IBM® Security Access Manager for Enterprise Single Sign-On

Version 8.2.1

Administrator Guide

SC23-9951-05

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

Administrator Guide

SC23-9951-05

Note
Before using this information and the product it supports, read the information in "Notices" on page 87.

Edition notice

Note: This edition applies to version 8.2.1 of IBM Security Access Manager for Enterprise Single Sign-On, (product number 5724–V67) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this publication

This guide is intended for the Administrators. It covers the different Administrator tasks. *IBM Security Access Manager for Enterprise Single Sign-On Administrator 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.

Accessibility

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

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

Technical training

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

Support information

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

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

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

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

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems,

products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Chapter 1. Overview

Administrators manage users, roles, policies, authentication factors, 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 back up the IMS Server.

What to do	Where to find information
Manage users • Assign and revoke roles.	Chapter 2, "Managing users and roles," on page 3
Manage 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
Manage authentication factors • Modify policies that are related to authentication factors like passwords, RFID, and smart cards.	Chapter 4, "Managing authentication factors," on page 19
Generate reports • Use audit information for enhanced IBM Security Access Manager for Enterprise Single Sign-On administration.	Chapter 6, "Report administration," on page 29
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

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 list.
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. You must assign users to a Help desk role so that Help desk officers can view and manage users that are 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. Choose 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.

Option	Description
Authentication service	This link contains the different types of authentication services that are 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 that are 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 that are 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 task is optional. 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 features
- 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**
   - **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 alphanumeric characters. The name is case-sensitive, so **Example** and **example** are two different template names.
4. In the **Administrative Policies** panel, choose 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 you create 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 that you want to apply under **Apply user policy template**.
8. Click **Apply to selected results**. **Apply to all results** 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 you do not have to apply a User Policy Template manually 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**.
4. Restart the WebSphere Application Server.

Note: Any changes in the user policy template assignment requires a restart of the WebSphere Application Server. Services will be temporarily unavailable until you restart the servers.

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 you create 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 that is filtered as they match all or any of the criteria.
   - Select **Match all of these criteria** to match every search attribute criteria that you have set.
   - Select **Match any of these criteria** to match some and not all the criteria that 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 on your computer.
Host name	Specifies the unique name or identification of your domain.
IP address	Specifies the Internet Protocol address or the unique number that is assigned to your computer in a network. **Note:** IBM Security Access Manager for Enterprise Single Sign-On 8.1 and later 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 you use 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**.

Viewing and setting policy priorities

If a policy is defined for two scopes, define which takes higher priority. For example, if the policy priority is a machine, then only the machine policy is effective.

Policies can be modified only by Help desk officers and Administrators. These policies affect the behavior of the whole system and must be modified only when it is necessary. These policies are set at deployment and followed through. Changes to these policies are propagated to clients the next time AccessAgent synchronizes with the IMS Server.

Important: Older versions of AccessAgent still use the original policy priorities, and values do not change after upgrade of the IMS Server. To change policy priorities, upgrade all installations of AccessAgent to version 8.2.1. For more information, see:

- "Viewing policy priorities"
- "Setting policy priorities"

Viewing policy priorities

If you want to view the current scope and the priority level of a policy, use the command `managePolPriority --policyId [name of policy]`.

Before you begin

Run `setupCmdLine.bat` to configure the path to the WebSphere® Application Server profile where the IMS Server is installed. Set the value to WAS_PROFILE_HOME.

About this task

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

Procedure

1. Launch the Windows command prompt.
2. Navigate to the batch file folder. Type `<IMS installation folder>\bin`, then press **Enter**.
3. Type `managePolPriority.bat` to view the information about running the batch file, then press **Enter**.
4. Type `managePolPriority --policyId [name of policy]`, then press **Enter**. The scope and priority of a specific policy are displayed.
5. Type `exit` to close the command prompt and then press **Enter**.

Setting policy priorities

System, machine, and user policies each have unique and overlapping policy parameters. Certain policies such as AccessAgent lock and unlock, desktop inactivity, and logon and logoff can be defined in more than one policy type. In deployments where many policies are defined, several policies can overlap. In this case, use the `managePolPriority` command-line utility to manage policy priorities.

Procedure

1. Launch the Windows command prompt.
   a. Click **Start** > **Run**.
   b. Enter `cmd` in the **Open** field.
   c. Click **OK**. The command prompt window is displayed.
2. Navigate to the batch file folder. Type `<IMS installation folder>\bin`, then press **Enter**.
3. To change the scope of the policy, enter the following information.

   ```
   managePolPriority
   --policyId [name of policy]--scope [scp ims or scp machine] --templateId
   [template ID]
   ```

   The scope that is given highest priority is assigned a value of 1, the next scope is assigned with a value of 2, and so on.

   Note: Provide a template ID to specify the assigned template of the machine, user, or system.
4. Press **Enter**.

5. Type `exit` to close the command prompt and then press **Enter**.

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
- 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 22
- "Generating authorization codes for users" on page 23
- "Revoking authentication factors" on page 24

Setting password policies

Configure 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 that is 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 that is 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**, choose 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 that you want to delete for an ActiveCode-enabled authentication service account.
5. Click **Delete account**.
6. Click **OK**.

Revoking authentication factors

Revoke the strong authentication factor or Wallet when the user leaves the organization or when a strong 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 you set 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. Managing AccessProfiles in AccessAssistant or Web Workplace

As an Administrator, you can create and edit AccessProfiles for applications. If you do not have AccessStudio, create and update AccessProfiles in AccessAssistant or Web Workplace. After which, synchronize the data with the IMS Server.

See the following topics for more information:

- "Creating AccessProfiles"
- "Editing AccessProfiles" on page 28
- "Data synchronization with the IMS Server" on page 28

Creating AccessProfiles

Create an AccessProfile for an application through AccessAssistant or Web Workplace, so that you or users can single sign-on to applications from the My Web Workplace page.

Procedure

- If you want to create an AccessProfile for an application
  1. In the AccessAssistant or Web Workplace navigation panel, click **Manage AccessProfiles**.
  2. In the Manage AccessProfiles page, click **Add AccessProfile**.
  3. Provide the basic information about the AccessProfile such as the logon URL, the authentication service, and application, including which account data template to use.
  4. Click **Download logon page** to download the logon page into a new browser window.
  5. Click **Extract logon form** to generate the logon form.
  6. Click **Load logon form** to load the generated logon form in a new browser window.
  7. Click **Generate test signature** to identify the user name and password fields from the logon form.
  8. Click **Proceed to test** to verify the generated signature.
  9. Click **Go to final step**.
- If you want to add an authentication service entry in the list of available authentication services
  1. In the AccessAssistant or Web Workplace navigation panel, click **Manage AccessProfiles**.
  2. In the Manage AccessProfiles page, click **Add AccessProfile**.
  3. Click **Create new authentication service**.
  4. Assign an ID for the authentication service.
  5. Provide a display name and description.
  6. Assign a default account data template for the authentication service.
- If you want to add an application entry in the list of available authentication services

1. In the AccessAssistant or Web Workplace navigation panel, click **Manage AccessProfiles**.
2. In the Manage AccessProfiles page, click **Add AccessProfile**.
3. Click **Create new application**.
4. Assign an ID for the application.
5. Provide a display name and description.

Editing AccessProfiles

You can use the AccessAssistant or Web Workplace Manage AccessProfiles option to view and edit an AccessProfile configuration for an application. You can also delete an AccessProfile when necessary.

Procedure

- If you want to modify an AccessProfile configuration
  1. In the AccessAssistant or Web Workplace navigation panel, click **Manage AccessProfiles**.
  2. In the Manage AccessProfiles page, click the name of the selected application.
  3. Edit the details of the AccessProfile accordingly.
  4. Click **Update**.
- If you want to delete an AccessProfile
  1. In the AccessAssistant or Web Workplace navigation panel, click **Manage AccessProfiles**.
  2. In the Manage AccessProfiles page, click the name of the selected application.
  3. Click **Delete**.

Data synchronization with the IMS Server

You must regularly synchronize the AccessProfiles and other data that you created or updated from AccessAssistant or Web Workplace with the IMS Server.

In the AccessAssistant or Web Workplace navigation panel, click **Synchronize system data with IMS Server**.

Chapter 6. Report administration

The IBM Security Access Manager for Enterprise Single Sign-On solution supports the IBM Cognos® reporting framework for report generation.

Available reports

The IBM Security Access Manager for Enterprise Single Sign-On reporting package includes the following reports:

Application Usage Report
Use this report to track and monitor the activities of one or more users for each authentication services.

Help desk Activity Report
Use this report to track and monitor the activities of one or more Help desk users.

Token Information Report
Use this report to track and monitor the activities performed by the user on the registered authentication factors.

User Information Report
Use this report to track and monitor the activities of one or more users.

For more information about each of these reports, see "Report descriptions and parameters" on page 45.

Note: For the BIRT-based format of these reports, use IBM Tivoli Common Reporting version 2.1.1. See Appendix A, "Tivoli Common Reporting," on page 55.

IBM Cognos reporting framework

Use the IBM Cognos reporting framework to create and analyze IBM Security Access Manager for Enterprise Single Sign-On reports. With this framework, you can modify the schema and generate reports in different formats.

Note: Cognos reporting does not support Microsoft SQL Server database. Use DB2® database or Oracle database instead.

The IBM Cognos reporting framework includes the following items:

Reporting model
Represents the business view of the IBM Security Access Manager for Enterprise Single Sign-On data. You can use the models to customize and generate different types of IBM Security Access Manager for Enterprise Single Sign-On that suit your requirements.

Static reports
Ready-to-use reports that are bundled with the IBM Security Access Manager for Enterprise Single Sign-On reporting package.

IBM Cognos Business Intelligence reporting components

This topic describes the IBM Cognos Business Intelligence reporting components that you might use while you work with the IBM Security Access Manager for Enterprise Single Sign-On Cognos report models.

Query Studio

Query Studio is the reporting tool for creating simple queries and reports in IBM Cognos Business Intelligence. To use Query Studio effectively, you must be familiar with your organization's business and its data. You might also want to be familiar with other components of IBM Cognos Business Intelligence.

Report Studio

Report Studio is a Web-based report authoring tool that professional report authors and developers use to build sophisticated, multiple-page, multiple-query reports against multiple databases. With Report Studio, you can create any reports that your organization requires, such as invoices, statements, and weekly sales and inventory reports.

Your reports can contain any number of report objects, such as charts, crosstabs, lists, and also non-BI components such as images, logos, and live embedded applications that you can link to other information.

IBM Cognos Business Intelligence Connection

IBM Cognos Business Intelligence Connection is the portal to IBM Cognos Business Intelligence software. IBM Cognos Business Intelligence Connection provides a single access point to all corporate data available in IBM Cognos Business Intelligence software.

You can use IBM Cognos Business Intelligence Connection to create and run reports and cubes and distribute reports. You can also use it to create and run agents and schedule entries.

Framework Manager

Framework Manager is a metadata modeling tool that drives query generation for IBM Cognos Business Intelligence software. A model is a collection of metadata that includes physical information and business information for one or more data sources.

IBM Cognos Business Intelligence software enables Performance Management on normalized and denormalized relational data sources and various OLAP data sources. When you add security and multilingual capabilities, one model can serve the reporting, ad hoc querying, and analysis needs of many groups of users around the globe.

Before you do anything in IBM Cognos Business Intelligence Framework Manager, you must thoroughly understand the reporting problem that you want to solve.

Prerequisites for IBM Cognos report server

To work with the IBM Security Access Manager for Enterprise Single Sign-On Cognos-based reports, set up the IBM Cognos report server.

You must install the software in the following table:

Table 1. Software requirements for IBM Cognos report server

Software	For more information, see
IBM Cognos Business Intelligence Server, version 10.2.1 Fix Pack 1	1. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp. 2. Search for **Business Intelligence Installation and Configuration Guide 10.2.1.1**. 3. Search for the installation information and follow the procedure.
Web server	1. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp. 2. In the right pane of the home page, under **Supported hardware and software** section, click **IBM Cognos 10.2.1 Business Intelligence software environments**. 3. Click **10.2.1** tab. 4. Click **Software** in the **Requirements by type** column under the section **IBM Cognos Business Intelligence 10.2.1**. 5. Search for **Web Servers** section.
Data sources	1. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp. 2. In the right pane of the home page, under **Supported hardware and software** section, click **IBM Cognos 10.2.1 Business Intelligence software environments**. 3. Click **10.2.1** tab. 4. Click **Software** in the **Requirements by type** column under the section **IBM Cognos Business Intelligence 10.2.1**. 5. Search for **Data Sources** section.

Note: Optionally, you can install IBM Framework Manager, version 10.2.1 Fix Pack 1 if you want to customize the reports or models.

Installation of IBM Cognos reporting components

Installation of IBM Cognos reporting components is optional. You need these components only if you use the IBM Security Access Manager for Enterprise Single Sign-On Cognos-based reports.

You must complete the installation before you can access and work with IBM Security Access Manager for Enterprise Single Sign-On Cognos-based reports.

Note: IBM Cognos reporting does not support Microsoft SQL Server database as content store. Use DB2 database or Oracle database instead.

The following table describes the installation and synchronization process.

Table 2. Installation process

Task	For more information
Install Cognos Business Intelligence 10.2.1 Fix Pack 1.	1. Access http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp. 2. Search for **Install Cognos BI on one computer**.
Install Framework Manager 10.2.1 Fix Pack 1. **Note:** This task is optional. Install this component only if you want to customize the reports or models.	1. Access http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp. 2. Search for **Installing Framework Manager**.

Cognos reporting

The IBM Security Access Manager for Enterprise Single Sign-On Cognos-based reports are available at IBM Passport Advantage®:

- `ISAMESSOReportingModel_8.2.1.zip`
- `ISAMESSOReportingPackage_8.2.1.zip`

Note: You must set the locale to English or to any supported language before you run any of the reports. See “Setting language preferences” on page 43. Otherwise, you might encounter a "Language not supported" issue.

Configuration of IBM Cognos reporting components

After you install the prerequisites for the Cognos Business Intelligence server, configure the Framework Manager, and create a content store database. Then, configure the web gateway and web server.

During the database configuration process, ensure that you complete the points in the following note.

Note:

- IBM Cognos reporting does not support Microsoft SQL Server database as content store. Use DB2 database or Oracle database instead.
- Set the `JAVA_HOME` environment variable to point to the JVM used by the application server.
- You must use the enterprise database as IBM Cognos content store.
- Delete the existing data source and create a new data source to enable an option of generating DDL during creation of the content store database. For information about data source creation, see “Creating a data source” on page 35.

The following table describes the configuration process.

Table 3. Configure IBM Cognos reporting components

Task	For more information
Configure Framework Manager.	1. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp. 2. Search for **Configuring Framework Manager on a 64-bit computer**.
Create a content store in the database.	1. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp. 2. Search for **Start IBM Cognos Configuration** and complete the steps as per your operating system. 3. Search for **Create a content store database**.
Configure the web gateway.	1. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp. 2. Search for **Configure the gateway**.
Configure your web server.	1. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp. 2. Search for **Configure your web server**.

Setting report server execution mode

You must have a report server execution mode that is set to 32-bit mode for the report packages that do not use dynamic query mode.

Procedure

1. Start IBM Cognos Business Intelligence Configuration.
2. In the **Explorer** panel, click **Environment**.
3. Click the **Value** box for **Report server execution mode**.
4. Select **32-bit**.
5. From the **File** menu, click **Save**.

What to do next

Restart the IBM Cognos Business Intelligence service. Complete the following steps:

1. Access the IBM Cognos Business Intelligence Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp.
2. Search for **Restarting the IBM Cognos Business Intelligence service to apply configuration settings**.

Setting environment variables

You must set the database environment variables for a user before you start the IBM Cognos processes.

Procedure

1. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp.
2. Search for **Database environment variables**.

What to do next

Start the Cognos service from IBM Cognos Configuration to host the IBM Cognos portal. Complete the following steps:

1. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp.
2. Search for **Starting or stopping the Cognos service**.

Importing the report package

Import the report package to work with the bundled report models and the static reports.

Before you begin

- Copy the reporting package files to the directory where your deployment archives are saved. The default location is `c10_location/deployment`. For more information about the reporting packages, see "Installation of IBM Cognos reporting components" on page 31.
- To access the **Content Administration** area in IBM Cognos Administration, you must have the required permissions for the administration tasks secured feature.

Procedure

1. Access the IBM Cognos Gateway URI. For example, `https://`*`hostname:port`*`/ibmcognos/cgi-bin/cognos.cgi`. The *localhost* is the IP address or network host name where IBM Cognos gateway is configured. The *portnumber* is the port on which the IBM Cognos gateway is configured.
2. Go to **Launch**.
3. In the IBM Cognos Administration window, click the **Configuration** tab.
4. Click **Content Administration**.
5. Clear the history.
6. On the toolbar, click `New Import` icon. The New Import wizard opens.
7. In the **Deployment Archive** box, select the reporting package **ISAMESSOReportingPackage_8.2.1**.
8. Click **Next**.
9. In the **Specify a name and description** window, you can add the description and screen tip.
10. Click **Next**.
11. In the **Select the public folders and directory content** window, select the model that is displayed.
12. In the **Specify the general options** page, select whether to include access permissions and references to external namespaces, and an owner for the entries after they are imported.

13. Click **Next**. The summary information opens.
14. Review the summary information. Click **Next**.
15. In the **Select an action** page, click **Save and run once**.
16. Click **Finish**.
17. Specify the time and date for the run.
18. Click **Run**.
19. Review the run time. Click **OK**.
20. When the import file operation is submitted, click **Finish**.

Results

You can now use the report package to create reports and to run the sample reports. The sample reports are available in the reporting model on the **Public Folders** tab in the IBM Cognos portal.

Creating a data source

To work with the IBM Security Access Manager for Enterprise Single Sign-On Cognos-based reports, you must create a data source.

Before you begin

- Use `ISAMESSO` as the data source name.
- If you are working with DB2 database client, copy the file `db2cli.dll` from the DB2 client installation directory to the *<IBM Cognos installation directory>*`/bin` folder.
- Catalog the database if the data source is remote. Use the following commands:
  - `db2 catalog tcpip node <alias-name> remote <remote-DB-server> server <port-no>`
  - `db2 catalog database <remote-dbe> as <alias-name> at node <alias-name>`

Procedure

1. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp.
2. Search for **Creating a data source** and complete the steps.

What to do next

Note: Corrupted attribute names are displayed in the reports for `Arabic`, `Chinese`, `Hebrew`, `Japanese`, `Korean`, and `Russian` languages. Double-byte character set (DBCS) characters appear to be corrupted in the reports. Edit the data source so that the data flow is in Unicode format. Complete the following steps:

1. On the Work with Reports page, click **Launch** > **IBM Cognos Administration**.
2. Click **Configuration** to open the data source connection.
3. Click **ISAMESSO**.
4. Under the **Actions** column, click **Set properties-ISAMESSO**.
5. On the **Set properties-ISAMESSO** window, click **Connection**.
6. In the **Connection String** field, click the pencil symbol to edit the connection string.
7. In the **Collation Sequence** field, type `@UNICODE`.
8. Click **OK**.

9. Run the report to verify that the text is no longer corrupted.

Enabling the drill-through for PDF format

You must enable the drill-through functionality to run the drill-through reports in the PDF format.

Before you begin

Disable any pop-up blocking software in the browser.

Procedure

1. Open IBM Cognos Configuration.
2. Specify the fully qualified domain name for all the URIs that are defined.
3. Save the configuration.
4. Restart the IBM Cognos service. Complete the following steps:
   a. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp.
   b. Search for **Restarting the IBM Cognos service to apply configuration settings**.
5. In the **Explorer** window, click **Environment**.
6. In the **Group Properties** window, copy the value in the **Gateway URI** box.
7. Paste the copied **Gateway URI** value in the supported browser.
8. Run the report that you want.

Results

The drill-through report is run successfully in the PDF format.

Security layer configuration around the data model and reports

An access to the data model and reports can be restricted to a set of authorization roles. The users can create the authorization roles and associate them with the reporting entities. Only entitled users can access the data model or reports.

Authentication and authorization for IBM Cognos reports

IBM Cognos Business Intelligence administrators can set up the folders that store the reports. They can then secure those folders so that only authorized users can view, change, or perform other tasks by using the reports in the folder. To set up access control on the reports, administrators can set up the user authentication and define the access control for the set of users.

User authentication setup by using LDAP

You can configure IBM Cognos 10.2.1 Fix Pack 1 components to use an LDAP namespace for authentication when the users are in an LDAP user directory.

Configuring an LDAP Namespace for IBM Directory Server

If you configure a new LDAP namespace for use with the IBM Directory Server, you must modify the necessary settings and change the values for all properties of the IBM Directory objects.

Procedure

1. Open IBM Cognos Configuration.
2. In the Explorer window, under **Security**, right-click **Authentication**.
3. Click **New resource** > **Namespace**.
4. In the **Name** box, type a name for your authentication namespace.
5. In the **Type** list, click **LDAP-General default values**.
6. Click **OK**. The new authentication namespace resource appears in the Explorer window, under the **Authentication** component.
7. In the Properties window, for the **Namespace ID** property, specify a unique identifier for the namespace.

   Tip: Do not use colons (:) in the Namespace ID property.
   For **Host and Port**, specify `<Hostname>:<port>`. For example, `localhost:389`.
8. Specify the values for all other properties to ensure that IBM Cognos 10.2.1 Fix Pack 1 can locate and use your existing authentication namespace.
   - For **Base Distinguished Name**, specify the entry for a user search.
   - For **User lookup**, specify `(uid=${userID})`.
   - For **Bind user DN and password**, specify `cn=root`. For example, `cn=root` as a user name and `secret` as a password.

     Note: Specify the values if you want an LDAP authentication provider to bind to the directory server by using a specific bind user DN and password. If no values are specified, an LDAP authentication namespace binds as anonymous.
9. If you do not use external identity mapping, use bind credentials to search an LDAP directory server. Complete the following items.
   - Set **Use external identity** to **False**.
   - Set **Use bind credentials for search** to **True**.
   - Specify the user ID and password for **Bind user DN and password**.
10. To configure an LDAP advanced mapping properties, see the values that are specified in the following table.

Table 4. LDAP advanced mapping values

Mappings	LDAP property	LDAP value
Folder	Object class	`organizationalunit`, `organization`, and `container`
	Description	`description`
	Name	`ou`, `o`, and `cn`
Group	Object class	`groupofnames`
	Description	`description`
	Member	`member`
	Name	`cn`
Account	Object class	`inetorgperson`

Table 4. LDAP advanced mapping values (continued)

Mappings	LDAP property	LDAP value
	Business phone	telephonenumber
	Content locale	(leave blank)
	Description	description
	Email	mail
	Fax/Phone	facsimiletelephonenumber
	Given name	givenname
	Home phone	homephone
	Mobile phone	mobile
	Name	cn
	Pager phone	pager
	Password	userPassword
	Postal address	postaladdress
	Product locale	(leave blank)
	Surname	sn
	Username	uid

If the schema is modified, you must make extra mapping changes.

11. To prevent the anonymous access, complete the following steps:
    a. Go to **Security** > **Authentication** > **Cognos**.
    b. Set **Allow anonymous access?** to **False**.
12. From the **File** menu, click **Save**.

Results

A new LDAP namespace is configured with the appropriate values.

What to do next

Create the users in an LDAP. See "Creating users in an LDAP."

Creating users in an LDAP

See the example in this procedure that uses an LDAP utility to create users in LDAP.

Procedure

1. Open an LDAP utility. For example, if you are using the IBM Directory Server, the LDAP utility is `idsldapadd`.
2. Import the sample file `LdapEntries.ldif` that lists all the users who are authorized to access the reports. See the following example.

Results

After the successful import operation, you can see the users that are created in `ou=users,ou=SWG`.

Example

A sample file: `LdapEntries.ldif`

In this example, dc=com is the root entry. Specify the entry according to the schema that you use.

```
dn: ou=SWG, dc=com
ou: SWG
objectClass: top
objectClass: organizationalUnit

dn: ou=users,ou=SWG, dc=com
ou: users
objectClass: top
objectClass: organizationalUnit

dn: uid=steves,ou=users,ou=SWG, dc=com
uid: steves
userPassword:: hello123
objectClass: inetOrgPerson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: Wiley
cn: Steves

dn: uid=PortalAdmin,ou=users,ou=SWG, dc=com
userPassword:: hello123
uid: PortalAdmin
objectClass: inetOrgPerson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: Poon
cn: Chuck

dn: uid=william,ou=users,ou=SWG, dc=com
userPassword:: hello123
uid: william
objectClass: inetOrgPerson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: Hanes
cn: William

dn: uid=lucy,ou=users,ou=SWG, dc=com
userPassword:: hello123
uid: lucy
objectClass: inetOrgPerson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: Haye
cn: Lucy
```

What to do next

Authenticate IBM Cognos Business Intelligence by using an LDAP user. Complete these steps:

1. Access the IBM Cognos Business Intelligence Gateway URI. For example, http://*localhost:portnumber*/ibmcognos/cgi-bin/cognos.cgi. The *localhost* is the IP address or network host name where IBM Cognos Business Intelligence gateway is configured. The *portnumber* is the port on which the IBM Cognos Business Intelligence gateway is configured.
2. Select the configured **Namespace**, and click **OK**.
3. Enter your LDAP user ID and password.

4. Click **OK**.

Access control definition for the reports and reporting packages

You can define the access control for the LDAP users who are the members of a role that is defined in the IBM Cognos Business Intelligence namespace. Access can be granted to those users who are the members of a defined role.

A user who has the system administrator privileges can grant the access.

Initially, all users are the members of the system administrator. Therefore, you can log in with your LDAP user authentication in IBM Cognos Business Intelligence and access the administration section before you restrict the administration access.

Restricting administration access and adding an LDAP user to system administrator role

You can restrict the IBM Cognos Business Intelligence administration access by using the system administrators role in IBM Cognos Business Intelligence namespace. You can also add an LDAP user to the system administrator role for IBM Cognos Business Intelligence report administration.

Procedure

1. Log in to IBM Cognos Business Intelligence with an LDAP user whom you want to assign the system administrator role.
2. Go to **Launch**, and click **IBM Cognos Business Intelligence Administration**.
3. Click the **Security** tab.
4. In the **Users, Groups, and Roles** section, click **Cognos**.
5. Navigate to **System Administrator** role.
6. Click the **More** link.
7. Under **Available actions**, click **Set properties**.
8. Click the **Members** tab.
9. Click the **Add** link.
10. Under **Available entries** section, click an LDAP namespace.
11. Select the **Show users in the list** check box.
12. Select the user whom you want to assign the system administrator role and make it into selected entries list.
13. Click **OK**.
14. Select **Everyone** from the members entry.
15. Click the **Remove** link to ensure that only the added users can have the system administration access.
16. Click **OK**.
17. Click the **Permissions** tab.
18. Verify that the system administrators are listed and they are provided all the permissions.

    If no permissions are provided, then select the system administrators and grant all the permissions. Select the **Override the access permissions acquired from the parent entry** check box to grant the permissions.
19. Click **OK**.

Results

An LDAP user is added with the system administrator role.

What to do next

Create a role and add LDAP users as the members to that role. See "Creating a role and adding LDAP users as members."

Creating a role and adding LDAP users as members

The topic describes the procedure to create a role in IBM Cognos and add the members from an LDAP namespace to it.

Procedure

1. Log in to IBM Cognos with an LDAP user who has the system administrator privileges. For example, `PortalAdmin`.
2. Go to **Launch**, and click **IBM Cognos Administration**.
3. Click the **Security** tab.
4. In the **Users, Groups, and Roles** section, click **Cognos**.
5. Click the **New Role** icon from the palette.
6. Specify the name for a role. For example, `ISAMESSOAuditor`.
7. Add the description and the screen tip.
8. Click **Next**.
9. Under **Select the members**, click **Add**.
10. Under **Available Entries Directory**, click an LDAP namespace.
11. Select the **Show users in the list** check box.
12. Select the users whom you want to add as the members to the role and make it into selected entries list.
13. Click **OK**.
14. Click **Finish**.

Results

A new role is created and LDAP users are added as the members to the new role.

Defining an access to the report by using a role

You can define an access to the report by using a role. All the members of a role can access the report or reports.

Procedure

1. Log in to IBM Cognos with an LDAP user who has the system administrator privileges. For example, `PortalAdmin`.
2. Under **Public Folders**, click the reporting package **ISAMESSOReportingPackage_8.2.1**.
3. Click the **More** link on the **Actions** toolbar that is associated with the report for which you want to provide the access.
4. Under **Available actions**, click **Set properties**.
5. Click the **Permissions** tab.
6. Select the **Override the access permissions acquired from the parent entry** check box.
7. Click **Add** link at the bottom of the list of entries.

8. Click **Cognos**.
9. Select the role that you want to add and make it to the selected entries.
10. Click **OK**.
11. Select the role and grant the permissions.
12. Optional: Remove other roles for which you do not want to provide the access.
13. Click **OK**.

Results

An access is defined to the report by using a role and all the members of a role can access the reports.

Defining an access to the reporting package by using a role

You can define an access to the report package by using a role. All the members of a role can access the report package.

Procedure

1. Log in to IBM Cognos with an LDAP user who has the system administrator privileges. For example, `PortalAdmin`.
2. Under **Public Folders**, click the **More** link on the **Actions** toolbar that is associated with the report package **ISAMESSOReportingPackage_8.2.1**.
3. Under **Available actions**, click **Set properties**.
4. Click the **Permissions** tab.
5. Select the **Override the access permissions acquired from the parent entry** check box.
6. Click the **Add** link at the bottom of the list of entries.
7. Click **Cognos**.
8. Select the role that you want to add and make it to the selected entries.
9. Click **OK**.
10. Select the role and grant the permissions.
11. Optional: Remove other roles for which you do not want to provide the access.
12. Click **OK**.

Results

An access is defined for the reporting package by using a role and the members of a role can access the reporting package.

References for IBM Cognos report security configuration

Use the following references that provide information about the topics that are related to the security configuration for the IBM Cognos reports.

Access the IBM Cognos Business Intelligence 10.2.1 documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp and search for the following terms.

- **Security model**.
- **Authentication providers**.
- **Add or remove members of a cognos group or role**.

- **Create a cognos group or role**.
- **Authorization**.
- **Access permissions and credentials**.

Globalization overview

You can use the globalization features of IBM Security Access Manager for Enterprise Single Sign-On Cognos report models to produce the reports in your own language.

Language support overview

IBM Security Access Manager for Enterprise Single Sign-On Cognos reports support the following languages.

- cs=Czech
- de=German
- en=English
- es=Spanish
- fr=French
- hu=Hungarian
- it=Italian
- ja=Japanese
- ko=Korean
- pl=Polish
- pt_BR=Brazilian Portuguese
- ru=Russian
- zh_CN=Simplified Chinese
- zh_TW=Traditional Chinese
- nl=Dutch

Messages or terms related to the globalization

In the reports, some of the column values might display the term `Language not supported`

When you select the language that is not supported by the reporting model, the value in the column is displayed as `Language not supported`.

Setting language preferences

You can personalize the way data appears in IBM Cognos workspace by changing your preferences. You can set the product language or content language to get the preferred output format of the reports.

Before you begin

Install and configure the IBM Cognos Business Intelligence Server version 10.2.1 Fix Pack 1.

Procedure

1. In the IBM Cognos Connection window, click **My Area Options** menu button.
2. Click **My Preferences**.

3. In the Set Preferences window, under the **Regional options** section, select **Product language**. Product language specifies the language that the IBM Cognos user interface uses.
4. In the Set Preferences window, under the **Regional options** section, select **Content language**. Content language specifies the language that is used to view and produce content in IBM Cognos such as data in the reports.
5. Click **OK**.

Results

You can view the reports or user interface in the language that you specified.

References

Reference information is organized to help you locate particular facts quickly.

Report model configuration by using IBM Cognos components

To customize reports, you might be required to configure the report model. The following table provides a list of the basic tasks for configuring any IBM Cognos report model. It also provides information about the user guide for some IBM Cognos components.

Table 5. Basic tasks to configure report model

Tasks	**Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp.**
Framework Manager user guide.	Search for **Framework Manager User Guide 10.2.1**.
Query Studio user guide.	Search for **Query Studio User Guide 10.2.1**.
Report Studio user guide	Search for **Report Studio User Guide 10.2.1**.
Cognos Connection user guide	Search for **Cognos Connection User Guide 10.2.1**.
Import the metadata from the relational database.	Search for **Importing metadata from relational databases**.
Create a relationship.	Search for **Creating relationships**.
Modify a relationship.	Search for **Modifying a relationship**.
Create a complex expression for a relationship.	Search for **Creating complex expressions for a relationship**.
Create a data source query subject.	Search for **Data source query subjects**.
Create a model query subject.	Search for **Model query subjects**.
Update query subjects.	Search for **Updating query subjects**.
Create or modify a package.	Search for **Creating or modifying packages**.
Publish a package.	Search for **Publishing packages**.

Migration of Tivoli Common Reporting reports to IBM Cognos reports

If you want to convert the Business Intelligence and Reporting Tools (BIRT) reports to IBM Cognos reports, see the IBM Tivoli Common Reporting version 2.1.1 product documentation.

Search for "Converting BIRT reports to Cognos reports" at http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ttcr_converting_birt_to_cognos.html.

Report descriptions and parameters

Each of the IBM Security Access Manager for Enterprise Single Sign-On Cognos-based reports have parameters, which you can use to filter the scope of the report.

To create and view these reports, see “Generating the report through IBM Cognos Business Intelligence” on page 52.

Note: You must set the locale to English or to any supported language before you run any of the reports. See “Setting language preferences” on page 43. Otherwise, you might encounter a "Language not supported" issue.

Application Usage Report

Use this report to track and monitor the activities of one or more users for each authentication services.

The following table describes the parameters for filtering the report.

Table 6. Filters for the Application Usage Report

Parameter	Description
Audit Operation Date Range Start Date	Displays all events from the specified date.
Audit Operation Date Range End Date	Displays all events until the specified date.
Event	Displays the list of application usage events.
Authentication Service	Display the authentication service used for authentication.
User Name	Displays the unique identifier of the IBM Security Access Manager for Enterprise Single Sign-On user.

See “Generating the report through IBM Cognos Business Intelligence” on page 52.

Help desk Activity Report

Use this report to track and monitor the activities of one or more Help desk users.

The following table describes the parameters for filtering the report.

Table 7. Filters for the Help desk Activity Report

Parameter	Description
Audit Operation Date Range Start Date	Displays all events from the specified date.
Audit Operation Date Range End Date	Displays all events until the specified date.
Helpdesk User Name	Displays the unique identifier of the IBM Security Access Manager for Enterprise Single Sign-On Help desk user.
User Name	Displays the unique identifier of the IBM Security Access Manager for Enterprise Single Sign-On user.

Table 7. Filters for the Help desk Activity Report (continued)

Parameter	Description
Audit Event	Displays the actions and events performed by the IBM Security Access Manager for Enterprise Single Sign-On Help desk user. The supported audit events are: • ActiveCode-enabled authentication service account activation. • ActiveCode-enabled authentication service account addition. • ActiveCode-enabled authentication service account locked. • ActiveCode-enabled authentication service account removal. • Authentication factor revocation. • Authorization code issuance for online verification. • Mobile ActiveCode user sign up. • Revoke user.

See "Generating the report through IBM Cognos Business Intelligence" on page 52.

Token Information Report

Use this report to track and monitor the activities performed by the user on the registered authentication factors.

The following table describes the parameters for filtering the report.

Table 8. Filters for the Token Information Report

Parameter	Description
Audit Operation Date Range Start Date	Displays all events from the specified date.
Audit Operation Date Range End Date	Displays all events until the specified date.
User Name	Displays the user whose operation needs to be audited.
Token Type	Displays the type of authentication factors: • Fingerprint • OTP Token • RFID • Smart Card
Event	Displays the actions and events performed by the IBM Security Access Manager for Enterprise Single Sign-On user. The supported audit events are: • Authentication factor revocation • Register authentication factor

See "Generating the report through IBM Cognos Business Intelligence" on page 52.

User Information Report

Use this report to track and monitor the activities of one or more users.

The following table describes the parameters for filtering the report.

Table 9. Filters for the User Information Report

Parameter	Description
Audit Operation Date Range Start Date	Displays all events from the specified date.
Audit Operation Date Range End Date	Displays all events until the specified date.
User Enterprise ID	Displays the unique identifier of the IBM Security Access Manager for Enterprise Single Sign-On user.
Event	Displays the actions and events performed by the IBM Security Access Manager for Enterprise Single Sign-On user. The supported events are: • Sign up user • Mobile ActiveCode user sign up • OTP ActiveCode initialization • Revoke user and Delete user

See "Generating the report through IBM Cognos Business Intelligence" on page 52.

Report models

Use the IBM Security Access Manager for Enterprise Single Sign-On Cognos report models to generate different types of reports that suit your requirements.

Query Items

Query items are the smallest pieces of the model in a report. It represents a single characteristic of something, such as the date that a product was introduced.

Query subjects or dimensions contain query items. For example, a query subject that references an entire table contains query items that represent each column in the table.

Query items are the most important objects for creating reports. They use query item properties of query items to build their reports.

Query Subjects

Query subjects consists of a set of query items that have an inherent relationship. In most cases, query subjects behave like tables. Query subjects produce the same set of rows regardless of which columns were queried.

Namespaces

Uniquely identifies query items, dimensions, query subjects, and other objects. You import different databases into separate namespaces to avoid duplicate names.

Packages

Creates reports, analyses, and ad hoc queries. Packages are a subset of the dimensions, query subjects, and other objects that are defined in the project. A package is published to the IBM Cognos server.

ISAMESSO Module model

You can use the ISAMESSO Module model to customize the IBM Security Access Manager for Enterprise Single Sign-On Cognos-based reports.

The ISAMESSO Module model for IBM Security Access Manager for Enterprise Single Sign-On consists of the following namespaces:

Table 10. ISAMESSO Module model namespaces

Namespace	For information about query subjects and query items, see
ESSO Audit	"ESSO Audit namespace for ISAMESSO Module."

Query subjects and query items for the report models

Use the query subjects and query items information to customize the IBM Security Access Manager for Enterprise Single Sign-On Cognos-based reports.

ESSO Audit namespace for ISAMESSO Module

The ESSO Audit namespace provides information about the history of actions for the IBM Security Access Manager for Enterprise Single Sign-On users.

Query subjects for ESSO Audit namespace

The following table lists the query subjects in the ESSO Audit namespace for the ISAMESSO Module model.

Table 11. Query subjects in the ESSO Audit namespace

Report	Query subject	Description
Application Usage Report	Application Audit	Represents the authentication service activity of one or more users.
Help desk Activity Report	Helpdesk Audit	Represents the activity of one or more IBM Security Access Manager for Enterprise Single Sign-On Help desk users.
Token Information Report	Token Audit	Represents the activity of one or more user based on token type.
User Information Report	User Audit	Represents the audit of actions that are performed by the IBM Security Access Manager for Enterprise Single Sign-On user.

Query items for ESSO Audit namespace

The following table lists the query items in the ESSO Audit namespace.

Table 12. Query items in the ESSO Audit namespace

Query subject	Query items and their description
Application Audit	**User Machine IP Address** The unique identifier of the machine that is used by the IBM Security Access Manager for Enterprise Single Sign-On user. **Authentication Service** The users authentication service that is defined in IBM Security Access Manager for Enterprise Single Sign-On. **Application User Name** The user who has the privileged to perform the operation. **Event** The list of authentication service activities that users perform. The supported events are: • Auto-fill authentication service password • ActiveCode verification • Fortify authentication service password • Mobile ActiveCode request with application password • Mobile ActiveCode request with ISAM ESSO password • Privileged ID Check Out • Privileged ID Check In • RADIUS authentication RADIUS challenge-response **Result** Indicates whether the audit event is successful. **Description** The detailed description of the activity performed by the IBM Security Access Manager for Enterprise Single Sign-On user. **Server Machine** The server machine details. **Time of Activity** The time when the audit event happened. **User Name** The name of the IBM Security Access Manager for Enterprise Single Sign-On user.

Table 12. Query items in the `ESSO Audit` namespace (continued)

Query subject	Query items and their description
Helpdesk Audit	**User Ent ID** The unique identifier of the IBM Security Access Manager for Enterprise Single Sign-On user. **Ent ID** The unique identifier of the IBM Security Access Manager for Enterprise Single Sign-On help desk user. **Event** The action or event that is performed by the IBM Security Access Manager for Enterprise Single Sign-On Helpdesk user. The supported audit events are: • ActiveCode-enabled authentication service account activation. • ActiveCode-enabled authentication service account addition. • ActiveCode-enabled authentication service account locked. • ActiveCode-enabled authentication service account removal. • Authentication factor revocation. • Authorization code issuance for online verification. • Mobile ActiveCode user sign up. • Revoke user. **Result** Indicates whether the audit event is successful. **User Machine IP Address** The unique identifier of the machine that is used by the IBM Security Access Manager for Enterprise Single Sign-On user. **Server Machine** The server machine IP address or host name. **Time of Activity** The time when the audit event happened. **Description** The detailed description of the activity performed by the IBM Security Access Manager for Enterprise Single Sign-On user. **Mnemonic Code** Numeric code for the action that is performed by the IBM Security Access Manager for Enterprise Single Sign-On user.

Table 12. Query items in the ESSO Audit namespace (continued)

Query subject	Query items and their description
Token Audit	**User Name** The name of the IBM Security Access Manager for Enterprise Single Sign-On user. **Server Machine** The server machine details. **User Machine IP Address** The unique identifier of the machine that is used by the IBM Security Access Manager for Enterprise Single Sign-On user. **Event** The action or event that is performed by the IBM Security Access Manager for Enterprise Single Sign-On user. The supported audit events are: • Authentication factor revocation • Register authentication factor **User Enterprise ID** The unique identifier of the IBM Security Access Manager for Enterprise Single Sign-On user. **Time of Activity** The time when the audit event happened. **Result** Indicates whether the audit event is successful. **Token Type** The token types for which the event is generated. The supported token types are: • Fingerprint • OTP Token • RFID • Smart Card **Mnemonic Code** The mnemonic code of the event. **Token Type Code** The token type codes.

Table 12. Query items in the `ESSO Audit` namespace (continued)

Query subject	Query items and their description
User Audit	**User Attribute Name** The attribute name for IBM Security Access Manager for Enterprise Single Sign-On user. **User Name** The name of the IBM Security Access Manager for Enterprise Single Sign-On user. **User Enterprise ID** The unique identifier of the IBM Security Access Manager for Enterprise Single Sign-On user. **Server Machine** The server machine IP address or host name. **Event** The action that is performed by the IBM Security Access Manager for Enterprise Single Sign-On user. The supported audit events are: • Sign up user • Mobile ActiveCode user sign up • OTP ActiveCode initialization • Revoke user • Delete user **Mnemonic Code** Numeric code for the action that is performed by the IBM Security Access Manager for Enterprise Single Sign-On user. **Time of Activity** The time when the audit event happened. **Result** Indicates whether the audit event is successful.

Generating the report through IBM Cognos Business Intelligence

Each report type has its own set of search parameters to filter the report data based on your requirements. Use these search parameters to generate the content for your selected report.

About this task

You can choose the output format of the reports. For more information about the supported report format, search **Report Formats** from the IBM Cognos Business Intelligence product documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp.

Note:

- You can export the report data in plain format if you use formats other than HTML or PDF. The reports that are generated in such formats do not support some of the IBM Cognos interactive features. For example, `charts`. Use HTML or PDF formats for running interactive reports.
- Any time stamp in the following reports is in Greenwich Mean Time (GMT) format.
- Use the Report Studio to change the column title names in the layout to meet the specific needs of your company.

Procedure

1. Open IBM Cognos Connection.
2. Select the report model **ISAMESSOReportingPackage_8.2.1**.
3. Select the specific report.
4. Specify the parameters for the report.
   a. Enter a keyword or % in the filter field and click **Search**.
   b. Select the values from the **Results** list and click **Insert** to add the selected parameter values to the **Choice** list.
5. Click **Finish**. The Prompt Page Summary is displayed, which provides an overview of the specified report parameters.
6. Click **Page Down** to view the details of the report.

Troubleshooting

You might encounter some problems or limitations when you generate reports. This section describes the known problems and suggested solutions, including the known limitations of the IBM Security Access Manager for Enterprise Single Sign-On Cognos-based reports.

Problems and their solutions

Unable to view the Cognos drill through reports in Microsoft Internet Explorer version 10

If you are using the Microsoft Internet Explorer version 10 browser, the Cognos drill through reports might not work.

Solution

Complete the following steps:

1. Enable the compatibility view.
   a. In the Microsoft Internet Explorer 10 menu, go to **Tools**.
   b. Select **Compatibility View**.
2. Add the IBM Cognos website to the trusted sites list.
3. In the Microsoft Internet Explorer 10 menu, go to **Tools** > **Internet Options**.
4. On the **Security** tab, click the **Trusted sites** icon.
5. Click **Sites**.
6. In the **Add this website to the zone** box, add the IBM Cognos website address.
7. Click **Add**.
8. Click **Close**.

Long filter values are not shown completely on the prompt pages

Follow the technote link http://www-01.ibm.com/support/docview.wss?uid=swg21341018 to resolve this issue. The information in the technote also applies to IBM Cognos Business Intelligence 10.2.1 Fix Pack 1.

Generating reports is slow and causes timeouts

You might encounter slow performance or transaction time-outs during report generation for certain reports against large data sets.

To improve performance and reduce time-outs, follow these best practices:

- When you run the large reports in PDF output format, specify the appropriate filters or parameters and avoid the usage of the default filter **'Any'** that fetches all the records.
- In a large data deployment, specify the HTML output format. HTML format supports the pagination, which renders one page at a time and provides the options to move to the next pages.
- Tune the database. See the *IBM Security Identity Manager Performance Tuning Guide* at http://www-01.ibm.com/support/docview.wss?uid=swg27036205 for suggested indexes to set on columns in Report DB tables.

Known limitations

The Prompt Page Summary table in the IBM Cognos Business Intelligence Report shows "--" as the parameter value when more than 1000 filters per prompt is selected.

IBM Cognos Business Intelligence Reports provide the option for multiple selection. You can select more than one value for each parameter in the prompt page. When you select several values to filter the report, text overflow can occur and '--' is displayed instead in the Prompt Page Summary table.

Solution

Avoid selecting too many values for each parameter in the prompt page.

Languages that are not supported by the IBM Cognos Business Intelligence Server 10.2.1 Fix Pack 1

IBM Cognos Business Intelligence Server 10.2.1 Fix Pack 1 does not support the following languages:

- ar=Arabic
- iw=Hebrew

Note: The unsupported languages are not in the **Product Language** list, although they are displayed in the **Content Language** list in the Cognos configuration of IBM Cognos Business Intelligence Business Intelligence Server.

Appendix A. Tivoli Common Reporting

You can use Tivoli Common Reporting to generate and view the BIRT-based IBM Security Access Manager for Enterprise Single Sign-On reports.

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

Installation or upgrade to IBM Tivoli Common Reporting version 2.1.1

See the IBM Tivoli Common Reporting version 2.1.1 product documentation.

- For installation, see http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/index.jsp?topic=%2Fcom.ibm.tivoli.tcr.doc_211%2Fttcr_install.html.
- For upgrade, see http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ctcr_upgrade.html.

Generating reports in Tivoli Common Reporting tool 2.1.1

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 8.2.1 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 Microsoft Internet Explorer.
2. Log on using your user ID and password.
3. Select **Reporting** > **Common reporting** > **IBM Security Products** > **SAM Enterprise Single Sign On v8.2.1**.
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 B. 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 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*.

Custom audit logs

IBM Security Access Manager for Enterprise Single Sign-On has a custom audit log action framework that can log any event on the desktop. For example, log event where the user opens a Microsoft Word file. This customizable tracking capability leverages the AccessAgent plug-ins platform to automate collation of custom audit trails at the enterprise end-points.

To enable custom audit logging:

1. Define the custom event in the IMS Server through AccessAdmin.
2. Create the AccessProfile to generate the audit logs with the custom event. See *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide* for the procedure.
3. Search for the custom event through AccessAdmin or see the logged events in one or more audit reports through Tivoli Common Reporting.

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 you click 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 B, “Audit log events,” on page 57 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*.

Appendix C. 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 D. Updating policies in an upgraded IMS Server

If you are upgrading to IMS Server version 8.2.1, 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 F, "Changed policies from 8.1 to 8.2," on page 71 or Appendix G, "Changed policies from 8.0.1 to 8.2," on page 79 and identify the policy to be updated.
2. Navigate to `<IMS_INSTALL_8.2.1 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 E. Changed policies from 8.2 to 8.2.1

This section provides a list of the policy changes displayed in AccessAdmin 8.2 and AccessAdmin 8.2.1.

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

pid_wallet_inject_pwd_entry_option_default

8.2	8.2.1
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	*Display name* Default single sign-on password entry option *Description* Default single sign-on password entry option

pid_auth_inject_pwd_entry_option_default

8.2	8.2.1
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.	*Display name* Default single sign-on password entry option for the authentication service *Description* Default single sign-on password entry option for the authentication service. This policy overrides the system-wide default single sign-on password entry option.

pid_app_inject_pwd_entry_option_default

8.2	8.2.1
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.	*Display name* Default single sign-on password entry option for the application *Description* Default single sign-on password entry option for the application. This policy overrides the system-wide and the authentication service default single sign-on password entry options.

pid_auth_reauth_with_enc_pwd_enabled

8.2	8.2.1

pid_auth_reauth_with_enc_pwd_enabled

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

pid_auth_sso_enabled

8.2	**8.2.1**
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	*Display name* Enable single sign-on? *Description* Whether to enable single sign-on for the authentication service

pid_wallet_personal_app_sso_enabled

8.2	**8.2.1**
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	*Display name* Enable single sign-on for personal authentication services? *Description* Whether to enable single sign-on for personal authentication services

pid_app_reauth_with_enc_pwd_enabled

8.2	**8.2.1**
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	*Display name* Require re-authentication before performing single sign-on ? *Description* Whether password re-authentication is required before performing single sign-on for the application

pid_wallet_inject_pwd_entry_option_list

8.2	**8.2.1**
Description List of available password entry options for single sign-on using the automatic sign-on mode	*Description* List of available password entry options for single sign-on

pid_accessanywhere_app_sso_enabled

8.2	**8.2.1**

pid_accessanywhere_app_sso_enabled

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 to applications in AccessAssistant? *Description* Whether the user can single sign-on to applications through AccessAssistant

pid_engina_bypass_hot_key_policy_priority

8.2	**8.2.1**
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	*Display name* Policy priority for ESSO GINA Bypass Hot Key *Description* Whether the system or machine policy can be enforced for ESSO GINA Bypass Hot Key

pid_sso_policy_priority

8.2	**8.2.1**
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	*Display name* Policy priority for single sign-on *Description* Whether the user or machine policy can be enforced for single sign-on

pid_sso_user_control_enabled

8.2.	**8.2.1**
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	*Display name* Allow user to enable/disable single sign-on? *Description* Whether to allow user to enable/disable single sign-on

pid_lock_transparent_text

8.2	**8.2.1**
Display name Transparent screen lock message	*Display name* Transparent screen lock message

pid_lock_transparent_hot_key_enabled

8.2	**8.2.1**
Display name Enable transparent screen lock hot key?	*Display name* Enable transparent screen lock hot key?

Appendix F. 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 automatic sign-on? *Description* Whether password reauthentication is required before automatic sign-on for the authentication service	*Display name* Require re-authentication before single sign-on using the automatic sign-on mode? *Description* Whether password reauthentication is required before 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 G. 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

Notices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

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

Trademarks

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

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

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

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

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

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

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

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

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

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

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

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

Privacy Policy Considerations

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

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

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

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

Glossary

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

The following cross-references are used in this glossary:

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

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

A

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

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

account data item
The user credentials required for logon.

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

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

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

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

Active Directory credential
The Active Directory user name and password.

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

active radio frequency identification (active RFID) A second authentication factor and presence detector. See also radio frequency identification.

active RFID
See active radio frequency identification.

AD See Active Directory.

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

API See application programming interface.

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

application policy
A collection of policies and attributes governing access to applications.

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

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

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

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

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

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

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

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

B

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

base image
A template for a virtual desktop.

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

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

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

C

CA See certificate authority.

CAPI See cryptographic application programming interface.

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

CCOW
See Clinical Context Object Workgroup.

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

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

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

CLI See command-line interface.

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

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

command-line interface (CLI)
A computer interface in which the input and output are text based.

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

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

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

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

CSN See Card Serial Number.

CSP See cryptographic service provider.

D

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

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

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

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

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

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

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

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

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

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

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

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

DLL See dynamic link library.

DN See distinguished name.

DNS See domain name server.

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

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

E

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

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

ESSO See enterprise single sign-on.

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

F

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

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

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

FIPS See Federal Information Processing Standard.

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

FQDN
See fully qualified domain name.

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

G

GINA See graphical identification and authentication.

GPO See group policy object.

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

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

H

HA See high availability.

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

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

hot key
A key sequence used to shift operations

between different applications or between different functions of an application.

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

I

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

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

J

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

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

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

JMX See Java Management Extensions.

JRE See Java runtime environment.

JVM See Java virtual machine.

K

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

L

LDAP See Lightweight Directory Access Protocol.

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

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

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

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

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

M

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

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

N

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

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

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

O

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

OTP See one-time password.

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

P

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

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

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

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

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

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

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

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

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

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

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

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

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

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

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

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

R

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

RADIUS
See remote authentication dial-in user service.

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

RDP See remote desktop protocol.

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

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

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

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

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

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

RFID See radio frequency identification.

root CA
See root certificate authority.

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

S

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

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

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

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

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

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

security trust service chain
A group of module instances that are

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

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

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

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

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

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

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

sign up
To request a resource.

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

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

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

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

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

SMTP See Simple Mail Transfer Protocol.

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

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

SPI See service provider interface.

SSL See Secure Sockets Layer.

SSL VPN
See Secure Sockets Layer virtual private network.

SSO See single sign-on.

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

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

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

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

STS See Security Token Service.

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

T

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

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

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

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

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

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

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

tty See terminal type.

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

U

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

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

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

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

V

VB See Visual Basic.

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

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

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

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

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

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

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

VMM See Virtual Member Manager.

VPN See virtual private network.

W

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

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

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

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

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

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

Index

Q

R

S

T

U

W

Printed in USA

SC23-9951-05