IBM® Security Access Manager for Enterprise Single Sign-On
Version 8.2.1.1

Help Desk Guide

SC23-9953-04

IBM® Security Access Manager for Enterprise Single Sign-On
Version 8.2.1.1

Help Desk Guide

SC23-9953-04

Note

Before using this information and the product it supports, read the information in “Notices” on page 17.

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 Help desk officers. *IBM Security Access Manager for Enterprise Single Sign-On Help Desk Guide* provides Help desk officers information about managing queries and requests from users usually about their authentication factors. Use this guide together with the IBM® Security Access Manager for Enterprise Single Sign-On Policies Definition Guide.

Access to publications and terminology

This section provides:

- A list of publications in the "IBM Security Access Manager for Enterprise Single Sign-On library."
- Links to "Online publications" on page viii.
- A link to the "IBM Terminology website" on page viii.

IBM Security Access Manager for Enterprise Single Sign-On library

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

- *IBM Security Access Manager for Enterprise Single Sign-On Quick Start Guide*, CF3T3ML

  IBM Security Access Manager for Enterprise Single Sign-On Quick Start Guide provides a quick start on the main installation and configuration tasks to deploy and use IBM Security Access Manager for Enterprise Single Sign-On.
- *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*, SC23995206

  IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide contains information about planning your deployment and preparing your environment. It provides an overview of the product features and components, the required installation and configuration, and the different deployment scenarios. It also describes how to achieve high availability and disaster recovery. Read this guide before you do any installation or configuration tasks.
- *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*, GI11930904

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

  This guide helps you to install the different product components and their required middleware. It also includes the initial configurations that are required to complete the product deployment. It covers procedures for using virtual appliance, WebSphere® Application Server Base editions, and Network Deployment.
- *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*, GC23969204

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

- *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide*, SC23995105

  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.
- *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide*, SC23969404

  IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide provides detailed descriptions of the different user, machine, and system policies that Administrators can configure in AccessAdmin. Use this guide along with the IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide.
- *IBM Security Access Manager for Enterprise Single Sign-On Help Desk Guide*, SC23995304

  This guide is intended for Help desk officers. *IBM Security Access Manager for Enterprise Single Sign-On Help Desk Guide* provides Help desk officers information about managing queries and requests from users usually about their authentication factors. Use this guide together with the IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide.
- *IBM Security Access Manager for Enterprise Single Sign-On User Guide*, SC23995005

  This guide is intended for the users. *IBM Security Access Manager for Enterprise Single Sign-On User Guide* provides instructions for using AccessAgent and Web Workplace.
- *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide*, GC23969303

  IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide provides information about issues with regards to installation, upgrade, and product usage. This guide covers the known issues and limitations of the product. It helps you determine the symptoms and workaround for the problem. It also provides information about fixes, knowledge bases, and support.
- *IBM Security Access Manager for Enterprise Single Sign-On Error Message Reference Guide*, GC14762402

  IBM Security Access Manager for Enterprise Single Sign-On Error Message Reference Guide describes all the informational, warning, and error messages that are associated with IBM Security Access Manager for Enterprise Single Sign-On.
- *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide*, SC23995605

  IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide provides information about creating and using AccessProfiles. This guide provides procedures for creating and editing standard and advanced AccessProfiles for different application types. It also covers information about managing authentication services and application objects, and information about other functions and features of AccessStudio.
- *IBM Security Access Manager for Enterprise Single Sign-On AccessProfile Widgets Guide*, SC27444401

  IBM Security Access Manager for Enterprise Single Sign-On AccessProfile Widgets Guide provides information about creating and using widgets.

- *IBM Security Access Manager for Enterprise Single Sign-On Tivoli® Endpoint Manager Integration Guide*, SC27562000

  IBM Security Access Manager for Enterprise Single Sign-On Tivoli Endpoint Manager Integration Guide provides information about how to create and deploy Fixlets for AccessAgent installation, upgrade or patch management. It also includes topics about using and customizing the dashboard to view information about AccessAgent deployment on the endpoints.
- *IBM Security Access Manager for Enterprise Single Sign-On Provisioning Integration Guide*, SC23995704

  IBM Security Access Manager for Enterprise Single Sign-On Provisioning Integration Guide provides information about the different Java™ and SOAP API for provisioning. It also covers procedures for installing and configuring the Provisioning Agent.
- *IBM Security Access Manager for Enterprise Single Sign-On Web API for Credential Management Guide*, SC14764601

  IBM Security Access Manager for Enterprise Single Sign-On Web API for Credential Management Guide provides information about installing and configuring the Web API for credential management.
- *IBM Security Access Manager for Enterprise Single Sign-On Serial ID SPI Guide*, SC14762601

  IBM Security Access Manager for Enterprise Single Sign-On Serial ID SPI Guide describes how to integrate any device with serial numbers and use it as a second authentication factor with AccessAgent.
- *IBM Security Access Manager for Enterprise Single Sign-On Epic Integration Guide*, SC27562300

  IBM Security Access Manager for Enterprise Single Sign-On Epic Integration Guide provides information about the IBM Security Access Manager for Enterprise Single Sign-On and Epic integration, including supported workflows, configurations, and deployment.
- *IBM Security Access Manager for Enterprise Single Sign-On Context Management Integration Guide*, SC23995404

  IBM Security Access Manager for Enterprise Single Sign-On Context Management Integration Guide provides information about installing, configuring, and testing the Context Management integrated solution in each client workstation.
- *IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Mobile Guide*, SC27562101

  IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Mobile Guide provides information about the deployment and use of single sign-on on mobile devices.
- *IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Virtual Desktop Infrastructure Guide*, SC27562201

  IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Virtual Desktop Infrastructure Guide provides information about setting up single sign-on support on a Virtual Desktop Infrastructure, and the different user workflows for accessing the virtual desktop.
- *IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Terminal Server and Citrix Server Guide*, SC27566801

  IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Terminal Server and Citrix Server Guide provides information about the required configurations and supported workflows in the Terminal and Citrix Servers.

Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Security Access Manager for Enterprise Single Sign-On library
The product documentation site (http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itamesso.doc_8.2.1/kc-homepage.html) displays the welcome page and navigation for the library.

IBM Security Systems Documentation Central
IBM Security Systems Documentation Central provides an alphabetical list of all IBM Security Systems product libraries and links to the online documentation for specific versions of each product.

IBM Publications Center
IBM Publications Center offers customized search functions to help you find all the IBM publications you need.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology.

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 on Help desk tasks

As a Help desk officer, you can manage users, manage authentication factors, modify policies, and view system and machine policies in AccessAdmin.

See the following topics for more information:

What to do	Where to find information
Manage users • Verify user identity. • View user profiles. **Note:** Only Administrators can revoke users.	• "Verifying user identity" • "Viewing a user profile" on page 3
Manage second authentication factors • Help users with second authentication factors.	Chapter 2, "Managing authentication factors," on page 5
Modify policies • Modify user policies such as Wallet and AccessAgent policies. **Note:** You can modify user policies except administrative policies.	Chapter 3, "Modifying policies," on page 11
View system and machine policies • View machine and system scope policies.	Chapter 4, "Viewing policies," on page 15

To learn more about the user workflows, see the *IBM Security Access Manager for Enterprise Single Sign-On User Guide*.

To learn more about common issues and problems, see the *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide*.

Verifying user identity

You must verify the identity of the user to prevent unauthorized access to protected systems.

- You might communicate with the user personally, online, or over the telephone. Set a standard method of verifying the identity of the user in line with your corporate policies.
- You might require a user to provide information such as an employee number or the maiden name of the mother. Make sure that you verify the accuracy of the credentials information.

There are cases when a user might acquire the identity of a co-worker to gain unauthorized access. If you suspect that the user is committing fraud, request for more information and make sure that you deal with it according to your corporate policies.

Good security practices

You must advise users on the different data security practices so that they can protect their data from unauthorized access.

Table 1. Data security practices

Practice	Description
Choose strong passwords and keep them secure **Note:** The Administrator can configure the required password length and maximum number of attempts to log on before the Wallet is locked.	Advise users to choose passwords that are not easy to decode. A strong password is longer and is a combination of uppercase characters, lowercase characters, numbers, and special characters.
Do not forget the secret	Secrets help users set new passwords in case they forget their passwords.
Safeguard the second authentication factor	The second authentication factor fortifies the Wallet, and must be kept in a secure place.
Safeguard the desktop	If users are leaving their workstations, tell them to always lock their computer.
Report loss of a second authentication factor	Advise the users to immediately inform Help desk if their second authentication factor is missing or misplaced. **Important:** When a user reports a missing second authentication factor, revoke the second authentication factor immediately. For more information, see “Revoking authentication factors” on page 9.

Logging on to AccessAdmin

Use AccessAdmin to manage users, authentication factors, and policies.

Procedure

1. Navigate to AccessAdmin.
   - If you are using a load balancer, access `https://<loadbalancer_hostname>:<ihs_ssl_port>/admin`.
   - If you are not using 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 user name and password.
4. Click **Log on**.

Checking the IMS Server status

When you check the status of the IMS Server, you can also view the server availability and version number.

Procedure

1. Log on to AccessAdmin.
2. Select **System** > **Status**. The page displays license information and IMS Server system logs.

Viewing a user profile

Use AccessAdmin to view a user profile.

Procedure

1. Log on to AccessAdmin.
2. Click **My users** under **Search Users**.

   Note: If no users are displayed, request your Administrator to assign users to you.
3. Click the user name. The following links are displayed.

Option	Description
Audit logs	These logs contain the specific details of user activity logs. For example: time of the activity, the type of activity, and the SOCI ID.
Authentication service	This link contains the different types of authentication services that are enabled for the user.

4. Scroll down the page. Under **User Profile**, the following details are displayed. You can modify these details except for the Administrative Policies.
   - Name
   - Last name
   - E-mail address
   - Enterprise user name
   - User principle name
   - Mobile ActiveCode phone number
   - Mobile ActiveCode e-mail address
   - Mobile AcitveCode preferences
   - Helpdesk Authorization
   - Authentication Factors
   - OTP Token Assignment
   - Cached Wallets
   - Wallet Access Control
   - Administrative Policies (for administrators only)
   - Authentication Policies
   - AccessAssistant and Web Workplace Policies
   - Wallet Policies
   - AccessAgent Policies
   - Authentication Service Policies

Chapter 2. Managing authentication factors

Managing second authentication factors involve tasks such as distribution, maintenance, and safekeeping of these authentication factors.

Task	Description
Providing second authentication factors to new employees	Orient each new employee on the basic concepts of IBM Security Access Manager for Enterprise Single Sign-On.
Replacing lost second authentication factors	The second authentication factor must be revoked when it is lost or stolen to prevent unauthorized use. **Note:** Revocation is permanent within the IBM Security Access Manager for Enterprise Single Sign-On system. When a second authentication factor is revoked, it cannot be reused unless it is registered again.
Safeguarding unused second authentication factors	Second authentication factors are of no value without user credentials, or unless registered with the IMS Server. Only one Help desk officer is required to monitor the inventory of second authentication factors. A contingency plan must be set in case the designated officer is not available.

For managing authentication factors with AccessAdmin, see the following topics:

- “Modifying second authentication factor-related policies”
- “Generating authorization codes for users” on page 8
- “Revoking authentication factors” on page 9

Modifying second authentication factor-related policies

Second authentication factor-specific policies are only applicable to users with more than one authentication factor. Modify the policies appropriate to the type of second authentication factor that is used by the user.

Smart card policies

Smart card policies are the policies that you can set to define how AccessAgent must behave when the user use a smart card for authentication.

Procedure

1. Log on to AccessAdmin.
2. Navigate to the profile of the user.
3. Click **AccessAgent Policies**.
4. Under **Smart card Policies**, complete the following field:

Option	Description
Smart card removal actions	The action that AccessAgent takes when the smart card is removed.

5. Click **Update**.

Hybrid smart card policies

Hybrid smart card policies are the policies that you can set to define how AccessAgent must behave when the user use a hybrid smart card for authentication.

Procedure

1. Log on to AccessAdmin.
2. Navigate to the profile of the user.
3. Click **AccessAgent Policies**.
4. Under **Hybrid Smart card Policies**, complete the following fields:

Option	Description
Enable single factor smart card unlock	Specifies whether 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 the single factor smart card logon time expiry when a user logs on using a smart card and PIN.
Actions on the desktop for using the same smart card if user logged on with single factor	The action that AccessAgent takes when the same smart card is presented when the user is logged in with a single factor.
Confirmation countdown duration, in seconds, on the desktop, for using the same smart card	The countdown time frame for the specified action to take place after tapping the same smart card.
Actions on the desktop for using a different smart card if the user logged on with single factor	The action that AccessAgent takes when a different smart card is presented when the user is logged in with a single factor.
Confirmation countdown duration, in seconds, on the desktop, for using a different smart card	The countdown time frame for the specified action to take place after tapping a different smart card.

5. Click **Update**.

RFID policies

RFID policies are the policies that you can set to define how AccessAgent must behave when the user use an RFID card for authentication.

Procedure

1. Log on to AccessAdmin.
2. Navigate to the profile of the user.
3. Click **AccessAgent Policies**.
4. Under **RFID Policies**, complete the following fields:

Option	Description
Actions on the desktop for tapping same RFID	Specifies the action that AccessAgent performs when the logged on user taps the RFID card on the reader again.
Confirmation countdown duration in seconds, on the desktop, for tapping same RFID on the card reader	Specifies the number of seconds that AccessAgent displays a message box. This box is displayed after the same RFID card is tapped on the reader. The message box provides two options for the user, one of which must be selected before the specified number of seconds expire. The user can either click **Yes** to proceed with the action, or **No** to reactivate the desktop.
Enable RFID-only unlock	If you set this policy to **Yes**, then the user can unlock the RFID card in a specified duration that does not require a password.
Time expiry, in seconds, for RFID-only unlock	Specifies the number of seconds that AccessAgent can apply an RFID-only unlock that does not require a password.
Time expiry, in minutes, for RFID-only logon	Specifies the number of minutes that AccessAgent can apply RFID-only logon that does not require a password.
Actions on tapping different RFID on desktop	Specifies the actions that AccessAgent performs when a user tap a different RFID card on the reader while another user is logged on.
Confirmation countdown duration in seconds, on the desktop, for tapping different RFID on the card reader	Specifies the number of seconds that AccessAgent displays a message box. This box is displayed after a user tap a different RFID card on the reader. The message box provides two options for the user, one of which must be selected before the specified number of seconds expire. The user can either click **Yes** so that AccessAgent can proceed with the action, or **No** to reactivate the desktop.

5. Click **Update**.

Fingerprint policies

Fingerprint policies are the policies that you can set to define how AccessAgent must behave when the user use a fingerprint for authentication.

Procedure

1. Log on to AccessAdmin.
2. Navigate to the profile of the user.
3. Click **AccessAgent Policies**.
4. Under **Fingerprint Policies**, complete the following fields:

Option	Description
Actions on the desktop for tapping the same finger	Specifies the action that AccessAgent performs when a logged on user imprints the same finger on the fingerprint reader.
Confirmation countdown duration, in seconds, on the desktop, for tapping the same finger on the fingerprint reader	Specifies the number of seconds that AccessAgent displays a message box. This box is displayed after a user imprinted the same finger on the fingerprint reader. The message box provides two options for the user, one of which must be selected before the specified number of seconds expire. The user can either click **Yes** so that AccessAgent can proceed with the action, or **No** to reactivate the desktop.
Actions on the desktop for tapping a different finger	Specifies the action that AccessAgent performs when another user imprints a finger on the reader, even though another user is logged on.
Confirmation countdown duration, in seconds, on the desktop, for tapping a different finger on the fingerprint reader	Specifies the number of seconds that AccessAgent displays a message box. This box is displayed after a different user places a finger on the fingerprint reader. The message box provides two options for the user, one of which must be selected before the specified number of seconds expire. The user can either click **Yes** so that AccessAgent can proceed with the action, or **No** to reactivate the desktop.

5. Click **Update**.

Generating authorization codes for users

An authorization code is a system-generated code that is used as an authentication factor for specific scenarios. It can be used for password reset, and temporary bypass of an authentication factor.

Procedure

1. Navigate to the profile of the user.
2. Ask the user whether a request code is displayed on screen.
   - If there is a request code, click **Temporary offline access to the Wallet** in the **Help desk Authorization** panel, 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, unlock account, temporary online access or registration of second factors** in the **Help desk Authorization** panel.

3. Select a validity period from the options in the list.
4. Click **Issue authorization code**.

Enabling ActiveCode for the user

ActiveCode is a randomly generated, event-based one-time password. Users use ActiveCodes to log on to web applications, AccessAssistant or Web Workplace, and applications supporting RADIUS, such as VPN Servers.

Procedure

1. Navigate to the profile of the user.
2. Under the user name, click **Authentication services**.
3. In **ActiveCode-enabled authentication service**, select the ActiveCode-enabled authentication services of the new user.
4. Enter the user name for the ActiveCode-enabled authentication service.
5. 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 a user enters a wrong ActiveCode several times.

Procedure

1. Navigate to the profile of the user.
2. Under the user name, click **Authentication services**.
3. In **ActiveCode-enabled authentication service**, select the user name and the ActiveCode-enabled authentication service to disable.
4. Select **Locked** from the **Status** list.
5. Click **Update status**.

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. Navigate to the profile of the user.
2. Under the user name, click **Authentication services**.
3. In **ActiveCode-enabled authentication service**, select the user name that you want to delete for an ActiveCode-enabled authentication service account.
4. Click **Delete account**.
5. Click **OK**.

Revoking authentication factors

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

Procedure

1. Navigate to the profile of the user.
2. Scroll down to the **Authentication Factors** panel.
3. Select the check box of the Wallet or authentication factor to revoke.
4. Click **Revoke**.

Chapter 3. Modifying policies

As a Help desk officer, you can modify user policies and view system and machine policies.

The following table summarizes the privileges of an Administrator and Help desk officer on policies.

Table 2. Privileges of an Administrator and Help desk officer on policies

Role	System Policies	Machine Policies	User Policies
Administrator	can view and modify	can view and modify	can view and modify
Help desk	view only	view only	can view and modify, except administrative policies

For more information about modifying and viewing policies:

- "Modifying AccessAgent policies"
- "Modifying Wallet policies" on page 13

Modifying AccessAgent policies

You can modify the policies that define the behavioral patterns of AccessAgent on a computer when a user is logged on.

Lock/Unlock policies

Lock and unlock policies are the policies that you can set to define when and how AccessAgent locks and unlocks the user session.

Procedure

1. Log on to AccessAdmin.
2. Navigate to the profile of the user.
3. Click **AccessAgent Policies**.
4. Under **Lock/Unlock Policies**, complete the following fields:

Option	Description
Enable lock script during locking of the user's AccessAgent session	If you select **Yes**, AccessAgent runs a lock script when locking an AccessAgent session.
Lock script type	Specifies the type of lock script to run when locking a session.
Lock script code	Specifies the source code of the lock script to run when locking a session.
Enable unlock script when user unlocks an existing AccessAgent session	If you select **Yes**, AccessAgent runs an unlock script when unlocking an existing AccessAgent session.
Unlock script type	Specifies the type of unlock script to run when unlocking a session.
Unlock script code	Specifies the source code of the unlock script to run when unlocking a session.

Option	Description
Unlock computer policy	Specifies the type of user who can unlock a computer after a logged on user is locked. Same user is the user who locked the computer. Admin is the Windows user with Administrator privileges on the computer.
Confirmation countdown, in seconds, for unlocking by a different user	Specifies the number of seconds a different user can unlock the computer.

5. Click **Update**.

Roaming session policies

Roaming session policies are the policies that you can set to define the AccessAgent action on a remote session when computer is locked or session is logged off.

Procedure

1. Under **Roaming session policies**, complete the following fields:

Option	Description
Actions on remote session while locking local computer	Option to disconnect the Terminal server session or log off the remote AccessAgent while locking the local computer.
Actions on remote session before logging off local session	Option to disconnect the Terminal server session or log off the remote AccessAgent before logging off the local AccessAgent.

2. Click **Update**.

Logon/Logoff policies

Logon and logoff policies are the policies that you can set to define how a user is logged on or logged off from a user session.

Procedure

1. Under **Logon/Logoff Policies**, complete the following fields:

Option	Description
Enable logon script during user logon	If you set this policy to **Enabled**, a script runs whenever the user logs on to AccessAgent. The logon script specifies various actions that AccessAgent performs upon logon, such as selecting the applications to start, or selecting the connecting network resources.
Logon script type	Specifies the types of logon script that is used with AccessAgent.
Logon script code	Use this option so that Administrators can copy the logon script source code in the text box.

Option	Description
Enable logoff script during user logoff	Specifies the running of a script whenever the user logs off from AccessAgent. The logoff script specifies various actions that AccessAgent performs upon logoff, such as selecting the applications to close and selecting the disconnecting network resources.
Logoff script type	Specifies the types of logoff script that is used with AccessAgent.
Logoff script code	Use this option so that Administrators can copy the logoff script source code in the text box.
Allow user to manually log off AccessAgent	If you set this policy to **Yes**, then users can log off from AccessAgent manually.
Actions on manual logoff by user	Specifies the action AccessAgent performs when the user logs off.
Confirmation countdown duration, in seconds, for manual logoff by user	Specifies the number of seconds the computer can request the user to confirm logoff after a period of inactivity.

2. Click **Update**.

Modifying Wallet policies

You can set Wallet policies such as exporting and the display of passwords in AccessAdmin.

Procedure

1. Navigate to the profile of the user.
2. Under **User Profile**, click **Wallet Policies**.
3. Complete the following fields:

Option	Description
Enable "Never" for enterprise authentication services	• If you set the policy to **Yes**, then a user can set an enterprise authentication services password entry option to **Never**. • If you set the policy to **No**, then the password entry option does not have the option **Never**.
Enable single sign-on using the automatic sign-on mode for personal authentication services	Specifies whether to enable automatic sign-on to authentication services.
Option for displaying of application passwords in AccessAgent	Specifies whether to display application passwords in the Wallet Manager of AccessAgent through the **Show passwords** option.
Option for exporting of application passwords in AccessAgent	Specifies whether to export application passwords in the Wallet Manager of AccessAgent through the **Export?** option.
Allow user to enable/disable single sign-on using the automatic sign-on mode	If you set the policy to **Yes**, then the user can enable automatic sign-on.

Option	Description
List of Wallet items that can be edited by the user through AccessAgent	Each Wallet item that the user can edit through AccessAgent is highlighted.

4. Click **Update**.

Setting Wallet authentication policies

A Wallet contains the credentials of a user, like passwords. Access to the Wallet is strengthened by enforcing the use of additional authentication factors, such as an RFID card or a smart card.

Procedure

1. Navigate to the profile of the user.
2. Under **User Profile**, click **Authentication Policies**.
3. Select the corresponding Wallet authentication policy.
4. Click **Update**.

Revoking cached Wallets

Revoke the cached user Wallets if the machine contains many Wallets that are no longer needed or if users cannot log on to their cached Wallets. When the cached Wallets are revoked, users can download a new Wallet from the IMS Server.

Procedure

1. Navigate to the profile of the user.
2. Scroll down to the **Cached Wallet** panel.
3. Select the check box of the Wallet that you want to revoke.
4. Click **Revoke**.

Locking Wallets

You can lock a Wallet to temporarily prevent access to the Wallet of the user. A good example is when the user goes for an extended holiday or when an employee leaves the organization.

Procedure

1. Navigate to the profile of the user.
2. Under **User Profile**, click **Wallet Access Control**.
3. Click **Lock Wallet**.

Chapter 4. Viewing policies

If you want to know or verify the values that are set for a particular user, machine or system policy, open AccessAdmin and select the corresponding policy category.

See the following topics for more information:
- "Viewing a user or machine policy template"
- "Viewing system policies"
- "Viewing administrative policies"

Viewing a user or machine policy template

You can view user and machine policy templates. Only administrators can modify them.

Procedure

1. In the AccessAdmin navigation panel, select your template.
   - For user policy templates, select **User Policy Templates** > **[name of the template]**.
   - For machine policy templates, select **Machine Policy Templates** > **Template assignments** > **[name of the template]**.

   Take note of the following information.
   - There is one Default template.

     If the Administrator defines the templates, these templates are displayed in the other templates available under the **Policy Templates** option in the navigation panel.
   - These other templates are fully configurable and the naming convention is set by the Administrator.
2. Click the policy to view the details.

Viewing system policies

You can view system policies in AccessAdmin.

Procedure

1. In the AccessAdmin navigation panel, select **System** > **System policies**.
2. Click the policy to view the details.

Viewing administrative policies

You can view administrative policies in AccessAdmin.

1. Navigate to the profile of the user.
2. Under **User Profile**, click **Administrative Policies**.

The current role and the Help desk identities are displayed.

The **Update**, **Revoke**, and **Delete user** buttons are not enabled because you cannot modify this setting.

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

Printed in USA

SC23-9953-04