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

User Guide

SC23-9950-03

IBM® Security Access Manager for Enterprise Single Sign-On

Version 8.2

User Guide

SC23-9950-03

Note

Before using this information and the product it supports, read the information in “Notices” on page 31.

Edition notice

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

Contents

About this publication

The IBM® Security Access Manager for Enterprise Single Sign-On provides sign-on and sign-off automation, authentication management, and user tracking to provide a seamless path to strong digital identity. The *IBM Security Access Manager for Enterprise Single Sign-On User Guide* provides information about setting up and understanding the main functionalities of the product.

Intended audience

This publication is for new and experienced users of IBM Security Access Manager for Enterprise Single Sign-On AccessAgent, AccessAssistant, and Web Workplace.

This publication is for users who must perform the following tasks:

- Usage workflow setup
- Password and authentication setup
- Self-service tasks, such as resetting passwords and logging on using AccessAssistant

Readers must be familiar with the following topics:

- Installing and setting up authentication factors
- The workflow preferences of the organization (for example, for tasks such as sign-up, logon, logoff, and unlock workstations)

What this publication contains

This publication contains the following sections:

- Chapter 1, “Using IBM Security Access Manager for Enterprise Single Sign-On,” on page 1

  Provides step-by-step instructions for signing up with AccessAgent, logging on to AccessAgent, locking your computer, and unlocking your computer. The procedures depend on the type of desktop or workstation setup and additional authentication used.
- Chapter 2, “Using self-service features,” on page 15

  Describes some of the self-service functions in IBM Security Access Manager for Enterprise Single Sign-On, which are functions that can be managed by users with minimal assistance from an Administrator or Help desk officer.
- Chapter 3, “Using AccessAssistant,” on page 21

  Describes the different features of AccessAssistant and step-by-step instructions on how to use it.
- Chapter 4, “Using Web Workplace,” on page 25

  Provides step-by-step instructions on using Web Workplace and logging on successfully to Web-based applications from another computer.

Publications

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

IBM Security Access Manager for Enterprise Single Sign-On library

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

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

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

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

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

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

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

  This guide is intended for the Administrators. It covers the different Administrator tasks. This guide provides procedures for creating and assigning policy templates, editing policy values, generating logs and reports, and backing up the IMS Server and its database. Use this guide together with the IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide.
- *IBM Security Access Manager for Enterprise Single Sign-On Help Desk Guide*, SC23995303

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

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

  Read this guide if you have any issues with regards to installation, upgrade, and product usage. This guide covers the known issues and limitations of the product. It helps you determine the symptoms and workaround for the problem. It also provides information about fixes, knowledge bases, and support.

- *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide*, SC23995603

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

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

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

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

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

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

  This guide is intended for the end users. This guide provides instructions for using AccessAgent and Web Workplace.
- *IBM Security Access Manager for Enterprise Single Sign-On Error Message Reference Guide*, GC14762400

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

Accessing terminology online

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

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

Accessing publications online

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

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

Ordering publications

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

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

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

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

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

Accessibility

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

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

Tivoli technical training

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

Tivoli user groups

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

- 23,000+ members
- 144+ groups

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

Support information

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

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

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

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

Conventions used in this publication

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

Typeface conventions

This publication uses the following typeface conventions:

Bold

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

Italic

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

`Monospace`

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

Operating system-dependent variables and paths

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

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

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

Chapter 1. Using IBM Security Access Manager for Enterprise Single Sign-On

IBM Security Access Manager for Enterprise Single Sign-On is a fortified single sign-on that uses automation technology to augment security.

See the following topics for more information.

- "About single sign-on"
- "Overview on user tasks" on page 3
- "Supported desktop scenarios" on page 4
- "Signing up with other enterprise identities" on page 14
- "Using other authentication factors" on page 6

About single sign-on

You can enter one user ID and password to access multiple applications with single sign-on.

IBM Security Access Manager for Enterprise Single Sign-On is fortified because:

- The solution enhances security for enterprises by choosing from several authentication factors to provide two-factor authentication.
- Passwords for different applications can be strengthened by automating the periodic change of AccessAgent passwords. You can avoid leaking passwords through social engineering.

How single sign-on works

After logging in AccessAgent, it automatically captures and auto-fills your application credentials from and to the application clients that you launch.

Whenever an application is launched, AccessAgent monitors for single sign-on events and performs capture and auto-fill of logon credentials, which are saved in a *Wallet*.

When performing single sign-on into an application, AccessAgent retrieves the logon credentials from the wallet. This wallet is stored securely at the IBM Security Access Manager for Enterprise Single Sign-On server.

You can still access your wallet even when you use a different machine later. The wallet is also cached in encrypted form in your machine. Therefore, you can still enjoy single sign-on even if the server is offline. Access to the wallet is protected by a password and other authentication factors.

AccessAgent information

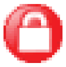
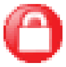
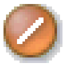
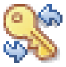
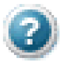
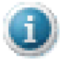
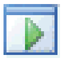
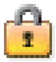
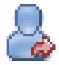
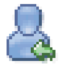
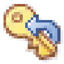
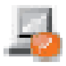
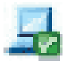
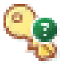
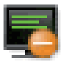
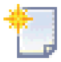
You can now view all components installed by AccessAgent and its corresponding version numbers. Do the following steps:

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

IBM Security Access Manager for Enterprise Single Sign-On icons

The following icons are used in IBM Security Access Manager for Enterprise Single Sign-On.

Visible when 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
	Session information
	Launch the application
	Lock your computer
	Log off fromAccessAgent
	Log on toAccessAgent
	Reset your password
	IMS Server connection is not available. For more information, see "About IMS Server connectivity" on page 3.
	IMS Server connection is available. For more information, see "About IMS Server connectivity" on page 3.
	Set your secrets
	Shut down your computer
	Sign up to IBM Security Access Manager for Enterprise Single Sign-On

Visible when user is logged on

Icon	Description
🔄	Switch users in the desktop
🔓	Unlock your computer
	Go to Windows GINA to log on
	Go to Windows GINA to unlock
	Manage your Wallet

Visible when fingerprint readers are detected

Icon	Description
	Fingerprint reader is not ready
	Fingerprint reader is ready

About IMS Server connectivity

This topic provides information about the AccessAgent and IMS Server connection.

If the IMS Server is offline or the connection between AccessAgent and the IMS Server is not available, you can still log on as long as you have a cached Wallet.

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

Overview on user tasks

After installing IBM Security Access Manager for Enterprise Single Sign-On, you can begin setting up the different ways to use the product.

What to do	Where to find information
Understand how IBM Security Access Manager for Enterprise Single Sign-On works.	Chapter 1, "Using IBM Security Access Manager for Enterprise Single Sign-On," on page 1
Know how to use self-service features.	Chapter 2, "Using self-service features," on page 15
Know how to use Web Workplace.	Chapter 4, "Using Web Workplace," on page 25
Know how to use AccessAssistant.	Chapter 3, "Using AccessAssistant," on page 21

Supported desktop scenarios

IBM Security Access Manager for Enterprise Single Sign-On works in different desktop scenarios.

- Personal workstation is owned and customized by one user only.
- Shared desktops have multiple users who share a generic Windows desktop.
- Private desktops have multiple users who have their own customized Microsoft Windows desktops in a workstation.

About your password

Your password secures access to your Wallet.

The length of the 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 directory password as your password.

Signing up with AccessAgent entails registering with the IMS Server and creating a Wallet. All application credentials are stored in your Wallet. Signing up ensures that your credentials are backed up on the server and are retrievable when needed.

You can associate your Wallet with a second authentication factor such as a smart card, an Active Proximity Badge, an RFID card, and other devices. The second authentication factor reinforces your password and protects the contents of your Wallet.

Use the following guidelines for specifying an ISAMESSO 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.

See the following topics for more information.

- "Signing up using your password (AD sync)"
- "Logging on using your password" on page 5

Signing up using your password (AD sync)

When you sign up, be sure to have an enterprise identity or a user name assigned to you by your organization. Your enterprise identity can be your e-mail 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 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
5. Click **Next**.
6. If prompted again, select another question and enter the answer.
   - Mark **Hide** if you do not want to show your answer.
   - Mark **Register more questions** for additional secrets.

Signing up using your password (non-AD 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.
   - Mark **Hide** if you do not want to show your answer.
   - Mark **Register more questions** for additional 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, perform the following steps:

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.

See the following topics for more information.

- "Using passive RFID authentication"
- "Using active RFID authentication" on page 8
- "Using fingerprint authentication" on page 9
- "Using smart card authentication" on page 11

Using passive RFID authentication

Passive RFID devices have no internal power source. Passive 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 passive RFID devices to be small enough to be embedded into thin identification cards.

An RFID card is an example of a passive RFID device. The combination of an RFID card and a password ensures a secure, two-factor authentication process. You can use an RFID card to access computers, doors, or elevators.

See the following topics for more information.

- "Signing up" on page 7
- "Unlocking your computer" on page 7

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 passive RFID reader is attached to the USB port of your computer.
- Your passive 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 lock and 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:
Procedure

- Right-click the **AccessAgent** icon located 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 active RFID authentication

An active RFID device has an internal power source that powers the integrated circuits and broadcast the radio signal to the reader. The active RFID device transmits at a higher power level than a passive device. The higher power level of transmission enables the device to broadcast at longer distances, and can be applied in various scenarios.

Active RFID devices are bigger and more expensive to produce. The Active Proximity Badge is an example of an active RFID device.

The Active Proximity Badge works when the badge is in a certain range from the reader. When you walk away from the reader, the computer locks. When your badge is in the range of the reader, the computer unlocks. This scenario is true given that no obstacles are blocking the area between your badge and the reader.

Your badge automatically switches off after nine hours of use. When the badge is switched off, the reader does not detect it. It must be switched on.

See the following topics for more information.
- "Signing up"
- "Unlocking your computer" on page 9

Signing up

When you are using an active RFID card or active proximity badge as your second authentication factor, use it to initiate the sign-up process.

Before you begin

Before you sign up, make sure that:
- The Active Proximity Badge reader is attached to the USB port of your computer.
- Your Active Proximity Badge card is available.

Procedure

1. Turn on and present your Active Proximity Badge to the reader. The AccessAgent window displays all the badges detected by the reader.
2. Click the ID number of the badge you want to sign up with.
3. Click **Register Badge**.

   Note: There might be several badges detected. Make sure that you select the one that you are authorized to register. The badge ID is printed on the back of your Active Proximity Badge.
4. Click **No** when AccessAgent asks if you already have an IBM Security Access Manager for Enterprise Single Sign-On user name and password.
5. Enter your enterprise directory user name and password.
6. Click **Next**.
7. Enter your new password.

   The new password must match the specified criteria.

If your password has not fulfilled all the criteria, it is not accepted.

8. Enter the new password in the **Confirm password** field.
9. Click **Next**.
10. Select a question.
11. Enter the answer.

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

Unlocking your computer

You can unlock your computer by using your Active Proximity Badge without a password in a specified time. Contact your Administrator for information about the duration. In this procedure, the Active Proximity Badge is used as the active RFID authentication factor.

Before you begin

Make sure that your badge is on.

Procedure

1. Move in the frequency range of the reader.
2. Select your user name from the list of available badges.
3. Enter your password.
4. Click **OK**.

Locking your computer:
Procedure

To lock your computer with active RFID, follow any of these steps:

- Move out of the frequency range of the reader.
- Turn off your badge.

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.

IBM Security Access Manager for Enterprise Single Sign-On 8.2 supports these biometric service provider and fingerprint readers:

- BIO-key Biometric Service Provider (BSP)
- DigitalPersona
- UPEK

BIO-key Biometric Service Provider (BSP) is a biometric middleware that enables IBM Security Access Manager for Enterprise Single Sign-On to work with any fingerprint reader that is already supported by BIO-key. See http://www.bio-key.com.

See the following topics for more information.

- "Signing up" on page 10
- "Signing up more than one fingerprint" on page 10
- "Locking and unlocking your computer" on page 10

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 has been 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 issued by either a corporate PKI or a trusted external PKI.

See the following topics for more information.

- “Signing up”
- “Locking and unlocking your computer”

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.

See the following topics for more information.

- “Signing up”
- “Locking and unlocking your computer”

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 another authentication device

You can sign up for the second time if you lost the first authentication device 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 you want to register.

   Example: If you are registering an Active Proximity Badge, select the Badge you want to register by clicking on the badge number.
2. Click **Register**. AccessAgent displays a dialog box and verifies if 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**.

Logging on using an OTP

You can log on to applications by using a one time password or OTP for authentication.

Procedure

1. Launch the application.
2. Enter the user name and password.
3. Press your OTP token.
4. Enter the OTP provided by the OTP token.
5. Optional: If you lost the OTP token, call the Help desk for an authorization code.
6. Optional: Enter the authorization code followed by a secret.

Logging on using an OTP and MAC

You can log on to applications by using both Mobile ActiveCode or MAC and a one-time password or OTP for authentication.

Procedure

1. Launch the application.
2. Enter a user name and password.
3. Enter the MAC received by mobile phone or e-mail, or the OTP provided by the OTP token.
4. Optional: If you lost both the mobile phone and the OTP token, call Help desk for an authorization code.
5. Optional: Enter the authorization code followed by a secret.

Signing up with other enterprise identities

Your organization might not use Active Directory as its enterprise identity. In this case, the IBM Security Access Manager for Enterprise Single Sign-On identity is bound to an enterprise application directory service, such as Tivoli Directory Server.

Your IBM Security Access Manager for Enterprise Single Sign-On user name and password are the same as your enterprise application user name and password. The sign-up sequence for other Enterprise IDs varies according to the deployment preference of your organization. Ensure that you follow the on-screen instructions.

Using applications in a terminal server

You can use AccessAgent when using applications in a terminal server if AccessAgent is installed on the terminal server.

If you are logged on to AccessAgent from a local computer, then AccessAgent on terminal server uses lightweight mode. This mode enhances performance by using a smaller memory footprint.

Chapter 2. Using self-service features

With these features, you can perform basic tasks, such as resetting passwords and secrets with minimal assistance from the Help desk or your Administrator.

Important: Log on using your password if you want to view, change, and export passwords.

See the following topics for more information.

- "Managing Wallets"
- "Changing passwords" on page 18
- "Resetting passwords without IMS Server connectivity" on page 18
- "Resetting passwords with IMS Server connectivity" on page 19
- "Setting self-service secrets in AccessAgent" on page 19
- "Bypassing strong authentication" on page 19

Managing Wallets

The Wallet Manager manages the passwords stored in your Wallet. Use it to configure the settings for the passwords 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 selected in the Wallet is displayed.

Password entry options

The Password Entry column consists of a drop-down menu with the options to apply to a password. These options are useful if you have multiple credentials for the same authentication service. See this table for more information.

Table 1. 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 asks you to select the stored user name and password for the application before logging on. If you have more than one account 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 the **Export passwords** button.
2. Mark 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 entering an application user name and password for an application, AccessAgent prompts you 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 at a later date.
- 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

When searching for credentials, use the search box in the Wallet Manager.

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 Manage Wallet window, click the user name of an authentication service.
2. Delete the user by performing either of the following steps:
   - 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

You can change the application settings for an authentication service.

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 passwords for the Wallet based on a specified duration.

Procedure

1. In the notification area, double-click on 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.
3. 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.
4. Click **OK** to close the dialog box. AccessAgent displays a request code.
5. Copy the request code displayed on the window.
6. Contact Help desk for an authorization code.
7. Enter the authorization code.
8. Click **Next**.
9. Enter the answer to the secret question.
10. Click **Next**.
11. Enter the new password.

    The new password must match the specified requirements.
12. Enter the new password again in the **Confirm password** field.
13. Click **Finish**.
14. 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 additional 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 drop-down 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 drop-down 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, RFID Card, or Active Proximity Badge.

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. Turn on the computer.
2. Press **Ctrl+Alt+Del** to log on, or 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. Using AccessAssistant

AccessAssistant is a Web-based interface that provides password self-help.

- With the Web automatic sign-on feature, you can log on to enterprise Web applications by clicking on the links from AccessAssistant, Web Workplace, or enterprise portals. Use the IBM Security Access Manager for Enterprise Single Sign-On password to log on to all applications.
- To use AccessAssistant, you must log on with the IBM Security Access Manager for Enterprise Single Sign-On Password. If the password is set up to synchronize with the Windows password, you can also use your Windows password to log on.
- Use AccessAssistant to obtain the latest credentials to log on to applications.

When logged on, you can also use the following features of AccessAssistant:

- Web automatic sign-on
- User sign-up
- Application credential management (only applications that have AccessProfiles for Web automatic sign-on are listed)
- Secret reset
- Password reset
- User profile modification
- Optional two-factor authentication
- Synchronization of Wallets, AccessProfiles, and policies

See the following topics for more information.

- "Signing up to AccessAssistant"
- "Logging on to AccessAssistant" on page 22
- "Managing applications in AccessAssistant" on page 22
- "Retrieving passwords" on page 24
- "Resetting secrets" on page 23
- "Resetting passwords" on page 23

Signing up to AccessAssistant

Use AccessAssistant to retrieve passwords if AccessAgent cannot be used. AccessAssistant lets you access enterprise applications through SSL VPN from home computers or Internet cafes. AccessAssistant can also automatically log on to Web-based enterprise applications.

Procedure

1. Navigate to AccessAssistant.
   - If you are using a load balancer, access *https://<loadbalancer_hostname>:<ihs_ssl_port>/aawwp*.
   - If you are not using a load balancer, access *https://<ims_hostname>:<ihs_ssl_port>/aawwp*.

   For example: *http://server1:80/aawwp*.

   Note: For more information, check with your administrator.

2. In the AccessAssistant left navigation panel, click **Sign up**.
3. Enter your Windows user name and password which you normally use to log on to your computer every day up to this point.
4. Click **Next**.

   If you do not want the answers displayed, mark **Hide answer**.
5. Select a secret question.

   The answer to this question must be at least three characters long.
6. Click **Finish**.

Logging on to AccessAssistant

When you are logged on, you have full access to all the application user names and passwords stored in your Wallet.

Procedure

1. In the AccessAssistant left navigation panel, click **Log on**.
2. Enter your IBM Security Access Manager for Enterprise Single Sign-On user name and password.
3. Click **Next**. You now have access to AccessAssistant features.

Logging in using two-factor authentication

You can log on to AccessAssistant by using two-factor authentication.

Procedure

1. Launch AccessAssistant and log on.
2. If two-factor authentication is turned on, supply one of the following to log on, in addition to your IBM Security Access Manager for Enterprise Single Sign-On password:
   - Authorization code issued by Help desk.
   - Mobile ActiveCode, which can be sent to user through mobile phone or email.
   - One-time Password (OTP) provided by an OTP token. For example: VASCO Digipass.

Managing applications in AccessAssistant

When logged on, the enterprise and personal Web applications available for you are listed in the panel of the AccessAssistant page.

Click on the application name on the list. A new browser page opens with the requested application.

See the following topics for more information.
- "Adding accounts to applications"
- "Editing application passwords" on page 23
- "Deleting accounts from applications" on page 23

Adding accounts to applications

If the application to log on is not in your Wallet, it means that AccessAssistant has not captured your user name and password.

Procedure

1. Click **Add** in the Manage logon accounts page to add one or more user names for the application.
2. Select an application from the drop-down list.
3. Enter your user name and password.
4. Enter your password again to confirm.
5. Click **Save**.

Editing application passwords

You can change your application passwords in AccessAssistant.

Procedure

1. Click **Edit password** next to the corresponding user name in the **My Wallet** page.
2. In the **Edit password** window, enter the new password.
3. Enter the new password again to confirm.
4. Click **Save**.

Deleting accounts from applications

You can delete your application accounts that are not needed from your Wallet.

Procedure

1. Select the check box next to the corresponding application.
2. Click **Delete**.

Resetting secrets

AccessAssistant offers a host of self-service capabilities to the users, such as the ability to reset their secret questions and answers. You can reset passwords by providing a subset of previously specified secret questions.

Procedure

1. In the AccessAssistant left navigation panel, click **Reset secrets**.
2. Select a new secret question from the drop-down 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

   Mark **Hide answer** if you do not want the answer to be visible.
4. You can specify an optional second secret question and secret answer.
5. Click **Reset**.

Resetting passwords

You must provide the correct answer to the verification question before you can reset the password in AccessAssistant.

Procedure

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. Select a question from the **Question** drop-down list.
5. Enter the secret answer.
6. Click **Next**.
7. Enter your new IBM Security Access Manager for Enterprise Single Sign-On password.

   The new password must meet the requirements listed on the right panel.
8. Enter the new password again to confirm.
9. Click **Next**.

Retrieving passwords

You can select an option on how you can retrieve your passwords in AccessAssistant.

About this task

The two password retrieval options are:

- Display the password on the browser
- Copy the password to the clipboard and paste it in the **Password** field.

Procedure

1. Select a password retrieval option.
2. Select the application check box.
3. Click **Get password**. If you select **Display password on the browser**, the password displays in the monitor. Make sure that you have some privacy before displaying the password.

Chapter 4. Using Web Workplace

You can perform AccessAgent tasks from a Web browser by using Web Workplace. It is an automatic sign-on feature without installing AccessAgent on your computer.

You must remember one password to log on to all applications. Combined with the reverse proxy feature, Web automatic sign-on can support a large variety of Web applications.

Web Workplace authenticates the password. If the password is set up to synchronize with the Windows password, users can use their Windows password to log on.

See the following topics for more information.
- "Signing up to Web Workplace"
- "Logging on to Web Workplace"
- "Managing applications in Web Workplace" on page 26
- "Resetting secrets" on page 28
- "Resetting passwords with authorization codes" on page 28
- "Unlocking an Active Directory account" on page 29

Signing up to Web Workplace

Web Workplace is especially useful when you cannot install AccessAgent. For example, there are users who must access enterprise applications through Secure Sockets Layer virtual private network from home computers or Internet cafes. Web Workplace can automatically log the user on to Web-based enterprise applications.

Procedure

1. Navigate to `https://<imsserver_url>/aawwp?isWwp=true`.

   Note: For more information, check with your administrator.
2. In the Web Workplace navigation panel, click **Sign up**.
3. Enter your Windows user name and password.
4. Click **Next**.
5. Select a question.

   The answer to this question must be at least three characters long.

   Note: Mark **Hide answer** if you do not want the answers displayed.
6. Click **Finish**.

Logging on to Web Workplace

After logging on, you have full access to all the application user names and passwords stored in your Wallet. When logged on, you can also use all the features of Web Workplace.

Procedure

1. In the Web Workplace navigation panel, click **Log on**.
2. Enter your IBM Security Access Manager for Enterprise Single Sign-On user name and password.
3. Click **Next**.

Logging on using OTP or MAC

You can log on using an OTP or MAC if AccessAssistant or Web Workplace is enabled for both OTP and MAC authentication.

Procedure

1. Launch AccessAssistant or Web Workplace.
2. Enter your IBM Security Access Manager for Enterprise Single Sign-On user name and password.
3. Enter the MAC received by mobile phone or email, or enter the OTP provided by the OTP token.
4. Optional: If you lost both the mobile phone and OTP token, call Help desk for an authorization code.
5. Optional: Enter the authorization code to log on.

Managing applications in Web Workplace

Managing Web Workplace applications include adding, editing, and deleting application accounts. It also includes setting the application logon preferences and default application account.

See the following topics for more information.

- "Logging on to applications"
- "Capturing user names and passwords"
- "Setting application logon preferences" on page 27
- "Adding accounts to applications" on page 27
- "Editing application passwords" on page 27
- "Deleting accounts from applications" on page 28

Logging on to applications

When you are logged on to Web Workplace, all the enterprise and personal Web applications are listed in the right panel of the Web Workplace page.

Procedure

Click the application name. A new browser page opens with the requested application, and you are automatically signed on to the application.

Capturing user names and passwords

If the user name for automatic logon field is empty, it means that Web Workplace has not captured the user name and password for that application.

Procedure

1. Click the application name.
2. Enter your user name and password for the application.

3. Enter your password again to confirm.
4. Click **Save**.

Setting application logon preferences

You can set your logon preferences for an application. For example, you can set automatic logon to an application.

Procedure

1. Click **Manage** from the **My Web Workplace** screen panel to set your application logon preferences.

   If there is only one profile in the application, the **Automatic logon** check box is selected by default.If there are two or more applications, you can disable automatic logon for each application.

   Note: If there are multiple profiles for one application, you cannot clear the **Automatic logon** check box for the first profile set for automatic logon. However, you can select another profile and set it for automatic logon.
2. Click **Update**.

Setting the default application account

If you have two accounts for the same application, you can set Web Workplace to select the default application account for automatic logon.

Procedure

1. Select the check box of the account to be assigned as the default account.
2. Click **Update**.

Adding accounts to applications

You can add more accounts to applications in Web Workplace.

Procedure

1. In the **Manage logon accounts** page, click **Add user name** to add more than one user name for an application. The Add user account window is displayed.
2. Select an application from the list.
3. Enter the new user name.
4. Enter a password.
5. Enter the password again to confirm.
6. Click **Save**.

Editing application passwords

You can edit your application password in Web Workplace.

Procedure

1. In the Manage logon accounts page, click **Edit password** next to the user name. The Edit password window is displayed.
2. Enter the new password.
3. Enter the new password again to confirm.
4. Click **Update**.

Deleting accounts from applications

You can delete accounts from applications in Web Workplace.

Procedure

1. Select the check box next to the corresponding account.
2. Click **Delete**.
3. In the Manage logon accounts page, click **Delete** next to the user name.

Resetting secrets

You can reset your passwords by specifying answers to secret questions in Web Workplace.

Procedure

1. In the Web Workplace navigation panel, click **Reset my secrets**.
2. Select a new secret question from the drop-down list.
3. Enter the secret answer.

   If you do not want the answer to be visible, mark **Hide answer**.

   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
4. Specify an optional second secret question and answer.
5. Click **Reset** to save the new secret question and answer.

Resetting passwords with authorization codes

Contact the Help desk to request for an authorization code. The contact information is available on your Web Workplace page.

Procedure

1. In the **Web Workplace** 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 secret answer.
5. Provide the secret answers to the other secret questions.
6. Contact the Help desk to request for an authorization code.
7. Enter the authorization code.

   The authorization code is not case sensitive.
8. Click **Next**.
9. Enter a new password.
10. Enter the new password again.
11. Click **Next**.

Unlocking an Active Directory account

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

Procedure

1. Click the **Unlock account** link in Web Workplace.
2. Enter a user name.
3. Select a domain.
4. Click **Next**.
5. Contact Help desk to request for an authorization code.
6. Enter the authorization code.
7. Click **Next**.
8. Enter one secret answer.
9. Click **Next**.

Resetting OATH-based OTP tokens in AccessAssistant or Web Workplace

Use AccessAssistant or Web Workplace to reset OATH-based OTP tokens.

About this task

The OTP might be out-of-sync with the IMS Server because the A-Key uses OATH OTP, which is event-based. The OTP can be out-of-sync if the user presses the token button too many times without using the displayed OTP for authentication.

Procedure

1. Log on to AccessAssistant or Web Workplace.
2. Click the **Reset OTP token**.
3. Select the serial number of the token.
4. Generate three consecutive OTPs by using the token and enter each of them in the appropriate text boxes.
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 (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

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

Trademarks

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

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

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

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

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

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

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

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

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

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

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

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

Glossary

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

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

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

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

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

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

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

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

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

Account data item. The user credentials required for logon.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Desktop application. Application that runs in a desktop.

Desktop Manager. Manages concurrent user desktops on a single workstation

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ESSO credentials. The ISAM ESSO user name and password.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Nodes. A logical group of managed servers.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Shared workstation. A workstation shared among users.

Sign up. To request a resource.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Index

Printed in USA

SC23-9950-03