

IBM® Security Access Manager for Enterprise Single
Sign-On
Version 8.2.2

Configuration Guide

IBM

IBM® Security Access Manager for Enterprise Single
Sign-On
Version 8.2.2

Configuration Guide

IBM

Note

Before using this information and the product it supports, read the information in "Notices" on page 81.

Edition notice

Note: This edition applies to version 8.2.2 of IBM Security Access Manager for Enterprise Single Sign-On, (product number 5724-V67) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2002, 2015.

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

Contents

About this publication	v
Accessibility	v
Technical training.	v
Support information.	v
Statement of Good Security Practices	v

Chapter 1. Configuring the IMS Server . 1

Accessing the IMS Configuration Utility	1
Provisioning IMS Server Administrators	1
Basic settings	2
Adding an authentication service	2
Configuring the IMS Server to use directory servers	3
Enabling biometric support	10
Advanced settings	10
Setting AccessAdmin	10
Setting the IMS Server.	16
Setting the data source	21
IMS Bridge	24
Configuring user authentication	25
Utilities.	27
Uploading system data	27
Exporting the IMS Server configuration with the IMS Configuration Utility	28
Importing the IMS Server configuration with the IMS Configuration Utility	29
Translating event and result codes.	31
Configuring HTTP compression	31

Chapter 2. Backing up and recovering the IMS Server, WebSphere Application Server profiles, and database 33

Backing up WebSphere Application Server profiles	33
Restoring the WebSphere Application Server profiles	34
Backing up the database in DB2	34
Restoring the database in DB2	35

Chapter 3. Configuring AccessAgent 37

Configuring the AccessAgent user interface.	37
Launching applications from ESSO Credential Provider	37
Changing the AccessAgent banner.	40
Disabling the ESSO Credential Provider	40
Configuring the AccessAgent functionality features	41
Changing the Ctrl+Alt+Delete support in Windows 7 or later	41
Transparent Screen Lock support in Windows 7 and later	41
Enabling and customizing the Transparent Screen Lock in Windows 7 or later	42
Enabling single sign-on for Java applications	43
Enabling Help in dialogs launched in the context of AccessProfiles.	44

Configuring event reporting in the Windows Event log	44
Configuring the system modal message box	45
Disabling application write-access to Windows registry.	45
Configuring the AccessAgent accessibility features	46
Enabling animation effect for AccessAgent	46
AccessAgent keyboard shortcuts	46

Chapter 4. Configuring a strong authentication setup 47

Setting up RFID authentication	47
Setting up fingerprint authentication	48
Installing the Native Library Invoker resource adapter.	48
Integrating a BIO-key fingerprint reader.	49
Setting up smart card authentication	51
Enabling two-way SSL.	52
Importing smart card CA certificates	52
Enabling smart card authentication	53
Configuring hybrid smart cards	56
Setting up Kerberos authentication	56
Configuring IMS Server for Kerberos authentication	56
Configuring the AccessAgent for Kerberos authentication	57
Verifying the Kerberos configuration	57
Setting up policies for Kerberos authentication	58

Chapter 5. Configuring a secure deployment. 59

Removing sample WebSphere Application Server servlets and applications	59
Securing access to configuration data.	59
Setting a limit on logon attempts	60
Restricting HTTP connections	60
Disabling directory browsing	61

Chapter 6. Logging on to AccessAdmin 63

Chapter 7. Setting up policy templates 65

Chapter 8. Automatically assigning User Policy Templates to new users . . 67

Chapter 9. Excluding machine attributes. 69

Chapter 10. Configuring JMX support 71

Chapter 11. Command-line interface reference. 73

cleanImsConfig command	73
----------------------------------	----

deployIsamessolms command	74
deployIsamessolmsConfig command	75
exportImsConfig command	75
managePolPriority command	76
setupCmdLine command	76
upgradeSymCrypto command	76
uploadDpx command	77
uploadOath command	78
uploadSync command	78

Notices 81

Glossary 85

A.	85
B.	86
C.	86
D.	87
E.	88
F.	88

G.	88
H.	88
I	89
J	89
K.	89
L.	89
M	89
N.	90
O.	90
P.	90
R.	91
S.	91
T.	93
U.	93
V.	93
W	94

Index 95

About this publication

IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide provides information about configuring the IMS Server settings, the AccessAgent user interface, and its behavior.

Accessibility

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

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

Technical training

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

Support information

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

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

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

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

Statement of Good Security Practices

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

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

Chapter 1. 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*.

For more information:

- “Accessing the IMS Configuration Utility”
- “Provisioning IMS Server Administrators”
- “Basic settings” on page 2
- “Advanced settings” on page 10
- “Utilities” on page 27

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://imsdmgr.jke.com: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.

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. Note: You can store the authentication service display name in multiple languages, depending on the language that is specified by the user during logon.
Description	Enter a short description of the authentication service. Note: You can store the authentication service description in multiple languages, depending on the language that is specified by the user during logon.
Account data template ID	Select an account data template ID from the list. The template ID defines the structure of the account data to be captured for the authentication service. For example, <code>adt_ciuser_cspwd</code> means that the selected account data template captures a user name that is not case-sensitive and a case-sensitive password.
Authentication service groups	Select the group for the authentication service from the 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 you configure 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 you restart 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 it authenticates the user.

For more information about the solution, see *Unable to authenticate when a repository is down* in the WebSphere Application Server documentation.

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 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 IBM Security Identity Manager Active Directory Adapter, unless you want to use the Self-Service Password Reset feature in AccessAssistant and the Active Directory is configured without SSL transport.

For LDAP and Active Directory enabled SSL connections, you must add the directory server SSL certificates to the WebSphere Application Server and restart WebSphere Application Server before configuring the enterprise directories. 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 “Planning worksheet” in the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.

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. If password synchronization is enabled, when the user logs in to AccessAgent or AccessAssistant, 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 IBM Security Identity Manager Active Directory Adapter. In an SSL environment, you do not have to install the IBM Security 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	<p>Connect using</p> <p>You can select only Domain controller host name / FQDN.</p> <p>Domain controller FQDN Specify the fully qualified domain name of the domain controller. For example: adserver.team.example.com where team.example.com is the domain name server.</p> <p>Domain DNS name Specify the domain name of the Active Directory server that is connected to the IMS Server. For example: team.example.com</p> <p>Domain NetBIOS name Specify the NetBIOS computer name. The NetBIOS computer name is typically the same as the host name of the computer in the same domain. For example: mydirsvr</p> <p>Note:</p> <ul style="list-style-type: none">• The NetBIOS name is not validated by the IMS Server. You must provide the correct name.• To determine the correct NetBIOS computer name, go to the Microsoft website at www.microsoft.com and search for "nbtstat". See instructions on how to use nbtstat to determine the NetBIOS computer name. <p>Port Specify the port number. For example: the default is 389 (without SSL) or 636 (with SSL).</p> <p>Bind user name Specify the user name of the lookup user. For example: lookupusr.</p>

Option	Parameters
	<p>Password Enter the password for the lookup user.</p> <p>Base distinguished name At least one base distinguished name is required. The base distinguished name indicates the starting point for searches in this directory server. For authorization purposes, this field is case sensitive by default. Match the case in your directory server.</p> <p>For example: For a user with a DN of <code>cn=lookupusr,cn=users,dc=team,dc=example,dc=com</code>, specify the base distinguished name with any of the following options: <code>cn=users,dc=team,dc=example,dc=com</code> or <code>dc=team,dc=example,dc=com</code>.</p> <p>Failover domain controllers Use a failover domain controller for replicated Active Directory servers in a high availability configuration.</p> <p>Specify the host name or the fully qualified domain name, and the port number of the secondary domain controller. The secondary domain controller is used when the primary domain controller fails.</p>
If you are using SSL	<p>Connect using If you are using SSL, you can connect to the server by using a Domain DNS name or a Domain controller host name / FQDN. If you are using a domain name server to resolve host names or IP addresses, select Domain DNS name.</p> <p>If you select Domain controller host name / FQDN, the Domain controller host name / FQDN is displayed.</p> <p>Domain controller host name / FQDN If you choose to connect using Domain controller host name / FQDN, the domain controller host name or fully qualified domain name is displayed.</p> <p>Domain DNS name The domain name of the Active Directory server that is connected to the IMS Server is displayed. For example: <code>team.example.com</code></p> <p>Domain NetBIOS name 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: <code>mydirsvr</code></p> <p>Note:</p> <ul style="list-style-type: none"> • The NetBIOS name is not validated by the IMS Server. You must provide the correct name. • To determine the correct NetBIOS computer name, go to the Microsoft website at www.microsoft.com and search for "nbtstat". See instructions on how to use nbtstat to determine the NetBIOS computer name. <p>Bind distinguished name 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 do directory lookups. A DN is made up of attribute=value pairs, which are separated by commas. For example: <code>cn=lookupusr,cn=users,dc=team,dc=example,dc=com</code></p>

Option	Parameters
	<p>Password Enter the password for the lookup user.</p> <p>Base distinguished name At least one base distinguished name is required. The base distinguished name indicates the starting point for searches in this directory server. For authorization purposes, this field is case-sensitive by default. Match the case in your directory server.</p> <p>For example: For a user with a DN of <code>cn=lookupusr,cn=users,dc=team,dc=example,dc=com</code>, specify the base distinguished name with any of the following options: <code>cn=users,dc=team,dc=example,dc=com</code> or <code>dc=team,dc=example,dc=com</code>.</p> <p>Failover domain controllers This field is displayed only if you choose a connection using Domain controller host name / FQDN.</p> <p>Use a failover domain controller for replicated Active Directory servers in a high availability configuration.</p> <p>Specify the host name or the fully qualified domain name, and the port number of the secondary domain controller. The secondary domain controller is used when the primary domain controller fails.</p>

9. If password synchronization is enabled:
 - a. You can choose to enable **AccessAssistant password reset**.
If you choose to enable this feature, users can reset their passwords in AccessAssistant.
 - b. If you enabled **AccessAssistant 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 you specify 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 Security 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 “Planning worksheet” in the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.

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 more 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 do directory lookups on the server.

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

Password

Enter the password for the lookup user.

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, which are separated by commas. For example: `cn=lookupusr,ou=users,o=example,c=us`.

Password

Enter the password for the lookup user.

User name attributes

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

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

For LDAP, the default is cn.

Base distinguished name

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

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

Failover domain controllers

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

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

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. 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 user name 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**.

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.

For more information:

- “Setting AccessAdmin”
- “Setting the IMS Server” on page 16
- “Setting the data source” on page 21
- “IMS Bridge” on page 24
- “Configuring user authentication” on page 25

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 that is 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. Note: <ol style="list-style-type: none"> The IMS Server uses the selected locale during the following scenarios: <ul style="list-style-type: none"> A new HTTP session is established. The cookie does not store the selected locale. 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. AccessAgent (versions older than 8.1) also uses this locale. 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.
Key type attribute	Enter the attribute that provides information about the type of key being used. 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. 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. 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. 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.

Option	Description
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. These logs are displayed on the status page of AccessAdmin.
Policy assignment attribute	Enter the attribute that is 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 list. <ul style="list-style-type: none"> • true - enables the delete user button • false - does not enable the delete user button
Authorization code expiration	Shows the different expiry times possible for authorization code expiry on AccessAdmin. 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}. The number represents how many hours/days/weeks/months (For example: 1d is one day, 2w is two weeks). Enter an expiry time and then click Add . 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. Enter a display type and then click Add . 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 list.

Option	Description
Non-certificate authentication access types	<p>Enter the access types for non-certificate authentication.</p> <p>Enter an access type and then click Add.</p> <p>To remove an access type, click the Remove button next to the access type.</p>
Attributes used on the user interface	<p>Enter the attributes that AccessAdmin uses with display names and display types.</p> <p>Enter an attribute and then click Add.</p> <p>To remove an attribute, click the Remove button.</p>
Searchable LDAP attributes	<p>Enter the LDAP attributes that support the IMS Server queries.</p> <p>The format is [LDAP Attribute]:[Display Name]:[Display Order]. Enter an attribute, and then click Add.</p> <p>To remove an attribute, click the Remove button.</p>
Policy display configuration file location	<p>Enter the name of the file that determines the policies and in what order to display them on the AccessAdmin UI.</p>
Custom user interface policies	<p>List the policies with custom user interfaces.</p> <p>The value is in the format of a comma-separated policy ID and class name. For example: pid_bind, IBM.ims.ui.component.Binder.</p> <p>Enter a policy and click Add.</p> <p>To remove a policy, click the Remove button next to the policy.</p>
Custom user interface attributes	<p>Enter the attributes with custom user interfaces.</p> <p>The value is in the format of a comma-separated attribute name and class name. For example, gsmNumber, IBM.ims.ui.component.GsmNumber.</p> <p>Enter an attribute and click Add.</p> <p>To remove an attribute, click the Remove button next to the attribute.</p>

- 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 that are based on user interface searches.

- Click **Update**.

Changing the help files URL

Use IMS Configuration Utility to change the help file link in AccessAdmin.

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://www.ibm.com/support/knowledgecenter/SS9JLE_8.2.2 .

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. 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. This option restricts a session to the created IP address. Select a value. The default value is false . <ul style="list-style-type: none">• true - checks the IP address of the client• false - does not check the IP address of the client

Option	Description
Check session inactivity	Specify whether sessions are timed out because of inactivity. Select a value. The default value is true . <ul style="list-style-type: none"> • true - session times out after a period of inactivity. • false - session does not time out.
Session inactivity timeout, in minutes	Enter the inactivity timeout in minutes. The default value is 15 minutes.
Check forced session timeout	Specify whether to force the client to log on again after a fixed time. Select a value. The default value is false . <ul style="list-style-type: none"> • true - client is forced to log on after a period of inactivity • false - session does not time out.
Forced session timeout, in minutes	Enter the forced timeout in minutes. 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. Enter an enterprise ID and then click Add . To remove an enterprise ID, click the Remove next to the enterprise ID.
Role assignment attribute name	Enter the name of an Active Directory attribute that is 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.

- 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). There must be a matching entry in the <code>IMSRole</code> table of the database under <code>roleID</code> .
Bound IMS user role	After a successful registration of the user, the role of the user is set to 2 (user). Multiple entries can be specified for multiple roles. There must be a matching entry in the <code>IMSRole</code> table of the database under <code>roleID</code> .
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. This option must match one of the <code>attrName</code> fields in <code>IMSAttributeName</code> table.
Software key allowed	Specify whether software keys can be used.

- Click **Update**.

Specifying machine attributes

You can assign machine policy templates to different groups of computers that are 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

- Log on to the IMS Configuration Utility.
- Navigate to **Advanced Settings > AccessAdmin > Machine attributes**.
- 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 that is used as criterion for searching computer attributes.

- Click **Update**.

Setting the IMS Server

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

Enabling log-signing

If you want to enable log-signing on 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 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** next to the table name.

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

Configuring syslog settings

Use the IMS Configuration Utility to forward audit log records to any external SysLog server. This utility enables syslog and defines 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	<p>Specify the list of tables where the logs are stored in the syslog server.</p> <p>The available tables are:</p> <ul style="list-style-type: none">• logSystemManagementActivity• logSystemOps• logUserAdminActivity• logUserService• logUserActivity <p>Select a table and then click Add.</p> <p>To remove a table from the list, click the Remove button next to the table name.</p>
Syslog server port	Enter the port number at which the syslog daemon is listening.
Syslog server hostname	Enter the host name of the syslog server.
Syslog logging facility	Enter the integer value of the facility that is used for logging to the syslog server.
Syslog field-separator	Enter the field separator character that is 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 that is 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 that is 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 that is used in the IMS Server. The keypairs are used for IMS Server CA and user certificates.
Alias for IMS Soft CA in the keystore	Enter the alias that is 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. 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. This option is used only if <code>IBM.events.HandleImmediately</code> 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 that is 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 > Miscellaneous**.
3. Complete the following fields:

Option	Description
Application binding tasks	Enter the class names of the tasks that are 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. For more information, see Chapter 9, "Excluding machine attributes," on page 69.
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**.

Configuring the server for a Layer 7 load balancer

The IMS Server configuration file, `ims.xml`, contains three parameters to configure for Layer 7 load balancer support in a high availability or clustered deployment.

Procedure

1. Open the IMS Server configuration file `<WAS profile directory>\config\tamesso\config\ims.xml` in a text editor.
2. Specify the following parameters:

encentuate.ims.clientIp.customHeader.name

Set this parameter to the header name where the load balancer adds the

client IP address into. Typically, this value is set to **X-Forwarded-For**. If this value is not defined or set, the default behavior is to retrieve the client IP address from the request.

encentuate.ims.clientIp.customHeader.delimiter

This parameter is optional. If multiple values are set, for example, where there is more than one load balancer, the character set is used as a separator.

Example 1

ip1, ip2, ip3

You specified "," as the value for this parameter.

Example 2 (default)

ip1 ip2 ip3

encentuate.ims.clientIp.customHeader.isRTL

This parameter is optional. If you are specifying multiple load balancers and you are adding the source IP address of the request to the same header, this parameter specifies how the load balancer appends the IP address to the list.

Example 1 (Default)

clientip lb1ip lb2ip

Example 2

lb2ip lb1ip clientip

Set this parameter to yes if the IP address is written to the start of the list, and not at the end of the list.

3. Restart the IMS Server after you complete the configuration.

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 that are 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).

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

4. View the following fields:

Option	Description
Default data object type	<p>Displays the default ds.do_type if :</p> <ul style="list-style-type: none"> No value is specified during a request for a connection Data source parameters for other <code>ds.do_types</code> are not found <p>Note: ds stands for data store and do is a data object.</p>
Path to data source configuration file for IMS Server	Displays the configuration file path for the IMS Server.
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 Server data source settings

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

Procedure

- Log on to the IMS Configuration Utility.
- Navigate to **Advanced Settings > Data Source > IMS data source**.
- 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 .

Option	Description
IMS database name	Enter the name of the IMS Server database.
IMS database user name	Enter the user name that is used to log on to the database.
IMS database password	Enter the corresponding password for the user name that is 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 that is 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 that is used to log on to the log database.
IMS log database password	Enter the corresponding password for the user name that is used to log on to the database.
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**.

IMS Bridge

The IMS Server interfaces with other applications through message connectors and IMS Server provisioning bridges. Configure the IMS Bridge to provision users.

Adding IMS Bridge user names

Use the IMS Configuration Utility to add IMS Bridge user names. An IMS Bridge is a module that is 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. Note: IBM Security Access Manager for Enterprise Single Sign-On, version 8.2.1, supports Internet Protocol version 6 (IPv6). 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.

About this task


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 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.
IMS Bridge IP addresses	Enter the IP addresses from which the IMS Bridge can access the IMS Server. Note: IBM Security Access Manager for Enterprise Single Sign-On, version 8.2.1, 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**.

Related information:

 Requirements for using the IMS Bridge for user provisioning in an upgraded IMS Server

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, 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 > 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.

Option	Description
Allow non-certificate authentication by default	Specify whether all users can access non-certificate based authentication by default. 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. 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.
Backup software key character sets	Add or remove the Character sets that can be supported by the IMS Server. Specify one of the following values: <ul style="list-style-type: none"> • Form character_set • N2 • Character_set • D2 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 > 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 > User authentication > Authorization code**.
3. Complete the following fields:

Option	Description
Authorization code enabled	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. 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 that are supported by the IMS Server and the classes that implement the vendor-specific algorithms.

5. Click **Update**.

Utilities

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

For more information:

- “Uploading system data”
- “Exporting the IMS Server configuration with the IMS Configuration Utility” on page 28
- “Importing the IMS Server configuration with the IMS Configuration Utility” on page 29
- “Translating event and result codes” on page 31

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 that is 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 then 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):exportCell101:(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
If <Location /> is not found, add the following lines after the last occurrence of </Location>
<Location />
SetOutputFilter DEFLATE
SetEnvIfNoCase Request_URI\.(?:gif|jpe?g|png)\$ no-gzip dont-vary
SetInputFilter DEFLATE
</Location>

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 28
 - “Importing the IMS Server configuration with the IMS Configuration Utility” on page 29
- WebSphere Application Server profiles
 - “Backing up WebSphere Application Server profiles”
 - “Restoring the WebSphere Application Server profiles” on page 34
- Database
 - “Backing up the database in DB2” on page 34
 - “Restoring the database in DB2” on page 35

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 command: `cd <was_home>\bin` For example:
`cd c:\Program Files\IBM\WebSphere\AppServer\bin`
3. Use the WebSphere Application Server **manageprofiles** command with the **backupProfile** parameter.

```
manageprofiles.bat -backupProfile -profileName <profile_name>  
-backupFile <backupFile_name>
```

For example:

Stand-alone

```
manageprofiles.bat -backupProfile -profileName AppSrv01  
-backupFile c:\backup\AppSrv01ymmdd.zip
```

Network deployment

```
manageprofiles.bat -backupProfile -profileName Dmgr01 -backupFile  
c:\backup\Dmgr01ymmdd.zip
```

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\AppSrv01ymmdd.zip The **manageprofiles** command-line tool always restores to the same path the profile was backed up from.
3. Verify that the profile is restored. Browse to the <was_home>\profiles directory. For example, <was_home>\profiles\AppSrv01. If the profile is restored successfully, a folder for the restored profile is displayed.

Results

The profile is restored successfully.

Tip: If you are completing this task as part of a server restoration procedure, do not start the profile. Determine whether you must restore the database first or later.

Backing up the database in DB2

Back up the database in DB2 before you do 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 want to back up the database as part of a server upgrade process, see the upgrade procedures to determine whether 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 that you want to restore.
3. Select the **Restore to an existing database**.
4. Click **Next**.
5. In **Available backup images**, select the backup that you made.
6. Click the right arrow 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 you install AccessAgent, you can configure its user interface, functions, and accessibility features.

For more information:

- “Configuring the AccessAgent user interface”
- “Configuring the AccessAgent functionality features” on page 41
- “Configuring the AccessAgent accessibility features” on page 46

Configuring the AccessAgent user interface

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

For more information:

- “Launching applications from ESSO Credential Provider”
- “Changing the AccessAgent banner” on page 40
- “Disabling the ESSO Credential Provider” on page 40

Launching applications from ESSO Credential Provider

Configure ESSO Credential Provider so that you can start an application by clicking a link in the AccessAgent panel.

Use this feature to open:

- AccessAssistant with a web browser to complete self-service password reset.
- A vendor application to complete 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 Credential Provider Policies**.
3. Complete the following fields:

Option	Description
Enable application launch from ESSO Credential Provider	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 Credential Provider. For example, Self-service password reset .
Command line for application launch	Set the command line that launches the application. For example, C:\Program Files\Internet Explorer\iexplore.exe.

4. Click **Add**.

Note: If the application is launched from the Welcome screen or Locked screen from Microsoft Windows 7 and later, the owner of the process for the application is also **System**.

Use the following command line to launch AccessAssistant 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.

Note: If you want to use the AccessAssistant self-service password reset and the following conditions exist, you must install the Tivoli Identity Manager Active Directory Adapter:

- Active Directory password synchronization is enabled
- SSL is not enabled in the Enterprise Directory connection configuration

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 started in the context of the Guest account. Use the Windows **runas** command to start 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 start the application. Consider that the VBScript is stored on 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_engine_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-0 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. For example:

```
32-bit aa-8.2.1.0100\{9713108D-08D5-474E-92A3-09CD7B63DB34}\Config
```

```
64-bit aa-8.2.1.0100_x64\{E72C4028-45BB-4EE6-8563-3066EEB39A84}\Config
```

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

Disabling the ESSO Credential Provider

You can deploy the AccessAgent without the ESSO Credential Provider for Windows 7 and later.

Procedure

1. Navigate to the **Config** folder of the AccessAgent installation package. For example:

```
32-bit aa-8.2.2.0100\{9713108D-08D5-474E-92A3-09CD7B63DB34}\Config
```

```
64-bit aa-8.2.2.0100_x64\{E72C4028-45BB-4EE6-8563-3066EEB39A84}\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 features include event reporting, hot key enablement, and bidirectional language support.

For more information:

- “Changing the Ctrl+Alt+Delete support in Windows 7 or later”
- “Transparent Screen Lock support in Windows 7 and later”
- “Enabling and customizing the Transparent Screen Lock in Windows 7 or later” on page 42
- “Enabling single sign-on for Java applications” on page 43
- “Enabling Help in dialogs launched in the context of AccessProfiles” on page 44
- “Configuring event reporting in the Windows Event log” on page 44
- “Configuring the system modal message box” on page 45
- “Disabling application write-access to Windows registry” on page 45

Changing the Ctrl+Alt+Delete support in Windows 7 or later

In Windows 7 and later, **Interactive login: Do not require Ctrl+Alt+Del** is always enabled by default when you are running the AccessAgent installer. 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**.
3. Click **OK**.
4. Select **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**.
5. Right-click and select **DisableCAD**.
6. Modify the value to 0.

Transparent Screen Lock support in Windows 7 and later

With the Transparent Screen Lock feature in Windows 7 and later, you can monitor running applications on the shared desktop even when the desktop is locked. You can use Transparent Screen Lock in a shared desktop on a 32-bit or 64-bit computer.

You can monitor running applications across all the connected monitors. You can see the applications on your desktop, but you cannot interact with any of them.

Note: In Windows 8 and 10 64-bit, some of the running applications, such as Microsoft Internet Explorer and Task Manager, are not updated when the desktop is locked.

You can enable this feature in AccessAdmin. When this feature is enabled and the computer is locked, you see the following user interface on your computer instead of the standard Windows Lock Screen:

- Your Windows desktop.
- An IBM Security Access Manager for Enterprise Single Sign-On notification box that displays which user is logged on and how to unlock the computer.

You can unlock your computer through any of the following options:

- Using an IBM Security Access Manager for Enterprise Single Sign-On hot key.
For example: CTRL+ALT+E.
This hot key is configurable.
- Using the standard Transparent Screen Lock hot key: CTRL+ESC.
You can enable or disable this hot key, but it is not configurable.
- Tapping your RFID card.

Note:

- If you want to unlock your computer with only the RFID card, you must enable `pid_rfid_only_unlock_enabled`.
- Some users can tap their RFID card and provide their password to unlock the Transparent Screen Lock.

Screen Lock differences in Windows XP and in Windows 7 and later

The Transparent Screen Lock feature is implemented differently in Windows XP and in Windows 7 and later.

Table 1. Difference between the implementation in Windows XP and in Windows 7 or later

In Windows XP	In Windows 7 and later
<p>The following policies are ignored when Transparent Screen Lock is enabled:</p> <ul style="list-style-type: none"> • <code>pid_unlock_option</code> • <code>pid_script_unlock_type</code> • <code>pid_script_unlock_code</code> <p>For more information about lock and unlock policies, see <i>IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide</i>.</p>	<p>The following policies are supported:</p> <ul style="list-style-type: none"> • <code>pid_script_unlock_type</code> • <code>pid_script_unlock_code</code> <p>The following policies are supported but with limitations:</p> <ul style="list-style-type: none"> • <code>pid_unlock_option</code> • <code>pid_rfid_tap_different_action</code> <p>For more information about policy limitations in Windows 7 or later, see <i>IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide</i>.</p>
<p>The Transparent Screen Lock message (<code>pid_lock_transparent_text</code>) can contain up to 40-characters.</p>	<p>The Transparent Screen Lock message does not have a 40-character limit, but it is a suggested limit.</p>

Enabling and customizing the Transparent Screen Lock in Windows 7 or later

To use Transparent Screen Lock, enable it in AccessAdmin. You also can customize the hot key and message that is associated with this feature.

Before you begin

- Windows 7: Enable the Windows Aero theme in your 32-bit or 64-bit computer.
- Install .NET Framework 3.5 if it is not installed already.

Procedure

1. Log on to AccessAdmin.
2. Select your machine policy template.
3. Select **AccessAgent Policies > Lock/Unlock Policies**.
4. Set **Screen lock option** to **Transparent screen lock**.
5. Click **Update**.
6. Optional. Customize the hot key settings in AccessAdmin.
 - a. Navigate to **System > System policies > AccessAgent Policies > Hot Key Policies**.
 - b. Customize the following settings:

Display name	Policy ID
Transparent screen lock message	pid_lock_transparent_text
Enable transparent screen lock hot key	pid_lock_transparent_hot_key_enabled
Enable ISAM ESSO Hot Key	pid_enc_hot_key_enabled
ISAM ESSO Hot Key sequence	pid_enc_hot_key_sequence

Note: There is a limited allowed combination for the hot key sequence. For more information about hot key policies, see *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide*.

- c. Click **Update**.

Enabling single sign-on for Java applications

Single sign-on is supported on 32-bit Java applications and on Java applets if the Java Virtual Machine version used is between 1.1 and 1.6 update 12.

About this task

If you configure single sign-on after you install AccessAgent, complete 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`.
5. Enter `JVMSupport [/dall {default}] [/uall] [/d path] [/dold path] [/dnew path] [/u path] [/uold path] [/unew path] [/?]`

Option	Description
<code>/dall</code>	Deploy JVM Support for all JVMs detected in the Windows registry.
<code>/uall</code>	Remove JVM Support for all JVMs detected in the Windows registry.
<code>/d [path]</code>	Deploy JVM Support to the JVM installed at the specified path.

Option	Description
/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).
/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.

Enabling Help in dialogs launched in the context of AccessProfiles

Use the **Help** function in dialogs launched in the context of AccessProfiles 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**.
 - **1** - Enables the **Help**.
8. Click **OK**.

Note: To not enable the help on the ESSO Credential Provider, set **AAOnlineHelpLink** to EMPTY STRING under HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\DeploymentOptions.

Restriction: When you click **Help**, the browser in the Citrix session stops responding

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**.

Disabling application write-access to Windows registry

By default, AccessAgent uses the Windows registry to store certain policies that require a computer restart to take effect. Some data, such as the last logged on username, is also stored in the Windows registry. If your organization does not allow registry write access, use the file-based policy storage.

About this task

In a file-based policy storage, policies are stored in C:\Program Files\IBM\ISAM ESSO\AA\Data\ConfigData.ini.

Procedure

1. On your Windows desktop, click **Start > Run**.
2. In the **Open** field, enter regedit.
3. Click **OK**.
4. Select HKEY_LOCAL_MACHINE\Software\IBM\ISAM ESSO\Temp.
5. Create a FullRegistryEnabled registry key if it does not exist.
 - a. Right-click and select **New > DWORD Value**.
 - b. Enter FullRegistryEnabled.
6. Right-click FullRegistryEnabled and set the value to 0.

7. Click **OK**.
8. Restart the computer.

Configuring the AccessAgent accessibility features

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

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 **Alt** key, 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 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.

For more information:

- "Setting up RFID authentication"
- "Setting up fingerprint authentication" on page 48
- "Setting up smart card authentication" on page 51
- "Setting up Kerberos authentication" on page 56

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:

- See "Requirements for authentication devices" in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide* for the supported software and version.
- If you want to use other supported RFID readers, set up the machine policy directly. See *Setting up the machine policy*.
- Ensure that you have write permissions on the Windows registry.

Procedure

1. 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.
2. 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}"
```

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

Note: You can also do this step after AccessAgent is installed. In this scenario, double-click the DeploymentOptions.reg file to apply it. Make sure that you have write permissions on the Windows registry.

5. In AccessAdmin, set the machine policy **Authentication second factors supported** (pid_second_factors_supported_list) to **RFID**.

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

Setting up fingerprint authentication

You can use fingerprint as an alternative authentication factor to password. To set up fingerprint authentication, install the Native Library Invoker resource adapter and the fingerprint readers.

Important:

See "Set up Kerberos Authentication" in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide* to evaluate and verify that your workstation meets the requirements and compatibilities to set up Kerberos authentication.

Do one of the following:

- If your workstation is compatible, it is recommended that you set up Kerberos authentication.
- If your workstation is not compatible, proceed to set up the fingerprint authentication.

See "Requirements for authentication devices" in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide* for the supported software and version.

- "Installing the Native Library Invoker resource adapter"
- "Integrating a BIO-key fingerprint reader" on page 49

Installing the Native Library Invoker resource adapter

If you need fingerprint authentication support, you must manually install this resource adapter on every scope 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 scope 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.

Repeat these steps for each scope.

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.

Before you begin

See "Requirements for authentication devices" in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide* for the supported software and version.

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.

About this task

Repeat these steps for each Application Server.

Procedure

1. Install the Native Library Invoker resource adapter.
2. Install the BIO-key Biometric Service Provider drivers on the IMS Server.
 - a. Start the BIO-key installer.
 - b. In the BIO-key Reader Setup dialog box, select the manual setup of the biometric reader files option.
 - c. Select the biometric reader files to use. Wait for the completion of the installation.

Note: Selecting all biometric reader files might cause performance issues.
 - d. Select the manual selection of biometric readers option.
 - e. Select the biometric reader that you want from the list of installed readers.
 - f. Complete the installation steps.
3. Navigate to the IBM Security Access Manager for Enterprise Single Sign-On installation package.
4. Open the deploymentPack.biometrics_<IMS Server version>\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. In AccessAdmin, set the machine policy **Authentication second factors supported** (pid_second_factors_supported_list) to **Fingerprint**.

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.

Before you begin

You must install the BIO-key Biometric Service Provider before deploying Bio-key in AccessAgent. For more information about deploying BIO-key Biometric Service Provider, see “Deploying BIO-key Biometric Service Provider in the IMS Server” on page 49

Procedure

1. Install the BIO-key Biometric Service Provider.
2. Open the AccessAgent Installer folder.
3. Navigate to the **Customization** folder. For example:
32-bit <AccessAgent installer package>\{9713108D-08D5-474E-92A3-09CD7B63DB34}\Customization
64-bit <AccessAgent installer package>\{E72C4028-45BB-4EE6-8563-3066EEB39A84}\Customization
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 ESS0.
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 ESS0\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 before BIO-key, follow these steps:
 - a. Run FP3-BioKey.reg. This file is in the **Customization** folder under the AccessAgent installation folder. For example:

```
32-bit aa-8.2.1.0100\{9713108D-08D5-474E-92A3-09CD7B63DB34}\Customization
```



```
64-bit aa-8.2.1.0100_x64\{E72C4028-45BB-4EE6-8563-3066EEB39A84}\Customization
```
 - b. Repeat steps 8 to 12.

Setting up smart card authentication

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

Important:

See "Set up Kerberos Authentication" in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide* to evaluate and verify that your workstation meets the requirements and compatibilities to set up Kerberos authentication.

Do one of the following:

- If your workstation is compatible, it is recommended that you set up Kerberos authentication.
- If your workstation is not compatible, proceed to set up the smart card authentication.

See "Requirements for authentication devices" in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide* for the supported software and version.

- "Enabling two-way SSL" on page 52
- "Importing smart card CA certificates" on page 52
- "Enabling smart card authentication" on page 53
- "Configuring hybrid smart cards" on page 56
- "Importing smart card CA certificates" on page 52

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 display in the list of smart cards that are 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 that are registered with Windows. By default, AccessAgent automatically detects the CSP module that is used to access an inserted smart card. The inserted smart card is 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	<p>If the smart card keypair cannot be used to do RSA encryption, this value must be set to 0.</p> <p>AccessAgent uses a signature-based mechanism to encrypt the Wallet instead of the encryption-based mechanism, which is the default.</p>	No
ContainerSpecLevel	DWORD	<p>By default, AccessAgent searches for the authentication certificate in the default container on the smart card.</p> <p>A default container is a special certificate container that can be accessed without specifying the container name.</p> <p>However, if the authentication certificate used by AccessAgent is not in the default container, AccessAgent must specify the name of the container.</p> <p>CSPs follow different conventions for accepting container names. This parameter defines the container name format.</p> <ul style="list-style-type: none"> • #1: \\.\<reader-name>\<container-id> • #2: \\.\<reader-name>\\ • #3: <container-id> • #4: NULL (default) <p>If this parameter is set to 1 or 3, AccessAgent enumerates the containers and searches for the authentication certificate that is based on the AuthCertIssuerList and AuthCertKeyUsageBits parameters.</p>	No

Middleware Parameter	Type	Values	Mandatory?
AuthCertIssuerList	REG_MULTI_SZ	<p>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.</p> <p>This multi-string must include the Common Names (CN) of the issuers of the authentication certificate.</p> <p>For a smart card certificate to be selected for authentication, the name of the certificate issuer must be present in this list.</p>	No
AuthCertKeyUsageBits	DWORD	<p>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.</p> <p>This hexadecimal value is the bitwise-OR value of the possible key usage values that are defined in the certificate.</p> <p>The possible key usage bits as defined in the X509v3 specification are:</p> <ul style="list-style-type: none"> • 0x80: digital signature • 0x40: non-repudiation • 0x20: key encipherment • 0x10: data encipherment • 0x08: key agreement • 0x04: certificate signing • 0x02: CRL signing <p>An example of CertSearchKeyUsageBits is A0, which allows the use of the keypair for digital signatures and key encipherment.</p>	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 computer.

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.

Setting up Kerberos authentication

IBM Security Access Manager for Enterprise Single Sign-On supports Kerberos-based login to AccessAgent in personal workstations.

See "Set up Kerberos Authentication" in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide* to verify that your workstation meets the requirements and compatibilities to set up Kerberos authentication.

Configuring IMS Server for Kerberos authentication

Configure the Kerberos environment to enable single sign-on by using IBM Security Access Manager for Enterprise Single Sign-On.

Procedure

1. Create the Active Directory user and register the Service Principal Name (SPN).
 - a. Copy the CreateUserAndKeytab.PS1 file from the IMS Server\bin folder to the Active Directory server.
 - b. Launch the PowerShell command prompt to run the CreateUserAndKeytab.PS1 script on the Active Directory server.
 - 1) Provide the Active Directory account password.
 - 2) Provide the Active Directory domain name. For example: jke.com
 - 3) Provide the fully qualified IMS Server location. For example: <ImMachineName>.jke.com.

Note: This is the value that is set as the IMS Server location when you are installing AccessAgent.

A keytab file is created (For example: <ActiveDirectoryMachineName>.jke.com.keytab) and the Service Principal Name (SPN) is registered on the Active Directory user account object. It is located in the same location as the CreateUserAndKeytab.PS1 script.

Important:

The Kerberos Key Distribution Center (KDC) is a network service that supplies session tickets and temporary session keys to users and computers that are within an Active Directory domain.

The Kerberos Key Distribution Center (KDC) runs on each domain controller as part of Active Directory Domain Services (AD DS).

- When multiple domains are configured, For configuration of multiple, ensure that a trust relationship exists between the domain controller hosting the KDC and the other domain controllers that are configured on IMS Server enterprise directories.
 - The trust direction **must** at least, be from the domain controller hosting the SPN to other domain controllers.
 - If the Active Directory domain controllers are located in different forests, a forest trust **must** exist from the KDC forest to the other forests.
 - The fully qualified IMS Server location **must** be suffixed with the domain name of the domain controller that is hosting the SPN.
2. Create a Kerberos configuration file on the WebSphere Application Server machine.
 - a. Copy the keytab file that is created in Step 1 to the WebSphere Application Server machine.
 - b. On the WebSphere Application Server workstation, run the `configureSpnego.bat` file.

For example, `C:/IBM/ISAM ESS0/IMS Server/bin>configureSpnego.bat --domainName jke.com --kdcHost <ActiveDirectoryMachineName>.jke.com --keytabPath "c:/Test/jke.com.keytab" --imsLocation <ImMachineName>.jke.com`
 3. In the WebSphere Application Server console, fully synchronize the nodes.
 4. Restart WebSphere Application Server.

Note: The keytab Path denotes where the keytab file is.

What to do next

Verify that you have configured Kerberos correctly. See “Verifying the Kerberos configuration.”

Configuring the AccessAgent for Kerberos authentication

You must disable the ESSO Credential Provider on the client computers for Kerberos authentication.

Procedure

Disable the ESSO Credential Provider. See “Disabling the ESSO Credential Provider” on page 40.

Verifying the Kerberos configuration

Verify that Kerberos is configured correctly.

Procedure

1. Enable Internet Explorer to use the Integrated Windows Authentication.
 - a. Navigate to **Internet options**.
 - b. Click **Security > Local intranet**.
 - c. Click **Sites**.
 - d. In Local intranet, click **Advanced**.
 - e. Add the fully qualified hostname in Step 1 from "Configuring IMS Server for Kerberos authentication" on page 56.
2. In Internet Explorer, verify that you are able to log in automatically to <https://imsurl/ims/services/encentuate.ims.service.ContainerAuthentication?WSDL> by using a domain user.

Note: If you are not automatically logged in, see "Known issues and workarounds" on Kerberos configuration in the *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide*.

What to do next

See Chapter 7, "Setting up policy templates," on page 65 to set the authentication provider.

Setting up policies for Kerberos authentication

Set the policies for Kerberos authentication by using Setup Assistant.

Procedure

1. Log on to AccessAdmin.
2. Create a new **Machine Policy Template** or use an existing **Machine Policy Template**.
3. Set `pid_auth_provider` to SPNEGO.
4. Set the system policy, `pid_secret_option` to 0.

Chapter 5. 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 60

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

- “Restricting HTTP connections” on page 60
- “Disabling directory browsing” on page 61

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 that are 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 occurs 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://%{HTTP_HOST}/$1 [L,R]
</VirtualHost>
```

- **If non-standard HTTP and HTTPS ports are used:**

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

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

- **http_port_number**: Replace the **http_port** number with the custom HTTP port number configured in your environment.
- **https_port_number**: Replace the **https_port** number with the custom HTTPS port number configured in your environment.

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.

Chapter 6. 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:// <ihs_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**.

Chapter 7. 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**.

Chapter 8. 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**.

Chapter 9. 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 list:
 - **ipAddress** (default value)
 - **hostName**
 - **aaVersion**
 - **machineGroups**
 - **machineTag**
4. Click **Add**.
5. Click **Update**.

Chapter 10. 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
```

Chapter 11. Command-line interface reference

You can use different commands that are available in Windows, Linux, and Jython 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 7 and Windows Server 2008 or later with Windows User Account Control (UAC) enabled. Run all Administrators with the Admin Approval Mode policy enabled.

To run the command-line tools:

1. Right-click the **cmd** icon.
2. Click **Run As Administrator**.
3. Click **Continue** to proceed.

For more information.

- “cleanImsConfig command”
- “deployIsamessoIms command” on page 74
- “deployIsamessoImsConfig command” on page 75
- “exportImsConfig command” on page 75
- “managePolPriority command” on page 76
- “setupCmdLine command” on page 76
- “upgradeSymCrypto command” on page 76
- “uploadDpx command” on page 77
- “uploadOath command” on page 78
- “uploadSync command” on page 78

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
```

Notices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com[®] are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information; at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.



Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Privacy Policy Considerations

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

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

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

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

Glossary

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

The following cross-references are used in this glossary:

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

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

A

account data

The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag

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

account data item

The user credentials required for logon.

account data item template

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

account data template

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

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)

A hierarchical directory service that enables centralized, secure management

of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential

The Active Directory user name and password.

Active Directory password synchronization

An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification (active RFID)

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

active RFID

See active radio frequency identification.

AD See Active Directory.

administrator

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

API See application programming interface.

application

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

application policy

A collection of policies and attributes governing access to applications.

application programming interface (API)

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

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

authentication factor

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

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

authentication service

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

authorization code

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

auto-capture

A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on

A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

B

base distinguished name

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

base image

A template for a virtual desktop.

bidirectional language

A language that uses a script, such as Arabic and Hebrew, whose general flow of text proceeds horizontally from right to left, but numbers, English, and other left-to-right language text are written from left to right.

bind distinguished name

A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory.

biometrics

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

C

CA See certificate authority.

CAPI See cryptographic application programming interface.

Card Serial Number (CSN)

A unique data item that identifies a hybrid smart card. It has no relation to the certificates installed in the smart card

CCOW

See Clinical Context Object Workgroup.

cell

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

certificate

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

certificate authority (CA)

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

CLI See command-line interface.

Clinical Context Object Workgroup (CCOW)

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

cluster

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

command-line interface (CLI)

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

credential

Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a

user ID and password are credentials that allow access to network and system resources.

cryptographic application programming interface (CAPI)

An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

cryptographic service provider (CSP)

A feature of the i5/OS™ operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

CSN See Card Serial Number.

CSP See cryptographic service provider.

D

dashboard

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

database server

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

data source

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

deployment manager

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

deployment manager profile

A WebSphere Application Server runtime environment that manages operations for a logical group, or cell, of other servers.

deprovision

To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool

A collection of virtual desktops of similar

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

directory

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

directory service

A directory of names, profile information, and machine addresses of every user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery

The process of restoring a database, system, policies after a partial or complete site failure that was caused by a catastrophic event such as an earthquake or fire. Typically, disaster recovery requires a full backup at another location.

disaster recovery site

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

distinguished name (DN)

The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region.

DLL See dynamic link library.

DN See distinguished name.

DNS See domain name server.

domain name server (DNS)

A server program that supplies name-to-address conversion by mapping domain names to IP addresses.

dynamic link library (DLL)

A file containing executable code and data bound to a program at load time or run time, rather than during linking. The code and data in a DLL can be shared by several applications simultaneously.

E

enterprise directory

A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)

A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

ESSO See enterprise single sign-on.

event code

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

F

failover

An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

fast user switching

A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)

A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

FIPS See Federal Information Processing Standard.

fix pack

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

FQDN

See fully qualified domain name.

fully qualified domain name (FQDN)

In Internet communications, the name of a host system that includes all of the subnames of the domain name. An example of a fully qualified domain name is rchland.vnet.ibm.com. See also host name.

G

GINA See graphical identification and authentication.

GPO See group policy object.

graphical identification and authentication (GINA)

A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)

A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

high availability (HA)

The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

host name

In Internet communication, the name given to a computer. The host name might be a fully qualified domain name such as mycomputer.city.company.com, or it might be a specific subname such as mycomputer. See also fully qualified domain name, IP address.

hot key

A key sequence used to shift operations

between different applications or between different functions of an application.

hybrid smart card

An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

interactive graphical mode

A series of panels that prompts for information to complete the installation.

IP address

A unique address for a device or logical unit on a network that uses the Internet Protocol standard. See also host name.

J

Java Management Extensions (JMX)

A means of doing management of and through Java technology. JMX is a universal, open extension of the Java programming language for management that can be deployed across all industries, wherever management is needed.

Java runtime environment (JRE)

A subset of a Java developer kit that contains the core executable programs and files that constitute the standard Java platform. The JRE includes the Java virtual machine (JVM), core classes, and supporting files.

Java virtual machine (JVM)

A software implementation of a processor that runs compiled Java code (applets and applications).

JMX See Java Management Extensions.

JRE See Java runtime environment.

JVM See Java virtual machine.

K

keystore

In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication

and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol (LDAP)

An open protocol that uses TCP/IP to provide access to directories that support an X.500 model. An LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode

A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Terminal or Citrix Server and improves the single sign-on startup duration.

linked clone

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

load balancing

The monitoring of application servers and management of the workload on servers. If one server exceeds its workload, requests are forwarded to another server with more capacity.

lookup user

A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

managed node

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

mobile authentication

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

N

network deployment

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

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

node agent

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

O

one-time password (OTP)

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

OTP See one-time password.

OTP token

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

P

password aging

A security feature by which the superuser can specify how often users must change their passwords.

password complexity policy

A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

personal identification number (PIN)

In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

PIN See personal identification number.

pinnable state

A state from an AccessProfile widget that

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

PKCS See Public Key Cryptography Standards.

policy template

A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector

A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor

The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

private key

In computer security, the secret half of a cryptographic key pair that is used with a public key algorithm. The private key is known only to its owner. Private keys are typically used to digitally sign data and to decrypt data that has been encrypted with the corresponding public key.

provision

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

provisioning API

An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge

An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning system

A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

Public Key Cryptography Standards (PKCS)

A set of industry-standard protocols used for secure information exchange on the Internet. Domino® Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

published application

An application installed on Citrix XenApp server that can be accessed from Citrix ICA Clients.

published desktop

A Citrix XenApp feature where users have remote access to a full Windows desktop from any device, anywhere, at any time.

R**radio frequency identification (RFID)**

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

random password

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

RDP See remote desktop protocol.

registry

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

registry hive

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

remote desktop protocol (RDP)

A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

replication

The process of maintaining a defined set of data in more than one location. Replication involves copying designated changes for one location (a source) to another (a target) and synchronizing the data in both locations.

revoke

To remove a privilege or an authority from an authorization identifier.

RFID See radio frequency identification.

root CA

See root certificate authority.

root certificate authority (root CA)

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

S

scope A reference to the applicability of a policy, at the system, user, or machine level.

secret question

A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access

The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Sockets Layer (SSL)

A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

Secure Sockets Layer virtual private network (SSL VPN)

A form of VPN that can be used with a standard web browser.

Security Token Service (STS)

A web service that is used for issuing and exchanging security tokens.

security trust service chain

A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

serial ID service provider interface

A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number

A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator

A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)

An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use the device as a second factor in AccessAgent.

signature

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

sign-on automation

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

sign up

To request a resource.

silent mode

A method for installing or uninstalling a product component from the command line with no GUI display. When using silent mode, you specify the data required by the installation or uninstallation program directly on the command line or in a file (called an option file or response file).

Simple Mail Transfer Protocol (SMTP)

An Internet application protocol for transferring mail among users of the Internet.

single sign-on (SSO)

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

smart card

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

smart card middleware

Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot

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

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet. See also web service.

SPI See service provider interface.

SSL See Secure Sockets Layer.

SSL VPN

See Secure Sockets Layer virtual private network.

SSO See single sign-on.

stand-alone deployment

A deployment where the IMS Server is deployed on an independent WebSphere Application Server profile.

stand-alone server

A fully operational server that is managed independently of all other servers, using its own administrative console.

strong authentication

A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity

An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

STS See Security Token Service.

system modal message

A system dialog box that is typically used to display important messages. When a system modal message is displayed,

nothing else can be selected on the screen until the message is closed.

T

terminal emulator

A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

terminal type (tty)

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

thin client

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

transparent screen lock

An feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

trigger

In profiling, an event that causes transitions between states in a states engine, such as, the loading of a web page or the appearance of a window on the desktop.

trust service chain

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

truststore

In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

tty See terminal type.

two-factor authentication

The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

uniform resource identifier

A compact string of characters for identifying an abstract or physical resource.

user credential

Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning

The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user provisioning

The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

VB See Visual Basic.

virtual appliance

A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual channel connector

A connector that is used in a terminal services environment. The virtual channel connector establishes a virtual communication channel to manage the remote sessions between the Client AccessAgent component and the Server AccessAgent.

virtual desktop

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

virtual desktop infrastructure

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

Virtual Member Manager (VMM)

A WebSphere Application Server component that provides applications with a secure facility to access basic

organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)

An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure.

Visual Basic (VB)

An event-driven programming language and integrated development environment (IDE) from Microsoft.

VMM See Virtual Member Manager.

VPN See virtual private network.

WS-Trust

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

W

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

wallet caching

The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager

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

web server

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

web service

A self-contained, self-describing modular application that can be published, discovered, and invoked over a network using standard network protocols. Typically, XML is used to tag the data, SOAP is used to transfer the data, WSDL is used for describing the services available, and UDDI is used for listing what services are available. See also SOAP.

Index

A

- AccessAdmin 10
 - form-based logon 14
 - help URL 14
 - logon 63
 - machine attributes 16
 - session settings 14
 - user attributes 15
 - user interface 10
- AccessAgent
 - animation 46
 - automatic Java sign-on 43
 - configuring interface 37
 - banner 40
 - functionality 41
 - keyboard shortcuts 46
 - launching applications 37
 - transparent screen lock 42
- accessibility v, 46
- animation 46
- Authenex A-Key tokens 78
- authentication setup 47

B

- backup
 - database 33
 - IMS Server 33
 - WAS profiles 33
- base distinguished name
 - Active Directory 3
 - LDAP 7
- bind distinguished name
 - Active Directory 3
 - LDAP 7
- BIO-key
 - deploying in AccessAgent 49
 - deploying in IMS Server 49
 - installation 49
 - NLI resource adapter 48
- biometric
 - See fingerprint

C

- cleanImsConfig command 73
- clientIp.customHeader.delimiter 20
- clientIp.customHeader.isRTL 20
- clientIp.customHeader.name 20
- cn attribute 9
- command-line reference 73
 - cleanImsConfig command 73
 - deployIsmessolms command 74
 - deployIsmessolmsConfig command 75
 - exportImsConfig command 75
 - managePolPriority command 76
 - setupCmdLine command 76
 - upgradeSymCrypto command 76
 - uploadDpx command 77

command-line reference (*continued*)

- uploadOath command 78
- uploadSync command 79

CSV files 78

D

- data source
 - general 21
 - IMS 22
 - log data 23
- database
 - backup 34
 - restore 35
- deployIsmessolms command 74
- deployIsmessolmsConfig command 75
- deployment security 59
 - disabling directory browsing 61
 - removing sample servlets 59
 - restricting HTTP connections 60
 - securing access to data 59
 - setting a logon limit 60
- Digipass 77
- directory servers
 - See enterprise directories
- distinguished name (DN) 8
- DNS (Domain Name System) 4
- Domain Name System (DNS) 4
- DPX files 77

E

- EAR files 75
- education v
- encentuate.ims 20
- enterprise directories
 - description 3
 - LDAP 3, 7
 - lookup user 3, 7
 - Microsoft Active Directory 3
 - Security Directory Server 7
 - testing connection 9
- enterprise directory servers 3
- ESSO Credential Provider 40
- ESSO GINA 40
- event reporting 44
- exportImsConfig command 75

F

- fingerprint 47, 48

G

- glossary 85

H

- Help, Observer 44
- HTTP compression 31
- hybrid smart card 56

I

- IBM
 - Software Support v
 - Support Assistant v
- IMS Bridges
 - basic settings 25
 - IMS Handler 24
 - user names 24
- IMS Configuration keys
 - AccessAdmin 10
 - data source (advanced settings) 21
 - IMS Bridge 24
 - IMS Server settings 16
 - user authentication 25
- IMS Configuration Utility 1, 10
 - adding authentication services 2
 - basic settings 2
 - biometric support 10
 - exporting server configurations 28
 - importing server configurations 29
 - logon 1
 - provisioning administrators 1
 - startup settings 19
 - translating codes 31
 - uploading system data 27
 - utilities 27
- IMS Server 16
 - attribute name 20
 - backup 33
 - certificate 18
 - diagnostic tool 10
 - events system 19
 - keystore 18
 - log server information 18
 - log-signing 17
 - miscellaneous settings 20
 - recovery 33
 - symmetric crypto 18
 - syslog 17

J

- JAR files 28, 75
- Java 43
- JMX 71

K

- keyboard shortcuts 46

L

- Layer 7 20

LDAP
 attribute names 20
 servers 7
load balancer 20

M

machine attributes 69
mail attribute 9
managePolPriority command 76
manageprofiles command 33
Microsoft Active Directory 3

N

NetBIOS
 LDAP configuration 7
 Microsoft Active Directory
 configuration 3

O

Observer Help 44
OTP and MAC 47

P

passwords
 reset 3
 synchronization 3
policy templates 65
problem-determination v
profiles
 backup 33
 restore 34
publications
 statement of good security
 practices v

R

RFID 47

S

security deployment 59
Security Directory Server 7
setupCmdLine command 76
smart card 47
 authentication 51, 53
 hybrid 56
 importing certificates 52
SSL
 Active Directory 5
 LDAP servers 8
system data 27
system modal message 45

T

Tivoli Identity Manager Active Directory
 Adapter 3
training v
transparent screen lock 42

transparent screen lock (*continued*)
 Windows 10 41
 Windows 7 41
 Windows 8 41
two-way SSL 52

U

upgradeSymCrypto command 76
uploadDpx command 77
uploadOath command 78
uploadSync command 79
user authentication
 authorization code 27
 biometrics 27
 logon 25
 password 26
user name attribute 9
user policy templates 67

V

Virtual Member Manager component 3

W

WAS profiles backup 33
Windows 7, Windows 8
 transparent screen lock 42
Windows 7, Windows 8, Windows 10
 Ctrl+Alt+Delete 41
Windows registry 45



Printed in USA