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

Tivoli Endpoint Manager Integration Guide

SC27-5620-00

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

Tivoli Endpoint Manager Integration Guide

SC27-5620-00

Note
Before using this information and the product it supports, read the information in "Notices" on page 27.

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

Figures

Tables

About this publication

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.

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 xii.
- A link to the "IBM Terminology website" on page xii.

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

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

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

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

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

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

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

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

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

  This guide is intended for the Administrators. It covers the different Administrator tasks. *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide* provides procedures for creating and assigning policy templates, editing policy values, generating logs and reports, and backing up the IMS Server and its database. Use this guide together with the IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide.
- *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide*, SC23969404

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Online publications

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

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

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

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

IBM Terminology website

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

Accessibility

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

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

Technical training

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

Support information

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

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

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

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

Statement of Good Security Practices

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

Chapter 1. Overview

IBM Security Access Manager for Enterprise Single Sign-On integrates with IBM Tivoli® Endpoint Manager 8.2 for the automatic deployment of AccessAgent 8.2.1 and its fix pack on client computers.

Use IBM Tivoli Endpoint Manager to complete the following tasks:

- Create and configure a Fixlet to install or upgrade AccessAgent.
- Create and configure a Fixlet to apply a fix pack or interim fix on the AccessAgent deployments.
- Collect data about the AccessAgent deployment and view data on the IBM Tivoli Endpoint Manager dashboard.
- Create a customized AccessAgent deployment dashboard.

System requirements

Verify that your system meets both the IBM Tivoli Endpoint Manager and IBM Security Access Manager for Enterprise Single Sign-On system requirements before you deploy the server and client components. Compliance with requirements can prevent deployment issues.

Table 1. System requirements

System requirements for	See
IBM Tivoli Endpoint Manager	"Tivoli Endpoint Manager Operating Requirements" in the Tivoli Endpoint Manager documentation (http://pic.dhe.ibm.com/infocenter/tivihelp/v26r1/index.jsp?topic=/com.ibm.tem.doc_8.2/Platform/Adm/c_tivoli_endpoint_manager_operat.html).
IBM Security Access Manager for Enterprise Single Sign-On	"Hardware and software requirements" in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*. The hardware and software requirements that are published are accurate at the time of publication. See the detailed system requirements document at http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/softwareReqsForProduct.html. 1. Enter `Access Manager for Enterprise Single Sign-on`. 2. Select the product version. 3. Select the operating system. 4. Click **Submit**.

Integration requirements

The IBM Tivoli Endpoint Manager and IBM Security Access Manager for Enterprise Single Sign-On integration requires that you install the Tivoli Endpoint Manager components.

Table 2. Integration requirements

Tasks	See
Install the following Tivoli Endpoint Manager components on the server: • Tivoli Endpoint Manager Server • Tivoli Endpoint Manager Console Install the following Tivoli Endpoint Manager components on the client where you want to deploy AccessAgent: • Tivoli Endpoint Manager Client	The following guides in the IBM Tivoli Endpoint Manager product documentation: • *Tivoli Endpoint Manager Administrator's Guide* • *Tivoli Endpoint Manager Console Operators Guide*
Create a site where you want to group the AccessAgent Fixlets, dashboards, and analysis.	"Creating Custom Sites" from the *Tivoli Endpoint Manager Console Operators Guide*. For more information, see the IBM Tivoli Endpoint Manager product documentation.
Upload the required files on the server with the **Windows Software Distribution Wizard**.	**For AccessAgent installation or upgrade Fixlet** "Uploading the AccessAgent installer file" on page 5 **For AccessAgent patch management Fixlet** "Uploading the AccessAgent fix pack or interim fix" on page 11 **For dashboard** "Deploying and viewing the dashboard" on page 15
Create or edit the Fixlet.	**For AccessAgent installation or upgrade Fixlet** "Customizing and importing the Fixlet" on page 6 **For AccessAgent patch management Fixlet** "Customizing and importing the Fixlet (patch management)" on page 13 **For dashboard** "Deploying and viewing the dashboard" on page 15

Related information:

IBM Tivoli Endpoint Manager product documentation

Creating Custom Sites

Benefits

The IBM Tivoli Endpoint Manager and IBM Security Access Manager for Enterprise Single Sign-On integration provides key benefits to your organization.

The key benefits are:

- Easier AccessAgent deployment. You can easily manage which computers to install AccessAgent.
- Both Administrators and regular users can install AccessAgent, a fix pack, or an interim fix on the client.
- IBM Tivoli Endpoint Manager for Patch Management delivers patches for AccessAgent through a single console.
  - Client computers that run with Tivoli Endpoint Manager Client and AccessAgent are regularly checked for vulnerabilities.
  - If there is any new fix pack or interim fix for AccessAgent, IBM Tivoli Endpoint Manager deploys it to the subscribed client with Fixlets.

Chapter 2. Fixlet for AccessAgent installation or upgrade

Use the roadmap to create and deploy a Fixlet for installing or upgrading AccessAgent from previous releases to the latest release version.

Table 3. Installation or upgrade roadmap

	Task	See
1.	Customize the AccessAgent installer through the `SetupHlp.ini` file.	"Customizing the AccessAgent installer"
2.	Create a site where you want to group the AccessAgent Fixlets.	"Creating Custom Sites" in the *Tivoli Endpoint Manager Console Operators Guide*. For more information, see the IBM Tivoli Endpoint Manager product documentation.
3.	Upload the AccessAgent installer in the BES Server through the **Windows Software Distribution Wizard** .	"Uploading the AccessAgent installer file"
4.	Import the `*.BES` file to the Fixlet repository on your site.	"Customizing and importing the Fixlet" on page 6
5.	Deploy the Fixlet.	"Deploying the Fixlet" on page 7

Related information:

Creating Custom Sites

Customizing the AccessAgent installer

Customize the behavior of the AccessAgent installer through the `SetupHlp.ini` file.

About this task

For more information, see "Response file parameters (`SetupHlp.ini`)" in the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.

Procedure

1. Access the `SetupHlp.ini`, which is located in the `Config` folder. For example:

   32-bit `aa-8.2.1.0100\{9713108D-08D5-474E-92A3-09CD7B63DB34}\Config`

   64-bit `aa-8.2.1.0100_x64\{E72C4028-45BB-4EE6-8563-3066EEB39A84}\Config`
2. Set the value of `RebootEnabled` to `0` to disable computer restart.
3. Set the value of `ImsConfigurationEnabled` to
   - `1` - To download the Machine Wallet from the IMS Server.
   - `0` - To bypass the downloading of the Machine Wallet from the IMS Server.
4. Optional: If you set `ImsConfigurationEnabled` to `1`, specify a valid IMS Server name for `ImsServerName`. For example: `IMSServer.example.com`

Uploading the AccessAgent installer file

Use the **Windows Software Distribution Wizard** to upload the AccessAgent installer file to the BES Server. Use this distribution wizard to distribute the installer files if you do not have an HTTP Server to host downloads.

Before you begin

You must have a copy of the AccessAgent installer file.

About this task

The wizard guides you through the required information to upload the AccessAgent installer into a shared server from which client computers can access and download it. You also use this wizard to obtain information about the uploaded installer file such as the SHA1, download link, and size.

The file that you select is uploaded on the BES Server. A *SHA1* Checksum is calculated for security and caching purposes.

Procedure

1. Log on to the Tivoli Endpoint Manager Console.
2. Select **Wizards** > **BES Support** > **Windows Software Distribution Wizard**.
3. Specify the name of the application you want to deploy. This name is displayed in the **Task** tab in the BES Server. For example: `AccessAgent`
4. Specify the source of the package to be deployed to the BES Client computers.

   For new installation or upgrade, select the **Folder** and **Include Subfolders** check box.
5. Click **Next**.
6. Complete the wizard with the default settings.
7. Click **Finish** to compress and upload the AccessAgent installer files. The Create Task window is displayed.
8. On the **Actions** tab, copy and store the `Prefetch...` line from the action script. For example: `aa-8.2.1.0501.exe.tmp sha1:1772361bb95e1d8e34b462110708f91fe687fa94 size:83147051`
9. Cancel the task creation. Do not save the created task.

What to do next

"Customizing and importing the Fixlet"

Customizing and importing the Fixlet

This customized Fixlet accesses the AccessAgent installer that you uploaded and installs it to the relevant or target computers.

About this task

Customize the sample Fixlet (`.BES` file) with the values from step 8 of Uploading the AccessAgent installer file. Import the Fixlet in to your custom site.

Procedure

1. Get the sample Fixlet file `AccessAgent Installer Deployment.BES` from the source code package.
2. Replace the value of the following parameters in the file with the value that you copied from uploading the AccessAgent installer file in the **Windows Software Distribution Wizard**. For example:

```
parameter "AAVersion" =  "<AAVersion>"
parameter "name" = "<name>"
parameter "name64" = "<name64>"
parameter "sha1" = "<sha1>"
parameter "sha164" = "<sha164>"
parameter "size" = "<size64>"
parameter "size64" = "<size64>"
parameter "url" = "<url>"
parameter "url64" = "<url64>"
```

Important: The AccessAgent version must be in Windows Format like `08.02.03001` or `08.02.00501`.

3. Save the file.
4. In the Tivoli Endpoint Manager Console, click **File** > **Import**.
5. Select the `AccessAgent Installer Deployment.BES`.
6. In the Create Fixlet window, import the file in your custom site.

What to do next

- "Adding your server to the white list"
- "Deploying the Fixlet"

Adding your server to the white list

IBM Tivoli Endpoint Manager uses a white-list for dynamic downloading to ensure that only trusted sites are accessed. As such, you must add your server to this white-list to avoid an error during Fixlet deployment.

The dynamic downloading white-list is in `<BES Server Install Path>\Mirror Server\Config\DownloadWhitelist.txt`. This file contains a list of URLs formatted as regular expressions. For example:

```
http://.*\.sitename\.com/.*
http://software\.sitename\.com/.*
http://download\.sitename\.com/patches/JustThisOneFile\.qfx
```

The URL you provide in a prefetch statement must match an entry in the white-list before it can be downloaded. If a requested URL fails to match an entry in the white-list, the download immediately fails with status `NotAvailable`. A note is made in the Relay log containing the URL that failed to pass. An empty or non-existent white-list causes all dynamic downloads to fail. A white-list entry of ".*" (dot star) allows any URL to be downloaded.

For more information about the white-list, see "Dynamic Downloading" in the IBM Tivoli Endpoint Manager product documentation.

Related information:

http://pic.dhe.ibm.com/infocenter/tivihelp/v26r1/topic/com.ibm.tem.doc_8.2/Platform/Action/c_dynamic_downloading.html

Deploying the Fixlet

To deploy the Fixlet, run the action script on the computers that you specified and on the schedule and other criteria that you set.

Before you begin

Complete the following tasks:

1. "Customizing the AccessAgent installer" on page 5
2. "Uploading the AccessAgent installer file" on page 5
3. "Customizing and importing the Fixlet" on page 6

About this task

You can use this procedure for AccessAgent installation, upgrade or patch management.

Procedure

1. Open the relevant AccessAgent Fixlet.
2. Click **Take Action**.
3. In the Take Action window, define the settings for the Fixlet deployment.
   a. Specify the target computers.
   b. Schedule the Fixlet deployment and how the Fixlet must behave when deployed.

      You can have a supervised or non-supervised deployment. For supervised Fixlet deployment, the AccessAgent installation requires Administrator privileges.
   c. Define the user participation in the deployment.

      Select from the following options:

      Run only when there is no user logged on
      Select this option for silent installation.

      Run independently of user presence, and display the user interface to the selected users
      Select this option so that even users who are not Administrators, can install AccessAgent.

      Run when at least one of the selected users is logged on, and only display the user interface to those users

      Select this option if you want only Administrators to install AccessAgent.

      Select users in the Local user group Administrators.
   d. Choose whether to display a message before or while the action is running.
   e. Optional: Make the action an offer.
   f. Under Post-Action, select **Restart computer after action completes**. You can also select other actions to be implemented after the Fixlet is deployed.
   g. Define to which computer the Fixlet is relevant or applicable.
   h. Define the success criteria for the Fixlet deployment.
   i. Use the action script from the original Fixlet or use a different action script.
   j. Click **OK**.

Results

The Fixlet is applied on the specified computers.

Related information:


Action


Deploying the Action

Chapter 3. Fixlet for AccessAgent patch management

The Fixlet can automatically deploy the required patches on a 32-bit or 64-bit endpoint.

Use the following roadmap to create and deploy a Fixlet for installing AccessAgent fix pack or interim fix. Use the Fixlet to automatically deploy the required patches on a 32-bit or 64-bit endpoint.

Note: AccessAgent fix packs and interim fixes are cumulative. Patches with a higher version number always contain the content of patches with a lower version number. For example, you do not need to install `8.2.1-ISS-SAMESSO-AA-FP0012` before you install `8.2.1-ISS-SAMESSO-AA-IF0014`. The interim fix contains the preceding fix pack.

Table 4. Patch management roadmap

	Task	See
1.	Create a site where you want to group the AccessAgent Fixlets.	"Creating Custom Sites" in the *Tivoli Endpoint Manager Console Operators Guide*. For more information, see the IBM Tivoli Endpoint Manager product documentation.
2.	Upload the AccessAgent fix pack or interim fix in the BES Server through the **Windows Software Distribution Wizard**.	"Uploading the AccessAgent fix pack or interim fix"
3.	Upload the `AAPatchInfo.txt` in to your custom site.	"Uploading the AAPatchInfo.txt file" on page 13
4.	Import the `*.BES` file to the Fixlet repository on your site.	"Customizing and importing the Fixlet (patch management)" on page 13
5.	Deploy the Fixlet.	"Deploying the Fixlet" on page 7

Note: For subsequent AccessAgent fix packs or interim fix deployment, you need to complete steps 2, 3, and 5 only.

Related information:

Creating Custom Sites

Uploading the AccessAgent fix pack or interim fix

Use the **Windows Software Distribution Wizard** to upload the AccessAgent fix pack or interim fix to the BES Server. Use this distribution wizard to host the files if you do not have an HTTP Server to host downloads.

Before you begin

You must have a copy of the AccessAgent fix pack or interim fix.

For example:

- `8.2.1-ISS-SAMESSO-AA-FP0014_32.msp`
- `8.2.1-ISS-SAMESSO-AA-FP0014_64.msp`

About this task

The wizard guides you through the required information to upload the AccessAgent patches into a shared server from which client computers can access it. You also use this wizard to obtain information about the uploaded fix pack or interim fix file such as the *SHA1*, download link, and size.

The file that you select is uploaded on the BES Server. A *SHA1* Checksum is calculated and stored in the action for security and caching purposes.

Procedure

1. Log on to the Tivoli Endpoint Manager Console.
2. Select **Wizards** > **BES Support** > **Windows Software Distribution Wizard**.
3. Specify the name of the application you want to deploy. This name is displayed in the Task tab in the BES Server. For example: `AccessAgent Patch Management`
4. Specify the source of the package to be deployed to the BES Client computers. Select **File** then browse for the `.msp` file.
5. Click **Next**.
6. Complete the wizard with the default settings.
7. Click **Finish** to compress and upload the AccessAgent installer files. The Create Task window is displayed.
8. On the Actions tab, get the patch information from the action script. For example:

   For 32-bit

   ```
   8.2.1-ISS-SAMESSO-AA-FP0015_32.msp.tmp
   sha1:6104a5624d57ab9e97e13ee02a224c165200734a size:24107498
   http://WMSvc-W2K8RAA1:52311/Uploads/
   6104a5624d57ab9e97e13ee02a224c165200734a/8.2.1-ISS-SAMESSO-AA-
   FP0015_32.msp.tmp
   ```

   For 64-bit

   ```
   8.2.1-ISS-SAMESSO-AA-FP0014_64.msp.tmp
   sha1:1772361bb95e1d8e34b462110708f91fe687fa94 size:83147051
   http://WMSvc-W2K8RAA1:52311/Uploads/
   1772361bb95e1d8e34b462110708f91fe687fa94/8.2.1-ISS-SAMESSO-AA-
   FP0016_64.msp.tmp
   ```

9. Create a text file with the file name `AAPatchInfo.txt`
10. Edit the `AAPatchInfo.txt` with the information from step 8.

    Note:

    - The patch information for the patch file must be in this format: `name=<name> sha1=<sha1> size=<size> url=<url>`
    - You can provide the patch information for both 32-bit and 64-bit patches at the same time.
    - Each patch information must be specified in ONE continuous line.

      ```
      name=8.2.1-ISS-SAMESSO-AA-FP0015_32.msp.tmp
      sha1=6104a5624d57ab9e97e13ee02a224c165200734a size=24107498
      url=http://WMSvc-W2K8RAA1:52311/Uploads/
      6104a5624d57ab9e97e13ee02a224c165200734a/ 8.2.1-ISS-SAMESSO-AA-
      FP0015_32.msp.tmp name=8.2.1-ISS-SAMESSO-AA-FP0015_64.msp.tmp
      sha1=1772361bb95e1d8e34b462110708f91fe687fa946  size=24107498
      ```

```
url=http://WMSvc-W2K8RAA1:52311/Uploads/
1772361bb95e1d8e34b462110708f91fe687fa946/ 8.2.1-ISS-SAMESSO-AA-
FP0015_64.msp.tmp
```

What to do next

"Customizing and importing the Fixlet (patch management)"

Uploading the AAPatchInfo.txt file

The `AAPatchInfo.txt` file contains the information of the `.msp` file that you uploaded. Upload the `AAPatchInfo.txt` file in your custom site so that you can reuse the Fixlet for other fix packs or interim fixes.

Procedure

1. On the Tivoli Endpoint Manager Console, select your custom site.
2. Right-click **Files** > **Add files**.
3. In **Add to site**, select your custom site.
4. Browse for the location of the `AAPatchInfo.txt` file.
5. Select **Send to clients**.
6. Click **Add files** to finish.

Customizing and importing the Fixlet (patch management)

Customize the sample Fixlet. Import the Fixlet in to your custom site. This customized Fixlet accesses the AccessAgent fix pack or interim fix that you uploaded and installs it to the relevant or target computers.

Procedure

1. Get the sample Fixlet file `AccessAgent Patch Deployment.BES` from the source code package.
2. Optional: Customize the Fixlet file based on the requirements or preference of the organization.
3. Save the file.
4. In the Tivoli Endpoint Manager Console, click **File** > **Import**.
5. Select the `.BES` file for new AccessAgent installation.
6. In the Create Fixlet window, import the file in your custom site.

What to do next

- "Adding your server to the white list" on page 7
- "Deploying the Fixlet" on page 7

Chapter 4. AccessAgent dashboard

The IBM Tivoli Endpoint Manager and IBM Security Access Manager for Enterprise Single Sign-On dashboard provides a visual overview and textual information that is related to the AccessAgent deployment on the endpoints.

You can collect the following data:

- The version of AccessAgent running on the endpoints
- The maintenance level of AccessAgent running on the endpoints
- The type of second authentication factors that are supported on the endpoints
- The types of AccessAgent desktop configuration per endpoint
- Whether the endpoint is a Citrix Server

You can generate and view the following charts:

- The number of endpoints and the AccessAgent version (maintenance level)
- The maximum number of endpoints and the authentication factors
- The number of endpoints for each AccessAgent desktop configuration, whether shared, private, or personal desktop configuration
- The number of endpoints for each operating system or Citrix Server

Deploying and viewing the dashboard

In the dashboard, you can view diagrams and statistics that summarize the AccessAgent deployment on the endpoints.

Before you begin

Ensure that you have a copy of the `AccessAgent Deployment Status Dashboard` package.

About this task

The following files or terms are used:

- `Collect Client Info for Dashboard.bes` file - The dashboard Fixlet.
- *AccessAgent_site* - A variable. The actual name depends on your setup.

Procedure

1. Log on to the Tivoli Endpoint Manager Console.
2. Upload the `DashboardInfoCollector`.
   a. Select **Wizards** > **BES Support** > **Windows Software Distribution Wizard**.
   b. Specify the name of the application you want to deploy. This name is displayed in the Task tab in the BES Server.
   c. Specify the source of the package to be deployed to the BES Client computers.

      Select the **Folder** and **Include Subfolders** check box.
   d. Complete the wizard with the default settings.
   e. Click **Finish** to compress and upload the file. The Create Task window is displayed.

f. Keep a copy of the prefetch item line. You need this information to update the dashboard Fixlet.

3. Import all of the `.BES` files from the **Analyses** folder.
   a. In the Tivoli Endpoint Manager Console, click **File** > **Import**.
   b. Select all the `.BES` files.
   c. Import the file in your custom site.
4. Edit and import the `Collect Client Info for Dashboard.bes` file from the **Fixlets** folder.
   a. Open the `Collect Client Info for Dashboard.bes` file with any text editor.
   b. Search for the following parameters:

```
parameter "name" = "<name>"
parameter "sha1" = "<sha1>"
parameter "size" = "<size>"
parameter "url" = "<url>"
```

   c. Replace the variables `<name>`, `<sha1>`, `<size>`, `<url>` with the values from the prefetch item line that you noted from step 2 on page 15
   d. In the Tivoli Endpoint Manager Console, click **File** > **Import**.
   e. Select the `Collect Client Info for Dashboard.bes` file.
   f. Import the file in your custom site.
5. Import all other files from the `AccessAgent Deployment Status Dashboard` package into your custom site.
   a. On the Tivoli Endpoint Manager Console, select your custom site.
   b. Right-click **Files** > **Add files**. The Add Files to Site window is displayed.
   c. In the **Add to site**, select your custom site.
   d. Browse for the location of the files.
   e. Click **Add files** to finish.
6. Optional: Run the Fixlet one time to retrieve the updated data for the shared desktop information in the desktop configuration dashboard.

   Note: If the desktop configuration of the organization changes frequently, run the dashboard Fixlet regularly. Set a regular schedule to run the Fixlet.
7. Select **Sites** > **Custom Sites** > *AccessAgent_site* > **Dashboards** > **Deployment Overview**.
8. When prompted, enable the dynamic content. The AccessAgent Deployment Overview dashboard is displayed.

Installed AccessAgent version

Use the dashboard to view a statistics report of the AccessAgent deployment in the organization.

The dashboard displays a pie chart diagram and table that summarizes:

- The different AccessAgent versions that run on *x* number of endpoints in the organization.
- The AccessAgent release version and maintenance level.

To view the computer-specific information, click the **AccessAgent Deployment Status** link.

Use these statistics for analysis. Based on these data, you can learn the following information:

- Determine how many and which endpoints require an AccessAgent upgrade.
- Determine the number of endpoints that have the latest patches and those endpoints that require patch updates.

Second factor enabled

Use the dashboard to view a statistics report of the second authentication factors that are enabled in the organization.

The dashboard displays a pie chart diagram and its corresponding table of statistics. The dashboard summarizes the following information:

- The types of authentication factors that are supported in the deployment.
- The *x* number of endpoints that uses these authentication factors.

To view the computer-specific information, click the **AccessAgent Second Factor** link.

Use these statistics for analysis. Based on these data, you can learn the following information:

- Determine the type of authentication factors that users are likely to use for a set of endpoints.
- Determine the number of endpoints that are configured to handle a smart card, RFID, or fingerprint reader.
- Determine the number of users who logs on to AccessAgent with smart card, RFID, fingerprint, or password only.

With this information, you can analyze and improve the security and accessibility of the endpoints in the organization.

Desktop configuration

Use the dashboard to view a statistics report of the desktop configuration in the organization, whether they use a shared, private, or personal desktop configuration.

The dashboard displays a pie chart diagram and table that summarizes:

- The types of desktop configuration that are implemented or available in the organization. The types are shared, private, or personal.

  Shared workstation

  This configuration applies for organizations where users share common workstations. For example, healthcare organizations where doctors and nurses share workstations that are deployed throughout the hospital.

  Criteria to determine whether the desktop configuration is shared:

  – The `pid_unlock_option` policy is set to `3`.

  Private desktop (Windows XP)

  In a private desktop mode, users have their own Windows desktop in a workstation. The private desktop (Windows XP) is visible to only the individual user. No other user can view it.

  Criteria to determine whether the desktop configuration is private:

  – The `pid_lusm_sessions_max` policy is set to `1`.

Personal workstation

This configuration is more applicable for organizations where users are assigned their own workstations. These workstations are not shared with any other users.

- The *x* number of endpoints that uses these desktop configurations.

Note:

- If you see a `Not available` entry in the dashboard, it can be caused by a misconfiguration of the endpoint, or the Fixlet is not running.
- If the shared workstation or personal workstation is using AccessAgent version 8.1, the dashboard cannot collect and display the actual statistics data. `Not available` is displayed instead.

To view the computer-specific information, click the **AccessAgent Deployment Configuration** link.

Use these statistics for analysis. Based on these data, you can

- Determine how many and which endpoints require desktop configuration changes.

Endpoint information

Use the dashboard to view a statistics report on the operating systems that are supported in the AccessAgent deployment.

The dashboard displays a pie chart diagram and table that summarizes:

- The operating systems that are used in the AccessAgent deployment.
- Whether AccessAgent is deployed on a Citrix Server.
- The number of endpoints that run on each of the listed operating systems.

To view the computer-specific information, click the **AccessAgent Client Information** link.

Use these statistics for analysis. You can learn the following information:

- Determine whether AccessAgent is running on a Citrix Server.
- Determine the number of AccessAgent workstations that runs on which operating systems .

You can determine which operating system is critical and which one is less important in the organization.

Chapter 5. Dashboard customization

Your organization might require the collection of new categories of statistical information. To display this information, you can add new sections to the dashboard. Each new section requires a corresponding JavaScript file to generate the new content.

Creating a section in the dashboard

You can collect a new category of statistical information and display these statistics as a new section in the dashboard. A new section in the dashboard consists of a pie diagram and its corresponding table of statistics.

Before you begin

Ensure that you have a copy of the `AccessAgent Deployment Status Dashboard` package. You must modify the following files from this package:

- `accessagent-deployment.ojo`: The central controller of all the dashboard files. Use this file to link the different JavaScript files that are necessary to create, update, and display the contents of the dashboard.
- `accessagent-deployment_en-us.xml`: The string resource file. Use this file to declare the text labels to display in the dashboard user interface.
- `Dashboards.js` - Use this file to specify the different JavaScript file names that corresponds to each of the sections that are displayed in the dashboard user interface.

Procedure

1. Create an `Analyses` to collect specific information about the AccessAgent deployment that you want to add in your current dashboard. See the topic about creating analyses from the *Tivoli Endpoint Manager Console Operators Guide* in the IBM Tivoli Endpoint Manager product documentation.
2. Create a JavaScript file for the new section. See "Creating your own JavaScript file" on page 20.

   Important: The JavaScript file name must be the same as the global variable name that is defined inside the JavaScript file.
   For example:
   - `SampleDashboardSection.js` is the JavaScript file name.
   - `SampleDashboardSection` is the global variable name.
3. Add the JavaScript file name in the `Dashboards.js`. For example:

   ```
   var g_DashboardList = ["DeploymentInfo","SecondFactor","DesktopConfig",
   "EndpointInfo","SampleDashboardSection"];
   ```
4. Add the JavaScript file in the `accessagent-deployment.ojo`. For example:

   ```
   <script type="text/javascript" src="OJOShared.js"></script>
   <script type="text/javascript" src="JSResourceManager.js"></script>
   <script type="text/javascript" src="swfobject.js"></script>
   <script type="text/javascript" src="AC_OETags_Flash.js"></script>
   <script type="text/javascript" src="Dashboards.js"></script>
   <script type="text/javascript" src="CreateHTMLContent.js"></script>
   <script type="text/javascript" src="dsUtils.js"></script>
   <script type="text/javascript" src="Util.js"></script>
   <script type="text/javascript" src="DesktopConfig.js"></script>
   ```

```
<script type="text/javascript" src="DeploymentInfo.js"></script>
<script type="text/javascript" src="EndpointInfo.js"></script>
<script type="text/javascript" src="SecondFactor.js"></script>
<script type="text/javascript" src="SampleDashboardSection.js"></script>
<script type="text/javascript" src="Accessagent_Deployment.js"></script>
```

What to do next

"Deploying and viewing the dashboard" on page 15

Creating your own JavaScript file

Each statistic section that is displayed in the dashboard requires a corresponding JavaScript file. This JavaScript file contains a set of different functions that are run to generate the content for that section in the dashboard.

About this task

The JavaScript file contains the following main functions:

- `SampleDashboardSection.build = function()`: This function is called when updating the pie chart and the table in the dashboard section.
- `SampleDashboardSection.buildHTML = function(index)`: This function is called when creating the HTML code for the dashboard section.

Procedure

1. Create a JavaScript file for the new section.

   Note:

   The sample code shows how to create a dashboard section with two `.BES` properties. One of the `.BES` properties is used to categorize endpoints. You may add more `.BES` properties, see "Utility functions" on page 22.

   - Replace the content in <> with proper values.
   - The resource key and value pair must be defined in `accessagent-deployment_en-us.xml`. See step 2 on page 22.
   - Use the same property for function `funcKeyGenerating` and `funcFlashVarsGenerating`.

```
SampleDashboardSection = function() {
/**
    *[Func]This function will be called when a new dashboard is created
   *or the refresh button on the ISAM ESSO Dashboard is clicked.
    *It gets raw input data from analyses, update the pie chart and
   *table in a section accordingly.
    */
    this.build = function() {

       var property1 = "<Put your own property name>";
       var property1Array = EvaluateRelevance
       ("<Put your own bes property relevance here>");
       var property2 = "<Put your own property name>";
       var property2Array = EvaluateRelevance
       ("<Put your own bes property relevance here>");

       var map = createSortableMap(this.funcKeyGenerating, property1,
       property1Array, property2, property2Array);

       updateDashboard(map,
       "<ID for the HTML Table elemement>",
```

```
      "<ID for the pie chart>",
      "<ID for the HTML Div elemement of the pie chart>",
      this.funcFlashVarsGenerating);
   };

   /**
   *[Func]This fucntion will be called when a new dashboard is created.
   *It generates HTML layout for the section.
   */
   this.buildHTML = function(index) {

      var htmlCreator = new HTMLContentCreator();

      var tableHead_resourceNamesBundle = ["<Resource key of the first table
      head item >",
      "<Resource key of the second table head item>", "NumberOfEndPoints"];


      htmlCreator.createSectionHTML(index,
      "<ID for the HTML Div elemement of the pie chart>",
      "<Resource key of the title of the pie chart>",
      "<ID for the HTML Table elemement>",
      "<Resource key of the caption of table>",
      tableHead_resourceNamesBundle);

      htmlCreator.createAnalysisInfo("<ID for the HTML Table elemement>",
      "<Name of the associate BES Analysis>");

   }

   /**
   *[Func]Create input parameter "FlashVars" for the pie chart flash object.
   */
   this.funcFlashVarsGenerating = function(map) {
      var flashVars = "";
      var displayName;
      var str;

      var keys = map.getSortedKeys();
      for (var i in keys) {
      str = map.get(keys[i])["<Name of either property you defined in build
       function>"];
      flashVars = flashVars.concat(str, "=", map.get(keys[i]).numOfInstances,
       "&");
       }

       return flashVars;
   };

   /**
   *[Func]Create categorization/sort key to count the statistics.
   */
   this.funcKeyGenerating = function(endpointItem) {
       return endpointItem["<Name of either property you defined in build
       function>"];
   };
}
```

Important:

- The JavaScript file name must be the same as the variable name that is defined inside the JavaScript file. In this example:
  - `SampleDashboardSection.js` is the JavaScript file name.
  - `SampleDashboardSection` is the variable name.

Tip: You can see the following files from the AccessAgent Deployment Status Dashboard package for the sample content:

- DeploymentInfo.js
- DesktopConfig.js
- EndpointInfo.js
- SecondFactor.js

2. Add the text labels for the new section, in the accessagent-deployment_en-us.xml file by using any text editor.
   a. Add a <map></map> entry for each new text label that you want to display in the dashboard.
   b. Assign a unique ID inside the<key></key> parameters, for each text label.
   c. Specify the actual text label to be displayed in the dashboard user interface.

   For example:

```
<map>
  <key>AAMaintenanceLevel</key>
   <value>Maintenance Level</value>
</map>
```

Utility functions

The JavaScript for the new dashboard section implements several utility functions.

createSortableMap

Definition	createSortableMap(funcKeyGenerating, property1, property1Array, property2, property2Array,...);
Description	Converts the raw analyses data to map.
Parameters	• funcKeyGenerating - (Function) To generate the key of entries • property1, property2 - (String) The output of analyses • property1Array, property2Array- (Array) Property of the same end point • ... - indicates that you can add more pairs of (property, propertyArray)
Return Values	SortableCategoryMap

updateDashboard

Definition	updateDashboard(map, tableID, pieChartID, pieChartDivID, funcFlashVarsGenerating)
Description	Generic function to fill up the information in the pie chart and table.
Parameters	• map- (Object SortableCategoryMap) Created by createSortableMap • tableID - (String) The ID for the HTML Table element • pieChartID - (String) The ID for the pie chart • pieChartDivID - (String) The ID for the HTML Div element of the pie chart • funcFlashVarsGenerating- (Function) To generate the input parameter "FlashVars" for flash object
Return Values	Nothing

HTMLContentCreator.createSectionHTML

Definition	`HTMLContentCreator.createSectionHTML(index, piechartDivID, piechartTitle_resourceName, tableID,tableTitle_resourceName, tableHead_resourceNamesBundle);`
Description	This function generates the HTML layout for the section. It is called when a new dashboard is created.
Parameters	• `index` - (Integer) The order of the section in `g_DashboardList` • `piechartDivID` - (String) The ID for the HTML Div element of the pie chart • `piechartTitle_resourceName` - (String) The resource key of the name of the pie chart • `tableID` - (String) The ID for the HTML Table element • `tableTitle_resourceName` - (String) The resource key of the name of the table • `tableHead_resourceNamesBundle`- (Array of strings) These are the resource keys of the head of the table
Return Values	Nothing

HTMLContentCreator.createAnalysisInfo

Definition	`HTMLContentCreator.createAnalysisInfo(tableID, analysisName)`
Description	Function to create the description string. For example: `"For detailed machine specific information, go to BES Analysis AccessAgent Deployment Status."`
Parameters	• `tableID` - (String) The ID for the HTML Table element • `analysisName` - (String) The name of the associate BES Analysis
Return Values	Nothing

AccessAgent SDK

The `AccessAgent Deployment Status Dashboard` package includes an `AASDK.dll` file, which is a COM-based DLL file. You can use this file to collect AccessAgent 8.2.1 information that you want to display in the dashboard.

The Desktop configuration section in the dashboard uses the `AASDK.dll` file to collect data related to machine policies.

AASDK.AAPolicyProvider

Use this object to query AccessAgent policies on the endpoint.

Definition	`HRESULT RetrieveUnsignedLongPolicy([in]BSTR bstrPolicyId, [in]ULONG ulDefaultVal, [out,retval]ULONG* lPolicyVal);`
Description	Obtain unsigned long machine policy for AccessAgent.
Parameters	• `bstrPolicyId` - Policy ID • `ulDefaultVal` - Default value of the policy • `lPolicyVal` - Actual value of the policy
Return Values	

Definition	`HRESULT RetrieveStringPolicy([in]BSTR bstrPolicyId, [in]BSTR bstrDefaultVal, [out,retval]BSTR* bstrPolicyVal);`
Description	Obtain string machine policy for AccessAgent.
Parameters	• `bstrPolicyId` - Policy ID • `bstrDefaultVal` - Default value of the policy • `bstrPolicyVal` - Actual value of the policy
Return Values	

Definition	`HRESULT RetrieveBoolPolicy([in]BSTR bstrPolicyId, [in]VARIANT_BOOL bDefaultVal,[out,retval]VARIANT_BOOL* bPolicyVal);`
Description	Obtain boolean machine policy for AccessAgent.
Parameters	• `bstrPolicyId` - Policy ID • `bDefaultVal` - Default value of the policy • `bPolicyVal` - Actual value of the policy
Return Values	

AASDK.AboutInfoProvider

Use this object to query for the registry root and install path on the endpoint.

Definition	`HRESULT GetAARegistryRoot([out,retval] BSTR* bstrAARegistryRoot);`
Description	Obtain AccessAgent registry subroot path.
Parameters	`bstrAARegistryRoot` - AccessAgent registry subroot
Return Values	

Definition	`HRESULT GetAAInstallPath([out,retval] BSTR* bstrAAInstallPath);`
Description	Obtain AccessAgent installation path.
Parameters	`bstrAAInstallPath` - AccessAgent installation path
Return Values	

Chapter 6. Known issues and limitations

There are some known issues and limitations in the IBM Tivoli Endpoint Manager and IBM Security Access Manager for Enterprise Single Sign-On integration that might affect the Fixlet deployment or the dashboard results.

Known issues

Known issues in the IBM Tivoli Endpoint Manager or in the IBM Security Access Manager for Enterprise Single Sign-On can affect how the IBM Tivoli Endpoint Manager behaves or processes the information that is received from the AccessAgent deployment.

The IBM Tivoli Endpoint Manager and IBM Security Access Manager for Enterprise Single Sign-On integration has the following known issues:

The dashboard analyses result might not be correct if any of the end points are installed on a virtual desktop infrastructure.

Issue: The IBM Tivoli Endpoint Manager cannot recognize end points that are deployed in a virtual desktop infrastructure. For example, there are two virtual desktops that are installed with AccessAgent and the IBM Tivoli Endpoint Manager client. Each time the virtual desktop infrastructure pool is refreshed or updated, new computers with the same name are registered as new end points. Analyses data is recorded for these computers, which affects the dashboard results.

Workaround: Use a database cleanup tool to delete computer data that is older than a specified amount of time. For example, computers that have not checked-in.

Limitations

Limitations in the IBM Tivoli Endpoint Manager or in the IBM Security Access Manager for Enterprise Single Sign-On can affect how the IBM Tivoli Endpoint Manager behaves or processes information that is received from the AccessAgent deployment.

The IBM Tivoli Endpoint Manager and IBM Security Access Manager for Enterprise Single Sign-On integration has the following known limitations:

- If the shared workstation or personal workstation is using AccessAgent version 8.1, the dashboard cannot collect and display the actual statistics data. `Not available` is displayed instead.
- The AccessAgent SDK can only be used with AccessAgent 8.2 or 8.2.1.

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

T

U

W

Printed in USA

SC27-5620-00