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

AccessAgent on Terminal Server and Citrix Server Guide

SC27-5668-01

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

AccessAgent on Terminal Server and Citrix Server Guide

SC27-5668-01

Note
Before using this information and the product it supports, read the information in "Notices" on page 19.

Edition notice

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

Contents

About this publication

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

Access to publications and terminology

This section provides:

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

IBM® Security Access Manager for Enterprise Single Sign-On library

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

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

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

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

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

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

  IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide provides information about configuring the IMS Server settings, the AccessAgent user interface, and its behavior.
- *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide*, SC23995105

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

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

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

- *IBM Security Access Manager for Enterprise Single Sign-On Help Desk Guide*, SC23995304

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

- *IBM Security Access Manager for Enterprise Single Sign-On User Guide*, SC23995005

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

- *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide*, GC23969303

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

- *IBM Security Access Manager for Enterprise Single Sign-On Error Message Reference Guide*, GC14762402

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

- *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide*, SC23995605

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

- *IBM Security Access Manager for Enterprise Single Sign-On AccessProfile Widgets Guide*, SC27444401

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

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

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

- *IBM Security Access Manager for Enterprise Single Sign-On Provisioning Integration Guide*, SC23995704

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

- *IBM Security Access Manager for Enterprise Single Sign-On Web API for Credential Management Guide*, SC14764601

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

- *IBM Security Access Manager for Enterprise Single Sign-On Serial ID SPI Guide*, SC14762601

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

- *IBM Security Access Manager for Enterprise Single Sign-On Epic Integration Guide*, SC27562300

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

- *IBM Security Access Manager for Enterprise Single Sign-On Context Management Integration Guide*, SC23995404

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

- *IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Mobile Guide*, SC27562101

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

- *IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Virtual Desktop Infrastructure Guide*, SC27562201

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

- *IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Terminal Server and Citrix Server Guide*, SC27566801

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

Online publications

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

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

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

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

IBM Terminology website

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

Accessibility

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

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

Technical training

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

Support information

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

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

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

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

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Chapter 1. AccessAgent on Citrix and Terminal Servers

IBM Security Access Manager for Enterprise Single Sign-On supports single sign-on and authentication services for applications that are hosted on Citrix and Terminal Servers – Citrix XenApp Servers or Terminal Services.

You must install AccessAgent on each Citrix or Terminal Server.

For every remote session on Citrix or Terminal Server, there is a running AccessAgent instance. AccessAgent helps users single sign-on to their applications on the particular remote session. Users can later reconnect to the same remote session on the Citrix or Terminal Server through any client computer.

See the following topics:

Chapter 2. Deployment models

You can choose an AccessAgent deployment model that is based on your terminal services requirements and on your terminal services environment.

The single sign-on experience on a Citrix or Terminal Server varies, depending on the following factors:

- How you deployed AccessAgent
- How you configured the policies

The deployment model type that you choose from depends on the following setup considerations:

- Are you using Terminal Services or Citrix XenApp Servers?
- Are you using Citrix XenApp Server or Citrix XenDesktop 7.0?
- Is Active Directory password synchronization enabled?
- Are you using thin clients, workstations, or both?

  Note: Thin clients refer to machines without AccessAgent. Workstations refer to machines with AccessAgent.
- Are you using two-factor authentication on your server?

Deployment model selection guidelines

There are four deployment models for Citrix and Terminal Servers. You must identify the directory services and single sign-on requirements for thin clients, workstations, or both. You must also identify the type of authentication factors you expect to deploy in a terminal services environment.

Use the following guidelines to help you select the best deployment model for a terminal services environment.

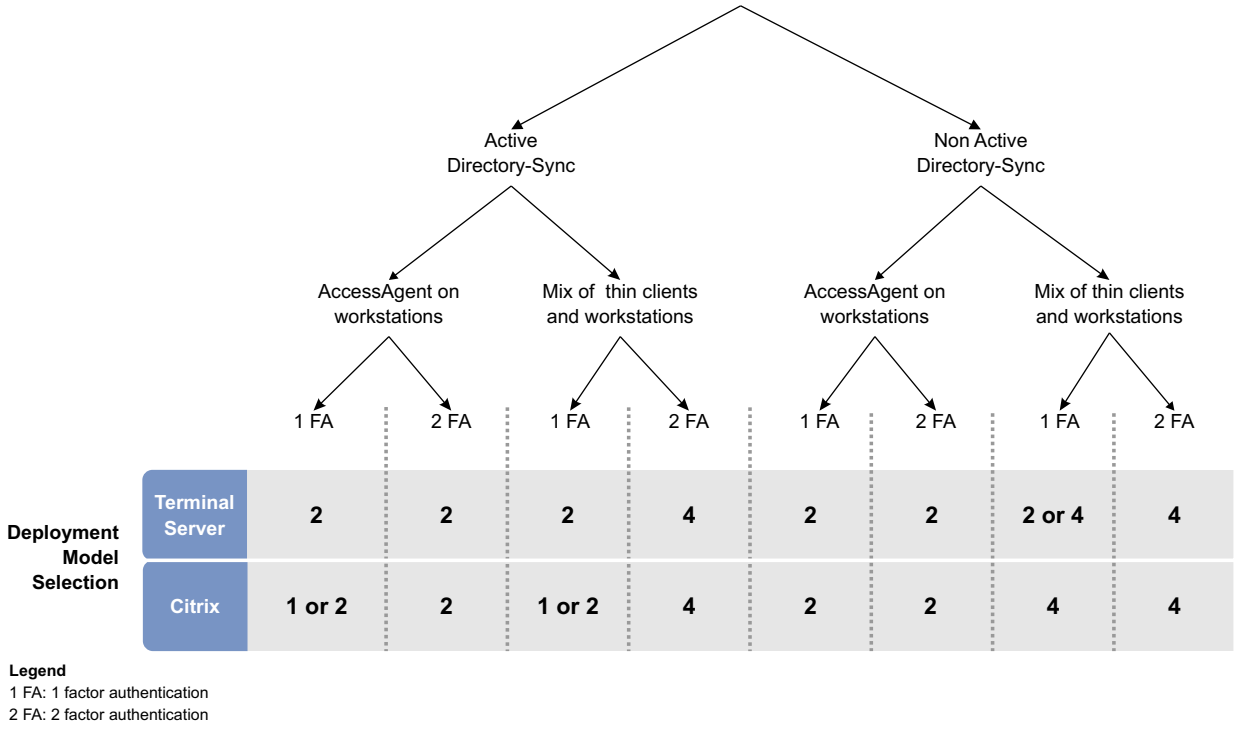

Figure 1. Deployment model selection guidelines on Citrix and Terminal Servers environments

After you choose a deployment model, complete the configuration tasks for the model:

- Chapter 3, "Model 1: Basic configuration," on page 5
- Chapter 4, "Model 2: Virtual Channel Connector configuration," on page 7
- Chapter 5, "Model 3: Generic terminal session," on page 13
- Chapter 6, "Model 4: Two-tier AccessAgent configuration," on page 15

Chapter 3. Model 1: Basic configuration

The basic configuration model consists of deploying Server AccessAgent on the Citrix or Terminal Server and enabling the ESSO Network Provider.

In this configuration, the Server AccessAgent automatically logs on the user to the Wallet upon logon to the Citrix or Terminal Server remote session.

Any Wallet changes in the Client AccessAgent or Server AccessAgent are not immediately synchronized between the Client AccessAgent and Server AccessAgent.

Deploying basic configuration

You can deploy basic configuration on Terminal or Citrix Server. Configure the AccessAgent and the Citrix or Terminal Server to deploy Model 1.

Before you begin

To specify the single sign-on options for Model 1, you must modify the `SetupHlp.ini` file before you install the Server AccessAgent. You can access this file in the **Config** folder of the AccessAgent installation package. Modify the following options on the `SetupHlp.ini` file:

Option	Description
`EncentuateNetworkProviderEnabled`	Set to `1` to enable the ESSO Network Provider.
`EncentuateCredentialProviderEnabled` and `EnginaEnabled`	Set to `0` to disable the ESSO GINA and ESSO Credential Provider.

Procedure

1. Complete the following tasks on the Citrix or Terminal Server:
   a. Install the AccessAgent on the Citrix or Terminal Server.
   b. Log on to AccessAdmin and set the `pid_en_network_provider_enabled` policy to `1`.
2. Client machine configuration. There is no required installation and configuration on the client machine.
3. Optional configuration. There is no optional configuration for Model 1.

Single sign-on experience

The user single sign-on experience varies, depending on how you deploy the AccessAgent. If you deploy the basic configuration, users can automatically log on to the Wallet, single sign-on to profiled applications, and manage credentials.

In this configuration, the user can:

- Log on to the Citrix or Terminal Server remote session with Active Directory credentials. The user is automatically logged on to the Wallet.
- Access published applications in seamless mode. The Server AccessAgent tray icon is added to the client taskbar.

- Single sign-on to profiled applications.
- Manage the Wallet through Server AccessAgent.

Chapter 4. Model 2: Virtual Channel Connector configuration

The Server AccessAgent connects to the Client AccessAgent through a Virtual Channel Connector to retrieve the user credentials and authenticate the user.

You must install AccessAgent on your server and client.

Virtual Channel Connector

The Virtual Channel Connector between the Client AccessAgent and the Server AccessAgent is built on top of the Virtual Channel Connector SDK from Citrix or Microsoft.

The following diagram illustrates the communication between the terminal server and the client machine.

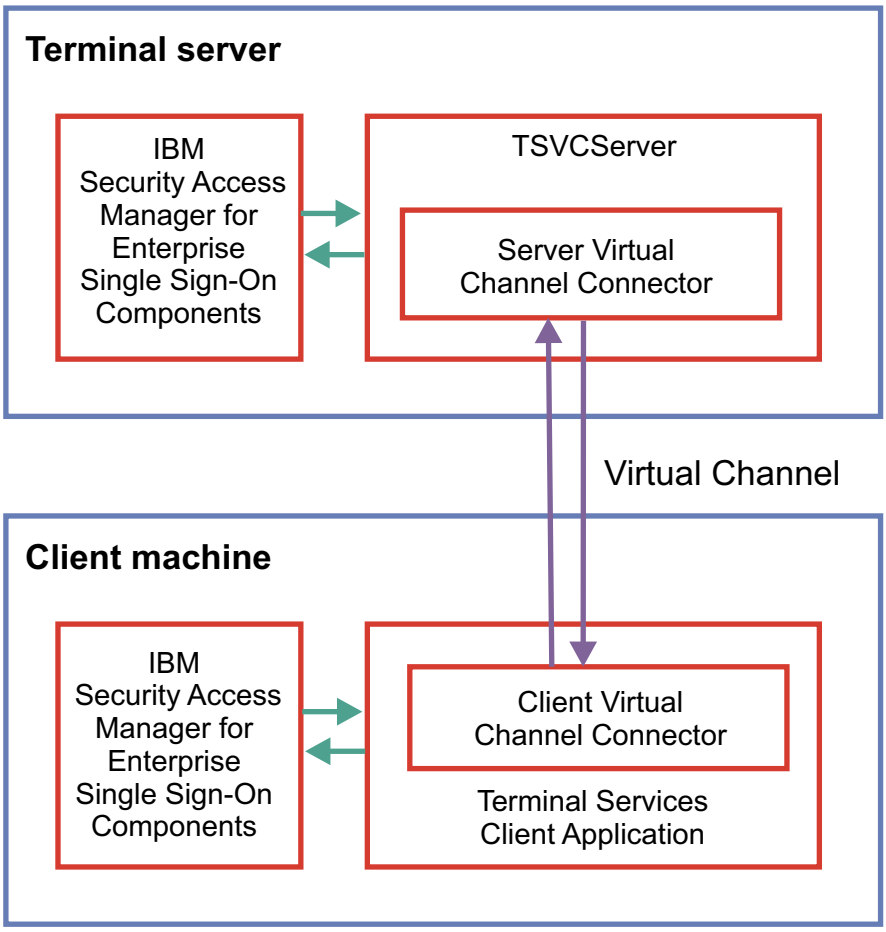

Figure 2. Communication between the terminal server and the client machine

Standard mode and lightweight mode

In Virtual Channel Connector configuration, you can set the Server AccessAgent to run in lightweight mode.

Running in lightweight mode can reduce the memory footprint of AccessAgent on a Citrix or Terminal Server and can improve the single sign-on startup duration.

See the following table for a comparison of the two AccessAgent modes.

Features	Standard mode (with virtual channel)	Lightweight mode
Performance	Normal	Better
User experience	Automatic logon to Server AccessAgent with Client AccessAgent credentials	Automatic logon to Server AccessAgent with Client AccessAgent credentials
Supported authentication factors on Client AccessAgent	RFID	All authentication factors
Synchronize changes between Client AccessAgent and Server AccessAgent	Yes (through IMS Server)	Yes
AccessAgent Wallet cached on the Server	Yes	Never
Behavior of AccessAgent when users log on and log off from AccessAgent	Logs off remote AccessAgent and disconnects the remote session	Disconnects remote session

Deploying Virtual Channel Connector configuration

You can deploy Virtual Channel Connector configuration on Citrix or Terminal Server. Configure the AccessAgent and the Citrix or Terminal Server to deploy Model 2.

Before you begin

To specify the installation and single sign-on options for Model 2, you must modify the `SetupHlp.ini` file before you install the Server AccessAgent. Modify the following options on the `SetupHlp.ini` file:

Option	Description
`EncentuateNetworkProviderEnabled`	Set to `0` to disable the ESSO Network Provider.
`EncentuateCredentialProviderEnabled` and `EnginaEnabled`	Set to `0` to disable the ESSO GINA and ESSO Credential Provider.

Option	Description
CitrixVirtualChannelConnectorMode	Applicable only for Citrix server deployment. Set to 2 to enable the Virtual Channel Connector from the server and run AccessAgent in standard mode. Set to 3 to enable theVirtual Channel Connector from the server and run AccessAgent in lightweight mode. Set to 4 to enable the Virtual Channel Connector from the server and run AccessAgent in enforced lightweight mode.

You must also modify the SetupHlp.ini file before you install the Client AccessAgent on Citrix client machine. Modify the following options on the SetupHlp.ini file:

Option	Description
CitrixVirtualChannelConnectorMode	Set to 1 to enable the Virtual Channel Connector on the client computer.
ICAClientInstallDir	Specify the installation directory for the Citrix ICA Client.

Note: There are no required changes in the SetupHlp.ini file before you install the Client AccessAgent on Terminal Server client machine.

Procedure

1. On the Citrix or Terminal Server, install the Server AccessAgent. If you encounter an error in deploying the Virtual Channel Connector on the Citrix server, see "Deploying Virtual Channel Connector on Citrix server" on page 10.
2. On the client machine, install the Client AccessAgent. If you encounter an error in deploying the Virtual Channel Connector on the Citrix client machine, deploy the Virtual Channel Connector manually. See "Deploying Virtual Channel Connector on Citrix client" on page 10.
3. Optional: Change the Server AccessAgent to run in lightweight mode or standard mode after installation. To change the Server AccessAgent mode, modify the **TSLightweight Mode** policy in the root\DeploymentOptions.

Table 1. TSLightweight Mode policy value

TSLightweight Mode policy value	Description
0	Deploys the Server AccessAgent in standard mode.
1 (default)	Deploys the Server AccessAgent in lightweight mode.
2	Enforces lightweight mode. The Server AccessAgent always operates in lightweight mode. The session in the Server AccessAgent does not start when there is no Client AccessAgent.

Deploying Virtual Channel Connector on Citrix server

You can deploy the Virtual Channel Connector on Citrix server by modifying the `SetupHlp.ini` file and installing the Server AccessAgent. If you encounter an error during installation, you can manually deploy Virtual Channel Connector on your Citrix server.

Procedure

Register the server connector file with AccessAgent.

1. On your Windows desktop, click **Start** > **Run**.
2. In the **Open** field, enter `regedit` and click **OK**. The Registry Editor is displayed.
3. Open `HKLM\SOFTWARE\IBM\ISAM ESSO`.
4. Create the `HKLM\SOFTWARE\IBM\ISAM ESSO\AccessAgent\Integration\TerminalServices\ServerSPI` key.
5. In the `HKLM\SOFTWARE\IBM\ISAM ESSO\AccessAgent\Integration\TerminalServices\ServerSPI` key, create the following string values:

Value Name	Value Data
ICA	`ICAVCServer.dll`

Deploying Virtual Channel Connector on Citrix client

You can deploy Virtual Channel Connector on Citrix client by modifying the `SetupHlp.ini` file and installing the Client AccessAgent. If you encounter an error during installation, you can manually deploy Virtual Channel Connector on your Citrix client.

Procedure

1. Copy the client connector DLL file. For example: `ICAVCClient.dll`, from the AccessAgent Program Files folder to the Citrix XenApp Plug-in installation folder.
2. Copy the `EncVcClient.dll` file from the AccessAgent Program Files folder to the Citrix XenApp Plug-in installation folder.
3. Configure the Citrix client registry for the client connector DLL file.
   a. On your Windows desktop, click **Start** > **Run**.
   b. In the **Open** field, enter `regedit` and click **OK**. The Registry Editor is displayed.

      Note:
      - For a Windows 32-bit operating system, the Citrix registry hive is `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`.
      - For a Windows x64 operating system, the Citrix registry hive is `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\`.

   c. Modify the VirtualDriverEx.
      1) Select `<Citrix registry hive>\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0\`.
      2) Double-click **VirtualDriverEx**.
      3) In the **Value data** field, add `ICAVCClient`.
      4) Click **OK**.

d. Create an ICAVCClient.

1) Open <Citrix registry hive>\ICA Client\Engine\Configuration\Advanced\Modules\.

2) Create the <Citrix registry hive>\ICA Client\Engine\Configuration\Advanced\Modules\ICAVCClient key.

3) In the <Citrix registry hive>\ICA Client\Engine\Configuration\Advanced\Modules\ICAVCClient\ key, create the following string values:

Value Name	Value Data
DriverName	ICAVCClient.dll
DriverNameWin16	ICAVCClient.dll
DriverNameWin32	ICAVCClient.dll

Single sign-on experience

The user single sign-on experience varies, depending on how you deploy the AccessAgent. If you deploy theVirtual Channel Connector, users are automatically logged on to the remote sessions after users log on to Client AccessAgent.

In this configuration, the user can:

- Log on to the Client AccessAgent.
- Start a Citrix or Terminal Server session. The Client AccessAgent logs on the user to the remote session.
- In the standard mode,
  - Server AccessAgent starts and Server AccessAgent and Client AccessAgent are synchronized.
  - User is automatically logged on to the AccessAgent by using the Client AccessAgent credential.
  - The Server AccessAgent tray icon is added to the client taskbar when the user access published applications in seamless mode.
  - User can single sign-on to profiled applications.
  - User can manage the Wallet through Client AccessAgent.

    Note: If the terminal server policy for displaying new options on remote AccessAgent is enabled, the user can manage the Wallet through the Client AccessAgent and Server AccessAgent.
- In the lightweight mode,
  - Server AccessAgent is not started.
  - User can single sign-on to profiled applications.
  - User can manage the Wallet through Client AccessAgent.

Chapter 5. Model 3: Generic terminal session

A generic terminal configuration consists of a Server AccessAgent deployed on a generic terminal session.

A generic desktop session is hosted on a dedicated tier of the Citrix or Terminal Server. Different users can share access to applications hosted in the remote session from a thin client machine.

Important: This configuration is intended for thin client users.

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 or ESSO Credential Provider.

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.

Model 3 limitations

Consider the following single sign-on limitations in a terminal services deployment with generic terminal sessions:

- Users can use only RFID as the second authentication factor device.
- Users cannot roam terminal session.

Deploying generic terminal session

You can deploy single sign-on services on a generic terminal session. Configure the AccessAgent and the Citrix or Terminal Server to deploy Model 3.

Before you begin

The following settings are the required generic terminal server configurations to implement Model 3. These terminal servers are dedicated to serve thin client machines only.

- Configure the generic terminal server to automatically log on to the Citrix or Terminal Server with a single designated low-privilege generic Active Directory credential.
- Configure the generic 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 times out, the desktop screen must be locked.

To specify the single sign-on options for Model 3, you must modify the `SetupHlp.ini` file before you install the Server AccessAgent. Modify the following options on the `SetupHlp.ini` file:

Option	Description
`EncentuateNetworkProviderEnabled`	Set to `0` to disable the ESSO Network Provider.
`EncentuateCredentialProviderEnabled` and `EnginaEnabled`	Set to `1` to enable the ESSO GINA and ESSO Credential Provider.

Procedure

1. Complete the following tasks on the Citrix or Terminal Server:
   a. Install the AccessAgent on the Citrix or Terminal Server.
   b. Assign a shared desktop policy template at Server AccessAgent.
2. Configure the thin client to automatically log on to the Citrix or Terminal Server with a single designated low-privilege generic Active Directory credential. The credential is the same account as the one setup for auto-logon on the generic terminal server.
3. Optional: If you are using RFID as the authentication factor, you must complete the following tasks:
   a. Enable serial port redirection at the thin client and target terminal server.
   b. Enforce two-factor authentication by setting the user authentication policy at AccessAdmin.
   c. Enable the RFID authentication if required. See Chapter 7, “Customizing AccessAgent on Citrix and Terminal Servers,” on page 17.

Single sign-on experience

The user single sign-on experience varies, depending on how you deploy the AccessAgent. If you deploy the generic terminal session configuration, the user logs on to a lock screen to start a session.

In this configuration, the user can do the following tasks:

- Log on to the ESSO GINA or ESSO Credential Provider lock screen to start a session. User can log on to the Server AccessAgent with password or RFID.
- Single sign-on to profiled applications.
- Manage the Wallet through the Server AccessAgent.

Chapter 6. Model 4: Two-tier AccessAgent configuration

A two-tier AccessAgent configuration is a combination of deploying a Virtual Channel Connector and a generic remote desktop. This configuration is intended for deployments that require mixed-client two-factor authentication.

A two-tier AccessAgent configuration involves two terminal servers:

- A generic terminal server for deployment with thin clients
- Target Citrix or Terminal Server for deployment with workstations

A generic terminal server hosts a generic remote desktop. The server accepts thin client connections and automatically connects to the target Citrix or Terminal Server acting as a proxy.

The target Citrix or Terminal Server hosts the Terminal Server sessions and Citrix applications.

The following diagram illustrates the communication between the terminal servers and the client machines.

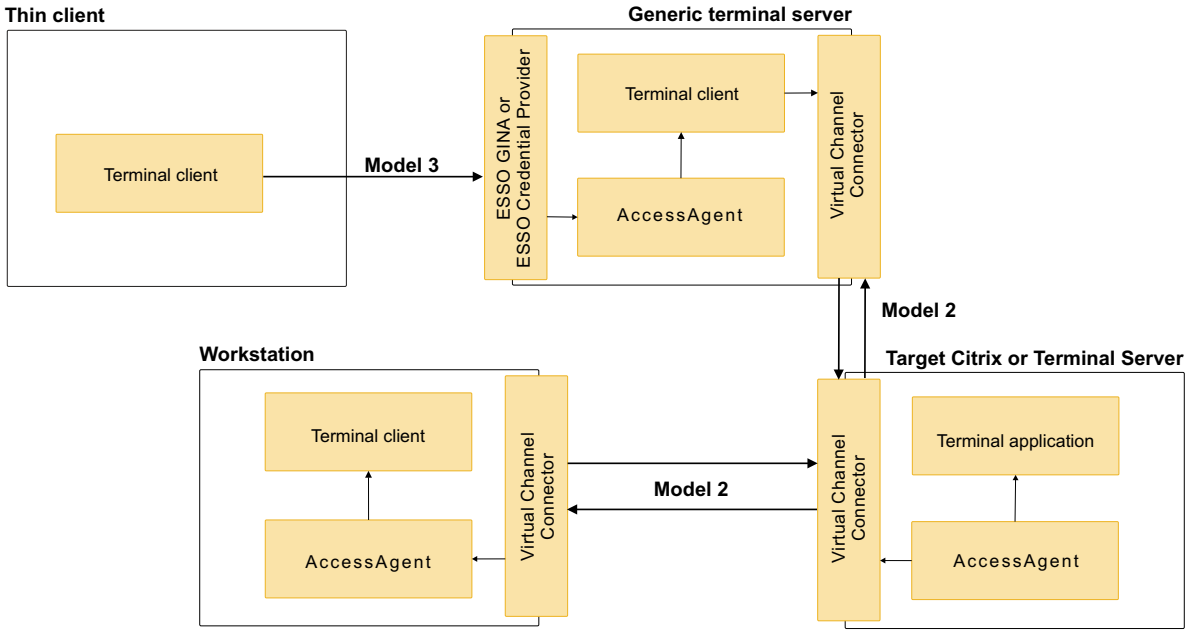

Figure 3. Communication between the terminal servers and client machines

The thin client users connect to the generic terminal server by using the Model 3 configuration. The generic terminal server then connects to the target Citrix or Terminal Server through Virtual Channel Connector, or by using the Model 2 configuration.

The workstation client users connect to the target Citrix or Terminal Server through Virtual Channel Connector, or by using the Model 2 configuration.

Deploying two-tier AccessAgent configuration

You can deploy a two-tier AccessAgent configuration on Citrix or Terminal Server. Configure the target Citrix or Terminal Server, generic terminal server, thin clients, and workstations to deploy Model 4.

Procedure

1. On the target Citrix or Terminal Server, complete the tasks for configuring the Citrix or Terminal Server as enumerated in Model 2 configuration. See "Deploying Virtual Channel Connector configuration" on page 8.
2. On the generic terminal server, you must complete the following tasks:
   a. Complete the tasks in configuring the generic terminal server in Model 3 configuration except the installation of AccessAgent. See "Deploying generic terminal session" on page 13.
   b. Configure the generic terminal server as a client machine. Complete the tasks in configuring a client machine as discussed in Model 2 configuration. See "Deploying Virtual Channel Connector configuration" on page 8.
   c. Configure the generic server to automatically log on to the target Citrix or Terminal Server.
3. On the thin client machine, configure the thin client to automatically log on to the Citrix or Terminal Server with a single designated low-privilege generic Active Directory credential. This credential is the same as the one setup for auto-logon on the generic terminal server.
4. On the workstation client machine, complete the tasks for configuring the client machine as stated in Model 2 configuration. See "Deploying Virtual Channel Connector configuration" on page 8.

Single sign-on experience

The user single sign-on experience varies, depending on how you deploy the AccessAgent. If you deploy the two-tier AccessAgent configuration, the single sign-on experience is similar when you deploy the Model 2 and Model 3 configurations.

Workstation users

In this configuration, the single sign-on experience for workstation users is the same as the single sign-on experience for Virtual Channel Connector configuration. See Model 2 "Single sign-on experience" on page 11.

Thin client users

In this configuration, the single sign-on experience for thin client users is the same as the single sign-on experience for generic terminal session configuration. See Model 3 "Single sign-on experience" on page 14.

Chapter 7. Customizing AccessAgent on Citrix and Terminal Servers

You can customize the behavior of AccessAgent when users log on to a session on a Citrix or Terminal Server.

Procedure

1. Log on to AccessAdmin.
2. Go to **Machine Policy Templates** > **Template assignments**.
3. Click a policy template.
4. Go to **AccessAgent Policies** > **Terminal Server Policies**.
5. Complete the following fields:

Option	Description
Enable auto-launching of AccessAgent logon prompt	Identifies whether to launch the AccessAgent logon dialog if AccessAgent is not logged on when a Citrix application or a Terminal Server session is launched.
Use ESSO GINA or ESSO Credential Provider logon when there is no local AccessAgent session	Whether to use ESSO GINA or ESSO Credential Provider logon or Microsoft GINA logon for the Terminal Server session, when there is no local AccessAgent session.
Log off remote AccessAgent when reconnecting from workstation without local AccessAgent session	Whether to log off remote AccessAgent when user, with no local AccessAgent session, reconnects to an existing session on Citrix or Terminal Server.
Option for displaying menu options on remote AccessAgent	Whether to display menu options on AccessAgent user interface in a Citrix or Terminal Server session.

6. Complete the following fields only if you want RFID to be enabled for thin clients:

Option	Description
Enable COM port redirection	Identifies whether the device monitoring mechanism must redirect the COM port from the client computer to the Citrix or Terminal Server.
Virtual COM port on Citrix or Terminal Server	Virtual COM port on the Citrix or Terminal Server to which data from the client COM port gets redirected to.
Physical COM port on client machine	Physical COM port on the client to which the authentication device, or the RFID reader, is connected to. The redirection takes place from this port to the virtual COM port of the Citrix or Terminal Server.

7. Click **Update**.
8. Assign the updated machine policy template to the Citrix or Terminal Server.

Notices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

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

Trademarks

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

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

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

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

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

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

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

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

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

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

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

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

Privacy Policy Considerations

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

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

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

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

Glossary

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

The following cross-references are used in this glossary:

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

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

A

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

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

account data item
The user credentials required for logon.

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

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

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

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

Active Directory credential
The Active Directory user name and password.

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

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

active RFID
See active radio frequency identification.

AD See Active Directory.

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

API See application programming interface.

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

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

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

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

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

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

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

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

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

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

B

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

base image
A template for a virtual desktop.

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

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

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

C

CA See certificate authority.

CAPI See cryptographic application programming interface.

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

CCOW
See Clinical Context Object Workgroup.

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

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

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

CLI See command-line interface.

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

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

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

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

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

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

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

CSN See Card Serial Number.

CSP See cryptographic service provider.

D

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

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

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

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

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

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

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

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

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

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

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

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

DLL See dynamic link library.

DN See distinguished name.

DNS See domain name server.

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

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

E

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

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

ESSO See enterprise single sign-on.

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

F

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

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

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

FIPS See Federal Information Processing Standard.

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

FQDN
See fully qualified domain name.

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

G

GINA See graphical identification and authentication.

GPO See group policy object.

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

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

H

HA See high availability.

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

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

hot key
A key sequence used to shift operations

between different applications or between different functions of an application.

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

I

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

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

J

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

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

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

JMX See Java Management Extensions.

JRE See Java runtime environment.

JVM See Java virtual machine.

K

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

L

LDAP See Lightweight Directory Access Protocol.

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

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

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

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

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

M

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

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

N

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

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

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

O

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

OTP See one-time password.

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

P

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

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

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

PIN See personal identification number.

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

PKCS See Public Key Cryptography Standards.

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

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

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

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

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

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

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

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

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

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

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

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

R

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

RADIUS
See remote authentication dial-in user service.

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

RDP See remote desktop protocol.

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

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

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

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

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

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

RFID See radio frequency identification.

root CA
See root certificate authority.

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

S

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

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

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

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

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

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

security trust service chain
A group of module instances that are

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

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

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

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

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

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

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

sign up
To request a resource.

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

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

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

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

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

SMTP See Simple Mail Transfer Protocol.

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

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

SPI See service provider interface.

SSL See Secure Sockets Layer.

SSL VPN
See Secure Sockets Layer virtual private network.

SSO See single sign-on.

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

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

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

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

STS See Security Token Service.

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

T

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

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

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

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

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

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

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

tty See terminal type.

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

U

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

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

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

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

V

VB See Visual Basic.

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

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

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

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

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

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

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

VMM See Virtual Member Manager.

VPN See virtual private network.

W

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

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

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

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

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

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

Index

Printed in USA

SC27-5668-01