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

Administrator Guide

SC23-9951-03

IBM® Security Access Manager for Enterprise Single Sign-On

Version 8.2

Administrator Guide

SC23-9951-03

Note

Before using this information and the product it supports, read the information in “Notices” on page 59.

Edition notice

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

Contents

About this publication

The IBM® Security Access Manager for Enterprise Single Sign-On provides sign-on and sign-off automation, authentication management, and user tracking to provide a seamless path to strong digital identity. The *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide* describes the procedures for setting up, administering, and testing the product and its components. It covers the functionality and setup options of the product, including internal implementation details.

Intended audience

This publication is for technical users who understand how IBM Security Access Manager for Enterprise Single Sign-On can be enhanced and customized for a specific use of a customer.

This publication is for Administrators and system programmers who must perform the following tasks:

- Maintain the IMS Server.
- Manage users and roles.
- Manage policies and policy templates.
- Manage authentication factors.
- Generate audit logs and reports.

Readers must be familiar with the following topics:

- Managing servers and databases.
- Information specific to the organization.

What this publication contains

This publication contains the following sections:

- Chapter 1, "Overview," on page 1

  Provides an overview of the IBM Security Access Manager for Enterprise Single Sign-On administrative tasks and description about AccessAdmin.
- Chapter 2, "Managing users and roles," on page 3

  Guides you on how to manage users and assign roles by using AccessAdmin.
- Chapter 3, "Managing policy templates," on page 7

  Provides descriptions about policy templates and guides you on how to create and delete templates for users and computers.
- Chapter 4, "Managing authentication factors," on page 17

  Covers the different authentication factors and guides you on how to manage authentication factor-related policies.
- Chapter 5, "Collecting logs and generating audit reports," on page 25

  Guides you on how to generate audit reports and collect audit logs.
- Appendix A, "Accessing the IMS Configuration Utility," on page 31

  Provides instructions on how you can access the IMS Configuration Utility.
- Appendix B, "Updating policies in an upgraded IMS Server," on page 33

Provides instructions on how you can update policies when you are upgrading your IMS Server.

- Appendix C, "Changed policies from 8.1 to 8.2," on page 35

  Provides a list of all policies that have changed from 8.1 to 8.2.
- Appendix D, "Changed policies from 8.0.1 to 8.2," on page 43

  Provides a list of all policies that have changed from 8.0.1 to 8.2.
- Appendix E, "Audit log events," on page 51

  Provides detailed descriptions about the different types of logs, such as User, Administrator, and System logs.

Publications

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

IBM Security Access Manager for Enterprise Single Sign-On library

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

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

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

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

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

  This guide helps you to install the different product components and their required middleware, and also do the initial configurations required to complete the product deployment. It covers procedures for using virtual appliance, WebSphere® Application Server Base editions, and Network Deployment.
- *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*, GC23969201

  Read this guide if you want to configure the IMS Server settings, the AccessAgent user interface, and its behavior.
- *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide*, SC23995103

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

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

  This guide is intended for Help desk officers. The guide helps Help desk officers to manage queries and requests from users usually about their authentication factors. Use this guide together with the IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide.
- *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide*, SC23969401

  Read this guide for the detailed descriptions of the different user, machine, and system policies that Administrators can configure in AccessAdmin. Use this guide along with the IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide.
- *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide*, GC23969301

  Read this guide if you have any issues with regards to installation, upgrade, and product usage. This guide covers the known issues and limitations of the product. It helps you determine the symptoms and workaround for the problem. It also provides information about fixes, knowledge bases, and support.
- *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide*, SC23995603

  Read this guide if you want to create or edit profiles. This guide provides procedures for creating and editing standard and advanced AccessProfiles for different application types. It also covers information about managing authentication services and application objects, and information about other functions and features of AccessStudio.
- *IBM Security Access Manager for Enterprise Single Sign-On Provisioning Integration Guide*, SC23995703

  Read this guide for information about the different Java™ and SOAP API for provisioning. It also covers procedures for installing and configuring the Provisioning Agent.
- *IBM Security Access Manager for Enterprise Single Sign-On Web API for Credential Management Guide*, SC14764600

  Read this guide if you want to install and configure the Web API for credential management.
- *IBM Security Access Manager for Enterprise Single Sign-On Lightweight AccessAgent mode on Terminal Server SDK Guide*, SC14765700

  Read this guide for the details on how to develop a virtual channel connector that integrates AccessAgent with Terminal Services applications.
- *IBM Security Access Manager for Enterprise Single Sign-On Serial ID SPI Guide*, SC14762600

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

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

  This guide is intended for the end users. This guide provides instructions for using AccessAgent and Web Workplace.

- *IBM Security Access Manager for Enterprise Single Sign-On Error Message Reference Guide*, GC14762400

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

Accessing terminology online

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

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

Accessing publications online

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

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

Ordering publications

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

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

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

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

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

Accessibility

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

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

Tivoli technical training

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

Tivoli user groups

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

- 23,000+ members
- 144+ groups

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

Support information

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

Online

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

IBM Support Assistant

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

Troubleshooting Guide

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

Conventions used in this publication

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

Typeface conventions

This publication uses the following typeface conventions:

Bold

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

Italic

- Citations (examples: titles of publications, diskettes, and CDs)
- Words defined in text (example: a nonswitched line is called a *point-to-point line*)

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

`Monospace`

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

Operating system-dependent variables and paths

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

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

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

Chapter 1. Overview

This section provides an overview about the different tasks of an Administrator. Use AccessAdmin to manage users, roles, policies, and reports.

See the following topics for more information.
- "Administrative tasks"
- "Logging on to AccessAdmin"

Administrative tasks

As an Administrator, you can manage users, policy templates, authentication factors, reports, and perform IMS Server backups.

What to do	Where to find information
Manage users • Assign and revoke roles.	Chapter 2, "Managing users and roles," on page 3
Managing policy templates • Use machine, user, and system policy templates to control the behavior of the entire IBM Security Access Manager for Enterprise Single Sign-On system.	Chapter 3, "Managing policy templates," on page 7
Managing authentication factors • Modify policies related to authentication factors like passwords, RFID, and smart cards.	Chapter 4, "Managing authentication factors," on page 17
Generate reports • Use audit information for enhanced IBM Security Access Manager for Enterprise Single Sign-On administration.	Chapter 5, "Collecting logs and generating audit reports," on page 25
Back up the IMS Server	See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for more details.

Logging on to AccessAdmin

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

Procedure

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

4. Click **Log on**.

Chapter 2. Managing users and roles

There are three roles in IBM Security Access Manager for Enterprise Single Sign-On: Administrator, Help desk, and user. You can assign roles, assign users to a Help desk role, delete users, and view user settings.

See the following topics for more information.

- "Assigning roles"
- "Assigning users to a Help desk" on page 4
- "Revoking users" on page 4
- "Viewing a user profile" on page 4
- "Assigning users and templates to a Help desk" on page 5

Assigning roles

You can assign a user with an Administrator role, a Help desk role, or a user role in AccessAdmin.

About this task

Each role has a different scope of responsibilities and privileges:

Administrator

- Is provisioned during the IMS Server configuration.
- Has full access to the AccessAdmin and AccessStudio applications.
- Can demote and promote any user to the Administrator or Help Desk role in AccessAdmin. An Administrator cannot demote its own account.
- Can create, upload, and download AccessProfiles from the IMS Server.

Help desk officer

- Can manage user authentication factors and user policies.
- Can issue authorization codes.

User

- Can log on to various systems and applications.
- Can ask the Administrators and Help desk officers for help when users forget their passwords or get locked out of their accounts.

Procedure

1. Log on to AccessAdmin.
2. Search for the user.
3. In the **User Profile** page, scroll down to the **Administrative Policies** panel.
4. Select the role in the drop-down box.
5. Click **Update**.

Assigning users to a Help desk

When users need assistance with the product, they request help from their appointed Help desk officers. Therefore, you must assign users to a Help desk role so that the appropriate Help desk officers can view and manage all users assigned to them.

Procedure

1. Log on to AccessAdmin.
2. Search for a user.
3. In the **User profile** page, scroll down to **Administrative Policies**.
4. Select the Help desk officer to which you want to assign that user.
5. Click **Update**.

Revoking users

You can revoke or de-provision a user. This task is typically done when the user leaves the organization.

About this task

Revoking the user permanently disables the user account and prevents any user with the same name from being created. When you revoke a user, all user audit data are retained in the database.

A de-provisioned user cannot log on to AccessAgent. If the de-provisioned user attempts to log on to AccessAgent, the user cached Wallet is deleted. The user does not have subsequent access even if AccessAgent cannot connect to the IMS Server.

Procedure

1. Log on to AccessAdmin.
2. Search for the user.
3. Under **User Profile**, scroll down to the **Administrative Policies** panel.
4. Click **Revoke user**.
5. Click **Update**.

Viewing a user profile

Search for user profiles in AccessAdmin so you can view their authentication and administrative settings.

Procedure

1. Log on to AccessAdmin.
2. Select **Search users** > **Search**.
3. Enter the subject of your search in the **Search for** field.

   Tip: To find partially matching results, enter the characters, and then an asterisk (*). For example: To find all users with user names that begin with the letter `i`, enter `i*`.
4. Select a search criteria from **Search by**.
5. Click **Search**.
6. Click the user name. The following links are displayed.

Option	Description
Audit logs	This link contains specific details about user activity. For example: Time, IP address, and the SOCI ID.
Authentication service	This link contains the different types of authentication services enabled for the user.

7. Scroll down the page. The following details are displayed under **User Profile**.
   - Name
   - Last name
   - E-mail address
   - Enterprise user name
   - User principle name
   - Mobile ActiveCode phone number
   - Mobile ActiveCode e-mail address
   - Mobile AcitveCode preferences
   - Help desk Authorization
   - Authentication Factors
   - OTP Token Assignment
   - Cached Wallets
   - Wallet Access Control
   - Administrative Policies
   - Authentication Policies
   - AccessAssistant and Web Workplace Policies
   - Wallet Policies
   - AccessAgent Policies
   - Authentication Service Policies

Assigning users and templates to a Help desk

Users request product assistance from their appointed Help desk officers. For such a case, you must assign users to a Help desk so that the appropriate Help desk officers can view and manage all users assigned to them.

About this task

Determine if a new Help desk user can manage all new users. If so, you can automatically assign all policy templates and new users to the new Help desk user.

Procedure

1. Log on to the IMS Configuration Utility.
2. Select **Advanced Settings** > **AccessAdmin** > **User Attributes** > **Automatically assign all policy templates and users to new Help desk user**.
3. Click **Update**.

Chapter 3. Managing policy templates

A policy template is a set of predefined user or computer policies that can be applied to users or computers. You can create, assign, and configure user and computer policy templates. System policies do not have a template.

The following table provides details about the Administrator and Help desk roles and their policy privileges.

Role	System Policies	Computer Policies	User Policies
Administrator	Can view and modify	Can view and modify	Can view and modify
Help desk	Can view only	Can view only	Can view and modify, except administrative policies Can modify: • Wallet authentication policies • AccessAgent policies

The following table provides details about the tasks involved in managing User and Machine Policy Templates and System Policies.

What to do	Where to find information
Automatically create a User or Machine Policy Template. *(Optional)*	"Setting up policy templates" on page 8
Create a User Policy Template.	"Creating a User Policy Template" on page 9
Apply a User Policy Template.	"Applying a User Policy Template" on page 9
Automatically assign a User Policy Template to new users. *(Optional)*	"Automatically assigning User Policy Templates to new users" on page 10
Delete a User Policy Template. *(Optional)*	"Deleting a user or machine policy template" on page 11
Create a Machine Policy Template.	"Creating a Machine Policy Template" on page 12
Apply a Machine Policy Template.	"Applying a Machine Policy Template" on page 12
Automatically assign a Machine Policy Template to computers. *(Optional)*	"Setting machine criteria" on page 13
Delete a Machine Policy Template. *(Optional)*	"Deleting a user or machine policy template" on page 11
Set system policies.	"Setting system policies" on page 15
Set authentication service policies.	"Setting authentication service policies" on page 16
Set application policies.	"Setting application policies" on page 16

Setting up policy templates

Use Setup assistant to set up policy templates.

About this task

This is an optional task. You can manually create a Machine Policy Template if you prefer.

In this procedure, you can specify the following settings for your organization:

- Automatic sign up or self service features
- Second authentication factors or a combination of these
- Shared or personal workstations
- AccessAgent enablement for Citrix or Terminal Server
- RFID-only logon
- Hybrid smart card-only logon

Procedure

1. Log on to AccessAdmin.
2. Click **Setup assistant**.
3. Click **Begin**.
4. Select your initial system settings.
   - **Enable automatic sign up**
   - **Enable self-service features**
5. Click **Next**.
6. Select the second factors that your users can use to authenticate.
   - **RFID card**
   - **Active RFID badge**
   - **Fingerprint**
   - **RFID card or fingerprint**
   - **Smart card**
   - **Hybrid Smart card**
7. Click **Next**.
8. Select whether your users are using personal or shared workstations.
   - **Support shared workstations**
   - **Support personal workstations**
9. Click **Next**.
10. Select the appropriate desktop types for your users.
    - **Use a shared desktop**
    - **Support private desktops**
    - **Support roaming desktops**
11. Click **Next**.
12. Select whether you want AccessAgent to be enabled for Citrix or Terminal Server.
13. Click **Next**.
14. Type a name for the policy template.

15. Click **Next**.
16. Select whether your users can use combinations of authentication factors to logon.
17. Click **Next**.
18. Specify your RFID-only logon settings.
19. Click **Next**.
20. Specify your single factor hybrid smart card settings.
21. Click **Next**.
22. Click **Next**.
23. Click **Done**.

Creating a User Policy Template

For a faster policy implementation, use a policy template to apply a set of policies to a specific set of users.

About this task

- A User Policy Template is automatically applied to a user upon registration.
- If you modify any of the policies in the User Policy Template, reassign the updated template to the users to implement the policy changes. For more information, see “Applying a User Policy Template.”
- The existing policies of the users also remain the same when attributes of the user are changed or when the User Policy Template matching criteria is changed.

Procedure

1. Log on to AccessAdmin.
2. Select **User Policy Templates** > **New template**.
3. Enter a name at **Template Name**. The name can be composed of any alpha-numeric characters. The name is case-sensitive, so **Example** and **example** are two different template names.
4. In the **Administrative Policies** panel, select the Help desk officer to whom this new policy template applies.
5. Click the panel heading to expand the policies.
6. Specify information for any of these policies. For example, under **Authentication Policies**, select a **Wallet authentication policy**.
7. Click **Add** to save the new settings. The new template is displayed in the AccessAdmin navigation panel.

Applying a User Policy Template

After creating a User Policy Template, you must apply it to your users so that the policies are implemented.

Procedure

1. Log on to AccessAdmin.
2. Select **Search users** > **Search**.
3. Enter the subject of your search in the **Search for** field.

Tip:
To find partially matching results, enter the characters, and then an asterisk (*). For example: To find all users with user names that begin with the letter `i`, enter `i*`.

   a. Select a search criteria from the **Search by** list.
   b. Click **Search**.

4. Optional: Select any of the following groups:
   - My users
   - All Administrators
   - All help desk users
   - All revoked users
5. Specify the number of results to view per page.
6. Select one or more users by selecting the check box next to the corresponding user. Click **Select all** if you want to assign policies to all users in the page.
7. Select the template you want to apply under **Apply user policy template**.
8. Click **Apply to selected results**. The **Apply to all results** button is applicable to the users displayed on the page.

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**.

Applying policy changes

If there are specific policies that you want to apply to specific users only, do this task so that the rest of your users still follow the policies previously assigned to them.

Procedure

1. Log on to AccessAdmin.
2. Select **Search users** > **Search**.
3. Enter the subject of your search in the **Search for** field.

   Tip: To find partially matching results, enter the characters, and then an asterisk (*). For example: To find all users with user names that begin with the letter `i`, enter `i*`.

   a. Select a search criteria from the **Search by** list.

   b. Click **Search**.
4. Optional: Select any of the following groups:
   - My users
   - All Administrators
   - All help desk users
   - All revoked users
5. Specify the number of results to view per page.
6. Select one or more users by selecting the check box next to the corresponding user.
7. Optional: Click **Select all** if you want to assign policies to all users in the page.
8. Under **Apply policies**, click **Show user policies** to view the polices you want to apply.
9. Click **Apply to selected results**.
10. Optional: Click **Apply to all results** if you want to select all the users displayed on the page.

Deleting a user or machine policy template

Delete a user or machine policy template if it is no longer applicable to the user or computer.

Procedure

1. Log on to AccessAdmin.
2. From the navigation panel, select the appropriate user or computer policy template page.
   - For user policy templates, select **User Policy Templates** > *name of template*.
   - For computer policy templates, select **Machine Policy Templates** > **Template Assignments** > *name of template*.
3. Scroll to the bottom of the page and click **Delete**.

Creating a Machine Policy Template

Use a policy template to apply a set of policies to a specific set of computers for faster policy implementation.

About this task

The default Machine Policy Template:

- Does not have any machine criteria.
- Is applied automatically if there are no other templates applicable to the computer.
- Is always the last item in the list of **Preferred policy templates**.

The machine policy template at the top of the **Preferred policy templates** list is the first template applied to a computer.

Tip:
If you want a Machine Policy Template to be automatically applied to computers that match a criteria, see "Setting machine criteria" on page 13.

Procedure

1. Log on to AccessAdmin.
2. Select **Machine Policy Templates** > **New template**.
3. Enter a name for the new template. The name can be composed of any alpha-numeric characters. The name is case-sensitive, so **Example** and **example** are two different template names.
4. Specify whether the new machine policy template is the default template or the template for specific computers.

   See "Setting machine criteria" on page 13 for more details.
5. Click the panel heading to expand the policies.
6. Specify information for any of these policies. For example, under **Authentication Policies**, add a second authentication factor.
7. Click **Add** to save the new settings.

Applying a Machine Policy Template

After creating a Machine Policy Template, you must apply it to specific computers so that the policies are implemented. Machine policy templates are used as reference for the policy settings applicable to a computer of a specific criteria.

About this task

Machine policy templates are applied to computers only during computer registration. Subsequent changes to computer attributes do not affect the machine policy template assignment.

Procedure

1. Log on to AccessAdmin.
2. Select **Machines** > **Search**.
3. Click the computer name link.
4. Under **Machine policy template assignment**, select a template from the list.
5. Click **Assign**.

Setting machine criteria

When creating a machine policy template, you can select a computer that matches all or any of the specified criteria.

Procedure

1. Specify whether you want the computer filtered as they match all or any of the criteria.
   - Select **Match all of these criteria** to match every search attribute criteria you have set.
   - Select **Match any of these criteria** to match some and not all the criteria you have set.
2. Click the **+** icon to add criteria fields and click the **x** icon to delete.

   Note: The order by which the criteria is displayed does not matter. You can use the **up** and **down** arrows to set a preferred order for your criteria.
3. Select attribute options from the list.

Option	Description
AccessAgent version	Specifies the version of AccessAgent installed in your computer.
Host name	Specifies the unique name or identification of your domain.
IP address	Specifies the Internet Protocol address or the unique number assigned to your computer in a network. **Note:** IBM Security Access Manager for Enterprise Single Sign-On 8.1 supports Internet Protocol version 6 (IPv6).
Active Directory groups	Specifies the Active Directory security group of your computer. A computer can belong to several groups. This criterion is satisfied as long as the computer matches to at least one of the groups.
Machine tag	Specifies a registry entry to identify the computer.

4. Use the following comparison operators:
   - **is**: if you want to search for the exact attribute
   - **is not**: if you do not want to match this criteria to any attribute
   - **is like**: if you want to search for a similar attribute
5. You can also use the following wildcard or character combinations in the criteria field when using the **is like** option.
   - `abc` - Use this combination if you know what you are looking for. It specifies the letters search string.
   - `*abc` - Use this combination if you are not sure of the first letter but you know the succeeding letters of your search string.
   - `abc*` - Use this combination if you know the first few letters of the search string except for the last letter.

Creating machine tags

You can use the machine tag attribute during machine template assignment. This machine attribute is useful in deployments where the IMS Server uses another enterprise directory like Tivoli Directory Server.

About this task

This attribute is also useful in some Active Directory scenarios. For example, there are instances where computers are not managed by Active Directory or when there is complex grouping requirements not met by AccessAdmin. Machine tags are the unique identifiers in these scenarios.

You can assign tags to different groups of computers. You can then use the `machinetag` attribute to assign Machine Policy Templates to different groups of computers.

Procedure

1. On the Windows desktop, click **Start** > **Run**.
2. In the **Open** field, enter `regedit` and click **OK**.
3. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\DeploymentOptions`.
4. Right-click and select **New** > **String Value**.
5. Enter `MachineTag`.
6. Right click `MachineTag` and select **Modify**.
7. Enter a name. For example, `mycomputer`.
8. Click **OK**.

What to do next

You can now assign machine policy templates by using the machine tag attribute. For more information, see “Applying a Machine Policy Template” on page 12. Make sure that you use the `Machine tag` attribute when searching for computers.

Searching for computers

You can search for computers either through machine attributes or through machine policy templates.

Searching by attributes

Searching by attributes lets you search for computers based on computer information.

Procedure

1. Select **Machines** > **Search**.
2. Enter an asterisk (*) in the **Search For** field to search for all computers.
3. Select a specific attribute from the **Search by** field.
4. Click **Search**.

   You can search for a computer by using any of these search attributes:

Option	Description
Host name	Specifies the unique name or identification of your domain.

Option	Description
IP address	Specifies the Internet Protocol address or the unique number assigned to your computer in a network.
AccessAgent version	Specifies the version of AccessAgent installed in your computer.
Active Directory groups	Specifies the Active Directory security group of your computer. A computer can belong to several groups. This criterion is satisfied if the computer matches at least one of the groups.
Machine tag	Specifies the computer policy template to which the computer is grouped.

5. Click **Search**.

Searching by template

Use AccessAdmin to search for computers by using machine policy templates.

Procedure

1. Select **Machines** > **Search**.
2. Select a template from the **Search in template** list.
3. Click **Search**.

Sorting the order of Machine Policy Templates

You can sort the Machine Policy Templates so that your preferred templates are listed based on priority.

Procedure

1. Log on to AccessAdmin.
2. Select **Machine Policy Templates** > **Template assignments**.
3. Navigate to **Machine policy template assignments** > **Preferred policy templates**.
4. Sort the order of the policy templates by selecting the template, and then clicking either the **Up** arrow or **Down** arrow to move it.

   Note: You can click the machine policy template link to view, delete, reset, or edit the details of the machine policy template.
5. Click **Update** to apply the changes in the sequence of the preferred policy templates.
6. In the **Default machine policy template** list, select the template you want to set as default.

   This template is applied automatically when none of the other machine policy templates are applicable to the computer.
7. Click **Update** to apply the changes in the **Preferred policy templates**.

Setting system policies

System policies are policies that are applicable to all users and computers. Use AccessAdmin to access and modify a system policy.

Procedure

1. Log on to AccessAdmin.
2. Select **System** > **System Policies**.
3. Click the panel heading to expand the policies.
4. Update the policies.
5. Click **Update**.

Setting authentication service policies

You can verify the validity of an account through an authentication service. You can set the password and authentication policies for an authentication service.

Procedure

1. Log on to AccessAdmin.
2. Select **System** > **Authentication Service Policies**.
3. Click an authentication service.
4. Click **Password Policies**.
5. Update the policies.
6. Click **Update**.
7. Click **Authentication Policies**.
8. Update the policies.
9. Click **Update**.

Setting application policies

You can set the password, reauthentication, and log off policies for specific applications in AccessAdmin.

Procedure

1. Log on to AccessAdmin.
2. Select **System** > **Application Policies**.
3. Click an application.
4. Update the **Application Policies**.
5. Click **Update**.

Chapter 4. Managing authentication factors

As Administrator, you can modify the settings on the authentication factors of your users. You can modify authentication-related policies in AccessAdmin.

IBM Security Access Manager for Enterprise Single Sign-On supports the following authentication factors:

- Password
- RFID
- Password and RFID
- ARFID
- Fingerprint
- Smart card
- Hybrid smart card
- Mobile ActiveCode
- One-time password (OTP)

See the following topics for more information.

- "Setting password policies"
- "Setting the authentication factor policies"
- "Setting authentication service policies" on page 16
- "Setting policies for both fingerprint and RFID authentication" on page 20
- "Generating authorization codes for users" on page 21
- "Revoking authentication factors" on page 22

Setting password policies

Set password policies in AccessAdmin to ensure that users create strong passwords.

About this task

For Active Directory deployments, IBM Security Access Manager for Enterprise Single Sign-On depends on the Active Directory password policies. This procedure applies to non-Active Directory password synchronization scenarios.

Procedure

1. Log on to AccessAdmin.
2. Navigate to **System** > **System policies** > **Password Policies**.
3. Modify the policies.
4. Click **Update** to confirm the changes.

Setting the authentication factor policies

You can configure the AccessAgent behavior or action for a selected second authentication factor. You can also modify time-related settings of the authentication factor.

Before you begin

Log on to AccessAdmin.

Procedure

- **Smart card policies**
  1. Under **User Policy Templates**:
     - Select **New template** > **AccessAgent Policies** > **Smart card Policies**.
     - Optional: Select *name of template* > **AccessAgent Policies** > **Smart card Policies**.
  2. Complete the following fields:

Option	Description
Smart card removal actions	The action that AccessAgent takes when the smart card is removed.
Enable single factor smart card unlock	Specifies whether the single factor smart card unlock is supported.
Time expiry, in seconds, for single factor smart card unlock	Specifies the expiration, indicated in seconds, for single factor smart card unlock.
Time expiry, in minutes, for single factor smart card logon	Specifies the expiration, indicated in minutes, for single factor smart card logon.
Extend single factor smart card logon time expiry when user logs on with smart card and PIN	Specifies whether to extend single factor smart card logon time expiry when the user logs on by using smart card and PIN.
Actions on presenting same smart card on desktop if user logged on with single factor	The action that AccessAgent takes when the same smart card is presented when the user is logged on with a single factor.
Confirmation countdown duration, in seconds, for presenting the same smart card on desktop	The countdown time frame for the specified action to take place after tapping the same smart card.
Actions on presenting different smart card on desktop if user logged on with single factor	The countdown time frame for the specified action to take place after tapping a different smart card when the user is logged on with a single factor.
Confirmation countdown duration, in seconds, for presenting a different smart card on desktop	The countdown time frame for the specified action to take place after tapping a different smart card.

  3. Click **Update**.
- **RFID policies**
  1. Under **User Policy Templates**:
     - Select **New template** > **AccessAgent Policies** > **RFID Policies**.
     - Optional: Select *name of template* > **AccessAgent Policies** > **RFID Policies**.
  2. Complete the following fields:

Option	Description
Actions on tapping same RFID on desktop	The action that AccessAgent takes when the logged on user taps the RFID Card on the reader again.

Option	Description
Confirmation countdown duration, in seconds, for tapping same RFID on desktop	The countdown time frame for the specified action to take place after tapping the same RFID Card on the reader. A dialog box is displayed with a countdown timer. The user must specify whether AccessAgent reacts to the same RFID tap. The user can either click **Yes** so that AccessAgent can react, or **No** to reactivate the desktop. If the user clicks neither option during the specified countdown time frame, AccessAgent reacts to the same RFID tap.
Enable RFID-only unlock	Specifies whether RFID-only unlock is supported.
Time expiry, in seconds, for RFID-only unlock	Specifies the expiration indicated in seconds, for RFID-only unlock.
Time expiry, in minutes, for RFID-only logon	Specifies the expiration indicated in minutes, for RFID-only unlock.
Actions on tapping different RFID on desktop	The action that AccessAgent takes when another user taps the RFID Card on the reader, even if there is a user already logged on.
Confirmation countdown duration, in seconds, for tapping different RFID on desktop	The countdown time frame for the specified action to take place after tapping a different RFID Card on the reader. A dialog box is displayed with a countdown timer. The user must specify whether AccessAgent reacts to a different RFID tap. The user can either click **Yes** to let AccessAgent react, or **No** to reactivate the desktop. If the user clicks neither option during the specified countdown time frame, AccessAgent reacts to a different RFID tap.

3. Click **Update**.

- **Fingerprint Policies**
  1. Under **User Policy Templates**:
     - Select **New template** > **AccessAgent Policies** > **Fingerprint Policies**.
     - Optional: Select *name of template* > **AccessAgent Policies** > **Fingerprint Policies**.
  2. Complete the following fields:

Option	Description
Actions on tapping same fingerprint on desktop	The action that AccessAgent takes when a logged on user imprints a finger on the fingerprint reader.

Option	Description
Confirmation countdown duration, in seconds, for tapping same finger on desktop	The countdown time frame for the specified action to take place after a logged on user imprints a finger on the fingerprint reader. A dialog box is displayed with a countdown timer. The user must specify whether AccessAgent reacts to the finger imprint. The user can either click **Yes** to let AccessAgent react, or **No** to reactivate the desktop. If the user clicks neither option during the specified countdown time frame, AccessAgent reacts to the finger imprint.
Actions on tapping different finger on desktop	The action that AccessAgent takes when another user imprints a finger on the reader, even though there is one user already logged on.
Confirmation countdown duration, in seconds, for tapping different finger on desktop	The countdown time frame for the specified action to take place after imprinting a different finger on the fingerprint reader. A dialog box is displayed with a countdown timer. The user must specify whether AccessAgent reacts to a different finger imprint. The user can either click **Yes** to let AccessAgent react, or **No** to reactivate the desktop. If the user clicks neither option during the specified countdown time frame, AccessAgent reacts to a different finger imprint.

3. Click **Update**.

Setting policies for both fingerprint and RFID authentication

If your organization uses both fingerprint and RFID for authentication, make sure to set the appropriate policies first.

Procedure

1. Log on to AccessAdmin.
2. Under **Machine Policy Templates**:
   - Select **New template** > **Authentication Policies**.
   - (Optional) Select *name of template* > **Authentication Policies**.
3. In the **Authentication second factors supported** field, set to **Fingerprint** and **RFID** (in that order) if AccessAgent prompts for a fingerprint during sign up and click **Add**. Set the **Authentication second factors supported** to **RFID** and **Fingerprint** (in that order) if AccessAgent prompts for an RFID card during sign up.
4. Under **System**, select **System policies** > **Configurable Text Policies** > **EnGINA Text Policies**.
5. Set **Instructions for fingerprint or RFID log on (Maximum 2 lines)**.

6. Under **System**, select **System policies** > **Configurable Text Policies** > **Unlock Text Policies**.
7. Set the configurable text policies for simultaneous Fingerprint and RFID support:
   - **Instructions for unlocking with fingerprint or RFID when unlock policy is 'only the same user can unlock' (Maximum 2 lines)**
   - **Instructions for unlocking with fingerprint or RFID when unlock policy is 'any user with or without current desktop account in Wallet can unlock' (Maximum 2 lines)**
   - **Instructions for unlocking with fingerprint or RFID when unlock policy is 'only the same user can unlock, but different user can relog on to Windows' (Maximum 2 lines)**
8. Click **Update**.

Generating authorization codes for users

You can issue authorization codes to users when they lose their second authentication factors or when they forget their passwords.

Procedure

1. Log on to AccessAdmin.
2. Search for a user.
3. Navigate to **User Profile** > **Helpdesk Authorization**.
4. Ask the user whether a request code is displayed on screen.
   - If there is a request code, click **Temporary offline access to the Wallet** and enter the request code.

     Tip: The user has a request code because connectivity to the IMS Server might not be available.

     As a security measure, the user must provide a request code before you can issue an authorization code for temporary offline access.

     Note: You must inform the user that for temporary offline access, the new password is only valid for that computer.
   - If there is no request code, click **Password reset, temporary online access or registration of second factors**.
5. Enter the **Authorization request code**.

   The code is not case sensitive.
6. Select a validity period from the options in the list.
7. Click **Issue authorization code**.

Enabling ActiveCode for the user

ActiveCodes are short-term authentication codes that serve as second-factor authentication. When an authentication service is ActiveCode-enabled, the user needs an ActiveCode each time they use the authentication service.

Procedure

1. Log on to AccessAdmin.
2. Search for the user.
3. In the user settings, click **Authentication services**.

4. In **ActiveCode-enabled authentication service**, select the ActiveCode-enabled authentication services of the new user.
5. Enter the user name for the ActiveCode-enabled authentication service.
6. Click **Add Account**.

Locking the ActiveCode-enabled authentication service for users

To temporarily prevent a user from using an ActiveCode-enabled authentication service, you can lock the service. You can also set the service to lock a user automatically after entering the wrong ActiveCodes several times.

Procedure

1. Log on to AccessAdmin.
2. Search for the user.
3. In the user settings, click **Authentication services**.
4. In **ActiveCode-enabled authentication service**, select the user name and the ActiveCode-enabled authentication service to disable.
5. Select **Locked** from the **Status** list.
6. Click **Update status** to confirm the change.

Deleting ActiveCode for users

You can delete the access of a user to an ActiveCode-enabled authentication service if the user no longer uses it.

Procedure

1. Log on to AccessAdmin.
2. Search for the user.
3. In the user settings, click **Authentication services**.
4. In **ActiveCode-enabled authentication service**, select the user name you want to delete for an ActiveCode-enabled authentication service account.
5. Click **Delete account**.
6. Click **OK**.

Revoking authentication factors

Revoke the second authentication factor or Wallet when the user leaves the organization or when a second authentication factor is reported lost or stolen.

Procedure

1. Log on to AccessAdmin.
2. Search for the user.
3. In the settings of the user, scroll down to the **Authentication Factors** panel. All authentication factors are displayed.
4. Select the check box of the Wallet or authentication factor to revoke.
5. Click **Revoke**.

Setting Wallet policies

You can set Wallet policies such as synchronization interval with the IMS Server, Wallet caching option, exporting, and the display of passwords in AccessAdmin.

Procedure

1. Log on to AccessAdmin.
2. For user scope Wallet policies, navigate to **User Policy Templates** > **New template** > **Create new policy template** > **Wallet Policies**.
3. Optional: Navigate to **User Policy Templates** > *name of template* > **Create new policy template** > **Wallet Policies**.
4. For system scope Wallet policies, navigate to **System** > **System policies** > **Wallet Policies** panel.
5. Modify the policies.
6. Click **Update**.

Setting Wallet authentication policies

A Wallet contains the user name and password of the user. Enforce the use of authentication factors to secure access to the Wallet.

About this task

When setting a Wallet authentication policy:

If you select	The following authentication is required
Smart card	A smart card PIN
Fingerprint	Fingerprint authentication
Password	Password + RFID is enabled

Procedure

1. Log on to AccessAdmin.
2. Navigate to **User Policy Templates** > **New Template**.
3. Optional: Navigate to **User Policy Templates** > *name of template*.
4. In the **Authentication Policies** panel, select the check box corresponding to the preferred Wallet authentication policy.
5. Click **Add**.

Locking Wallets

You can lock the Wallet to prevent a user from accessing the Wallet.

About this task

You can lock the Wallet of a user to:

- Temporarily bar access to the user Wallet. For example, when the user goes for an extended holiday or a prolonged medical leave.
- Prevent access until the user is revoked from the IMS Server. For example, when a user leaves the organization.

Procedure

1. Log on to AccessAdmin.
2. Search for the user.
3. Navigate to **User Profile** > **Wallet Access Control**.
4. Click **Lock**.

Chapter 5. Collecting logs and generating audit reports

Use AccessAdmin to collect audit logs. Use the Tivoli Common Reporting (TCR) tool to generate audit reports.

See the following topics for more information.

- "Collecting audit logs in AccessAdmin"
- "Generating reports in Tivoli Common Reporting tool 1.2" on page 26
- "Generating reports in Tivoli Common Reporting tool 2.1" on page 28

Collecting audit logs in AccessAdmin

An audit log displays the details of each activity. For example: user name, date, and the result of the activity. Select an event and period to limit the scope of the query.

Procedure

1. Log on to AccessAdmin.
2. Select **System** > **Audit Logs**.
3. Select an event from the **Choose search criterion** field.

   To select multiple events, press the **Ctrl** key on your keyboard while clicking an event.
4. Select **Search From** to specify the date range of the activity. Specify the **Search from** and **Search to** dates.
   - You can either enter the date or click the date picker to select a day, a month, or a year.
   - You can either enter the time or click the up and down arrow to change the time.
   - To search from a number of days before the current date, select **Search by preceding days**, and enter a number in the field.
5. To save the search criteria for future retrieval, select **Save query as** and enter a file name.
6. Click **Search**. The audit logs are displayed.

   Note: See Appendix E, "Audit log events," on page 51 for more details.

Viewing user audit logs

User audit logs contain a detailed list of all the user actions. Search for the user to view the corresponding user logs.

Procedure

1. Log on to AccessAdmin.
2. Search for a user.
3. In the user settings, click **Audit logs**. The log entries of the user are displayed.

Tracking custom events

You can track custom events through their assigned event codes.

About this task

You can create custom events to track application-specific events such as:

- Access to confidential data
- Attempted access to application features that the user is not authorized to use
- Access to application outside office hours

Procedure

1. Log on to AccessAdmin.
2. Select **System Policies** > **AccessAudit policies**.
3. Add each pair of event code and display text to `List of custom audit event codes and their corresponding display names`.

   Each event is entered as `<Event Code>`,`<Display Text>`, where the event code is a hexadecimal code in the range `0x43015000` to `0x43015FFF`, inclusive. For example, `0x43015001,Access to confidential data`.
4. Click **Update**.
5. Using AccessStudio, create an AccessProfile that tracks the event and submits an audit log with that event code.

   For more information about creating AccessProfiles, see the *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide*.

Generating reports in Tivoli Common Reporting tool 1.2

You can generate Application Usage, Help desk Activity, Token Information, and User Information reports with the Tivoli Common Reporting tool 1.2.

Before you begin

Make sure that the reporting tool is installed. If not, run the IBM Security Access Manager for Enterprise Single Sign-On 8.2 reporting tools by using the command-line utility:

```
install <TCR Absolute Path> <TCR Server Name> <TCR username>
<TCR password> --user <Database username> --pwd <Database
password> --vendor <Database vendor (either db2, sqlserver
or oracle)> --dbname <database or schema name in database
server> --ip <IP address for database server> --port
<Port number of database server> --verbose
```

Where:

<TCR Absolute Path><TCR Server Name> is the fully qualified path name to server on which the Tivoli Integrated Portal and the Common Reporting tool is installed. Typically this is `C:\IBM\tivoli\tip server1`.

<TCR username> is the username of the Tivoli Integrated Portal user who has permission to run reports.

<TCR password> is the password associated with *<TCR username>*.

--user <Database username> is the name of the database administrator.

--pwd <Database password> is the password associated with *<Database username>*.

--vendor <Database vendor> is the name of the database company.

--dbname <database or schema name in database server> is the name of the database or schema in the database server.

--ip <IP address for database server> is the IP address of your database server.

--port <Port number of database server> is the port number of your database server.

--verbose indicates that you want to see the results of issuing this command.

Example:

```
C:\......>install C:\IBM\tivoli\tip server1
tipAdmin p@ssw0rd --user dbUser --pwd p@ssw0rd --vendor db2
--dbname MSTSCRP --ip 127.0.0.1 --port 50000 --verbose
```

Note: Change the Tivoli Common Reporting Java Database Connectivity (JDBC) Driver absolute path in the `Install.bat` file if it is different from the following example:

```
set driverPath=\products\tcr\lib\birt-runtime-2_2_2
\ReportEngine\plugins\org.eclipse.birt.report.data.oda.
jdbc_2.2.2.r22x_v20071206\drivers
```

Do not change the default path.

See http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ic-home.html for more information about Tivoli Common Reporting, and its installation procedure.

About this task

The Tivoli Common Reporting tool:

- Generates reports in HTML, PDF, Microsoft Excel, or Adobe PostScript format.
- Does not support Arabic and Hebrew language.

Procedure

1. On your Windows desktop, select **Start** > **Programs** > **Tivoli Common Reporting** > **Start Tivoli Common Reporting Server**.
2. Enter your user name and password in the **Tivoli Integrated Portal** > **Reporting** > **Common Reporting**.
3. In the navigation pane, select **Report Sets** > **IBM Security Products** > **IBM Security Access Manager for Enterprise Single Sign On**.
4. Right-click on any of the following reports you want to generate.
   - **Application Usage Report**
   - **Help desk Activity Report**
   - **Token Information Report**
   - **User Information Report**

   See Appendix F, “Audit reports,” on page 57 for more details.
5. Select an output format from the **View as** pop-up menu.
6. Click **Run**.

Generating reports in Tivoli Common Reporting tool 2.1

You can generate Application Usage, Help desk Activity, Token Information, and User Information reports with the Tivoli Common Reporting tool.

Before you begin

Make sure that the reporting tool is installed. If not, run the IBM Security Access Manager for Enterprise Single Sign-On 8.2 reporting tools using the command-line utility:

```
install <TCR Absolute Path> <TCR Server Name> <TCR username>
<TCR password> --user <Database username> --pwd <Database
password> --vendor <Database vendor (either db2, sqlserver
or oracle)> --dbname <database or schema name in database
server> --ip <IP address for database server> --port
<Port number of database server> --verbose
```

Where:

<TCR Absolute Path><TCR Server Name> is the fully qualified path name to server on which the Tivoli Integrated Portal and the Common Reporting tool is installed. Typically this is `C:\IBM\tivoli\tip` server1.

<TCR username> is the username of the Tivoli Integrated Portal user who has permission to run reports.

<TCR password> is the password associated with *<TCR username>*.

--user <Database username> is the name of the database administrator.

--pwd <Database password> is the password associated with *<Database username>*.

--vendor <Database vendor> is the name of the database company.

--dbname <database or schema name in database server> is the name of the database or schema in the database server.

--ip <IP address for database server> is the IP address of your database server.

--port <Port number of database server> is the port number of your database server.

--verbose indicates that you want to see the results of issuing this command.

Example:

```
C:\......>install C:\IBM\tivoli\tip server1
tipAdmin p@ssw0rd --user dbUser --pwd p@ssw0rd --vendor db2
--dbname MSTSCRP --ip 127.0.0.1 --port 50000 --verbose
```

Note: Change the Tivoli Common Reporting Java Database Connectivity (JDBC) Driver absolute path in the `Install.bat` file if it is different from the following example:

```
set driverPath=\products\tcr\lib\birt-runtime-2_2_2
\ReportEngine\plugins\org.eclipse.birt.report.data.oda.
jdbc_2.2.2.r22x_v20071206\drivers
```

Do not change the default path.

Procedure

1. Navigate to `https://localhost:16311/ibm/console/`. For optimum results, use Internet Explorer.
2. Log on using your user ID and password.
3. Select **Reporting** > **Common reporting** > **IBM Security Products** > **SAM Enterprise Single Sign On v8.2**.
4. Click any of the following reports you want to generate.
   - **Application Usage Report**
   - **Help desk Activity Report**
   - **Token Information Report**
   - **User Information Report**
5. Enter the information in the **Work with reports** page.
6. Click **Finish**. To view the report in another format, click the **View in <format> Format** icon in the upper right corner of the page.

Appendix A. Accessing the IMS Configuration Utility

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

Procedure

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

Appendix B. Updating policies in an upgraded IMS Server

If you are upgrading to IMS Server version 8.2, make sure that the updated policies are shown in AccessAdmin. For more information about the policies, see the *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide*.

Procedure

1. See Appendix C, "Changed policies from 8.1 to 8.2," on page 35 or Appendix D, "Changed policies from 8.0.1 to 8.2," on page 43 and identify the policy to be updated.
2. Navigate to `<IMS_INSTALL_8.2 FOLDER>/com.ibm.tamesso.ims-delhi.build.boot\src\config\data\config`.
3. Open `policy_sync_data.xml`.
4. Copy the policy definition to be updated.
5. Paste and save it as a new file.
6. Upload the policy file.
   a. Log on to the IMS Configuration Utility.
   b. Navigate to **Utilities** > **Upload System Data**.
   c. Select **Data file**.
   d. Locate the new policy file.
   e. Click **Upload**.
7. Restart the IMS Server.

Example

1. You want the new display name and description of the policy `pid_enc_hot_key_policy_priority` to be displayed in AccessAdmin.
2. Copy the entire text in the policy definition tags of the policy `pid_enc_hot_key_policy_priority`.

```
 <policy_definition>

....
<id>pid_enc_hot_key_policy_priority</id>

....
<display_name>Policy priority for ISAM ESSO Hot Key</display_name>

<descrption>Whether the system or machine policy should be
enforced for TAM E-SSO Hot Key.</descrption>

....

.....
</policy_definition>
```

3. Paste the text into a new file and save it.
4. Upload the file in the IMS Configuration Utility.
5. Restart the IMS Server.

Appendix C. Changed policies from 8.1 to 8.2

This section provides a list of the policy changes displayed in AccessAdmin 8.1 and AccessAdmin 8.2.

The following policies have been updated. Compare the display name and description.

pid_unlock_user_name_prefill_option

8.1	8.2
Description Option for prefilling TAM E-SSO unlock prompt with a user name	*Description* Option for prefilling ISAM ESSO unlock prompt with a user name

pid_wallet_inject_pwd_entry_option_default

8.1	8.2
Display name Default automatic sign-on password entry option *Description* Default single sign-on using the automatic sign-on mode password entry option	*Display name* Default single sign-on using the automatic sign-on mode password entry option *Description* Default single sign-on using the automatic sign-on mode password entry option

pid_auth_inject_pwd_entry_option_default

8.1	8.2
Display name Default automatic sign-on password entry option for the authentication service *Description* Default automatic sign-on password entry option for the authentication service. This policy overrides the system-wide default automatic sign-on password entry option	*Display name* Default single sign-on using the automatic sign-on mode password entry option for the authentication service *Description* Default single sign-on using the automatic sign-on mode password entry option for the authentication service. This policy overrides the system-wide default single sign-on using the automatic sign-on mode password entry option

pid_app_inject_pwd_entry_option_default

8.1	8.2
Display name Default automatic sign-on password entry option for the application *Description* Default automatic sign-on password entry option for the application. This policy overrides the system- wide and the authentication service default automatic sign-on password entry options	*Display name* Default single sign-on using the automatic sign-on mode password entry option for the application *Description* Default single sign-on using the automatic sign-on mode password entry option for the application. This policy overrides the system-wide and the authentication service default single sign-on using the automatic sign-on mode password entry options

pid_auth_reauth_with_enc_pwd_enabled

8.1	8.2
Display name Require re-authentication before performing automatic sign-on? *Description* Whether password reauthentication is required before performing automatic sign-on for the authentication service	*Display name* Require re-authentication before performing single sign-on using the automatic sign-on mode? *Description* Whether password reauthentication is required before performing single sign-on using the automatic sign-on mode for the authentication service

pid_auth_sso_enabled

8.1	8.2
Display name Enable automatic sign-on? *Description* Whether to enable automatic sign-on for the authentication service	*Display name* Enable single sign-on using the automatic sign-on mode? *Description* Whether to enable single sign-on using the automatic sign-on mode for the authentication service

pid_wallet_personal_app_sso_enabled

8.1	8.2
Display name Enable automatic sign-on for personal authentication services? *Description* Whether to enable automatic sign-on for personal authentication services	*Display name* Enable single sign-on using the automatic sign-on mode for personal authentication services? *Description* Whether to enable auto-learning for single sign-on using the automatic sign-on mode to applications

pid_engina_welcome_text

8.1	8.2
Display name Configurable text for EnGINA welcome message.	*Display name* Configurable text for ESSO GINA welcome message.

pid_enc_hot_key_policy_priority

8.1	8.2
Display name Policy priority for TAM E-SSO Hot Key *Description* Whether to enforce the system or machine policy for TAM E-SSO Hot Key.	*Display name* Policy priority for ISAM ESSO Hot Key *Description* Whether to enforce the system or machine policy for ISAM ESSO Hot Key.

pid_enc_hot_key_enabled

8.1	8.2
Display name Enable TAM E-SSO Hot Key? *Description* Whether TAM E-SSO Hot Key is enabled	*Display name* Enable ISAM ESSO Hot Key? *Description* Whether ISAM ESSO Hot Key is enabled

pid_enc_hot_key_action

8.1	8.2
Display name TAM E-SSO Hot Key press actions at desktop when AccessAgent is logged on *Description* Actions to be performed by AccessAgent if TAM E-SSO Hot Key is pressed at desktop while AccessAgent is logged on.	*Display name* ISAM ESSO Hot Key press actions at desktop when AccessAgent is logged on *Description* Actions to be performed by AccessAgent if ISAM ESSO Hot Key is pressed at desktop while AccessAgent is logged on.

pid_enc_hot_key_action_countdown_secs

8.1	8.2
Display name Confirmation countdown duration, in seconds, for pressing TAM E-SSO Hot Key *Description* Confirmation countdown duration, in seconds, for pressing TAM E-SSO Hot Key. 0 to disable confirmation countdown.	*Display name* Confirmation countdown duration, in seconds, for pressing ISAM ESSO Hot Key *Description* Confirmation countdown duration in seconds, for pressing ISAM ESSO Hot Key. 0 to disable confirmation countdown.

pid_engina_policy_priority

8.1	8.2
Display name Policy priority for EnGINA *Description* Whether to enforce the system or machine policy for EnGINA.	*Display name* Policy priority for ESSO GINA *Description* Whether to enforce the system or machine policy for ESSO GINA.

pid_engina_logon_prompt_timeout_secs

8.1	8.2
Description Logon prompt time-out, in seconds, for EnGINA logon, desktop logon, and unlock computer. After time-out, welcome text or locked computer text is displayed.	*Description* Logon prompt time-out in seconds, for ESSO GINA logon, desktop logon, and unlock computer. After time-out, the welcome text or locked computer text is displayed.

pid_app_reauth_with_enc_pwd_enabled

8.1	8.2
Display name Require re-authentication before performing automatic sign-on? *Description* Whether password reauthentication is required before performing automatic sign-on for the application.	*Display name* Require re-authentication before performing single sign-on using the automatic sign-on mode ? *Description* Whether password reauthentication is required before performing single sign-on using the automatic sign-on mode for the application.

pid_wallet_inject_pwd_entry_option_list

8.1	8.2

pid_wallet_inject_pwd_entry_option_list

Description List of available password entry options for automatic sign-on	*Description* List of available password entry options for single sign-on using the automatic sign-on mode

pid_accessanywhere_app_sso_enabled

8.1	8.2
Display name Enable automatic sign-on to applications in AccessAssistant? *Description* Whether the user can perform automatic sign-on to applications through AccessAssistant.	*Display name* Enable single sign-on using the automatic sign-on mode to applications in AccessAssistant? *Description* Whether the user can perform single sign-on using the automatic sign-on mode to applications through AccessAssistant.

pid_engina_bypass_hot_key_policy_priority

8.1	8.2
Display name Policy priority for EnGINA Bypass Hot Key *Description* Whether to enforce the system or machine policy for EnGINA Bypass Hot Key.	*Display name* Policy priority for ESSO GINA Bypass Hot Key *Description* Whether to enforce the system or machine policy for ESSO GINA Bypass Hot Key.

pid_engina_bypass_hot_key_enabled

8.1	8.2
Display name Enable EnGINA Bypass Hot Key? *Description* Whether EnGINA Bypass Hot Key is enabled.	*Display name* Enable ESSO GINA Bypass Hot Key? *Description* Whether ESSO GINA Bypass Hot Key is enabled.

pid_engina_bypass_hot_key_sequence

8.1	8.2
Display name EnGINA Bypass Hot Key sequence *Description* The EnGINA Bypass Hot Key sequence. Maximum of 3 keys from the set: {Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E}.	*Display name* ESSO GINA Bypass Hot Key sequence *Description* The ESSO GINA Bypass Hot Key sequence. Maximum of 3 keys from the set: {Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E}.

pid_engina_bypass_automatic_text

8.1	8.2
Display name Message for automatic EnGINA bypass *Description* Configurable text message for automatic EnGINA bypass.	*Display name* Message for automatic ESSO GINA bypass *Description* Configurable text message for automatic ESSO GINA bypass.

pid_enc_hot_key_not_logged_on_action

8.1	8.2

pid_enc_hot_key_not_logged_on_action

Display name TAM E-SSO Hot Key press actions at desktop when AccessAgent is not logged on *Description* Actions to be performed by AccessAgent if TAM E-SSO Hot Key is pressed at desktop while AccessAgent is not logged on.	*Display name* ISAM ESSO Hot Key press actions at desktop when AccessAgent is not logged on *Description* Actions to be performed by AccessAgent if ISAM ESSO Hot Key is pressed at desktop while AccessAgent is not logged on.

pid_sso_policy_priority

8.1	8.2
Display name Policy priority for automatic sign-on *Description* Whether to enforce the user or machine policy for automatic sign-on.	*Display name* Policy priority for single sign-on using the automatic sign-on mode *Description* Whether to enforce the user or machine policy for single sign-on using the automatic sign-on mode.

pid_sso_user_control_enabled

8.1	8.2
Display name Allow user to enable/disable automatic sign-on? *Description* Whether to enable/disable automatic sign-on.	*Display name* Allow user to enable/disable single sign-on using the automatic sign-on mode? *Description* Whether to enable/disable single sign-on using the automatic sign-on mode.

pid_lusm_sessions_max

8.1	8.2
Display name Maximum number of concurrent user sessions on a workstation	*Display name* Maximum number of concurrent user sessions on a workstation (only for Windows XP)

pid_lusm_session_replacement_option

8.1	8.2
Display name Session replacement option	*Display name* Session replacement option (only for Windows XP)

pid_lusm_sia_list

8.1	8.2
Display name Single instance applications list	*Display name* Single instance applications list (only for Windows XP)

pid_lusm_sia_launch_option

8.1	8.2
Display name Action on launching a second instance of a single instance application	*Display name* Action on launching a second instance of a single instance application (only for Windows XP)

pid_lusm_generic_accounts_enabled

8.1	8.2
Display name Enable use of generic accounts to create user desktops?	*Display name* Enable use of generic accounts to create user desktops? (only for Windows XP)

pid_engina_winlogon_option_enabled

8.1	8.2
Display name Whether to enable the option to go to Windows Logon directly from EnGINA	*Display name* Whether to enable the option to go to Windows Logon directly from ESSO GINA.

pid_engina_app_launch_enabled

8.1	8.2
Display name Enable application launch from EnGINA? *Description* Whether to enable the launching of an application from EnGINA welcome or locked screen.	*Display name* Enable application launch from ESSO GINA? *Description* Whether to enable the launching of an application from ESSO GINA welcome or locked screen.

pid_engina_app_launch_label

8.1	8.2
Description Display label for the link on EnGINA welcome or locked screen, for launching an application.	*Description* Display label for the link on ESSO GINA welcome or the locked screen, for launching an application

pid_engina_app_launch_cmd

8.1	8.2
Description Command line for launching an application from EnGINA welcome or locked screen.	*Description* Command line for launching an application from ESSO GINA welcome or locked screen.

pid_engina_bypass_automatic_enabled

8.1	8.2
Display name Enable automatic EnGINA bypass? *Description* Whether automatic EnGINA Bypass is enabled.	*Display name* Enable automatic ESSO GINA bypass? *Description* Whether automatic ESSO GINA bypass is enabled.

pid_lock_transparent_text

8.1	8.2
Display name Transparent screen lock message	*Display name* Transparent screen lock message (only for Windows XP)

pid_lock_transparent_hot_key_enabled

8.1	8.2

pid_lock_transparent_hot_key_enabled

Display name Enable transparent screen lock hot key?	*Display name* Enable transparent screen lock hot key? (only for Windows XP)

pid_ts_engina_logon_no_local_session_enabled

8.1	**8.2**
Display name Use EnGINA logon when there is no local AccessAgent session? *Description* Whether to use EnGINA logon or Microsoft GINA logon for the Terminal Server session, when there is no local AccessAgent session.	*Display name* Use ESSO GINA when there is no local AccessAgent session? *Description* Whether to use ESSO GINA logon or Microsoft GINA logon for the Terminal Server session, when there is no local AccessAgent session.

pid_engina_ui_enabled

8.1	**8.2**
Display name Enable TAM E-SSO UI when Windows is logged off or locked? *Description* Whether to display the TAM E-SSO UI instead of the Windows UI when Windows is logged off or locked.	*Display name* Enable ISAM ESSO UI when Windows is logged off or locked *Description* Whether to display the ISAM ESSO UI instead of the Windows UI when Windows is logged off or locked.

Appendix D. Changed policies from 8.0.1 to 8.2

This section provides a list of the policy changes displayed in AccessAdmin 8.0.1 and AccessAdmin 8.2.

The following policies have been updated. Compare the display name and description.

pid_wallet_inject_pwd_entry_option_default

8.1	8.2
Display name Default automatic sign-on password entry option *Description* Default single sign-on using the automatic sign-on mode password entry option	*Display name* Default single sign-on using the automatic sign-on mode password entry option *Description* Default single sign-on using the automatic sign-on mode password entry option

pid_auth_inject_pwd_entry_option_default

8.1	8.2
Display name Default automatic sign-on password entry option for the authentication service *Description* Default automatic sign-on password entry option for the authentication service. This policy overrides the system-wide default automatic sign-on password entry option	*Display name* Default single sign-on using the automatic sign-on mode password entry option for the authentication service *Description* Default single sign-on using the automatic sign-on mode password entry option for the authentication service. This policy overrides the system-wide default single sign-on using the automatic sign-on mode password entry option

pid_app_inject_pwd_entry_option_default

8.1	8.2
Display name Default automatic sign-on password entry option for the application *Description* Default automatic sign-on password entry option for the application. This policy overrides the system- wide and the authentication service default automatic sign-on password entry options	*Display name* Default single sign-on using the automatic sign-on mode password entry option for the application *Description* Default single sign-on using the automatic sign-on mode password entry option for the application. This policy overrides the system-wide and the authentication service default single sign-on using the automatic sign-on mode password entry options

pid_auth_reauth_with_enc_pwd_enabled

8.1	8.2

pid_auth_reauth_with_enc_pwd_enabled

Display name Require re-authentication before performing automatic sign-on? *Description* Whether password re-authentication is required before performing automatic sign-on for the authentication service	*Display name* Require re-authentication before performing single sign-on using the automatic sign-on mode? *Description* Whether password re-authentication is required before performing single sign-on using the automatic sign-on mode for the authentication service

`pid_usb_key_removal_policy_priority` to `pid_desktop_inactivity_policy_priority`

8.1	**8.2**
Display name Policy priority for USB Key removal *Description* Whether to enforce the user or machine policy for USB Key removal.	*Display name* Policy priority for desktop inactivity *Description* Whether to enforce the system or machine policy for desktop inactivity.

`pid_usb_key_removal_action` to `pid_desktop_inactivity_action`

8.1	**8.2**
Display name USB Key removal actions *Description* Actions to be performed when USB Key is removed.	*Display name* Desktop inactivity actions *Description* Actions to be performed by AccessAgent after a period of desktop inactivity.

pid_wallet_personal_app_sso_enabled

8.1	**8.2**
Display name Enable automatic sign-on for personal authentication services? *Description* Whether to enable automatic sign-on for personal authentication services	*Display name* Enable single sign-on using the automatic sign-on mode for personal authentication services? *Description* Whether to enable auto-learning for single sign-on using the automatic sign-on mode to applications

pid_sso_auto_learn_enabled

8.1	**8.2**
Display name Enable auto-learning? *Description* Whether to enable auto-learning for automatic sign-on to applications.	*Display name* Enable auto-learning? *Description* Whether to enable auto-learning for single sign-on using the automatic sign-on mode to applications.

pid_engina_welcome_text

8.1	**8.2**
Display name Configurable text for EnGINA welcome message.	*Display name* Configurable text for ESSO GINA welcome message.

pid_enc_hot_key_policy_priority

8.1	**8.2**

pid_enc_hot_key_policy_priority

Display name Policy priority for TAM E-SSO Hot Key *Description* Whether to enforce the system or machine policy for TAM E-SSO Hot Key.	*Display name* Policy priority for ISAM ESSO Hot Key *Description* Whether to enforce the system or machine policy for ISAM ESSO Hot Key.

pid_enc_hot_key_enabled

8.1	**8.2**
Display name Enable TAM E-SSO Hot Key? *Description* Whether TAM E-SSO Hot Key is enabled	*Display name* Enable ISAM ESSO Hot Key? *Description* Whether ISAM ESSO Hot Key is enabled

pid_enc_hot_key_sequence

8.1	**8.2**
Display name TAM E-SSO Hot Key sequence *Description* The TAM E-SSO Hot Key sequence. Maximum of 3 keys from the set: {Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E}	*Display name* ISAM ESSO Hot Key sequence *Description* The ISAM ESSO Hot Key sequence. Maximum of 3 keys from the set: {Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E}.

pid_enc_hot_key_action

8.1	**8.2**
Display name TAM E-SSO Hot Key press actions at desktop when AccessAgent is logged on *Description* Actions to be performed by AccessAgent if TAM E-SSO Hot Key is pressed at desktop while AccessAgent is logged on.	*Display name* ISAM ESSO Hot Key press actions at desktop when AccessAgent is logged on *Description* Actions to be performed by AccessAgent if ISAM ESSO Hot Key is pressed at desktop while AccessAgent is logged on.

pid_enc_hot_key_action_countdown_secs

8.1	**8.2**
Display name Confirmation countdown duration, in seconds, for pressing TAM E-SSO Hot Key *Description* Confirmation countdown duration, in seconds, for pressing TAM E-SSO Hot Key. 0 to disable confirmation countdown.	*Display name* Confirmation countdown duration, in seconds, for pressing ISAM ESSO Hot Key *Description* Confirmation countdown duration in seconds, for pressing ISAM ESSO Hot Key. 0 to disable confirmation countdown.

pid_engina_policy_priority

8.1	**8.2**
Display name Policy priority for EnGINA *Description* Whether to enforce the system or machine policy for EnGINA.	*Display name* Policy priority for ESSO GINA *Description* Whether to enforce the system or machine policy for ESSO GINA.

pid_engina_logon_prompt_timeout_secs

8.1	8.2
Description Logon prompt time-out, in seconds, for EnGINA logon, desktop logon, and unlock computer. After time-out, welcome text or locked computer text is displayed.	*Description* Logon prompt time-out in seconds, for ESSO GINA logon, desktop logon, and unlock computer. After time-out, welcome text or locked computer text is displayed.

pid_app_reauth_with_enc_pwd_enabled

8.1	8.2
Display name Require re-authentication before performing automatic sign-on? *Description* Whether password re-authentication is required before performing automatic sign-on for the application.	*Display name* Require re-authentication before performing single sign-on using the automatic sign-on mode ? *Description* Whether password re-authentication is required before performing single sign-on using the automatic sign-on mode for the application.

pid_accessanywhere_app_sso_enabled

8.1	8.2
Display name Enable automatic sign-on to applications in AccessAssistant? *Description* Whether the user can perform automatic sign-on to applications through AccessAssistant.	*Display name* Enable single sign-on using the automatic sign-on mode to applications in AccessAssistant? *Description* Whether the user can perform single sign-on using the automatic sign-on mode to applications through AccessAssistant.

pid_engina_bypass_hot_key_policy_priority

8.1	8.2
Display name Policy priority for EnGINA Bypass Hot Key *Description* Whether to enforce the system or machine policy for EnGINA Bypass Hot Key.	*Display name* Policy priority for ESSO GINA Bypass Hot Key *Description* Whether to enforce the system or machine policy for ESSO GINA Bypass Hot Key.

pid_engina_bypass_hot_key_enabled

8.1	8.2
Display name Enable EnGINA Bypass Hot Key? *Description* Whether EnGINA Bypass Hot Key is enabled.	*Display name* Enable ESSO GINA Bypass Hot Key? *Description* Whether ESSO GINA Bypass Hot Key is enabled.

pid_engina_bypass_hot_key_sequence

8.1	8.2

pid_engina_bypass_hot_key_sequence

Display name EnGINA Bypass Hot Key sequence *Description* The EnGINA Bypass Hot Key sequence. Maximum of 3 keys from the set: {Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E}.	*Display name* ESSO GINA Bypass Hot Key sequence *Description* The ESSO GINA Bypass Hot Key sequence. Maximum of 3 keys from the set: {Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E}.

pid_engina_bypass_automatic_text

8.1	8.2
Display name Message for automatic EnGINA bypass *Description* Configurable text message for automatic EnGINA bypass.	*Display name* Message for automatic ESSO GINA bypass *Description* Configurable text message for automatic ESSO GINA bypass.

pid_enc_hot_key_not_logged_on_action

8.1	8.2
Display name TAM E-SSO Hot Key press actions at desktop when AccessAgent is not logged on *Description* Actions to be performed by AccessAgent if TAM E-SSO Hot Key is pressed at desktop while AccessAgent is not logged on.	*Display name* ISAM ESSO Hot Key press actions at desktop when AccessAgent is not logged on *Description* Actions to be performed by AccessAgent if ISAM ESSO Hot Key is pressed at desktop while AccessAgent is not logged on.

pid_sso_policy_priority

8.1	8.2
Display name Policy priority for automatic sign-on *Description* Whether to enforce the user or machine policy for automatic sign-on.	*Display name* Policy priority for single sign-on using the automatic sign-on mode *Description* Whether to enforce the user or machine policy for single sign-on using the automatic sign-on mode.

pid_sso_user_control_enabled

8.1	8.2
Display name Allow user to enable/disable automatic sign-on? *Description* Whether to enable/disable automatic sign-on.	*Display name* Allow user to enable/disable single sign-on using the automatic sign-on mode ? *Description* Whether to enable/disable single sign-on using the automatic sign-on mode.

pid_lusm_sessions_max

8.1	8.2
Display name Maximum number of concurrent user sessions on a workstation	*Display name* Maximum number of concurrent user sessions on a workstation (only for Windows XP)

pid_lusm_session_replacement_option

8.1	8.2
Display name Session replacement option	*Display name* Session replacement option (only for Windows XP)

pid_lusm_sia_list

8.1	8.2
Display name Single instance applications list	*Display name* Single instance applications list (only for Windows XP)

pid_lusm_sia_launch_option

8.1	8.2
Display name Action on launching a second instance of a single instance application	*Display name* Action on launching a second instance of a single instance application (only for Windows XP)

pid_lusm_generic_accounts_enabled

8.1	8.2
Display name Enable use of generic accounts to create user desktops?	*Display name* Enable use of generic accounts to create user desktops? (only for Windows XP)

pid_engina_winlogon_option_enabled

8.1	8.2
Display name Whether to enable the option to go to Windows Logon directly from EnGINA	*Display name* Whether to enable the option to go to Windows Logon directly from ESSO GINA.

pid_engina_app_launch_enabled

8.1	8.2
Display name Enable application launch from EnGINA? *Description* Whether to enable the launching of an application from EnGINA welcome or locked screen.	*Display name* Enable application launch from ESSO GINA? *Description* Whether to enable the launching of an application from ESSO GINA welcome or locked screen.

pid_engina_app_launch_label

8.1	8.2
Description Display label for the link on EnGINA welcome or locked screen, for launching an application.	*Description* Display label for the link on ESSO GINA welcome or locked screen, for launching an application

pid_engina_app_launch_cmd

8.1	8.2
Description Command line for launching an application from EnGINA welcome or locked screen.	*Description* Command line for launching an application from ESSO GINA welcome or locked screen.

pid_engina_bypass_automatic_enabled

8.1	8.2
Display name Enable automatic EnGINA bypass? *Description* Whether automatic EnGINA Bypass is enabled.	*Display name* Enable automatic ESSO GINA bypass? *Description* Whether automatic ESSO GINA bypass is enabled.

pid_lock_transparent_text

8.1	8.2
Display name Transparent screen lock message	*Display name* Transparent screen lock message (only for Windows XP)

pid_lock_transparent_hot_key_enabled

8.1	8.2
Display name Enable transparent screen lock hot key?	*Display name* Enable transparent screen lock hot key? (only for Windows XP)

pid_ts_engina_logon_no_local_session_enabled

8.1	8.2
Display name Use EnGINA logon when there is no local AccessAgent session? *Description* Whether to use EnGINA logon or Microsoft GINA logon for the Terminal Server session, when there is no local AccessAgent session.	*Display name* Use ESSO GINA when there is no local AccessAgent session? *Description* Whether to use ESSO GINA logon or Microsoft GINA logon for the Terminal Server session, when there is no local AccessAgent session.

Appendix E. Audit log events

IBM Security Access Manager for Enterprise Single Sign-On generates event logs at all end-points.

Administrators and Help desk officers can access the audit logs for individual users. Only Administrators can run full queries on audit logs, access the Help desk logs, and generate reports on Help desk and user activity. Users do not have read/write access to these logs.

Types of logs

There are three types of logs:

1. *User logs* - logs of user activities.
2. *Administrator logs* - logs of the Administrator and Help desk activities.
3. *System logs* - The system logs are message and error logs for the IMS Server itself. System logs are primarily used for troubleshooting server issues and monitoring system health.

IBM Security Access Manager for Enterprise Single Sign-On tracks the following information:

- What applications users access
- Who accessed these applications
- Details about the accounts used
- When users accessed these applications, and from where they are accessed

Web Workplace also generates audit logs for the *auto-fill* event for each application logon attempt. However, Web Workplace cannot generate audit logs indicating whether the logon is successful.

Storage and sync

If AccessAgent is connected to the IMS Server, AccessAgent audit logs are immediately submitted to the IMS Server. The IMS Server stores the audit logs on a relational database. If there is no network connection to the IMS Server, AccessAgent temporarily caches the event logs on the local computer. The logs are submitted to IMS Server when network connection to the IMS Server is restored.

User event

The following are the user-related events that are logged.

Audit Log Event	Description
Add account credential to the Wallet	When a user adds account credentials into the Wallet manually and not captured by the AccessAgent.
Auto-capture authentication service password	When the AccessAgent captures account credentials for the user and stores it into the Wallet.

Audit Log Event	Description
Auto-fill authentication service password	When the AccessAgent injects (auto-fills) account credentials into an application logon screen for the user after reading them from the Wallet. This event is logged for enterprise authentication services only. AccessAgent logs the event irrespective of whether the logon is successful.
Fortify authentication service password	When the AccessAgent generates random passwords on a change password screen and auto-fills it into the new password fields and clicks submit.
Log on authentication service	When a user logs on to an authentication service. This event is not automatically generated by AccessAgent. It must be explicitly modeled in the respective AccessProfiles. This event differs from the Autofill. This event is a validated logon, and is logged only when a user successfully logs on to the application.
Log off authentication service	When a user logs from an authentication service. This event is not automatically generated by AccessAgent. It needs to be explicitly modeled in the respective AccessProfiles.
Log on to AccessAgent	When a user logs on to AccessAgent.
Sign up user	When a user signs up with the IMS Server.
Register authentication factor	When a user registers an authentication factor like RFID badge, fingerprint, and others.
Store cached Wallet on hard disk or ISAM ESSO USB Key	When a user Wallet is cached.
Unlock computer	When the computer is unlocked.
Reset ISAM ESSO password offline	When the ISAM ESSO password is reset offline using the backup software key (BSK) mechanism.
Reset ISAM ESSO password online	When the ISAM ESSO password is reset online with the Help desk generated authorization code or self-service secrets.
Authorization Code issuance through self-service	When a user requests authorization code for password reset or for second factor registration over email or SMS channel.
Mobile ActiveCode request with ISAM ESSO password	When a user requests for a Mobile ActiveCode for an application that uses the ISAM ESSO password to perform its first step in the authentication process.
Mobile ActiveCode request with application password	When a user requests for a Mobile ActiveCode for an application that has its own password as its first step in the authentication process.

Audit Log Event	Description
ActiveCode verification	When the user submits the Mobile ActiveCode for verification. This event can be translated as the final step in the two-step authentication process involving ActiveCode enabled applications.
RADIUS authentication	When the RADIUS client (VPN server) initiates a RADIUS authentication request to the IMS Server. This event usually occurs when the user enters the application password and the VPN server delegates this authentication to the IMS Server RADIUS component. This event is the first step in the two-step authentication process with Mobile ActiveCode.
RADIUS challenge response	When the RADIUS client (VPN server) initiates a RADIUS challenge-response to the IMS Server. This event usually occurs when the user enters the mobile ActiveCode delivered to the user through the SMS or email channel. The VPN server delegates this authentication to the IMS Server RADIUS component. This event is the second step in the two-step authentication process with Mobile ActiveCode.

Administrator / Help desk event

The following are the Administrator and Help desk events that are logged.

Audit Log Event	Description
Authorization code issuance for online verification	When a Help desk or administrator generates an authorization code for the user when the user has connectivity to the IMS.
Authorization code issuance for offline verification	When the Help desk or administrator generates an authorization code for the user to reset the password when the user does not have connectivity to the IMS Server. (Backup Software Key BSK workflow)
Provision ISAM ESSO user account	When administrator provisions an ISAM ESSO user account.
Update System Policy	When an administrator updates the system policy.
Update User Policy	When an administrator or Help desk updates a user policy.
Authentication factor revocation	When a user authentication factor is revoked by the Administrator or Help desk.
Revoke user	When a user is revoked by an administrator or Help desk.
Mobile ActiveCode user sign-up	When a mobile ActiveCode user is signed up through AccessAdmin.

Audit Log Event	Description
ActiveCode-enabled authentication service account activation	When a Mobile ActiveCode account is activated by an Administrator or Help desk through the Users Authentication Services page on AccessAdmin.
ActiveCode-enabled authentication service account addition	When a Mobile ActiveCode account is added to the user through CLT or through the Users Authentication Services page on the AccessAdmin by the Administrator or Help desk.
ActiveCode-enabled authentication service account locked	When a Mobile ActiveCode account is locked through the Users Authentication Services page on the AccessAdmin by the Administrator or Help desk.
ActiveCode-enabled authentication service account removal	When a Mobile ActiveCode account is deleted through the Users Authentication Services page on the AccessAdmin by the Administrator or Help desk.
OTP ActiveCode initialization	When the OTP ActiveCode is initialized by the AccessAgent for the first time.
OTP Token Reset	When the OTP Token is reset.

System logs

The following are the log files useful for troubleshooting IBM Security Access Manager for Enterprise Single Sign-On installation and configuration issues:

- `C:\Program Files\IBM\SAM E-SSO\IMS Server\ISAM_ESSO_IMS_Server_InstallLog.log`
- `C:\Program Files\IBM\WebSphere\AppServer\profiles\<AppSrv01>\logs`
- `C:\Program Files\IBM\HTTPServer\logs`
- `C:\Program Files\IBM\ISAM ESSO\Logs`

Note: The IMS Server audit logs records the Proxy IP address instead of the end-user machine IP address.

When troubleshooting IMS Server issues, make a copy of the system logs before you start the IMS Server. Starting the IMS Server clears the system logs.

Audit log queries

Use AccessAdmin to search and view the different audit log events. Search results include:

- Date and time of occurrence
- Event that caused the entry
- User name for the authentication service
- Name of the authentication service
- Help desk user name
- SOCI ID
- IP address
- Event result

Event logs

Each event displayed in AccessAdmin is specified in the IMS Server configuration file and can be modified through the IMS Configuration Utility.

You can translate event codes and result codes through the Code Translation utility. See *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

Appendix F. Audit reports

Use Tivoli Common Reporting to create, customize, and manage audit reports.

IMS Server reports are packaged as BIRT reports that can be imported into any Tivoli Common Reporting server. Tivoli Common Reporting connects directly to the database. As such, you can use Tivoli Common Reporting to produce reports on the audit events, even if the IMS Server is not running.

There are four reports bundled with IBM Security Access Manager for Enterprise Single Sign-On:

Note: For Tivoli Common Reporting version 2.1:
- The TCR-BIRT user interface supports bidirectional language but the reports generated do not support bidirectional languages.
- TCR-Cognos also does not support bidirectional languages.

Report Type	Description	Content
Application Usage	An application usage report contains the authentication service activity of one or more users, sorted by event, and time. The report also displays the machine IP address and full name of each user.	• Sequence Number • User Name • Authentication Service • Application User Name • Event • Date Begin • Date End • Result • Time of activity • User machine IP address
Help desk Activity	A Help desk activity report contains the activity of one or more Help desk users sorted by event and time. The report also displays the machine IP address, token type, token ID, and the full name of each Help desk user. Token type and token ID are displayed only if such information is available.	• Sequence Number • Help desk User Name • User Name • Event • Date Begin • Date End • Result • Time of activity • User machine IP address

Report Type	Description	Content
Token Information	A token information report contains the activity of one or more users sorted by token type, event, and time. The report also displays the users machine IP address and the full name of the user.	• Sequence Number • User Name • Event • Token Type • Date Begin • Date End • Result • Time of activity • User machine IP address
User Information	A user information report contains the activity of one or more users sorted by event, result, and time. The report also displays the user machine IP addresses and the full name of the users.	• Sequence Number • User Name • Event • Date Begin • Date End • Result • Time of activity • User machine IP address

Tivoli Common Reporting generates reports in HTML, PDF, Microsoft Excel, or Adobe PostScript format.

Tivoli Common Reporting tool does not support Arabic and Hebrew language.

See http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc/tcr_welcome.htm for more information about Tivoli Common Reporting, including its installation procedure.

Notices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

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

Trademarks

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

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

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

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

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

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

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

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

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

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

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

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

Glossary

AccessAdmin. A web-based management console that Administrators and Helpdesk officers use to administer the IMS Server and to manage users and policies.

AccessAgent plug-in. A piece of script, written in VBscript or Javascript, that is embedded within an AccessProfile to perform custom checking of conditions or to execute custom actions. It is used for extending the capability of an AccessProfile beyond the built-in triggers and actions.

AccessAgent. The client software that manages the identity of the user, authenticates the user, and automates single sign-on and sign-off.

AccessAssistant. The web-based interface that helps users to reset their passwords and retrieve their application credentials.

AccessProfile widget / widget. An independent AccessProfile that consists of pinnable states, which can be used to build another AccessProfile.

AccessProfiles. AccessAgent uses these XML specifications to identify application screens that it can perform single sign-on and automation.

AccessStudio. An application used by Administrators for creating and maintaining AccessProfiles.

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

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

Account data item. The user credentials required for logon.

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

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

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

Active Directory (AD). A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credentials. The Active Directory user name and password.

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

Active RFID (ARFID). ARFID is both a second authentication factor and a presence detector. It can detect the presence of a user and AccessAgent can be configured to perform specific actions. In previous releases, it is called Active Proximity Badge.

ActiveCode. Short-lived authentication codes that are generated and verified by IBM Security Access Manager for Enterprise Single Sign-On. There are two types of ActiveCodes: Mobile ActiveCodes and Predictive ActiveCodes.

Mobile ActiveCodes are generated by IBM Security Access Manager for Enterprise Single Sign-On and dispatched to the mobile phone or email account of the user. Predictive ActiveCodes, or One Time Passwords, are generated from OTP tokens when a user presses its button.

Combined with alternative channels or devices, ActiveCodes provide effective second-factor authentication.

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

Application policies. A collection of policies and attributes governing access to applications.

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

Application. One or more computer programs or software components that provide a function in direct support of a specific business process or processes. In AccessStudio, it is the system that provides the user interface for reading or entering the authentication credentials.

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

Authentication factor. The different devices, biometrics, or secrets required as credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

Authentication service. In IBM Security Access Manager for Enterprise Single Sign-On, a service that verifies the validity of an account against their own user store or against a corporate directory. Identifies the authentication service associated with a screen. Account data saved under a particular authentication service is retrieved and auto-filled for the logon screen that is defined. Account data captured from the logon screen defined is saved under this authentication service.

Authorization code. An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass with AccessAgent, AccessAssistant, and Web Workplace.

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

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

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

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

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

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

Card Serial Number (CSN). A unique data item that identifies a hybrid smart card. It has no relation to the certificates installed in the smart card

Cell. In WebSphere Application Server, a cell is a virtual unit that consists of a deployment manager and one or more nodes.

Certificate authority (CA). A trusted organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate.

IMS Server Certificate. Used in IBM Security Access Manager for Enterprise Single Sign-On. The IMS Server Certificate allows clients to identify and authenticate an IMS Server.

Client AccessAgent. AccessAgent installed and running on the client machine.

Client workstation, client machine, client computers. Computers where AccessAgent installed.

Clinical Context Object Workgroup (CCOW). A vendor independent standard, for the interchange of information between clinical applications in the healthcare industry.

Clustering. In WebSphere Application Server, clustering is the ability to group application servers.

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

Command line interface. A computer interface in which the input command is a string of text characters.

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

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

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

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

Database (DB) server. A software program that uses a database manager to provide database services to software programs or computers.

DB2®. A family of IBM licensed programs for relational database management.

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

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

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

Desktop application. Application that runs in a desktop.

Desktop Manager. Manages concurrent user desktops on a single workstation

Direct auth-info. In profiling, direct auth-info is a direct reference to an existing authentication service.

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

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

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

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

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

Distributed IMS Server. The IMS Servers are deployed in multiple geographical locations.

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

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

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

Enterprise Single Sign-On (ESSO). A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

Enterprise user name. The user name of a user account in the enterprise directory.

ESSO audit logs. A log file that contains a record of system events and responses. ESSO audit logs are stored in the IMS Database.

ESSO Credential Provider. Previously known as the Encentuate Credential Provider (EnCredentialProvider), this is the IBM Security Access Manager for Enterprise Single Sign-On GINA for Windows Vista and Windows 7.

ESSO credentials. The ISAM ESSO user name and password.

ESSO GINA. Previously known as the Encentuate GINA (EnGINA). IBM Security Access Manager for Enterprise Single Sign-On GINA provides a user interface that is integrated with authentication factors and provide password resets and second factor bypass options.

ESSO Network Provider. Previously known as the Encentuate Network Provider (EnNetworkProvider). An AccessAgent module that captures the Active Directory server credentials and uses these credentials to automatically log on the users to their Wallet.

ESSO password. The password that secures access to the user Wallet.

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

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

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

Federal Information Processing Standard (FIPS). A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

Fix pack. A cumulative collection of fixes that is made available between scheduled refresh packs, manufacturing refreshes, or releases. It is intended to allow customers to move to a specific maintenance level.

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

Graphical Identification and Authentication (GINA). A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

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

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

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

Hot key. A key sequence used to shift operations between different applications or between different functions of an application.

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

IBM HTTP server. A web server. IBM offers a web server, called the IBM HTTP Server, that accepts requests from clients and forward to the application server.

IMS Bridge. A module embedded in third-party applications and systems to call to IMS APIs for provisioning and other purposes.

IMS Configuration Utility. A utility of the IMS Server that allows Administrators to manage lower-level configuration settings for the IMS Server.

IMS Configuration wizard. Administrators use the wizard to configure the IMS Server during installation.

IMS Connector. A module that connects IMS to external systems to dispatch a mobile active code to a messaging gateway.

IMS data source. A WebSphere Application Server configuration object that defines the location and parameters for accessing the IMS database.

IMS Database. The relational database where the IMS Server stores all ESSO system, machine, and user data and audit logs.

IMS Root CA. The root certificate authority that signs certificates for securing traffic between AccessAgent and IMS Server.

IMS Server. An integrated management system for ISAM ESSO that provides a central point of secure access administration for an enterprise. It enables centralized management of user identities, AccessProfiles, authentication policies, provides loss management, certificate management, and audit management for the enterprise.

Indirect auth-info. In profiling, indirect auth-info is an indirect reference to an existing authentication service.

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

IP address. A unique address for a device or logical unit on a network that uses the Internet Protocol standard.

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

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

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

Keystore. In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted, or public, keys.

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

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

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

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

Main AccessProfile. The AccessProfile that contains one or more AccessProfile widgets

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

Microsoft Cryptographic application programming interface (CAPI). An interface specification from Microsoft for modules that provide cryptographic functionality and that allow access to smart cards.

Mobile ActiveCode (MAC). A one-time password that is used by users for two-factor authentication in Web Workplace, AccessAssistant, and other applications. This OTP is randomly generated and dispatched to user through SMS or email.

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

Network deployment. Also known as a clustered deployment. A type of deployment where the IMS Server is deployed on a WebSphere Application Server cluster.

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

Nodes. A logical group of managed servers.

One-Time Password (OTP). A one-use password generated for an authentication event, sometimes communicated between the client and the server through a secure channel.

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

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

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

Personal applications. Windows and web-based applications where AccessAgent can store and enter credentials.

Some examples of personal applications are web-based mail sites such as Company Mail, Internet banking sites, online shopping sites, chat, or instant messaging programs.

Personal desktop. The desktop is not shared with any other users.

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

Pinnable state. A state from the AccessProfile widget that is declared as 'Can be pinned in another AccessProfile'.

Pinned state. A pinnable state that is attached to a state in the main AccessProfile.

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

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

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

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

Private desktop. Under this desktop scheme, users have their own Windows desktops in a workstation. When a previous user return to the workstation and unlocks it, AccessAgent switches to the desktop session of the previous user and resumes the last task.

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

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

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

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

Provision. To provide, deploy, and track a service, component, application, or resource.

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

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

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

Radio Frequency Identification (RFID). An automatic identification and data capture technology that identifies unique items and transmits data using radio waves.

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

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

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

Remote Authentication Dial-In User Service (RADIUS). An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

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

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

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

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

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

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

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

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

Secure Sockets Layer virtual private network (SSL VPN). A form of VPN that can be used with a standard web browser.

Security Token Service (STS). A web service used for issuing and exchanging of security tokens.

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

Self-service features. Features in IBM Security Access Manager for Enterprise Single Sign-On which users can use to perform basic tasks such as resetting passwords and secrets with minimal assistance from Help desk or your Administrator.

Serial ID Service Provider Interface (SPI). A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

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

Server AccessAgent. AccessAgent deployed on a Microsoft Windows Terminal Server or a Citrix server.

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

Service Provider Interface (SPI). An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

Session management. Management of user session on private desktops and shared desktops.

Shared desktop. A desktop configuration where multiple users share a generic Windows desktop.

Shared workstation. A workstation shared among users.

Sign up. To request a resource.

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

sign-on information. Information required to provide access to users to any secure application. This information can include user names, passwords, domain information, and certificates.

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

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

Simple Mail Transfer Protocol (SMTP). An Internet application protocol for transferring mail among users of the Internet.

Simple Object Access Protocol (SOAP). A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

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

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

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

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

Stand-alone server. A fully operational server that is managed independently of all other servers, and it uses its own administrative console.

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

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

System modal message. A system dialog box that is typically used to display important messages. When a system modal message is displayed, nothing else can be selected on the screen until the message is closed.

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

Thin client. A client machine that has little or no installed software. It has access to applications and desktop sessions that is running on network servers that are connected to it. A thin client machine is an alternative to a full-function client such as a workstation.

Tivoli Common Reporting tool. A reporting component that you can use to create, customize, and manage reports.

Tivoli Identity Manager adapter. An intermediary software component that allows IBM Security Access Manager for Enterprise Single Sign-On to communicate with Tivoli Identity Manager.

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

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

Trust service chain. A chain of modules operating in different modes. For example: validate, map and issue.

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

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

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

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

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

User deprovisioning. Removing the user account from IBM Security Access Manager for Enterprise Single Sign-On.

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

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

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

Virtual Member Manager (VMM). A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

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

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

Wallet caching. When performing single sign-on for an application, AccessAgent retrieves the logon credentials from the user credential Wallet. The user credential Wallet is downloaded on the user machine and stored securely on the IMS Server. So users can access their Wallet even when they log on to IBM Security Access Manager for Enterprise Single Sign-On from a different machine later.

Wallet manager. The IBM Security Access Manager for Enterprise Single Sign-On GUI component that users can use to manage application credentials in the personal identity Wallet.

Wallet Password. A password that secures access to the Wallet.

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

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

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

Web Workplace. A web-based interface that users can log on to enterprise web applications by clicking links without entering the passwords for individual applications. This interface can be integrated with the existing portal or SSL VPN of the customer.

WebSphere Administrative console. A graphical administrative Java application client that makes method calls to resource beans in the administrative server to access or modify a resource within the domain.

WebSphere Application Server profile. The WebSphere Application Server administrator user name and profile. Defines the runtime environment.

WebSphere Application Server. Software that runs on a web server and that can deploy, integrate, execute, and manage e-business applications.

Windows logon screen, Windows logon UI mode. The screen where users enter their user name and password to log on to the Windows desktop.

Windows native fast user switching. A Windows XP feature which allows users to quickly switch between user accounts.

Windows Terminal Services. A Microsoft Windows component that users use to access applications and data on a remote computer over a network.

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

Index

Printed in USA

SC23-9951-03