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

Planning and Deployment Guide

SC23-9952-03

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

Planning and Deployment Guide

SC23-9952-03

Note
Before using this information and the product it supports, read the information in "Notices" on page 147.

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

Figures

About this publication

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 Planning and Deployment Guide* provides an overview of the different deployment scenarios, procedures, and requirements, including descriptions of the different product components and features.

Intended audience

This publication is for Administrators assigned to deploy IBM Security Access Manager for Enterprise Single Sign-On in the organization.

Readers must be familiar with the following topics:

- Virtual appliance
- High availability and disaster recovery
- Authentication factors
- Citrix/Terminal Servers

What this publication contains

This publication contains the following sections:

- Chapter 1, “Product overview,” on page 1

  Describes an overview of the product components and what you mustprepare.
- Chapter 2, “Deployment requirements,” on page 13

  Describes the hardware, software, and network requirements you mustdeploy the product successfully.
- Chapter 3, “Planning for deployment,” on page 21

  Describes what you mustprepare and what you mustplan a deployment.
- Chapter 4, “Planning for high availability and disaster recovery,” on page 33

  Describes the plans for deploying in a high availability environment.
- Chapter 5, “Planning for performance,” on page 43

  Describes some tips for optimizing performance.
- Chapter 6, “Planning for security,” on page 47

  Describes the steps to secure a deployment.
- Chapter 7, “Planning for installation,” on page 51

  Describes an outline of installation steps for each scenario; stand-alone, virtual appliance; multitier network deployment.
- Chapter 8, “Planning for an upgrade,” on page 65

  Describes an outline of the steps to complete an upgrade.
- Chapter 9, “Planning for configuration,” on page 71

  Describes how to configure the deployment components.
- Chapter 10, “Planning for authentication factors,” on page 89

  Describes the authentication factors you can use for a custom single-sign on solution.

- Chapter 11, “Session management,” on page 117
  Describes how to manage sessions.
- Chapter 12, “AccessAgent on Citrix/Terminal Servers,” on page 123
  Describes how AccessAgent works in a Citrix/Terminal server.
- Chapter 13, “Logging, auditing, and reporting,” on page 135
  Describes the available audit and reporting features.
- Chapter 14, “Product maintenance,” on page 143
  Describes data backup, fix packs, and database maintenance.
- “Change password and reset password,” on page 145
  Describes the change password and reset password workflow.

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. Product overview

IBM Security Access Manager for Enterprise Single Sign-On delivers a simple, flexible, and complete identity and access management solution at the enterprise endpoints. This product automates access to corporate information, strengthens security, and enforces compliance at the enterprise endpoints.

To learn more about the product features and components, see the following topics:

Product components

Familiarize yourself with the components of IBM Security Access Manager for Enterprise Single Sign-On.

AccessAgent

AccessAgent is the client software configured to connect to the IMS Server. AccessAgent is deployed on the Windows desktop (*Client AccessAgent*). You can also deploy it on the Citrix/Terminal Server (*Server AccessAgent*).

AccessAgent performs these functions:

- Manages user identity.
- Authenticates the user with a combination of authentication factors. AccessAgent integrates with various strong authentication devices to authenticate the user.
- Automates single sign-on and sign-off into Windows and various applications.
- Manages multiple user sessions on the same workstation through its session management capabilities.
- Maintains audit logs of user activities on the IMS Server.
- Synchronizes AccessProfiles, Credential Wallet, and various policy settings with the IMS Server.

AccessAgent has a graphical interface where users can manage:

- Their application credentials stored in their Credential Wallet.
- Their own ISAM ESSO password and authentication factors.

AccessAgent can run on Windows only.

IMS Server

IMS Server is the central management server implemented as an application running on WebSphere Application Server and works with the IBM HTTP Server.

The IMS Server performs the following functions:

- Stores and manages user credentials, AccessProfiles, identity Wallets, policies, and audit logs.
- Provides a central point of secure access administration for an enterprise.
- Provides loss management of authentication tokens, certificate management, and audit management for the enterprise.
- Provides a Web-based interface for Administrators to manage users, second authentication factors, machine, and system policies.
- Integrates with enterprise directories through VMM and integrates with provisioning systems through a provisioning bridge.

AccessStudio

AccessStudio is the application used by Administrators for creating and maintaining AccessProfiles. AccessProfiles automates sign-on or sign-off and custom workflows. An AccessProfile contains a definition of the characteristics of the login and change password screens of an application. It contains instructions on handling automation for an application.

You can create standard or advanced AccessProfiles depending on the application complexity.

AccessStudio can run on Windows only.

See *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide* for more information about the AccessStudio related concepts.

WebSphere Application Server

The WebSphere Application Server is an application server that hosts the IMS Server.

IBM HTTP Server

The IBM HTTP Server is a web server that is configured to work with the application server.

Database Server

The IMS Server stores all its data, including audit logs from AccessAgent, in a relational database. The IMS Server database contains these classes of data:

- System data - includes AccessProfiles, system policies, user and machine policy templates, and other system configuration data. Expected data volume is not more than 10 MB.
- User data - includes application credentials and user policies. Expected data volume is approximately 200 KB per user.
- Machine data - includes any machine policies and information about deployed machines.
- Audit logs - events related to user and administrator activities are stored in the database. Client-server communication logs are also recorded in to the IMS Server database. Audit logs require no more than 7 GB per 1000 users for a log retention period of one year.

The IMS Server and the IMS Server database can share one physical computer. However, the preferred deployment model is to separate the functions on two physical or virtual servers.

AccessAdmin

AccessAdmin is the Web-based management console that Administrators and Helpdesk officers use for:

- Searching and administering users
- Managing user, machine, system, and application policies
- Searching and viewing logs

AccessAssistant

The Web-based interface that provides users with the following functions:

- Password self-help
- Password reset
- Wallet identity management

Web Workplace

The Web-based interface where users can single sign-on to their Web applications if there is no AccessAgent installed in client computers.

Users can single sign-on to web applications from any web browser running on any operating system, with credentials stored in the Wallet. Users can access Web Workplace either directly through the Web Workplace portal, or through the Enterprise portal.

Web Workplace can only single sign-on to a web application that has a Web Workplace AccessProfile defined for it. Web Workplace depends on the native JavaScript support of the browser to implement automatic logon to designated web applications. There is no need to install client-side applications or browser plug-ins on the client computer.

Web Workplace AccessProfiles are created from the Web Workplace Administrator web interface, and cannot be generated from AccessStudio.

The current version of Web Workplace can support single sign-on to simple web applications with regular HTML-based logon forms. Web Workplace does not support the following types of web applications:

- Applications that use basic authentication.
- Applications where the logon form is Flash-based, or uses Java applet or ActiveX.
- Applications that involve complex dynamic HTML/JavaScript.
- Applications with built-in mechanisms to prevent independent software vendor manipulation.

Users must click the Web Workplace link to launch and automatically log on to a web application. The user cannot single sign-on if the user visits the web application directly by typing the URL into the browser. Two-factor authentication is implemented with One-Time Password (OTP) and Mobile ActiveCode (MAC) as the second factors.

Tivoli Common Reporting

Tivoli Common Reporting is a reporting component that lets you create, customize, and manage reports.

See "Audit reports" on page 139 for information about the various reports that you can generate.

Enterprise Directory

Enterprise directory is a directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. IMS Server connects to the enterprise directory to verify user credentials during sign-up, change password and also during logon.

See "Configuring IMS Server to use the directory server" on page 72.

Distribution and packaging

The IMS Server, AccessAgent, and AccessStudio are in the form of Windows setup files. Familiarize yourself with the IBM Security Access Manager for Enterprise Single Sign-On packaging and distribution.

Product component installers are available in the following media:

- Installation DVDs
- Downloadable files from the IBM Support Site

  Note: You must provide the exact name of the product in the search criteria.
  - IBM Support & downloads
  - IBM Passport Advantage® website
  - IBM Extreme Leverage website

Important: Copy the installer to your local disk drive before running the installer.

Packages

IBM Security Access Manager for Enterprise Single Sign-On is available in two packages:

IBM Security Access Manager for Enterprise Single Sign-On Standard

This package includes the following features:

- Session Management for personal desktop
- Password self service through the login screen
- Centralized logging
- Customizable reporting
- AccessAdmin configuration
- Choice of virtual appliance deployment

IBM Security Access Manager for Enterprise Single Sign-On Suite

This package is a combination of the Standard package and the following features:

- Strong authentication
- Session management

- Context management
- User provisioning
- Customizable tracking, password self-service through AccessAssistant, remote access and single sign-on through Web Workplace, and integration with authentication devices from independent software vendors.

Features

Learn about the different IBM Security Access Manager for Enterprise Single Sign-On features that are available.

Single Sign-On with workflow automation

IBM Security Access Manager for Enterprise Single Sign-On provides single sign-on and workflow automation on shared and personal workstations.

You can automate user access to all corporate applications such as Web, desktop, generic computer terminals, and legacy applications by using policies and AccessProfiles. AccessStudio helps users to automate their logon and logoff workflow, through login and logoff scripts and AccessAgent plug-ins.

Users need to remember only one password. Users authenticate once, and IBM Security Access Manager for Enterprise Single Sign-On does the rest.

Strong authentication

Weak passwords and wrong management of passwords can compromise security. IBM Security Access Manager for Enterprise Single Sign-On provides strong authentication services to prevent unauthorized access to confidential corporate information and IT networks.

You can set user, machine, and system policies. You can configure IBM Security Access Manager for Enterprise Single Sign-On to enforce screen locks, graceful log offs, application logout, application shutdown, automatic termination of inactive sessions, and so on.

IBM Security Access Manager for Enterprise Single Sign-On integrates with existing authentication factors. IBM Security Access Manager for Enterprise Single Sign-On combines the use of primary authentication factors and second authentication factors. Primary authentication factors are user passwords and secrets. Second authentication factors are smart cards, RFID, Active RFID, fingerprint, and one-time passwords.

IBM Security Access Manager for Enterprise Single Sign-On:

- Provides open authentication devices interface to support a wide range of smart cards.
- Supports easy integration with serial ID card devices such as RFID badges.
- Provides BIO-key support to leverage a broader range of biometric devices.
- Supports the use of hybrid smart cards.

Secure session management

IBM Security Access Manager for Enterprise Single Sign-On provides session management on both the Windows workstation and on the Citrix/Terminal Server. AccessAgent provides personal, shared (kiosk), and private (kiosk with multiple sessions) desktop modes. Users can share workstations, and roam easily and securely from one workstation to another.

You can enforce inactivity timeout policies, or use session lock, unlock, logon, and logout scripts to secure the user session.

Auditing and reporting

IBM Security Access Manager for Enterprise Single Sign-On records audit events including user log on and log out of applications. All audit logs are stored in a central relational database. The logs provide the meta-information that can guide compliance and IT Administrators to a more detailed analysis.

As an Administrator, you can query event logs in AccessAdmin or use Tivoli Common Reporting to generate user-centric audit reports, and custom reports.

Critical AccessAgent errors or events are recorded in the Windows Application Event log.

Password reset

IBM Security Access Manager for Enterprise Single Sign-On provides a password reset functionality.

Users can reset their ISAM ESSO password from any workstation through a challenge-response process. During AccessAgent sign-up, the users provide a number of secrets (answers to challenge questions), which can be used later to do a self-service reset password. See “Change password and reset password,” on page 145.

Policy management

IBM Security Access Manager for Enterprise Single Sign-On uses policies to control the behavior of its components. There are user policies, system policies, and machines policies. You can configure these policies through AccessAdmin.

Integration with user provisioning technologies

IBM Security Access Manager for Enterprise Single Sign-On can be integrated with user provisioning technologies to provide end-to-end identity lifecycle management.

When provisioned, users can single sign-on to applications on shared and personal workstations by using only one password. There is no need to register each application user name and password because all user credentials are automatically provisioned.

IBM Security Access Manager for Enterprise Single Sign-On provides end-to-end identity and access management by integrating with the centralized identity management functions of IBM Tivoli Identity Manager.

Support for a virtual appliance deployment

The IMS Server can be easily installed and configured by using a virtual image that runs on a hypervisor. The virtual image contains a preinstalled WebSphere Application Server, IBM HTTP Server, Tivoli Common Reporting, and IMS Server. You need only to deploy, activate, and configure the virtual appliance. However, an external database is still required.

Note: Virtual appliance is designed to run on VMWare ESX/ESXi hypersivor only. Configuring it to run on other hypersivor and virtualization solutions is not supported.

Utilities

IBM Security Access Manager for Enterprise Single Sign-On provides the following utilities:

- An Export Import configuration tool

  Use this tool to automate the replication of the IMS Server configuration. You can easily export the IMS Server configuration details such as the IMS Server root certificate, data source, and enterprise directories. The Export Import configuration tool is useful if you want to:
  - Set up a high availability environment
  - Set up a disaster recovery environment
  - Reuse the IMS Server configuration from a Test environment to a Production environment or vice versa
  - Reuse the IMS Server configuration from a Proof-of-Concept to a Production environment or vice versa
  - Back up the IMS Server configuration for your current WebSphere Application Server Stand-alone or Network Deployment setup
- A diagnostic test page

  Use this page to check the enterprise directory connector.
- A code translation utility

  You can use this tool to query event codes and result codes and to view their corresponding descriptions.

Lightweight mode AccessAgent for Citrix/Terminal Server

AccessAgent installed on a Citrix/Terminal Server can run on lightweight mode. Running on lightweight mode can reduce the memory footprint of AccessAgent on a Citrix/Terminal Server and it can improve the single sign-on startup time.

Support for Federal Information Processing Standards and Internet Protocol Version 6 (IPv6)

IBM Security Access Manager for Enterprise Single Sign-On uses FIPS 140-2 compliant cryptographic algorithms by using FIPS-compliant security providers such as GSKit and IBMJCEFIPS. Client workstations running on Microsoft Windows XP must at least have Service Pack 3 applied for FIPS 140-2 compliance.

IBM Security Access Manager for Enterprise Single Sign-On supports Internet Protocol Version 6 (IPv6) for communication.

Accessibility features

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

IBM strives to provide products with usable access for everyone, regardless of age or ability.

IBM Security Access Manager for Enterprise Single Sign-On has the following accessibility features:

- There are keyboard shortcuts to use AccessAgent.

  See "AccessAgent keyboard shortcuts" in the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.
- There are text equivalent for information conveyed through an image.

  AccessAgent provides better visual feedback for fingerprint scans. There are equivalent text for the icons and images displayed.
- AccessAgent inherits the system settings for font, size, and color for all user interface. IBM Security Access Manager for Enterprise Single Sign-On also supports systems setting for high-contrast for all AccessAgent user interface.

  See "Changing the AccessAgent interface" in the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.
- There is an option to display animation in a non-animated presentation mode.

  See "Enabling animation effect for AccessAgent" in the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.
- AccessAgent uses standard Windows control.
- AccessAgent have proper text labels and tool tips.
- There is an option to adjust the response times on timed instructions.

  The countdown durations are configurable through policies which the user cannot directly change. However, when the user is prompted with a countdown, the user can always cancel the action which allows the user to extend the duration.
- Information displayed have no dependency on color.
- Accessible documentation

  The *IBM Security Access Manager for Enterprise Single Sign-On* Information Center, and its related publications, are accessibility-enabled. The accessibility features of the information center are described at *http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.iehsc.doc%2Fiehs34_accessibility.html*.

  You can also view the publications for IBM Security Access Manager for Enterprise Single Sign-On in Adobe Portable Document Format (PDF) using the Adobe Acrobat Reader.

Keyboard navigation

This product uses standard Microsoft Windows navigation keys. For example:

- To traverse to the next link, button, or topic, press Tab inside a frame page).
- To go to the next link, button or topic node from inside a frame (page), press Tab.
- To expand and collapse a tree node, press the Right and Left arrows.
- To move to the next topic node, press the Down arrow or Tab.
- To move to the previous topic node, press the Up arrow or Shift+Tab.

- To scroll all the way up or down, press Home or End.
- To go back, press Alt+Left arrow; to go forward press Alt+Right arrow.
- To go to the next frame, press Ctrl+Tab.
- To move to previous frame, press Shift+Ctrl+Tab.
- To print the current page or active frame, press Ctrl+P.

For a list of standard keyboard shortcuts in Microsoft Windows, see the Keyboard Assistance information from Microsoft at http://www.microsoft.com/enable/products/keyboard.aspx.

IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility:

Supported languages

IBM Security Access Manager for Enterprise Single Sign-On installers already include the language packs for the supported languages. Individual language packs are not provided.

You can use AccessAgent to provide single sign-on in applications of various languages. User interface labels, application credentials, policy descriptions, and values can be displayed in both English and non-English languages.

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

- Arabic
- Brazilian Portuguese
- Chinese - Simplified Chinese
- Chinese - Traditional Chinese
- Czech
- Danish
- Dutch - Netherlands
- English - United States
- Finnish
- French - France
- German - Germany
- Hebrew
- Hungarian
- Italian - Italy
- Japanese
- Korean
- Polish
- Russian
- Spanish - Spain

IBM Security Access Manager for Enterprise Single Sign-On provides bidirectional language support. Bidirectional language support includes display of languages which are written from right to left such as Arabic or Hebrew. When the user

installs the IMS Server, AccessAgent, and AccessStudio and selects a bidirectional language, the user interface is automatically aligned right to left.

Supported languages for virtual appliance

If you are using virtual appliance, the supported languages vary for each of the product installed in it. Use the following table for guidance on the supported languages.

Language	Activation screens	WebSphere Application Server	Tivoli Common Reporting	IMS Server
Arabic	No	No	No	Yes
Brazilian Portuguese	Yes	Yes	Yes	Yes
Chinese - Simplified Chinese	Yes	Yes	Yes	Yes
Chinese - Traditional Chinese	Yes	Yes	Yes	Yes
Czech	Yes	Yes	Yes	Yes
Danish	No	No	No	Yes
Dutch - Netherlands	No	No	No	Yes
English - United States	Yes	Yes	Yes	Yes
Finnish	No	No	No	Yes
French - France	Yes	Yes	Yes	Yes
German - Germany	Yes	Yes	Yes	Yes
Hebrew	No	No	No	Yes
Hungarian	Yes	Yes	No	Yes
Italian - Italy	Yes	Yes	Yes	Yes
Japanese	Yes	Yes	Yes	Yes
Korean	Yes	Yes	Yes	Yes
Polish	Yes	Yes	Yes	Yes
Russian	Yes	Yes	Yes	Yes
Spanish - Spain	Yes	Yes	No	Yes

Supported applications and profiles

The IMS Server installer carries a default set of AccessProfiles for a basic set of applications.

Supported applications

The AccessStudio wizard auto-generates single sign-on AccessProfiles for a broad range of applications, including:

- Windows applications
- Web applications accessed through the Microsoft Internet Explorer or Mozilla Firefox browser
- 32-bit and 64-bit mainframe applications
- TTY applications based on text-out technology such as Putty
- Visual Basic applications
- .Net applications
- Mainframe HLLAPI (login screen only)
- Applications with owner-drawn user interfaces (login screen only)
- 32-bit Java applications (login screen only)
- 32-bit Java applets (browser-based, login screen only)

These AccessProfiles can run on Windows 2008, Windows XP, Windows Vista, and Windows 7.

Bundled AccessProfiles

IBM Security Access Manager for Enterprise Single Sign-On 8.2 provides the following AccessProfiles for all supported languages:

AccessProfile	Type
Microsoft Windows Explorer	• Windows XP • Windows Vista • Windows 7 • Windows 2008
Microsoft Windows Logon (GINA)	
Microsoft Windows Remote Desktop Logon	
Microsoft Internet Explorer	
Mozilla Firefox	
Web Autolearn	• Microsoft Internet Explorer 7, 8, and 9 • Mozilla Firefox 3.5 and 3.6

Profiles available for download

AccessProfiles are released for a fixed set of logon workflow for third party applications. AccessProfiles are released for various languages and environments.

IBM Security Access Manager for Enterprise Single Sign-On 8.2 provides AccessProfiles in the IBM Support site.

AccessProfiles can be downloaded from the AccessProfiles Library at https://www-304.ibm.com/support/docview.wss?uid=swg21470500&wv=1.

Check the AccessProfiles release notes for the supported environment, workflow, and version. If the environment is not supported, you can customize the AccessProfile.

Note: IBM does not support customization or other modifications to an AccessProfile. If you experience a problem with a customized AccessProfile, IBM Support might require the problem to be demonstrated on the GA version of the AccessProfile.

Chapter 2. Deployment requirements

Familiarize yourself with what you must have and do to successfully deploy IBM Security Access Manager for Enterprise Single Sign-On.

See the following topics:

Hardware and software requirements

Verify the different requirements and compatible versions for each of the IBM Security Access Manager for Enterprise Single Sign-On components. You must have administrator privileges to install the required software.

Requirements for the IMS Server

Hardware requirements depend on usage. For the hardware requirements of software that is not listed in this section, see the documentation provided with that product.

Note: The IMS Server runs on the WebSphere Application Server on Windows server platform only. With, the IMS Server hardware requirements are already accommodated when you comply to the WebSphere Application Server hardware requirements.

Hardware requirements

Table 1. Hardware requirements for IMS Server

Software	Hardware
IBM DB2®	• 2 GB RAM • 20 GB disk space
IBM WebSphere Application Server Network Deployment	• 2 GHz processor • 8 GB disk space • 3 GB RAM
IBM HTTP Server	• 1 GB RAM • 1 GB disk space

Hardware requirements (virtualization)

Table 2. Hardware requirements for IMS Server (virtualization)

Software	Virtual hardware requirements (minimum)
• VMware ESX and ESXi 3.5 or 4.0	• 2 Virtual processors • 4 GB Virtual RAM

Supported operating systems

- Microsoft Windows Server 2003 (x86), Standard, Datacenter, and Enterprise Editions
- Microsoft Windows Server 2008 Service Pack 2 (x86 and x64), Standard, Datacenter, and Enterprise Editions
- Microsoft Windows Server 2008 R2 Service Pack 1 (x64) Standard, Datacenter, and Enterprise Editions

Supported software

Install and configure the following software to successfully install and run the IMS Server:

Note:

- Sample instructions and guidelines on installing the supported software are provided. For the detailed and up-to-date procedures, see the relevant product documentation.
- IBM WebSphere Application Server (Base and Network Deployment Edition) x86 works only with IBM HTTP Server x86 and vice versa.
- IBM WebSphere Application Server (Base and Network Deployment Edition) x64 works only with IBM HTTP Server x64 and vice versa.
- Do not combine x86 and x64 middleware versions. If you use a middleware for x64, use the x64 version of the other middleware and operating systems.

Table 3. Supported software

Middleware	Supported software	Supported version
Application server	IBM WebSphere Application Server (Base and Network Deployment Edition)	• 7.0 (x86 and x64) with the latest fix pack
Web server	IBM HTTP Server	• 7.0 (x86 and x64) with the latest fix pack
Database server	IBM DB2 (Workgroup and Enterprise Server Edition) with DB2 JDBC driver 4.0	• 9.5 (x86 and x64) • 9.7 (x86 and x64)
	Oracle database	• 10g R2 (x86 and x64) • 11g R1 (x86 and x64) • 11g R2 (x86 and x64)
	Microsoft SQL Server (Standard and Enterprise Editions) with SQL JDBC driver 3.0	• 2005 Service Pack 4 (x86 and x64) • 2008 Service Pack 2 (x86 and x64) • 2008 R2 (x86 and x64)
Directory server	Microsoft Windows Active Directory	• 2003 Service Pack 2 (x86) • 2008 Service Pack 2 (x86 and x64) • 2008 R2 Service Pack 1 (x64)
	IBM Tivoli Directory Server	• 6.2.0 (x86 and x64) • 6.3.0 (x86 and x64)
	LDAP compatible directory server	• 3.0
Reporting tool	IBM Tivoli Common Reporting	• 2.1 • 1.2

Required fix packs

Download the latest fix packs for the following products:

- For IBM DB2, go to www-01.ibm.com/support/docview.wss?uid=swg27007053

  Note: For Oracle or Microsoft SQL Server, download the latest service packs and patches from the product website.
- For IBM WebSphere Application Server v7.0 and related subcomponents, go to www-01.ibm.com/support/docview.wss?uid=swg27014463
  - IBM WebSphere Application Server v7.0
  - IBM HTTP Server v7.0
  - IBM HTTP Server v7.0 plug-in for WebSphere
  - IBM Update Installer v7.0

  Note: For WebSphere Application Server v7.0, use fix pack 17 or later.

Requirements for AccessAgent and AccessStudio

The following are the hardware, network, and software requirements for AccessAgent and AccessStudio. AccessAgent and AccessStudio works only on Windows platforms.

The following table list the hardware requirements for AccessAgent and AccessStudio:

Table 4. Hardware requirements for AccessAgent and AccessStudio

Platform	AccessAgent minimum requirements	AccessStudio minimum requirements
Windows XP memory	512 MB	512 MB
Windows Vista memory	1 GB	1 GB
Windows 7 memory	1 GB	1 GB
Hard disk space	200 MB	300 MB

Supported operating systems

Table 5. Supported operating systems

Platform	x86	x64
Microsoft Windows XP Professional	Service Pack 3	Service Pack 2
Microsoft Windows Vista	Service Pack 2	Service Pack 2
Microsoft Windows 7	Service Pack 1	Service Pack 1
Microsoft Windows Server 2003	Service Pack 2	Service Pack 2
Microsoft Windows Server 2008	Service Pack 2	Service Pack 1

Note:

- Use a 32-bit AccessAgent installer on a Windows 32-bit operating system. A 32-bit AccessAgent is not supported on a 64-bit Windows operating system.

- Use a 64-bit AccessAgent installer on a 64-bit Windows operating system.
- AccessAgent is not supported on Microsoft Windows XP, Windows Vista, and Windows 7 WOW64 mode.
- AccessAgent is not supported on Microsoft Windows 7 XP mode.
- A 32-bit AccessStudio can be installed on a 32-bit or 64-bit Windows operating system.

Supported software

Install the following components before you install AccessStudio 8.2:

- AccessAgent version 8.2
- Microsoft .NET Framework 2.0 for Windows XP Professional only
- Microsoft .NET Framework 2.0 Language Pack for Windows XP Professional only

  To support languages other than English, download the Microsoft .NET Framework 2.0 Redistributable Package (x86) Language Pack for translation of messages. Go to the Microsoft website at http://www.microsoft.com and search for ".NET Framework Version 2.0 Redistributable Language Pack".

The following are the supported software for virtualization:

- Citrix XenApp version 5.0 and 6.0
- Citrix ICA Client and Web plug-in version 12.*x*
- Microsoft App-V version 4.6 (x86 and x64)
- Microsoft Hyper-V Server

The AccessAgent installation automatically installs the following software:

- Microsoft C Runtime Library
- MSXML version 4.0 and 6.0

Supported web browsers

Table 6. Supported web browsers

Web browsers	Supported Versions
Microsoft Windows Internet Explorer	• 7.0 • 8.0 • 9.0
Mozilla Firefox	• 3.5 • 3.6

Requirements for IMS Configuration Utility, AccessAdmin, AccessAssistant, and Web Workplace

This section lists the supported web browsers for IMS Configuration Utility, AccessAdmin, AccessAssistant, and Web Workplace.

Supported web browsers

Table 7. Supported web browsers

Web browsers	Supported Versions
Microsoft Windows Internet Explorer	• 7.0 • 8.0 • 9.0
Mozilla Firefox	• 3.5 • 3.6

Requirements for authentication devices

This section lists the supported software for biometrics, smart cards, or RFIDs for authentication.

Table 8. Supported software for authentication devices

Category	Supported software	Supported version
Biometric	BIO-key Biometric Service Provider	• 1.9.*x* (x86) • 1.10.*x* (x86)
	UPEK BioAPI SDK	• 3.0 (x86) • 3.5 (x86)
	Digital Persona Gold Fingerprint Recognition Software	• 3.2 (x86)
Smart Card	Gemalto Classic Client	6.0 (x86)
	Gemalto Access Client	5.5 (x86)
	SafeSign Identity Client	3.0 (x86)
	Charismatics Smart Security Interface	4.8 (x86)
	Spanish DNIe	(x86)
Hybrid Smart Card	Gemalto Classic Client v6	
	Gemalto Prox-DU	
	OMNIKEY 5x21	
Passive RFID	RFIdeas pcProxAPI SDK	6.5 (x86) and (x64)
Active RFID	Ensure Tech ETSecure SDK	4.0 (x86)

Compatibility Matrix

The following matrix summarizes the version compatibility for the IBM Security Access Manager for Enterprise Single Sign-On components.

Table 9. Version compatibility for the IBM Security Access Manager for Enterprise Single Sign-On components

IMS Server version	AccessAgent version	AccessStudio version
8.2	8.2	8.2
8.2	8.1	8.1

Network requirements

Validate and verify the list of available default ports that might be used by each component in a deployment.

You must ensure that the following ports are available before using the product installation program. The following table lists the default port numbers used by different components.

For a custom deployment, remember that you can use a planning worksheet to record updates to any custom port numbers in your deployment.

Default port numbers	Used By
80	IBM HTTP Server (Web server port)
8008	IBM HTTP Server Administration port
443	IBM HTTP Server SSL port
9080	IBM WebSphere Application Server virtual host port number, in the JVM.
1433	Microsoft SQL Server
1521	Oracle
8880	SOAP port to IBM WebSphere Application Server Stand-alone Deployment
8879	SOAP port to IBM WebSphere Application Server Network Deployment
9043	IBM WebSphere Application Server Network Deployment administrative console secure port (https)
9060	IBM WebSphere Application Server Network Deployment administrative console non-secure port (http)
9443	IBM WebSphere Application Server Network Deployment SSL port
50000	IBM DB2 instance port
60010	IBM DB2 base port

For the complete list of ports used by WebSphere Application Server, see the WebSphere Application Server information center: http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp

For the complete list of ports used by your database vendor, check the vendor-provided documentation.

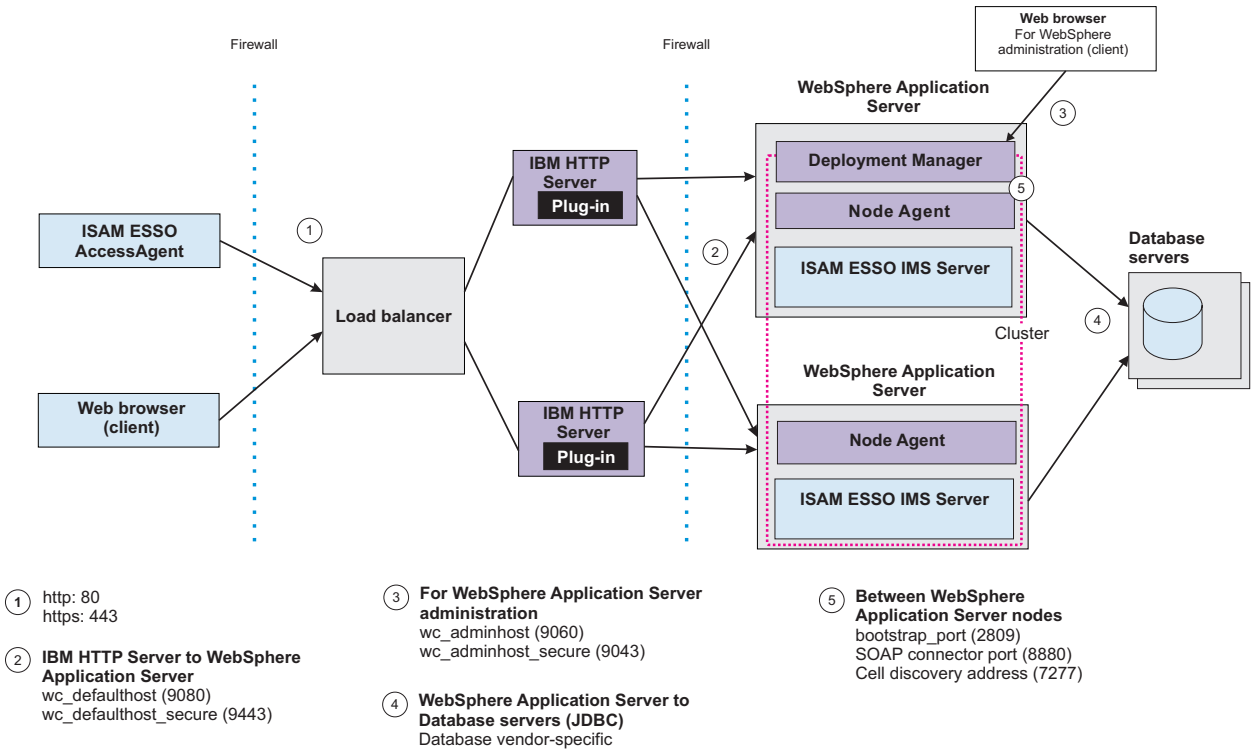

Figure 1. A sample of the typical HTTP and HTTPS SOAP port connections between the AccessAgent client and the IMS Server. Port numbers might vary for each deployment.

Implementation skills

To successfully develop and deploy IBM Security Access Manager for Enterprise Single Sign-On, you must know and have the required specialized skills.

The following are the required implementation skills:

Type	Description
General skills	• Operating system administration skills on Windows • Client/server application communication and scalability concepts • Methods for distributing Windows applications to large numbers of workstations
Directory and database skills	• Active Directory administration skills • Database installation and configuration skills • Database maintenance skills • LDAP-based user registry skills if Active Directory is not used

Type	Description
WebSphere Application Server skills	• Skilled in installing, configuring, and maintaining WebSphere Application Server in a high availability environment • Familiarity with the WebSphere Application Server documentation
IBM Security Access Manager for Enterprise Single Sign-On skills	• Understanding of IBM Security Access Manager for Enterprise Single Sign-On component architecture • Policy configuration • Profiling applications • Ability to troubleshoot IBM Security Access Manager for Enterprise Single Sign-On configuration issues

Chapter 3. Planning for deployment

There are several factors that affect the successful deployment of IBM Security Access Manager for Enterprise Single Sign-On. You must plan carefully. Know what you have, need and must do to successfully install or upgrade, or ensure the high availability and disaster recovery of IBM Security Access Manager for Enterprise Single Sign-On.

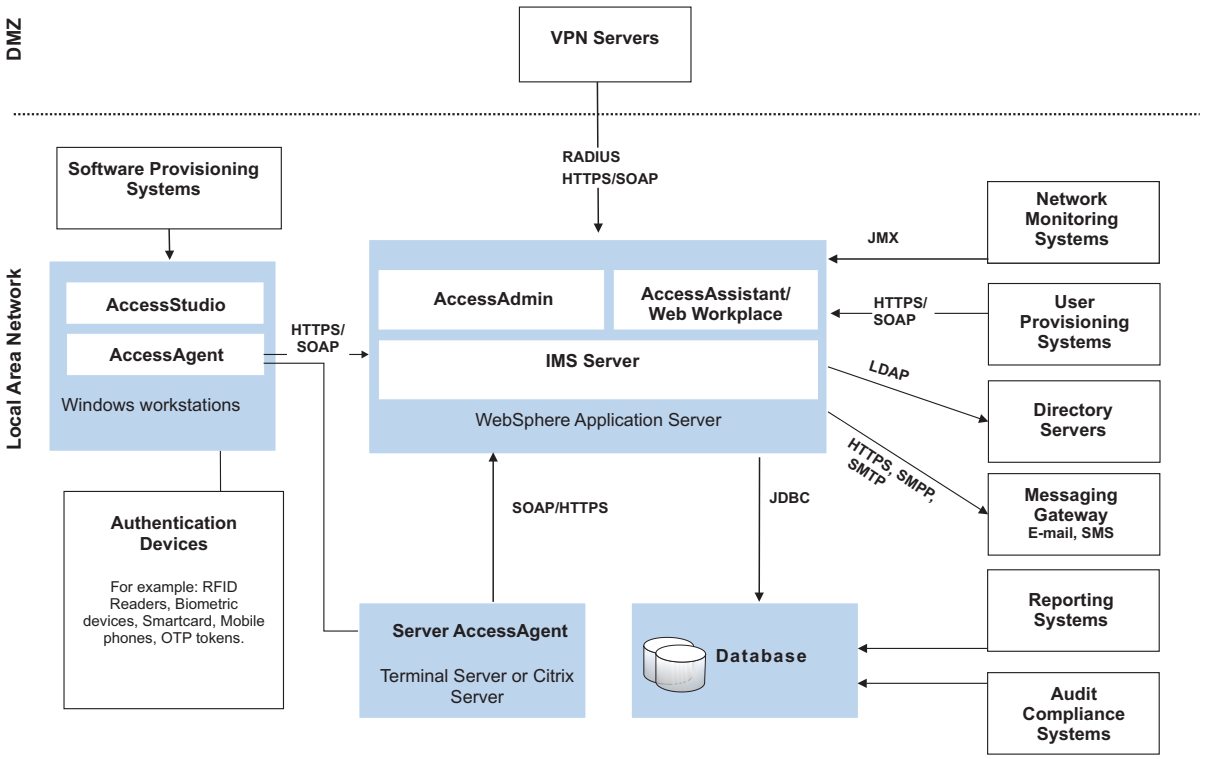

Figure 2. Overview of the IBM Security Access Manager for Enterprise Single Sign-On solution and integration with additional systems in an enterprise.

You can use the following guidelines on how to start planning for IBM Security Access Manager for Enterprise Single Sign-On deployment:

- "Deployment sizes"
- "Deployment phases" on page 22
- "Deployment tasks" on page 23
- "Product deployment overview" on page 24
- "Deployment considerations" on page 26

Deployment sizes

The deployment size determines the complexity and duration of the deployment. Medium to large-scale deployments require more time and resources compared to small scale deployments.

Factors

The number of users and applications to use single sign-on service determines the size of the deployment.

Number and types of users and desktops

The size of the deployment is directly proportional to the number of users and desktops. As the number of users increases, the more dependent the system is on proper server sizing and tuning. If the number of users increases then the network bandwidth consumption also increases.

Number and size of profiles

The number and complexity of the profiles to be created also affects the deployment time. Profiling complex applications can increase the overall time of deployment. Consider the number of applications that require advanced profiling techniques.

Small scale deployments

A small scale deployment typically consists of less than 10,000 users and less than 50 profiles.

You can have a single server machine hosting the IBM HTTP Server, WebSphere Application Server, and the database server hosting the IMS Server database.

Medium scale to large-scale deployments

A medium scale deployment typically consists of 10,000 to 50,000 users. A large-scale deployment typically consists of more than 50,000 users and requires more than 50 profiles.

You can use a multiple tier architecture with an IP load balancer or you can choose a a distributed IMS Server deployment.

Deployment phases

Deploy IBM Security Access Manager for Enterprise Single Sign-On in phases especially for medium-scale and large-scale deployments.

Test phase

During the test phase, the test team tests the software based on the documented procedures and reports any issues found, to the development team.

Pilot phase

The pilot phase involves deploying IBM Security Access Manager for Enterprise Single Sign-On to a relatively small number of users. The purpose of this phase is to discover and address any issues in the installation, configuration, and administration procedures.

In this phase:

- Target a selected number of users

  Focus on users that are representative of the types of users who are going to use AccessAgent. Consider the location, language, and job role of the user.

- Target a selected number of applications

  For deployments that have hundreds of applications to profile, it can take a long time. Prioritize those applications that have significant business impact or user acceptance. There is a higher chance to develop profiles correctly if there is focus on a selected number of applications.
- Enforce two-factor authentication for a selected number of users

Production phase

The production phase takes place after the pilot phase has proven that the IBM Security Access Manager for Enterprise Single Sign-On deployment to the selected users is stable.

In the production phase, IBM Security Access Manager for Enterprise Single Sign-On is deployed to the entire scope of users. The same procedures used in the pilot phase, is used in the production phase.

Deployment tasks

IBM Security Access Manager for Enterprise Single Sign-On deployment involves installation and configuration of the different product components, including administrative tasks.

Installation

Installation involves the following tasks:

- Installing the required middleware such as the WebSphere Application Server, the IBM HTTP Server, a database server, and a directory server
- Installing the IMS Server
- Installing AccessAgent on user workstations
- Installing AccessStudio to create AccessProfiles

See Chapter 7, “Planning for installation,” on page 51 for the different installation methods and options, including descriptions about the product component installation.

See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for the installation procedures.

Configuration

Configuration involves the following tasks:

- Provisioning the IMS Server Administrators
- Configuring the IMS Server to use the directory server
- Backing up and recovering the IMS Server
- Configuring the AccessAgent user interface
- Securing the deployment
- Securing user sessions
- Improving the IMS Server and the AccessAgent performance
- Configuring the Citrix/Terminal Server
- Configuring the IMS Server and the AccessAgent to support the different authentication factors

See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for the configuration procedures.

Administration

Administration involves the following tasks:

- Reviewing and updating AccessProfiles
- Managing users and roles
- Managing authentication factors
- Collecting logs and generating audit reports

See the *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide* for the procedures.

Product deployment overview

IBM Security Access Manager for Enterprise Single Sign-On deployment in an organization involves the installation and configuration of the different product components, policy configurations, and AccessProfiles.

Before you begin

There must be an enterprise directory that is existing and is operating.

Example deployment

Task	Reference Guide
Install the WebSphere Application Server on each IMS Server host running on the Windows Server.	• *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*
Install the Update Installer on each IMS Server host.	• *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*
Install and configure the IBM HTTP Server on each IMS Server host or on a separate tier of hosts.	• *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*
Install and apply the latest fix packs for the WebSphere Application Server and IBM HTTP Server.	
Install a database server instance on a designated database host if there is none.	• *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*
Create a Database Administrator.	• *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*
Create an Enterprise Directory *lookup user*. The *lookup user* is someone who authenticates himself 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 enterprise repository.	• *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*

Task	Reference Guide
Create an IMS Server database. This database serves as the central repository for all IBM Security Access Manager for Enterprise Single Sign-On system and user data.	• *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*
Run the IMS Server installer on either an existing or dedicated server to install the IMS Server applications – ISAMESSOIMS and ISAMESSOIMSConfig.	• *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*
Configure the IMS Server for initial use with the IMS Server Configuration Wizard. Configure the IMS Server data sources, certificate, URL, and enterprise directory.	• *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*
Use the Setup Assistant tool in the IMS Configuration Utility to provision the first IMS Administrator. **Note:** You can also configure the enterprise directory if you have not done it yet.	• *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*
Use the Setup Assistant tool in AccessAdmin to configure the default system, machine, and user policies. • Set up the system policies. • Set up the machine policies. • Set up the user policies and set the default user policy template. You can create multiple user policy templates for different groups of users. Make sure that the policy templates are assigned correctly.	• *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide* • *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide*
Deploy RFID, smart card, and biometric readers and software to employee client workstation, where appropriate.	• *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*
Pre-configure several AccessAgent parameters by modifying the `SetupHlp.ini` file found in the AccessAgent **Config** folder.	• *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*
Pre-provision users.	• *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*
Install AccessAgent on all employee client workstations and Citrix/Terminal Server that require single sign-on services. You can deploy AccessAgent through a Tivoli Provisioning Manager, an Active Directory Group Policy Object (AD GPO) or other push installation options for Windows.	• *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*
Install AccessStudio on an Administrator workstation to manage single sign-on profiles.	• *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*
Use AccessStudio to create and upload AccessProfiles for supported authentication services and applications through automatic logon or logoff.	• *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide*

Task	Reference Guide
(Optional) Create scripts. • Create a logon script to automatically launch applications when users log on to AccessAgent. Include the logon script in the policy template. • Create a logoff script to do clean up operations after users log off from AccessAgent. Include the logoff script in the policy template. • Create lock or unlock scripts to perform actions before users lock the screen or after users unlock the screen. Include the lock and unlock scripts in the policy template.	
(Optional) Install the Tivoli Common Reporting on some host.	• *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*
Import the IMS Server reports and configure Tivoli Common Reporting to point to the IMS Server database.	• *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide*
Let users log on either through AccessAgent or AccessAssistant.	• *IBM Security Access Manager for Enterprise Single Sign-On User Guide*

Deployment considerations

There are several factors that affect the successful deployment of IBM Security Access Manager for Enterprise Single Sign-On. This topic provides a list of what you need to consider when deployingIBM Security Access Manager for Enterprise Single Sign-On.

Installation package

IBM Security Access Manager for Enterprise Single Sign-On is available in Standard and Suite packages. The IBM Security Access Manager for Enterprise Single Sign-On features that the organization can use might vary depending on the package to be deployed.

Consideration:

- Before you proceed with the installation, determine whether to deploy a standard or suite package.

See “Distribution and packaging” on page 4 for information about the Standard and Suite packages.

Installation method

IBM Security Access Manager for Enterprise Single Sign-On is deployed by components. There are options on how to deploy each component. The IMS Server can be installed with interactive graphical mode or with virtual appliance. AccessAgent and AccessStudio can be installed with interactive graphical mode or silent mode.

Considerations:

- Determine which installation mode is applicable for the organization.
- Fingerprint authentication is not supported on a virtual appliance deployment.

See “Installation options” on page 54 for a comparison of the different installation options for the different product components:

High availability and disaster recovery

There are different ways to ensure IBM Security Access Manager for Enterprise Single Sign-On high availability and disaster recovery, from caching Wallets to using load balancers and clusters.

Considerations:

- Determine the high availability requirements.
- Collect information necessary to estimate hardware sizing for high availability:
  - peak hour traffic estimates
  - peak installation and user sign-up rates
  - database utilization
  - clustering requirements
  - load balancing architecture requirements
- Determine the preferred method to achieve high availability. Choices are:
  - Using load balancers and clusters
  - Using virtual appliance and the Export and Import configuration tools
  - Distributing the IMS Server
- Determine failover and recovery criteria.
- Determine backup and restore strategy.
- Set up DR environment in a separate site or location.

See Chapter 4, “Planning for high availability and disaster recovery,” on page 33 for the options to achieve high availability.

Performance tuning

You can configure IMS Server and AccessAgent to achieve better performance.

Considerations:

- Identify the potential performance problems and establish numeric values that categorize acceptable behavior.
- Identify the most active time when users tend to log on to AccessAgent.
- Estimate the number of users involved.
- Identify the synchronization interval.

Application server tier

IMS Server runs on a WebSphere Application Server.

Considerations:

- Determine whether to do a stand-alone or network deployment.
- For network deployment, determine the number of nodes and clusters.

You need at least two WebSphere Application Server nodes to achieve high availability. Add more nodes into the cluster to achieve scalability.

Web server tier

The web tier typically serves as the front end of the deployment. The web server manages incoming requests from the client computers or from a load balancer and distributes the requests to the application server.

Considerations:

- Determine the number of web servers to deploy.

  You need at least two web servers to achieve high availability. If you have more than one web server, you must use a load balancer.
- Determine whether to install the web server on the same computer where the application server is installed.

Directory server

IMS Server can be configured to use an existing or new directory server to identify and validate a user during sign-up.

Considerations:

- Determine whether to use an Active Directory or a generic LDAP. The combination of Active Directory and LDAP as directory servers is not supported.
- If Active Directory is used, determine whether:
  - To enable or disable Active Directory password synchronization. This feature is not available when using a generic LDAP.
  - To use multiple Active Directory domains. If you are using a generic LDAP, you cannot configure multiple LDAP domains.

  If LDAP is used or if Active Directory password synchronization is disabled, the Tivoli Identity Manager Active Directory Adapter is not required.
- Determine whether to provide self-service password reset through AccessAssistant.
- If Active Directory password synchronization and password reset through AccessAssistant are enabled, determine whether to use SSL connection. If there is no SSL connection, a Tivoli Identity Manager Active Directory Adapter is required.
- Distinguished names must be unique for a collection of users or groups over all directory servers. For example: If `uid=imsadmin,o=ibm` exists in *LDAP1*, it must not exist in *LDAP2*, and in *LDAP3*.
- Ensure that the LDAP short name is unique for a realm across registries. For example: `imsadmin`.
- Ensure that the base distinguished names for all registries used within a realm must not overlap. For example: If the *LDAP1* value is `c=us,o=ibm`, *LDAP2* must not be `o=ibm`.

See “Configuring IMS Server to use the directory server” on page 72 for more information about directory servers.

See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for configuring the directory server.

Database server

A database server is required to store AccessProfiles, user credentials, policies, and audit logs.

Considerations:

- Verify if the database server and its version are supported. See “Requirements for the IMS Server” on page 13. Database configuration settings vary depending on the selected database.
- Determine whether to install the database server on the same computer where the IMS Server is installed.
- Determine whether to implement database clustering and replication.
- Verify the network connection between the IMS Server and database server if they are in different workstations or servers.
- Determine the path of the database.
- Synchronize the system clocks if the IMS Server database and IMS Server are running on different computers.

See "Preparing the database server" in the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for the specific requirements for each supported database.

Session management

IBM Security Access Manager for Enterprise Single Sign-On can be deployed on personal workstations or shared workstations; in private desktops or user desktops; on Microsoft Remote desktops or on Citrix XenApp Servers. Furthermore, AccessAgent can run in lightweight mode on Microsoft Remote desktops or on Citrix XenApp Servers.

Considerations:

- Identify and understand the session management requirements
- Determine whether to deploy AccessAgent on personal or shared workstations.
- Determine whether to implement a shared desktop or a private desktop for the users.
- Determine whether to implement two-factor authentication and identify the authentication factor.
- Identify the corporate security policies
- Determine if the organization wants to deploy IBM Security Access Manager for Enterprise Single Sign-On on Microsoft Remote desktops or on Citrix XenApp Servers.
- Determine whether to set Server AccessAgent on standard mode or lightweight mode.
- Determine if the organization is using thin clients.
- Determine the required configuration such as whether to enable or disable Active Directory password synchronization, Network Provider, and others.

See Chapter 11, “Session management,” on page 117 for the different desktop modes, and for the implementation overview.

See Chapter 12, "AccessAgent on Citrix/Terminal Servers," on page 123 for deploying IBM Security Access Manager for Enterprise Single Sign-On on Microsoft Remote desktops or on Citrix XenApp Servers.

See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for configuring the Citrix/Terminal Server and lightweight mode.

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

Auditing and reporting

You can install Tivoli Common Reporting to generate the IBM Security Access Manager for Enterprise Single Sign-On audit reports. You can also modify the log level settings.

Considerations:

- Identify the auditing requirements.
- Define the custom audit logs to be generated.
- Configure the audit log events.
- Define the specific duration for which the audit logs are required.

See Chapter 13, "Logging, auditing, and reporting," on page 135 for the different logs and reports that can be queried or generated.

Application profiles

Single sign-on to applications within the organization is a core function of IBM Security Access Manager for Enterprise Single Sign-On. This core capability depends on successfully profiling the applications with AccessStudio.

Considerations:

- Identify the applications to be profiled including exact part numbers, version numbers, and patch levels.
- Determine whether the bundled profiles meet the application requirements.
- Determine the priority of the applications. Know the numbers of users for each application, as well as the business impact.
- Understand the behavior of the applications. Know the application logon and logoff process.
- Identify the error scenarios of the application.
- Determine and categorize the different types of applications are Web, Windows, mainframe, Java, or others.
- Determine the password policies for each application.
- Determine which application password change workflow is required.
- Determine if any applications share credentials.
- Determine the application credential fields. An application typically has username and password fields but some applications might have additional fields as part of a credential.
- Identify challenging applications.
- Identify applications with complex workflows or uses non-standard user interface libraries.

- Determine if the applications support different locales. Identify which locales are used by the users.
- Determine whether to create standard or advanced AccessProfiles.

Authentication

You can deploy IBM Security Access Manager for Enterprise Single Sign-On with two-factor authentication, and self-service password reset. You can also enable Active Directory password synchronization, ESSO GINA, and ESSO Credential Provider.

Considerations:

- Identify the authentication requirements.
- Identify the policy for new, change, and reset passwords.
- Determine whether to implement two-factor authentication and identify the authentication factor.
- Determine whether to enable the ESSO GINA.
- Identify the existing authentication factors.
- Determine whether IBM Security Access Manager for Enterprise Single Sign-On supports the existing authentication factors and their respective middleware.
- Ensure that the authentication devices and middleware are already installed, tested, and functioning before you deploy the product.
- Identify the password requirements.
- Determine whether to enable self-service.
- Be careful when formulating the series of question users must answer to reset their passwords. Issues of privacy and cultural sensitivity must be considered.
- Review the security questions with the Legal department to ensure that the questions are in compliance with local privacy laws.

See Chapter 10, “Planning for authentication factors,” on page 89 for information about the primary and second authentication factors.

Provisioning

You can provision users through a provisioning system.

Considerations:

- Determine whether to use a provisioning system such as Tivoli Identity Manager.
- Determine whether users can sign up for authentication and sign-on services through AccessAgent or AccessAssistant.
- Determine whether to provision users before the AccessAgent push-out installation.

See “Provisioning users” on page 81.

Security

Secure the IBM Security Access Manager for Enterprise Single Sign-On deployment and related components to mitigate against potential security risks.

Considerations:

- Identify the security policy of the organization.
- Determine the security hardening requirements.
- Identify the options for securing the Application tier.
- Identify the options for securing the Web-tier.
- Identify a secure location for the hardware or systems running the software.

See Chapter 6, “Planning for security,” on page 47.

Chapter 4. Planning for high availability and disaster recovery

Implementing high availability is about ensuring that services are always available. Disaster recovery is the process of restoring the IBM Security Access Manager for Enterprise Single Sign-On service to a production state in the event of an outage.

Scenarios when AccessAgent connects to the IMS Server

An AccessAgent connection to the IMS Server is required for each of the following events:

Post-installation

After AccessAgent is installed, AccessAgent connects to the IMS Server to download certificates, AccessProfiles, policies, and other system data.

Sign-ups

When new users sign-up to register new accounts, secrets and authentication factors.

Logons

When users log on, AccessAgent connects to the IMS Server to:

- Check if the account or the authentication factor has been revoked.
- Download or synchronize system and user data.
- Verify the authorization code for second factor bypass.

Unlocks

When the ESSO GINA is unlocked, AccessAgent connects to the IMS Server to:

- Check if the account or the authentication factor has been revoked.
- Download or synchronize system and user data.

Synchronization

AccessAgent periodically connects to the IMS Server to synchronize system, machine-specific, and user-specific data with the IMS Server. The configurable synchronization time interval is set to 30 minutes by default.

Single sign-on credential capture

When using single sign-on to submit a newly captured credential to the IMS Server.

Logging

When AccessAgent submits an event audit log to the IMS Server.

Password change

When changing the ISAM ESSO password.

When the server is not available

When the IMS Server is not available, the following functions are also not available:

- New user sign-up.

- Logon from workstation without cached Wallet.
- Logon with second factor bypass or second factor registration.
- Change of the ISAM E-SSO password.
- Upload and distribution of new and updated AccessProfiles.
- Access to AccessAdmin.
- Access to AccessAssistant and Web Workplace.

High availability

IBM Security Access Manager for Enterprise Single Sign-On supports high availability deployments.

- **Client-side high availability**
  - If the IMS Server is not available, AccessAgent can remain functional because AccessAgent caches system data into a machine Wallet and user data into individual user cached Wallets.
  - When the server is offline, AccessAgent can continue to authenticate users with one or two authentication factors by using the authentication data cached on the computer.
  - AccessAgent can provide single sign-on for the user when the server is offline by using the cached ESSO user Wallet.
  - If the user forgets the password or second authentication factor, IBM Security Access Manager for Enterprise Single Sign-On provides various ways for users to regain access to the user Wallet. For example, the user can reset the password through self-service secrets even if the IMS Server is offline.
- **Database high availability**

  IBM Security Access Manager for Enterprise Single Sign-On leverages on industry standard databases for additional storage. Enterprises can reuse the existing data-tier infrastructure for high availability, recovery, and maintenance.
- **Directory server high availability**
  - IBM Security Access Manager for Enterprise Single Sign-On does not store any data on the enterprise directory (IBM Security Access Manager for Enterprise Single Sign-On does not require any directory schema extensions) and does not connect to the directory server for most single sign-on scenarios.
  - IBM Security Access Manager for Enterprise Single Sign-On relies on the directory server to verify user identities during sign-up. If password synchronization is configured, IBM Security Access Manager for Enterprise Single Sign-On also connects to the directory server when performing password reset and password synchronization.
  - To ensure high availability, configure the virtual member manager component of the WebSphere Application Server to communicate to any Active Directory domain controller instead of a specific domain controller.

See the following topics:

- "Wallet caching" on page 35
- "IMS Server database high availability" on page 35
- "Virtual appliance replication for high availability" on page 36
- "Distributed servers or clusters in multiple locations" on page 37
- "Load balancing and clustering" on page 39
- "Disaster recovery" on page 40

Wallet caching

Each AccessAgent has a machine Wallet that caches data such as AccessProfiles, system policies, and machine policies. This machine Wallet is downloaded immediately after installation of AccessAgent.

AccessAgent can also cache the single sign-on data of the user into individual cached Wallets on each computer that the user logs on to. The cached Wallet contains user authentication data, and application credentials in the user single sign-on Wallet.

Since system and user data are cached, AccessAgent can still authenticate users and perform single sign-on even if it is not connected to the IMS Server.

The cached Wallets are encrypted and stored in *system_drive*:\Program Files\IBM\ISAM ESSO\AA\Cryptoboxes. The cached Wallets are encrypted files and are not accessible to non-Administrator users.

AccessAgent also caches single sign-on profiles, policies, the user Wallet, and generated audit logs on local storage in an encrypted form.

Both machine and user cached Wallets are periodically synchronized with the IMS Server.

When Wallet caching is useful

When a new credential is captured or an existing credential is updated, the following steps occur:

1. AccessAgent updates the locally cached Wallet and the IMS Server immediately.
2. If the IMS Server connection is not available, the captured credentials and audit log data are cached in the user Wallet. These data are submitted at a later time.

   When the IMS Server connection is restored, AccessAgent attempts to submit captured credentials and audit log data immediately to the IMS Server.

   By default, the periodic synchronization is set to every 30 minutes.
3. The next time the user logs on to the AccessAgent from another workstation, AccessAgent synchronizes with the IMS Server. The changes are then updated into the cached Wallet on that workstation.

IMS Server database high availability

IBM Security Access Manager for Enterprise Single Sign-On interfaces with corporate directories without changing the directory schema. There is no additional load or high availability requirements for existing directory services.IBM Security Access Manager for Enterprise Single Sign-On leverages on the existing high-availability features of the database products that it works with – IBM DB2, Microsoft SQL Server and Oracle.

The most popular method for database high availability is using the database clustering feature together with a compatible third-party high availability solution such as Microsoft Cluster Server (MSCS). A typical clustered configuration involves an active-passive pair of database nodes with access to a shared disk storage. Newer versions of database products provide alternative high availability solutions that do not require a shared disk storage to maintain an active-passive configuration. For example, Microsoft SQL Server 2005 Database Mirroring feature and DB2 HADR feature.

DB2 HADR feature may not necessarily support automatic failover in its basic configuration. Additional software components such as *SA-MP* for DB2 and additional configuration at the database and WebSphere Application Server are required to support automatic failover. For example, configuration of the JDBC connection string. You can create a WebSphere Application Server data source with the JNDI key of "jdbc/ims", and an associated J2C alias "imsauthdata" with the multi-node JDBC connection string during the initial IMS Server configuration.

IBM Security Access Manager for Enterprise Single Sign-On also support DB2 SQL replication feature. However, this feature is more appropriate for a distributed IMS Server setup.

Virtual appliance replication for high availability

Another way to achieve high availability is to use virtual appliance and the Export and Import configuration tool.

Use the Export and Import configuration tool to replicate IMS Server configurations among virtual appliances. You can deploy and activate two or more virtual appliances. After a virtual appliance is configured completely, you can export the configuration to another deployed virtual appliance.

Note: The virtual image does not have a preinstalled database server. However, an external database is still required and it needs to be separately configured for high availability.

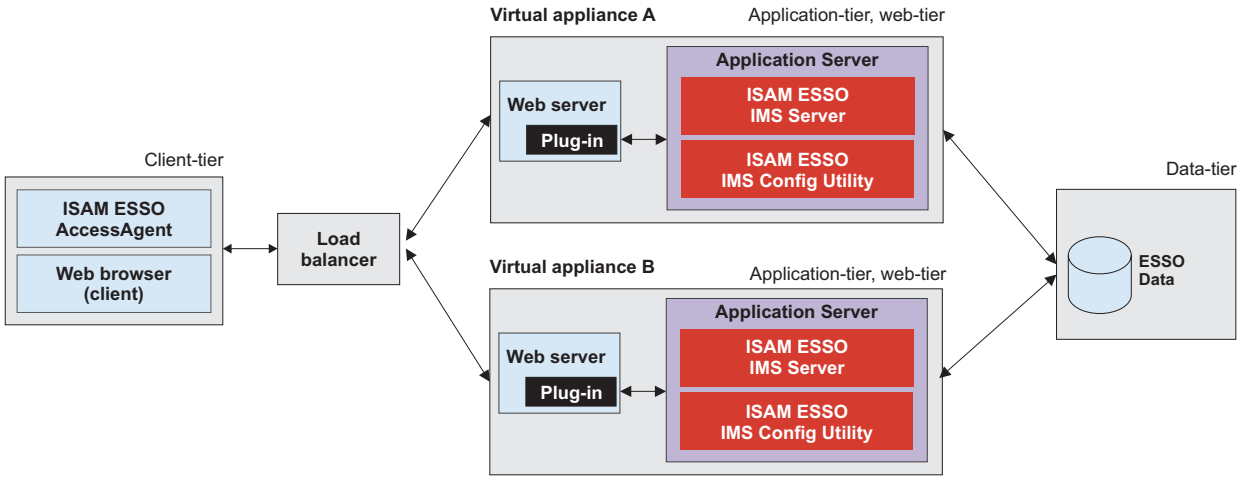

Figure 3. An example of two virtual appliance replicas that are configured the same way for high availability with a load balancer.

Considerations for virtual appliances in a high availability deployment:

- After making any server configuration changes, remember to synchronize changes between the replicas. Synchronize changes between the replicas by exporting and importing the configuration again.
- The overhead of synchronizing the IMS Server configuration increases as the number of replicas increase. See the WebSphere Application Server Network Deployment (clustered) approach for the management of multiple IMS Server nodes. See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for more details.

After the first virtual appliance node is configured, use the Export configuration tool to export the IMS Server configuration. Use the Import configuration tool to replicate the IMS Server configuration on the other virtual appliances. However, you must manually synchronize the IMS Server configurations.

See the following references:

- "Setting up a server with a virtual appliance" in the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*
- "Exporting the IMS configuration in the IMS Configuration Utility" in the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*
- "Importing the IMS configuration in the IMS Configuration Utility" in the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*

Distributed servers or clusters in multiple locations

Customers with users and offices in multiple geographical locations can deploy separate clusters of the IMS Server and database in geographically separated sites. This option distributes and localizes the traffic and load.

A distributed IMS Server setup consists of multiple sites. Each site has its set of IMS Servers and database instances. All IMS Servers at each site point to the corresponding IMS Server database servers at that site.

Deploying IMS Servers across multiple sites has the following benefits:

- It minimizes cross-site traffic. AccessAgents communicate locally or communicate with the nearest IMS Server for improved bandwidth and response time.
- Failure of any single IMS Server site has no impact on the users of other sites. Additional sites provide several backups.

How a geographically distributed or multi-site deployment works

A typical distributed IMS Server setup has one designated *main site*, and one or more *satellite sites*. Configure the IMS Server at the *satellite site* to be the same as the *main site*, except for the database connection parameters, enterprise directory, and messaging gateways.

You can configure each *satellite site* to replicate local changes bidirectionally with the *main site*. Changes made to system, machine, and user data at either the *main site* or *satellite site* is replicated to all sites. However, the audit logs can be replicated in a unidirectional flow from the IMS Server database at the satellite site to the IMS Server database at the master site.

Each IMS Server has different virtual IP numbers at each site. All instances of the IMS Server in a site share a common virtual IP number through a load balancer. Use the split-horizon DNS technique where the IMS Servers at all sites share the same DNS name. All AccessAgents are configured to point to this common DNS name.

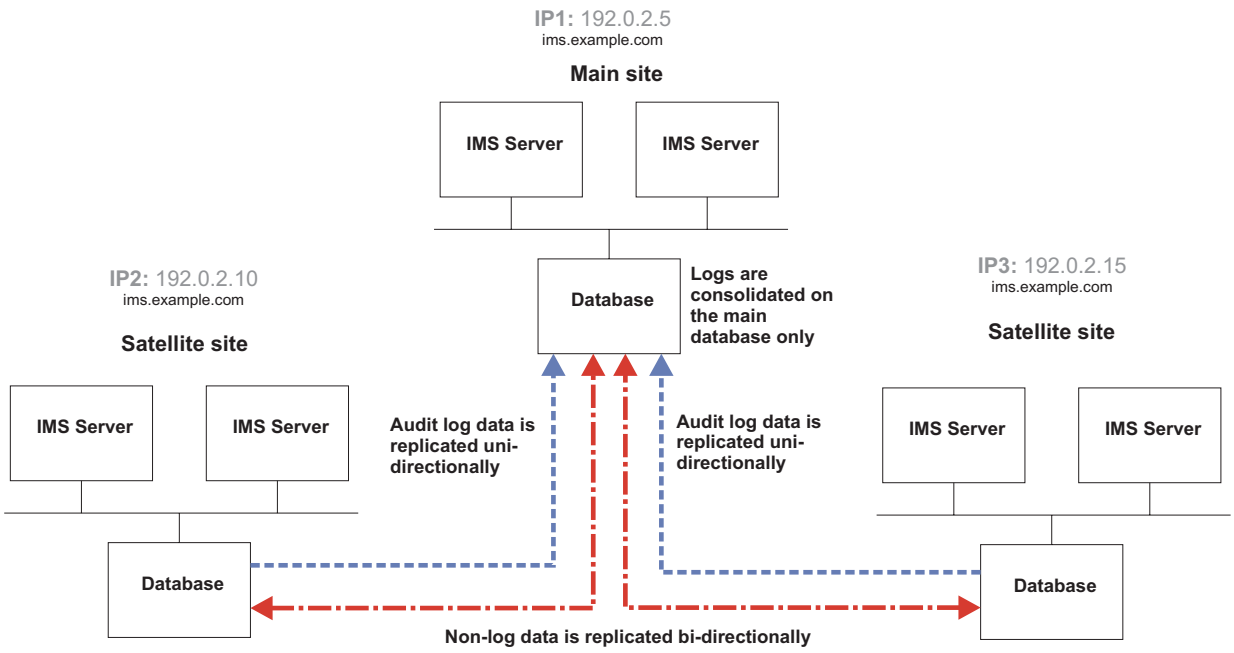

Figure 4. An example of how data is replicated between two satellites and a main site in a geographically distributed IMS Server deployment.

For example, IMS Servers at *Site 1* have a virtual IP of `192.0.2.10`. The IMS Servers at *Site 2* have a virtual IP of `192.0.2.15` but all the IMS Servers share the DNS name of `ims.example.com`.

If an IMS Server site becomes unavailable. For example: The IBM DB2 is down, the AccessAgent connected to this IMS Server site is redirected to the local or nearest active IMS Server site.

An alternative configuration is that each IMS Server site maintains its own unique IMS Server DNS name. In this configuration:

- The IMS Server at each site has its own unique IMS Server DNS name and virtual IP.
- The AccessAgent at each site is configured to communicate with the DNS name of the IMS Servers at that site.
- The IMS Server and AccessAgent installations at each site are installed and configured to different IMS Server DNS names.

Database replication

Use database replication to cross-replicate data between the IMS Server databases located at each site.

Database replication technologies vary between vendors. For this release, IBM Security Access Manager for Enterprise Single Sign-On supports only database replication for DB2.

The IMS Server at the *main site* hosts the master IMS Server database. The database server at each site can be stand-alone, clustered, or mirrored for high availability.

Load balancing and clustering

You can achieve high availability for the IMS Server by setting up multiple hosts with the IMS Server. Use a load balancer as the deployment front end with session-awareness and automatic failover capabilities.

The IMS Server architecture consists of multiple tiers:

- Load balancer
- Web server-tier (IBM HTTP Server)
- Application-tier (WebSphere Application Server)
- Data-tier (For example, DB2, Oracle or Microsoft SQL Server)

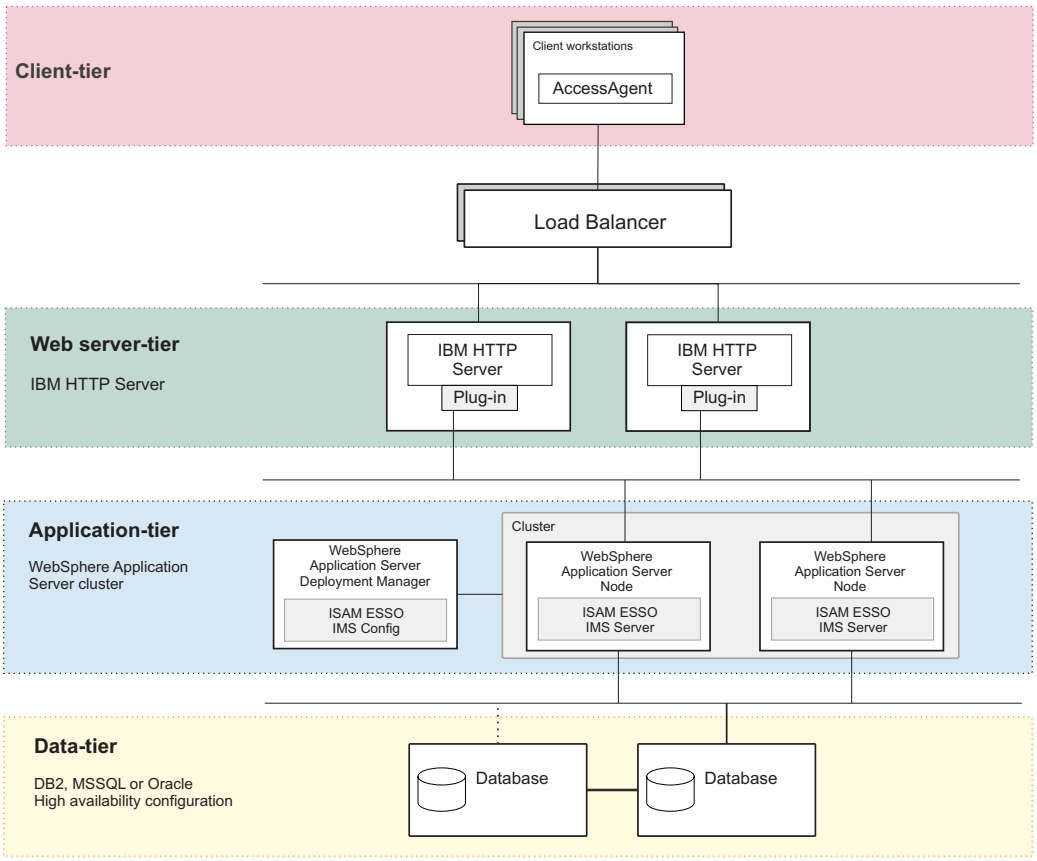

Figure 5. A multi-tiered deployment with a load balancing IP infrastructure as the deployment front end for distributing client requests.

The load balancer routes traffic to the Web Server tier, which in turn routes traffic to the Application Server tier. The load balancer is responsible for distributing incoming requests evenly to a collection of IMS Servers on the application-tier. By using a load balancer with session affinity, traffic from each client is always routed to the same IBM HTTP Server.

To set up a cluster for network deployment, see "Setting up a cluster (network deployment)" in the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.

Load balancing considerations on Windows platforms

If the IBM HTTP Server is deployed on a computer running Windows Server 2003 or later, leverage on the built-in Microsoft Network Load Balancing Service.

Microsoft Network Load Balancing Service acts as a software-based load balancer to the Web Server tier. In this case, there is no need for a separate load balancer hardware component in front of the Web Server tier.

In this setup, the Microsoft Cluster Service must not be enabled on the host machines for IBM HTTP Server. Microsoft does not support running Network Load Balancing Service and Microsoft Cluster Service on the same computer.

Load balancer requirements and considerations

The IMS Server can work with any regular IP-based load balancer. The load balancer can be a hardware-based appliance or a software-based equivalent.

For network deployment

In this configuration, it does not matter whether the IBM HTTP Server is located on the same host as the WebSphere Application Server or not. Each IBM HTTP Server can send requests to any WebSphere Application Server instances, on the same or different host. However, make sure that the WebSphere Application Server plug-in on each IBM HTTP Server node is configured properly.

The load balancer must have the following capabilities:

- Can load balance across the IBM HTTP Server nodes, and
- Can perform failover if a node is non-responsive.
- Can ensure client or session affinity by routing traffic from the same AccessAgent client or session to the same IBM HTTP Server node.
- Can ping a static IBM HTTP Server web page to verify whether the IBM HTTP Server node is available or not.

For virtual appliance deployment

In this configuration, there is no reliance on the IBM HTTP Server to load-balance across the WebSphere Application Server. Each IBM HTTP Server is routed to the WebSphere Application Server instance on the same virtual appliance only.

The load balancer must have the following capabilities:

- Can load-balance across the IBM HTTP Servers (one IBM HTTP Server in each virtual appliance).
- Can ensure client or session affinity by routing traffic from same AccessAgent client or session to the same IBM HTTP Server.
- Can ping a static IBM HTTP Server web page to verify whether the IBM HTTP Server node is available or not.

Disaster recovery

You can set up disaster recovery for IBM Security Access Manager for Enterprise Single Sign-On by setting up a standby of the IMS Server and its database at a designated disaster recovery site.

Considerations for disaster recovery design are different from availability. Disaster recovery focuses on the actions and processes to recover from a disaster that has struck existing infrastructure.

How to set up

Configure the IMS Server to use the same configuration as the active IMS Server except the IP address and the IMS Server database.

Use the Export Import configuration tool to copy the Production environment configuration and replicate it in the Disaster Recovery environment.

You can keep the standby database updated through log shipping or the database mirroring technologies of the respective database vendors. For example, DB2 HADR, Database Mirroring for Microsoft SQL 2005 and DataGuard for Oracle.

Recovering from a disaster

Upon a disaster, the operations staff must do the following tasks:

- Switch the standby database to active mode so that AccessAgent is redirected to synchronize with the IMS Servers at the disaster recovery site.
- Start up the IMS Server service on the standby server hosts.
- Switch the DNS settings so that AccessAgent points to the IMS Server at the disaster recovery site.

Chapter 5. Planning for performance

Configure IBM Security Access Manager for Enterprise Single Sign-On for an improved system performance.

See the following topics:

- "Factors that affect performance"
- "Improving the performance"

Factors that affect performance

Different factors such as memory allocation and data synchronization can affect the IMS Server and AccessAgent performance. Know more about these factors and the estimated network bandwidth consumption for the different events between AccessAgent and the IMS Server.

IMS Server and AccessAgent performance

The IMS Server and AccessAgent performance can be faster or slower depending on the following factors:

- The amount of memory allocated to IMS Server and to the Java Virtual Machine (JVM).
- Frequency of data synchronization between the AccessAgent and the IMS Server.
- The number of concurrent AccessAgent connections to the IMS Server.
- Quality of network connection from various AccessAgents to IMS Servers, and between the IMS Server and its database server.
- Processor speed of the IMS Server.
- The database pool size and timeout values.
- The number of concurrent users signed up.
- The number of concurrent users logged on with cached Wallets.
- The number of concurrent users logged on without cached Wallets.
- The number of AccessProfiles.
- The number of cached Wallets on a machine.

Improving the performance

Configure the AccessAgent and IMS Server settings to improve data synchronization, to improve the AccessAgent startup time, and to prevent memory errors.

Install AccessAgent with a prepackaged Wallet

Using a prepackaged machine Wallet during AccessAgent installation minimizes the overhead on the IMS Server during the initial download of system data during AccessAgent installation. AccessAgent downloads only incremental updates from the IMS Server.

This approach is for deployments where AccessAgent is deployed to several machines concurrently.

A prepackaged Wallet consists of system-scope policies, AccessProfiles, and the IMS Server certificate. The AccessAgent installer loads this prepackaged Wallet onto the machine before connecting to the IMS Server to download updates.

When you install AccessAgent, you can load the prepackaged Wallet. AccessAgent populates the machine Wallet before connecting to the IMS Server to download updates.

To install AccessAgent with a prepackaged Wallet, see the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.

Set the MaxSyncTimes

An option of "MaxSyncTimes" is added in Setuphlp.ini, to specify the maximum number of times to synchronize with the IMS Server during installation.

This option is useful for AccessAgent installation on several hundreds of machines and when the installer does not include a prepackaged Wallet.

With this option, AccessAgent downloads the system data from the IMS Server in case the initial attempts are rejected because of too many AccessAgent doing the same thing at the same time.

Enable the IBM HTTP Server compression

AccessAgent performance is affected by the large amount of data that is downloaded. IBM HTTP Server can compress and send data in gzip format to AccessAgent. By compressing pages and packets on the web-tier, you can reduce the time taken to transmit each response to a client request over the network. IBM HTTP Server compression is helpful when there is limited network bandwidth between the AccessAgent and the IMS Server.

IBM HTTP Server compression is disabled by default. To enable this feature, see the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

Increase the Java heap size

Increase the minimum and maximum Java Virtual Machine (JVM) heap size limit in WebSphere Application Server. Increasing the heap size can improve startup, prevent out of memory errors, and reduce disk swapping.

See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for the procedures.

Enable fast unlock

Enable and set the fast unlock grace period (pid_fast_unlock_grace_period_mins). This machine policy is applicable for all second factors, including smart card. With the fast unlock feature, users can unlock their workstations without contacting the IMS Server, and within a specific time period.

AccessAgent retrieves the last unlock time of the workstation and checks if it is within the configured time period.

- If the last unlock time is within the time period, AccessAgent determines if the unlocking user is the currently logged in ESSO user or the Windows user owning the current session.

- If it is the same user, AccessAgent unlocks the workstation without performing any check to IMS Server.
- Upon unlock, AccessAgent performs full authentication with IMS Server. AccessAgent uses the authentication factor used to unlock the workstation in the background.

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

Configure the IMS Server throttling policy

Set **Maximum thread size in download service** to 10 or less. Configure this setting in the IMS Configuration Utility, under **Advanced settings** > **IMS Server** > **Miscellaneous**.

The IMS Server throttling policy sets the limit of concurrent threads in the IMS DownloadService. When many users download large sizes of AccessProfiles concurrently, it can cause IMS Server to go out of memory. Setting this policy to the correct number prevents the IMS Server from going out of memory.

Other options

There are other ways you can improve the IMS Server and AccessAgent performance:

- Remove unnecessary or unused AccessProfiles. Right-click each unused AccessProfile and click **Delete**.
- Exclude the AccessStudio installation folder from certain runtime scans. For example: antivirus scans.
- Roll out additional IMS Servers to handle the load from AccessAgent. Use a load balancer to distribute the incoming traffic from various AccessAgent installations into multiple IMS Servers.
- Enhance the processor and memory of the IMS Server and the processor memory and disk storage of the database server.
- Ensure that the IBM HTTP Server tier is configured to accept the peak number of HTTP connections from various clients.
- For shared workstation deployments, ensure that the cached Wallet expiry period (if enabled) is set to a duration that ensures a good probability that each cached Wallet does not expire in between visits by user to the same workstation.
- Ensure the transaction isolation level for the IMS Server data source at the WebSphere Application Server, is set to Read-Committed (SQL, Oracle) and Cursor Stability (DB2).
- Periodically run the IMS Server database pruning scripts downloadable from support site.
- Ensure that the IMS Server database is maintained regularly as per database best practices. Enable the "automatic maintenance" feature of the database if manual database maintenance practices are not in place.
- Apply the latest IMS Server fix pack.

Chapter 6. Planning for security

Secure the IBM Security Access Manager for Enterprise Single Sign-On deployment on servers, workstations, remote desktop environments, and thin clients.

See the following topics for the different security measures:

- "General security measures"
- "Application server security"
- "User session security" on page 48

General security measures

Ensure that you comply with the general security requirements before you configure the application server security settings and the different authentication and session security-related policies.

The following are the general security requirements for the product deployment:

- Host the IMS Server and its required middleware in a secured data center on the main site and DR site.
- Harden the operating system of the IBM HTTP Server, WebSphere Application Server, and database server hosts against intrusion attacks.
- Apply strict access controls on the IBM HTTP Server, WebSphere Application Server, and database server hosts.
- Back up the IMS Server and WebSphere Application Server folders.
- Store the IMS Server database on a secure location.
- Protect each computer with firewalls, anti-virus, anti-malware tools.
- Implement role-based access control to protect access to operations in IMS Configuration Utility and in AccessAdmin.

Application server security

The WebSphere Application Server hosts the IMS Server. Secure the application server to protect the IMS Server applications, configuration folders, and files.

Enable application security

The IMS Server leverages WebSphere Application Server application security to protect access to IMS Configuration Utility. Only users granted with the *Web Configurator Administrator* role have rights to access this application. Enable application security so that the *Web Configurator Administrator* can reconfigure and restart the IMS Server remotely from a web browser.

Increase the WebSphere Application Server Root CA key size

To further secure new installations of the IMS Server, you can increase the key size for the root CA to 2048 bits. Increase the root CA key store size to increase the encryption strength. You also use the root CA to sign other certificates including IMS Server and SSL certificates.

See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for the procedures.

Secure access to configuration data and files

Restrict all access to the WebSphere Application Server configuration folders and key files to Administrators only.

See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for the procedures.

Remove sample WebSphere Application Server applications

Verify that there are no sample WebSphere Application servlets or applications installed on a production application server.

See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for the procedures.

Limit unsuccessful online login attempts

Set up an account lock out threshold for unsuccessful online login attempts. This security measure disables a user account if malicious actions are launched against that account and reduces the chances that the malicious actions compromise the account.

See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for the procedures.

Web server security

Consider some of the following ways to secure access to the servers:

- Restrict HTTP connections and redirect client requests to secure HTTPS.
- Disable directory browsing on the web server.
- Increase the SSL key size.
- Enable SSL for all AccessAgent and IMS Server communication.

  See "Enabling SSL directives on the IBM HTTP Server" in the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.

See "WebSphere Application Server Security advanced security hardening" at http://www.ibm.com/developerworks/websphere/techjournal/1004_botzum/1004_botzum.html for advanced security and hardening details.

User session security

Securing the user session is preventing unauthorized personnel from accessing the user desktop or stealing the application credentials of the user. There are different options for securing the user session on a private or shared desktop.

Password policies

Enforce password policies such as password aging and password complexity policies. Implementing these password policies protect the user against password guessing attacks.

Password aging
You can enable password aging and define the maximum password age. For example, after 90 days, the user has to change the password.

Password complexity
You can define the minimum and maximum length of the password, and the minimum number of numeric and alphabetic characters. You can also set whether to allow mixed uppercase and lowercase characters.

Note: For Active Directory deployments, IBM Security Access Manager for Enterprise Single Sign-On depends on the Active Directory password policies.

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

Two-factor and fingerprint authentication

Enforce the use of a second authentication factor to prevent an attacker from impersonating a legitimate user through theft or forgery of any single authentication factor. You can use RFID cards, smart cards, or hybrid smart cards for two-factor authentication.

See "Two-factor authentication" on page 90 for the different authentication devices that can secure a session.

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

Lock and unlock policies

Define the scenarios on when to lock and unlock the user desktop to prevent unauthorized access. These policies are important particularly for those using shared workstations.

You can configure the lock and unlock policies for the following sample scenarios:

- Desktop inactivity
- The authentication factor is removed from the reader
- The authentication factor is presented to the reader
- The Windows screen saver is activated

See the *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide* for the lock and unlock policy details.

Inactivity timeout policy

IBM Security Access Manager for Enterprise Single Sign-On can be configured to enforce a timeout policy if the user walks away from a workstation without logging out. On inactivity, ISAM ESSO can be configured to trigger one of the following actions. These actions are not applicable for private desktop mode.

- Lock the desktop screen while keeping the applications active.
- Auto-sign off from all active applications.
- Log off the users from their ISAM ESSO Wallets.
- Log out of the Windows session.
- Customize using session login and logout scripts.

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

Session lock, unlock, logon, and logout scripts

This feature is only applicable for shared desktop mode.

You can use session lock and session unlock scripts to automatically minimize or close applications that must not be displayed.

You can also use session logon and session logout scripts that enable any *walk away* policy to be automated and enforced.

See the *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide* for the policies that you can set during logon and logoff, lock and unlock.

Security questions (Secrets)

Set up security questions for users to answer when they want to reset their passwords. These security questions help with user verification. Review the security questions with the Legal department to ensure that the questions are in compliance with local privacy laws.

Presence detectors and walk away policies

This feature is only applicable for shared desktop mode.

IBM Security Access Manager for Enterprise Single Sign-On supports the use of presence detectors, such as sonar devices and active RFID. These presence detectors can detect if the user is away from the workstation and trigger actions without waiting for an inactivity interval.

IBM Security Access Manager for Enterprise Single Sign-On also automates the *walk away* security policy. When the user walks away, you can configure IBM Security Access Manager for Enterprise Single Sign-On to log out the user from the Wallet or from the Windows session, or to lock the computer.

For more information about presence detector-related policies, see *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide*.

Chapter 7. Planning for installation

There are different ways to install each of the product components and there are several factors to consider when installing these components.

See the following topics to plan your installation:

- "IMS Server preinstallation considerations"
- "Installation options" on page 54
- "Installation overview" on page 55
- "Planning for the IMS Server deployment" on page 57
- "Planning for client deployments" on page 61

See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for the detailed installation steps.

IMS Server preinstallation considerations

Before you start the installation of IBM Security Access Manager for Enterprise Single Sign-On, check the considerations for the host names, port numbers, user accounts, and fix packs.

Host names

- Choose a host name that is not likely to change, and that is resolvable through the DNS in your network or a file of a host.

  This approach gives you the option to move the server to another computer with a different IP address and still maintain a stable URL. Ensure that the host name is fully qualified.

  Important: To avoid connection problems, especially in a multiserver deployment with remote servers, specify host name values consistently to ensure that host names can be resolved. For more information about choosing host name values, see the topic on "host name values" in the WebSphere Application Server information center (http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.installation.nd.doc/info/ae/ae/rins_hostname.html).
- Avoid the use of host names that cannot be resolved with a DNS. Avoid host names, such as *localhost* or the loopback adapter `127.0.0.1`.

Ports

You can use the default ports for a standard installation on a clean computer. For advanced or custom deployments, you might have to use different port numbers.

If you intend to use the default ports, ensure that the port is not yet assigned and are available before using the product installation program.

1. Check the availability of the ports required by IBM Security Access Manager for Enterprise Single Sign-On.
2. Open a port checking utility on the computer. Alternatively, check the firewall rules for the system.

On Microsoft Windows, you can use the **netstat -b** command to check if the port is available. To learn more, go to the Microsoft web site at http://www.microsoft.com and search for "netstat".

3. If the port is already assigned, choose another value when prompted by the installation program.

The following table lists the default port numbers used by different components.

Use the planning worksheet in the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* to help you record ports that have been allocated during the installation.

Default port numbers	Used By
80	IBM HTTP Server (Web server port)
8008	IBM HTTP Server Administration port
443	IBM HTTP Server SSL port
9080	IBM WebSphere Application Server virtual host port number in the Java Virtual Machine.
1433	Microsoft SQL Server
1521	Oracle
8880, 8879	SOAP port to IBM WebSphere Application Server Network Deployment
9043, 9044	IBM WebSphere Application Server Network Deployment administrative console secure port
9060, 9061	IBM WebSphere Application Server Network Deployment administrative console
9443	IBM WebSphere Application Server Network Deployment SSL port
50000	IBM DB2 instance port
60010	IBM DB2 base port

Accounts for middleware components

This guide uses placeholder names for accounts that you must provide during the installation of the various components.

The following accounts are created during the installation of the product components. You do not create the accounts manually.

Component	Sample user logon name	Description
DB2	db2admin	The DB2 service user account ID is created during the installation of DB2. On a workgroup, the local db2admin service user account is added to the local **administrators** group. On a domain or directory server, the db2admin account is added to the **administrators** group. **Note:** Use the database service user account to create and perform administrative functions on the computer.
WebSphere Application Server Network Deployment	wasadmin	The WebSphere service administrator user account is created during the installation of the WebSphere Application Server Network Deployment.
IBM HTTP Server	httpadmin	The user account is created during the installation of IBM HTTP Server.
Tivoli Common Reporting	tcrAdmin	The reader user account to view reports.
(For Active Directory only) Active Directory Adapter	timadAdapterAdmin	You must install the Active Directory Adapter if an Active Directory Enterprise directory is used. The adapter requires you to supply an Active Directory administrator account for the Active Directory Adapter to perform administrative tasks.

Fix packs

Download the latest fixes for your product, platform, and version. If you are installing the products on separate servers, store the downloaded patches and fix packs on a centralized network accessible file share for easy access.

- IBM DB2 version 9.7

  https://www-304.ibm.com/support/docview.wss?rs=71&uid=swg21321001

  Note: If you are using Microsoft SQL Server or Oracle Database, download the latest patches or service packs from the vendors web site.
- IBM WebSphere Application Server version 7.0

  http://www-01.ibm.com/support/docview.wss?uid=swg27014463

  Download the latest fix packs for the WebSphere Application Server and the following WebSphere Application Server subcomponents:

  – WebSphere Update Installer

- IBM HTTP Server
- IBM HTTP Server plug-in for WebSphere

Installation options

Learn about the installation options for IBM Security Access Manager for Enterprise Single Sign-On components.

Installing IMS Server

The following table compares the options for installing the IMS Server.

Option	Description
Using interactive graphical mode	• You must install and configure: – WebSphere Application Server 7.0 – IBM HTTP Server Version 7.0 – IBM Update Installer for WebSphere software Version 7.0 – IBM Tivoli Common Reporting Version 2.1 – Your preferred database server
Using virtual appliance	• You must have VMWare ESXi. • The virtual image is preinstalled with the following components: – WebSphere Application Server Hypervisor Edition Version 7.0 – IBM Update Installer for WebSphere software Version 7.0 – IBM HTTP Server Version 7.0 – IBM Tivoli Common Reporting Version 2.1 – IMS Server product component for IBM Security Access Manager for Enterprise Single Sign-On Version 8.2

Installing AccessAgent

The following table compares the options for installing the AccessAgent client:

Option	Description
Using Setup.exe	• You can install AccessAgent in your preferred language. • You can also use the AccessAgent interface in different languages. • You specify the Server name and port number during installation.
Using AccessAgent.msi	• You can install AccessAgent in English or apply a language transform to add support for other languages. Use Active Directory Group Policy Object (AD GPO) to apply a language transform before you deploy the software.

Option	Description
Using silent mode	• For silent installations, specify the IMS Server name in the SetupHlp.ini. See "Response file parameters (SetupHlp.ini)" in the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for its content details.

Installing AccessStudio

The following table compares the options for installing the AccessStudio client:

Option	Description
Using Setup.exe	• You can install AccessStudio in your preferred language. • You can also use the AccessStudio interface in different languages.
Using AccessStudio.msi	• You can install AccessStudio in English or apply a language transform to add support for other languages. Use Active Directory Group Policy Object (AD GPO) to apply a language transform before you deploy the software.

Installation overview

Learn about the installation packages and installation prerequisites for each product component.

IMS Server installation

When you run the installer, it unpacks the IMS Server applications and configuration files into the designated installation folder. The installer also offers to deploy the IMS Server application files into the designated WebSphere Application Server environment. The installer supports installation on both WebSphere Application Server Base and WebSphere Application Server Network Deployment editions.

Prepare the server hosts for the IMS Server and make sure that the software prerequisites have been installed and configured before you run the IMS Server installer.

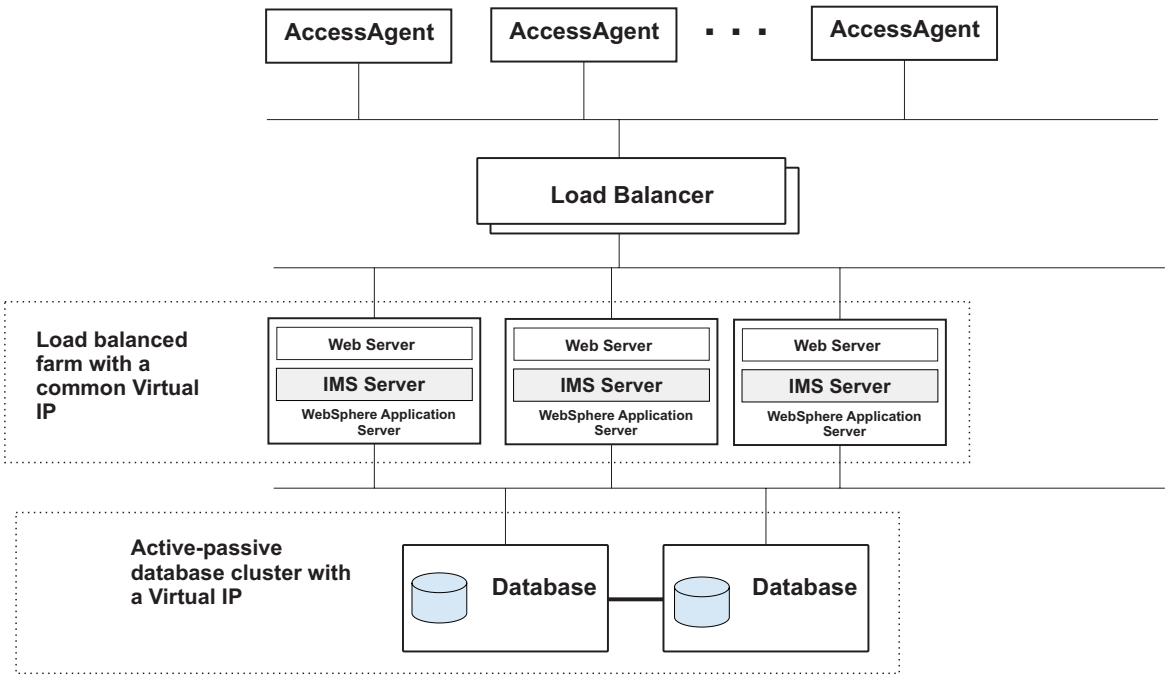

Figure 6. An example of a load balanced farm of IMS™ Servers with an IP load balancing infrastructure.

For high availability configuration, prepare the IP load balancing infrastructure. The IP load balancer can be either a hardware or software load-balancer. The IP load balancer must route traffic from any client back to the same member host in the server farm.

You can also deploy the IMS Server as a virtual appliance. This installation option simplifies the initial installation and deployment procedures for IMS Server.

AccessAgent installation

The AccessAgent installation package comes in the form of MSI and EXE files, and some configuration files.

The configuration files indicate the location of the IMS Server, whether a GINA replacement is required, and a few other installation options.

You can do a push-installation of the MSI and configuration files on the target Windows workstations and servers through typical software distribution systems. For example: Microsoft Active Directory Group Policy Object (AD GPO) and Tivoli Provisioning Manager.

You can also use an application provisioning software like Tivoli Provisioning Manager. AccessAgent is installed silently with the required "language" support added as an MSI option. Reboot the computer after completing the installation.

Alternatively, you can download the installation package to individual target machines and manually install it from there. You must have Administrator rights on the computer to do this option. If you use the EXE installer, you are prompted to select the language for AccessAgent during the installation process.

If you want to enforce two-factor authentication, you must install the required third-party drivers and libraries before you install AccessAgent.

Note: Do not remove `deploymentscript.vbs` directly. Keep `preremove` and `postcopy` sub. Comment out the content of these two subs instead. Otherwise, it causes installation error.

AccessStudio installation

The AccessStudio installer is an InstallShield-generated MSI file intended for Administrators. You can install AccessStudio manually on the Administrator user workstation.

You must install AccessAgent and Windows .NET Framework 2.0 before you install the AccessStudio. An error is displayed if either of these prerequisites are missing at the time of installation.

Planning for the IMS Server deployment

For scalability considerations, the IMS Server can be deployed in a number of configurations; stand-alone, cluster, multiple tiers, virtual appliance or in a geographically distributed IMS Server configuration.

You can deploy the IMS Server in any of the following ways:

Stand-alone server

The IMS Server is deployed on a stand-alone WebSphere Application Server profile. The web server and application server are typically installed and configured on the same host. A stand-alone deployment scenario is typically used for pilot or small scale deployments.

Multi-tiered deployment

Server components on all three tiers can be scaled vertically or horizontally. On the application-tier, the IMS Server can be deployed on a WebSphere Application Server cluster (network deployment). The data-tier can also be deployed in a high availability cluster. On the web-tier, the IBM HTTP Server can be installed on a separate server tier.

Virtual appliance deployment

The IMS Server can be deployed as a virtual appliance on a hypervisor platform. The virtual appliance includes a pre-installed IMS Server, the IBM HTTP Server, and the WebSphere Application Server in a stand-alone configuration. The data-tier can be deployed separately in a high availability cluster.

Geographically distributed or multi-site configuration

In a geographically distributed deployment, there are multiple IMS Server hosts and Database servers deployed on multiple sites. Database replication is configured for the data-tier to synchronize data between the sites periodically.

The IMS Server can be deployed in a WebSphere Application Server stand-alone or cluster, or a virtual appliance.

See the following topics:

- "Stand-alone deployment" on page 58

- "Network deployment (clustered)" on page 59
- "Virtual appliance deployment" on page 60
- "Distributed servers or clusters in multiple locations" on page 37

Stand-alone deployment

In a stand-alone deployment, the IMS Server applications are deployed on a stand-alone WebSphere Application Server profile.

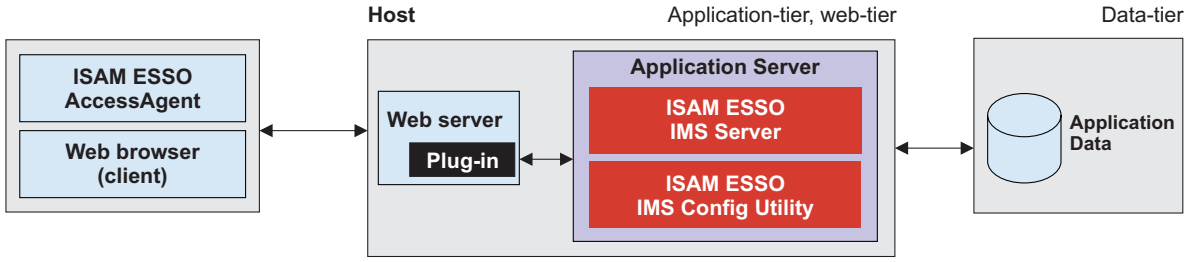

Figure 7. Example of a stand-alone deployment of the IMS Server.

The web server and application server are installed and configured on the same *Host*. This scenario is typically used for pilot and small scale deployments.

Implementation overview

The following steps outline how to set up a stand-alone environment for the IMS Server. See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.

1. Check and comply with the requirements.
2. Install and configure the required middleware on the Host.
   a. Prepare the Database server. If you are using DB2 or Oracle, create the IMS Server database.
   b. Install WebSphere Application Server.
   c. Install the WebSphere update installer.
   d. Install the WebSphere Application Server fix packs.
   e. Create a stand-alone WebSphere Application Server profile.
   f. Install the IBM HTTP Server
   g. Install IBM HTTP Server fix packs .
   h. Start the WebSphere Application Server profile.
3. Deploy the IMS Server applications in the WebSphere Application Server.
4. Verify the IMS Server deployment on the WebSphere Application Server.
5. To implement biometric support, install the Native Library Invoker (NLI) resource adapter.
6. Configure the IBM HTTP Server.
7. Configure the IMS Server.
8. Restart the WebSphere Application Server.
9. Configure your single sign-on authentication environment. See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

10. If you want to create, customize, and manage reports, install Tivoli Common Reporting.

Network deployment (clustered)

The Network Deployment consists of multiple WebSphere Application Servers in a cluster, where the IMS Server is managed as a single domain by the Deployment Manager.

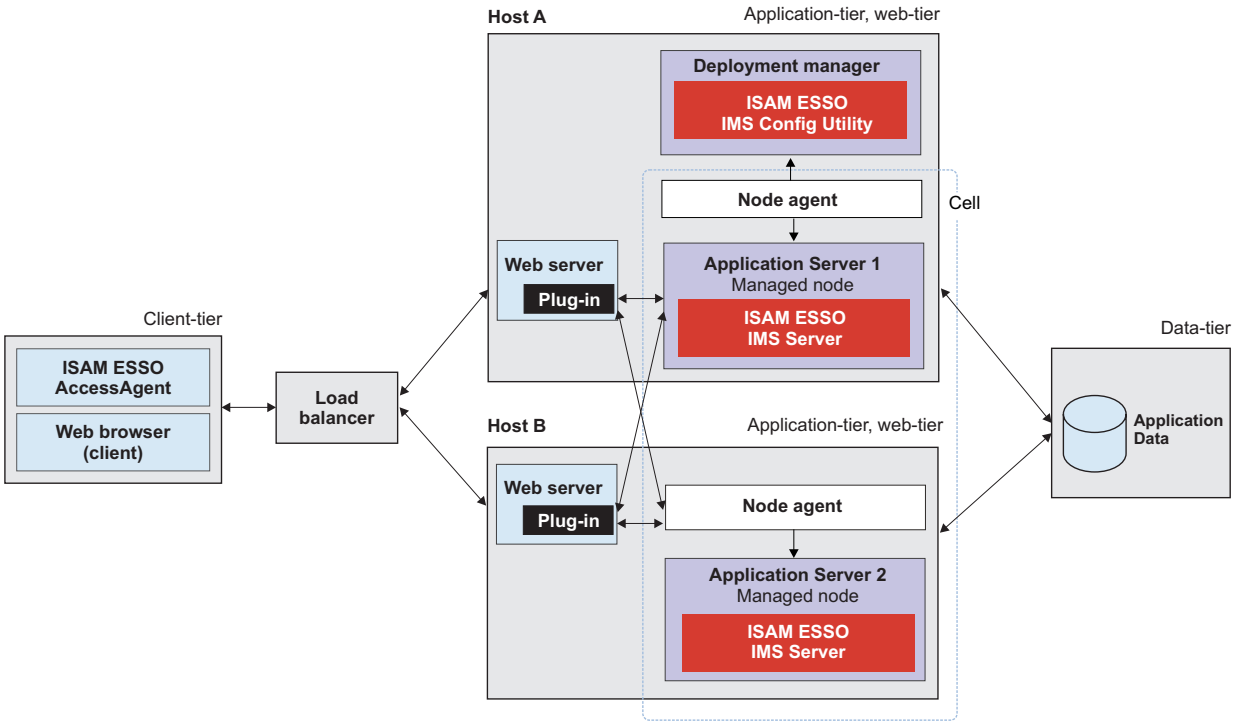

Figure 8. Example of IBM Security Access Manager for Enterprise Single Sign-On in a two node network deployment cluster for high availability

Use a network deployment (cluster) to sustain a high availability environment. The web servers are deployed on the same application-tier host. A load balancer is at the front of the deployment. Alternatively, the web servers and application servers can be deployed on separate *hosts*. A network deployment scenario is typically used for medium to large-scale deployments.

You might want to add additional application servers to an existing network deployment scenario for any of the following reasons:

- To build redundancy into your product deployment (high availability).
- To restore an application server that has failed.
- To have deployments that support higher volume of requests or support more users.

Implementation overview

The following list is an overview of how to do a network deployment.

1. Check and comply with the requirements.
2. Install and configure the required middleware.

a. Prepare the database server. If you are using DB2 or Oracle, create the IMS Server database.
b. On Host A, install WebSphere Application Server.
c. On Host A, install the WebSphere update installer.
d. On Host A, install the WebSphere Application Server fix packs.
e. On Host A, create a deployment manager profile and custom server profile.
f. On Host B, install WebSphere Application Server.
g. On Host B, install the WebSphere update installer.
h. On Host B, install the WebSphere Application Server fix packs.
i. On Host B, create a custom server profile.
j. On Host A and B, install the IBM HTTP Server.
k. Install the IBM HTTP Server fix packs.
l. Create a cluster. Add Host A and Host B as cluster members.
m. Start the WebSphere Application Server profile.

3. Deploy the IMS Server applications in the WebSphere Application Server.
4. Verify the IMS Server deployment on the WebSphere Application Server.
5. To implement biometric support, install the Native Library Invoker (NLI) resource adapter.
6. Configure the IBM HTTP Server.
7. Configure the IMS Server.
8. Restart the WebSphere Application Server.
9. Configure your single sign-on authentication environment. See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.
10. If you want to create, customize, and manage reports, install Tivoli Common Reporting.

Virtual appliance deployment

You can do a virtual appliance deployment for instances where you are not familiar with WebSphere Application Server or for a simpler way to deploy IMS Server.

In a virtual appliance deployment, the IMS Server is deployed from a virtual image that runs on a VMware ESX and ESXi. The virtual image contains SUSE Linux Enterprise Server, WebSphere Application Server Hypervisor Edition, Tivoli Common Reporting, IBM HTTP Server, and the IMS Server application. The virtual image does not include a database server.

Note: Virtual appliance is designed to run on VMWare ESX/ESXi Hypersivor only. Configuring it to run on other Hypersivor and virtualization solutions is not supported.

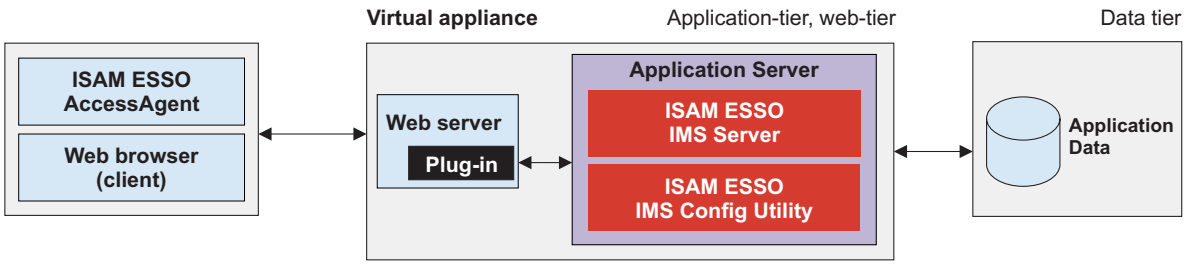

Figure 9. Deploying the IMS Server with a virtual appliance.

Implementation overview

The following list is an overview of how to do a virtual appliance deployment.

Tip: For high availability, deploy at most two virtual appliances as a replica, and do a manual synchronization. See "Virtual appliance replication for high availability" on page 36.

1. Check and comply with the requirements.
2. Prepare the database server.
3. Deploy the IMS Server virtual appliance on VMware ESX and ESXi.
4. Activate and configure the virtual appliance.
5. Configure your single sign-on authentication environment.

For more detailed procedures, see the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* and *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

Planning for client deployments

You can use the AccessAgent as a single sign-on client on Windows workstations or on Citrix/Terminal Servers

See the following topics:

- "Planning for installation of AccessAgent on Terminal Service or Citrix clients" on page 62
- "Planning for the Windows interactive logon experience" on page 63
- Chapter 11, "Session management," on page 117
- "Two-factor authentication" on page 90

To install or upgrade your AccessAgent version, see the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.

Upgrading AccessAgent clients

If you have a previous version of the AccessAgent clients, you must upgrade the IMS Server hosts to the latest version. You must upgrade the IMS Server before you upgrade the AccessAgent clients. See "Upgrading AccessAgent" on page 67 for more information about upgrading the clients.

Enterprise installation strategies

An enterprise installation strategy involves a mass deployment of the AccessAgent packages on multiple workstations in a repeatable way.

To deploy the packages on groups of workstations remotely, you can use a software provisioning solution like Tivoli Provisioning Manager or Active Directory Group Policy Objects.

For a silent installation, you can prepare a response file with preset deployment parameters. The response file contains parameters for the IMS Server host, license information, installation path, and product settings that are specific to your deployment environment. You can also customize the packages with additional settings to provide a custom enterprise logon experience.

Installation from a shared network folder is not supported.

Planning for AccessAgent installation on Terminal Service or Citrix clients

For terminal service deployments, you must deploy both the server and client version of AccessAgent.

You deploy the server version of AccessAgent on the Terminal Server and the client version AccessAgent on the Terminal Service/Citrix client. For terminal service environments, you can deploy the AccessAgent client in lightweight mode configuration, with a lower memory footprint on terminal service clients.

See Chapter 12, “AccessAgent on Citrix/Terminal Servers,” on page 123 for terminal service deployments with AccessAgent.

Planning for installations with two-factor authentication

If you are using two-factor authentication devices, install and set up the necessary drivers for your authentication devices before deploying AccessAgent. If you are combining two-factor authentication with desktop session management schemes, see “Two-factor authentication” on page 90.

Planning for installation on workstations with shared and private desktop switching schemes (session management)

See Chapter 11, “Session management,” on page 117 for the authentication considerations with session management schemes.

Planning for installation of AccessAgent on Terminal Service or Citrix clients

AccessAgent is the client software that performs single sign-on and authentication services. AccessAgent can single sign-on users to applications hosted on either the Windows workstations or on the Citrix/Terminal Server.

Client AccessAgent is AccessAgent installed on the user workstations. *Server AccessAgent* is AccessAgent deployed on Microsoft Windows Terminal Server and Citrix XenApp Server.

Planning for the Windows interactive logon experience

AccessAgent can be deployed on Windows workstations in GINA or GINA-less mode.

The following table shows the supported logon screen, desktop configuration, and whether two-factor authentication is supported when AccessAgent is deployed with or without GINA.

When AccessAgent is deployed with	Interactive logon with	Supported desktop configurations	Two-factor authentication support
GINA mode on	ESSO AccessAgent screen Windows Logon screen	• Shared desktop • Private desktop • Personal desktop	Yes
GINA mode off	Windows Logon screen	• Personal desktop • Roaming desktop	No

Note: On Windows XP, Windows Server 2003, and on earlier Windows versions, the interactive logon settings are controlled by either the ESSO GINA or MSGINA authentication modules. On Windows Vista and later versions, the GINA-based logon architecture is replaced with a *Credential Provider* model.

- In GINA mode, users log on to the Windows desktop through the ESSO AccessAgent screen with their ISAM ESSO credentials.

  Users are logged into their Wallet, and automatically logged into Windows using their Windows credentials.
- In GINA-less mode, users log on to the Windows desktop through the regular Windows Logon screen with their Active Directory credentials.

  AccessAgent then uses the same credentials to log on the users to their cached Wallet and to IMS Server.

  AccessAgent uses a module called ESSO Network Provider to capture the Active Directory credentials and to use these credentials to automatically log on the users to their Wallet.

  Note: Active Directory password synchronization must be enabled for ESSO Network Provider to work properly.

MSGINA is not replaced and is still available when users click the **Go to Windows to log on** link in the ESSO AccessAgent screen.

The ESSO AccessAgent screen is required for shared desktop and private desktop configurations and when using two-factor authentication. ESSO GINA also provides self-service sign-up and password reset services on the ESSO AccessAgent screen.

Chapter 8. Planning for an upgrade

IBM Security Access Manager for Enterprise Single Sign-On supports upgrade of previous product releases to the latest release to use the new and enhanced features. IBM Security Access Manager for Enterprise Single Sign-On upgrade is done per component similar to installation.

To upgrade the product, perform the following tasks in the same order as listed:

1. Upgrade the IMS Server.
2. Upgrade the deployed AccessAgents.
3. Upgrade the deployed AccessStudio clients.

Version compatibility

IBM Security Access Manager for Enterprise Single Sign-On supports the following version compatibility.

- The upgraded IMS Server 8.2 is compatible with AccessAgent 8.0.1 before you upgrade to AccessAgent 8.2.
- Upgrading the IMS Server does not overwrite the data. Existing data, settings, AccessProfiles, plug-ins, events, and other customization are preserved. The data and settings can be reused even after you upgrade IBM Security Access Manager for Enterprise Single Sign-On.
- Web Workplace and AccessAssistant are always upgraded together with the IMS Server.
- AccessStudio is only compatible with the same version of AccessAgent.

See the following topics to learn about the different upgrade options, upgrade results, upgrade considerations, and limitations for each component:

- "Upgrading the IMS Server"
- "Upgrading AccessAgent" on page 67
- "Upgrading AccessStudio" on page 68

Upgrading the IMS Server

Upgrade to IMS Server 8.2 if you want to use the new and enhanced product features. Upgrading IMS Server involves installing and configuring the IMS Server data source, certificate, and enterprise directory. The IMS Server upgrade process varies depending on the upgrade scenario.

Upgrade options

The following upgrade options are supported:

Current version	Upgrade path
8.1	Do a direct upgrade to version 8.2.
8.0.1	Do a direct upgrade to version 8.2.
8.0.0	Upgrade to 8.0.1 and then upgrade to 8.2
3.6	Upgrade to 8.0.1 and then upgrade to 8.2

How to upgrade

You can upgrade the IMS Server through the IMS Server installer and the Upgrade Configuration Wizard.

However, the detailed upgrade procedure varies depending on the current IMS Server version and on the following setup:

- Upgrade from a stand-alone setup
- Upgrade from a network deployment setup
- Upgrade from a Tomcat high availability environment (applicable only for 3.6 or 8.0

See "Upgrading to 8.2" in the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for the upgrade procedures.

What happens when you upgrade

When you upgrade to IMS Server 8.2:

- The IMS Server installation directory is changed.
  - By default, IMS Server 8.0.1 is installed in `C:\Encentuate\IMS Server\`.
  - IMS Server 8.2 is installed in `C:\Program Files\IBM\ISAM ESSO\IMS Server`.
- IMS Server 8.0.1 and 8.1 use the Active Directory (ADSI) Connector. IMS Server 8.2 uses the WebSphere Application Server Virtual Member Manager component to communicate with the Active Directory or to a single LDAP server. The Upgrade wizard migrates the ADSI configurations to the WebSphere Application Server Virtual Member Manager component.
- For upgrade from IMS Server 8.1 to 8.2, the WebSphere Application Server profiles are preserved.
- Any manual changes applied previously to `policyConfig.xml` are overwritten.
- There are no required changes on the database or enterprise directories. The installer makes the changes as necessary.

Upgrade considerations and limitations

Consider the following options, limitations, and changes before you upgrade:

- Upgrade the IMS Server through the interactive graphical mode.
- Upgrade the IMS Server before you upgrade the client components.
- The virtual appliance distribution of the IMS Server does not support upgrades from earlier IMS Server versions.
- To upgrade IMS Server 3.6 or 8.0 to 8.0.1, see http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.itamesso.doc_8.0.1/tasks/IMS_Installation_Upgrading_existing_IMSServer_installation.html.
- IMS Server 8.0.1 and 8.0 use a Tomcat application server instead of WebSphere Application Server.
- You must prepare the required 8.2 middleware before you upgrade IMS Server 8.0.1 and 8.0.

Table 10. Determining if middleware installation is required for a server deployment.

If you are upgrading the server from	J2EE Server / Application Server before upgrade	Install middleware before upgrade:
8.0	Apache Tomcat Server	Yes.

Table 10. Determining if middleware installation is required for a server deployment. (continued)

If you are upgrading the server from	J2EE Server / Application Server before upgrade	Install middleware before upgrade:
8.0.1	Apache Tomcat Server	Yes.
8.1	WebSphere Application Server	No.

- If you are using a stand-alone WebSphere Application Server environment, install the IMS Server on the application server host.
- For a WebSphere Application Server Network Deployment environment, install the IMS Server on the deployment manager host.
- If you want to back up your WebSphere Application Server profile, uninstall IMS Server from the Integrated Solutions Console.
- If you are planning to use a new server for the upgraded version, first upgrade the existing server and then use the *Export and Import configuration tool* to move to a new server.
- To avoid an IMS Server crash during upgrade, set **Maximum thread size in download service** to 10 or less. Set this policy in the IMS Configuration Utility, under **Advanced settings** > **Setting the IMS Server** > **Miscellaneous**.

Upgrading AccessAgent

Upgrade to AccessAgent 8.2 to use the new and enhanced AccessAgent features such as running in lightweight mode, an accessible user interface, and others. Upgrading AccessAgent involves replacing the old AccessAgent version but preserving the existing configurations.

Upgrade options

The following upgrade options are supported:

Current version	Upgrade path
8.1	Do a direct upgrade to version 8.2.
8.0.1	Do a direct upgrade to version 8.2.
8.0	Do a direct upgrade to version 8.2.

How to upgrade

Upgrading AccessAgent from *8.x* to 8.2 is like doing a new installation. You install AccessAgent 8.2 in all of the machines where AccessAgent *8.x* is installed. To upgrade AccessAgent to 8.2, follow the instructions in *Upgrading to 8.2* in the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.

What happens when you upgrade

When you upgrade to AccessAgent 8.2:

- By default, AccessAgent 8.0, 8.0.1 or 8.1 is installed in `C:\Program Files\Encentuate\`. When you upgrade, the AccessAgent 8.2 installer automatically uninstalls the existing AccessAgent and the new version is installed in `C:\Program Files\IBM\ISAM ESSO\`.

- If you have an existing AccessAgent installed and a Wallet with user credentials, installing the new version automatically moves the Wallet with user credentials to the new version. AccessAgent upgrade does not require any change on the IMS Server.

  After the upgrade, users can use AccessAgent with all their applications and web sites without any further action.
- The following data are preserved and moved to the new AccessAgent installation directory:
  - existing user and machine Wallets
  - system data
  - fingerprint and smart card settings
  - registry entries from `HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\DeploymentOptions`
  - registry entries from `HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\Integration`

Upgrade considerations and limitations

Consider the following options, limitations, and changes before you upgrade:

- Upgrade the IMS Server before you upgrade AccessAgent.
- When you upgrade AccessAgent, make sure that you upgrade AccessStudio to the same version.
- Upgrade from AccessAgent 8.1 (x86) on a 64-bit platform to AccessAgent 8.2 (x64), is not supported. To upgrade, you have to manually uninstall AccessAgent 8.1 (x86) and install AccessAgent 8.2 (x64).
- When you uninstall AccessAgent 8.1 (x86), the existing Wallets are removed.
- Any manual setting done in other registry locations as part of some interim fix needs to be manually redone after the upgrade.
- For Citrix connectors, manually reinstall the Citrix virtual channel connector.

Upgrading AccessStudio

Upgrade to AccessStudio 8.2 if you upgraded AccessAgent to 8.2. Upgrading AccessStudio involves replacing the old AccessStudio version.

How to upgrade

Upgrading AccessStudio from *8.x* to 8.2 is just like doing a new installation. You install AccessStudio 8.2 in the Administrator workstation where AccessStudio *8.x* is installed. To upgrade AccessStudio to 8.2, follow the instructions in *Upgrading to 8.2* in the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.

What happens when you upgrade

When you upgrade to AccessAgent 8.2:

- By default, AccessStudio 8.0, 8.0.1, or 8.1 is installed in `C:\Program Files\Encentuate\`. When you upgrade, theAccessStudio 8.2 installer automatically uninstalls the existing AccessStudio and the new version is installed in `C:\Program Files\IBM\ISAM ESSO\ECSS\AccessStudio`.
- The profiles created in the previous release are preserved and can be accessed, edited, and saved in a new version.

Upgrade considerations and limitations

Consider the following options, limitations, and changes before you upgrade:

- Upgrade the IMS Server before you upgrade AccessStudio.
- Ensure that you upgrade AccessStudio to the same version of AccessAgent. AccessStudio is only compatible with the same version of AccessAgent.

Chapter 9. Planning for configuration

Configure the IMS Server, client components, application profiles, and single sign-on policies to complete the deployment.

See the following topics for more information about the different configurations and configuration tools:

Configuring the IMS Server

Configuring the IMS Server involves configuring the IMS Server configuration properties. You configure the IMS Server to communicate with the other components such as enterprise directory server, database server, AccessAgent, and AccessStudio.

The IMS Server configuration properties are stored in an XML file in the WebSphere Application Server configuration repository `ims.xml`.

The configuration properties include:

- Enterprise directory connection parameters.
- IMS Server database connection and pooling parameters.
- Messaging connector parameters.
- Audit logging parameters.
- IMS Server bridge parameters.
- One time password (OTP) authentication configuration parameters.
- IMS Server session inactivity timeout parameters.
- AccessAdmin display options.

To apply any configuration changes, you must restart the IMS Server application.

Configuration tools

Configure the IMS Server through these tools:

IMS Configuration Wizard

Use this wizard during installation and initial configuration of the IMS Server.

After you deploy the IMS Server application to the WebSphere Application Server, open IMS Configuration Wizard. Install the IMS Server schemas into the designated IMS Server database, and configure the environmental certificate infrastructure settings. This configuration is only done once.

URL:

- If you are using WebSphere Application Server stand-alone deployment: *https://<was_hostname>:<admin_ssl_port>/front*
- If you are using WebSphere Application Server Network Deployment: *https://<dmgr_hostname>:<admin_ssl_port>/front*

For example: `https://localhost:9043/front`.

IMS Configuration Utility

Use this interface for post installation configuration of the IMS Server.

URL:

- If you are using WebSphere Application Server stand-alone: *https://<was_hostname>:<admin_ssl_port>/webconf*
- If you are using WebSphere Application Server Network Deployment: *https://<dmgr_hostname>:<admin_ssl_port>/webconf*

For example: `https://localhost:9043/webconf`.

Configuring IMS Server to use the directory server

IBM Security Access Manager for Enterprise Single Sign-On leverages on the enterprise directory server to identify and validate a user. Configuring IMS Server to use a directory server involves adding a new repository in the IMS Server database. It also involves configuring the connection between the IMS Server and the enterprise directory server.

IBM Security Access Manager for Enterprise Single Sign-On supports integration with either an Active Directory or any generic LDAP Server. IMS Server uses the WebSphere Application Server Virtual Member Manager component to communicate with these servers. See "Hardware and software requirements" on page 13 for the supported directory servers.

IBM Security Access Manager for Enterprise Single Sign-On does not change the directory schema or write any data on the enterprise directory server. The IMS Server connects to the enterprise directory server in the following scenarios:

- New user registrations
- Change and reset password requests for deployments with Active Directory password synchronization
- New machine registration for deployments with Active Directory as the enterprise directory
- Verification of Active Directory password before resynchronization
- Search by LDAP attribute

Only users with accounts in the designated enterprise directory can sign-up for an IBM Security Access Manager for Enterprise Single Sign-On account. Only users

with active enterprise directory accounts can access their IBM Security Access Manager for Enterprise Single Sign-On Wallet.

Configuration tool

You can configure IMS Server to use the enterprise directory server through the following options:

Using the IMS Configuration Wizard

After the IMS Server installation, some initial configurations are required and done through the IMS Configuration Wizard. Configuring the enterprise directory server is an option provided in the IMS Configuration Wizard, but you can choose to do this configuration later.

On the IMS Configuration Wizard, you can choose to add a new repository and select the type of directory server.

See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for the procedures.

Using the IMS Configuration Utility

You can configure the enterprise directory server through the IMS Configuration Utility following scenarios:

- If you choose not to configure the enterprise directory server through the IMS Configuration Wizard.
- If you already added a new repository through the IMS Configuration Wizard but decided to complete the configuration at a later time.

See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for the procedures.

Using Active Directory

IBM Security Access Manager for Enterprise Single Sign-On supports the configuration of multiple Active Directory domains. You can add a new Active Directory domain or edit the details of an existing Active Directory.

Additionally, the IMS Server can look up the directory for attributes of Windows workstations joined to the domain. IMS Server can use these attributes to select a machine group policy template to apply onto the computer.

Active Directory password synchronization

Active Directory passwords log on users to their Wallets and to single sign-on and log on users to their applications. When this policy is enabled, the ISAM ESSO password is synchronized with the Active Directory password. Users can always log on to the AccessAgent with their latest Active Directory credentials.

Password synchronization is applicable only to Active Directory deployments.

Password synchronization is required for any of the following scenarios:

- Automatic sign up
- Self-service reset of Active Directory password through AccessAgent or AccessAssistant
- GINA-less AccessAgent deployments to workstations
- Virtual Desktop Infrastructure (VDI) deployments

- Web Workplace deployments involving integration with SSL VPN

Password synchronization is suggested for these scenarios.

- Private desktop deployments
- Citrix/Terminal Server deployments involving thin clients
- Deployments without the Citrix SDK integration

IBM Security Access Manager for Enterprise Single Sign-On keeps its password in sync with Active Directory whenever either of the password is changed or reset. Users must remember their Active Directory password only, and can always use their latest Active Directory password to logon to AccessAgent or AccessAssistant or Web Workplace.

When the user changes the ISAM ESSO password through AccessAgent change password feature

AccessAgent changes the Active Directory password in the Active Directory and then changes the ISAM ESSO password.

If the Active Directory password change request fails, AccessAgent does not change the ISAM ESSO password and does reject the request with an error message.

When the user resets the ISAM ESSO password through AccessAgent reset password feature

AccessAgent changes the Active Directory password in the Active Directory and then changes the ISAM ESSO password.

If the Active Directory password change request fails, AccessAgent, does not reset the ISAM ESSO password and does reject the request with an error message.

The reset password feature runs an Active Directory change password operation in the Active Directory with the old password stored in the user Wallet.

When the user resets the ISAM ESSO password through AccessAssistant or Web Workplace

AccessAssistant or Web Workplace relies on either the WebSphere Application Server virtual member manager or the Tivoli Identity Manager Active Directory Adapter to perform an administrative reset of the Active Directory password. The ISAM ESSO password is then updated to the same value.

If AccessAssistant or Web Workplace cannot to reset the user Active Directory password, the reset password request fails and the ISAM ESSO password remains unchanged.

If the user changes Active Directory password through Microsoft GINA

AccessAgent captures the new password and attempts to update the ISAM ESSO password immediately.

If AccessAgent cannot to immediately update the ISAM ESSO password, the password becomes momentarily out-of-sync, and is resynced on the next online logon.

If the Administrator resets the Active Directory password of the user

AccessAgent resynchronize the ISAM ESSO password upon the next logon of the user to AccessAgent, AccessAssistant or Web Workplace with the new Active Directory password.

During this logon, IMS Server verifies the new Active Directory password against the Active Directory, then changes the ISAM ESSO password accordingly.

If the IBM Security Access Manager for Enterprise Single Sign-On and Identity Manager integration is in place

Resetting the ISAM ESSO password through Identity Manager resets the ISAM ESSO password, resets the Active Directory password, and updates the Active Directory password in the user Wallet. This feature can be enabled only if the "system-defined secret" feature is also enabled.

Using the Tivoli Identity Manager Active Directory (AD) adapter

The Tivoli Identity Manager AD adapter is required if all of the following conditions exist:

- the Active Directory password synchronization is enabled
- the Active Directory domain controller does not support LDAPs
- AccessAssistant and Web Workplace self-service password reset is used

If any of the conditions are not met, there is no need for a Tivoli Identity Manager AD adapter.

Using a generic LDAP Server

IBM Security Access Manager for Enterprise Single Sign-On supports the configuration of a single LDAP repository. You cannot add another LDAP repository if you have already added LDAP in the enterprise directory.

Password synchonization is not available for users of the LDAP directory server. Password synchronization is only available for Active Directory.

If you are using an LDAP-compatible directory server other than IBM Tivoli Directory Server, there might be additional configuration steps.

By default, the IMS Server directory server configuration sets the LDAP directory type to IBM Tivoli Directory Server.

To set the directory type for a generic LDAP server, other than IBM Tivoli Directory Server:

1. Complete the LDAP server configuration for the IMS Server.

   Complete the directory server configuration by using the IMS Configuration Utility or the IMS Configuration Wizard.
2. Change the LDAP directory type.
   a. Log on to the WebSphere administrative console.
   b. In the administrative console, click **Security** > **Global security**.
   c. Under **User account repository**, in the **Available realm definitions** list, verify that **Federated repositories** is selected.
   d. Click **Configure**.
   e. Under **Related Items**, click **Manage repositories**.
   f. Click the LDAP server you configured.
   g. In **Directory type**, select the correct directory type. For example: IBM Lotus® Domino®.
   h. Click **Apply**.

3. Restart the WebSphere Application Server.

Configuring the IMS Server to use the database server

A database server is required to store all of the IBM Security Access Manager for Enterprise Single Sign-On system, machine, and user data, including audit logs. You configure the IMS Server to connect to a database server to store and retrieve data.

You can install a new database server or use an existing database server. You can use an IBM DB2, Microsoft SQL Server, or Oracle Database. See "Hardware and software requirements" on page 13 for the supported Database servers.

Database server configuration involves specifying the data source and the database connection details, and creating a database schema. If the customer is using:

IBM DB2 and Oracle

- Customer can pre-create the IMS Server database without the IMS Server schema definitions.

  During the IMS Server configuration, customer must provide the database information so that the IMS Server can point to the database. An example of database information is the database user account credentials for the specific database.

  The IMS Configuration Wizard applies the schema definitions into the database.
- Customer can also pre-create the IMS Server database and also pre-install the IMS Server schema definitions.

  During the IMS Server configuration, customer must provide the database information so that the IMS Server can point to the database. An example of database information is the database user account credentials for the specific database.

Microsoft SQL

- Customer can pre-create the IMS Server database without the IMS Server schema definitions.

  During the IMS Server configuration, customer must provide the database information so that the IMS Server can point to the database. An example of database information is the database user account credentials for the specific database.

  The IMS Configuration Wizard applies the schema definitions into the database.
- Customer must setup and identify an SQL Server host.

  During the IMS Server configuration, customer must provide the database information so that the IMS Server can point to the database. An example of database information is the database user account credentials for the specific database.

  The IMS Server Configuration Wizard creates the IMS Server database and applies the schema definitions into it.
- Customer can also pre-create the IMS Server database and also pre-install the IMS Server schema definitions.

  During the IMS Server configuration, customer must provide the database information so that the IMS Server can point to the database. An example of database information is the database user account credentials for the specific database.

Configuration tool

You can configure the IMS Server and database server through the following options:

Using the IMS Configuration Wizard

After the IMS Server installation, configure the database server through the IMS Configuration Wizard. Database server configuration is a required task to complete the IMS Server deployment. You must complete the database configuration through this wizard.

With the IMS Configuration Wizard:

- You provide the required data source information
- You can create your own database schema or let the wizard automatically create the database schema
- You specify the database connection details such as the database connection port number and the host name

See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for the procedures.

Using the IMS Configuration Utility

In the IMS Configuration Utility advanced settings, you can configure the data source settings.

Configure the data source in the IMS Configuration Utility only if you are:

- replicating the database
- moving the database server location

See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for the procedures.

Configuring the application server

IMS Server is an application that runs on the WebSphere Application Server. IMS Server can be deployed on a WebSphere Application Server stand-alone or clustered environment.

The application server configuration might vary depending on whether you have a stand-alone or clustered environment. In general, configuring the WebSphere Application Server involves creating or choosing profiles, enabling the application security and configuring the Java heap size. It can also involve recreating the Root CA when applicable.

Configuration tool

You configure the WebSphere Application Server through the administrative console. You must have administrator privileges.

- Select **Start** > **All Programs** > **IBM WebSphere** > **Application Server <*version*>** > **Profiles** > **<*profile name*>** > **Administrative console**.
- Log on to the Integrated Solutions Console.

See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for the procedures.

Creating profiles

A WebSphere Application Server profile defines the runtime environment for the WebSphere Application Server nodes.

Create the profile before you install the IMS Server. You can create profiles with the command **manageprofiles** or the graphical Profile Management tool. See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for the procedures.

You can create the following profiles for different deployment scenarios.

WebSphere Application Server Profiles	When to use
Stand-alone *application server* profile	For single-server or stand-alone environments.
Deployment manager: *management* profile	For a network deployment environment, create this profile first.
Managed member nodes: *custom* profile	For a network deployment environment, create custom nodes and later use the administrative console to install the server application to the various custom nodes.

Note:

- Do not use `Administrator` as the WebSphere Application Server administrator user name during IMS Server profile creation.
- Ensure that the administrative user name that you provide for the WebSphere administrator does not exist on the directory server.

  For example: If the WebSphere administrator you provide is `wasadmin`, then the user `wasadmin` must not exist on the corporate enterprise directory. Choose a user name that is least likely to conflict with your potential enterprise directory users.

Restriction: The WebSphere Application Server administrative console does not have a domain list box. The administrative console cannot distinguish between an "admin" user in the file-based repository and an "admin" user in the configured enterprise directory.

The port numbers and setting used for each profile you create is always recorded in the `AboutThisProfile.txt` file. The file is stored in `<was_home>/profiles/<profile_name>/logs`. This file is helpful when you must determine the correct port number for a profile.

Stand-alone profiles

For single-server or stand-alone environments, use the stand-alone application server profile. For example: *AppSrv01*.

Note: This profile must be running before you install the IMS Server.

Deployment manager profiles

A deployment manager is a server that manages operations for a logical group, or cell, of other servers. In a network deployment, you use a group of servers to provide workload balancing and failover. The deployment manager is the central location for administering the servers and clusters in the cell.

The deployment manager profile is the first profile that you create so that you can create a network deployment environment.

You cannot deploy applications to the deployment manager itself but you can create custom nodes. Federate the custom nodes into the deployment manager to create a cell, a group of nodes, or clusters that can be managed from one location.

Note: This profile must be running before you install the IMS Server.

Custom profiles

To configure a network deployment environment, create custom nodes and federate them into the deployment manager. Later, you can use the WebSphere Application Server administrative console to install the IMS Server application on the various member nodes.

Unlike a stand-alone profile, a custom profile is an empty node that does not contain the default server that the stand-alone profile includes. After the custom profile has been federated to the deployment manager, the node becomes a *managed node*.

A managed node, which contains a node agent, is managed by a deployment manager.

Note: Ensure that you install the required WebSphere Application Server fix pack on each node of the cluster.

Server security and performance

Configure the application server to ensure security and to improve the IMS Server performance.

Configuring the Java heap size

You can tune the minimum and maximum Java Virtual Machine (JVM) heap size limit in WebSphere Application Server. Increasing heap size can improve the IMS Server startup, can prevent out of memory errors, and can reduce disk swapping.

For WebSphere Application Server on a 32-bits Windows host, the optimal heap size is between 1024 to 1280 MB.

For WebSphere Application Server on a 64-bits Windows host, a larger heap above 1280 MB can be allocated but it depends on the availability of the physical RAM.

If you have multiple servers, configure the Java heap size for every server in the cluster.

You can configure the Java heap size in the administrative console. Do this task before you install IMS Server on the WebSphere Application Server.

See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for the procedures.

Recreating the root CA

The WebSphere Application Server root CA has a default key size of 1024 bits. You can change the root CA key size to 2048 bits for increased security. The root CA certificate signs the default certificates in the key store. The certificates are for securing internal WebSphere Application Server communications.

Recreating the root CA is an optional task and is applicable only for new installations of the IMS Server. If you choose to change the root CA key size to 2048 bits, these steps must be completed before you run the IMS Configuration Wizard.

See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for the procedures.

Configuring the web server

The web server handles incoming requests from client computers or from a load balancer if there are multiple web servers. Configuring IBM HTTP Server involves granting remote server administration rights and securing the connection between the IBM HTTP Server and the WebSphere Application Server. You can also centralize the connection points for each web server.

Configuration tool

You configure the web server through the administrative console. You must have administrator privileges.

- Select **Start** > **All Programs** > **IBM WebSphere** > **Application Server <*version*>** > **Profiles** > **<*profile name*>** > **Administrative console**.
- Log on to the Integrated Solutions Console.

See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for the procedures.

Server security

Ensure a secure communication between AccessAgent and the IMS Server by configuring the IBM HTTP Server to forward connection requests over a Secure Sockets Layer (SSL).

Enabling SSL directives

By default, SSL communication is disabled on the IBM HTTP Server. Enable the SSL directives to encrypt traffic coming to and from the IBM HTTP Server.

To enable SSL, you must add the SSL Apache directive to the `httpd.conf` file. If you have multiple web servers, enable the SSL for every web server.

You can enable the SSL directives in the administrative console. Do this task before you install IMS Server on the WebSphere Application Server.

See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for the procedures.

Recreating the SSL certificate

The WebSphere Application Server SSL certificate has a default key size of 1024 bits. You can recreate the certificate size to 2048 bits for increased security.

Recreating the SSL certificate is an optional task and is applicable only for new installations of the IMS Server. If you must upgrade the default SSL certificate for IBM HTTP Server to 2048 bits, you must complete this task before you install the IMS Server.

If you are using multiple web servers, perform the steps on additional CMSKeyStores in the administrative console.

See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for the procedures.

Provisioning users

User provisioning is signing up user to use the IBM Security Access Manager for Enterprise Single Sign-On. When provisioning the user, the IBM Security Access Manager for Enterprise Single Sign-On account is created and stored in the IMS Server database.

The optimum process for most environments is to provision users after completing the following tasks in this order:

1. Installing the IMS Server.
2. Deploying the IMS Server.
3. Configuring the directory server
4. Provisioning an IMS Server Administrator.

Users are provisioned through the following options:

- Self-service sign-up through AccessAgent or through AccessAssistant Web Workplace. Users can click the sign-up link.
- Automatic sign-up through AccessAgent or through AccessAssistant Web Workplace when user first logs on with Active Directory credentials. This option is applicable only if Active Directory synchronization is enabled.
- Provisioning API

Provisioning tools

Users can be provisioned through the following option:

Using a provisioning system

You can use a provisioning system such as a Tivoli Identity Manager or other integrated third party solutions that can call the IBM Security Access Manager for Enterprise Single Sign-On provisioning APIs.

With provisioning systems, user credential Wallets can be provisioned and populated even before the first user logs on to AccessAgent.

To integrate with Tivoli Identity Manager, you must deploy the Tivoli Identity Manager Adapter for IBM Security Access Manager for Enterprise Single Sign-On into the Tivoli Identity Manager server. For the adapter details, see https://www-304.ibm.com/support/docview.wss?rs=644&uid=swg21396546&context=SSTFWV&cs=utf-8&lang=en&loc=en_US.

See the *IBM Security Access Manager for Enterprise Single Sign-On Provisioning Integration Guide* for the provisioning APIs.

De-provisioning users

User de-provisioning is revoking the user Wallet or the second authentication factor. This task is typically done when the user leaves the organization.

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

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

De-provisioning tool

Users can be de-provisioned from IBM Security Access Manager for Enterprise Single Sign-On through the following options:

Using AccessAdmin

If you provisioned a user through IMS Configuration Utility, you can revoke the Wallet or authentication factor through AccessAdmin.

See the *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide* for the procedures.

Using a provisioning system

You can use a provisioning system such as a Tivoli Identity Manager or other integrated third party solutions that can call the IBM Security Access Manager for Enterprise Single Sign-On provisioning APIs.

When Tivoli Identity Manager deprovisions users, it raises an event to the IBM Security Access Manager for Enterprise Single Sign-On adapter, which communicates with the IMS Server to delete the users.

When Tivoli Identity Manager deprovisions an enterprise application account, the command is sent to the IMS Server. IMS Server deletes the application record from the user Wallets.

See the *IBM Security Access Manager for Enterprise Single Sign-On Provisioning Integration Guide* for the provisioning APIs.

Configuring AccessAgent

Configuring AccessAgent might involve modifying the AccessAgent interface, or configuring its behavior or functions for particular scenarios.

Some settings can be configured before or after installing AccessAgent.

Example of possible configurations that affect the AccessAgent interface:

- You can change the AccessAgent or personalize the appearance of the AccessAgent interface.
- You can enable the **Help** button.
- You can enable or disable animation effects.

Example of possible configurations that affect the AccessAgent behavior or functions:

- You can configure AccessAgent deployed on the Citrix/Terminal Server to run on either *standard mode* or *lightweight mode*.
- You can enable or disable the ESSO GINA or ESSO Credential Provider.
- You can enable or disable the ESSO Network Provider.
- You can enable the **Ctrl+Alt+Delete** support in Windows 7.
- You can enable single sign-on for Java applications.
- You can enable or disable event reporting.
- You can enable the emergency hot key for private desktops.
- You can enable bidirectional language support.
- You can enable password reset.

See Chapter 12, “AccessAgent on Citrix/Terminal Servers,” on page 123.

Configuration tools

Configure AccessAgent through the following options:

Editing the SetupHlp.ini response file
You can pre-configure several AccessAgent setup parameters by modifying the `SetupHlp.ini` file before running the AccessAgent installer. The `SetupHlp.ini` file is located in the AccessAgent `Config` installation directory.

See "Setuphlp.ini configuration options" in the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for its content details.

See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for the AccessAgent configurations and the corresponding procedures.

Editing the DeploymentOptions
You can modify AccessAgent registry options in the **DeploymentOptions.reg** file located in the AccessAgent **Reg** folder.

You can also add new registry entries or edit the existing entries in the `[HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\DeploymentOptions]`.

See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for the different AccessAgent configurations and the corresponding procedures.

Using AccessAdmin
Set the machine-related policies through AccessAdmin under Machine Policy Templates.

See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for the different AccessAgent configurations and the corresponding procedures.

Configuring system, machine, and user group policies

AccessAgent, AccessAssistant, and Web Workplace behavior can be configured and controlled through a set of system, machine, and user policies.

Policies are created and modified to enforce the rules set by the business. Before a production deployment, you must have all of your policies clearly defined as

direct translations of the business security requirements. Modifying policies after the deployment cannot be avoided, but the suggested process for most environments is to define policies before deployment to production.

You can start configuring policies after an IMS Server installation. These policies are stored in the IMS Server database. You can modify these policies and apply the changes without restarting the IMS Server.

Configuration tool

Using AccessAdmin

You can use the Setup Assistant tool in AccessAdmin to configure the default system, machine, and user policies.

Alternatively, you can modify the policies in the respective policy templates.

See the following guides:

- *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide* for the different system, machine, and user policies.
- *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide* for more information about managing policy templates.

Configuring applications for single sign-on

Configuring applications for single sign-on involves configuring an authentication service and configuring AccessProfiles.

The IMS Server installer is packaged with a default set of AccessProfiles that provide single sign-on for a standard set of applications. AccessProfiles are preinstalled in the IMS Server database during the IMS Server installation.

For the list of supported applications and bundled AccessProfiles, see "Supported applications and profiles" on page 10.

For the list of available AccessProfiles, see the AccessProfile Library: https://www-304.ibm.com/support/docview.wss?uid=swg21470500&wv=1

To add single sign-on support for a wider base of enterprise applications, you can use AccessStudio to create additional AccessProfiles.

AccessStudio is a Windows-based application which Application and Security Administrators use to:

- Define new applications and authentication services.
- Create, modify, and test AccessProfiles for one or more applications.

AccessProfiles consist of an authentication service and a logical reference to an application. A single application can be associated with several AccessProfiles, but you can associate an AccessProfile with only one application.

Authentication services can be configured as either an enterprise or a personal authentication service.

Difference between enterprise authentication service and personal authentication service:

- Single sign-on to enterprise authentication services is audit-logged by default but not for personal authentication services.
- Policies related to enterprise authentication services can be set but not for personal authentication services.

Implementation

To configure applications for single sign-on:

1. Configure an authentication service.
2. Configure an AccessProfile.
3. Move the authentication service profile to the enterprise authentication services.

Configuration tools

Using AccessStudio

You can use AccessStudio to:

- Create or modify authentication services.
- Associate authentication services with AccessProfiles.
- Create or modify authentication service groups and group links.
- Create or modify standard and advanced AccessProfiles for different application types.

See the *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide* for the procedures.

Using AccessAdmin

You can use AccessAdmin to:

- Register and define an authentication service in the IMS Server.
- Set an authentication service as either an *enterprise authentication service* or as a *personal authentication service*.

See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for the procedures.

Distributing profiles

Test the AccessProfiles and then upload to the IMS Server for distribution to various AccessAgents. You do not need to restart the IMS Server to update profiles. Updated profiles are synchronized across the various AccessAgent clients deployed on workstations within the next synchronization period.

Product customization

IBM Security Access Manager for Enterprise Single Sign-On is configurable and customizable. You can customize certain aspects of the product based on how you intend to use the product.

Customization capabilities

You can do the following customization:

- Extend single sign-on and workflow automation support to any number of applications by creating and uploading additional AccessProfiles to the IMS Server.

- Define custom triggers and actions in the AccessProfile to meet the single sign-on or automation requirements for the application. This custom trigger or action calls on theAccessAgent plug-in which you can write in VBScript or JScript.
- Use any standard SQL reporting tool to connect to the IMS Server database and generate audit reports.

  The IMS Server database schema comes with a number of predefined database views intended for external reporting use.
- Create or enhance an AccessProfile to report on specific events in any specific application. For example, launching of a certain screen, or the display of certain types of data, or the clicking of a button on a screen.
- Use a Serial ID SPI to integrateAccessAgent with any device with serial numbers like RFID.

  To support any designated RFID card or reader, you must develop the Windows DLL defined in the Serial Provider Interface. At deployment time, this DLL needs to be installed onto the designated user workstations. AccessAgent uses this DLL to talk to the corresponding RFID reader. See *IBM Security Access Manager for Enterprise Single Sign-On Serial ID SPI Guide*.
- Customize the AccessAgent user interface. You can:
  - Change the logon banner.
  - Customize the displayed text for logon screens. For example, you can customize the displayed text for logon and welcome messages for different authentication factors.
  - Enable or disable system tray pop-up messages.
  - Enable or disable right-click menu options.
  - Enable or disable the link to bypass logon through Windows GINA.
  - Enable or disable custom self-help web sites or applications.
  - Control the display of available system tray menu options.
- Customize AccessAgent behavior or functions. You can:
  - Enable or disable ESSO GINA.
  - Enable or disable automatic sign-on to applications.
  - Set up custom hot keys for ease of use or for emergency bypass scenarios.
  - Configure error message prompts to display in a system modal mode. For example, when an AccessAgent error message prompt displays, you cannot open or use other applications on your desktop until you respond to the prompt.
  - Add in any files or scripts to be distributed with the AccessAgent installer in the **config** folder.
  - Apply changes to the MSI installer file based on the software distribution mechanism.
  - Add language support.
  - Set up different authentication factors for different groups of machines.
  - Set up session management. You can configure workstations in Shared Desktop or Private Desktop modes to support fast user switching on these machines.
  - Set up Wallet protection and management policies.
  - Customize the list of questions and the number of questions prompted during registration and verification. You can also customize the required number of correct answers.

Customization can be applied without recompiling or reinstalling the product components. Changes are automatically propagated to all AccessAgent either immediately, or upon restart of the computer.

Customization data are automatically preserved and are not overwritten during upgrades.

Configuration tools

Using SetupHlp.ini file and DeploymentOptions

Some features require installer customization. You can modify AccessAgent setup parameters in the **SetupHlp.ini** file and the registry options through **Config** installation directory.

Using AccessAdmin

Some features can be customized when you edit policies in AccessAdmin. You can configure system, machine, and user-related policies through AccessAdmin.

Using AccessStudio

Use the AccessStudio tool to create or modify AccessProfiles for different applications and to upload these profiles to the IMS Server. The IMS Server distributes these profiles to all AccessAgent.

See the *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide* for the procedures.

Using APIs and SPIs

IBM Security Access Manager for Enterprise Single Sign-On includes APIs and SPIs to integrate with third-party solutions and products. See "Integrating with other solutions with APIs and SPIs" for the different APIs and SPIs.

Integrating with other solutions with APIs and SPIs

IBM Security Access Manager for Enterprise Single Sign-On includes APIs and SPIs for integration with other products and solutions.

ISAM ESSO Provisioning API

IMS Server has a provisioning API that helps you to:

- Provision and de-provision ISAM ESSO accounts
- Add, delete, and update application credentials on the ISAM ESSO Wallet
- Retrieve a list of active user IDs for account reconciliation purposes
- Reset the ISAM ESSO password

AccessAgent plug-in APIs

AccessAgent plug-in APIs are VBScript or Java script code that performs some custom action as part of a custom trigger or action inside an AccessProfile. Use these APIs to:

- Perform audit logging
- Add, delete, or modify Wallet contents
- Modify Wallet policies
- Perform automation tasks through a VBScript or JScript

See *IBM Security Access Manager for Enterprise Single Sign-On Provisioning Integration Guide*.

Mobile ActiveCode APIs

The API enables third-party applications to integrate with the IMS Server to achieve strong authentication with Mobile ActiveCodes.

Serial ID SPI

Provides a generic device management framework for AccessAgent to support any new device containing serial numbers and use it as a second authentication factor.

Serial ID is a unique, randomized, and non-public string of bytes associated with a physical token carried by the user. Examples include the card serial IDs embedded in RFID badges and magnetic stripe cards.

To support various Serial ID readers from different vendors and for different types of tokens, AccessAgent relies on a common interface to talk to each type of reader. This interface is called the Serial ID Service Provider Interface.

To integrate with any device, a corresponding "provider" dynamic link library (DLL) that implements the interface needs to be co-deployed with AccessAgent. Use the provider DLL to detect the presentation of the serial ID card or token, and read the serial ID.

AccessAgent is bundled with Serial ID provider DLLs for some types of RFID card readers. Vendors, partners, and customers can also integrate additional brands or types of serial ID readers by developing provider DLLs for these devices.

See *IBM Security Access Manager for Enterprise Single Sign-On Serial ID SPI Guide*.

Web API for credential management

You can install or run AccessAgent on a computer with a Windows operating system only. Other platforms such as Linux and Mac OS are currently not supported.

A set of Web API is exposed from the IMS Server. With this Web API, you can get, set, and delete user credentials on the IMS Server.

This feature requires integration and support from IBM partners.

See *IBM Security Access Manager for Enterprise Single Sign-On Web API for Credential Management Guide*.

Chapter 10. Planning for authentication factors

IBM Security Access Manager for Enterprise Single Sign-On supports the use of different authentication factors such as fingerprints, RFID and smart card devices, and one-time passwords.

See the following topics:

Primary authentication factors

You can use the IBM Security Access Manager for Enterprise Single Sign-On password, and directory server credentials as primary authentication factors. Secrets are typically used to recover credentials or as an alternative to bypass a secondary authentication factor.

ISAM ESSO passwords

When the user signs up with AccessAgent, the user registers with the IMS Server and creates a Wallet. The user is prompted to provide a password for the user Wallet. The user can use the Active Directory password as the ISAM ESSO password. The minimum and maximum length of the password can be configured. For example: 6-20.

All application credentials are stored in the user Wallet. The ISAM ESSO password is the primary authentication factor for accessing and securing the user Wallet. AccessAgent locks the Wallet if the user enters a wrong password for five consecutive times. The number of allowed attempts is set by the organization.

The user does not have to remember all the application passwords. The ISAM ESSO password enables the user to automatically sign on to the applications listed on the Wallet.

LDAP or Active Directory passwords

Users can use enterprise directory credentials to sign-up to AccessAgent. For logon, users can use enterprise directory credentials if the Active Directory password synchronization is enabled.

If the Active Directory password is the primary password for logging on to computers and applications, enable the Active Directory password synchronization

feature. Password synchronization synchronizes the ISAM ESSO password with the Active Directory password. Users can use the same password to log on to all computers, with or without AccessAgent.

If Active Directory password synchronization is enabled, the corporate Active Directory password policies supersede the ISAM ESSO password policies.

Secrets

Secrets are information that only the user knows. When a user signs up for a Wallet, the user is prompted to select one or more questions from a list and answers to those questions. All the questions are customizable and configurable.

Primary secret is the first secret that the user answers while signing up. This primary secret (answer) cannot be changed.

Users must provide a secret that is not likely to change and is not easily forgotten even if it is not used for a long time.

Note: The user can use all the characters in the ISO Latin-1 character set in creating secrets, except for characters µ and ß.

You can allow users to provide more than one secret.

There are two types of secrets:

User-defined secrets

By default, IBM Security Access Manager for Enterprise Single Sign-On prompts the user to specify user-defined secrets during sign-up. These secrets help users:

- reset passwords
- bypass the use of a second authentication factor

System-defined secrets

If you enable the system-defined secret option, the user does not have to specify a secret during AccessAgent sign-up.

AccessAgent does not prompt the user for a secret to do reset password, Active Directory password synchronization, and offline recovery.

If you set the AccessAgent to use system-defined secrets, this setting cannot be changed again.

If you provisioned users into the IMS Server through a third-party provisioning system, enable system-defined secrets only if you want to reset the user password.

Two-factor authentication

Use a second factor device such as smart card or RFID card to enforce strong authentication.

Authentication policies can vary per user group and per machine group. For example: You can roll out RFID cards to users in one department, smart cards to another group of users, and password only authentication for a third group of users. You can configure some machines with RFID readers and others with fingerprint readers. You can allow users to register more than one second factor

like RFID card and smart card, or to easily switch from one second factor to another factor. Users can have multiple authentication factors registered.

Complete the following steps to enable two-factor authentication:

1. Install the required drivers or authentication device middleware on the workstations.
2. Create a machine policy that supports the selected authentication factor.
3. Assign the machine policy.
4. Register the authentication factor in IBM Security Access Manager for Enterprise Single Sign-On.

Regardless of choice of authentication factors, you can centrally manage all authentication policies through AccessAdmin. In addition, IBM Security Access Manager for Enterprise Single Sign-On supports device service provider interface, enabling easy integration with serial ID devices.

AccessAgent integrates with the middleware or libraries of the supported authentication devices. As such, user can log on, log off, lock, or unlock AccessAgent with an authentication factor.

Fingerprint authentication

IBM Security Access Manager for Enterprise Single Sign-On supports fingerprint authentication of users in both personal and shared workstations.

How it works

Users can log on, lock, and unlock AccessAgent with fingerprint only. Users must scan their fingerprint into the fingerprint reader. Users might scan their finger on any of the following screens:

- Welcome screen
- Log on screen
- Sign up screen
- Reset password screen

This process results to a fingerprint registration template and the template is stored in the IMS Server database. This registration template can be cached in the computer running AccessAgent.

When the users scan their registered fingerprints, the fingerprint reference templates are compared to each cached fingerprint registration templates. If the template is not found, the users are prompted for their ISAM ESSO username. The username and reference template are authenticated against the IMS Server database.

Note: The UI is disabled on a successful fingerprint scan. If the fingerprint reader is unable to read the fingerprint properly, an error message is displayed on AccessAgent.

IBM Security Access Manager for Enterprise Single Sign-On relies on the third-party biometric software to:

- Integrate with the fingerprint reader and capture the fingerprint reference template (for logon) and fingerprint registration template (for new fingerprint registration).

- Verify a logon fingerprint reference template against the stored fingerprint registration template.

To use fingerprint authentication:

- The users must sign-up with IBM Security Access Manager for Enterprise Single Sign-On with a fingerprint.
- The users must register their fingerprints.

  Note:
  - The users can register 1-10 fingerprints. The users can also delete or replace the existing registered fingerprints.
  - You can configure the maximum number of fingerprints allowed for each registration by using the `pid_fingerprint_registration_max` policy.
  - The users are prompted to scan their finger several times during registration depending on the fingerprint reader and the biometric SDK.
- The users must log on to AccessAgent with the registered fingerprint.

Fingerprint tap same and tap different

Fingerprint tap same
: The fingerprint scanned is registered to the logged-in AccessAgent user.

Fingerprint tap different
: The fingerprint scanned is not registered to the logged-in AccessAgent user.

Requirements and compatibility

Fingerprint authentication support requires a third-party biometric software, registered fingerprints, and a fingerprint reader.

Requirements specification

The middleware or SDK, and fingerprint reader must at least meet the following specifications:

Category	Requirements
Biometric middleware	• The same biometric middleware must be used across all machines in the deployment. Mixing biometric middleware across a deployment is not supported. • IBM Security Access Manager for Enterprise Single Sign-On relies on the 1:1 verification capabilities of the underlying biometric vendor. IBM Security Access Manager for Enterprise Single Sign-On always verifies a presented fingerprint against the fingerprint registration template for the specific finger. • IBM Security Access Manager for Enterprise Single Sign-On integrates with the following middleware: – BIO-key Biometric Service Provider – DigitalPersona Gold SDK 3.2 – UPEK BioAPI SDK
Fingerprint reader	• Mixing different fingerprint readers is allowed as long as the same biometric middleware can support different readers interchangeably. For example, if the fingerprint template captured by one brand of reader can be used for verification with another brand of reader.

Supported middleware and devices

These biometric middleware and fingerprint readers are supported:

Category	Requirements
Middleware	• BIO-key Biometric Service Provider – 1.9.*x* (x86) – 1.10.*x* (x86) • DigitalPersona Gold Fingerprint Recognition Software – 3.2 (x86) • UPEK BioAPI SDK – 3.0 (x86) – 3.5 (x86)
Fingerprint readers	• Fingerprint readers compatible with the following middleware: – BIO-key – DigitalPersona – UPEK **Note:** See http://www.bio-key.com/fingerprintbiometrics/supported_devices.asp for the list of supported devices from BIO-key.

Deployment

Learn how to deploy support for fingerprint authentication.

Using BIO-key

Main tasks to configure IBM Security Access Manager for Enterprise Single Sign-On for fingerprint authentication with BIO-key:

1. Install the BIO-key Biometric Service Provider drivers in the IMS Server and in AccessAgent.
2. Enable fingerprint support in the IMS Server by applying the bio-key deployment package and enabling the fingerprint authentication factor in the machine and user policy templates.
3. Configure user authentication for fingerprint support.

See "Integrating a BIO-key fingerprint reader" in the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for the detailed integration procedure.

Using DigitalPersona

Main tasks to configure IBM Security Access Manager for Enterprise Single Sign-On for fingerprint authentication with DigitalPersona:

1. Install the DigitalPersona Fingerprint Gold SDK in the IMS Server and in AccessAgent.
2. Enable fingerprint support in the IMS Server by applying the digitalpersona deployment package and enabling the fingerprint authentication factor in the machine and user policy templates.
3. Configure user authentication for fingerprint support.

See "Integrating a DigitalPersona fingerprint reader" in the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for the detailed integration procedure.

Using UPEK

Main tasks to configure IBM Security Access Manager for Enterprise Single Sign-On for fingerprint authentication with UPEK:

1. Install the UPEK BioAPI SDK drivers in the IMS Server and in AccessAgent.
2. Enable fingerprint support in the IMS Server by applying the UPEK deployment package and enabling the fingerprint authentication factor in the machine and user policy templates.
3. Configure user authentication for fingerprint support.

See "Integrating a UPEK biometric reader" in the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for the detailed integration procedure.

Policies

Sample policies that you can set when enforcing fingerprint authentication.

AccessAdmin policy	Description
pid_fingerprint_tap_same_action	Actions to be performed by AccessAgent when the currently logged on user taps a finger on the reader.

AccessAdmin policy	Description
pid_fingerprint_tap_same_action_countdown_secs	Confirmation countdown duration, in seconds, for tapping same finger on desktop
pid_fingerprint_tap_different_action	Actions to be performed by AccessAgent when a finger is tapped on desktop and does not belong to the currently logged on user.
pid_fingerprint_tap_different_action_countdown_secs	Confirmation countdown duration, in seconds, for tapping different finger on desktop
pid_fingerprint_registration_max	Maximum number of fingerprints that each user is allowed to register.
pid_fast_logon_enabled	Users with cached Wallet can log on to AccessAgent without authenticating with the IMS Server. To perform validation after logon, you must enable background authentication.
pid_background_auth_enabled_option	Option to specify if AccessAgent must perform authentication with IMS Server in the background. **Note:** Enable background authentication to check with the IMS Server the validity of the scanned fingerprint.

See *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide* for more information about these policies.

Smart card authentication

IBM Security Access Manager for Enterprise Single Sign-On supports the use of smart cards for user authentication in both personal and shared workstations.

How it works

Users can log on, lock, and unlock AccessAgent with smart card and PIN only. Insert the smart card into the smart card reader and provide the smart card PIN when prompted.

Note: The smart card PIN is not related to the ISAM ESSO password. IBM Security Access Manager for Enterprise Single Sign-On does not manage and reset the smart card PIN.

To use smart card authentication, register the smart card as a secondary authentication factor.

Requirements and compatibility

Smart card authentication support requires a smart card middleware, a smart card, a smart card reader, and a smart card PIN. To know what middleware, card or reader is supported, check the requirements specification.

Requirements specification

The smart card, reader, and middleware must at least meet the following specifications:

Category	Requirements
Smart card middleware	• The smart card middleware can support the chosen smart card and the reader. • The smart card middleware exposes Microsoft CAPI interface to communicate with smart cards. AccessAgent accesses the smart card through this interface. • The Cryptographic Service Provider (CSP) implementing the CAPI interface can support the following functions: – silent mode of operation so that it does not prompt user for smart card insertion, or certificate selection, or PIN entry – verification of the smart card PIN – enumeration and reading of certificates from the smart card – hashing and signing operations with the keypair that corresponds to the authentication certificate There is a *Smart Card PKCS#11 Cryptographic Service Provider* available for download at: http://www-01.ibm.com/support/docview.wss?uid=swg24026504. This is a Microsoft CAPI-compliant CSP that can be used to integrate with smart card middleware that exposes PKCS#11 APIs only.
Smart card	• The smart card can perform RSA cryptographic operations. • The smart card contains an RSA key pair and a corresponding X.509 certificate that is suitable for authentication. The certificate must allow the use of the key pair for client authentication and digital signatures • Private objects on the smart card, including private keys, must be protected by a PIN known to the user.
Smart card reader	• The reader is compliant with the PC/SC standard.

Supported middleware and devices

These smart card middleware are supported:

Category	Requirements
Middleware	• Gemalto Classic Client 6.0 (x86) • Gemalto Access Client 5.5 (x86) • SafeSign Identity Client 3.0 (x86) • Charismathics Smart Security Interface 4.8 (x86) • Spanish DNIe (x86)

Deployment

Learn how to deploy support for smart card authentication.

Road map

These are the main tasks to configure IBM Security Access Manager for Enterprise Single Sign-On to provide smart card authentication.

1. Ensure that the smart card middleware and reader driver are already installed on the computer. AccessAgent does not carry any drivers or middleware that might be necessary to support smart cards.
2. Ensure that the IMS Server and AccessAgent are installed before the smart card authentication support deployment.
3. Import all of the CA certificates from the issuer chain into the IBM HTTP Server truststore. You can import certificates in `Base64` and `DER` format.

   Consult your smart card vendor on how to get the smart card CA certificate.
4. Enable two-way SSL on the IBM HTTP Server through the IBM Integrated Solutions Console. See "Enabling two-way SSL" in the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.
5. If the smart card contains a separate certificate for signing and encryption, you must do additional configurations. See "Enabling smart card authentication" in the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.
6. Create a smart card policy template through the SetupAssistant in AccessAdmin.

   You must add smart card as an authentication factor.

See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for the detailed procedures.

Modes of smart card authentication

AccessAgent supports four modes of smart card authentication to cater to different customer requirements.

Configuration 1

This configuration is applicable for all platforms.

In this configuration, ESSO GINA and ESSO Credential Provider are enabled.

The user workflow for this configuration is as follows:

1. The user logs on with smart card to AccessAgent.
2. AccessAgent logs on the user to Windows with password.

This mode is suitable for a customer that does not have an enterprise PKI in place, but leverages on user smart cards like the national ID card, before granting access to Windows and various applications.

Configure the following settings:

SetupHlp.ini parameter	Value
EnginaEnabled	1
EncentuateCredentialProviderEnabled	1

AccessAdmin policy	Value
pid_sc_win_logon_enabled	false
pid_engina_ui_enabled	true
pid_second_factors_supported_list	smart card

Note:

- For the SetupHlp.ini parameter details, see *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.
- For the policy details, see *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide*.

Configuration 2

This configuration is applicable for Windows XP only.

In this configuration, ESSO GINA is enabled.

The user workflow for this configuration is as follows:

1. The user logs on with smart card to AccessAgent.
2. AccessAgent logs on the user to Windows with smart card.

This mode is suitable for a customer that has an Active Directory-based enterprise PKI in place, and enforces smart card authentication for both Windows and AccessAgent. The smart card must contain a Windows-compatible certificate that is issued by a CA that is trusted by the enterprise Active Directory.

Configure the following settings:

SetupHlp.ini parameter	Value
EnginaEnabled	1
EncentuateCredentialProviderEnabled	1

AccessAdmin policy	Value
pid_sc_win_logon_enabled	true
pid_engina_ui_enabled	true
pid_second_factors_supported_list	smart card

Note:

- For the SetupHlp.ini parameter details, see *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.
- For the policy details, see *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide*.

Configuration 3

This configuration is applicable for all platforms. It is suitable for deployments in Windows 7.

In this configuration, ESSO GINA and ESSO Credential Provider are enabled but are not visible. The `pid_engina_ui_enabled` policy is set to False.

The user workflow for this configuration is as follows:

1. The user logs on with smart card to Windows.
2. The user logs on with smart card to AccessAgent.

Configure the following settings:

SetupHlp.ini parameter	**Value**
EnginaEnabled	1
EncentuateCredentialProviderEnabled	1
EncentuateNetworkProviderEnabled	1

AccessAdmin policy	**Value**
pid_sc_win_logon_enabled	true
pid_engina_ui_enabled	false
pid_en_network_provider_enabled	true
pid_second_factors_supported_list	smart card

Note:

- For the SetupHlp.ini parameter details, see *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.
- For the policy details, see *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide*.

Configuration 4

This configuration is applicable for all platforms.

In this configuration, ESSO GINA and ESSO Credential Provider are not installed or enabled on user computers.

The user workflow for this configuration is as follows:

1. The user logs on with smart card to Windows.
2. The user manually logs on to AccessAgent from a Windows desktop.
3. AccessAgent automatically prompts the user for the smart card PIN.
4. The user needs to re-enter the smart card PIN to log on to AccessAgent.

Configure the following settings:

SetupHlp.ini parameter	**Value**
EnginaEnabled	0
EncentuateCredentialProviderEnabled	0

SetupHlp.ini parameter	Value
EncentuateNetworkProviderEnabled	1

AccessAdmin policy	Value
pid_en_network_provider_enabled	true
pid_second_factors_supported_list	smart card

Note:

- For the SetupHlp.ini parameter details, see *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.
- For the policy details, see *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide*.

Policies

The following table lists the sample policies that you can set for enforcing smart card authentication.

AccessAdmin policy	Description
pid_second_factors_supported_list	Set smart card as the second authentication factor.
pid_sc_win_logon_enabled	Specify whether to enable Windows smart card logon.
pid_engina_ui_enabled	Specify whether to enable the ISAM ESSO UI when Windows is logged off or locked.
pid_en_network_provider_enabled	Specify whether to enable Network Provider.
pid_sc_removal_action	Specify the action to be performed when a smart card is removed.
pid_wallet_authentication_option	Specify the combination of authentication factors that can be used for logon. • If the policy value contains both **Smart card** and **Password** then a user can log on to AccessAgent with either a smart card or the ISAM ESSO password. • If the policy value contains **Smart card** only then the user can log on with a smart card only.
pid_unlock_option	Specify who can unlock the computer.
pid_sc_map_cert_to_entdir_acc_enabled	Specify whether to enable automatic mapping of certificate to enterprise directory account during sign up.

See *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide* for more information about these policies.

Support scope and limitations

Familiarize yourself with the scope and limitations of the smart card authentication support.

- IBM Security Access Manager for Enterprise Single Sign-On uses the smart card in read-only mode. The user credential Wallet is not stored on the smart card.
- The credential Wallet is cached on the workstations protected by a keypair in the smart card.
- IBM Security Access Manager for Enterprise Single Sign-On does not provide card management facilities, such as changing the PIN of a smart card, personalizing, or unblocking a smart card.
- The users cannot log on with smart card in AccessAssistant.
- If the smart card certificate used for authentication is renewed by the PKI, the product treats the smart card as unregistered, and the user must register the smart card again.
- If more than one smart card are attached to the workstation, then AccessAgent cannot proceed to log on with smart cards.
- If the smart card authentication certificate is a private object such as the case in DNIe smart cards, then the following limitations apply:
  - Failed logon attempts because of wrong PIN entry is not recorded in the audit log.
  - In Windows Vista or Windows 7, Fast User Switching (FUS) triggered by inserting a different smart card does not work. A user must manually click the **Switch User** navigational link to trigger FUS.
  - ISAMESSO username is not shown in the AccessAgent PIN prompt screen.

Smart card revocation and expiry

You can terminate the use of a smart card as an authentication factor in two ways: Revoke the registered smart card or revoke the certificate.

Revoke the registered smart card registered from AccessAdmin

If a user tries to log on with the smart card, AccessAgent detects that the smart card is not registered. AccessAgent deletes any existing smart card credentials cached on the machine and informs the user that the smart card is not registered. The user might register the smart card again and provide the required credentials.

Revoke the certificate issued to the smart card

To check the revocation status of the smart card certificates, the IBM HTTP Server must be configured to check either the CRL or OCSP status. If the user tries to log on to AccessAgent with the revoked or expired smart card certificate, the SSL client authentication with IBM HTTP Server fails. In this case, AccessAgent deletes any existing smart card credentials cached on the machine and informs the user that the smart card cannot be authenticated. After this point, the user cannot use the smart card to log on to AccessAgent even if IBM HTTP Server is not reachable.

Only IBM HTTP Server can perform CRL/OCSP look up and checking the expiry. If the user has the smart card credentials cached on a machine and the IBM HTTP Server is not reachable, the user can log on to the machine even with a revoked or an expired certificate.

Hybrid smart card authentication

IBM Security Access Manager for Enterprise Single Sign-On supports the use of hybrid smart cards for user authentication in both personal and shared workstations.

How it works

Hybrid smart cards are made of embedded PKI microprocessor with contact interface and RFID chip with contactless interface. Users can log on and unlock the Windows desktop with a smart card without re-entering the smart card PIN within a configurable grace period. The grace period is measured from the last two-factor authentication time.

Outside the grace period, the user logs on with smart card and PIN through contact interface. Within the grace period, user can log on with smart card only through contactless interface across workstations. The logged on user can also unlock the Windows desktop with smart card only through contactless interface.

Note: The smart card PIN is not related to the ISAM ESSO password.

To use hybrid smart card authentication, the users must register the hybrid smart cards as secondary authentication factors.

Hybrid smart card tap same and tap different

Tap same

When the user taps the same hybrid smart card tapped during an AccessAgent session, the Windows desktop is locked. This behavior is configured through the smart card tap same machine policy.

Tap different

When a different hybrid smart card is tapped during an AccessAgent session, the previous user is logged off and the new user is logged on. This behavior is configured through the smart card tap different machine policy.

Requirements and compatibility

Hybrid smart card authentication support requires smart card middleware, a smart card, a smart card reader, and a smart card PIN. To know what middleware, card or reader is supported, check the requirements specification.

Requirements specification

The smart card, reader, and middleware must at least meet the following specifications:

Category	Requirements
Smart card middleware	• The smart card middleware can support the chosen smart card and the reader. • The smart card middleware exposes Microsoft CAPI interface to communicate with smart cards. AccessAgent accesses the smart card through this interface. • The Cryptographic Service Provider (CSP) implementing the CAPI interface can support the following functions: – Silent mode of operation so that it does not prompt the user for a smart card, or certificate selection, or PIN entry – Verification of the smart card PIN – Enumeration and reading of certificates from the smart card – Hashing and signing operations with the keypair that corresponds to the authentication certificate There is a *Smart Card PKCS#11 Cryptographic Service Provider* available for download at: http://www-01.ibm.com/support/docview.wss?uid=swg24026504. This is a Microsoft CAPI-compliant CSP that can be used to integrate with smart card middleware that exposes PKCS#11 APIs only. This Provider translates the MS-CAPI calls issued by ISAM ESSO into PKCS#11 calls to the native middleware libraries.
Smart card	• User card serial number must be unique and cannot be derived from any publicly available information about the user. • The smart card is an ISO 7816 compliant card. • The smart card can perform RSA cryptographic operations. • The smart card contains an RSA key pair and a corresponding X.509 certificate that is suitable for authentication. The certificate must allow the use of the key pair for client authentication and digital signatures • Private objects on the smart card, including private keys, must be protected by a PIN known to the user. • When queried for the Card Serial Number (CSN), the smart card must always return a consistent value. • The CSN must not be part of a private object.

Category	Requirements
Smart card reader	• The reader is compliant with the PC/SC standard. • The reader must have contact and contactless interfaces.

Supported middleware and devices

The following are the supported smart card, middleware, and reader:

Category	Requirements
Middleware	• Gemalto Classic Client v6
Readers	• Gemalto Prox-DU • OMNIKEY 5x21

Deployment

Learn how to deploy support for hybrid smart card authentication.

Road map

These are the main tasks to configure IBM Security Access Manager for Enterprise Single Sign-On to provide hybrid smart card authentication.

1. The hybrid smart card middleware and reader driver must already be installed on the computer. AccessAgent does not carry any drivers or middleware that might be necessary to support hybrid smart cards.
2. The IMS Server and AccessAgent must be installed before the hybrid smart card authentication support deployment.
3. Import all of the CA certificates from the issuer chain into the IBM HTTP Server truststore. You can import certificates in `Base64` and `DER` format.

   Consult your smart card vendor on how to get the smart card certificate.
4. Enable two-way SSL on the IBM HTTP Server through the IBM Integrated Solutions Console. See "Enabling two-way SSL" in the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.
5. You must do additional configurations if the hybrid smart card contains a separate certificate for signing and encryption. See "Enabling smart card authentication" in the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.
6. Create a hybrid smart card policy template through the SetupAssistant in AccessAdmin.

   Add hybrid smart card as an authentication factor.

See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for the detailed procedures.

Policies

Sample policies that you can set when enforcing hybrid smart card authentication.

AccessAdmin Policy	Description
pid_second_factors_supported_list	The second factors supported on this machine. This policy also controls the Wallet registration policy and imposes a constraint on the Wallet locks available for logon.
pid_sc_1f_logon_enabled	Whether to allow single factor smart card logon without PIN by a user who has recently logged on using smart card and PIN on the same or another computer. This policy applies if logon happens in the duration specified by the single factor smart card logon timeout.
pid_sc_1f_logon_timeout_mins	Time expiry, in minutes, for single factor smart card logon. After this duration, single factor smart card logon is not allowed.
pid_sc_1f_unlock_enabled	Whether to allow single factor smart card unlock without PIN by the same user who locked the computer, if unlock happens within a specified duration.
pid_sc_1f_unlock_timeout_secs	Time expiry, in seconds, for single factor smart card unlock. After this duration timed from last lock, single factor smart card unlock is not allowed.
pid_sc_1f_logon_extension_allowed	Whether to extend the time expiry for single factor smart card logon when user logs on with smart card and PIN before grace period expires.
pid_sc_present_same_action	Actions on presenting same smart card on desktop. This policy is effective only if the current user session starts with single factor smart card logon.
pid_sc_present_same_action_countdown_secs	Confirmation countdown duration, in seconds, for presenting the same smart card on the desktop.
pid_sc_present_different_action	Actions on presenting a different smart card on desktop. This policy is effective only if the current user session starts with single factor smart card logon. If a no-card serial number card is presented, it is considered to be a different card.
pid_sc_present_different_action_countdown_secs	Confirmation countdown duration, in seconds, for presenting a different smart card on the desktop

See the *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide* for more information about these policies.

Support scope and limitations

Familiarize yourself with the scope and limitations of the hybrid smart card authentication support.

In addition to the Smart card support scope and limitations, the hybrid smart card authentication support has the following limitations:

- Single-factor smart card logon requires a cached Wallet.

- Certificate associated with the CSN is not revalidated before single-factor authentication logon, and certificate revocation cannot be detected.
- EnGINA and Credential Provider must be enabled and visible.
- Smart card logon to Windows is not supported.
- If the certificate inside a registered smart card is replaced but the CSN remains the same, the smart card must be revoked from AccessAdmin before it can be registered with the new certificate.
- The user must always tap a hybrid smart card before inserting it into the reader.

RFID authentication

IBM Security Access Manager for Enterprise Single Sign-On supports the use of RFID cards for user authentication in both personal and shared workstations.

How it works

Users can log on, lock, and unlock AccessAgent with the following combinations, depending on the value you set for the Wallet authentication option policy:

- RFID only
- ISAM ESSO password and RFID

To use RFID authentication:

- The users must register the RFID card as a secondary authentication factor.
- The RFID card reader must be plugged into the computer before starting it. If the device is not detected upon startup, the users must restart their computers. Do not unplug and plug-in the RFID card reader while AccessAgent is running.

RFID only logon and RFID only unlock

RFID only logon

You can allow users who initially logged on to a workstation with their RFID card and password to log on or unlock any workstation with only their RFID card, but for the following conditions:

- Only for a pre-configured grace period after the initial two-factor logon.
- Only if they use the same card used for the two-factor logon earlier.
- Only from workstations where their credential Wallets are cached.
- Only if the workstation has network connection to the IMS Server.

In all other scenarios, users have to log on with both their RFID and passwords.

This feature is disabled by default and can be limited to a specific group of machines only.

RFID only unlock

You can allow users who initially logged on to a workstation with their RFID card and password, to unlock their workstation with their RFID card only but for the following conditions:

- Only within a pre-configured grace period.
- Only from workstations that users are currently logged on.

This feature is disabled by default and can be limited to a specific group of machines only.

RFID tap same and RFID tap different

These concepts apply when a user is logged on to an AccessAgent session, the screen is not locked, and an RFID card is tapped on to the reader.

RFID tap same
When the user taps the same RFID card that was previously tapped during an AccessAgent session. Use this configuration to set up a "tap in, tap out" workflow.

RFID tap different
When the user taps a different RFID card during an AccessAgent session. This configuration is applicable if the *userA* left the workstation unattended, and *userB* comes along and taps the RFID card to log on to the AccessAgent session.

When a different RFID card is tapped, the machine is locked and prompts for a password. If *fast user switching* is enabled, it triggers a user switch in Windows Vista and Windows 7. It depends on the policy value set by your organization.

Requirements and compatibility

RFID authentication support requires an RFID card middleware, an RFID card, and an RFID card reader.

Supported middleware and devices

The following are the supported RFID card readers. IBM Security Access Manager for Enterprise Single Sign-On supports RFID cards that are supported and compatible with these readers.

Reader	HID Prox Card	Indala Prox Card	Casi-Rusco Prox Card	Electronic Marin (EM) Prox Card	iCLASS Card	Legic RF Standard Card	Mifare Card (32 bit CSN)	Mifare Card (> 32 bit CSN)
GIGA-TMS Proximity Reader MFR135 (PCMCIA reader for Mifare cards) **Important:** This reader is not supported on Microsoft Windows Vista.	No	No	No	No	No	No	Yes	Yes
GIGA-TMS Proximity Reader PCR300MU (USB reader for Mifare cards)	No	No	No	No	No	No	Yes	Yes
Altrus Mifare Desktop Reader Writer A1MF (USB reader for Mifare cards)	No	No	No	No	No	No	Yes	Yes
RDR-60P2AKP	Yes	No	No	No	No	No	No	No
RF IDeas RDR-7172AKU	No	No	No	No	Yes	No	Yes	Yes

Reader	HID Prox Card	Indala Prox Card	Casi-Rusco Prox Card	Electronic Marin (EM) Prox Card	iCLASS Card	Legic RF Standard Card	Mifare Card (32 bit CSN)	Mifare Card (> 32 bit CSN)
RF IDeas RDR-7582AKU	No	No	No	No	Yes	No	Yes	Yes
RF IDeas RDR-6082AKU	Yes	No	No	No	No	No	No	No
RF IDeas BSE-PCPRXH-U	Yes	No	No	No	No	No	No	No
RF IDeas BSE-PCPRXH-232 (serial port reader)	Yes	No	No	No	No	No	No	No
RF IDeas RDR-6081AK2 (serial port reader)	Yes	No	No	No	No	No	No	No
RF IDeas BSE-RFID1356IUSB-ID	No	No	No	No	Yes	No	Yes	Yes
RF IDeas RDR-6E72AKU	No	No	No	Yes	No	No	No	No
RF IDeas BSE-PCPROXMU	No	Yes	No	No	No	No	No	No
RF IDeas BSE-OPLHU	Yes	No	No	No	No	No	No	No
RF IDeas RDR-6272-AKU	No	No	No	Yes	No	No	No	No
RF IDeas RDR-6072 BKU	Yes	No	No	No	No	No	No	No
RF IDeas RDR-7L82AKU	No	No	No	No	No	Yes	No	No
RF IDeas pcProx	Yes	No	No	Yes	No	No	Yes	No
RF IDeas AIR ID	No	No	No	Yes	No	No	No	No

IBM Security Access Manager for Enterprise Single Sign-On has a Service Provider Interface (SPI) for devices that contain serial numbers, like RFID. Use the SPI to integrate any device with serial numbers and use it as a second factor in AccessAgent. See the *IBM Security Access Manager for Enterprise Single Sign-On Serial ID SPI Guide*.

Deployment

Learn how to deploy support for RFID card authentication.

Roadmap

These are the main tasks to configure IBM Security Access Manager for Enterprise Single Sign-On to provide RFID card authentication.

1. Specify the reader in the DeploymentOptions registry file of the AccessAgent installer.
2. Install the RFID card device middleware and reader driver.

3. Install AccessAgent.
4. Define the RFID policies in AccessAdmin.

See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for the detailed procedures.

Policies

You can set the following sample policies when enforcing RFID authentication.

AccessAdmin Policy	Description
pid_rfid_tap_same_action	Actions to be performed by AccessAgent when the currently logged on user taps the RFID card on the desktop.
pid_rfid_tap_same_action_countdown_secs	Confirmation countdown duration, in seconds, for tapping same RFID on desktop.
pid_rfid_tap_different_action	Actions to be performed by AccessAgent when an RFID card is tapped on the desktop and does not belong to the currently logged on user.
pid_rfid_tap_different_action_countdown_secs	Confirmation countdown duration, in seconds, for tapping different RFID on desktop.
pid_rfid_only_unlock_enabled	Whether to allow RFID-only unlock (without password) by the same user who locked the computer, if unlock happens in the duration specified by pid_rfid_only_unlock_timeout_secs.
pid_rfid_only_unlock_timeout_secs	Time expiry, in seconds, for RFID-only unlock. After this duration (timed from last lock), RFID-only unlock is not allowed.
pid_rfid_only_logon_enabled	Whether to allow RFID-only log on (without password).
pid_rfid_only_logon_timeout_mins	Time expiry, in minutes, for RFID-only logon. After this duration (timed from last logon with RFID and password), RFID-only logon is not allowed.

See the *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide* for more information about these policies.

Active RFID (ARFID) authentication

IBM Security Access Manager for Enterprise Single Sign-On supports the use of Active RFID cards for user authentication in both personal and shared workstations.

How it works

Users can log on, lock, and unlock AccessAgent with the following combinations, depending on the value you set for the Wallet authentication option policy:

- ARFID only (for unlock only)
- ISAM ESSO password and ARFID

ARFID works almost the same way as a typical RFID card and it is used for both two-factor authentication and presence detection. ARFID has an RFID, and works with a proximity reader. However, ARFID differs from an RFID card in the

proximity range. With a typical RFID card, the card must be close to the reader. You can configure the proximity range for ARFID.

To use ARFID authentication, the users must register the ARFID cards as secondary authentication factors.

Requirements and compatibility

ARFID card authentication support requires an ARFID card middleware, an ARFID card, and an ARFID card reader.

Supported middleware

The following are the supported ARFID middleware, card, and reader:

Category	Requirements
Middleware	Ensure Tech ETSecure SDK 4.0
ARFID card and reader	XyLoc, XyLoc NL, XyLoc XC

Considerations

Note the following considerations when you are using the XyLoc Keys and Locks:

- The North American and European versions of the XyLoc Keys and Locks use different frequency ranges.
- North American Keys can work with North American Locks only.
- European Keys can work with European Locks only.
- North American versions are indicated with "FCC" on the Lock and "RF Band: North America" on the Key.
- European versions are indicated with "CE" on the Lock and "RF Band: Europe" on the Key.
- Water can significantly reduce the signal strength, and any body part might block the radio signal. For example, folding your arms over the Key, or walking away with your back facing the Lock.
- Do not place the Lock on or near metallic objects. Metallic objects can block or reflect the radio signal. If it must be placed on a metallic surface, it must be shielded with a thick non-metallic object.
- Cordless phones with a 900 MHz range in the U.S. might interfere with the North American version of XyLoc. Such interference might reduce the signal range significantly.
- Line of sight between Key and Lock is preferred for XyLoc to work optimally.
- Ensure Technologies specifies that the Lock and Key are placed at around the same level. If the Lock is mounted on the monitor, then the Key is around the upper part of the body.
- The battery lasts for 9 to 12 months on average. Keys issued before September 2006 have an average life span of one year. The age of the battery does not adversely affect signal strength. Battery tends to maintain a rather constant power throughout its life span until the final one or two weeks.
- The XyLoc Service has a logging feature that is useful for troubleshooting. The logs are stored in `C:\Program Files\Ensure Technologies\XyLoc`.

  Each data packet sent from any Key in the vicinity is logged. Each Key sends two packets per second, one from each antenna of each Key.

  The logs indicate the Key-ID, as well as signal strength received by the Lock.

You can set **Logging** to 1 in [HKEY_LOCAL_MACHINE\SOFTWARE\EnsureTechnologies\XyLoc] then stop and start the XyLoc Security System service.

Deployment

Learn how to deploy support for ARFID card authentication.

Roadmap

These are the main tasks to configure IBM Security Access Manager for Enterprise Single Sign-On to provide ARFID card authentication.

1. Install AccessAgent. Active RFID is automatically deployed.
2. If you install the SDK after you install AccessAgent, set up the service dependency manually.
3. Configure the Active RFID support in AccessAdmin.

See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* for the detailed procedures.

Policies

Sample policies that you can set when enforcing ARFID authentication.

AccessAdmin Policy	Description
pid_arfid_presentation_range_max	Maximum range for recognizing that an active proximity badge is presented.
pid_arfid_removal_range_min	Minimum range for recognizing that an active proximity badge is removed.
pid_rfid_only_unlock_enabled	Whether to allow RFID-only unlock (without password) by the same user who locked the computer, and in the duration specified in pid_rfid_only_unlock_timeout_secs.

See the *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide* for more information about these policies.

OTP and Mobile ActiveCode authentication

IBM Security Access Manager for Enterprise Single Sign-On supports the use of one-time passwords (OTP) and Mobile ActiveCodes (MAC) to authenticate users that logon to corporate VPN servers, AccessAssistant, or Web Workplace.

One-time password

One-time password is a randomly generated password, intended only for one user for a specific time and purpose and provided to the user either through SMS or an OTP token.

OTP is used as an authentication factor for users to log on to AccessAssistant or Web Workplace. OTP is also used for applications that use the IMS Server as the authentication server through RADIUS.

You use AccessAdmin to:

- Assign an OTP token to a user or revoke an OTP token from a user.
- Enable or disable authentication with an OTP token for an authentication service.

IBM Security Access Manager for Enterprise Single Sign-On supports the OATH HOTP algorithm and selected vendor-specific OTP algorithms. IBM Security Access Manager for Enterprise Single Sign-On supports the following devices:

- VASCO Digipass GO 3
- Authenex A-Key OATH-only token without USB interface (OATH-based OTP)

Authentication with OTP tokens is centrally logged in the IMS Server. Administrators or Helpdesk officers can view the audit logs through AccessAdmin, including logs reported by AccessAgent.

Mobile ActiveCodes

A Mobile ActiveCode is a randomly generated, event-based one-time password. The Mobile ActiveCode is generated on the IMS Server. The Mobile ActiveCode is delivered through a second channel, such as short message service (SMS) on mobile phones or through email.

The users can use Mobile Active Code to logon to the following applications:

- Applications supporting RADIUS, such as VPN Servers

  You must configure applications that support RADIUS to redirect the authentication to the IMS Server. Use this setup to have applications grant or deny access to users based on whether the OTP is successfully verified by the IMS Server.
- Web applications
- AccessAssistant or Web Workplace

Deployment

Learn how to deploy OTP or Mobile ActiveCode authentication support.

Roadmap for OTP authentication support

These are the main tasks to configure IBM Security Access Manager for Enterprise Single Sign-On to provide OTP authentication.

1. Upload the OATH files to the IMS Server.
2. Assign an OTP token to the selected user.
3. Set up the authentication service.
4. Configure the AccessAssistant and Web Workplace policies to use OTP.
5. Configure the machine, system, and user-related policies in AccessAdmin.

For the detailed procedures, see the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

Roadmap for MAC authentication support

These are the main tasks to configure IBM Security Access Manager for Enterprise Single Sign-On to provide MAC authentication.

1. Enable ActiveCode support in the IMS Server.
2. Configure the message connector.

3. Set up the authentication service.
4. Set selected user for Mobile ActiveCode authentication.
5. Configure the AccessAssistant and Web Workplace policies to use MAC.
6. Configure the machine, system, and user-related policies in AccessAdmin.

For the detailed procedures, see the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

Policies

You can set the following policies when enforcing OTP and MAC authentication.

Policy ID	Description
pid_accessanywhere_second_factor_default	Default second authentication factor for AccessAssistant and Web Workplace
pid_mac_max_validity_count	Maximum number of Mobile ActiveCodes that might be valid for a user at any time
pid_activecode_bypass_option	ActiveCode bypass option
pid_otp_append_secret_option	Option for appending a secret to OTP (time-based) and OTP (OATH)
pid_otp_reset_sample_count	Number of consecutive OTPs needed for resetting an OTP (OATH) token
pid_auth_authentication_option	Authentication modes to be supported
pid_mac_auth_enabled	Enable Mobile ActiveCode authentication?

See the *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide* for more information about these policies.

Authorization code authentication

An authorization code is a system-generated code used as an authentication factor for specific scenarios. There are two types of authorization code: online authorization code and offline authorization code.

An Administrator or Helpdesk can:

- Issue authorization codes through AccessAdmin. If the self-service authorization code feature is deployed, user can request for an authorization code through a mobile phone (SMS).
- Revoke the last-issued authorization code through AccessAdmin. However, the revocation prevents the user from reusing the same authorization code.

Online authorization code

Use this code if AccessAgent can connect to the IMS Server. The user can use the code several times until the code expires. The minimum code expiry is one day.

The online authorization code is used for:

- **Online password reset**

  AccessAgent asks the user for an authorization code and a secret.
- **Registration of authentication factor**

AccessAgent asks for the authorization code and password for the registration of the second authentication factor device of a particular kind.

- **Temporary bypass of authentication factor**

  An authorization code is required as a temporary replacement when the user has forgotten or lost the authentication factor or the device reader is not working or is missing.

  A temporary password-only lock is created for the Wallet on the computer. This temporary password-only lock expires when the authorization code expires. As such, the user can log on to the Wallet by just providing the user name and password until the authorization code expires.

Using the IMS Configuration Utility, you can:

- **Configure the length of the authorization code.**

  The code has a default of 12 characters and can have a maximum of 32 characters. Use the character set: `0123456789ABCDEF` for an online authorization code. The code is not case sensitive and any hyphens entered are ignored.
- **Configure the validity period.**

  The available options are at least one day and a maximum of 31 days. One month is the period from the issue date to the same day of the next month. The exact number of days depends on the month of issue. For example: From August 26 2012, 3 p.m. to September 26 2012, 3 p.m.

Offline authorization code

Use this code if AccessAgent cannot connect to the IMS Server. The user can use the offline authorization code once because the code is issued based on the request code that is displayed on AccessAgent.

The user must have a cached Wallet to use an offline authorization code.

The offline authorization code is used for

- **Temporary password reset**

  AccessAgent asks the user for an authorization code and a secret.
- **Temporary bypass of authentication factor**

  For example, the user lost the second authentication factor and cannot log on to AccessAgent because the Wallet authentication policy requires the second authentication factor. If the user clicks **but I do not have**, AccessAgent asks for an authorization code as a temporary replacement for the second factor.

  A temporary password-only lock is created for the Wallet on the computer. This temporary password-only lock expires when the authorization code expires. As such, the user can log on to the Wallet by just providing the user name and password until the authorization code expires.

You have the following options:

- Offline authorization codes are 16 characters long. Request codes are eight characters long and the codes change every minute.

  The default character set for both the request code and authorization code is `Z3467ACEFHJKRWXY`. The code is not case sensitive and any hyphens entered are ignored.
- Configure the validity period through AccessAdmin.

  The available options are at least one day and a maximum of 31 days. One month is the period from the issue date to the same day of the next month. The

exact number of days depends on the month of issue. For example: From August 26, 2011, 3 p.m. to September 26, 2011, 3 p.m.

Deployment

Learn how to implement the use of authorization codes.

Roadmap

These are the main tasks to configure IBM Security Access Manager for Enterprise Single Sign-On to use authorization code for authentication.

1. Enable the use of authorization code authentication in the IMS Server.
2. Set the authorization code expiration date.
3. Set the length of the authorization code, in characters.
4. Set the validity of the authorization code, in days.
5. Configure the AccessAssistant and Web Workplace policies to use authorization codes.
6. Configure the machine, system, and user-related policies in AccessAdmin.

For the detailed procedures, see the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

Policies

You can set the following policies when enforcing authorization code authentication.

AccessAdmin Policy	Description
pid_accessanywhere_second_factor_default	The default second authentication factor for logging on to AccessAssistant and Web Workplace
pid_selfhelp_authcode_enabled	Whether to enable self-service authorization code issuance using a mobile phone.
pid_selfhelp_authcode_request_from_any_phone_enabled	Whether to allow self-service authorization code to be requested from any phone.
pid_selfhelp_authcode_invalid_trial_count_max	The maximum number of invalid tries allowed before self-service authorization code request locks out

See the *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide* for more information about these policies.

Presence detectors

IBM Security Access Manager for Enterprise Single Sign-On supports the use of presence detectors to provide additional security to the user workstation.

A presence detector is a device that detects the presence of the user within its vicinity. When affixed to a computer, the device can notify AccessAgent when a user is in front of the computer or when the user moves away. A presence detector device eliminates the effort of manually locking the computer when the user leaves the computer for a short time.

Sonar devices

The sonar-based presence detector is used to immediately lock the computer when the user walks away without waiting for the desktop inactivity timeout. IBM Security Access Manager for Enterprise Single Sign-On supports the sonar-based presence detector *RF IDeas pcProx-Sonar BSE-PCPRXSNR pcProx-Sonar*.

The difference between Active RFID and the *pcProx-Sonar* is that an Active RFID has a unique ID that you can use to identify a user. You cannot use the pcProx-Sonar to identify a user because the pcProx-Sonar does not have an ID.

The device is attached to the USB port of the computer and is configured by the system as a keyboard. When the user moves away from the computer, the device sends keystrokes to the computer.

You can set AccessAgent to intercept these keystrokes and perform appropriate actions. For example, lock the computer. When the user approaches the computer, the device sends a different set of keystrokes to the computer. The device uses 40 kHz ultrasonic sound waves and can detect from a range of 5 inches to 5 feet. The user can move in the zone without triggering a walk away event.

Sonar devices can be combined with the following authentication factors:

- Password only
- RFID
- Fingerprint
- Smart card

You cannot combine this device with an Active RFID because it is also a presence detector.

Active RFID presence detector

Active RFID is both a second authentication factor and a presence detector because Active RFID detects the presence of a user.

You can configure AccessAgent to perform specific actions when using an Active RFID.

Chapter 11. Session management

IBM Security Access Manager for Enterprise Single Sign-On supports session management in personal workstations and shared workstations.

Personal workstations

The personal workstation configuration is more applicable for organizations where users are assigned their own workstations. These workstations are not shared with any other users.

A personal workstation configuration supports all authentication factors that AccessAgent supports.

Shared workstations

The shared workstation configuration is applicable for organizations where users share common workstations. For example, health care organizations where doctors and nurses share workstations that are deployed throughout the hospital.

Shared workstations support the following desktop modes:

- "Shared desktops"
- "Private desktops" on page 119

IBM Security Access Manager for Enterprise Single Sign-On supports user switching through any of these shared workstation desktop modes.

This configuration supports all authentication factors that AccessAgent supports.

Shared desktops

Shared desktops are one of the supported shared workstation modes. In a shared desktop mode, multiple users share a generic Windows desktop in one workstation. Enable ESSO GINA (for Windows XP) or ESSO Credential Provider (for Windows Vista and Windows 7) to use shared desktop mode.

In this mode:

- On startup, the user is automatically logged on to Windows with a generic Windows account and the screen is automatically locked.
- The users see the ESSO GINA lock screen instead of the MSGINA.
- The users authenticate through ESSO GINA to unlock the Windows desktop.
- Switching of users is faster because there is no need to logoff and re-logon to Windows whenever a different user unlocks into the desktop.

In this mode, after switching from *User A* to *User B*, the applications of *User A* remains open for *User B* unless those applications were closed prior to user switching. You can create AccessProfiles to automatically log off the enterprise applications when user switching occurs.

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

Configuring shared desktops

Implementing shared desktop mode involves the configuration of Windows settings and the configuration of system, machine, and user policies in AccessAdmin.

Windows configuration

The users can either have an Active Directory account or a local Windows account. Create a local Windows account if there is no Active Directory account.

These steps are generally performed by corporate Active Directory administrators. You are responsible for collaborating with them to ensure that the Windows configuration steps are in place before you begin configuring the shared desktop in AccessAdmin.

1. Create a domain user to be used for automatic logon to Windows.
2. Restrict the user rights by setting proper group membership and domain-level restrictions on applications, files, and services.

   Use the Global Policy Object editor to define the shared Windows account privileges. For example:

   - Restrict what users can see on the Start menu.
   - Do not allow logoff through the Start menu and **Ctrl+Alt+Del** sequence.

   For more information about applying policy settings for the Start menu in Windows, go to the Microsoft web site at http://www.microsoft.com. Search for "Policy settings for the Start menu".
3. Edit the registry on the shared workstation to enable automatic logon to Windows for the shared user.

   For more information about how to enable automatic logon for Windows, go to the Microsoft web site at http://www.microsoft.com. Search for "How to turn on automatic logon".

AccessAdmin configuration

After configuring the necessary Windows settings, you must configure IBM Security Access Manager for Enterprise Single Sign-On shared desktop settings in AccessAdmin. You can use the Setup Assistant.

You can set the following sample policies when you configure a shared desktop.

Note: Policy marked with (*) is a required configuration.

AccessAdmin policy	Description
pid_unlock_option	Unlock computer policy for controlling who can unlock a computer when it has been locked by a user who is logged on to AccessAgent.
pid_win_startup_action	Actions on Windows startup.
pid_win_fast_user_switching_enabled	Whether to enable support for Fast User Switching in Microsoft Windows Vista and later versions.
pid_fast_unlock_enabled	Whether to allow AccessAgent to perform unlock without performing any checks with the IMS Server.

AccessAdmin policy	Description
pid_engina_winlogon_option_enabled	Whether to enable the option to go to Windows logon directly from EnGINA.
pid_en_network_provider_enabled	Whether to enable the Network Provider.
pid_logoff_manual_enabled	Whether to allow user to manually log off from AccessAgent.
pid_logoff_manual_action	Actions to be performed by AccessAgent on manual logoff by the user.
pid_background_auth_enabled_option	Option to specify if AccessAgent must perform authentication with IMS Server in the background.
pid_background_auth_retry_mins	Time interval, in minutes, to initiate background authentication if AccessAgent cannot connect to IMS Server.

See *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide* for more information about these policies.

Private desktops

Private desktop is one of the supported shared workstation modes. In a private desktop mode, users have their own Windows desktop in a workstation. The private desktop is only visible to the individual user. No other user can view it. If the user copies anything into the clipboard from one desktop, the user cannot paste it into another desktop.

IBM Security Access Manager for Enterprise Single Sign-On supports private desktop mode in:

- Windows XP with the ESSO Desktop Manager
- Windows Vista and Windows 7 using the Windows native fast user switching feature

Private desktop mode is only available if ESSO GINA (for Windows XP) or ESSO Credential Provider (for Windows Vista and Windows 7) is enabled.

Private desktop for Windows XP

The private desktop mode on Windows XP is implemented by the *ISAM E-SSO Desktop Manager (EDM)* module in AccessAgent.

When a new user logs on from the ISAM ESSO logon screen, EDM verifies that the user is a valid user.

- If Active Directory password synchronization is enabled, EDM can use the Active Directory credentials to create the private Windows desktop for the user.
- If Active Directory password synchronization is not enabled, EDM cannot assume that the Active Directory credentials stored in the user Wallet are authentic or up-to-date. As such, EDM has to rely on the generic Windows accounts that are configured in the computer Windows registry to create individual desktops.

Access to each user desktop is protected by Windows access control. As long as each user account does not have administrative rights on the computer, it is not possible for a user to access data of other users. The EDM is designed to prevent malicious software or some other desktop management software from switching

from current desktop to another user desktop. If a third-party software performs desktop switching, AccessAgent locks the workstation.

Changes in behavior

If you are using private desktop mode in Windows XP, some Windows functions are disabled or replaced.

- **Log Off** and **Shut Down** buttons in the Start menu are not enabled for all user desktops. To log off, right-click AccessAgent or press **Ctrl+Alt+Delete** to activate ESSO GINA.

  Complete the following steps to re-enable these functions:

  – For the **Log Off** button, set the registry value `[HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\Windows\CurrentVersion\policies\ Explorer]"StartMenuLogoff"` to `0`.

  – For the **Shut Down** button, set the registry value `[HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer]"NoClose"` to `0`.

- The Microsoft Windows Security dialog that is launched by pressing **Ctrl+Alt+Delete**, is replaced by ESSO GINA.

  Using this dialog, you can lock your computer, log off from the computer, shut down your computer, and launch the Task Manager.

- The **Change password** option is not available.

  You can change your ISAM ESSO password or Active Directory password if these two passwords are synchronized. Right-click **AccessAgent** and choose **Change password**.

- The following Windows key combinations are disabled:

  – WIN + B
  – WIN + D
  – WIN + E
  – WIN + F
  – WIN + M
  – WIN + R
  – WIN + TAB
  – WIN + PAUSE

  Note: To enable the Windows hot keys, set the registry value `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\ Explorer]"NoWinKeys"` to `0`.

Limitations

- There is no **Reset password** link option in the ESSO GINA logon screen.
- Single Sign On to Windows Explorer is not supported.
- Some Windows user configuration settings like screensaver configuration must be configured from the default account desktop for it to be effective.
- AccessAgent can hold a maximum number of four sessions in private desktop with generic account enabled.

Configuring private desktops for Windows XP

Implementing private desktop for Windows XP involves the configuration of Windows settings and the configuration of system, machine, and user policies in AccessAdmin.

Windows configuration

Enable auto-admin logon to Windows. See http://support.microsoft.com/kb/310584.

If Active Directory is used, enable password synchronization so that EDM can use the enterprise Active Directory credentials to create the private Windows desktop for the user.

If there is no Active Directory, enable the user of the generic account to create user desktop.

AccessAdmin configuration

After configuring the necessary Windows settings, you must configure IBM Security Access Manager for Enterprise Single Sign-On private desktop for Windows XP settings in AccessAdmin. You can use the Setup Assistant.

You can set the following sample policies when you configure a private desktop for Windows XP.

Note: The policy marked with (*) is a required configuration.

AccessAdmin policy	Description
pid_lusm_sessions_max	*Maximum number of concurrent user sessions on a workstation (for Windows XP)
pid_lusm_generic_accounts_enabled	Enable use of generic accounts to create user desktops? (for Windows XP)
pid_lusm_auto_logon_acct_display_enabled	Enable display of auto-admin logon account in logon user interface? (for Windows XP)
pid_lusm_session_replacement_option	Session replacement option (for Windows XP)
pid_lusm_sia_list	Single instance applications list (for Windows XP)
pid_lusm_sia_launch_option	Action on launching a second instance of a single instance application (for Windows XP)
pid_wallet_logoff_action_for_apps_default	Default action for applications, when user logs off AccessAgent
pid_app_wallet_logoff_action	Action for the application, when user logs off AccessAgent
pid_fast_unlock_enabled	Enable fast unlock without IMS check
pid_win_startup_action	Windows startup actions
pid_desktop_inactivity_action	Desktop inactivity actions
pid_unlock_option	Unlock computer policy
pid_wallet_authentication_option	Wallet authentication policy

See *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide* for more information about these policies.

Private desktop for Windows Vista and Windows 7

The private desktop mode on Windows Vista and Windows 7 is implemented on top of the Windows Fast User Switch (FUS) feature.

Changes in behavior

Changes in behavior for private desktop on Windows Vista and Windows 7:

- You do not need to specify the maximum number of concurrent user sessions on a workstation. IBM Security Access Manager for Enterprise Single Sign-On leverages on Windows Vista and Windows 7 to control the number of active concurrent user sessions.
- On Windows Vista and Windows 7, Microsoft fast user switching compatibility service can be used to handle applications that cannot run in a multiple-user environment.
- Use of generic accounts is not supported because Windows Vista and Windows 7 fast user switching requires actual user accounts.
- Active Directory Group Policies Objects (AD GPO) in private desktops are applied automatically.

Configuring private desktops for Windows Vista and Windows 7

Implementing private desktop for Windows Vista and Windows 7 involves the configuration of Windows settings and the configuration of system, machine, and user policies in AccessAdmin.

AccessAdmin configuration

After configuring the necessary Windows settings, configure the IBM Security Access Manager for Enterprise Single Sign-On private desktop settings in AccessAdmin.

You can set the following sample policies when you configure a private desktop for Windows Vista and Windows 7.

Note: The policy marked with (*) is a required configuration.

AccessAdmin policy	Description
pid_win_fast_user_switching_enabled	*Enable support for Windows Fast User Switching?
pid_desktop_inactivity_action	Desktop inactivity actions

See *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide* for more information about these policies.

Chapter 12. AccessAgent on Citrix/Terminal Servers

IBM Security Access Manager for Enterprise Single Sign-On supports single sign-on and authentication services for applications hosted on *Citrix/Terminal Servers* – Citrix XenApp Servers or Microsoft Remote Desktop.

You must install AccessAgent on each *Citrix/Terminal Server*.

For every remote session on *Citrix/Terminal Server*, there is an AccessAgent instance running to help users single sign-on to their applications on the particular remote session. Users can later connect to the same remote session on the *Citrix/Terminal Server* through any client computer.

See the following topics:

- "Planning for installation of AccessAgent on Terminal Service or Citrix clients" on page 62
- "Standard mode and lightweight mode"
- "Deployment setup and configuration policies" on page 125
- "Deployment model selection guidelines" on page 126
- "Model 1: Basic configuration" on page 127
- "Model 2: Virtual channel connector configuration" on page 128
- "Model 3: Generic Terminal Session" on page 130
- "Model 4: Two-tier AccessAgent configuration" on page 131

Before you begin

The type of deployment model that you can choose from depends on your following considerations:

- Are you using Microsoft Remote Desktop Services (Terminal Services)[1] or Citrix XenApp Servers?
- Is Active Directory password synchronization enabled?
- Are you using thin clients, workstations, or both?
- Are you using two-factor authentication?

After you determine your combination of deployment factors, decide whether to enable any of the following options for the Server AccessAgent:

- ESSO GINA
- ESSO Network Provider
- Virtual channel connector

Standard mode and lightweight mode

AccessAgent installed on a Citrix/Terminal Server can run in *standard mode* or in *lightweight mode*.

1. On Windows Server 2003, Microsoft Remote Desktop Services is known as Terminal Services.

Running in lightweight mode can reduce the memory footprint of AccessAgent on a Citrix/Terminal Server and can improve the single sign-on startup duration. If you are using Citrix XenApp Server, the lightweight mode feature requires integration and support from IBM partners if the virtual channel is installed.

For a Citrix Server, if virtual channel connector is installed, and the ESSO GINA is disabled, lightweight mode is automatically enabled when the user is logged on to the Client AccessAgent.

On a Terminal Server, the virtual channel connector is automatically installed.

See the following table for a comparison of the two AccessAgent modes.

Features	Standard Mode		Lightweight mode
	Standard mode (without virtual channel)	**Standard mode (with virtual channel)**	
Performance	Normal	Normal	Better
User experience	Log on to Server AccessAgent is through EnGINA or Network Provider	Automatic log on to Server AccessAgent with Client AccessAgent credentials	Automatic log on to Server AccessAgent with Client AccessAgent credentials
Supported authentication factors	Not applicable	RFID	All authentication factors
Synchronize changes between Client AccessAgent and Server AccessAgent	No	Yes	Yes
AccessAgent Wallet cached on the Server	Yes	Yes	Never
Behavior of AccessAgent when users log on and log off.	Depends on GINA or Network Provider.	Log off remote AccessAgent and disconnect remote session.	Disconnect remote session

You can enable or disable lightweight mode with the **TSLightweight Mode** policy if virtual channel is installed.

TSLightweight Mode policy value	Description
0	• Disables lightweight mode. • The Server AccessAgent operates only in standard mode.
1	• Enables lightweight mode. • The Server AccessAgent operates in lightweight mode.
2	• Enforces lightweight mode. • The Server AccessAgent always operates in lightweight mode. The session in the Server AccessAgent does not start if there is no Client AccessAgent.

The Server AccessAgent mode varies depending on the version of the Client AccessAgent, Server AccessAgent, and the configured **TSLightweight Mode** policy value.

If you are using earlier versions of AccessAgent in your deployment, or if you are using thin clients, see the following table:

Client AccessAgent version	Server AccessAgent version	TSLightweight Mode policy value	Server AccessAgent mode
8.2	8.1 or earlier	Not applicable	Standard mode
8.1 or earlier	8.2	0, 1	Standard mode
8.1 or earlier	8.2	2	Not a supported configuration
Thin client or no AccessAgent	8.2	0, 1	Standard mode
Thin client or no AccessAgent	8.2	2	Not a supported configuration

Note:

- If ESSO GINA is enabled on Server AccessAgent, it is always in *Standard mode*.
- For console logons, Server AccessAgent mode is always in standard mode.
- For Server AccessAgent in standard mode, autologon to the Server AccessAgent works only for password-only or RFID and password logon at the client.
- When running in lightweight mode, there is no AccessAgent logon at the server. It works with any second authentication factor.

Deployment setup and configuration policies

The single sign-on experience on a Citrix/Terminal Server varies, depending on how you deploy AccessAgent and on the policies you configure.

Ways of deploying AccessAgent

You have the following setup options:

- Install AccessAgent on the Citrix/Terminal Server only (Server AccessAgent).
- Install AccessAgent on the client computer (Client AccessAgent) and on the Citrix/Terminal Server.
- Install AccessAgent on the client computer (Client AccessAgent) and on the Citrix/Terminal Server but use *Lightweight mode* (with virtual channel).

The AccessAgent installation program detects the Citrix/Terminal Server and it installs the required components.

If you have AccessAgent on the client computer, configure AccessAgent so that the user can automatically log on to the Citrix/Terminal Server session with a single sign-on AccessProfile.

For a Terminal Server deployment, the Server AccessAgent is automatically configured to communicate with the Client AccessAgent. For a Citrix Server deployment, you must manually configure the Server AccessAgent to communicate with the Client AccessAgent. You need a virtual channel connector. See the *IBM*

Security Access Manager for Enterprise Single Sign-On Lightweight AccessAgent mode on Terminal Server SDK Guide for information about developing a virtual channel connector.

Ensure that both AccessAgents connect to the same IMS Server to synchronize the credentials, Wallet changes, logon, and logoff events.

For standard mode only, the synchronization of Wallet contents depend on both the Client AccessAgent and ability of the Server AccessAgent to connect to the IMS Server. If one of the AccessAgent installations cannot connect to the IMS Server, the Client AccessAgent and Server AccessAgent do not have a consistent view of the Wallet if there are any changes.

Configuration policies

You can customize the Windows desktops or application logon experience hosted on the Citrix/Terminal Servers through these policies:

- Enable auto-launching of ESSO AccessAgent screen.
- Use ESSO GINA when there is no Client AccessAgent session.
- Log off Server AccessAgent when reconnecting from a computer without Client AccessAgent.
- Enable or disable:
  - ESSO Network Provider.
  - Two-factor authentication in Client AccessAgent.
  - ESSO GINA on the client or server.

When using RFID authentication from a thin client, you can enable these settings:

- COM port redirection
- Virtual COM port on Terminal Server
- Physical COM port on client computer

Deployment model selection guidelines

Use the following guidelines to help you select the best deployment model for a Terminal Services environment.

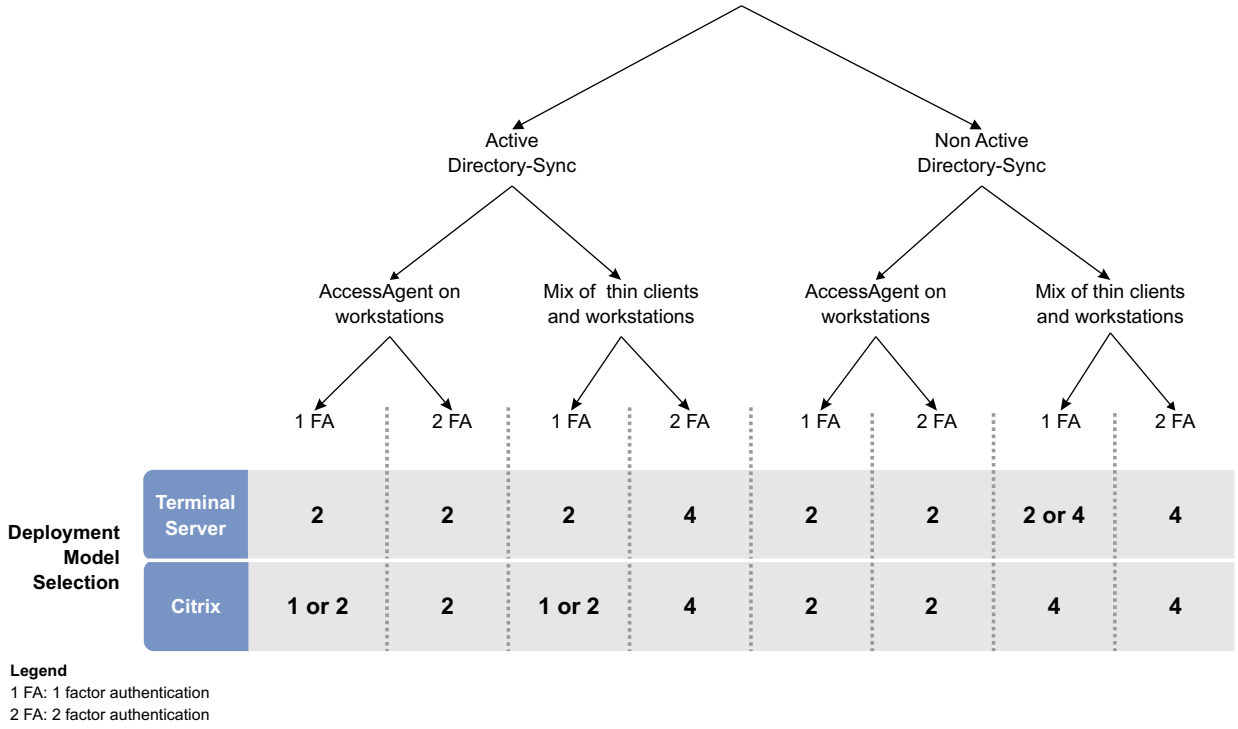

Figure 10. Deployment model selection guidelines on Terminal Server/Citrix environments.

To select the best deployment model for a terminal services environment, identify your terminal service requirements. Identify the single sign-on requirements for thin clients or workstations, directory services, and the type of authentication factors you expect to deploy in a Terminal Services environment.

After you choose a deployment model, complete the configuration tasks for the model:

- "Model 1: Basic configuration"
- "Model 2: Virtual channel connector configuration" on page 128
- "Model 3: Generic Terminal Session" on page 130
- "Model 4: Two-tier AccessAgent configuration" on page 131

Model 1: Basic configuration

A basic configuration consists of a Server AccessAgent without GINA and an enabled Network Provider. In this configuration, the Server AccessAgent automatically logs on the user in to the Wallet upon logon to the Citrix/Terminal Server remote session.

When there are Wallet changes on either the Client AccessAgent or Server AccessAgent, these changes are not immediately synchronized between the Client AccessAgent and Server AccessAgent.

Terminal Server configuration

To deploy a basic Citrix/Terminal Server configuration, configure the Citrix/Terminal Server and the terminal session settings.

Complete the following tasks:

- Configure the Citrix/Terminal Server to accept Active Directory credentials from the terminal client.

  If disabled, the user sees the remote MSGINA and logs on to the Citrix/Terminal Server through MSGINA.
- Configure the terminal session to roam if Active Directory credentials are not shared.
- Configure the terminal session to disconnect upon inactivity timeout.

ESSO configuration

To deploy a basic Citrix/Terminal Server configuration, configure the ESSO GINA, ESSO Network Provider, and user authentication policy.

This configuration is applicable when Active Directory password synchronization is enabled.

Complete the following tasks:

- Disable ESSO GINA for Server AccessAgent.
- Enable ESSO Network Provider for Server AccessAgent.
- If required, enforce two-factor authentication by setting the user authentication policy at AccessAdmin.

  In this model, two-factor authentication policy is only enforced at Client AccessAgent. Logon to Server AccessAgent remains password-only. Two-factor authentication cannot be enforced for thin clients.

Model 2: Virtual channel connector configuration

In this configuration, Server AccessAgent connects to the Client AccessAgent through a virtual channel, to retrieve the user credentials and authenticate the user.

Virtual channel connector configuration is the default configuration for Terminal Server deployments but not for Citrix. The Citrix virtual channel connector is not bundled with the product. The virtual channel between the Client AccessAgent and the Server AccessAgent is built on top of the virtual channel SDK from Citrix or Microsoft.

If you are using Microsoft Windows Terminal Services, this integration is implemented and available out-of-box. If you are using Citrix XenApp, use the virtual channel SDK from Citrix. On-site integration work and support from IBM partners is required. The client-side and server-side virtual channel connectors must be co-deployed with the respective AccessAgent installations at the client and server ends.

See *IBM Security Access Manager for Enterprise Single Sign-On Lightweight AccessAgent mode on Terminal Server SDK Guide*.

In this configuration, you can set Server AccessAgent to run in *lightweight mode*. To run *lightweight mode*, disable ESSO GINA. To enforce two-factor authentication in AccessAgent, you must disable the Network Provider. To learn more about standard and lightweight modes, see “Standard mode and lightweight mode” on page 123.

When the Client AccessAgent is locked or when a user is logged off, the Server AccessAgent can do any of the following actions:

- Log off the user from the Server AccessAgent.
- Disconnect or log off the user from the remote session.
- Log off the user from the Server AccessAgent and disconnect or log off the user from the remote session.

When a user reconnects to an existing remote session in the Server AccessAgent, the Server AccessAgent status is updated based on the connecting Client AccessAgent.

Terminal Server configuration

To deploy a virtual channel connector configuration, configure the Citrix/Terminal Server and the terminal session settings.

Complete the following tasks:

- Configure the terminal session to roam if Active Directory credentials are not shared.
- Configure the terminal session to disconnect upon desktop inactivity timeout.

ESSO configuration

To deploy a virtual channel connector configuration, you must also configure the ESSO GINA, ESSO Network Provider, and user authentication policy.

Complete the following tasks:

- Disable ESSO GINA.
- Disable ESSO Network Provider for Server AccessAgent when all users access Citrix/Terminal Server from workstation machines.
- Enable ESSO Network Provider for Server AccessAgent when:
  - users access Citrix/Terminal Server from a mix of workstations and thin client machines
  - users access Citrix/Terminal Server from these machines where two-factor authentication is not enforced

  In this case, users from thin clients log on to Server AccessAgent through the ESSO Network Provider, and does not use the Virtual Channel. In this scenario, the Server AccessAgent operates in *standard mode*.
- If two-factor authentication policy for user is enabled, two-factor authentication is enforced at the Client AccessAgent and effectively enforced at the Server AccessAgent. The assumption is that the ESSO Network Provider is disabled. The user can log on to the Server AccessAgent only if the user has already logged on with two-factor authentication in to the Client AccessAgent.

  However, logon to terminal session is based only on the Active Directory password of the user.

  Two-factor authentication cannot be enforced at all if thin clients are involved. In this case, users from thin client machines must log on to the Citrix/Terminal Server and the Server AccessAgent with Active Directory passwords. Make sure that Active Directory password synchronization and the ESSO Network Provider are enabled.

Model 3: Generic Terminal Session

A generic terminal configuration consists of a Server AccessAgent deployed on a generic terminal session. This configuration is intended for thin client users. A *generic desktop session* is hosted on a dedicated tier of the Citrix/Terminal Server. Different users can share access to applications hosted in the remote session from a thin client machine.

In this configuration, thin client machines are constantly connected to the remote terminal session that is logged on to a generic low-privileged Active Directory account. Server AccessAgent is configured to run in Shared Desktop mode on each terminal session. Users unlock into the terminal session by logging in through the Server AccessAgent ESSO GINA.

This configuration is useful for scenarios where:

- Applications are active in each terminal session because of long startup times
- AccessAgent automatically logs on and logs off different users from applications.

In this configuration, the users can unlock the remote session and log on to a Wallet with either a password or an RFID card.

Terminal Server configuration

To deploy single sign-on services on a generic terminal session, configure the Citrix/Terminal Server and the terminal session.

Complete the following tasks:

- Configure the terminal client session to roam if Active Directory credentials are not shared.
- Configure the terminal client session to disconnect upon desktop inactivity timeout.
- Configure the generic terminal server to automatically log on to the Citrix/Terminal Server with an Active Directory credential.
- Enable serial port redirection at the thin client and target terminal server only if you are using RFID as the authentication factor.

ESSO configuration

To deploy single sign-on services on a generic terminal session, you must also configure the ESSO GINA, ESSO Network Provider, and user authentication policy.

Complete the following tasks:

- Enable ESSO GINA.
- Disable ESSO Network Provider at Server AccessAgent.
- Enable shared desktop mode at Server AccessAgent.
- If required, enable RFID authentication.
- If RFID authentication is enabled, enforce two-factor authentication by setting the user authentication policy at AccessAdmin.
- Enable ESSO GINA log on when there is no Client AccessAgent session.

Generic terminal server configurations

Use the following settings to configure the generic terminal server in a terminal services deployment with generic terminal sessions.

The following settings are the required *generic terminal server* configurations to implement this mode. These terminal servers are dedicated to serve thin client machines only.

- Configure the terminal server to automatically log on to the Citrix/Terminal Server with a single designated low-privilege generic Active Directory credential.
- Configure the terminal server to allow unlimited terminal sessions for the generic Active Directory credential.
- Do not enable roaming for the terminal client session. If an idle session has timed out, the desktop screen must be locked.
- Enable serial port redirection at the thin client and terminal server.

Thin client configuration

Use the following settings to configure the thin clients in a terminal services deployment with generic terminal sessions.

The following are the required thin client configuration to implement this mode:

- Configure the thin client to automatically log on to the *Citrix/Terminal Server* with a single designated low-privilege generic Active Directory credential. This is the same account as the one setup for auto-logon on the generic Terminal Server.
- Thin client users can use RFID only as the second authentication factor.

Limitations

Consider the following limitations of single sign-on in a terminal services deployment with generic terminal sessions.

To implement this configuration:

- You need a dedicated tier for the Citrix/Terminal Server.
- The underlying Windows session uses a generic Active Directory account.
- For two-factor authentication, only thin clients and RFID readers that support serial port redirection have been tested.
- You must enable COM port redirection to enable two-factor authentication at the thin client.
- Only RFID can be used as a second authentication factor device.
- This configuration is applicable for shared desktop mode only.
- The terminal session cannot roam.

Model 4: Two-tier AccessAgent configuration

A two-tier AccessAgent configuration is a combination of using a virtual channel and a generic remote desktop. This configuration is intended for deployments that require mixed-client two-factor authentication.

Two-tier AccessAgent configuration involves two terminal servers.

- *Generic terminal server* for those using thin clients
- *Target terminal server* for those using workstations

Users can roam between workstations and thin clients and do a second authentication at either clients.

Generic terminal server hosts a generic remote desktop. Use the generic remote desktop to allow thin client users to use a second authentication factor and to

launch desktops or applications hosted from the *target terminal server*. You must install a Server AccessAgent and a virtual channel connector in this server.

If two-factor authentication is required when using a thin client, enable COM port redirection between the thin client and the *generic terminal server*. Only thin client hardware and RFID readers that support or emulate RS-232 devices can be used as thin clients.

The *target terminal server* hosts the terminal applications. Install a Server AccessAgent and a virtual channel connector on this server. However, ESSO GINA and the ESSO Network Provider must not be enabled.

You can set the Server AccessAgents in the *generic terminal server* and *target terminal server* in lightweight mode.

For Citrix XenApp deployments, Citrix SDK integration is required at both tiers and it involves a Services engagement. However, the *generic terminal server* can be either Microsoft Remote Desktop or Citrix XenApp Servers even if the *target terminal server* is Citrix XenApp.

Terminal Server configuration

To deploy two-tier AccessAgent configuration, configure the Citrix/Terminal Server and the terminal session settings.

Complete the following tasks:

- Configure the terminal client session to roam if Active Directory credentials are not shared.
- Configure the terminal client session to disconnect upon desktop inactivity timeout.
- Configure the terminal server to automatically log on to the Citrix/Terminal Server with an Active Directory credential.
- Enable serial port redirection at the thin client and target terminal server only if you are using RFID as the authentication factor.

ESSO configuration

To deploy two-tier AccessAgent configuration, you must also configure the ESSO GINA, ESSO Network Provider, and user authentication policy.

Complete the following tasks:

- Disable ESSO GINA on target Terminal Server.
- Disable ESSO GINA logon on a generic Terminal Server when there is no *Client AccessAgent* session.
- Enable Network Provider for *Server AccessAgent* when using thin client.

  When ESSO Network Provider is enabled, *Server AccessAgent* automatically logs the user in to the *Server AccessAgent*. The target Terminal *Server AccessAgent* uses the same credentials that the user used to log in to the generic *Citrix/Terminal Server* remote session.
- Enable Active Directory password synchronization.

  If users are using thin clients to log on to the *Server AccessAgent*, enable Active Directory password synchronization.
- Enforce two-factor authentication by setting the user authentication policy at AccessAdmin.

Thin clients cannot support two-factor authentication because there is no AccessAgent installed.

Two-factor authentication cannot be enforced at the *Server AccessAgent* because there is no ESSO AccessAgent screen displayed from which the user can authenticate. User authentication happens at the *Client AccessAgent*.

- Configure AccessAgent to log off the user or close the application when a different user unlocks it.

Chapter 13. Logging, auditing, and reporting

IBM Security Access Manager for Enterprise Single Sign-On provides auditing capability for its components to enable enhanced and customizable event tracking, and user-centric audit logs.

If auditing is enabled, IBM Security Access Manager for Enterprise Single Sign-On generates audit events and stores them in the IMS Server database.

IBM Security Access Manager for Enterprise Single Sign-On can be configured to forward its audit log records to any external SysLog server, such as Microsoft Operations Manager 2005.

Critical AccessAgent errors or events are recorded in the Windows Application Event log.

IBM Security Access Manager for Enterprise Single Sign-On has the following auditing and reporting features. See "Generating reports and audit logs" in the *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide* for the procedures.

- "Audit log events"
- "Custom audit logs" on page 139
- "Audit reports" on page 139

Audit log events

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

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

Types of logs

There are three types of logs:

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

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

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

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

Storage and sync

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

User event

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

Audit Log Event	Description
Add account credential to the Wallet	When a user adds account credentials into the Wallet manually and not captured by the AccessAgent.
Auto-capture authentication service password	When the AccessAgent captures account credentials for the user and stores it into the Wallet.
Auto-fill authentication service password	When the AccessAgent injects (auto-fills) account credentials into an application logon screen for the user after reading them from the Wallet. This event is logged for enterprise authentication services only. AccessAgent logs the event irrespective of whether the logon is successful.
Fortify authentication service password	When the AccessAgent generates random passwords on a change password screen and auto-fills it into the new password fields and clicks submit.
Log on authentication service	When a user logs on to an authentication service. This event is not automatically generated by AccessAgent. It must be explicitly modeled in the respective AccessProfiles. This event differs from the Autofill. This event is a validated logon, and is logged only when a user successfully logs on to the application.
Log off authentication service	When a user logs from an authentication service. This event is not automatically generated by AccessAgent. It needs to be explicitly modeled in the respective AccessProfiles.
Log on to AccessAgent	When a user logs on to AccessAgent.
Sign up user	When a user signs up with the IMS Server.
Register authentication factor	When a user registers an authentication factor like RFID badge, fingerprint, and others.
Store cached Wallet on hard disk or ISAM ESSO USB Key	When a user Wallet is cached.

Audit Log Event	Description
Unlock computer	When the computer is unlocked.
Reset ISAM ESSO password offline	When the ISAM ESSO password is reset offline using the backup software key (BSK) mechanism.
Reset ISAM ESSO password online	When the ISAM ESSO password is reset online with the Help desk generated authorization code or self-service secrets.
Authorization Code issuance through self-service	When a user requests authorization code for password reset or for second factor registration over email or SMS channel.
Mobile ActiveCode request with ISAM ESSO password	When a user requests for a Mobile ActiveCode for an application that uses the ISAM ESSO password to perform its first step in the authentication process.
Mobile ActiveCode request with application password	When a user requests for a Mobile ActiveCode for an application that has its own password as its first step in the authentication process.
ActiveCode verification	When the user submits the Mobile ActiveCode for verification. This event can be translated as the final step in the two-step authentication process involving ActiveCode enabled applications.
RADIUS authentication	When the RADIUS client (VPN server) initiates a RADIUS authentication request to the IMS Server. This event usually occurs when the user enters the application password and the VPN server delegates this authentication to the IMS Server RADIUS component. This event is the first step in the two-step authentication process with Mobile ActiveCode.
RADIUS challenge response	When the RADIUS client (VPN server) initiates a RADIUS challenge-response to the IMS Server. This event usually occurs when the user enters the mobile ActiveCode delivered to the user through the SMS or email channel. The VPN server delegates this authentication to the IMS Server RADIUS component. This event is the second step in the two-step authentication process with Mobile ActiveCode.

Administrator / Help desk event

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

Audit Log Event	Description
Authorization code issuance for online verification	When a Help desk or administrator generates an authorization code for the user when the user has connectivity to the IMS.

Audit Log Event	Description
Authorization code issuance for offline verification	When the Help desk or administrator generates an authorization code for the user to reset the password when the user does not have connectivity to the IMS Server. (Backup Software Key BSK workflow)
Provision ISAM ESSO user account	When administrator provisions an ISAM ESSO user account.
Update System Policy	When an administrator updates the system policy.
Update User Policy	When an administrator or Help desk updates a user policy.
Authentication factor revocation	When a user authentication factor is revoked by the Administrator or Help desk.
Revoke user	When a user is revoked by an administrator or Help desk.
Mobile ActiveCode user sign-up	When a mobile ActiveCode user is signed up through AccessAdmin.
ActiveCode-enabled authentication service account activation	When a Mobile ActiveCode account is activated by an Administrator or Help desk through the Users Authentication Services page on AccessAdmin.
ActiveCode-enabled authentication service account addition	When a Mobile ActiveCode account is added to the user through CLT or through the Users Authentication Services page on the AccessAdmin by the Administrator or Help desk.
ActiveCode-enabled authentication service account locked	When a Mobile ActiveCode account is locked through the Users Authentication Services page on the AccessAdmin by the Administrator or Help desk.
ActiveCode-enabled authentication service account removal	When a Mobile ActiveCode account is deleted through the Users Authentication Services page on the AccessAdmin by the Administrator or Help desk.
OTP ActiveCode initialization	When the OTP ActiveCode is initialized by the AccessAgent for the first time.
OTP Token Reset	When the OTP Token is reset.

System logs

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

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

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

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

Audit log queries

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

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

Event logs

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

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

Custom audit logs

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

To enable custom audit logging:

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

Audit reports

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

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

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

Note: For Tivoli Common Reporting version 2.1:

- The TCR-BIRT user interface supports bidirectional language but the reports generated do not support bidirectional languages.
- TCR-Cognos also does not support bidirectional languages.

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

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

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

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

Chapter 14. Product maintenance

After a successful product deployment, the next phase is product maintenance. Administrators must regularly backup data, apply fix packs, and perform database pruning when necessary.

See the following topics:

- "Backup and recovery"
- "Fix packs"
- "Database maintenance" on page 144

Fix packs

Fix packs are periodic bundling of interim fixes and other resolved APARs. Customers must plan for and implement fix packs as they are released to ensure that the deployed product is updated with the required fixes. Fixes provide changes to the software that can resolve known problems, add new functions, or keep the software operating efficiently.

Download the latest fixes and updates for IBM Security Access Manager for Enterprise Single Sign-On from Fix Central:http://www-933.ibm.com/support/fixcentral/.

See http://www.ibm.com/developerworks/wikis/display/tivoliim/Determining+Product+Fixpack+Levels for fix packs and version numbering conventions, **Version, Release, Modification Level and Fix**.

Backup and recovery

Backups are necessary to ensure high availability and disaster recovery. Developing plans for backup and recovery, can be part of your overall disaster recovery plan.

The backup and recovery plan that you develop for IBM Security Access Manager for Enterprise Single Sign-On must include the following considerations and requirements:

- What to back up
- Frequency of backups
- Types of backups
- Where to store backups
- Amount of time required for a recovery window

If you are performing an upgrade, back up your existing server configuration and data to avoid data loss.

What to back up:

- IMS Server configuration data

  Use the Export and Import configuration tool to back up and restore the IMS Server configuration data. This backup tool is applicable only for IMS Server version 8.2. For earlier versions, use the **`manageprofiles`** command.
- WebSphere Application Server profiles

Use the WebSphere Application Server **manageprofiles** command to back up the profile.

- IMS Server databases

  Database servers from different vendors include their own backup and recovery procedures. IBM Security Access Manager for Enterprise Single Sign-On leverages on existing backup and recovery features of the database products it works with – IBM DB2, Microsoft SQL Server, and Oracle.

Note: Always consider testing recovery procedures and quality of data in backups on a periodic basis. Testing the quality of backups ensures that the latest backups are always relevant, consistent, and recoverable in the event of an actual disaster.

See "Backing up and Restoring" in the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for the backup and recovery procedures.

Database maintenance

Plan for routine database maintenance tasks to optimize database performance. You can prune or remove historical information from the database and reduce the database size.

You can also establish routine database maintenance procedures to complete the following tasks such as database pruning, updating statistics, and reorganizing database tables. Database pruning removes historical information from the database to reduce the database size.

Some database support "automatic maintenance" which must be enabled if manual maintenance is not to be performed. See your vendor provided database documentation to determine the types of database maintenance tasks you can complete.

See http://www-304.ibm.com/support/docview.wss?uid=swg21572941 to download the database maintenance script.

Appendix. Change password and reset password

The AccessAgent window contains a change password and reset password option. Users can update their ISAM ESSO password through these options.

Change password

Your organization might schedule regular and compulsory change of ISAM ESSO password to ensure password security.

Users can change their ISAM ESSO password through AccessAgent. Active Directory password synchronization can be enabled or disabled.

When Active Directory password synchronization is enabled, the ISAM ESSO password is synchronized with the Active Directory password. If the Active Directory password synchronization is disabled, the change password feature changes only the ISAM ESSO password. The new ISAM ESSO password is not synchronized with the Active Directory password.

AccessAgent must be connected to the IMS Server for the change password function to succeed.

Workflow:

1. User clicks the **Change password** link from the AccessAgent window.
2. User provides the old password, the new password, and a confirmation of the new password.

   Note: The new password must match the specified password requirements.
3. AccessAgent changes the Active Directory password.
4. AccessAgent updates the ISAM ESSO password in the IMS Server.
5. AccessAgent updates the ISAM ESSO password in the cached Wallet.

Self-service password reset

Users can reset their ISAM ESSO password from any computer either through AccessAgent or through AccessAssistant. Active Directory password synchronization can be enabled or disabled.

Users can reset their ISAM ESSO password in case they forgot their password and they want to do an immediate reset. Users must answer correctly their registered secret questions to do a self-service password reset.

Using AccessAgent and Active Directory password synchronization is enabled

In this scenario, users must have an authorization code to reset their ISAM ESSO password.

If self-service password reset is enabled, users do not need to call Help desk. To reset the ISAM ESSO password, users must answer two or more secret questions. User must have registered secret questions and the user must be able to answer the secret questions.

Workflow if there is an IMS Server connectivity

1. User clicks the **Reset password** link from the AccessAgent window.

2. User provides the user name.
3. User provides the answers to the secret questions.
4. User provides the new password and a confirmation of the new password.
5. AccessAgent resets the Active Directory password.
6. AccessAgent updates the ISAM ESSO password in the IMS Server.
7. AccessAgent updates the ISAM ESSO password in the cached Wallet.

If AccessAgent cannot connect to the IMS Server, you are prompted that there is no IMS Server connectivity. You must have a temporary password to use AccessAgent. See "Resetting passwords without IMS Server connectivity in the *IBM Security Access Manager for Enterprise Single Sign-On User Guide*.

Using AccessAssistant

To use AccessAssistant, the user must have registered secret questions. The user must provide the correct answers to the secret questions. See the *IBM Security Access Manager for Enterprise Single Sign-On User Guide* for the procedure.

Active Directory password reset

The Active Directory password can be reset by the Active Directory Administrator or using the Tivoli Identity Manager. In this scenario, the ISAM ESSO password is not synchronized with the Active Directory password.

Workflow:

1. User logs on to AccessAgent with an old ISAM ESSO password.
2. AccessAgent connects to the IMS Server.
3. AccessAgent prompts the user that the password entered does not match the password stored in the user Wallet.
4. User enters the new Active Directory password.
5. User is prompted for the primary secret.
6. The IMS Server verifies the new password with the Active Directory.
7. The IMS Server updates the ISAM ESSO password accordingly.

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

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

Printed in USA

SC23-9952-03