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

User Guide

IBM® Security Access Manager for Enterprise Single Sign-On

Version 8.2.2

User Guide

Note

Before using this information and the product it supports, read the information in “Notices” on page 21.

Edition notice

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

Contents

About this publication

This guide is intended for the users. *IBM Security Access Manager for Enterprise Single Sign-On User Guide* provides instructions for using AccessAgent.

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 vii.
- 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,* CF49UML

  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*

  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*

  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 WebSphere® Application Server Base editions, and Network Deployment.
- *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*

  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*

  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*

  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*

  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*

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

  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*

  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*

  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*

  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 IBM Endpoint Manager Integration Guide*

  IBM Security Access Manager for Enterprise Single Sign-On IBM 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*

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 Guide*

  IBM Security Access Manager for Enterprise Single Sign-On Web API 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*

  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*

  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*

  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*

  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*

  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*

  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/v2r2/index.jsp?topic=/com.ibm.itamesso.doc_8.2.2/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. Single sign-on overview

With IBM Security Access Manager for Enterprise Single Sign-On, you can enter one user ID and password to access multiple applications.

You can also single sign-on to applications in a Citrix or Terminal Server if AccessAgent is installed on the Citrix or Terminal Server.

How single sign-on works

After you log on to AccessAgent, it automatically captures and auto-fills your application credentials from and to the application clients that you launch. These application credentials are saved in a *Wallet*.

When you single sign-on into an application, AccessAgent retrieves the application logon credentials from the Wallet. This Wallet is stored securely at the IBM Security Access Manager for Enterprise Single Sign-On IMS Server. AccessAgent downloads the Wallet from the IMS Server. As such, you can access your Wallet even when you use a different computer later.

If the IMS Server is offline or AccessAgent cannot connect to the IMS Server, you can still log on to AccessAgent if you have a cached Wallet. The cached Wallet is in encrypted form on your computer. You have to authenticate with your ISAM ESSO password and sometimes with another authentication factor if two-factor authentication is enabled.

The IMS Server is online if you can click **Sign up** or **Log on** in the AccessAgent navigational panel. The IMS Server connection refreshes every 30 minutes, or as determined by your Administrator.

AccessAgent information

If you want to view information about AccessAgent,

1. Right-click the AccessAgent icon in the system tray.
2. Select **About ISAM ESSO AccessAgent**.
3. Click **Export** to download the information in a text file.

IBM Security Access Manager for Enterprise Single Sign-On password

The ISAM ESSO password secures access to your Wallet.

The length of the ISAM ESSO password ranges from 6 to 20 characters, depending on the preference of your organization. When you sign up with AccessAgent, you must specify a password. You can use the enterprise Active Directory password as your ISAM ESSO password.

When you sign up with AccessAgent, you register the ISAM ESSO password with the IMS Server and you create a Wallet.

All application credentials are stored in the Wallet. Signing up ensures that your credentials are backed up on the IMS Server and are retrievable when needed.

You can associate your Wallet with a second authentication factor. The second authentication factor reinforces your password and protects the contents of your Wallet.

Use the following guidelines for specifying an ISAM ESSO password:

- Choose a password that is lengthy, unique, and a combination of uppercase letters, lowercase letters, and numbers.
- Do not use any of these words as passwords: dictionary words, the name of your pet, the name of your spouse or friend, or important dates.
- Never tell anyone your password, not even to the Help desk officer or Administrator.
- Never write down your password.
- Change your password as often as possible.

AccessAgent locks your Wallet after you attempt to log on five times with a wrong password. The number of logon attempts is set by your organization.

For more information, see the following topics:

- "Signing up using your password (Active Directory sync)" on page 5
- "Logging on using your password" on page 6
- "Changing passwords" on page 14
- "Resetting passwords without IMS Server connectivity" on page 15
- "Resetting passwords with IMS Server connectivity" on page 15

IBM Security Access Manager for Enterprise Single Sign-On icons

Several icons are used in IBM Security Access Manager for Enterprise Single Sign-On. Some of these icons are visible only when the user is logged on or when the fingerprint reader is detected

Table 1. Icons that are visible when the user is logged on

Icon	Description
🔒	AccessAgent is operating normally. When the icon is flashing, AccessAgent is: • synchronizing an authentication factor with the IMS Server • logging the user on
🔒	AccessAgent on the desktop and in the Start menu
⊘	Cancel ESSO GINA
🔑	Change your password
?	Access help
i	Session information

Table 1. Icons that are visible when the user is logged on (continued)

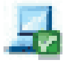
Icon	Description
	Launch the application
	Lock your computer
	Log off from AccessAgent
	Log on to AccessAgent
	Reset your password
	IMS Server connection is not available.
	IMS Server connection is available.
	Set your secrets
	Shut down your computer
	Sign up to IBM Security Access Manager for Enterprise Single Sign-On
	Switch users in the desktop
	Unlock your computer
	Go to Windows GINA to log on
	Go to Windows GINA to unlock
	Manage your Wallet

Table 2. Icons that are visible when a fingerprint reader is detected

Icon	Description
	Fingerprint reader is not ready
	Fingerprint reader is ready

Chapter 2. AccessAgent

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

Signing up using your password (Active Directory sync)

When you sign up, be sure to have an enterprise identity or a user name that is assigned to you by your organization. Your enterprise identity can be your email address, your Active Directory user name, or SAP user name, or any other enterprise directory user name. IBM Security Access Manager for Enterprise Single Sign-On takes your enterprise identity and uses it to label your Wallet.

Procedure

1. In the AccessAgent navigation panel, click **Sign up**.
2. Enter your enterprise directory user name and password.
3. Click **Next**.
4. Optional: If user defined secrets are enabled, you are prompted to select a question and enter the answer.

   If you forget your password, use your primary secret to retrieve your Wallet contents.

   Important: Do not forget your primary secret answer.
   - It is case-sensitive.
   - It can be used to recover your application credentials stored in the Wallet:
     - If you forget your ISAM ESSO password or
     - If your ISAM ESSO password is out-of-sync from your Active Directory (domain) password. This scenario is only applicable if Active Directory password synchronization is enabled where the ISAM ESSO password is expected to match the Active Directory password.

   Note: You can use all the characters in the ISO Latin-1 character set in creating or resetting secrets, except for the following characters:
   - µ
   - ß
5. Click **Next**.
6. If prompted again, select another question and enter the answer.
   - Select **Hide** if you do not want to show your answer.
   - Select **Register more questions** for more secrets.

Signing up using your password (non-Active Directory sync)

Verify with your administrator if you are in an Active Directory synchronization deployment. If not, follow this procedure.

Procedure

1. In the AccessAgent navigation panel, click **Sign up**.
2. Enter your enterprise directory user name and password.

3. Click **Next**.
4. Enter a password for your Wallet.

   The new password must match the specified requirements.
5. Confirm your password by entering the new password again in the **Confirm password** field.
6. Click **Next**.
7. Optional: If secrets are enabled, you are prompted to select a question and enter the answer.

   If you forget your password, use your secret to retrieve your Wallet contents.

   Note: You can use all the characters in the ISO Latin-1 character set in creating or resetting secrets, except for the following characters:
   - µ
   - ß
8. Click **Next**.
9. If prompted again, select another question and enter the answer.
   - Select **Hide** if you do not want to show your answer.
   - Select **Register more questions** for more secrets.

Logging on using your password

Use your password to log on to AccessAgent.

Procedure

1. Turn on the computer.
2. Click **Log on** in the AccessAgent navigation panel.
3. Enter your enterprise directory user name and password.

Locking and unlocking your computer

If you are moving away from your computer, lock it using AccessAgent to prevent unauthorized access to your computer.

Locking your computer

To lock your computer, you can do one of the following tasks:

- Right-click on the **AccessAgent** icon. From the menu, select **Lock this computer**.
- Press **Ctrl+Alt+Del** on your keyboard and click **Lock computer**.
- Double-click the **AccessAgent** icon. When the Session information window is displayed, click **Lock this computer**.

Unlocking your computer

To unlock your computer:

1. Click **Unlock this computer** in the navigation panel.
2. Enter your user name and password.
3. Click **Next**.

Using other authentication factors

Aside from your password, you can use another authentication factor such as RFID, fingerprint, and smart card to ensure strong authentication for your organization.

Using RFID authentication

RFID devices have no internal power source. RFID devices transmit radio signals from the radio frequency signals they receive, and are only active when a reader is nearby to power them. The lack of an internal power source enables RFID devices to be small enough to be embedded into thin identification cards.

The combination of an RFID card and a password ensures a secure, two-factor authentication process.

For more information:

- "Signing up"
- "Unlocking your computer"

Signing up

You must initiate the sign-up process with your RFID card when you are using it as your second factor authentication method.

Before you begin

Before you sign up, make sure that:

- The RFID reader is attached to the USB port of your computer.
- Your RFID card is available.

Procedure

1. When you see the AccessAgent welcome screen, tap your RFID card on the reader.
2. Click **No** when AccessAgent asks if you already have an IBM Security Access Manager for Enterprise Single Sign-On user name and password.
3. Enter your enterprise directory user name and password.
4. Click **Next**.
5. If prompted, enter your new password. Otherwise, proceed to step 8.

   The new password must match the specified requirements.
6. Confirm your password by entering the new password again in the **Confirm password** field.
7. Click **Next**.
8. Select a question and enter the answer.

   The answer is your secret, which you use in case you forget your password.
9. Click **Next**.
10. Click **Finish**. If sign-up is successful, the **AccessAgent** icon is displayed in the notification area of **Windows Desktop**.

Unlocking your computer

You can unlock your computer by using your RFID card.

Before you begin

Make sure that you have a cached Wallet in the workstation that you are logging in using RFID. A *Wallet* holds the user credentials that are required for single sign-on.

Procedure

1. Tap your RFID card on the reader.

   Note: If you leave your computer locked in a specified time, you can unlock it by tapping your RFID card on its reader without entering your password. The time limit is set by your Administrator.
2. Enter your password.
3. Click **OK**.

Locking your computer

You can lock your computer by using your RFID card.

Procedure

- Right-click the **AccessAgent** icon in the system tray. Select **Lock this computer**.
- Double-click the **AccessAgent** icon. When the Session information window is displayed, click **Lock this computer**.
- Press **Ctrl+Alt+Del** on your keyboard and click **Lock computer**.

Using fingerprint authentication

The fingerprint identification system recognizes your fingerprint as an authentication factor. The fingerprint reader translates your fingerprint into encrypted codes, which logs you on to AccessAgent.

Signing up

Before you sign up, make sure that the fingerprint reader is attached to the USB port of your computer.

Procedure

1. From the AccessAgent welcome screen, place your finger on the fingerprint reader.
2. Click **No** when AccessAgent asks if you already have an IBM Security Access Manager for Enterprise Single Sign-On user name and password.
3. If prompted, enter your Windows user name and password. Otherwise, proceed to the next step.
4. Click **Next**.
5. Place your finger on the fingerprint reader.
6. Click **Finish**. If sign-up is successful, the **AccessAgent** icon in the notification area of the Windows Desktop is displayed.

Signing up more than one fingerprint

Depending on the deployment options of your organization, you can use more than one fingerprint under the same user name. Before you sign up another fingerprint, make sure that the fingerprint reader is attached to the USB port of your computer.

Procedure

1. Lock your computer.

   For more information about locking your computer, see "Locking and unlocking your computer."
2. Place the new finger on the fingerprint reader.
3. Enter your enterprise directory user name when prompted.
4. Click **Next**.
5. Click **Register Fingerprint**.
6. Enter your user name and password.
7. Click **OK**.
8. Select the finger to sign up from the diagram.
9. Click **Next**.
10. Scan your finger five or four more times, depending on the reader. After the finger is successfully scanned for five times, you can now use that finger to log on to AccessAgent.

Locking and unlocking your computer

Before you lock or unlock your computer, make sure that the fingerprint reader is attached to the USB port of your computer. Perform either of the following tasks in this procedure to lock or unlock your computer.

Procedure

- Lock your computer by placing your registered finger on the fingerprint reader.
- To unlock your computer with your fingerprint, scan your fingerprint on the fingerprint reader.

Using smart card authentication

A smart card is a pocket-sized card that has an embedded microprocessor. Smart cards can do cryptographic operations, store, and process the digital credentials of the users securely.

A smart card can be used as an authentication factor. IBM Security Access Manager for Enterprise Single Sign-On provides certificate-based strong authentication when users access their Credential Wallet by using smart cards.

For smart cards to work in IBM Security Access Manager for Enterprise Single Sign-On, they must have cryptographic credentials. Smart cards must also have the corresponding certificate that is issued by either a corporate PKI or a trusted external PKI.

Signing up

Insert your smart card in the reader to initiate the sign-up process.

Before you begin

Make sure that:

- The smart card reader is attached to your computer.
- Your smart card is available.

Procedure

1. From the AccessAgent welcome screen, insert your smart card in the smart card reader.

2. Enter your smart card PIN.
3. Click **OK**. A message to register the smart card is displayed.
4. Click **Next**.
5. Click **No** when AccessAgent asks if you have an IBM Security Access Manager for Enterprise Single Sign-On user name and password.
6. Enter your enterprise directory user name and password.
7. Click **Next**.
8. If prompted, enter your new password. Otherwise, proceed to 11.

   The new password must match the specified requirements.
9. Confirm your password by entering the new password again in the **Confirm password** field.
10. Click **Next**.
11. Select a secret question and enter the answer.

    The answer is your secret, which you use in case you forget your password.
12. Click **Next**.
13. Click **Finish**. If sign-up is successful, the **AccessAgent** icon in the notification area of the **Windows Desktop** is displayed.

Locking and unlocking your computer

To lock or unlock your computer, remove or insert your smart card.

Before you begin

Make sure that:

- The smart card reader is attached to your computer.
- Your smart card is available.

Procedure

Perform either of the following tasks in this procedure to lock or unlock your computer.

- To lock your computer, remove your smart card from the reader. The **AccessAgent lock** screen is displayed and the computer is locked.
- To unlock your computer, insert the smart card in the reader. When prompted, enter the smart card PIN, and click **OK**.

Using hybrid smart card authentication

A hybrid smart card must be dual-chip. It consists of an embedded PKI microprocessor and an RFID chip with contact and contactless interface.

Signing up

Insert your hybrid smart card in the reader to initiate the sign-up process.

Before you begin

Make sure that:

- The hybrid smart card reader is attached to your computer.
- Your hybrid smart card is available.

About this task

A grace period can be configured by your Administrator so that you can log on without providing a PIN. For more information, consult your Administrator.

Procedure

1. From the AccessAgent welcome screen, tap your hybrid smart card in the hybrid smart card reader.
2. Insert your hybrid smart card.
3. Enter your hybrid smart card PIN.

Results

AccessAgent creates a cached Wallet.

Locking and unlocking your computer

Remove or insert your hybrid smart card to lock or unlock your computer.

Before you begin

Make sure that:

- The hybrid smart card reader is attached to your computer.
- Your hybrid smart card is available.

Procedure

Perform either of the following tasks in this procedure to lock or unlock your computer.

- To lock your computer, remove your hybrid smart card from the reader. The **AccessAgent lock** screen is displayed and the computer is locked.
- To unlock your computer, tap the hybrid smart card in the reader.

Signing up with another RFID card or smart card

You can sign up for the second time for another RFID card or smart card if you lost them or if you want to have two authentication devices.

Before you begin

Contact the Help desk for an authorization code.

Procedure

1. Present or tap the device that you want to register.
2. Click **Register**. AccessAgent displays a dialog box and verifies whether you already have an IBM Security Access Manager for Enterprise Single Sign-On user name and password.
3. Click **Yes** to confirm.
4. Enter the authorization code from Help desk.
5. Optional: If prompted, enter your secret.
6. Click **Next**.
7. Enter your password.
8. Click **Finish**.

Managing Wallets

The Wallet Manager manages the passwords that are stored in your Wallet. Use it to configure the settings for the passwords that are based on your needs and personal preferences.

Viewing Wallet contents

These options are only available if you are logged on. Choose either of the following options to access your Wallet.

Procedure

- Right-click on the **AccessAgent** icon in the notification area, then select **Manage Wallet**.

  OR
- Access your Wallet by using the **Manage Wallet** link in the AccessAgent navigation panel.

Viewing passwords

You cannot show the password in the Wallet Manager if you are using smart card or fingerprint for second factor authentication.

Procedure

1. From your Wallet, click an entry.
2. Select **Actions** > **Show password**.

   You can also right-click on the entry and select **Show password**.
3. Enter your password. The password from the application that is selected in the Wallet is displayed.

Password entry options

Use the Password Entry options if you have multiple credentials for the same authentication service.

Table 3. Password entry options

Password entry options	Description
Automatic Logon	AccessAgent automatically enters the selected user name and password and logs you on to the application.
Always	AccessAgent automatically enters your user name and password. To log on to an application, press **Enter** on your keyboard or click **OK**.
Ask	AccessAgent prompts you to select the stored user name and password for the application before you log on. If you have more than one account that is stored, use this option to choose the credentials to use for logging on to the application.
Never	AccessAgent never uses the selected user name and password.

Exporting passwords stored in the Wallet

You cannot export passwords in the Wallet Manager if you are using smart card or fingerprint for second factor authentication.

Procedure

1. Select **File** > **Export passwords**.

   You can also click **Export passwords**.
2. Select the appropriate export password option.
3. Click **Browse** to specify the folder that contains the exported passwords.
4. Enter the file name and select the file type of the exported passwords.
5. Click **Save**.

Setting applications to remember passwords

After you enter an application user name and password for an application, AccessAgent prompts to store the user name and password for that application.

About this task

Select any of the following options in the procedure for your application passwords:

- Store the credentials in your Wallet.
- Not store the credentials in your Wallet, but intend to store them later.
- Never store the credentials in your Wallet.

Procedure

- Click **Yes** to store the user name and password in your Wallet.
- Click **No** if you do not want the user name and password to be stored yet.

  The next time you log on to the application, AccessAgent displays the same dialog box for confirmation.
- Click **Never** if you do not want your user name and password to be stored for this application.

  The next time you log on to the application, AccessAgent no longer displays the dialog box for confirmation.

Adding new credentials to authentication services

You can add new credentials to an authentication service in your Wallet.

Procedure

1. In the **Manage Wallet** window, click the authentication service from the list.
2. Click **Actions** > **New Credential**.
3. Enter the user name and password.
4. Click **OK**.

Searching for credentials in the Wallet Manager

Use the search box in the Wallet Manager to search for credentials.

Procedure

1. Use the **Credential Search** field to find credential details in the Wallet Manager.
2. Enter any of the following details:
   - Authentication service name
   - User name
   - Type

- Password entry

As you enter the credential in the field, entries that match the search item are highlighted on the list.

Deleting credentials from an authentication service

You can delete credentials from an authentication service in the Wallet.

Procedure

1. In the Wallet Manager, click the user name of an authentication service.
2. Delete the user through either of these options:
   - Click **Delete**.
   - Right-click on the entry and select **Delete Credential**.

   The entry is removed from the list of authentication services in your Wallet.

Editing passwords

You can modify the passwords of authentication services in your Wallet.

Procedure

1. In the **Manage Wallet** window, click the user name of an authentication service.
2. Click **Edit Password**, or right-click on the user name and select **Edit Password**.
3. Enter the new password.
4. Click **OK** to confirm the change.

Editing application settings

When there are two or more applications for the same authentication service in your Wallet, you can change the application settings.

Procedure

1. Click the authentication service.
2. Click **Application Settings**.

   You can also right-click on the entry and select **Edit application settings**.
3. In the **Password Entry** column, provide the necessary changes.
4. Click **Close** to confirm the changes.

Changing passwords

To ensure that the password is not compromised, your organization might schedule compulsory password changes. Your organization can also request users to change Wallet passwords after a specified duration.

Procedure

1. In the notification area, double-click the **AccessAgent** icon, or right-click on the **AccessAgent** icon and select **Change password** from the menu. The Session information window is displayed.
2. Click **Change password**.
3. Enter your **Old password**.
4. Enter your **New password**.

   The new password must match the specified requirements.
5. Enter the new password again in the **Confirm password** field.

6. Click **Next**.
7. Click **OK**. AccessAgent notifies you if the password change is successful.
8. Click **Close** to return to your desktop.

Resetting passwords without IMS Server connectivity

This procedure assumes you cannot connect to the IMS Server. In this scenario, you need both a request code and an authorization code to reset your password.

Procedure

1. In the AccessAgent navigation panel, click **Reset password**.
2. Enter your user name and click **Next**. AccessAgent displays a dialog box, indicating that there is no IMS Server connectivity. You must create a temporary password on the computer to continue to use AccessAgent.
3. Click **OK** to close the dialog box. AccessAgent displays a request code.
4. Copy the request code that is displayed on the window.
5. Contact Help desk for an authorization code.
6. Enter the authorization code.
7. Click **Next**.
8. Enter the new password.

   The new password must match the specified requirements.
9. Enter the new password again in the **Confirm password** field.
10. Click **Finish**.
11. Click **OK** to close the dialog box.

Resetting passwords with IMS Server connectivity

This procedure assumes that you are successfully connected to the IMS Server. In this scenario, you need an authorization code to reset your password. If a self-service password reset is enabled, users can also reset their passwords without calling Help desk by answering two or more secret questions.

Procedure

1. In the AccessAgent navigation panel, click **Reset password**.
2. Contact Help desk for an authorization code.
3. Enter the authorization code.
4. Click **Next**.
5. Enter the answer to the secret question.
6. Click **Next**.
7. Enter the new password.

   The new password must match the specified requirements.
8. Enter the new password again in the **Confirm password** field.
9. Click **Finish**.
10. Click **OK** to close the dialog box.

Setting self-service secrets in AccessAgent

You can specify more secret questions and secret answers.

Procedure

1. Double-click the **AccessAgent** icon in the system tray. The Session information window is displayed.
2. Select **Set self-service secrets**.
3. Select a new secret question from the list.
4. Enter the secret answer.
   - Mark **Hide** if you do not want the answer to be visible.
   - To register more questions, mark **Register more questions**.

   Note: You can use all the characters in the ISO Latin-1 character set in creating and resetting secrets, except for the following characters:
   - µ
   - ß
5. Click **Next**.
6. Select another secret question from the list and enter the corresponding secret answer.
7. Click **Next**.
   - If you chose to register more questions, select another secret question and enter the corresponding secret answer. Click **Finish**.
   - If you chose not to register more questions, the AccessAgent panel closes and your new secret is saved.

Bypassing strong authentication

You can temporarily log on to AccessAgent without your second factor authentication device such as a smart card, or RFID Card.

About this task

If there is an IMS Server connection and a self-service bypass is enabled, a user can bypass strong authentication by answering two or more secret questions.

If there is no IMS Server connection, contact your Help desk for an authorization code.

Your temporary access expires when you receive a new second factor authentication device, or when the temporary access validity period ends.

Procedure

1. Start the computer.
2. Click **Log on** from the AccessAgent navigation panel.
3. Enter your user name and password.
4. Answer your secret questions.
5. Optional: If there is no IMS Server connection, contact Help desk for an authorization code.

   Note: If you do not have Internet connectivity, a request code is displayed in the AccessAgent window. Provide the request code to the Help desk officer. The Help desk officer then provides an authorization code.
6. Optional: Enter the authorization code.
7. Click **Next**. You are now logged on to AccessAgent.

Chapter 3. AccessAssistant

AccessAssistant is the web-based interface through which users can retrieve their application passwords, do a password reset and manage their Wallet user credentials.

The following services are available in AccessAssistant:

- ISAM ESSO password reset
- Active Directory account and Wallet unlock
- Web single sign-on
- Application user account management
- Secret reset
- Optional two-factor authentication

Signing up to AccessAssistant

You can use AccessAssistant to log on to Web-based enterprise applications if you do not have AccessAgent installed. You can also use AccessAssistant to manage AccessProfiles if you do not have AccessStudio.

Procedure

1. Open your browser.
2. With AccessAssistant , choose one of the following options:
   - If you are not using a load balancer, access `https://<ims_hostname>:<ihs_ssl_port>/aawwp`.
   - If webserver is configured properly, access `https://<ims_hostname>/aawwp`. For example: `https://server1:443/aawwp`.
3. In the navigation panel, click **Sign up**.
4. Enter your Windows user name and password and click **Next**.
5. Select a secret question.

   Note:
   - The answer to this question must be at least three characters long.
   - Select **Hide answer** if you do not want the answers displayed.
6. Click **Finish**.

Logging on to AccessAssistant

You can log on to AccessAssistant with your ISAM ESSO password or Active Directory password if Active Directory password synchronization is enabled.

About this task

After log on, you can have full access to the AccessAssistant features and services. You can access your Wallet and your applications. You can manage AccessProfiles, your passwords, secrets and others.

Procedure

1. Open AccessAssistant. See "Signing up to AccessAssistant."

2. Enter your IBM Security Access Manager for Enterprise Single Sign-On user name and password.
3. Click **Next**.

Logging on with a second authentication factor

A second authentication factor might be required when you log on to AccessAssistant.

Procedure

1. Open AccessAssistant.
2. Enter your IBM Security Access Manager for Enterprise Single Sign-On user name and password. You are prompted to provide a second authentication factor.
3. Provide the authorization code that is issued by Help desk.
4. Click **Next**.

Resetting passwords

You can reset your ISAM ESSO password in AccessAssistant either by using secrets or an authorization code.

Procedure

- If self-service password reset is enabled:
  1. In the AccessAssistant navigation panel, click **Reset password**.
  2. Enter your IBM Security Access Manager for Enterprise Single Sign-On user name and click **Next**.
  3. Select a question from the **Question** list, enter the secret answer and click **Next**.

     Note: Answer all of the secret questions.
  4. Enter your new ISAM ESSO password.
  5. Enter the new password again to confirm and click **Next**.
- If self-service password reset is not enabled and secret is not required:
  1. In the AccessAssistant navigation panel, click **Reset password**.
  2. Enter your IBM Security Access Manager for Enterprise Single Sign-On user name and click **Next**.
  3. Enter the authorization code that is issued by the Help desk and click **Next**.

     Note: The authorization code is not case sensitive.
  4. Enter your new ISAM ESSO password.
  5. Enter the new password again to confirm.
  6. Click **Next**.
- If self-service password reset is not enabled and a secret is required:
  1. In the AccessAssistant navigation panel, click **Reset password**.
  2. Enter your IBM Security Access Manager for Enterprise Single Sign-On user name.
  3. Click **Next**.
  4. Enter the authorization code that is issued by the Help desk and click **Next**.

Note: The authorization code is not case sensitive.

5. Select the primary secret question from the **Question** list, enter the primary secret answer and click **Next**.

   Note: Primary secret is the first secret that you answer while signing up. This primary secret (answer) cannot be changed.
6. Enter your new ISAM ESSO password.
7. Enter the new password again to confirm and click **Next**.

Unlocking an Active Directory account

Use an authorization code and secret to unlock your Active Directory account and Wallet.

Before you begin

Contact Help desk to request for an authorization code.

Procedure

1. In the AccessAssistantnavigation panel, click the **Unlock account**.
2. Enter your IBM Security Access Manager for Enterprise Single Sign-On user name.
3. Select a domain.
4. Click **Next**.
5. Enter the authorization code.
6. Click **Next**.
7. Enter one secret answer.
8. Click **Next**.

Retrieving passwords

You can retrieve your application password in AccessAssistant either by displaying the application password on the browser or copying it from the clipboard.

Procedure

1. In the navigation panel, click **My Wallet**.
2. Optional: If you want view your application password from AccessAssistant
   1. Select **Display password on the browser**.
   2. Select the application for which you want to view the password and click **Get password**. The password is displayed.

   Click << to hide the displayed password.
3. Optional: If you want to copy your application password from AccessAssistant
   1. Select **Copy the password to the clipboard to paste it into the password field**.
   2. Click **Get password**. The password is copied to the clipboard, which you can paste into the target password field.

   Note: The password is copied and stored to the clipboard in a specified period. After which, you cannot copy and paste it anymore.

Managing your application account in the Wallet

In the AccessAssistant My Wallet, you can add or delete an application account. You can also update the password for a particular application account.

Procedure

- If you want to delete an application account from the Wallet
  1. Select the check box of the application to be deleted. You can delete one or more applications from the list by selecting the appropriate check boxes.
  2. Click **Delete**. You are prompted to confirm the delete action.
  3. Click **OK**. The selected application account is deleted from the list.
- If you want to add new account credentials for a particular application
  1. Click **Add**.
  2. Select for which application you want to add a new account credential.
  3. Specify your application user name.
  4. Specify and confirm your password.
  5. Click **Save**. The new account credential is displayed in the My Wallet list.
- If you want to edit the password for a particular application account
  1. Select the application which you want to update the password.
  2. Specify and confirm your new password.
  3. Click **Update**.

Resetting secrets

If you forgot your secret questions and answers, you can do a reset in AccessAssistant. You need secrets to do a self-service password reset.

About this task

Important: The primary secret cannot be reset. You must not forget your primary secret.

Procedure

1. In the navigation panel, click **Reset secrets**.
2. Select a new secret question from the list.
3. Enter the secret answer.

   Note:

   You can use all the characters in the ISO Latin-1 character set in creating and resetting secrets, except for the following characters:

   - µ
   - ß

   Select **Hide answer** if you do not want the answer to be visible.
4. Repeat steps 2 to 3 until you have registered three secrets.
5. Click **Reset**.

Notices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

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

Trademarks

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

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

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

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

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

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

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

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

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

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

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

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

Privacy Policy Considerations

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

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

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

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

Glossary

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

The following cross-references are used in this glossary:

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

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

A

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

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

account data item
The user credentials required for logon.

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

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

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

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

Active Directory credential
The Active Directory user name and password.

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

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

active RFID
See active radio frequency identification.

AD
See Active Directory.

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

API
See application programming interface.

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

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

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

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

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

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

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

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

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

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

B

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

base image
A template for a virtual desktop.

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

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

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

C

CA See certificate authority.

CAPI See cryptographic application programming interface.

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

CCOW
See Clinical Context Object Workgroup.

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

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

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

CLI See command-line interface.

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

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

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

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

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

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

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

CSN See Card Serial Number.

CSP See cryptographic service provider.

D

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

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

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

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

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

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

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

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

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

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

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

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

DLL See dynamic link library.

DN See distinguished name.

DNS See domain name server.

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

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

E

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

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

ESSO See enterprise single sign-on.

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

F

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

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

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

FIPS See Federal Information Processing Standard.

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

FQDN
See fully qualified domain name.

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

G

GINA See graphical identification and authentication.

GPO See group policy object.

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

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

H

HA See high availability.

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

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

hot key
A key sequence used to shift operations

between different applications or between different functions of an application.

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

I

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

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

J

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

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

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

JMX See Java Management Extensions.

JRE See Java runtime environment.

JVM See Java virtual machine.

K

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

L

LDAP See Lightweight Directory Access Protocol.

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

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

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

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

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

M

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

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

N

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

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

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

O

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

OTP See one-time password.

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

P

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

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

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

PIN See personal identification number.

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

PKCS See Public Key Cryptography Standards.

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

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

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

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

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

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

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

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

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

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

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

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

R

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

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

RDP See remote desktop protocol.

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

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

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

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

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

RFID See radio frequency identification.

root CA
See root certificate authority.

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

S

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

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

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

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

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

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

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

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

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

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

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

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

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

sign up
To request a resource.

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

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

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

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

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

SMTP See Simple Mail Transfer Protocol.

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

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

SPI See service provider interface.

SSL See Secure Sockets Layer.

SSL VPN
See Secure Sockets Layer virtual private network.

SSO See single sign-on.

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

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

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

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

STS See Security Token Service.

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

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

T

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

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

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

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

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

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

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

tty See terminal type.

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

U

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

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

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

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

V

VB See Visual Basic.

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

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

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

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

Virtual Member Manager (VMM)
A WebSphere Application Server component that provides applications with a secure facility to access basic

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

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

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

VMM See Virtual Member Manager.

VPN See virtual private network.

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