIUS user name** | Specify whether to remove the domain component from the user name. |
| **Set the Prompt attribute in RADIUS challenge response reply packets** | Specify whether to set the Prompt attribute in RADIUS challenge response reply packets.<br><br>Some VPNs, like Checkpoint, do not require RADIUS packets with the Prompt attribute set. Others, like Aventail, require it to be set. |

| Option | Description |
|---|---|
| **Allow multiple RADIUS Class attributes** | Specify the LDAP attribute of the user to be correctly sent as multiple RADIUS Class attributes.<br><br>However, for VPNs that can handle only a single RADIUS Class attribute, this feature must be not be enabled. |
| **Enable detailed RADIUS server debug logging** | Using this attribute might affect performance and privacy, so enable only when needed for troubleshooting/debugging purposes. |
| **Clients of this RADIUS server** | Specify the list of RADIUS clients. IP address/FQDNs are specified in the key `radius.client.$ friendlyName.address`.<br><br>Click **Add**. |
| **Authentication realms for unregistered users** | Specify the list of Realms against which non-IMS Server users are authenticated and click **Add**.<br><br>If the VPN user ID and the LDAP user ID match, an LDAP type realm can retrieve the following:<br>• **`memberOf`**<br>• Other user attributes for registered IMS Server users |

4. Click **Update**.

## Configuring the RADIUS Client settings

Use the IMS Configuration Utility to specify the RADIUS Client settings. The settings include name, client secret, vendor-specific attributes, default unregistered user realm of RADIUS and enabling RADIUS challenge-response.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **AccessAdmin** > **User authentication** > **RADIUS server** > **Add configuration group**.
3. Select **Radius Client** from the drop-down list.
4. Click **Configure**.
5. Complete the following fields:

| Option | Description |
|---|---|
| **Name** | Enter the name of the new client. |
| **Client secret** | Enter the shared secret that encrypts communication between the RADIUS client and server. |
| **Vendor-specific attributes** | Enter the RADIUS attributes returned on successful authentication.<br><br>Click **Add**. |
| **Resolvable address of the client** | Enter the IP address or FQDN of the host listed as RADIUS client. |

| Option | Description |
| --- | --- |
| **Default unregistered user realm of RADIUS** | Enter the name of the default unregistered user realm for this RADIUS server. |
| **Enable RADIUS challenge-response** | Specify whether to enable RADIUS Challenge-Response for this VPN server. |
| **Default Challenge message on VPN user interface** | Enter the RADIUS Challenge message that the user sees on the VPN user interface. |
| **GSM-SMS Channel Challenge message on the VPN user interface** | Enter the RADIUS challenge message that the user sees on the VPN user interface if the MAC is sent by using an SMS gateway. For example, Web-based SMS message connector.<br><br>This step is only required if MAC is enabled. |
| **E-mail Channel Challenge message on the VPN user interface** | Enter the RADIUS challenge message that the user sees on the VPN user interface if the MAC is sent by using an email gateway. For example, email message connector.<br><br>This step is only required if MAC is enabled. |
| **Retry challenge message on VPN user interface** | Enter the RADIUS Challenge message that the user sees on the VPN user interface. |
| **MAC SMS or e-mail subject** | Enter the template of the SMS or email message the user receives with the MAC in it. |
| **Initial challenge-response authentication factor** | Specify the authentication factor. |
| **MAC SMS or e-mail content** | Enter the template of the SMS or email message the user receives with the MAC in it. |
| **Allow non-IMS users** | Select **No**.<br><br>This option prevents unregistered users from authenticating with the use of this VPN Server. |
| **Re-prompt users for MAC after a failure** | Specify whether to prompt users to reenter a MAC if it is not entered correctly.<br><br>The user receives a prompt until the account is locked. |

6. Click **Add**.

## Configuring the RADIUS realm settings

Use the IMS Configuration Utility to specify the RADIUS realm settings. The settings include the name, authentication realm type, authentication server address, and authentication server port.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced Settings** > **AccessAdmin** > **User authentication** > **RADIUS server** > **Add configuration group**.
3. Select **Radius Realm** from the drop-down list.
4. Click **Configure**.

5. Complete the following fields:

| Option | Description |
|---|---|
| **Name** | Enter the name of the new RADIUS realm. |
| **Authentication realm type** | Specify the type of authentication realm. |
| **Authentication server address** | Enter the address of the principal authentication server of this realm. |
| **Authentication server port** | Specify the port on which the authentication server listens to for authentication requests. |
| **RADIUS class attribute type** | Specify the type of RADIUS Class attribute that the realm returns. |
| **RADIUS realm secret** | Enter the shared secret between IMS Server and RADIUS, and the given RADIUS realm. |
| **LDAP search base** | Enter the distinguished name of the LDAP objects used as the roots for any LDAP search. |
| **LDAP lookup user** | Enter the user with permissions to search and retrieve LDAP attributes. |
| **LDAP lookup user password** | Enter the password of the RADIUS-LDAP lookup user. |
| **LDAP login attributes** | Specify the LDAP logon attributes that are searched when the user logs on. |
| **RADIUS class attribute equivalent on LDAP** | Specify the LDAP attribute returned to the RADIUS client as the Class standard RADIUS attribute. |

6. Click **Add**.

# Utilities

You can configure the different utilities for uploading system data, exporting and importing IMS configuration, and translating event codes.

See the following topics for more information.

- "Uploading system data"
- "Exporting the IMS Server configuration with the IMS Configuration Utility" on page 40
- "Importing the IMS Server configuration with the IMS Configuration Utility" on page 41
- "Translating event and result codes" on page 43

## Uploading system data

Use the upload system data utility to upload either a template file or a data file in the IMS Server.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Select **Utilities** > **Upload System Data**.
3. Complete the following field:

| Option | Description |
| --- | --- |
| **Select file type to be uploaded** | Specify whether the file type to be uploaded is **Template file** or a **Data file**. |

4. Click **Upload**.

# Exporting the IMS Server configuration with the IMS Configuration Utility

Use the Export IMS Server Configuration tool in the IMS Configuration Utility to back up the IMS Server configuration. When you export the IMS Server configuration, the configuration is stored in a Java archive file. You can download and import this file later into the same or different computer.

## Before you begin

Ensure that the IMS Server is installed, configured, and that it works.

## About this task

The following changes are included during the exporting of the IMS Server configuration:

- IMS Server configuration files
- JDBC settings
- All IMS Server keys and certificates
- WebSphere Application Server root CA key
- IBM HTTP Server SSL certificate
- IMS Server SOAP service URL
- Virtual Member Manager enterprise directories configuration
- Enterprise directories

The following changes are excluded during the exporting of the IMS Server configuration:

- Information stored in the IMS Server database. For example: IBM Security Access Manager for Enterprise Single Sign-On policies and user wallets.
- Manual changes on the WebSphere Application Server profile. For example: heap size values and session management on the modules.

## Procedure

1. Log on to the IMS Configuration Utility.
2. Under **Utilities**, click **Export IMS Configuration**. The **Export IMS Server Configuration** wizard is displayed.
3. Click **Begin**.
4. Accept the specified default values in the form if you used the default values during the WebSphere Application Server Root CA configuration. Otherwise, replace the default values.

   **Keystore name**
   Specify the root keystore name. For example, *NodeDefaultRootStore*.

   **Keystore scope**
   Specify the scope of the keystore. For example, *(cell):exportCell01:(node):exportNode01*.

**Keystore password**
Specify the assigned keystore password. For example, *WebAS*.

**Root CA alias name**
Specify the certificate alias of the Root CA . For example, *root*.

5. Click **Next**.
6. Accept the specified default values in the form if you used the default values during the IBM HTTP Server SSL Certificate configuration. Otherwise, replace the default values.

   **Keystore name**
   Specify the SSL certificate keystore name. For example, *CMSKeyStore*.

   **Keystore scope**
   Specify the scope name of the SSL certificate keystore. For example, *(cell):exportCell01:(node):exportNode01:(server):webserver1*.

   **Keystore password**
   Specify the SSL certificate keystore password. For example, *WebAS*.

   **SSL Alias**
   Specify the assigned alias for the SSL certificate. For example, *default*.
7. Click **Next**. The ISAM ESSO IMS Server **Export Configuration Summary** is displayed.
8. Review the summary of IMS Server configuration to be exported.
9. Click **Export**. The IMS Server configuration is exported.
10. Click **Download**.
11. Select **Save File** to store the IMS Server configuration JAR file.
12. Click **OK**.

## Importing the IMS Server configuration with the IMS Configuration Utility

Use the Import IMS Server configuration tool in the IMS Configuration Utility to import existing IMS Server configurations. Locate the IMS Server configuration JAR file that you exported and import it in the target computer.

### Before you begin

Make sure that on your target computer:

- You have an installed IMS Server.
- You are not running the IMS Configuration wizard and you have not yet configured the IMS Server.
- You have successfully exported the IMS Server configuration into a JAR file.
- You copy the IMS Server configuration JAR file.
- You know the location of the IMS Server database.
- You know the location of the enterprise directory.

### About this task

Importing the IMS Server configuration involves importing the IMS Server configuration files, data source, Root CA, IBM HTTP Server SSL certificate, and the enterprise directory connection configuration.

During the initial importing, all configurations are imported by default. For subsequent importing, IMS Server configuration files are imported by default. The other configurations are optional. For WebSphere Application Server Network Deployments, you can add multiple IBM HTTP Servers.

**Important:** If you have multiple instances of the IMS Server, be sure to import the same IMS Server configuration on *all* the servers to avoid server synchronization issues. Users might fail to log on if an outdated IMS Server configuration continues to exist on some of the servers.

## Procedure

1. Log on to the IMS Configuration Utility.
2. Under **Utilities**, click **Import IMS Configuration**.
3. Click **Browse** to locate and select the exported IMS Server configuration file. Examples:
   - For Windows: `C:/imsConfig_<hostname>_<yy mm dd>_hh:mm.ss.jar`.
   - For Linux: `/home/<user>/Desktop`
4. Click **Begin**.
5. Select the configuration to import. By default, all options are selected. To exclude a configuration type, clear the corresponding check box.

   **IMS Configuration Files**
   Imports the IMS Server configuration files.

   **Data source**
   Imports the IMS Server database data source details.

   **Root CA**
   Imports the root CA keystore name, password, and certificate alias.

   **IBM HTTP Server SSL Certificate**
   Imports the SSL certificate keystore name, scope, and alias.

   **Enterprise directories**
   Imports the enterprise directory repository connection configuration.
6. Click **Next**.
7. Edit the client keystore and truststore details if there are changes.

   **Certificate Alias**
   Specify the alias for the client certificate. For example: *default*.

   **Keystore Path**
   Specify the location of the client keystore. For example: `<was_home>/profiles/AppSvr01/etc/key.p12.`

   **Keystore Type**
   Specify the client keystore type. For example: `PKCS12`.

   **Keystore Password**
   Specify the password for the client root keystore. For example: `WebAS`.

   **Truststore Path**
   Specify the location of the client truststore. For example: `<was_home>/profiles/AppSvr01/etc/trust.p12.`

   **Truststore Type**
   Specify the client truststore type. For example: `PKCS12`.

   **Truststore Password**
   Specify the password for the client truststore. For example: `WebAS`.

8. Click **Next**.
9. Edit the IBM HTTP Server SSL Certificate details if there are changes.

   **Keystore Name**
   Specify the SSL certificate keystore name. For example: *CMSKeyStore*.

   **Keystore scope**
   Specify the scope name of the SSL certificate keystore. For example: `(cell):exportCell01:(node):exportNode01:(server):webserver1`.

   **SSL Alias**
   Specify the assigned alias for the SSL certificate. For example: `default`.
10. Click **Add**. The changes are displayed in the keystore table.
11. Click **Next**. The SAM E-SSO IMS Server Import Configuration Summary is displayed.
12. Review the summary of the IMS Server configurations to be imported.
13. Click **Import**. The IMS Server configurations are imported successfully.

    Depending on the imported configurations, you are instructed to restart either the WebSphere Application Server, the IBM HTTP Server, or the IMS Server.
14. Follow the instructions in the resulting message. You might be prompted to import the certificate.

## Translating event and result codes

Use the code translation utility to retrieve the corresponding description of the event code.

### Procedure

1. Select **Utilities** > **Code Translation**.
2. Select the type of code to translate.
3. Enter the code in `0x00000000` format. For example, `0x43000002`.
4. Click **Translate**.

# Configuring HTTP compression

Enable IBM HTTP Server compression to reduce the size of the data to be transferred to AccessAgent.

### 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 **Servers** > **Server Types** > **Web servers**.
4. Click the <*web_server_name*>. For example, **webserver1**.
5. Under **Additional Properties**, click **Configuration File**.
6. Search the following line and remove the comment tag:

   ```
   LoadModule deflate_module modules/mod_deflate.so
   ```
7. Search the `<Location/>` section and add the following lines:

   ```
   SetOutputFilter DEFLATE
   SetEnvIfNoCase Request_URI\.(?:gif|jpe?g|png)$ no-gzip dont-vary
   SetInputFilter DEFLATE
   ```
8. Click **OK**.

9. Restart the webserver.

# Chapter 2. Backing up and recovering the IMS Server, WebSphere Application Server profiles, and database

Back up the IMS Server, the WebSphere Application Server profiles, and the IMS Server database *before* an upgrade. Backups ensure that you can recover data if a data loss occurs.

See the following topics on how to back up the:

- IMS Server
  - "Exporting the IMS Server configuration with the IMS Configuration Utility" on page 40
  - "Importing the IMS Server configuration with the IMS Configuration Utility" on page 41
- WebSphere Application Server profiles
  - "Backing up WebSphere Application Server profiles"
  - "Restoring the WebSphere Application Server profiles" on page 46
- Database
  - "Backing up the database in DB2" on page 46
  - "Restoring the database in DB2" on page 47

## Backing up WebSphere Application Server profiles

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 the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for more details.
- (Network deployment) Node agents.
- IBM HTTP Server.

### Procedure

1. Open the command prompt.
2. Browse to the `<was_home>\bin` directory. For example, you can type the following: `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\AppSrv01yymmdd.zip
   ```

**Network deployment**

```
manageprofiles.bat -backupProfile -profileName Dmgr01 -backupFile
c:\backup\Dmgr01yymmdd.zip
```

# 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 this case occurs, you can delete the profile with the **manageprofiles** command or move the folder to another location.

## Procedure

1. In a command prompt, browse to the `<was_home>\bin` directory. Type `cd <was_home>\bin`.

   For example, `cd c:\Program Files\IBM\WebSphere\AppServer\bin`.
2. Restore the profile. Type **manageprofiles -restoreProfile -backup** *<backup_file_location>*. For example:

   **manageprofiles -restoreProfile -backup** `c:\backup\AppSrv01yymmdd.zip` The **manageprofiles** command-line tool always restores to the same path the profile was backed up from.
3. Verify that the profile is restored. Browse to the `<was_home>\profiles` directory. For example, `<was_home>\profiles\AppSrv01`. If the profile is restored successfully, a folder for the restored profile is displayed.

## Results

The profile is restored successfully.

**Tip:** If you are performing this task as part of a server restoration procedure, do not start the profile. Determine if you must restore the database first.

# Backing up the database in DB2

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

## Before you begin

Stop the following servers:

- IMS Server WebSphere Application Server profile.
- 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. Select **File System** in **Media Type** and then click **Add**.
6. Specify the path to store the backup files and click **OK**.
7. Click **Next**.
8. In the **Choose your backup options** page, click **Next**.
9. In the **Specify performance options for the backup** page, click **Next.**
10. Select **Run now without saving task history**.
11. Click **Next**.
12. Review the summary and click **Finish**.

### Results

The database is backed up successfully. Start the IBM HTTP Server, and the WebSphere Application Server.

If you are performing the database backup as part of a server upgrade process, see the upgrade procedures to determine if the procedures require the servers to be stopped before you continue with the upgrade procedures.

## Restoring the database in DB2

You can restore the database in DB2 to recover from a previous database backup.

### Before you begin

Ensure that the IBM HTTP Server is stopped.

### Procedure

1. Start the DB2 Control Center.
2. Right-click the database you want to restore.
3. Select the **Restore to an existing database**.
4. Click **Next**.
5. In **Available backup images**, select the backup you made.
6. Click the right arrow button and click **Next**.
7. In **Set non-automatic storage containers for redirected restore** page, click **Next**.
8. In **Choose your restore options** page, click **Next**.
9. In **Select performance options for the restore**, click **Next**.
10. Select **Run now without saving task history**.
11. Click **Next**.
12. Review the summary and click **Finish**. The database restore process begins.

### Results

The database is restored and starts successfully.

## 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.

For network deployments, be sure to start the node agents and then the cluster.

# Chapter 3. Configuring AccessAgent

After installing AccessAgent, you can configure its user interface, functionality, and accessibility features.

See the following topics for more information.

- "Configuring the AccessAgent user interface"
- "Configuring the AccessAgent functionality features" on page 53
- "Configuring the AccessAgent accessibility features" on page 59

## Configuring the AccessAgent user interface

You can configure the different user interface settings for the ESSO GINA. These settings include the AccessAgent banner, interface, and more.

See the following topics for more information.

- "Launching applications from ESSO GINA"
- "Changing the AccessAgent banner" on page 52
- "Changing the AccessAgent interface" on page 52
- "Disabling the ESSO GINA or ESSO Credential Provider" on page 52

### Launching applications from ESSO GINA

Configure ESSO GINA so that you can launch an application by clicking a link in the AccessAgent panel.

Use this feature to open:

- AccessAssistant with a web browser to perform self-service password reset.
- A vendor application to perform self-service password reset or registration.
- An application that is meant for public access without logging on to Windows.

To enable this feature, follow these steps:

1. Log on to AccessAdmin.
2. Under **Machine Policy Templates**, select **New Template** > **AccessAgent Policies** > **ESSO GINA Policies**.
3. Complete the following fields:

| Option | Description |
|---|---|
| Enable application launch from ESSO GINA | Set to 1 (Yes). |
| Display label for application launch | Set the text as label for the application launch link, which is shown in the panel of ESSO GINA.<br><br>For example, **Self-service password reset**. |
| Command line for application launch | Set the command line that launches the application.<br><br>For example, `C:\Program Files\Internet Explorer\iexplore.exe`. |

4. Click **Add**.

**Note:**

- If the application is launched from the Welcome screen, the owner of the process for the application is **System**.
- If the application is launched from a Locked screen, the owner of the process for the application is the **currently logged on desktop user**.
- If the application is launched from a Locked screen in Microsoft Windows Vista and later, the owner of the process for the application is also **System**.

Use the following command line to launch AccessAssistant or Web Workplace from the Microsoft Internet Explorer in kiosk mode: `"C:\Program Files\Internet Explorer\iexplore.exe" -k https://<IMS Server Name>/aawwp/app/reset_password_front_page.jsp`.

This method of launching applications has the following security issues:

- The user can access and modify files.

  For example, for Microsoft Internet Explorer, the user can right-click a graphic and select **Save Picture As**. A **File explorer** dialog box is displayed.
- The user can use features that are not intended for the user.

  For example, for Microsoft Internet Explorer, the user can press **Ctrl+O** to open any file or **Ctrl+N** to open a new browser window.

As a workaround for the security issues, create a Guest account with limited rights. The application is launched in the context of the Guest account. Use the Windows **runas** command to launch the application in the user context.

However, you must use a script to simulate keystrokes because **runas** requires the user to enter a password.

For example, a VBScript can launch the application. Consider that the VBScript is stored in the computer as `C:\launch_ie_as_guest.vbs`.

The script also sets the appropriate Microsoft Internet Explorer feature restrictions for the Guest account. The Machine policy **pid_engina_app_launch_cmd** is then set to `cscript C:\launch_ie_as_guest.vbs`.

**Tip:** See the *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide* for more details.

See the following `launch_ie_as_guest.vbs`.

```
On Error Resume Next

userName = "Guest"

userDomain = "EXAMPLE"

userPasswd = "password"

appRunasCmd = "C:\Program Files\Internet Explorer\iexplore.exe -k
https://<IMS Server Name>/aawwp/app/reset_password_front_page.jsp"

appCmd = """C:\Program Files\Internet Explorer\iexplore.exe"" -k
https://<IMS Server Name>/aawwp/app/reset_password_front_page.jsp"

Set WshShell = CreateObject("WScript.Shell")
```

```
Set WshNetwork = WScript.CreateObject("WScript.Network")

currUser = WshNetwork.UserName

If currUser = "SYSTEM" Then

' Launched from EnGINA welcome screen as System context

' Optional: Set Internet Explorer restrictions for System user

regKey = "HKEY_USERS\S-1-5-18\SOFTWARE\Policies\Microsoft\Internet Explorer
\Restrictions\"

WshShell.RegWrite regKey & "NoBrowserClose", 0, "REG_DWORD" 'Allow user to
close browser

WshShell.RegWrite regKey & "NoBrowserContextMenu", 1, "REG_DWORD" 'Disable
right-click menu

WshShell.RegWrite regKey & "NoFileOpen", 1, "REG_DWORD" 'Disable Ctrl-O to
open file

WshShell.RegWrite regKey & "NoOpenInNewWnd", 1, "REG_DWORD" 'Disable Ctrl-N
to open new
browser

' Launch application in System context as there is no user desktop

result = WshShell.Run(appCmd, 1, False)

Else

' Launched from EnGINA lock screen as user context

' Launch application using runas

Set WshEnv = WshShell.Environment("Process")

runasPath = WshEnv("SystemRoot")&"\System32\runas.exe"

result = WshShell.Run("runas /user:" & userDomain & "\" & userName & " " &
Chr(34) & appRunasCmd & Chr(34), 2, False)

WScript.Sleep 30 'Wait for cmd window to show up

WshShell.AppActivate(runasPath)

WshShell.SendKeys userPasswd & vbCrLf

' Optional: Set Internet Explorer restrictions

WScript.Sleep 1000 'Wait until user context loaded

Set wmiService = GetObject("winmgmts:{impersonationLevel=Impersonate}")

Set wmiUserAccount = wmiService.Get("Win32_UserAccount.Name='"& userName &"',
Domain='" & userDomain & "'")

userSid = wmiUserAccount.SID

regKey = "HKEY_USERS\" & userSid & "\SOFTWARE\Policies\Microsoft\Internet
Explorer\Restrictions\"

WshShell.RegWrite regKey & "NoBrowserClose", 0, "REG_DWORD" 'Allow user to
close browser

WshShell.RegWrite regKey & "NoBrowserContextMenu", 1, "REG_DWORD" 'Disable
```

```
right-click
menu

WshShell.RegWrite regKey & "NoFileOpen", 1, "REG_DWORD" 'Disable Ctrl-O to
open file

WshShell.RegWrite regKey & "NoOpenInNewWnd", 1, "REG_DWORD" 'Disable Ctrl-N
to open new browser

End If
```

## Changing the AccessAgent banner

You can customize the banner that is displayed on the AccessAgent user interface. The AccessAgent banner is displayed on the ISAM ESSO welcome screen on the logon, lock, and unlock windows.

### Before you begin

Make sure that your screen resolution is set at either 96 DPI or 120 DPI before you change the AccessAgent banner.

### Procedure

1. Prepare a bitmap file to use as an AccessAgent banner.
   - For 96 DPI screen resolutions, the bitmap must have a size of 432 x 64 pixels.
   - For 120 DPI screen resolutions, the bitmap must have a size of 576 x 80 pixels.
2. Name the file `logon_banner.bmp`.
3. Place the file in the `Config` folder of the installer.

   **Note:** If AccessAgent is already installed, place the file in the AccessAgent installation folder. For example: `C:\Program Files\IBM\ISAM ESSO\AA`.

## Changing the AccessAgent interface

You can personalize the appearance of the AccessAgent interface by changing the color schemes, font sizes, and high contrast scheme of Windows. This procedure is applicable to Windows XP.

### Procedure

1. Right-click on your desktop and select **Properties**.
2. Select the **Appearance** tab.
3. Select settings under **Windows and buttons**, **Color scheme** and **Font size**.
4. Click **OK**.

### Results

AccessAgent interface follows the newly created settings.

## Disabling the ESSO GINA or ESSO Credential Provider

You can deploy the AccessAgent without the ESSO GINA for Windows XP Professional or ESSO Credential Provider for Windows Vista or Windows 7.

### Procedure

1. Navigate to the **Config** folder of the AccessAgent installation package. For example, `C:\Downloads\ISAM ESSO\Config`.

2. Open the `SetupHlp.ini` file.
3. Set the values of the following parameters to `0`.
   - `EncentuateCredentialProviderEnabled`
   - `EnginaEnabled`
4. Set the value of `EncentuateNetworkProviderEnabled`.
   - Set the value to `1` if you want to automatically log on the user to AccessAgent by using the Windows credentials. This scenario is only applicable when the Active Directory password synchronization is enabled.
   - Set the value to `0` if you do not want to automatically log on the user to AccessAgent.
5. Close and save the file.
6. Install AccessAgent.

# Configuring the AccessAgent functionality features

You can configure the different functionality features of AccessAgent. The functionality features include event reporting, hot key enablement, and bidirectional language support.

See the following topics for more information.


- "Changing the Ctrl+Alt+Delete support in Windows 7"
- "Configuring the transparent screen lock settings"
- "Enabling single sign-on for Java applications" on page 55
- "Configuring AccessAgent to use EnWinNetUse" on page 56
- "Enabling the Observer Help" on page 57
- "Configuring event reporting in the Windows Event log" on page 58
- "Configuring the system modal message box" on page 58
- "Enabling emergency hot key for private desktops" on page 58


## Changing the Ctrl+Alt+Delete support in Windows 7

In Windows 7, **Interactive login: Do not require Ctrl+Alt+Del** is always enabled. You can configure AccessAgent to not enable the system setting.

### Procedure

1. On your Windows desktop, click **Start** > **Run**.
2. In the **Open** field, enter **`regedit`** then click **OK**.
3. Select `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`.
4. Right-click and select **DisableCAD**.
5. Modify the value to `0`.

## Configuring the transparent screen lock settings

With the transparent screen lock feature, users can lock their desktop screens but still see the contents of their desktop. You can enable or not enable the transparent screen lock and configure its settings and behavior in AccessAdmin.

## About this task

This feature applies only to shared desktop mode in Windows XP Professional and with RFID as the only authentication factor. The transparent screen lock feature is not supported in Microsoft Windows Vista and later versions, including Windows Server 2008.

When the user manually logs off from AccessAgent, the transparent screen lock is automatically not enabled and the desktop is unlocked.

**Tip:** For additional security, set the machine policy **Actions on manual logoff by user** to **Log off Wallet and lock computer**. See the *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide* for more details.

## Procedure

1. Log on to AccessAdmin.
2. Under **Machine Policy Templates**, select **New Template** > **AccessAgent Policies** > **Lock/Unlock Policies**.
3. Complete the following fields:

| Option | Description |
|---|---|
| Screen Lock Option | Set to **Transparent screen lock**. |
| Transparent screen lock message | Set the text to be shown at the window when Transparent screen lock is activated.<br><br>The default text is `Tap your RFID card or Ctrl+Alt+E to unlock.` |
| Enable transparent screen lock hot key | Select **Yes** to enable the **Ctrl+Esc** Hot Key as an alternative to the Hot Key during Transparent screen lock.<br><br>Use this additional Hot Key for remote access systems that can send only limited key sequences. For example, LANDesk. |

4. Scroll down the page and click **Hot Key Policies**.
5. Complete the following field:

| Option | Description |
|---|---|
| Enable ISAM ESSO hot key | Set to **Yes**. |

6. Click **Add**.

## Example

When the transparent screen lock is enabled, you can run a script to ensure that all applications are minimized except for one application.

The following code is an example of a VBScript that can run as a lock script (**pid_script_lock_enabled**). When the lock script is run, it minimizes all applications except the one with the title "Calculator".

```
appTitle = "Calculator"
Set objShell = CreateObject("Shell.Application")
objShell.MinimizeAll
Set WshShell = CreateObject("WScript.Shell")
```

```
WshShell.AppActivate(appTitle)
WScript.Sleep 100
WshShell.SendKeys "%( )"
Wshshell.Sendkeys "{ENTER}"
```

### What to do next

When transparent screen lock is enabled, the Windows key might not work. You must not enable the Windows key to enable transparent screen lock feature.

1. In your Active Directory computer, navigate to **Start** > **Administrative Tools**.
2. Right-click a group policy object.
3. Select **Edit**.
4. Navigate to **User Configuration** > **Windows Component** > **Windows Explorer**.
5. Click **Turn off Windows+X hotkeys**.
6. Select **Enabled**.
7. Click **OK**.
8. Restart the client computer.

## Enabling single sign-on for Java applications

Java Virtual Machine (JVM) performs automatic sign-on for 32- bit Java applications. JVM also does single sign-on in applets that run by using JVM 1.1 and JVM 1.2 or later.

### About this task

If you configure single sign-on after installing AccessAgent, perform these steps for each JVM that runs Java applications and applets. For JVM 1.2 or later, select **JVMInstallationDirectories** from the installer. Get the VBScript from `C:\Program Files\IBM\ISAM ESSO\ECSS\JavaSupport\JVMSupport.vbs`.

### Procedure

1. On your Windows desktop, click **Start** > **Run**.
2. In the **Open** field, enter **cmd**.
3. Click **OK**. The command prompt displays.
4. Run `JVMSupport.vbs`.
   - If you are in a 32-bit environment, use `C:\Windows\system32\cmd.exe`.
   - If you are in a 64-bit environment, use `C:\Windows\SYSWOW64\cmd.exe`.
5. Enter ***JVMSupport [/dall {default}] [/uall] [/d path] [/dold path] [/dnew path] [/u path] [/uold path] [/unew path] [/?]***

| Option | Description |
|---|---|
| **/dall** | Deploy JVM Support for all JVMs detected in the Windows registry. |
| **/uall** | Remove JVM Support for all JVMs detected in the Windows registry. |
| **/d [path]** | Deploy JVM Support to the JVM installed at the specified path. |
| **/dnew [path]** | Deploy JVM Support to the JVM installed at the specified path (for Java 1.2 or later). |
| **/dold [path]** | Deploy JVM Support to the JVM installed at the specified path (for Java 1.1). |

| Option | Description |
|---|---|
| **/u [path]** | Remove JVM Support to the JVM installed at the specified path. |
| **/unew [path]** | Remove JVM Support to the JVM installed at the specified path (for Java 1.2 or later). |
| **/uold [path]** | Remove JVM Support to the JVM installed at the specified path (for Java 1.1). |
| **/?** | Show this help message. |

**Note:** The /u and /d options attempt to automatically detect the Java Version at the specified path.

## Configuring AccessAgent to use EnWinNetUse

You can configure AccessAgent so that it uses EnWinNetUse when mapping user-specific network drives. Modify the AccessAgent logon script to start EnWinNetUse.exe with the appropriate parameters.

### Procedure

1. Set the following policies accordingly:
   - pid_script_logon_enabled
   - pid_script_logon_type
   - pid_script_logon_code

   **Note:** See the *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide* for more details.
2. Use AccessStudio to create an AccessProfile for EnWinNetUse, so that the appropriate Windows credentials can be auto-filled in the EnWinNetUse prompt. See the *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide* for more details.

### Results

When a user logs on to AccessAgent, the logon script opens the EnWinNetUse.exe file. AccessAgent automatically enters the Windows credentials. EnWinNetUse.exe maps the drives accordingly.

The application is installed with AccessAgent and is found in the IBM Security Access Manager for Enterprise Single Sign-On directory.

Run EnWinNetUse.exe from the command line. Enter

```
EnWinNetUse.exe [-d <drive letter(s)>] [-p <network path(s)>]
[-u <user name>] [-x <domain>] [-r] [–v] [-s]
```

| Command | Description |
|---|---|
| -d | Specifies a drive letter or list of drive letters.<br><br>You can:<br>• Use any unassigned letter, such as J. The colon (:) is required.<br>• Use * to automatically assign the drive letter.<br><br>When mapping multiple network drives, separate them with a forward slash (/). Do not put spaces in between<br><br>The network paths that you specify must have a one-to-one correspondence to the number of network drives in your environment. If they are not the same, the smaller list is effective. If an error occurs when mapping 1 drive, other drives continue to be mapped. |
| -p | Specifies network path or list of network paths.<br><br>When mapping multiple network drives, separate them with a forward slash (/). Do not put spaces in between unless space is part of the file or folder name.<br><br>The network paths that you specify must have a one-to-one correspondence to the number of network drives in your environment. If they are not the same, the smaller list is effective. If an error occurs when mapping 1 drive, other drives continue to be mapped. |
| -u | Any user name to be used for mapping the drives. |
| -x | Domain to be used for mapping the drives. |
| -r | Remember network drive connections. |
| -v | Turns on verbose error messages. |
| -s | Use simplified user interface (showing only user name, password, and domain). |

## Enabling the Observer Help

Use the Help function in the Observer window to access the IBM Security Access Manager for Enterprise Single Sign-On online publications.

### Procedure

1. On your Windows desktop, click **Start** > **Run**.
2. In the **Open** field, enter `regedit` and click **OK**.
3. Select `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\ECSS\DeploymentOptions`.
4. Right-click and select **New** > **DWORD Value**.
5. Enter `ObsOnlineHelpEnabled`.
6. Right-click **ObsOnlineHelpEnabled** and select **Modify**.
7. In the **Value data** field, specify one of the following values:
   - **0** - (default) Does not enable the **Help** button.
   - **1** - Enables the **Help** button.
8. Click **OK**.

**Note:** To not enable the help on the ISAM ESSO GINA, set **AAOnlineHelLink** to `EMPTY STRING` under `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\DeploymentOptions`.

## Configuring event reporting in the Windows Event log

Critical AccessAgent errors or Level 1 errors are recorded in the Windows Application Event log. You can enable or not enable this feature through registry entry configuration.

### Procedure

1. On your Windows desktop, click **Start** > **Run**.
2. In the **Open** field, enter `regedit` and click **OK**.
3. Select `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\DeploymentOptions`.
4. Right-click and select **New** > **DWORD Value**.
5. Enter `WindowsEventLogEnabled`.
6. Right-click **WindowsEventLogEnabled** and select **Modify**.
7. Specify one of the following values:
   - **0** - (default) Does not enable event reporting in the Windows Event log.
   - **1** - Enables event reporting in the Windows Event log.
8. Click **OK**.

## Configuring the system modal message box

When an AccessAgent error message requires your attention, you cannot open or use other applications on your desktop until you respond to it. You can enable or not enable this feature through registry entry configuration. This feature is not enabled by default.

### Procedure

1. On your Windows desktop, click **Start** > **Run**.
2. In the **Open** field, enter `regedit` and click **OK**.
3. Select `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\DeploymentOptions`.
4. Right-click and select **New** > **DWORD Value**.
5. Enter `SystemModalMessageEnabled`.
6. Right-click **SystemModalMessageEnabled** and select **Modify**.
7. Specify one of the following values:
   - **0** - (default) Does not enable the System Modal message box so you can continue working when an AccessAgent message is displayed.
   - **1** - Enables the System Modal message box so you cannot do anything else until you respond to the AccessAgent message.
8. Click **OK**.

## Enabling emergency hot key for private desktops

You can switch to the default Windows desktop by pressing a pre-defined hot key. Add a registry policy to enable this feature. For more information about hot key policies, see the *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide*.

### Procedure

1. On your Windows desktop, click **Start** > **Run**.
2. In the Open field, enter `regedit` and click **OK**.
3. Select **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **IBM** > **ISAM ESSO** > **DeploymentOptions**.

4. Right-click and select **New** > **DWORD Value**.
5. Enter `LUSMEmergencyBypassHotKeyEnabled`.
6. Right-click `LUSMEmergencyBypassHotKeyEnabled` and select **Modify**.
7. In the **Value data** field, specify 1.
8. Click **OK**.

# Configuring the AccessAgent accessibility features

You can configure the accessibility features of AccessAgent. The accessibility features include animation and keyboard shortcuts.

See the following topics for more information.

- "Enabling animation effect for AccessAgent"
- "AccessAgent keyboard shortcuts"

## Enabling animation effect for AccessAgent

AccessAgent supports animation for better visual accessibility.

### Procedure

1. Log on to AccessAdmin.
2. Navigate to **Machine policies** > **AccessAgent policies** > **Accessibility policies**.
3. Under **Enable Animation effect for AccessAgent**, select **Yes**.

## AccessAgent keyboard shortcuts

Every AccessAgent action can be accessed by using a keyboard shortcut.

When you press the keyboard button **Alt**, the AccessAgent user interface shows the keyboard equivalents by underlining the letter of the shortcut. All keyboard shortcuts must be pressed with **Alt** and the corresponding shortcut letter.

Example: Shortcut for unlocking your screen

1. With the IBM Security Access Manager for Enterprise Single Sign-On EnGINA on your screen, press **Alt** on your keyboard.
2. Look at the underlined letter of the user interface. The underlined letter in **Unlock this computer** is **k**.
3. Press **Alt+k** on your keyboard. You are prompted for the password to unlock your screen.

# Chapter 4. Configuring Citrix and Terminal Servers

You can configure IBM Security Access Manager for Enterprise Single Sign-On so that users can single sign-on and authenticate in applications hosted on Microsoft Terminal Server or Citrix XenApp Servers.

See the following topics for more information.

- "Configuring a Citrix deployment"
- "Configuring a Terminal Server deployment"
- "Changing the Server AccessAgent mode"
- "Customizing AccessAgent on the Citrix or Terminal Server" on page 62
- "Configuring the time threshold for synchronization timestamp" on page 63

## Configuring a Citrix deployment

You must assign machine policies and develop a virtual channel connector to deploy single sign-on and authentication services on a Citrix Server.

### Procedure

1. Apply the **Citrix and Terminal Server** Machine Policy Template generated by Setup Assistant to the Citrix Server.
2. Develop the virtual channel connector DLL and integrate AccessAgent with the Citrix Server. See the *IBM Security Access Manager for Enterprise Single Sign-On Lightweight AccessAgent mode on Terminal Server SDK Guide* for more details. See Appendix B, "Setting up policy templates," on page 93 for more details.

   **Tip:** Encryption is suggested when using Remote Desktop Protocol or Citrix with AccessAgent.

## Configuring a Terminal Server deployment

AccessAgent does not require additional configuration in the Terminal Server.

You must apply the Citrix and Terminal Server Machine Policy Template generated by Setup Assistant to the Terminal Server. See Appendix B, "Setting up policy templates," on page 93 for more details.

**Tip:** Encryption is suggested when using Remote Desktop Protocol or Citrix with AccessAgent.

## Changing the Server AccessAgent mode

The Server AccessAgent is the AccessAgent installed in the Terminal Server or Citrix server. The Server AccessAgent can run in standard mode or in lightweight mode. You can enable or not enable the lightweight mode by configuring the `TSLightweightMode` policy. The lightweight mode reduces the memory footprint and improves the single sign-on startup time.

### Before you begin

Do not enable the ESSO GINA or ESSO Credential Provider. For more information, see "Disabling the ESSO GINA or ESSO Credential Provider" on page 52.

### About this task

The lightweight mode feature for Citrix requires integration and support from IBM partners.

### Procedure

1. On your Windows desktop, click **Start** > **Run**.
2. In the **Open** field, enter **regedit** then click **OK**.
3. Select `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\DeploymentOptions`.
4. Right-click and select **New** > **DWORD Value**.
5. Enter `TSLightweightMode`.
6. Right-click **TSLightweightMode**.
7. Select **Modify**.
8. In the **Value data** field, specify a value.

   See the following table for the descriptions of each policy value.

| Value | Description |
|---|---|
| `0` | • Does not enable lightweight mode.<br>• The Server AccessAgent operates only in standard mode. |
| `1` (default) | • Enables lightweight mode.<br>• The Server AccessAgent operates in lightweight mode only if the Client AccessAgent, or the AccessAgent installed in the client computer, is version 8.1.1 or later. Otherwise, the Server AccessAgent operates in standard mode. |
| `2` | • Enforces lightweight mode.<br>• The Server AccessAgent always operates in lightweight mode. |

9. Click **OK**.

### What to do next

To use lightweight mode, inform your users to:

1. Log on to AccessAgent from their local computer.
2. Start a Citrix or Remote Desktop Protocol session.

## Customizing AccessAgent on the Citrix or Terminal Server

You can customize the behavior of AccessAgent when users log on to a session on a Citrix/Terminal Server.

1. Log on to AccessAdmin.
2. Navigate to **Machine Policy Templates** > **Template assignments**.
3. Click a policy template.
4. Navigate to **AccessAgent Policies** > **Terminal Server Policies**.
5. Complete the following fields:

| Option | Description |
|---|---|
| Enable auto-launching of AccessAgent logon prompt | Identifies whether to launch the AccessAgent logon dialog if AccessAgent is not logged on when a Terminal Server session or Citrix application is launched. |
| Use ESSO GINA logon when there is no local AccessAgent session | Whether to use ESSO GINA logon or Microsoft GINA logon for the Terminal Server session, when there is no local AccessAgent session. |
| Log off remote AccessAgent when reconnecting from workstation without local AccessAgent session | Whether to log off remote AccessAgent when user, with no local AccessAgent session, reconnects to an existing session on Terminal Server. |
| Option for displaying menu options on remote AccessAgent | Whether to display menu options on AccessAgent user interface in a Terminal Server session. |

6. Optional: Complete the following fields only if you want RFID to be enabled for thin clients:

| Option | Description |
|---|---|
| Enable COM port redirection | Identifies whether the device monitoring mechanism must perform COM port redirection from the client computer to the Terminal Server. |
| Virtual COM port on Terminal Server | Virtual COM port on the Terminal Server to which data from the client COM port gets redirected to. |
| Physical COM port on client machine | Physical COM port on the client to which the authentication device, or the RFID reader, is connected to. The redirection takes place from this port to the virtual COM port of the Terminal Server. |

7. Click **Update**.
8. Assign the newly updated machine policy template to the Terminal Server.

## Configuring the time threshold for synchronization timestamp

You can configure a policy to control the volume of data to be downloaded and synchronized from the IMS Server. Configuring this policy can improve system performance.

### About this task

Multiple client computers that are logged on to the Terminal Server try to download system data every time the IMS Server updates the data. This frequent data synchronization causes performance degradation. Use a policy that enables only one AccessAgent instance to download the system data in a threshold of **SystemSyncToleranceSecs**. This procedure applies to standard mode only.

### Procedure

1. On your Windows desktop, click **Start** > **Run**.
2. In the **Open** field, enter **regedit** then click **OK**.

3. Select `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\DeploymentOptions`.
4. Add **SystemSyncToleranceSecs**.
5. Enter a value. Default value is 300 seconds.
6. Click **OK**.

# Chapter 5. Configuring a strong authentication setup

Authentication factors come in different forms and functions, such as passwords and devices that work like a key. A strong authentication setup reduces the risk of security compromises. You can implement a second authentication factor or an alternative authentication factor to secure user sessions.

You can use the devices or codes as second authentication factors. You can also use fingerprint as an alternative authentication factor to password.

See the following topics for more information.

- "Setting up RFID authentication"
- "Setting up ARFID authentication" on page 66
- "Setting up fingerprint authentication" on page 67
- "Setting up smart card authentication" on page 70
- "Setting up OTP and MAC authentication" on page 78

**Tip:** See the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide* for a list of supported authentication devices and middleware.

## Setting up RFID authentication

Make sure that you have the necessary software and hardware of the reader that you are going to use. Install the drivers for the readers and check that the hardware and software are set up properly.

### Before you begin

**Important:**

- If you want to use the GIGA-TMS Proximity Readers PCR300MU, MFR 135 or Altrus RFID reader, open the AccessAgent installer folder. Search for the `Reg` folder.
- If you want to use other supported RFID readers, set up the machine policy directly. See Setting up the machine policy.

### Procedure

1. Open `DeploymentOptions.reg`. Browse for the corresponding reader.

   For example, if you want to use Altrus RFID Reader, the following information is in the DeploymentOptions.reg:

```
====== Mifare for Altrus
;[HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\SOCIAccess\DSPList\Mifare\Devices\ALTRUS]
;"DeviceTypeId"="Prolific ALTRUS"

;[HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\SOCIAccess\DSPList\Mifare\Devices\ALTRUS\Interfaces]

;[HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\SOCIAccess\DSPList\Mifare\Devices\ALTRUS\Interfaces\{216DE8B9-FD09-44f3-A39D-B8A6F7A078D8}]

;[HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\SOCIAccess\DSPList\Mifare\Devices\ALTRUS\Parameters]
;"CardType"="R_ALTRUS_32"

;[HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\SOCIAccess\DSPList\Mifare\Devices\ALTRUS\Trigger]
;"WinInterfaceClass"="{4D36E978-E325-11CE-BFC1-08002BE10318}"
```

2. Remove all instances of "`;`" at the beginning of each line except the first line.
3. Save the `DeploymentOptions.reg` file.

   **Note:** You can also do this step after AccessAgent is installed.

a. Before you restart the computer, copy the `DeploymentOptions.reg` file to your local computer.
b. Open, edit, then save the file.
c. Double-click the `DeploymentOptions.reg`.
d. Click **Yes** when a dialog box prompts you on whether you want to import the registry settings or not. The corresponding registry settings are also updated.

4. In AccessAdmin, set the machine policy **Authentication second factors supported** to **RFID**.

   See the *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide* for more details.

   **Important:** Plug in the RFID device to your computer before starting. If the device is not detected upon startup, restart your computer.

## Setting up ARFID authentication

Setting up ARFID varies on whether you have installed AccessAgent or not in the client computers.

See the following topics for more information.

- "Installing an ARFID reader in a computer with AccessAgent"
- "Installing an ARFID reader in a computer without AccessAgent"

### Installing an ARFID reader in a computer without AccessAgent

If AccessAgent is not yet installed, install Xyloc and then AccessAgent.

#### Procedure

1. Plug in the Xyloc reader into the computer USB port.
2. Run `setup.exe` to install the XyLoc Service on the client computer.
3. Install AccessAgent.

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

### Installing an ARFID reader in a computer with AccessAgent

You can set the appropriate registry settings if AccessAgent is installed.

#### Procedure

1. Plug in the XyLoc reader into the computer USB port.
2. Run `setup.exe` to install the XyLoc Service on the client computer.
3. On your Windows desktop, click **Start** > **Run**.
4. In the **Open** field, enter **`regedit`** then click **OK**.
5. Select `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SOCIAccess]` key in the registry.
6. Double-click **`DependOnService`**.
7. Type **`XyLoc Security System`** under the **Value data** field.
8. Click **OK**.
9. Restart the computer.

# Setting up fingerprint authentication

Setting up fingerprint authentication involves installing the Native Library Invoker resource adapter and installing the fingerprint readers. IBM Security Access Manager for Enterprise Single Sign-On supports BIO-key, DigitalPersona, and UPEK fingerprint readers.

See the following topics for more information.

- "Installing the Native Library Invoker resource adapter"
- "Integrating a BIO-key fingerprint reader" on page 68
- "Integrating a DigitalPersona fingerprint reader" on page 69
- "Integrating a UPEK fingerprint reader" on page 70

## Installing the Native Library Invoker resource adapter

If you need BIO key support for biometric or biometric verification systems, you must manually install this resource adapter on every node in the WebSphere cluster.

### About this task

The IMS Server installer does not automatically deploy the Native Library Invoker resource adapter to the WebSphere Application Server. You must install the Native Library Invoker (NLI) resource adapter on every node in the WebSphere Application Server cluster. After you install the adapter, specify the Java Naming and Directory Interface or 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 IBM Integrated Solutions Console.
3. In the Integrated Solutions Console left 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 and click **OK**.
9. In the **Messages** box at the top of the page, 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. Click **Save** in the **Messages** box at the top of the page.

# Integrating a BIO-key fingerprint reader

With the integration between BIO-key Biometric Service Provider (BSP) and IBM Security Access Manager for Enterprise Single Sign-On, users can work with any biometric reader that is supported by BIO-key.

## About this task

Only Administrators can integrate and deploy the BIO-key Biometric Service Provider (BSP) with IBM Security Access Manager for Enterprise Single Sign-On. The BIO-key Biometric Service Provider deployment processes for the IMS Server and AccessAgent are different.

## Deploying BIO-key Biometric Service Provider in the IMS Server

Set up the BIO-key Biometric Service Provider first in the IMS Server.

### Procedure

1. Install the Native Library Invoker resource adapter.
2. Install the BIO-key BSP drivers (BioAPI BSP SDK 1.9_266_Ship or later) in the IMS Server.
   a. Start the BIO-key installer.
   b. In the BIO-key Reader Setup dialog box, select the manual setup of biometric reader files option.
   c. Select the biometric reader files to use. Wait for the completion of the installation.

      **Note:** Selecting all biometric readers might cause performance issues.
   d. Select the manual selection of biometric readers option.
   e. Select the biometric reader that you are going to use from the list of readers installed.
   f. Complete the rest of the installation steps.
3. Navigate to the IBM Security Access Manager for Enterprise Single Sign-On installation package.
4. Open the `deploymentPack.biometrics\bio-key` folder.
5. Follow the steps in the README.txt to apply the deployment package for BIO-key.

   **Note:** Run as an Administrator in Windows Server 2008 or later.
6. Restart the WebSphere Application Server.
7. Set **pid_second_factors_supported_list** to **Fingerprint** in AccessAdmin. See the *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide* for more details.

**Deploying BIO-key Biometric Service Provider in AccessAgent:**

After deploying BIO-key Biometric Service Provider in the IMS Server, you can now deploy BIO-key in AccessAgent.

**Procedure**

1. Install BIO-key Biometric Service Provider (BSP) version 1.9.266 or later.
2. Open the AccessAgent Installer folder.
3. Navigate to the **Customization** folder.

4. Copy `FP3-BioKey.reg` to the `Reg` folder in the Installation folder.
5. Install AccessAgent.

   **Note:** The Bio-Key BSP installation creates registry settings in the Local Machine (HKLM) and Current User (HKCU) levels. AccessAgent uses only HKLM settings. HKCU settings are ignored even if these settings are set later by the user.
6. Open the AccessAgent installation directory. For example, `C:\Program Files\IBM\ISAM ESSO`.
7. Set `ResetBioAPIPermissions` in SetupHlp.ini to 1.
8. On your Windows desktop, click **Start** > **Run**.
9. In the **Open** field, enter `regedit` then click **OK**.
10. Select `HKLM\Software\IBM\ISAM ESSO\SOCIAccess\DSPList\{6EA4B6D4-8CDF-4C4E-8B40-CA6A20D0CD6B}\Devices\{5994DB8B-A2C3-4e0a-BC79-F274AE5ECC11}\UISPList\{68F86CB2-630B-4F15-9E2B-5A77B294E9E2}` in the Registry Editor.
11. Set the registry value **Enabled** to 1.
12. Restart the computer.
13. Optional: If you installed AccessAgent first before BIO-key, do the following additional steps:
    a. Run **FP3-BioKey.reg**. This file is located in the **Customization** folder under the AccessAgent installation folder.
    b. Repeat steps 8 to 12.

## Integrating a DigitalPersona fingerprint reader

If you choose to deploy DigitalPersona fingerprint reader, set it up first in the IMS Server and then in AccessAgent.

### Deploying DigitalPersona in the IMS Server

You must set up DigitalPersona in the IMS Server.

#### Procedure

1. Install the Native Library Invoker resource adapter.
2. Install the DigitalPersona Fingerprint Gold SDK 3.2.
3. Insert the IBM Security Access Manager for Enterprise Single Sign-On installation CD.
4. Click the `deploymentPack.biometrics\digital-persona` folder.
5. Follow the steps in the `README.txt` to apply the deployment package for DigitalPersona.
6. Restart the WebSphere Application Server.
7. Set **pid_second_factors_supported_list** to **Fingerprint** in AccessAdmin. See the *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide* for more details.

### Deploying a DigitalPersona biometric reader in AccessAgent

After setting up DigitalPersona in the IMS Server, you can now set it up in AccessAgent.

#### Procedure

1. Install AccessAgent in the client computer. See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for more details.
2. Install the DigitalPersona Fingerprint Gold SDK 3.2.

3. Restart the computer.

## Integrating a UPEK fingerprint reader

If you choose to deploy UPEK fingerprint reader, set it up first in the IMS Server and then in AccessAgent.

### Deploying a UPEK biometric reader in IMS Server

You can set up the UPEK biometric reader first in the IMS Server.

#### Procedure

1. Install the Native Library Invoker resource adapter.
2. Install the Upek BioAPI SDK.
3. Insert the IBM Security Access Manager for Enterprise Single Sign-On installation CD.
4. Click the `deploymentPack.biometrics\upek` folder.
5. Follow the steps in the README.txt to apply the deployment package for the UPEK biometric reader.
6. Restart the WebSphere Application Server.
7. Set **pid_second_factors_supported_list** to **Fingerprint** in AccessAdmin. See the *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide* for more details.

### Deploying a UPEK biometric reader in AccessAgent

After setting up UPEK biometric reader in IMS Server, you can now set it up in AccessAgent.

#### Procedure

1. Install the Upek BioAPI SDK.
2. Install AccessAgent 8.2.
3. Restart the computer.

# Setting up smart card authentication

Setting up smart card authentication involves enabling two-way SSL, importing smart card CA certificates, and configuring polices.

See the following topics for more information.


- "Enabling two-way SSL" on page 71
- "Importing smart card CA certificates" on page 71
- "Enabling smart card authentication" on page 72
- "Configuring hybrid smart cards" on page 75
- "Using the smart card self-certification tool" on page 75
- "Importing smart card CA certificates" on page 71
- "Configuring DNIe smart cards" on page 76
- "Unregistering the DNIe certificate store" on page 77
- "Adding a registry key for the DNIe smart card middleware" on page 77

## Enabling two-way SSL

You must enable two-way SSL on the IBM HTTP Server. The IMS Server relies on the SSL certificate setup on IBM HTTP Server for its mutual SSL authentication with its clients. This procedure is required for smart card authentication.

### 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 left navigation pane, select **Servers** > **Server Types** > **Web Servers** > *Web server name*.
4. Click **Configuration file**.
5. Add the lines marked **bold**:

```
<VirtualHost *:443>
SSLEnable
SSLProtocolDisable SSLv2
SSLClientAuth optional
SSLServerCert <IHS certificate alias>
</VirtualHost>
```

6. Click **OK**.

## Importing smart card CA certificates

You must import the certificate chain of the certificate authority (CA) issuing certificates to smart cards into the IBM HTTP Server truststore to enable smart card authentication.

### 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 left navigation pane, select **Servers** > **Server Types** > **Web Servers** > **<*Web server name*>**.
4. Click **Plug-in properties**.
5. Click **Manage Keys and Certificates**.
6. Click **Signer certificates**.
7. Click **Add**.
8. Complete the appropriate fields.
9. Click **OK**.
10. Save the changes.
11. Return to the Plug-in properties page.
12. Click the **Copy to Web server keystore** directory.
13. If you do not have the **SSLServerCert** *IHS certificate alias* setting in the `httpd.conf` configuration file, set the default certificate.
    a. Open the IBM HTTP Server Key Management Utility.
    b. Navigate to **Key Database File** > **Open** > **Browse** > **Plugins** > **Config** > **<*Web server name*>** > **plugin-key.kdb**.
    c. Click **OK**.
    d. Enter the keystore password. The default password is `WebAS`.
    e. Double-click the personal certificate with the **default** alias.

f. Select **Set the Certificate as the default**.
g. Click **OK**.

14. Restart the IBM HTTP Server.

## Enabling smart card authentication

Complete the following procedure if you want to use smart card authentication.

### Before you begin

Make sure the IMS Server and AccessAgent are installed.

### Procedure

1. Run the smart card installer. Before the installation process completes, the installer merges the entries in the registry file with the Windows Registry.
2. Create and apply the policies for smart card authentication.
   a. Log on to AccessAdmin.
   b. Navigate to **Machine Policy Templates** > **New template** > **Create new machine policy template** > **Authentication Policies**.
   c. Type `smart card`.
   d. Click **Add**.
   e. Scroll down the page and click **Add** again.
3. Optional: Edit the registry hive.
   a. Add the name of each supported smart card to the `HKLM\SOFTWARE\IBM\ISAM ESSO\SOCIAccess\SmartCard:SupportedCards` multi-string value.

      The name of the smart card must appear in the list of smart cards registered with Windows, which can be found under `HKLM\SOFTWARE\Microsoft\ Cryptography\Calais\SmartCards`.

      If the "SupportedCards" registry value is not specified, AccessAgent monitors ALL smart cards registered with Windows.By default, AccessAgent automatically detects the CSP module used to access an inserted smart card based on the registration of the smart card with Windows.

      However, if the CSP used is different from the one registered with Windows, then the DWORD registry value, *AutoDetectCardMiddlewareEnabled*, must be added under `[HKLM\SOFTWARE\IBM\ISAM ESSO\SOCIAccess\SmartCard]` and set to `0`.
   b. Create a key for the smart card middleware under `HKLM\SOFTWARE\IBM\ISAM ESSO\SOCIAccess\SmartCard\Middleware`.

      The name of the key can be any name that can be used to identify the middleware. Under the middleware key, create and set the following values that define the parameters for the middleware.

      If this middleware information is not configured, AccessAgent uses the default values for all middleware parameters.

| Middleware Parameter | Type | Values | Mandatory? |
|---|---|---|---|
| CSPName | REG_SZ | Name of the Cryptographic Service Provider module from the middleware. | Yes |

| Middleware Parameter | Type | Values | Mandatory? |
|---|---|---|---|
| RsaEncryptionEnabled | DWORD | If the smart card keypair cannot be used to perform RSA encryption, this value must be set to `0`.<br><br>AccessAgent uses a signature-based mechanism to encrypt the Wallet instead of the encryption-based mechanism which is the default. | No |
| ContainerSpecLevel | DWORD | By default, AccessAgent searches for the authentication certificate in the default container on the smart card.<br><br>A default container is a special certificate container that can be accessed without specifying the container name.<br><br>However, if the authentication certificate used by AccessAgent is not in the default container, AccessAgent must specify the name of the container.<br><br>CSPs follow different conventions for accepting container names. This parameter defines the container name format.<br>• #1: \\.\<reader-name>\<container-id><br>• #2: \\.\<reader-name>\\\<br>• #3: <container-id><br>• #4: NULL (default)<br><br>If this parameter is set to 1 or 3, AccessAgent enumerates the containers and searches for the authentication certificate based on the `AuthCertIssuerList` and `AuthCertKeyUsageBits` parameters. | No |

| Middleware Parameter | Type | Values | Mandatory? |
|---|---|---|---|
| AuthCertIssuerList | REG_MULTI_SZ | If the authentication certificate is not available in the default container, then AccessAgent uses this parameter to search the certificates available on the smart card.<br><br>This multi-string must include the Common Names (CN) of the issuers of the authentication certificate.<br><br>For a smart card certificate to be selected for authentication, the name of the certificate issuer must be present in this list. | No |
| AuthCertKeyUsageBits | DWORD | If the authentication certificate is not available in the default container, then AccessAgent uses this parameter to search the certificates available on the smart card.<br><br>This hexadecimal value is the bitwise-OR value of the possible key usage values defined in the certificate.<br><br>The possible key usage bits as defined in the X509v3 specification are:<br>• 0x80: digital signature<br>• 0x40: non-repudiation<br>• 0x20: key encipherment<br>• 0x10: data encipherment<br>• 0x08: key agreement<br>• 0x04: certificate signing<br>• 0x02: CRL signing<br><br>An example of `CertSearchKeyUsageBits` is `A0`, which allows the use of the keypair for digital signatures and key encipherment. | No |

c. Save the required registry settings in a .reg file and place the file in the `<AccessAgent installation folder>\Reg` folder.

4. Restart your machine.

## Configuring hybrid smart cards

IBM Security Access Manager for Enterprise Single Sign-On supports hybrid smart cards. You can enable single-factor logon for a hybrid smart card with a card serial number.

### Procedure

1. Log on to AccessAdmin.
2. Navigate to **Machine Policy Templates** > **New template** > **Create new machine policy template** > **Authentication Policies**
3. Type `hybrid smart card`.
4. Click **Add**.
5. Scroll down the page and click **Add** again.
6. Configure a grace period so that you can log in without a PIN across workstations. See the hybrid smart card policies section in the *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide*.

   **Note:** AccessAgent automatically creates the registry settings for the supported cards and readers.

## Using the smart card self-certification tool

Run the smart card self-certification tool to test whether the smart cards used by your organization are compatible withIBM Security Access Manager for Enterprise Single Sign-On.

### Before you begin

Make sure that you have the following items:

- A personalized smart card
- Drivers for the smart card reader (if applicable)
- Smart card middleware
- Smart card PIN
- The RSA keypair and the corresponding certificate issued by a Certification Authority or CA that are already stored in the smart card

For more information about the requirements, see the readme.txt file that is included with the smart card compatibility tool.

### About this task

By default, the tool runs smart card tests based on the following items:

- Windows Smart Card Service
- Cryptographic Service Provider (CSP) module

The smart card is compatible with IBM Security Access Manager for Enterprise Single Sign-On if the CSP tests are successful. CSP tests are successful if the following criteria are met:

- Certificate test is successful and outputs a certificate used by IBM Security Access Manager for Enterprise Single Sign-On for authentication.
- PIN verification test is successful.
- EITHER encryption test OR signature test is successful.

- The CSP supports the silent mode. The execution of the tests does not result in any pop-up dialog for PIN verification or certificate selection.

### Procedure

1. Extract the contents of the .zip file to a temporary folder. For example, `C:\temp\`.
2. Navigate to the temporary folder, then specify the parameters in the config.ini file.
   a. Double-click the config.ini file and enter parameters by using Notepad.exe.
   b. Optional: Specify the following basic parameters.

| Parameter | Description |
|---|---|
| PKCS11Lib | Name of the PKCS#11 library provided by the smart card middleware. If the .DLL file is not in the system path, specify the full path of the .DLL file. |
| CSPName | Name of the Cryptographic Service Provider (CSP) provided by the smart card middleware. |

   c. See the **readme** file for more details on other parameters.
   d. Save the configuration file.
3. Open the command prompt.
   a. Click **Start** > **Run**.
   b. In the **Open** field, enter `cmd`.
   c. Click **OK**.
4. Enter `>SCardCompatTool -i <path-to-config-file.ini>-o <log-file>`. For example, `>SCardCompatTool -i config.ini -o scardtest.log`.

### Results

A log file is generated and stored in the same folder as the compatibility tool folder. The following information is included in the log file:

- Logs - The logs are stored in the file specified in the command-line parameters. Each time you run the smart card compatibility tool, the logs are appended to the file.
- Certificate - The tool also extracts and stores the certificate of the smart card keypair used for testing in the file. The certificate file name is of the form: `<serial-number>.cer`.

## Configuring DNIe smart cards

IBM Security Access Manager for Enterprise Single Sign-On supports country-specific smart cards such as DNIe. Configure AccessAgent so that the smart cards work optimally with IBM Security Access Manager for Enterprise Single Sign-On.

### Procedure

1. Install the DNIe middleware.
2. Install and configure the smart card PKCS#11 Cryptographic Service Provider. See the *IBM Smart card PKCS#11 Cryptographic Service Provider User Guide* for more details.
3. Unregister the DNIe certificate store.

4. Add a registry key for the DNIe smart card middleware.

## Unregistering the DNIe certificate store

You must unregister the DNIe certificate store to complete the DNIe smart card configuration.

### Procedure

1. On your Windows desktop, click **Start** > **Run**.
2. In the **Open** field, enter **regedit** and click **OK**.
3. Select `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv\UsrDNIeCertStore`.
4. Right-click **Dll** and select **Modify**.
5. In the **Value data** field, delete the entry.
6. Click **OK**.

## Adding a registry key for the DNIe smart card middleware

After unregistering the DNIe certificate store, add a registry key for the DNIe smart card middleware. You must also create policies for certificate protection, exclusive access, and RSA encryption.

### Procedure

1. On your Windows desktop, click **Start** > **Run**.
2. In the **Open** field, enter **regedit** and click **OK**.
3. Create a smart card key.
   a. Select `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\SOCIAccess\`.
   b. Right-click and select **New** > **Key**.
   c. Enter `SmartCard`.
   d. Click **OK**
4. Create a **AutoDetectCardMiddlewareEnabled** policy.
   a. Select `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\SOCIAccess\SmartCard\`.
   b. Right-click and select **New** > **DWORD Value**.
   c. Enter `AutoDetectCardMiddlewareEnabled`.
   d. Right-click **AutoDetectCardMiddlewareEnabled** and select **Modify**.
   e. In the **Value data** field, specify `0`.
   f. Click **OK**.
5. Create an IBM smart card middleware key.
   a. Select `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\SOCIAccess\SmartCard\`.
   b. Right-click and select **New** > **Key**.
   c. Enter `Middleware`.
   d. Click **OK**.
   e. Select `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\SOCIAccess\SmartCard\Middleware\`.
   f. Right-click and select **New** > **Key**.
   g. Enter `IBM`.
   h. Click **OK**.
6. Set the Cryptographic Service Provider name.

a. Select HKEY_LOCAL_MACHINE\SOFTWARE\IBM\SOCIAccess\SmartCard\Middleware\IBM\.
b. Right-click and select **New** > **String Value**.
c. Enter CSPName.
d. Right-click **CSPName** and select **Modify**.
e. In the **Value data** field, specify IBM PKCS11 CSP.
f. Click **OK**.

7. Create a **CertProtectedByPIN** policy.
   a. Select HKEY_LOCAL_MACHINE\SOFTWARE\IBM\SOCIAccess\SmartCard\Middleware\IBM\.
   b. Right-click and select **New** > **DWORD Value**.
   c. Enter CertProtectedByPIN.
   d. Right-click **CertProtectedByPIN** and select **Modify**.
   e. In the **Value data** field, enter 1.
   f. Click **OK**.
8. Create a **ExclusiveAccess** policy.
   a. Select HKEY_LOCAL_MACHINE\SOFTWARE\IBM\SOCIAccess\SmartCard\Middleware\IBM\.
   b. Right-click and select **New** > **DWORD Value**.
   c. Enter ExclusiveAccess.
   d. Right-click **ExclusiveAccess** and select **Modify**.
   e. In the **Value data** field, enter 1.
   f. Click **OK**.
9. Create a **RsaEncryptionEnabled** policy.
   a. Select HKEY_LOCAL_MACHINE\SOFTWARE\IBM\SOCIAccess\SmartCard\Middleware\IBM\.
   b. Right-click and select **New** > **DWORD Value**.
   c. Enter RsaEncryptionEnabled.
   d. Right-click **RsaEncryptionEnabled** and select **Modify**.
   e. In the **Value data** field, enter 0.
   f. Click **OK**.

# Setting up OTP and MAC authentication

You can configure the settings for one-time passwords (OTP) and Mobile ActiveCodes (MAC) for strong authentication. The OTP can be configured for both OATH and VASCO.

See the following topics for more information.

- "Configuring OTP (OATH)"
- "Configuring OTP (VASCO)" on page 79
- "Configuring MAC" on page 81

## Configuring OTP (OATH)

OTP is a one-time use password generated for an authentication event, sometimes communicated between the client and the server through a secure channel. Configure OTP settings so that users can use OTP as their authentication factor.

### Procedure

1. Upload the OATH files to the IMS Server.
   a. Copy the OATH Seed file to the IMS Server.
   b. Put the OATH seed file in `<IMS Installation Folder>\ims\WEBINF\ lib`.
   c. Navigate to `<IMS install directory>` bin.
   d. Edit `setupcmdline.bat` and point it to the right WebSphere Application Server profile.
   e. Save and exit the application.
   f. Run the `uploadoath.bat` file by following this format: `uploadoath <was admin> <was password> --in <path of oath.txt> --out <log file>`.
   g. Restart the IMS Server.
2. Configure the OTP user in AccessAdmin.
   a. Log on to AccessAdmin.
   b. Search for your OTP user and select it.
   c. Click `OTP Token Assignment`.
   d. Click the OTP token.
   e. Click **Assign Token**.
   f. Reset the OTP token by getting three values.
3. Configure AccessAssistant.
   a. Log on to AccessAdmin.
   b. Click **Authentication service policies** under **System**.
   c. Select **AccessAssistant**.
   d. Click **Move to enterprise authentication services**.
   e. Click **AccessAssistant** under **Enterprise authentication services**.
   f. Click **Authentication Policies**.
   g. Under **Authentication modes to be supported**, select **Password**, **MAC**, **OTP (OATH)**, and **OTP (time-based)**.
   h. Click **Update**.
   i. Scroll up the page and click **Authentication Services**.
   j. Under **ActiveCode-enabled Authentication Services**, select **AccessAssistant**.
   k. Type the user name in the text box at the right.
   l. Click **Add Account**.
   m. Navigate to **User Policy Templates** > **New template** > **Create new policy template** > **Authentication Policies**.
   n. Set **Enable Mobile ActiveCode authentication** to **Yes**.
4. Configure the system policy.
   a. In AccessAdmin, navigate to **System** and click **System Policies**.
   b. Click **AccessAssistant and Web Workplace Policies**.
   c. Under **Default second authentication factor forAccessAssistant and Web Workplace**, select **OTP**.
   d. Click **Update**.

## Configuring OTP (VASCO)

IBM Security Access Manager for Enterprise Single Sign-On supports OTP authentication by VASCO. Configuring the OTP settings by VASCO involves uploading the files to the IMS Server, registering the user in AccessAdmin, and applying policies.

## Procedure

1. Upload the VASCO files to the IMS Server.
   a. Put the VASCO-support-1.x.y.jar in <IMS Installation Folder>\ims\WEBINF\lib.
   b. Log on to the WebSphere Administrator Console.
   c. Click **Resources** > **Resource Adapters** > **Resource adapters** > **IBM Security Access Manager for Enterprise Single Sign-On IMS Native Library Invoker J2C Resource**
   d. Add aal2wrap.jar in Classpath.
   e. In Native library path, give the full path to the folder containing aal2sdk.DLL.
   f. Click **OK** to save settings.
   g. Restart the WebSphere Application Server.
   h. Navigate to <IMS install directory> bin.
   i. Edit setupcmdline.bat and point it to the right WebSphere Application Server profile.
   j. Save and exit the application.
   k. Run the uploaddpx.bat file by following this format: uploaddpx <was admin> <was password> -d <VASCO folder where the dpx file is located> --encryptkey <key>. The key is located in the VASCO folder. For <VASCO folder where the dpx file is located>, you must use backslash.
2. Configure the OTP user in AccessAdmin.
   a. Log on to AccessAdmin.
   b. Search for your OTP user and select it.
   c. Click OTP Token Assignment.
   d. Select a VASCO token.
   e. Click **Assign Token**.
3. Configure AccessAssistant.
   a. In AccessAdmin, click **Authentication service policies** under **System**.
   b. Select **AccessAssistant**.
   c. Click **Move to enterprise authentication services**.
   d. Click **AccessAssistant** under **Enterprise authentication services**.
   e. Click **Authentication Policies**.
   f. Under **Authentication modes to be supported**, select **Password**, **MAC**, **OTP (OATH)**, **OTP**, **OTP (time-based)**.
   g. Click **Update**.
   h. Scroll up the page and click **Authentication Services**.
   i. Under **ActiveCode-enabled Authentication Services**, select **AccessAssistant**.
   j. Type the user name in the text box at the right.
   k. Click **Add Account**.
   l. Navigate to **User Policy Templates** > **New template** > **Create new policy template** > **Authentication Policies**.
   m. Set **Enable Mobile ActiveCode authentication** to **Yes**.
4. Configure the system policy.
   a. In AccessAdmin, navigate to **System** and click **System Policies**.
   b. Click **AccessAssistant and Web Workplace Policies**.

c. Under **Default second authentication factor for AccessAssistant and Web Workplace** , select **OTP**.
d. Click **Update**.

## Configuring MAC

Mobile ActiveCodes are one-time passwords that are randomly generated, event-based, and delivered through a secure second channel like email. You can configure MAC support so that users can use MAC as their authentication factor.

### Before you begin

Make sure that the following components are installed and configured:

- IMS Server
- WebSphere Application Server

### Procedure

1. Configure the IMS Configuration Utility.
   a. Log on to the IMS Configuration Utility.
   b. Navigate to **ActiveCode deployment**.
   c. Under **Allowed ActiveCode client IPs**, add your IMS Server address.
   d. Under **OTP token reset window**, set it to 1000.
   e. Under **Use MAC-only registration of users**, set to true.
   f. Click **Update**.
   g. Navigate to **Advanced settings** and click **Message connectors**.
   h. Select **SMTP Messaging Connector**.
   i. Click **Configure**.
   j. Type a text under **Message Connector Name**. For example, `emailsender`.
   k. Type a text under **Address Attribute Name**. For example, `emailAddress`.
   l. Type the **SMTP server URI**.
   m. Type an email address under **SMTP from address**.
   n. Type the **SMTP from friendly name**.
   o. Click **Add**.
   p. Restart IMS Server.
2. Configure AccessAssistant.
   a. Log on to AccessAdmin.
   b. Click **Authentication service policies** under **System**.
   c. Select **AccessAssistant**.
   d. Click **Move to enterprise authentication services**.
   e. Click **AccessAssistant** under **Enterprise authentication services**.
   f. Click **Authentication Policies**.
   g. Under **Authentication modes to be supported**, select **Password**, **MAC**, **OTP (OATH)**, **OTP**, **OTP (time-based)**.
   h. Click **Update**.
3. Configure MAC for the user.
   a. Search for the user in AccessAdmin.
   b. Click the user.
   c. Click **Authentication Policies**.

d. Set **Enable Mobile ActiveCode authentication** to Yes.
e. Click **Update**.
f. Scroll up the page and click **Authentication Services**.
g. Under **ActiveCode-enabled Authentication Services**, select **AccessAssistant**.
h. Type the user name in the text box at the right.
i. Click **Add Account**.
j. Click **Back to profile** on the top of the page.
k. Under **Mobile ActiveCode email address**, enter the email address where the user can receive the MAC.
l. Under **Mobile ActiveCode preference 1**, type the Message Connector Name. In the previous example, the name is `emailsender`.
m. Click **Update**.

4. Configure the system policy.
   a. In AccessAdmin, navigate to **System** and click **System Policies**.
   b. Click **AccessAssistant and Web Workplace Policies**.
   c. Under **Default second authentication factor for AccessAssistant and Web Workplace**, select **MAC**.
   d. Click **Update**.

## Configuring MAC-only registration of users

You can configure settings in the IMS Configuration Utility if you want MAC-only registration of users.

### Procedure

1. Log on to the IMS Configuration Utility..
2. Select **Basic Settings** > **ActiveCode Deployment**.
3. Set **Use MAC-only registration of users** to **true**.
4. Set the **The ActiveDirectory attribute to be displayed for MAC-only registration of users**, with the Active Directory attribute.
5. Set **Search filter used for MAC-only registration of users UI** to the filter for the user search facility during user registration.
6. Click **Update**.

## About RADIUS authentication

Users must authenticate with an OTP if they want to use the RADIUS authentication server. If the OTP is not configured, the authentication reverts to LDAP.

An enterprise application that uses OTP tokens for authentication prompts the user for a user name and password. The password can be the user password, or an application password.

For the second factor, the enterprise application can be configured to authenticate users with:

- Only OTP provided by a token
- Either OTP provided by a token or MAC

You can also configure a bypass option, in case the user loses the OTP token or the mobile phone for receiving MAC.

The bypass code might be configured among any of the following options:

- Authorization code and password
- Authorization code and enterprise account password
- Authorization code and secret

**Note:** The OTP token deployment is only applicable to the IMS Server.

## Configuring OTP token policy settings

Configure the OTP policy settings if you want your users to authenticate on AccessAssistant and Web Workplace.

### User policy settings

Use AccessAdmin to configure the user policy settings for AccessAssistant and Web Workplace. The user policy settings include whether to allow access to the Wallet, whether to require second factor authentication, and whether to display the personal authentication services in AccessAssistant and Web Workplace.

1. Log on to AccessAdmin.
2. Under **User Policy Templates**, select **New Template** > **AccessAssistant and Web Workplace Policies**.
3. Complete the following fields:

| Option | Description |
|---|---|
| Allow access to Wallet from AccessAssistant and Web Workplace | Specify whether Wallet access is enabled. |
| Second factor authentication required for AccessAssistant and Web Workplace | Specify whether second factor authentication is required or not. |
| Display personal authentication services in AccessAssistant and Web Workplace | Specify whether to display personal authentication services. |

4. Click **Add**.

### System policy settings

Use AccessAdmin to configure system policy settings of AccessAssistant and Web Workplace. The system policy settings include enabling automatic sign-on to applications, enabling editing of user profiles, and password display option in AccessAssistant.

1. Log on to AccessAdmin.
2. Under **System**, select **System policies** > **AccessAssistant and Web Workplace Policies**.
3. Complete the following fields:

| Option | Description |
|---|---|
| Enable automatic sign-on to applications in AccessAssistant | Specify if you want to automate sign-on to applications |
| Enable editing of user profile in AccessAssistant and Web Workplace | Specify if you want to change profiles of users |

| Option | Description |
| --- | --- |
| Interval, in minutes, for periodic synchronization of AccessAssistant and Web Workplacewith IMS Server | Specify the number of minutes where synchronization with IMS Server takes place |
| Password display option in AccessAssistant | Specify how the passwords are displayed |
| Default second authentication factor for AccessAssistant and Web Workplace | Specify what second authentication factor is used |
| Enable unlocking of account by user in AccessAssistant and Web Workplace | Specify whether unlocking of accounts is enabled inAccessAssistant and inWeb Workplace |

4. Click **Update**.

### Authentication service policy settings

Use AccessAdmin to configure the different policy settings for both enterprise and personal authentication services.

1. Log on to AccessAdmin.
2. Under **System**, select **Authentication service policies**.
3. Make the necessary changes under **Enterprise authentication services** and **Personal authentication services**.

### Application policy settings

Use AccessAdmin to configure the different policy settings for your applications.

1. Log on to AccessAdmin.
2. Under **System**, select **Application policies**.
3. Choose an application.
4. Make the necessary changes under **Application Policies**.
5. Click **Update**.

## Advanced settings for OATH-based OTPs

If your organization uses OATH-based OTPs, you can configure the advanced settings in the IMS Configuration Utility.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Select **ActiveCode Deployment**.
3. Complete the following fields:

| Option | Description |
| --- | --- |
| **OTP Look-Ahead Number** | An OATH-based OTP token might not be completely in-sync with the IMS Server if the user:<br>• presses the **OTP token** button and<br>• does not use the displayed OTP for authentication<br><br>This configuration key specifies the number of consecutive button presses that the user can make before the OTP token is reset (resynchronized). The default value is `25`. |
| **OTP token reset window** | When an OATH-based OTP token is reset, the IMS Server attempts to resynchronize with the OTP token. The IMS Server computes a series of consecutive OTPs until it finds a match with the three consecutive OTPs generated by the OTP token.<br><br>This configuration key specifies the maximum number of OTPs that the IMS Server tries during a single reset attempt.<br><br>If the IMS Server fails to reset an OTP token, the number must be increased. The default value is `100`. |

4. Restart the IMS Server.

# Chapter 6. Configuring a secure deployment

Secure the IBM Security Access Manager for Enterprise Single Sign-On deployment and related components to mitigate potential security risks. You must secure the deployment before publishing in a production environment.

You can secure the application-tier through the following tasks:

- "Removing sample WebSphere Application Server servlets and applications"
- "Securing access to configuration data"
- "Setting a limit on logon attempts" on page 88

You can secure the Web-tier through the following tasks:

- "Restricting HTTP connections" on page 88
- "Disabling directory browsing" on page 89

**Tip:** For more information about advanced security and hardening, see *WebSphere Application Server Security advanced security hardening* http://www.ibm.com/developerworks/websphere/techjournal/1004_botzum/1004_botzum.html

## Removing sample WebSphere Application Server servlets and applications

You must verify that there are no sample WebSphere Application servlets or applications installed on a production application server.

### Procedure

1. Log on to the WebSphere Administrative Console.
2. Click **Applications** > **Application Types** > **WebSphere enterprise applications**.
3. Select the check box for each sample or demo application.

   **Note:** If the IMS Server is already deployed on the WebSphere Application Server, the IMS Server applications are `ISAMESSOIMS` and `ISAMESSOIMSConfig`. These are not sample applications.
4. Click **Uninstall**.
5. Click **OK**.
6. In the messages box, click **Save**.

## Securing access to configuration data

You must restrict all access to the WebSphere Application Server configuration folders and key files to Administrators only. See your operating system guides for more details.

Make sure that the following folders and files are protected.

**Server configuration folders**

Network deployment: `<was_home>\profiles\Dmgr01\config\tamesso`

Standalone: `<was_home>\profiles\AppSrv01\config\tamesso`

**Key store files**

Network deployment: <was_home>\profiles*Dmgr01*\config\cells\<cell_name>\TAMESSOIMSKeystore.jks

Standalone: <was_home>\profiles*AppSrv01*\config\cells\<cell_name>\TAMESSOIMSKeystore.jks

## Setting a limit on logon attempts

You can set up an account lock out threshold for unsuccessful and non-certificate online logon attempts. An account lock out threshold does not enable a user account if malicious actions are launched against that account. By default, a maximum account lock out threshold is not configured.

### Procedure

1. Log on to the IMS Configuration Utility.
2. Click **User authentication** > **Logon**.
3. Specify a number in **Maximum consecutive failed non-certificate online login attempts**. This number represents the number of wrong logon attempts before the account is not enabled.
4. Restart the IMS Server.

## Restricting HTTP connections

You can use the IBM HTTP Server *mod_rewrite* module to restrict HTTP connections only to specific pages.

### About this task

SOAP and web traffic between the IMS Server and IBM HTTP Server occur over a secure HTTPS connection. HTTP is used only for the initial distribution of trusted certificates to the end points. After all trusted certificates are distributed to the endpoints, you can block the HTTP port. You can then redirect other HTTP requests to a secure HTTPS connection.

### Procedure

1. Log on to the WebSphere Administrative Console.
2. Click **Servers** > **Server Types** > **Web servers**.
3. Choose the Web server.
4. In **Additional Properties**, click **Configuration File**.
5. Add the following lines to the web server configuration file.
   - **If standard HTTP and HTTPS ports are used:**

     ```
     LoadModule rewrite_module modules/mod_rewrite.so
     <VirtualHost *:80>
     RewriteEngine on
     RewriteCond %{REQUEST_URI} !
     ^/ims/services/encentuate\.ims\.service\.DownloadService$
     RewriteRule ^/(.*) https://server_name/$1 [L,R] </VirtualHost>
     ```

     – server_name: Replace server name with your server name.
   - **If non-standard HTTP and HTTPS ports are used:**

     ```
     LoadModule rewrite_module modules/mod_rewrite.so
     <VirtualHost *:port_number>
     RewriteEngine on
     ```

```
RewriteCond %{REQUEST_URI} !
^/ims/services/encentuate\.ims\.service\.DownloadService$
RewriteRule ^/(.*) https://server_name/$1 [L,R] </VirtualHost>
```

- port_number Replace the port number with the custom HTTP or HTTPS port number.
- server_name Replace the server name with your server name.

6. Click **OK**.

## Disabling directory browsing

You can choose not to enable the directory traversal option in the IBM HTTP Server `httpd.conf` configuration file on the web server.

### About this task

If the remote IBM HTTP Server administrator permissions are granted in the WebSphere Application Server, you can also edit `httpd.conf` from the administrative console. For deployments with multiple web servers, you must apply the same change on each web server.

### Procedure

1. Log on to the WebSphere Administrative Console.
2. Click **Servers** > **Server Types** > **Web servers**.
3. Choose the Web server.
4. In **Additional Properties**, click **Configuration File**.
5. Locate the following **Options** directive with the **Indexes** parameter.

   ```
   Options Indexes FollowSymLinks
   ```

6. Replace the **Indexes** parameter with **-Indexes**.

   ```
   Options -Indexes FollowSymLinks
   ```

7. Click **OK**.
8. In the messages box, click **Save**.
9. Restart the IBM HTTP Server.

# Appendix A. Logging on to AccessAdmin

AccessAdmin is a web-based administrative interface of the IMS Server. Log on to AccessAdmin to manage users, policies, authentication factors, and reports.

## Procedure

1. Navigate to AccessAdmin.
   - If you use a load balancer, access
     `https:// <loadbalancer_hostname>:<ihs_ssl_port>/admin.`
   - If you do not use a load balancer, access
     `https:// <ims_hostname>:<ihs_ssl_port>/admin.`
2. Select a language for AccessAgent that is consistent with the location for which you want to apply policies.
3. Enter your administrator user name and password.
4. Click **Log on**.

# Appendix B. Setting up policy templates

One way to set up machine policies is by using the Setup Assistant. This task is optional. You can manually create a Machine Policy Template if you prefer.

## Procedure

1. Log on to AccessAdmin.
2. Click **Setup assistant**.
3. Click **Begin**.
4. Follow the instructions in the **Setup assistant** wizard.

# Appendix C. Automatically assigning User Policy Templates to new users

You can automatically assign User Policy Templates to new users so that you do not have to manually apply a User Policy Template every time a new user is registered.

## About this task

Use AccessAdmin and the IMS Configuration Utility to assign policy templates to new users during sign-up. In this procedure, **department** is used as an attribute in steps 1c and 3c.

## Procedure

1. Navigate to `C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\config\tamesso\config\EnterpriseDirectoryConfiguration.xml`.
   a. Change the value of `<isInitialized>false </isInitialized>` to `true`.
   b. Add `<BasicAttribute> <name>department</name></BasicAttribute>` under `attributesTOBESupported`.
   c. Add `<BasicAttribute><name>department</name></BasicAttribute>` under `entityAttributesToFetch`.
2. Modify the `encentuate.ims.ui.templateAsgAttribute` entry in the IMS Server configuration file.
   a. Log on to the IMS Configuration Utility.
   b. Select **Advanced Settings** > **AccessAdmin** > **User Interface** > **Policy assignment attribute**.
   c. Set **Policy assignment attribute** to `department`. In this example, specify **department** to be consistent with the example in step 1c. The **Attribute value** can be Finance, Marketing, or other attributes that are available in Active Directory.
   d. Restart the IMS Server.
3. Configure the mapping between the user attribute values and the policy template names in AccessAdmin.
   a. Log on to AccessAdmin.
   b. Select **User Policy Templates** > **Template assignments**.
   c. Specify the **Attribute value** and **Template for new users**.
   d. Click **Assign**.

# Appendix D. Excluding machine attributes

You can exclude computer attributes in the IMS Server. For example, if your computer IP address changes constantly, you can choose not to enable it to avoid frequent updates in the IMS Server.

## Procedure

1. Log on to the IMS Configuration Utility.
2. Navigate to **Advanced settings** > **IMS Server** > **Miscellaneous** > **Machine attributes to exclude from the IMS Server**.
3. Select any of the attributes in the drop-down box:
   - **ipAddress** (default value)
   - **hostName**
   - **aaVersion**
   - **machineGroups**
   - **machineTag**
4. Click **Add**.
5. Click **Update**.

# Appendix E. Configuring JMX support

You can use JMX to monitor the IMS Server beans - **ImsStateMbean** and **ImsConfigMBean**. You can use JConsole to connect to the WebSphere Application Server and retrieve the monitoring results.

## About this task

JConsole is located at <*was_home*>\java\bin\. For example, C:\Program Files\IBM\WebSphere\AppServer\java\bin\.

## Procedure

1. Navigate to the <*was_home*>\profiles\<*profile_name*>\properties folder. For example, C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01.
2. Open the sas.client.props file with any text editor.
3. Set the following values for these variables:
   - **com.ibm.CORBA.loginSource** =properties
   - **com.ibm.CORBA.loginUserid** = <*WAS Admin user ID*>. For example, wasadmin.
   - **com.ibm.CORBA.loginPassword** = <*WAS Admin password*>.
4. Restart the WebSphere Application Server.
5. Open the command-line tool.
6. Navigate to the <*was_home*>\bin.
7. Connect to the WebSphere Application Server with the following command:

   ```
   jconsole -J-Djava.class.path="<was_home>\java\lib\tools.jar";
   "<was_home>\java\lib\jconsole.jar";
   "<was_home>\runtimes\com.ibm.ws.admin.client_7.0.0.jar"
   -J-Dcom.ibm.CORBA.ConfigURL="file:<was_home>\profiles\
   <profile_name>\properties\sas.client.props"
   -J-Dcom.ibm.SSL.ConfigURL="file:<was_home>\profiles\
   <profile_name>\properties\ssl.client.props"
   service:jmx::iiop://<was_hostname>:BOOTSTRAP_ADDRESS/jndi/JMXConnector
   ```

   For example:

   ```
   jconsole -J-Djava.class.path="C:\Program Files\IBM\WebSphere\AppServer\
   java\lib\tools.jar";
   "C:\Program Files\IBM\WebSphere\AppServer\java\lib\jconsole.jar";
   "C:\Program Files\IBM\WebSphere\AppServer\runtimes\
   com.ibm.ws.admin.client_7.0.0.jar"
   -J-Dcom.ibm.CORBA.ConfigURL="file:C:\Program Files\IBM\WebSphere\AppServer\
   profiles\AppSrv01\properties\sas.client.props"
   -J-Dcom.ibm.SSL.ConfigURL="file:C:\Program Files\IBM\WebSphere\AppServer\
   profiles\AppSrv01\properties\ssl.client.props"
   service:jmx:iiop://localhost:2809/jndi/JMXConnector
   ```

# Appendix F. Planning worksheet

Use the planning worksheet as a reference for the default and sample values during the installation and configuration of the IBM Security Access Manager for Enterprise Single Sign-On server and other required software.

## Installation directories and other paths

The following table contains the different path variables used throughout the guide and the corresponding default values. In some cases, the variable name matches the name of an environment variable that is set in the operating system. For example, %TEMP% represents the environment variable %TEMP% for Windows.

**Note:** When installing the IBM Security Access Manager for Enterprise Single Sign-On on Windows systems, the default directory is typically the system program files directory `<system drive>:\Program Files\IBM\`, where the system drive is typically a C: drive. However, you can specify that IBM Security Access Manager for Enterprise Single Sign-On is installed on a disk drive other than the C: drive.

| Path variable | Component | Default directory |
|---|---|---|
| *<aa_home>* | AccessAgent | `C:\Program Files\IBM\ISAM ESSO\AA` |
| *<as_home>* | AccessStudio | `C:\Program Files\IBM\ISAM ESSO\AA\ECSS\AccessStudio` |
| *<db_home>* | DB2 | `C:\Program Files\IBM\SQLLIB` |
| *<ihs_home>* | IBM HTTP Server | `C:\Program Files\IBM\HTTPServer` |
| *<ims_home>* | IBM Security Access Manager for Enterprise Single Sign-On IMS Server | `C:\Program Files\IBM\ISAM ESSO\IMS Server` |
| *<jvm_home>* | Java Virtual Machine | `C:\Program Files\Java\jre1.5.0_11` |
| *<updi_home>* | IBM Update Installer for WebSphere Application Server | `C:\Program Files\IBM\WebSphere\ UpdateInstaller` |
| *<was_home>* | WebSphere Application Server | `C:\Program Files\IBM\WebSphere\ AppServer` |
| *<was_dmgr_home>* | WebSphere Application Server Network Deployment deployment manager profile | `C:\Program Files\IBM\WebSphere\ AppServer\profiles\Dmgr01` |
| *<%TEMP%>* | Windows directory for temporary files | When logged on as `Administrator`, `C:\Documents and Settings\ Administrator\Local Settings\Temp` |
| *<%PROGRAMFILES%>* | Windows directory for installed programs | `C:\Program Files` |

## Host names and ports

The following table contains the different variable host names and port numbers used throughout the guide.

| Variable | Description |
|---|---|
| *<was_hostname>* | Name of the host where the WebSphere Application Server is installed. |
| *<dmgr_hostname>* | Name of the host where the WebSphere Application Server Network Deployment Manager is installed. |
| *<ihs_hostname>* | Name of the host where the IBM HTTP Server is installed. |
| *<loadbalancer_hostname>* | Name of the host where the load balancer is installed. |
| *<ims_hostname>* | Name of the host where the IMS Server is installed. |
| *<ihs_ssl_port>* | IBM HTTP Server SSL port number. |
| *<admin_ssl_port>* | Administrative console secure port number. |

## URLs and addresses

The following table contains the different URLs and addresses used throughout the guide. The values vary depending on whether you are using WebSphere Application Server stand-alone or WebSphere Application Server Network Deployment.

| Description | Format | Example value |
|---|---|---|
| Integrated Solutions Console (WebSphere Application Server administrative console) | • If you are using WebSphere Application Server stand-alone:<br>*https://<was_hostname>:<admin_ssl_port>/ibm/console*<br>• If you are using WebSphere Application Server Network Deployment:<br>*https://<dmgr_hostname>:<admin_ssl_port>/ibm/console* | `https://localhost:9043/ibm/console`<br>or<br>`http://localhost:9060/ibm/console` |
| IMS Configuration Wizard | • If you are using WebSphere Application Server stand-alone:<br>*https://<was_hostname>:<admin_ssl_port>/front*<br>• If you are using WebSphere Application Server Network Deployment:<br>*https://<dmgr_hostname>:<admin_ssl_port>/front* | `https://localhost:9043/front` |
| IMS Configuration Utility | • If you are using WebSphere Application Server stand-alone:<br>*https://<was_hostname>:<admin_ssl_port>/webconf*<br>• If you are using WebSphere Application Server Network Deployment:<br>*https://<dmgr_hostname>:<admin_ssl_port>/webconf* | `https://localhost:9043/webconf` |

| Description | Format | Example value |
|---|---|---|
| AccessAdmin | • If you are using a load balancer:<br>*https://<loadbalancer_hostname>:<ihs_ssl_port>/admin*<br>• If you are not using a load balancer:<br>*https://<ims_hostname>:<ihs_ssl_port>/admin*<br>• If webserver is configured properly:<br>*https://ims_hostname>/admin* | • `https://imsserver:9443/admin`<br>• `https://imsserver/admin` |
| AccessAssistant | • If you are using a load balancer:<br>*https://<loadbalancer_hostname>:<ihs_ssl_port>/aawwp*<br>• If you are not using a load balancer:<br>*https://<ims_hostname>:<ihs_ssl_port>/aawwp* | `https://imsserver:9443/aawwp` |
| Web Workplace | • If you are using a load balancer:<br>*https://<loadbalancer_hostname>:<ihs_ssl_port>/aawwp?isWwp=true*<br>• If you are not using a load balancer:<br>*https://<ims_hostname>:<ihs_ssl_port>/aawwp?isWwp=true* | `https://imsserver:9443/aawwp?isWwp=true` |

## Users, profile names, and groups

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

| Variable | Description | Example value |
|---|---|---|
| *<profile name>* | WebSphere Application Server profile name.<br><br>The profile name is defined when creating profiles for WebSphere Application Server with the `manageprofiles` command-line tool or graphical Profile Management tool. | • If you are using WebSphere Application Server stand-alone:<br>`<AppSrv_profilename>`<br>• If you are using WebSphere Application Server Network Deployment:<br>– Deployment manager:<br>`<Dmgr_profilename>`<br>– Node<br>`<Custom_profilename>` |
| *<WAS Admin user ID>* | WebSphere administrator ID created during the installation of WebSphere Application Server. | `wasadmin` |
| *<IHS Admin user ID>* | HTTP Server administrator user ID created during the installation of the IBM HTTP Server. | `ihsadmin` |

| Variable | Description | Example value |
|---|---|---|
| *<DB2 Admin user ID>* | DB2 administrator service user ID for Microsoft Windows created during the installation of IBM DB2. | `db2admin` |
| *<IMS Admin user ID>* | IBM Security Access Manager for Enterprise Single Sign-On administrator.<br><br>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.<br><br>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`<br><br>`lookupusr` |
| *<VA non-root user ID>* | General user account for virtual appliance deployments. Created during virtual appliance activation and deployment. | `virtuser` |
| *<VA root user ID>* | Root user account for virtual appliance deployments. Used to log on to virtual appliance during boot up. | `root` |

## Installing IBM DB2

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

| Parameter | Default Value |
|---|---|
| Installation file | Workgroup Server Edition (limited use)<br>• `DB2_97_limited_CD_Win_x86.exe`<br>• `DB2_97_limited_CD_Win_x86-64.exe`<br>Enterprise Server Edition<br>• `DB2_ESE_V97_Win_x86.exe`<br>• `DB2_ESE_V97_Win_x86-64.exe`<br>**Note:** The installation files might vary according to the version and edition of DB2. |
| Installation directory | `C:\Program Files\IBM\SQLLIB` |
| *User information for the DB2 Administration Server* | |
| Domain | `None - use local user account` |
| User name | `db2admin` |

| Parameter | Default Value |
|---|---|
| Password | |
| DB2 instance | `Create the default DB2 instance` |
| Partitioning option for the default DB2 instance | `Single partition instance` |
| DB2 tools catalog | `None` |
| Set up your DB2 Server to send notifications | `No` |
| Enable operating system security | `Yes` |
| *DB2 administrators group* | |
| Domain | `None` |
| Group Name | `DB2ADMNS`<br>**Note:** This value is an example. You can specify your own value. |
| *DB2 users group* | |
| Domain | `None` |
| Group Name | `DB2USERS`<br>**Note:** This value is an example. You can specify your own value. |
| Port number | `50000` |

## Creating the IMS Server database

The following table contains the values that you must specify to create the IMS Server database.

| Parameter | Default Value |
|---|---|
| Database name | `imsdb`<br>**Note:** This value is an example. You can specify your own value. |
| Default path | `C:\` |
| Alias | `imsdb`<br>**Note:** This value is an example. You can specify your own value. |
| Comment | `DB for IMS`<br>**Note:** This value is an example. You can specify your own value. |
| Let DB2 manage my storage (automatic storage) | `Yes` |
| Default buffer pool and table space page size | `8K` |
| Use the database path as a storage path | `Yes` |
| Code set | `UTF-8` |
| Collating sequence | |
| Region | Default |

## Creating a DB2 user manually

The following table contains the values that you must specify, if you are creating a separate database user for IBM Security Access Manager for Enterprise Single Sign-On.

| Parameter | Default Value |
|---|---|
| DB2 user | `imsdb2admin` |

| Parameter | Default Value |
| --- | --- |
| Administrative privileges | • Connect to database<br>• Create tables<br>• Create packages |

## Installing WebSphere Application Server

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

| Parameter | Default Value |
| --- | --- |
| Installation file | `launchpad.exe` |
| Installation directory | `<was_home>` |
| WebSphere Application Server Environment | (None)<br><br>**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:<br><br>For WebSphere Application Server stand-alone product deployments<br>• Application server<br><br>For WebSphere Application Server Network Deployment (cluster)<br>• Deployment Manager<br>• Custom |
| Enable Administrative Security | `Yes` |
| WebSphere Administration user name | `wasadmin` |
| Deployment Manager profile name | `<Dmgr_profilename>` |
| Custom profile name (node) | `<Custom_profilename>` |
| Application server profile name | `<AppSrv_profilename>` |
| Cell name | `<Server01Node01Cell01>` |
| Deployment Manager node name | `<Server01Cell01>` |
| Application server node name | `<Server01Node01>` |
| HTTP server installation location | `<ihs_home>` |
| HTTP port | `80` |
| HTTP admin server port | `8080` |

## Installing IBM Update Installer for WebSphere software installation

The following table contains the values that you must specify when installing the IBM Update Installer for WebSphere Software Installation.

| Parameter | Default Value |
| --- | --- |
| Installation file | `install.exe` |
| Installation directory | `C:\Program Files\IBM\WebSphere\UpdateInstaller` |

## Installing the latest WebSphere Application Server fix pack

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

| Parameter | Default Value |
|---|---|
| Installation file | • 7.0.0-WS-WAS-WinX32-FP000000X.pak<br>• 7.0.0-WS-WAS-WinX64-FP000000X.pak |
| Installation directory | <was_home> |
| Maintenance Operation Selection | Install maintenance package |
| Maintenance package directory path | <updi_home>\maintenance |

## Installing IBM HTTP Server

The following table contains the values that you must specify when installing the IBM HTTP Server.

| Parameter | Default Value |
|---|---|
| Installation file | launchpad.exe |
| Installation directory | <ihs_home> |
| IBM HTTP Server HTTP Port | 80 |
| IBM HTTP Server HTTP Administration Port | 8008 |
| Run IBM HTTP Server as a Windows Service | Yes |
| Run IBM HTTP Administration as a Windows Service | Yes |
| Log on as a local system account | Yes |
| Log on as a specified user account | No |
| User name | Administrator<br>**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<br>**Note:** WebSphere Application Server account for administering IBM HTTP Server and the IBM HTTP Server plug-in. |
| IBM HTTP Server administration server authentication password | |
| Install IBM HTTP Server Plug-in for IBM WebSphere Application Server | Yes |
| Web server definition | <webserver1> |
| Host name or IP address for the Application Server | IMS82.samesso.ibm.com |

## Installing the latest IBM HTTP Server fix pack

The following table contains the values that you must specify when installing the latest IBM HTTP Server fix pack.

| Parameter | Default Value |
|---|---|
| Installation file | • 7.0.0-WS-IHS-WinX32-FP000000X.pak<br>• 7.0.0-WS-IHS-WinX64-FP000000X.pak |
| Installation directory | <ihs_home> |
| Maintenance Operation Selection | Install maintenance package |
| Maintenance package directory path | <was_home>\UpdateInstaller\maintenance |

## Configuring the IBM HTTP Server

The following table contains the values that you must specify when configuring the IBM HTTP Server to work with the WebSphere Application Server.

| Parameter | Default Value |
|---|---|
| Windows batch file | configure<webserver1>.bat |
| Original Location | <ihs_home>\Plugins\bin |
| Target Location | <was_home>\bin |
| com.ibm.SOAP.requestTimeoutproperty | 6000 |
| *Remote Web server management* | |
| Port | 8008 |
| User name | ihsadmin |
| Password | |
| Use SSL | No |
| Refresh configuration interval | 60 seconds |
| Plug-in configuration file name | plugin-cfg.xml |
| Plug-in keystore file name | plugin-key.kdb |
| Plug-in configuration directory and file name | <ihs_home>\Plugins\config\<webserver1>\ plugin-cfg.xml |
| Plug-in keystore directory and file name | <ihs_home>\Plugins\config\<webserver1>\ plugin-key.kdb |
| Automatically generate the plug-in configuration file | Yes |
| Automatically propagate the plug-in configuration file | Yes |
| Log file name | • <ihs_home>\Plugins\logs\<webserver1>\ http_plug-in.log<br>• <ims_home>\ISAM_E-SSO_IMS_Server_InstallLog.log |
| Log level | Error |

## Installing IMS Server

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

| Parameter | Default Value |
| --- | --- |
| Installation file | `imsinstaller_8.2.0.0.x.exe` |
| Installation folder | `<ims_home>` |
| Deploy IMS Server to WebSphere Application Server | • `Yes` - automatically deploys the IMS EAR file to WebSphere Application Server<br>• `No` - you must manually deploy the IMS EAR file to WebSphere Application Server |
| WebSphere Application Server Administration Security enabled | `Yes` |
| Administrative user name | `wasadmin`<br>**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 | • If you are using WebSphere Application Server stand-alone:<br>`<was_home>\profiles\ <AppSrv_profilename>\config\cells\ <Server01Cell01>\nodes\ <Server01Node01>\`<br>• If you are using WebSphere Application Server Network Deployment<br>`<was_home>\profiles\ <Dmgr_profilename>\config\cells\ <Server01Cell01>\` |
| SSL Trusted Java key store password | `WebAS` |
| SSL Java key store file | `key.p12` |
| SSL Java key store file location | • If you are using WebSphere Application Server stand-alone:<br>`<was_home>\profiles\ <AppSrv_profilename>\config\cells\ <Server01Cell01>\nodes\ <Server01Node01>\`<br>• If you are using WebSphere Application Server Network Deployment<br>`<was_home>\profiles\ <Dmgr_profilename>\config\cells\ <Server01Cell01>\` |
| SSL Java key store password | `WebAS` |
| WebSphere Application Server SOAP connector port | • For WebSphere Application Server stand-alone:<br>`8880`<br>• For WebSphere Application Server Network Deployment (deployment manager):<br>`8879` |

| Parameter | Default Value |
| --- | --- |
| SOAP connector port number location | • If you are using WebSphere Application Server stand-alone:<br>`<was_home>\profiles\<AppSrv_profilename>\logs\AboutThisProfile.txt`<br>• If you are using WebSphere Application Server Network Deployment<br>`<was_home>\profiles\<Dmgr_profilename>\logs\AboutThisProfile.txt` |
| IMS Server URL | Example: `https://localhost:9043/front`<br>• If you are using WebSphere Application Server stand-alone:<br>*https://<was_hostname>:<admin_ssl_port>/front*<br>• If you are using WebSphere Application Server Network Deployment:<br>*https://<dmgr_hostname>:<admin_ssl_port>/front* |

## Configuring the IMS Server

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

| Parameter | Default Value |
| --- | --- |
| JDBC provider name | `ISAM ESSO JDBC Provider` |
| Data source name | `ISAM ESSO IMS Server Data Source` |
| JNDI name | `jdbc/ims`<br>**Note:** The JNDI name is not editable. |
| J2C authentication data alias | `imsauthdata` |
| Create IMS Server database schema | `Yes` |
| Choose Database Type | • IBM DB2 Server<br>• Microsoft SQL Server<br>• Oracle Server |
| *Database Configuration - <database type>* | |
| Host Name | |
| Instance<br>**Note:** For Microsoft SQL Server only. | |
| Port | • For IBM DB2 Server: `50000`<br>• For Microsoft SQL Server: `1433`<br>• For Oracle Server: `1521` |
| Database Name<br>**Note:** For IBM DB2 only. | |
| SID<br>**Note:** For Oracle Server only. | |
| User Name | `db2admin` |
| User Password | |
| *Provide Root CA Details* | |

| Parameter | Default Value |
|---|---|
| Keystore name | `CellDefaultKeyStore` |
| Keystore password | |
| Root CA alias name | `root` |
| Fully qualified web server name | `web1.example.com` |
| *IMS Services URL* | |
| HTTPS port number | `443` |

## Configuring enterprise directory (LDAP or Active Directory)

The following table contains the values that you must specify when configuring the enterprise directory.

| Parameter | Default value |
|---|---|
| Host name | `ldapsvr.example.com` |
| Bind distinguished name | • For Active Directory:<br>`cn=lookupusr, cn=users,dc=team, dc=example, dc=com`<br>• For LDAP:<br>`cn=lookupusr, ou=users, o=example, c=us` |
| Base distinguished name | • For Active Directory:<br>`cn=users, dc=team, dc=example, dc=com`<br>• For LDAP:<br>`ou=users,o=example,c=us` |
| Domain | `team.example.com` |
| Port | `389` (without SSL)<br>`636` (with SSL) |

# Appendix G. Command-line interface reference

This section provides a list of different commands that you can use to configure the IMS Server.

Unless otherwise specified, the commands can be found in `<ims_home>\bin` directory.

Command-line tools are available in the following types:

- Windows batch scripts (`.bat` extension)
- Linux shell scripts (`.sh` extension)
- Jython script files (`.py` extension)

**Note:** Before you run the command-line tools, be sure to run the **`setupCmdLine`** tool to set the environment path.

**Important:** Run the command-line tools with administrator authority in Windows Vista, Windows 7 and Windows Server 2008 with Windows User Account Control (UAC) enabled. Run all Administrators with the Admin Approval Mode policy enabled.

Do the following steps to run the command-line tools:

1. Right-click a command prompt shortcut.
2. Click **Run As Administrator**.
3. Click **Continue** to proceed.

See the following commands for more information.



## cleanImsConfig command

Use this command to delete any existing IMS Server configurations such as certificates, database configurations. You can also use this command to reset the IMS Server to an unconfigured state.

### Syntax

`cleanImsConfig.sh <was_admin_name> <was_password>`

`cleanImsConfig.bat <was_admin_name> <was_password>`

### Description

To reset the IMS Server back to an unconfigured state, the command does the following tasks:

- Deletes IMS data sources.
- Deletes IMS keystore.
- Deletes enterprise directory connections.

  **Note:** The enterprise directory is not deleted. Only the IMS Server connection to enterprise directories are deleted.
- Replaces the SAM E-SSO config repository with a new config repository from the IMS installation directory.
- If the **cleanImsConfig** command is on a deployment manager node, it synchronizes all the nodes.

For a network deployment, run this command on the deployment manager node.

### Parameters

**<was_admin_name>**
Required parameter. Specify the WebSphere Application Server administrator name. For example, `wasadmin`.

**<was_password>**
Required parameter. Specify the WebSphere Application Server administrator password.

### Example

```
cleanImsConfig.sh wasadmin password

cleanImsConfig.bat wasadmin password
```

## deployIsamessoIms command

Use this command to deploy the IMS Server ISAMESSOIMS EAR file on the application server.

### Syntax

**deployIsamessoIms** *<was_admin_name> <was_admin_password>*

### Description

This command deploys the ISAMESSOIMS WebSphere Application Server EAR file as a WebSphere enterprise application.

### Parameters

**<was_admin_name>**
Required parameter. Specify the WebSphere Application Server administrator name. For example, `wasadmin`.

**<was_admin_password>**
Required parameter. Specify the WebSphere Application Server administrator password.

### Examples

```
deployIsamessoIms wasadmin password
```

## deployIsamessoImsConfig command

Use this command to deploy the IMS Server ISAMESSOIMSConfig EAR file on the application server.

### Syntax

deployIsamessoImsConfig.bat **<was_admin_name> <was_admin_password>**

### Description

Use this command to deploy the ISAMESSOIMSConfig EAR on the WebSphere Application Server as a WebSphere enterprise application. For a network deployment, you can deploy the ISAMESSOIMSConfig EAR on the deployment manager node.

### Parameters

**<was_admin_name>**
Required parameter. Specify the WebSphere Application Server administrator name. For example, wasadmin.

**<was_admin_password>**
Required parameter. Specify the WebSphere Application Server administrator password.

### Examples

```
deployIsamessoImsConfig wasadmin password
```

## exportImsConfig command

Use this command to export the IMS Server configuration to a Java Archive file.

### Syntax

exportImsConfig <*was_admin_name*> <*was_admin_password*> --outputFile=<*output_filename_path*>

### Description

The JAR file contains configurations about the target servers, database locations, and security certificates.

### Parameters

**<was_admin_name>**
Required parameter. Specify the WebSphere Application Server administrator name. For example, wasadmin.

**<was_password>**
Required parameter. Specify the WebSphere Application Server administrator password.

**--outputFile**
Required parameter. Specify the output directory and JAR file name. Remember to include the JAR file name extension. For example, `c:/backup/myxImsConfig.jar`

### Examples

```
exportImsConfig wasadmin password --outputFile=c:/backup/myxImsConfig.jar
```

## managePolPriority command

Use this command to manage the priority or precedence of policies.

### Description

The **managePolPriority** command determines the priority or precedence of policies.

### Parameters

None.

### Examples

```
managePolPriority
```

## setupCmdLine command

Use this command to define the environment variables for the command line and scripts to run successfully.

### Description

This command enables scripts to run successfully and define the environment variables for the command line.

### Parameters

There are no parameters for the setupCmdLine tool.

### Examples

```
setupCmdLine
```

## upgradeSymCrypto command

Use this command to upgrade the symbolic cryptographic keys.

### Description

This command upgrades all symbolic cryptographic keys.

### Parameters

None.

### Examples

**upgradeSymCrypto**

## uploadDpx command

Use this command to upload Digipass tokens in a .DPX file to the IMS Server so that an entire batch of Digipass tokens is recognized.

### Description

You must upload the tokens before you use the Digipass tokens.

```
uploadDpx.bat [-i inputFileName] [-v] [--encryptKey encryptKey]
[-o outputFileName] [--error error-file] [-h] [-f folder]
[--overWrite option]
```

**uploadDpx.bat -i** *c:\digipass.dpx* **--overwrite** *true*

### Parameters

**-i** <*input file name*>
Specifies the path to the .DPX file, including the name of the .DPX file.

**--encryptKey** <*encryptKey*>
Specifies the encryption key for the .DPX file.

**-o, --output** <*outputFileName*>
Specifies the output file name to which debug and output information are printed.

**--error** <*error-file*>
Specifies the error output file name.

**-h, --help**
Prints the help message.

**-v, --version**
Prints the version number of the tool.

**-- overWrite** <*option*>
Specifies if the .DPX information in the IMS Server for existing tokens in the unassigned list is overwritten (not enabled by default). <option> can be either **true** or **false**.

If enabled, existing tokens such as tokens recognized by the IMS Server that do not display in the .DPX files are not modified.

For existing tokens in the unassigned list that are in the .DPX files, the .DPX information in the IMS Server is overwritten with the ones in the .DPX files.

**Note:** Use the --overWrite <option> command when tokens go out-of-sync.

### Examples

**uploadDpx.bat -i** *c:\digipass.dpx* **--overwrite** *true*

## uploadOath command

Use this command to upload a `.CSV` text file that contains serial numbers and OATH seeds to the IMS Server. Therefore, an entire batch of Authenex A-Key tokens is recognized.

### Description

Each Authenex A-Key token uses an OATH seed to generate an OTP. Before an A-Key token can be used, the serial number and OATH seed must be uploaded to the IMS Server. The command-line tool **uploadOath.bat** uploads a *comma-separated value* (`.CSV`) text file.

When uploaded, the tokens in the CSV file displays in the list of unassigned tokens on AccessAdmin.

### Parameters

**-i** <*inputFileName*>
Full path of the `.CSV` text file for uploading OATH data. For example `-i c:\input_tokens.csv`

Each row in the `.CSV` file is of the format

"*a*, *b*".

where

*a* is the Serial number of OATH token

*b* is the OATH seed of the OATH token.

**<serial number>, <OATH seed>**

**-o, --output <outputFileName>**
Specifies the output file name to which debug/output information is printed. For example

**-o** c:\output.log

**--error <error-file>**
Specifies the error output file name.

**-v, --version**
Prints the version number of the tool.

**-h, --help**
Prints the help message.

### Examples

**uploadOath -i** *c:\input.csv* **-o** c:\output.log

**uploadOath -v**

## uploadSync command

Use this command to upload batches of profile data in an XML format and to synchronize the configuration with the IMS Server.

### Description

This command uploads XML data into the IMS Server and synchronizes the IMS Server configuration.

### Parameters

None.

### Example

```
uploadSync
```

## vrfyLogs command

Use this command to verify the recorded logs.

### Description

This command verifies the logs recorded in IBM Security Access Manager for Enterprise Single Sign-On.

### Parameters

None.

### Examples

```
vrfyLogs
```

## Scripts for Virtual Appliance

This section contains a list of all scripts that are used for collecting logs, configuring and installing the Tivoli Common Reporting Tool, and resetting the Virtual Appliance.

See the following topics for more information.

- "collectLogs command"
- "configureTcrforIms command" on page 120
- "installTcr command" on page 120
- "resetImsVa command" on page 121

## collectLogs command

Use this command to collect logs from the ISAMESSO IMS Virtual Appliance.

### Description

The logs collected include product logs, settings, and Linux OS logs. Select the option to get the minimal set of logs. If this option is not set, all logs and settings are collected from the image.

### Parameters

None.

### Examples

```
sh collectLogs.sh [--minimal]
```

## configureTcrforIms command

Use this command to point the Tivoli Common Reporting Tool to the IMS Server database and to configure it to import reports.

### Description

This command configures the Tivoli Common Reporting Tool manually.

### Parameters

**--dbName** *db_name*
Specify the IMS Server database.

**--dbType** *db_type*
Specify the database type. *db_type* is one of the following:

- db2
- sqlserver
- oracle

**--dbHostname** *db_hostname*
Specify the host name.

**--dbPort** *db_port*
Specify the port number.

**--dbUserName** *db_username*
Specify the user name.

**--dbUserPassword** *db_user_password*
Specify the password.

### Examples

**sh configureTcrForIms.sh** --dbName *db_name* --dbType *db_type* --dbHostname *db_hostname* --dbPort *db_port* --dbUserName *db_username* --dbUserPassword *password*

## installTcr command

Use this command to install the Tivoli Common Reporting tool manually.

### Description

This command installs the Tivoli Common Reporting tool manually. The Administrator user name is set to the non-root account that is created during activation.

### Parameters

None.

### Examples

```
sh installTcr.sh [tcr-admin-password]
```

## resetImsVa command

Use this command to reset the IMS Virtual Appliance.

### Description

This command resets the IMS Virtual Appliance and deletes all configuration changes made during activation and post-activation.

### Parameters

None.

### Examples

```
sh resetImsVa.sh
```

# Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

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

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

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

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

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

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

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

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

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

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

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

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

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

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

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

## Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information; at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.


Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Other company, product, and service names may be trademarks or service marks of others.

# Glossary

**AccessAdmin.** A web-based management console that Administrators and Helpdesk officers use to administer the IMS Server and to manage users and policies.

**AccessAgent plug-in.** A piece of script, written in VBscript or Javascript, that is embedded within an AccessProfile to perform custom checking of conditions or to execute custom actions. It is used for extending the capability of an AccessProfile beyond the built-in triggers and actions.

**AccessAgent.** The client software that manages the identity of the user, authenticates the user, and automates single sign-on and sign-off.

**AccessAssistant.** The web-based interface that helps users to reset their passwords and retrieve their application credentials.

**AccessProfile widget / widget.** An independent AccessProfile that consists of pinnable states, which can be used to build another AccessProfile.

**AccessProfiles.** AccessAgent uses these XML specifications to identify application screens that it can perform single sign-on and automation.

**AccessStudio.** An application used by Administrators for creating and maintaining AccessProfiles.

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

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

**Account data item.** The user credentials required for logon.

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

**Account data.** The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

**Action.** In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

**Active Directory (AD).** A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

**Active Directory credentials.** The Active Directory user name and password.

**Active Directory password synchronization.** An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

**Active RFID (ARFID).** ARFID is both a second authentication factor and a presence detector. It can detect the presence of a user and AccessAgent can be configured to perform specific actions. In previous releases, it is called Active Proximity Badge.

**ActiveCode.** Short-lived authentication codes that are generated and verified by IBM Security Access Manager for Enterprise Single Sign-On. There are two types of ActiveCodes: Mobile ActiveCodes and Predictive ActiveCodes.

Mobile ActiveCodes are generated by IBM Security Access Manager for Enterprise Single Sign-On and dispatched to the mobile phone or email account of the user. Predictive ActiveCodes, or One Time Passwords, are generated from OTP tokens when a user presses its button.

Combined with alternative channels or devices, ActiveCodes provide effective second-factor authentication.

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

**Application policies.** A collection of policies and attributes governing access to applications.

**Application programming interface (API).** An interface that allows an application program written in a high-level language to use specific data or functions of the operating system or another program.

**Application.** One or more computer programs or software components that provide a function in direct support of a specific business process or processes. In AccessStudio, it is the system that provides the user interface for reading or entering the authentication credentials.

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

**Authentication factor.** The different devices, biometrics, or secrets required as credentials for validating digital identities. Examples of authentication

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

**Authentication service.** In IBM Security Access Manager for Enterprise Single Sign-On, a service that verifies the validity of an account against their own user store or against a corporate directory. Identifies the authentication service associated with a screen. Account data saved under a particular authentication service is retrieved and auto-filled for the logon screen that is defined. Account data captured from the logon screen defined is saved under this authentication service.

**Authorization code.** An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass with AccessAgent, AccessAssistant, and Web Workplace.

**Auto-capture.** A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

**Automatic sign-on.** A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

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

**Bidirectional language.** A language that uses a script, such as Arabic and Hebrew, whose general flow of text proceeds horizontally from right to left, but numbers, English, and other left-to-right language text are written from left to right.

**Bind distinguished name.** A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also *Distinguished name*.

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

**Card Serial Number (CSN).** A unique data item that identifies a hybrid smart card. It has no relation to the certificates installed in the smart card

**Cell.** In WebSphere Application Server, a cell is a virtual unit that consists of a deployment manager and one or more nodes.

**Certificate authority (CA).** A trusted organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate.

**IMS Server Certificate.** Used in IBM Security Access Manager for Enterprise Single Sign-On. The IMS Server Certificate allows clients to identify and authenticate an IMS Server.

**Client AccessAgent.** AccessAgent installed and running on the client machine.

**Client workstation, client machine, client computers.** Computers where AccessAgent installed.

**Clinical Context Object Workgroup (CCOW).** A vendor independent standard, for the interchange of information between clinical applications in the healthcare industry.

**Clustering.** In WebSphere Application Server, clustering is the ability to group application servers.

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

**Command line interface.** A computer interface in which the input command is a string of text characters.

**Credentials.** Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

**Cryptographic application programming interface (CAPI).** An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

**Cryptographic Service Provider (CSP).** A feature of the i5/OS® operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

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

**Database (DB) server.** A software program that uses a database manager to provide database services to software programs or computers.

**DB2.** A family of IBM licensed programs for relational database management.

**Deployment manager profiles.** A WebSphere Application Server runtime environment that manages operations for a logical group, or cell, of other servers.

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

**Deprovision.** To remove a service or component. For example, to deprovision an account means to delete an account from a resource.

**Desktop application.** Application that runs in a desktop.

**Desktop Manager.** Manages concurrent user desktops on a single workstation

**Direct auth-info.** In profiling, direct auth-info is a direct reference to an existing authentication service.

**Directory service.** A directory of names, profile information, and computer addresses of every user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, or an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

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

**Disaster recovery site.** A secondary location for the production environment in case of a disaster.

**Disaster recovery.** The process of restoring a database, system, policies after a partial or complete site failure that was caused by a catastrophic event such as an earthquake or fire. Typically, disaster recovery requires a full backup at another location.

**Distinguished name.** The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region.

**Distributed IMS Server.** The IMS Servers are deployed in multiple geographical locations.

**Domain name server (DNS).** A server program that supplies name-to-address conversion by mapping domain names to IP addresses.

**Dynamic link library (DLL).** A file containing executable code and data bound to a program at load time or run time, rather than during linking. The code and data in a DLL can be shared by several applications simultaneously.

**Enterprise directory.** A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

**Enterprise Single Sign-On (ESSO).** A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

**Enterprise user name.** The user name of a user account in the enterprise directory.

**ESSO audit logs.** A log file that contains a record of system events and responses. ESSO audit logs are stored in the IMS Database.

**ESSO Credential Provider.** Previously known as the Encentuate Credential Provider (EnCredentialProvider), this is the IBM Security Access Manager for Enterprise Single Sign-On GINA for Windows Vista and Windows 7.

**ESSO credentials.** The ISAM ESSO user name and password.

**ESSO GINA.** Previously known as the Encentuate GINA (EnGINA). IBM Security Access Manager for Enterprise Single Sign-On GINA provides a user interface that is integrated with authentication factors and provide password resets and second factor bypass options.

**ESSO Network Provider.** Previously known as the Encentuate Network Provider (EnNetworkProvider). An AccessAgent module that captures the Active Directory server credentials and uses these credentials to automatically log on the users to their Wallet.

**ESSO password.** The password that secures access to the user Wallet.

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

**Failover.** An automatic operation that switches to a redundant or standby system in the event of a software, hardware, or network interruption.

**Fast user switching.** A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

**Federal Information Processing Standard (FIPS).** A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

**Fix pack.** A cumulative collection of fixes that is made available between scheduled refresh packs, manufacturing refreshes, or releases. It is intended to allow customers to move to a specific maintenance level.

**Fully qualified domain name (FQDN).** In Internet communications, the name of a host system that

includes all of the subnames of the domain name. An example of a fully qualified domain name is rchland.vnet.ibm.com.

**Graphical Identification and Authentication (GINA).** A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

**Group Policy Object (GPO).** A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

**High availability (HA).** The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

**Host name.** In Internet communication, the name given to a computer. The host name might be a fully qualified domain name such as `mycomputer.city.company.com`, or it might be a specific subname such as `mycomputer`.

**Hot key.** A key sequence used to shift operations between different applications or between different functions of an application.

**Hybrid smart card.** An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

**IBM HTTP server.** A web server. IBM offers a web server, called the IBM HTTP Server, that accepts requests from clients and forward to the application server.

**IMS Bridge.** A module embedded in third-party applications and systems to call to IMS APIs for provisioning and other purposes.

**IMS Configuration Utility.** A utility of the IMS Server that allows Administrators to manage lower-level configuration settings for the IMS Server.

**IMS Configuration wizard.** Administrators use the wizard to configure the IMS Server during installation.

**IMS Connector.** A module that connects IMS to external systems to dispatch a mobile active code to a messaging gateway.

**IMS data source.** A WebSphere Application Server configuration object that defines the location and parameters for accessing the IMS database.

**IMS Database.** The relational database where the IMS Server stores all ESSO system, machine, and user data and audit logs.

**IMS Root CA.** The root certificate authority that signs certificates for securing traffic between AccessAgent and IMS Server.

**IMS Server.** An integrated management system for ISAM ESSO that provides a central point of secure access administration for an enterprise. It enables centralized management of user identities, AccessProfiles, authentication policies, provides loss management, certificate management, and audit management for the enterprise.

**Indirect auth-info.** In profiling, indirect auth-info is an indirect reference to an existing authentication service.

**Interactive graphical mode.** A series of panels that prompts for information to complete the installation.

**IP address.** A unique address for a device or logical unit on a network that uses the Internet Protocol standard.

**Java Management Extensions (JMX).** A means of doing management of and through Java technology. JMX is a universal, open extension of the Java programming language for management that can be deployed across all industries, wherever management is needed.

**Java runtime environment (JRE).** A subset of a Java developer kit that contains the core executable programs and files that constitute the standard Java platform. The JRE includes the Java virtual machine (JVM), core classes, and supporting files.

**Java virtual machine (JVM).** A software implementation of a processor that runs compiled Java code (applets and applications).

**Keystore.** In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted, or public, keys.

**Lightweight Directory Access Protocol (LDAP).** An open protocol that uses TCP/IP to provide access to directories that support an X.500 model. An LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

**Lightweight mode.** A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

**Load balancing.** The monitoring of application servers and management of the workload on servers. If one server exceeds its workload, requests are forwarded to another server with more capacity.

**Lookup user.** A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

**Main AccessProfile.** The AccessProfile that contains one or more AccessProfile widgets

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

**Microsoft Cryptographic application programming interface (CAPI).** An interface specification from Microsoft for modules that provide cryptographic functionality and that allow access to smart cards.

**Mobile ActiveCode (MAC).** A one-time password that is used by users for two-factor authentication in Web Workplace, AccessAssistant, and other applications. This OTP is randomly generated and dispatched to user through SMS or email.

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

**Network deployment.** Also known as a clustered deployment. A type of deployment where the IMS Server is deployed on a WebSphere Application Server cluster.

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

**Nodes.** A logical group of managed servers.

**One-Time Password (OTP).** A one-use password generated for an authentication event, sometimes communicated between the client and the server through a secure channel.

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

**Password aging.** A security feature by which the superuser can specify how often users must change their passwords.

**Password complexity policy.** A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

**Personal applications.** Windows and web-based applications where AccessAgent can store and enter credentials.

Some examples of personal applications are web-based mail sites such as Company Mail, Internet banking sites, online shopping sites, chat, or instant messaging programs.

**Personal desktop.** The desktop is not shared with any other users.

**Personal Identification Number (PIN).** In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

**Pinnable state.** A state from the AccessProfile widget that is declared as 'Can be pinned in another AccessProfile'.

**Pinned state.** A pinnable state that is attached to a state in the main AccessProfile.

**Policy template.** A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

**Portal.** A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

**Presence detector.** A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

**Primary authentication factor.** The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

**Private desktop.** Under this desktop scheme, users have their own Windows desktops in a workstation. When a previous user return to the workstation and unlocks it, AccessAgent switches to the desktop session of the previous user and resumes the last task.

**Private key.** In computer security, the secret half of a cryptographic key pair that is used with a public key algorithm. The private key is known only to its owner. Private keys are typically used to digitally sign data and to decrypt data that has been encrypted with the corresponding public key.

**Provisioning API.** An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

**Provisioning bridge.** An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

**Provisioning system.** A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

**Provision.** To provide, deploy, and track a service, component, application, or resource.

**Public Key Cryptography Standards.** A set of industry-standard protocols used for secure information exchange on the Internet. Domino® Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

**Published application.** Application installed on Citrix XenApp server that can be accessed from Citrix ICA Clients.

**Published desktop.** A Citrix XenApp feature where users have remote access to a full Windows desktop from any device, anywhere, at any time.

**Radio Frequency Identification (RFID).** An automatic identification and data capture technology that identifies unique items and transmits data using radio waves.

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

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

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

**Remote Authentication Dial-In User Service (RADIUS).** An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

**Remote Desktop Protocol (RDP).** A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

**Replication.** The process of maintaining a defined set of data in more than one location. Replication involves copying designated changes for one location (a source) to another (a target) and synchronizing the data in both locations.

**Revoke.** To remove a privilege or an authority from an authorization identifier.

**Root certificate authority (CA).** The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

**Scope.** A reference to the applicability of a policy, at the system, user, or machine level.

**Secret question.** A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

**Secure Remote Access.** The solution that provides web browser-based single sign-on to all applications from outside the firewall.

**Secure Sockets Layer (SSL).** A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

**Secure Sockets Layer virtual private network (SSL VPN).** A form of VPN that can be used with a standard web browser.

**Security Token Service (STS).** A web service used for issuing and exchanging of security tokens.

**Security trust service chain.** A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

**Self-service features.** Features in IBM Security Access Manager for Enterprise Single Sign-On which users can use to perform basic tasks such as resetting passwords and secrets with minimal assistance from Help desk or your Administrator.

**Serial ID Service Provider Interface (SPI).** A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

**Serial number.** A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On Keys, which is unique to each Key and cannot be changed.

**Server AccessAgent.** AccessAgent deployed on a Microsoft Windows Terminal Server or a Citrix server.

**Server locator.** A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

**Service Provider Interface (SPI).** An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

**Session management.** Management of user session on private desktops and shared desktops.

**Shared desktop.** A desktop configuration where multiple users share a generic Windows desktop.

**Shared workstation.** A workstation shared among users.

**Sign up.** To request a resource.

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

**sign-on information.** Information required to provide access to users to any secure application. This information can include user names, passwords, domain information, and certificates.

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

**Silent mode.** A method for installing or uninstalling a product component from the command line with no GUI display. When using silent mode, you specify the data required by the installation or uninstallation program directly on the command line or in a file (called an option file or response file).

**Simple Mail Transfer Protocol (SMTP).** An Internet application protocol for transferring mail among users of the Internet.

**Simple Object Access Protocol (SOAP).** A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

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

**Smart card middleware.** Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

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

**Stand-alone deployment.** A deployment where the IMS Server is deployed on an independent WebSphere Application Server profile.

**Stand-alone server.** A fully operational server that is managed independently of all other servers, and it uses its own administrative console.

**Strong authentication.** A solution that uses multi-factor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

**Strong digital identity.** An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

**System modal message.** A system dialog box that is typically used to display important messages. When a system modal message is displayed, nothing else can be selected on the screen until the message is closed.

**Terminal emulator.** A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal

**Thin client.** A client machine that has little or no installed software. It has access to applications and desktop sessions that is running on network servers that are connected to it. A thin client machine is an alternative to a full-function client such as a workstation.

**Tivoli Common Reporting tool.** A reporting component that you can use to create, customize, and manage reports.

**Tivoli Identity Manager adapter.** An intermediary software component that allows IBM Security Access Manager for Enterprise Single Sign-On to communicate with Tivoli Identity Manager.

**Transparent screen lock.** A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

**Trigger.** In profiling, an event that causes transitions between states in a states engine, such as, the loading of a web page or the appearance of window on the desktop.

**Trust service chain.** A chain of modules operating in different modes. For example: validate, map and issue.

**Truststore.** In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys.

**TTY (terminal type).** A generic device driver for a text display. A tty typically performs input and output on a character-by-character basis.

**Two-factor authentication.** The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

**Uniform resource identifier.** A compact string of characters for identifying an abstract or physical resource.

**User credential.** Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

**User deprovisioning.** Removing the user account from IBM Security Access Manager for Enterprise Single Sign-On.

**User provisioning.** The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

**Virtual appliance.** A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

**Virtual channel connector.** A connector that is used in a terminal services environment. The virtual channel connector establishes a virtual communication channel to manage the remote sessions between the Client AccessAgent component and the Server AccessAgent.

**Virtual Member Manager (VMM).** A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

**Virtual Private Network (VPN).** An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure.

**Visual Basic (VB).** An event-driven programming language and integrated development environment (IDE) from Microsoft.

**Wallet caching.** When performing single sign-on for an application, AccessAgent retrieves the logon credentials from the user credential Wallet. The user credential Wallet is downloaded on the user machine and stored securely on the IMS Server. So users can access their Wallet even when they log on to IBM Security Access Manager for Enterprise Single Sign-On from a different machine later.

**Wallet manager.** The IBM Security Access Manager for Enterprise Single Sign-On GUI component that users can use to manage application credentials in the personal identity Wallet.

**Wallet Password.** A password that secures access to the Wallet.

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

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

**Web service.** A self-contained, self-describing modular application that can be published, discovered, and invoked over a network using standard network protocols. Typically, XML is used to tag the data, SOAP is used to transfer the data, WSDL is used for describing the services available, and UDDI is used for listing what services are available.

**Web Workplace.** A web-based interface that users can log on to enterprise web applications by clicking links without entering the passwords for individual applications. This interface can be integrated with the existing portal or SSL VPN of the customer.

**WebSphere Administrative console.** A graphical administrative Java application client that makes method calls to resource beans in the administrative server to access or modify a resource within the domain.

**WebSphere Application Server profile.** The WebSphere Application Server administrator user name and profile. Defines the runtime environment.

**WebSphere Application Server.** Software that runs on a web server and that can deploy, integrate, execute, and manage e-business applications.

**Windows logon screen, Windows logon UI mode.** The screen where users enter their user name and password to log on to the Windows desktop.

**Windows native fast user switching.** A Windows XP feature which allows users to quickly switch between user accounts.

**Windows Terminal Services.** A Microsoft Windows component that users use to access applications and data on a remote computer over a network.

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

# Index

## J



## K



## L



## M



## N



## O



## P



## R



## S



## T



## U



## V

## W

Printed in USA

GC23-9692-01