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

Troubleshooting and Support Guide

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

Troubleshooting and Support Guide

Note

Before using this information and the product it supports, read the information in "Notices" on page 57.

Edition notice

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

Contents

About this publication v
Accessibility v
Technical training. v
Support information. v
Statement of Good Security Practices v

Chapter 1. Troubleshooting and support 1

Chapter 2. Learning more 3
About troubleshooting 3
About connectivity problems 5
About fixes and updates 5
About messages 6
About performance problems and hangs 6
About traps, crashes, and abends 8

Chapter 3. Troubleshooting checklist . . 9

Chapter 4. Known issues and workarounds 11
Installation issues 11
Cannot install AccessAgent 11
Cannot install the IMS Server 12
AccessAgent cannot connect to the IMS Server . 12
AccessAgent cannot download the IMS Server certificate 13
Conflict with another application 13
AccessAgent cannot register the module. . . . 14
IBM HTTP Server does not start 14
Configuration issues 14
IMS Server configuration failed. 14
Directory server configuration issues 15
Node federation failed. 16
Cannot sign up through AccessAgent. 16
Unable to configure Kerberos on WebSphere Application Server 16
User is unable to log on to AccessAgent. . . . 17
Application credentials are not listed in wallet manager in AccessAgent 18
Authentication factor issues 18
Common password issues 18
Lost authentication devices 19
Bio-key verification UI is not displayed on the private desktop 19
Smart card takes time to be recognized and the IMS Server is offline 19
Error when signing up from ESSO Credential Provider with smart card logon to Windows enabled. 20
Logon issues 20
Cannot log on to AccessAdmin. 20
Form-based logon to AccessAdmin does not work 21
Cannot log on to AccessAssistant - password is not synchronized 21
Cannot log on to the Integrated Solutions Console. 21
Slow performance, startup, and logon failure . . 23
Wallet-related issues 23
Common Wallet issues 23
Machine Wallet is not downloaded 24
Operational issues 25
Issues that you might encounter when using the Transparent Screen Lock 25
Cannot connect to AccessAdmin 25
AccessAdmin - Service is not available 26
Cannot open the httpd.conf file. 26
Cannot authenticate when a repository is down 26
IMS Server cannot issue a certificate for an application 27
Cannot single sign-on in a command prompt . . 27
AccessProfile is not displayed in the properties pane. 28
AccessStudio might stop working when you use the **Convert to** option 28
OutOfMemory error when you open an AccessProfile 28
Key pressed on a window trigger does not fire 28
Successful logon page might not be captured correctly when creating a profile in Mozilla Firefox 28
Database slowdown because of buildup of unused cached Wallets. 29
Single sign-on does not work on Microsoft Internet Explorer 29
Fields that are not functional in AccessAdmin . . 29
Unexpected form validation when changing the SSL value in the IMS Configuration Wizard . . 29
A message request that contains the character (and) fails 29
Non-ASCII characters cannot be used for application user name in IMS Server 30
Browser 30
Microsoft Internet Explorer stops working . . . 30
Mozilla Firefox interferes with the AccessAgent single sign-on feature 31
Single sign-on does not work in Mozilla Firefox 31
Cannot capture logon credentials in Mozilla Firefox pop-up window 31
Cannot open web applications 32
Back button does not work 32
Verifications 32
Determining the type of IMS Server deployment 32
Determining the Server AccessAgent mode. . . 33

Chapter 5. Fixes. 35
Obtaining fixes 35
Receiving fix notifications 35

Chapter 6. Searching knowledge bases 37

Chapter 7. Analyzing data 39

Chapter 8. Collecting data 41

Message and trace logs 41

Message logs 42

Trace logs 43

Configuring log settings 44

Configuring message logging 44

Enabling trace logging. 45

Viewing logs 47

Using IBM Support Assistant 47

Using the IBM Support Assistant in graphical mode 47

Using the IBM Support Assistant in console mode 48

Chapter 9. Contacting support 51

IBM Support Assistant. 51

IBM software maintenance contracts 52

Determining the business impact 53

Describing a problem 53

Submitting data 53

Notices 57

Glossary 61

A. 61

B 62

C 62

D. 63

E 64

F 64

G. 64

H. 64

I 65

J 65

K. 65

L 65

M 65

N. 66

O. 66

P 66

R 67

S 67

T 69

U. 69

V. 69

W 70

Index 71

About this publication

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.

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. Troubleshooting and support

The troubleshooting process, in general, requires that you isolate and identify a problem, then seek a resolution. For IBM Security Access Manager for Enterprise Single Sign-On, you can use a troubleshooting checklist to help you. If the checklist does not lead you to a resolution, you can collect additional diagnostic data and analyze it yourself. You can also submit the data to IBM Software Support for analysis.

Troubleshooting topics for IBM Security Access Manager for Enterprise Single Sign-On are organized according to the sequence of these steps:

1. Learn more about a symptom or feature.

   Before you can successfully troubleshoot a symptom, or a problem with a specific product feature, you need a basic understanding of that symptom or feature.
2. Follow the troubleshooting checklist for the appropriate feature or symptom.

   The troubleshooting checklist offers a series of questions to guide you through the process of isolating and identifying a problem. If the problem is known to IBM, the checklist guides you to a published fix, solution, or workaround.

   If the troubleshooting checklist has not led you to a resolution, continue to the next step.
3. Collect diagnostic data.

   This information explains how to gather the necessary information that you, or IBM Software Support, must have to determine the source of a problem.
4. Analyze diagnostic data.

   This information explains how to analyze the diagnostic data that you collected.

Chapter 2. Learning more

The first step in the troubleshooting process is to learn more about the problem symptoms, or about the affected product feature.

To learn more about the product features, see the other publications. Start with the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

About troubleshooting

Troubleshooting is a systematic approach to solving a problem. The goal is to determine why something does not work as expected and how to resolve the problem.

The first step in the troubleshooting process is to describe the problem completely. A problem description helps IBM to determine where to start in finding the cause of the problem. This step includes asking yourself basic questions, such as:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem. A good problem description is the best way to start down the path of problem resolution.

What are the symptoms of the problem?

When starting to describe a problem, the most obvious question is "What is the problem?" The question might seem straightforward, however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, fail, performance degradation, or incorrect result?
- How does the problem affect the business?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few components to be considered when you are investigating problems. The following questions can help you to focus on where the problem occurs to isolate the problem layer.

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?

- Is the current environment and configuration supported?

Remember that getting a report from one layer does not mean that the problem originated from that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system, its version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration. Many problems can be traced back to incompatible levels of software that are not intended to run together or have not been fully tested together.

When does the problem occur?

Develop a detailed timeline of events leading up to a failure, especially for those cases that are one-time occurrences. You can most easily trace the problem timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information.

Typically, you must look only as far as the first suspicious event that you find in a diagnostic log. However, doing so is not always easy to do and takes practice. Knowing when to stop looking is especially difficult when multiple layers of technology are involved, and when each has its own diagnostic information.

To develop a detailed timeline of events, try to answer these questions:
- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to the preceding questions can help to provide you with a frame of reference in which to investigate the problem.

Under which conditions does the problem occur?

Knowing what other systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These and other questions about your environment can help you to identify the root cause of the problem:
- Does the problem always occur when the same task is being performed?
- Does a certain sequence of events must occur for the problem to surface?
- Do any other applications fail at the same time?

Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically with problems that can be reproduced, you have a larger set of tools or procedures at your disposal to help you investigate. Consequently, problems that you can reproduce are often easier to debug and solve. However, problems that you can reproduce can have a disadvantage. If the problem significantly affects business, you do not want it to recur. If possible, recreate the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.
- Can the problem be recreated on a test machine?

- Are multiple users or applications encountering the same type of problem?
- Can the problem be recreated by running a single command, a set of commands, or a particular application, or a stand-alone application?

About connectivity problems

Connectivity problems typically involve multiple systems, including software, hardware, and communications. The best way to troubleshoot connectivity problems is through a process of elimination.

First, collect relevant data and determine what you know, what data you have not yet collected, and what paths you can eliminate. At a minimum, answer the following questions.

- Are the communication paths operational?
- Has the initial connection been successful?
- Is the problem intermittent or persistent?
- Have changes been made to the communication network that would invalidate the previous directory entries?
- Where is the communication breakdown encountered? For example, was the breakdown between the client and a server?
- Is the problem encountered only within a specific application?
- What can you determine by the content of the message and the tokens that are returned in the message?
- Are other systems able to perform similar tasks successfully? If the task is a remote task, is it successful when performed locally?

Next, try to isolate the problem by answering the questions in the Chapter 3, “Troubleshooting checklist,” on page 9.

About fixes and updates

If you encounter a problem with the IBM Security Access Manager for Enterprise Single Sign-On software, first check the list of updates to confirm that your software is at the latest maintenance level. Next, check the list of problems fixed to see if IBM has already published an individual fix to resolve your problem.

These lists are located at the Tivoli® Support Web site for IBM Security Access Manager for Enterprise Single Sign-On http://www.ibm.com/software/sysmgmt/products/support/index.html. Select **IBM Security Access Manager for Enterprise Single Sign-On** from the **Support for specific Tivoli products** list.

Individual fixes are published as often as necessary to resolve defects in IBM Security Access Manager for Enterprise Single Sign-On. Two kinds of cumulative collections of fixes, called fix packs and refresh packs, are published periodically for IBM Security Access Manager for Enterprise Single Sign-On. Fix packs and refresh packs bring users up to the latest maintenance level. Install these update packages as early as possible to prevent problems.

To receive weekly notification of fixes and updates, subscribe to My Support email updates. For more information, refer to “Receiving fix notifications” on page 35.

The following table describes the characteristics of each fix.

Table 1. Maintenance types

Name	Characteristics
Fix	• A single fix that is published between updates to resolve a specific problem. • After you install a fix, test any functions that the fixed component might affect.
Fix pack	• A fix pack contains all fixes that have been published since the previous fix pack or refresh pack. A fix pack might also contain new fixes. • Fix packs increment the modification level of the product and are named accordingly, for example, 5.0.1 • A fix pack can update specific components, or it can update the entire product image. • During fix pack installation, all previously applied fixes are automatically uninstalled. • After you install a fix pack, conduct a regression-test for all of the critical functions. • The most recent two fix packs are available for download (for example, 5.0.2 and 5.0.1). Earlier fix packs are not available.
Refresh pack	• A refresh pack contains all fixes that have been published since the previous fix pack or refresh pack, and new fixes. • A refresh pack typically contains new function, in addition to fixes, and it updates the entire product image. • Refresh packs increment the modification level of the product and are named accordingly, for example, 5.0.1. • During refresh pack installation, all previously applied fixes are automatically uninstalled. • After you install a refresh pack, you conduct a regression-test on all of the critical functions.

About messages

You can often resolve the problem stated in the warning or error message you get from IBM Security Access Manager for Enterprise Single Sign-On by reading the entire message text and the recovery actions that are associated with the message.

You can find the full text of messages, their explanations, and the recovery actions by searching for the message identifier in the *IBM Security Access Manager for Enterprise Single Sign-On Error Message Reference Guide*.

About performance problems and hangs

Performance problems arise in many different situations. A hang is one type of performance problem in which users wait for a response for an indefinite time. Troubleshooting techniques for hangs are similar to the techniques you would use for other performance problems.

Here are some examples of situations in which performance problems become evident:

- Query performance is slower than expected.
- The workload or a batch job is not completing as soon as expected, or a reduction in the transaction rate or throughput occurs.

- The overall system slows down.
- A bottleneck is suspected in one of the system resources such as processor, I/O, or memory.
- Query or other workload processing is using more resource than is expected or available.
- One system is performing better than another.
- A query, application, or system hangs.

Hangs can be difficult to troubleshoot because the symptoms often seem to match the symptoms of other problems. For example, if a user is waiting for a long time for a response from a query, that user might think that the system hanged. In many cases, the query might be complex, and the system might also be heavily used at the time, so the system has not hung. But, the system might be slow to respond. Also, during a system shutdown, a significant buildup of activity can result in most or all commands seem to hang.

Aside from characterizing the problem correctly in terms of what the symptoms are, and where the symptoms are observed, you need several other pieces of information to put the problem in context. Symptoms typically range from slowness, too much resource used, and so on. The symptoms are typically found in a query, application, system resource, and so on.

Answer the following questions to quickly determine the best place to start looking for the cause of the performance problem.

1. When did the problem first occur?

   If the problem has been occurring for some time, you might be able to use historical data to find differences. Historical data helps you to focus on changes in system behavior and then focus on why these changes were introduced. You also must consider whether any recent changes occurred, such as hardware or software upgrades, a new application rollout, additional users, and so on.
2. Is the performance issue constant or intermittent?

   If the poor performance is continual, check if the system has started to handle a larger workload. You can also check if a shared database resource has become a bottleneck. Other potential causes of performance degradation include increased user activity, multiple large applications, or removal of hardware devices. If performance is poor only for brief periods, begin by looking for common applications or utilities that run at these times. If users report that a group of applications are experiencing performance issues, you can begin your analysis by focusing on these applications.
3. Does the problem appear to be system-wide or isolated to IBM Security Access Manager for Enterprise Single Sign-On or its components?

   System-wide performance problems suggest an issue outside of IBM Security Access Manager for Enterprise Single Sign-On. Something at the operating system level must be addressed.
4. If the problem is isolated to one component, does one particular activity cause the problem?

   If one component seems to be causing the problem, you can evaluate whether users who are reporting that specific activity, are experiencing a slowdown. You might be able to isolate the issue to one component and a specific activity.
5. Do you notice any common characteristics of the poor performance, or does the problem occur in random?

Determine if any common functions are involved. The function involvement might indicate that these functions are a point of contention.

About traps, crashes, and abends

The terms *trap*, *crash*, and abnormally end (*abend*) are often used synonymously.

If IBM Security Access Manager for Enterprise Single Sign-On cannot continue processing as the result of a trap, segmentation violation, or exception, it generates an error.

Most traps, crashes, and abends for IBM Security Access Manager for Enterprise Single Sign-On result in an exception. The exception is included in the message log, and typically does not require a trace to be enabled in order for it to be reported. However, these errors can be recorded in a trace log, if you are instructed to enable trace logging by IBM Support personnel. If you open a problem report with IBM, you must provide the trace log for analysis.

These errors can be recorded in a trace log, if you are instructed to enable trace logging by IBM Support personnel.

If you open a problem report with IBM, you might need to provide the trace log for analysis.

Generate trace files only when IBM Software Support asks you to do so, although IBM Security Access Manager for Enterprise Single Sign-On can generate trace logs on demand. See "Trace logs" on page 43 for more information.

Chapter 3. Troubleshooting checklist

The following questions can help you to identify the source of a problem that is occurring with IBM Security Access Manager for Enterprise Single Sign-On.

1. Are your fixes and fix packs up to date?

   See "Obtaining fixes" on page 35 for more information.
2. Does the IBM Knowledge Base contain additional information about the problem?

   See Chapter 6, "Searching knowledge bases," on page 37.
3. Are you receiving any error messages?

   See the IBM Security Access Manager for Enterprise Single Sign-On *IBM Security Access Manager for Enterprise Single Sign-On Error Message Reference* for information about error messages.
4. Do the logs contain any messages about the problem?

   See "Message logs" on page 42 and "Trace logs" on page 43 for more information.
5. Does the problem occur while installing or uninstalling one of the following features?
   - IBM Security Access Manager for Enterprise Single Sign-On or its components

     See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.
   - WebSphere® Application Server

     See the installation troubleshooting topics in the IBM WebSphere Application Server information center at http://www.ibm.com/software/webservers/appserv/was/library/
6. Does the problem occur when you are configuring IBM Security Access Manager for Enterprise Single Sign-On?

   See the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.
7. If you cannot resolve the problem in the preceding steps, gather additional information about the location of the problem, or conditions during which the problem occurs:
   - Did the problem occur during runtime processing?
     - Did it fail to connect?
     - Did it crash?
     - Did it have a performance problem such as slow response, or a "hang"?
     - Did it abend, trap, or throw a Java™ exception?
   - Does the problem occur while you configure a specific function?
   - Does the problem occur when you perform a specific task?

   The answers to these questions might help you determine the location of the problem and assist you in locating additional information about the problem. For example, if the problem occurs while configuring a specific function or performing a specific task, you might find a solution in the documentation of that function or task.

If the checklist does not guide you to a resolution, you can collect additional diagnostic data. The additional data might be necessary to IBM Support personnel to help you continue troubleshooting the problem. See Chapter 8, “Collecting data,” on page 41.

Chapter 4. Known issues and workarounds

You might encounter some issues and limitations during the deployment or usage of IBM Security Access Manager for Enterprise Single Sign-On. Select the possible category of the issue you encountered and search for the issue and workaround.

To get more information about the issue, see Chapter 8, “Collecting data,” on page 41.

Installation issues

You can encounter issues during or after the installation of the product component. These issues can prevent you from successfully installing or using the component. Learn more about these issues and their workaround.

Cannot install AccessAgent

Different factors can cause the AccessAgent installation to fail.

The AccessAgent installation can fail for any of the following reasons:

The AccessAgent installer might be corrupted.
The AccessAgent installation file might be corrupted if it is not downloaded properly. Download the file again and ensure that all the required files are available.

The AccessAgent is installed from a shared location or a server.
Do not install the AccessAgent from a shared location or server. Copy the installer to a local disk drive on your computer before you run the installer.

The AccessAgent installer is not compatible with the operating system.
If you are using a 64-bit operating system, use the 64-bit AccessAgent installer. If you are using a 32-bit operating system, use the 32-bit AccessAgent installer.

The user who installed AccessAgent does not have Administrator privileges.
To install AccessAgent, you must have Administrator privileges.

You enabled the Windows settings Protect your data.
This setting prevents you to start the AccessAgent installer. Right-click the installer, and clear the **Protect your data** option.

Windows Scripting Host version is not enabled.
When you run the AccessAgent installer in silent mode, the installation is completed but when you restart the computer, the installation is corrupted.

Check the following registries before you install AccessAgent:

- `HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\Enabled`
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\Enabled`

Cannot install the IMS Server

Different factors can cause the IMS Server installation to fail.

The IMS Server installation can fail for any of the following reasons:

Database server has low disk space

Before you install the IMS Server, ensure that you have enough disk space for the database server and for the computer that hosts the IMS Server. See "Hardware and software requirements" in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

WebSphere Application Server security details are not correct

Specify the correct application security details.

- Ensure that you enter the correct SOAP port.

  Note: You can determine the correct port number in the following directory for each profile. For example:

  Stand-alone: `<was_home>/profiles/<AppSrv01>/logs/AboutThisProfile.txt`

  Network deployment: `<was_home>/profiles/<Dmgr01>/logs/AboutThisProfile.txt`

  For example:

  – For WebSphere Application Server Stand-alone, the SOAP port for the application server is `8880`.

  – For WebSphere Application Server Network Deployment, the SOAP port for the Deployment Manager is `8879`.

- If the security validation for WebSphere Application Server fails, you entered the wrong information. In this case, you can restart the installer.

WebSphere Application Server administration security settings are not correct

Ensure that you specify the correct:

- WebSphere administrative user name and password
- SSL trusted keystore password

WebSphere Application Server is not available

Ensure that:

- The WebSphere Application Server is started.
- The host name can be resolved.

An Installer UI Error is prompted when the IMS Server installer is executed on Windows Server 2012

Do the following tasks:

1. Change the compatibility level of installer .exe to Windows 7.
2. Run the installer in the command line.
3. Add **`-i GUI`** or **`-i Console`**.

AccessAgent cannot connect to the IMS Server

Different factors can affect the AccessAgent and IMS Server connection.

To verify whether the computer can connect to the IMS Server, enter the AccessAdmin URL in your browser from the client computer. If the AccessAdmin page is not displayed, the connection is not established.

AccessAgent cannot connect to the IMS Server for the following reasons:

The IMS Server is not running.
Ensure that the `ISAMESSOIMS` application is started in the Integrated Solutions Console.

The IMS Server location is not correct.

During installation, AccessAgent tries to automatically connect to the IMS Server. If a connection cannot be established, you are prompted to enter the location of the IMS Server. Ensure that the information provided is correct.

IMS Server certificate "cn" is not consistent with AccessAgent
Ensure that the `cn` of the IMS Server certificate is the same name that is provided for the AccessAgent.

There is no network connection.
Ensure that you have an Internet connection.

The client computer has a personal firewall or anti-spyware that blocks traffic from AccessAgent.
Ensure that the personal firewall or anti-spyware does not block traffic from `winlogon.exe`.

AccessAgent cannot download the IMS Server certificate

The IMS Server certificate download might fail if AccessAgent cannot connect to the IMS Server. The IMS Server certificate is used to identify the IMS Server.

This issue occurs when:

- AccessAgent tries to connect with the IMS Server but because of a heavy load, the connection times out.
- The IMS Server is starting and the connection fails because the IMS Server is not yet available.

If configured properly, AccessAgent downloads the IMS Server certificate to the computer. If the IMS Server certificate is not automatically downloaded, download it through the following options after you install AccessAgent:

- Select **Start** > **All Programs** > **AccessAgent** > **Set IMS Server Location**.
- Run `C:\Program Files\IBM\ISAM ESSO\SetupCertDlg.exe`.

Conflict with another application

Certain applications that are installed on your computer can conflict with the AccessAgent installation.

Issue: During the AccessAgent installation, the following message is displayed:

```
The AccessAgent setup has detected a conflict with <Application Name>
which is installed on your computer.
This conflict might not allow AccessAgent to run properly.
Uninstall the conflicting application.
Click Yes to exit from the setup.
Click No to ignore the conflict and continue with the installation.
```

Workaround:

1. Cancel the AccessAgent installation.
2. Uninstall the application that causes the conflict.

   Note: Make sure that the application is no longer used before you uninstall the application.
3. Run the AccessAgent installer again.

Note: AccessAgent might not work properly if you ignore the message prompt and continue with the installation.

AccessAgent cannot register the module

You might encounter a module-related problem during the AccessAgent installation.

Issue: During the AccessAgent installation, the following message is displayed:

```
The system encountered a problem while registering a module (Error 1904).
```

Workaround:

1. Ensure that:
   - You have Administrator privileges.
   - You have permissions to write into the registry.
   - No third-party applications prevent your access to the `system32.dll` registry.
2. Uninstall AccessAgent.
3. Install AccessAgent.

IBM HTTP Server does not start

There are instances where you must start the IBM HTTP Server during the IMS Server installation and configuration.

The IBM HTTP Server cannot start if:

There is already an application, listening to the same port.
Use a utility like **`netstat`** to check whether a port is already in use. For example: **`netstat -na -p tcp -o`**.

The Administrator password is changed

Check whether the Administrator password was changed. If the password was changed, change the password for the service in the Windows service definition panel.

Configuration issues

You can encounter issues during or after the configuration of the product component. These issues can prevent you from successfully configuring or using the component. Learn more about these issues and their workaround.

IMS Server configuration failed

If you manually create a database and you want to create the schema manually, log out from the SQL database server as SA. Log on to SQL with the user name you specified when you created a database user name and schema name. Otherwise, the IMS Server configuration might fail because of a wrong database configuration. This procedure must be done before you run the IMS Configuration wizard.

Issue: In the IMS Configuration wizard, when you click **Save**, the error message "Failed to upload IMS Server Soft CA" is displayed.

Workaround:

Check your schema name in the SQL database server if it belongs to the user that you created for the database.

See the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide* for the steps to set up the database and schema manually.

To run the IMS Server configuration again, follow this procedure:

- Run the `cleanImsConfig.bat` script in `C:\Program Files\IBM\ISAM ESSO\IMS Server\bin\`.
- Run the IMS Configuration wizard after the database and schema configuration.

Directory server configuration issues

You might encounter issues that are related to the directory server configuration, which can cause the IMS Server deployment to fail.

Directory server configuration tips:

- The administrative user name that you supply for the WebSphere administrator must not exist on the directory server. Delete the user name from the Active Directory.
- Avoid creating an administrative user with the same user name as the WebSphere administrator. For example, if the WebSphere administrator you provide is `wasadmin`, then the user `wasadmin` must not exist on the corporate enterprise directory.
- Avoid the use of *administrator* as the WebSphere Application Server administrator.
- Choose a user name that is least likely to conflict with your potential existing enterprise directory users.
- If the directory server is using an SSL connection, remember to add the directory server SSL certificates to the WebSphere Application Server. See "Adding the directory server SSL certificate to WebSphere Application Server" in the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.
- After the directory server configuration, restart the WebSphere Application Server immediately to apply the configuration changes. If you configure the web server definition and the directory server before you restart the WebSphere Application Server, the configuration is not saved.
- Ensure that the directory server repositories are running, and you can connect to these repositories. If one or more of the configured repositories are unreachable, you cannot authenticate or stop the WebSphere Application Server.

  This issue is because of a security feature of the virtual member manager. The virtual member manager always checks all repositories before user authentication. For more information about the solution, see http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.wim.doc/UnableToAuthenticateWhenRepositoryIsDown.html.
- The NetBIOS name is not validated. You must provide the correct name.

- To determine the correct NetBIOS computer name, go to the Microsoft website at www.microsoft.com and search for "**nbtstat**". See instructions on how to use **nbtstat** to determine the NetBIOS computer name.

Node federation failed

You federate nodes to create a cluster on which you deploy the IMS Server.

The node federation can fail if:

Deployment Manager is not started
Before you federate the nodes again, ensure that the Deployment Manager is started.

The node has a higher fix pack level than the Deployment Manager
Do not apply a WebSphere Application Server fix pack level that is higher than the Deployment Manager fix pack level.

The nodes or the Deployment Manager cannot be reached.

There must be a two-way connection between the federated node and the Deployment Manager, and among the nodes. Each node must be able to contact the other nodes and the Deployment Manager.

Use the **ping** command to check the connection.

Cannot sign up through AccessAgent

The user cannot sign up with AccessAgent if the user name that is stored in the Active Directory contains a special character. For example, an apostrophe (').

Issue: This issue occurs for the following scenario:

1. IMS Server is installed and configured properly with WebSphere Application Server 7 and fix pack 9.
2. The directory server is configured properly.
3. When the user signs up with AccessAgent, the following error message is displayed:

```
Unable to register due to an unexpected error. Try again.
If the problem persists, contact your Helpdesk.
```

Workaround: Apply WebSphere Application Server fix pack 15 or later.

Unable to configure Kerberos on WebSphere Application Server

Use the workaround provided in this to topic when you are unable to configure Kerberos on WebSphere Application Server with `configureSpnego.bat`.

Symptom: The following error message appears when you are unable to configure Kerberos on WebSphere Application Server with `configureSpnego.bat`:

```
com.ibm.websphere.management.cmdframework.CommandException: org.ietf.jgss.GSSExc
eption, major code: 13, minor code: 0
        major string: Invalid credentials
        minor string: Cannot get credential from JAAS Subject for principal:
        HTTP/ndims.kdcad.jke.com@kdcad.jke.com
```

Issue: A previous Kerberos configuration is present on the WebSphere Application Server.

Workaround: Re-configure the Kerberos environment:

1. Run `configureSpnego.bat` to disable SPNEGO and to delete the SPNEGO configuration on WebSphere Application Server. For example: `configureSpnego.bat wasadmin <password> --disable`.
2. Delete **essokrbuser** on the Active Directory server.
3. Configure Kerberos.

   Note:
   See "Configuring for Kerberos Authentication" in the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

User is unable to log on to AccessAgent

Use the workarounds in this topic when you are unable to log on to AccessAgent after the initial configuration of Kerberos.

The user might not be able to log on to AccessAgent for any of the following reasons:

1. The Active Directory server is unable to locate the Service Principal Name (SPN) that was registered because an incorrect fully qualified domain name is specified during the creation of the keytab file.

Symptom: Unable to log in automatically to https://imsurl/ims/services/Aencentuate.ims.service.ContainerAuthentication?WSDL by using a domain user to verify that the Kerberos configuration is configured correctly.

Note: See "Verifying the Kerberos configuration" in the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

Workaround: Follow the procedure to reconfigure Kerberos with the correct fully qualified IMS Server location on the domain name server (DNS):

1. Run `configureSpnego.bat` to disable SPNEGO and to delete the SPNEGO configuration on WebSphere Application Server. For example: `configureSpnego.bat wasadmin p@ssw0rd --disable`.
2. Delete **essokrbuser** the Active Directory server.
3. Configure Kerberos.

   Note: See "Configuring for Kerberos Authentication" in the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

Note: Ensure that the fully qualified IMS Server location matches the IMS Server location that is set in AccessAgent.

2. The password of the Active Directory user that is created in "Configuring the Kerberos environment to enable Single Sign-On" in the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide* **is changed**

Symptom: The following WebSphere Application Server error logs appear when the Active Directory user is unable to log on to AccessAgent:

```
CWSPN0011E: A non-valid SPNEGO  token has been
encountered while authenticating a HttpServletRequest
```

Workaround: Follow the procedure to re-configure Kerberos with the correct fully qualified domain name on the domain name server (DNS):

1. Run `configureSpnego.bat` to disable SPNEGO and to delete the SPNEGO configuration on WebSphere Application Server. For example: `configureSpnego.bat wasadmin p@ssw0rd --disable`.
2. Delete the user on the Active Directory server.
3. Configure Kerberos.

   Note: See "Configuring for Kerberos Authentication" in the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

Note: Ensure that the fully qualified IMS Server location matches the IMS Server location that is set in AccessAgent.

3. The clock on the Active Directory server, WebSphere Application Server, and the AccessAgent machine is not synchronized

Symptom: The following WebSphere Application Server error logs appears when the Active Directory user that is created is unable to log on to AccessAgent:

```
CWSPN0011E: A non-valid SPNEGO token has been
encountered while authenticating a HttpServletRequest
```

Workaround: Set the clock on the Active Directory server, WebSphere Application Server, and the AccessAgent machine to be less than 5 minutes apart.

Application credentials are not listed in wallet manager in AccessAgent

Use the workaround in this topic when you are unable to see the application credentials in wallet manager.

Issue: The user is successfully logged on to AccessAgent but is unable to see the list of application credentials in wallet manager. The following error message appears on WebSphere Application Server:

```
SECJ0056E: Authentication failed for reason null; nested exception is:
        com.ibm.websphere.security.EntryNotFoundException
```

Cause: ESSO Credential Provider is enabled. AccessAgent authentication with SPNEGO is not supported when ESSO Credential Provider is enabled.

Workaround: Disable ESSO Credential Provider. See "Configuring AccessAgent" in the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

Authentication factor issues

You can encounter issues when you register or use an authentication factor. These issues can prevent you from logging on to an application. Learn more about these issues and their workaround.

Common password issues

The ISAM ESSO password is used to authenticate the identity of the user. The user must be authenticated before the user can access the system. You might encounter issues when you log on with your password or when you change or reset your password.

AccessAgent might not accept your password for any of the following reasons:

You did not enter the correct password.

If you forgot the password, request for an authorization code from the Help desk to reset the password.

You did not enter the password in the correct case.

Check whether the Caps Lock key is active, and that the characters are entered in the correct case.

Your password is not within the required length.

Password length can be configured by the Administrator. The password length can range from 6 to 20 characters, depending on the preference of the organization. Enter a new password that complies with the password length policy.

You did not enter the same password in the Confirm password field.

When you change the password, enter the same password in both the new password field and confirm password field.

Lost authentication devices

Smart cards or RFID cards are devices that are used to log on to, lock, and unlock AccessAgent, and to access the Wallet. If you lost your authentication device, you cannot log on to your Wallet and you cannot single sign-on to your applications.

If you lost your authentication device:

1. Request for a new authentication device, whichever is applicable.
2. Request for an authorization code.

   The authorization code is required to:

   - Associate the Wallet with the new authentication device.
   - Obtain temporary access to the Wallet in case the replacement is not yet available.

Bio-key verification UI is not displayed on the private desktop

When you scan your fingerprint into the fingerprint reader and it is not successful, the BIO-key verification UI is supposed to be displayed.

Issue: The BIO-key verification UI is enabled. However, the verification UI is not displayed when your fingerprint scan failed because of bad quality.

Workaround:

1. Open the Registry Editor.
2. Navigate to `[HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\SOCIAccess\DSPList\{6EA4B6D4-8CDF-4C4E-8B40-CA6A20D0CD6B}\Devices\{5994DB8B-A2C3-4e0a-BC79-F274AE5ECC11}\UISPList\{68F86CB2-630B-4F15-9E2B-5A77B294E9E2}]`
3. Set the **Enabled** registry value to 1.
4. Log off from Windows.
5. Log on to Windows.

Smart card takes time to be recognized and the IMS Server is offline

If the smart card takes a long time to be recognized, the IMS Server might be offline.

Issue: If a user removes a smart card when the security dialog is open, the smart card takes a long time to be recognized and IMS Server is offline.

Workaround: Click **Sign up** and insert the smart card again.

Error when signing up from ESSO Credential Provider with smart card logon to Windows enabled

An intermittent error occurs when a user signs up from ESSO Credential Provider with smart card logon to Windows enabled.

Issue: The issue happens when a user signs up with smart card from ESSO Credential Provider. After sign-up, AccessAgent captures the smart card PIN instead of the Windows password in the Wallet. When the user logs off and logs on to AccessAgent again, AccessAgent prompts to verify the correct Windows password.

Workaround: The user must enter the correct Windows password when AccessAgent prompts for it.

Logon issues

You can encounter issues when you log on to product components, Integrated Solutions Console, and various servers. These issues can prevent you from successfully using the component. Learn more about these issues and their workaround.

Cannot log on to AccessAdmin

Different factors can cause the logon to AccessAdmin to fail.

You cannot log on to AccessAdmin if:

You do not have Administrator rights

You can log on to AccessAdmin only if you have Administrator or Help desk rights.

The DNS name of the web server contains a special character.

Ensure that the DNS name does not contain special characters such as "_".

Form-based logon is not enabled

Ensure that form-based logon is enabled if:

- You are logging on to AccessAdmin from a browser on a remote computer, and
- You are not logged on to AccessAgent on that remote computer.

Form-based logon is not required if:

- You are logging on to AccessAdmin from a browser on a local computer, and
- You are logged on to AccessAgent on that remote computer.

Machine Wallet is not downloaded

If you log on to AccessAdmin from a browser on a remote computer and you are logged on to AccessAgent, ensure that the machine Wallet is downloaded.

Form-based logon to AccessAdmin does not work

If form-based logon is not enabled, you cannot log on to AccessAdmin from a remote computer with AccessAgent.

About this task

Form-based logon is enabled by default in IBM Security Access Manager for Enterprise Single Sign-On version 8.2.1.

If form-based logon is not enabled by default in the previous release, and you upgraded to version 8.2.1, form-based logon is not enabled. The previous setting is carried forward in 8.2.1.

Procedure

1. Open the IMS Configuration Utility.
2. Select **AccessAdmin** > **Login**.
3. Select **true** from the **Allow form-based login to AccessAdmin from remote machine** list.
4. Click **Update**.

   Note: If the form-based logon is not working from the local IMS Server machine, use the URL `https://localhost/admin` from the IMS Server machine instead of the DNS domain name.
5. For WebSphere Application Server Stand-alone deployment, restart the `ISAMESSOIMS` application.

   For WebSphere Application Server Network Deployment, do a full synchronization, and then restart the cluster.

Cannot log on to AccessAssistant - password is not synchronized

If the ISAM ESSO password is not synchronized with the Active Directory password, your logon might fail.

The issue occurs when:

1. You change or reset your password on AccessAgent.
2. You log on to AccessAssistant with the old password.

The following error message is displayed: `ISAM ESSO password is not synchronized with Active Directory password`.

This behavior is caused by a Microsoft limitation. For more information, see http://support.microsoft.com/kb/906305

Cannot log on to the Integrated Solutions Console

Different factors can cause the logon to the Integrated Solutions Console to fail.

You cannot log on to the Integrated Solutions Console for any of the following reasons:

Password is not correct
Ensure that you enter the correct password.

WebSphere Application Server administrator user name is stored in the WebSphere Application Server and in the Active Directory

- The administrative user name that you supply for the WebSphere administrator must not exist on the directory server. Delete the user name from the Active Directory.
- Avoid creating an administrative user with the same user name as the WebSphere administrator. For example, if the WebSphere administrator you provide is `wasadmin`, then the user `wasadmin` must not exist on the corporate enterprise directory.
- Avoid the use of *administrator* as the WebSphere Application Server administrator.
- Choose a user name that is least likely to conflict with your existing enterprise directory users.

An Active Directory is down or cannot be reached

Ensure that all the Active Directories are available and reachable.

Related issue: New user signup fails

If the lookup user password in Active Directory and on the IMS Configuration Utility are different, a new user sign-up task fails.

Issue:

1. You cannot log on to the Integrated Solutions Console.
2. You try to sign up the user, but it fails.

Workarounds:

Option 1

Change the lookup user password to the old password.

Option 2

When you create the lookup user in the Enterprise Directory, do not change the password and configure the password to never expire.

Option 3

1. Stop all WebSphere Application Server Java related processes.
2. Modify the `security.xml` in `<was_home>/profiles`.

   Find the first instance of "enabled" and set the parameter value to `False`.

   Tip: Back up the `security.xml` file before you modify it.
3. Start the WebSphere Application Server.
4. On the Active Directory, either create a lookup user or reset the password of the existing lookup user.
5. On the IMS Configuration Utility, edit the enterprise directory for which the lookup user password is changed.
6. Stop the WebSphere Application Server.
7. Start the WebSphere Application Server.
8. On the Integrated Solutions Console, enable the Administrative Security.
   a. On the Integrated Solutions Console navigation pane, select **Security** > **Global security**.
   b. On the **Global security** page, select **Enable administrative security**.

c. Click **Apply**.
d. Click **Save** in the **Messages** box at the top of the page.

Slow performance, startup, and logon failure

If performance is slow for AccessAgent or the IMS Server, or if AccessAgent logon or startup fails, the issue might be caused by an installed antivirus software.

About this task

An antivirus software can cause:

- Slower AccessAgent performance on the user computer, and Citrix and Terminal Servers.
- AccessAgent startup failure on the user computer, and Citrix and Terminal Servers.
- Intermittent AccessAgent logon failure on the Citrix and Terminal Servers.
- Slower IMS Server performance.

To resolve these problems, include the IBM Security Access Manager for Enterprise Single Sign-On folders in the exclusion list of the antivirus software. Use the following procedure if you use McAfee antivirus.

Procedure

1. Open the property pages of your antivirus scanner.
2. On the **Detection** tab, under **What not to scan**, use the exclusions feature.
3. Click **Exclusions** to open the **Set Exclusions** dialog box.
4. Add files, folders, or drives or edit an item in the list.
5. To add an item, click **Add** to open the **Add Exclusion Item** dialog box.
6. Under **What to exclude**, select the folder by using **By name/location**.
7. Under **When to exclude**, specify all options.
8. Click **OK** to save these settings and return to the **Set Exclusions** dialog box.
9. Click **OK** to save these settings and return to the **Detection** tab.
10. Click **Apply** to save these settings.

    Note: If this solution does not improve the performance of your computer, upgrade the antivirus software to the latest version. If the problem persists after the upgrade, uninstall the antivirus software for troubleshooting or as a temporary solution.

Wallet-related issues

You can encounter issues when you are using, downloading, or logging on to the Wallet. Learn more about these issues and their workaround.

Common Wallet issues

You might encounter issues when you are using the machine Wallet or user Wallet. See this topic for the common Wallet issues and the possible solutions.

User Wallet gets unloaded when the same ESSO account is used in multiple sessions

This issue occurs when there are two users using the same ESSO account on different user sessions on the same computer. For example, *UserA* logs on to *session_A* on *computer_A* using *ESSO_account_A*. Then, *UserB* logs on to *session_B* on *computer_A* using *ESSO_account_A*. When *UserA* logs off from *session_A* on *computer_A*, the Wallet of *UserB* gets unloaded.

Cannot use shared cached Wallet

A shared cached Wallet cannot be used if copy protection is enabled. Do not enable the policy for a shared Wallet deployment.

For more information, see `pid_wallet_cache_security_enabled` in the *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide*.

Temporary access to Wallet is expired

If you are given temporary access to the Wallet, the access is only valid for a predefined time. When the validity of the temporary access expires, you can no longer use the Wallet. Request for a new authorization code so that you can access the Wallet.

Wallet is locked

The Wallet is locked after a predefined number of failed logon attempts. The number of allowed failed logon attempts can be configured by the Administrator.

If your Wallet is locked, contact the Administrator.

Machine Wallet is not downloaded

To get more information about the issue, see "Machine Wallet is not downloaded."

Machine Wallet is not downloaded

AccessAgent creates the machine Wallet by downloading the latest policies and AccessProfiles from the current IMS Server.

You cannot log on to AccessAgent if the policies and AccessProfiles from the IMS Server are not downloaded successfully.

If AccessAgent cannot connect to the IMS Server, AccessAgent uses the policies and AccessProfiles specified in this file: `C:\Program Files\ISAM ESSO\AA\all_sync_data.xml`.

If AccessAgent cannot successfully download the policies and AccessProfiles from the IMS Server after several manual synchronization attempts, see "Downloading the machine Wallet" on page 25.

Verifying the downloaded machine Wallet

Complete this procedure to confirm that the machine Wallet was downloaded properly.

1. Run AccessStudio.
2. Load AccessProfiles from AccessAgent.
3. Click **sso_site_web_ims_admin** under **AccessProfiles**.

The machine Wallet is correct if the **@domain** field on the right panel is set to the **IMS Server name**. The machine Wallet is not downloaded properly if the **@domain** field displays **$hostname**.

Downloading the machine Wallet

Download the machine Wallet again if the machine Wallet is corrupted.

1. Log off from AccessAgent, if you are logged on.
2. Stop the following AccessAgent processes through the Task Manager.
   - `AATray.exe`
   - `Sync.exe`
3. Stop the `DataProvider` service by using `net stop dataprovider`.
4. Stop the `SOCIAccess` service by using `net stop sociaccess`. The `SOCIAccess` service automatically replaces any deleted machine Wallet file.
5. Delete the machine Wallet (machine.wlt).
6. Restart the computer.
7. Open AccessStudio.
8. Select **Tools** > **Backup System Data from IMS to File**.
9. Click **Backup**.
10. Save `all_sync_data.xml` in the `Config` folder of the AccessAgent installer package.

Operational issues

You can encounter issues when using the product components such as the IMS Server, AccessAgent, AccessStudio, AccessAdmin, or AccessAssistant. Learn more about these issues and their workaround.

Issues that you might encounter when using the Transparent Screen Lock

You can encounter issues when using the Transparent Screen Lock feature in Windows 7.

See the following possible issues and workaround:

A gray screen when the computer is locked.

Issue: Windows 7 AERO might not be enabled.

Workaround: Enable Windows 7 AERO.

The ISAM ESSO hot key does not work.

Issue: The ISAM ESSO hot key sequence that is displayed in the Transparent Screen Lock message (`pid_lock_transparent_text`) might not be in sync with the value set for the ISAM ESSO hot key sequence (pid_enc_hot_key_sequence).

Workaround: Ensure that the hot key sequence specified in the Transparent Screen Lock MESSAGE (`pid_lock_transparent_text`) matches the value that is set for the ISAM ESSO hot key sequence (`pid_enc_hot_key_sequence`).

Cannot connect to AccessAdmin

Different factors can affect the connection to AccessAdmin.

You cannot connect to AccessAdmin if:

The IMS Server is not running.
Ensure that the ISAMESSOIMS application is started in the Integrated Solutions Console.

There is no network connection.
Ensure that you have a network connection before you start AccessAdmin.

Ports are not available
Ensure that the required ports are available.

AccessAdmin - Service is not available

When you open AccessAdmin, the Service is not available, and an error is displayed. Check the logs for the details.

This error occurs on a WebSphere Application Server Network Deployment.

Issue: In the SystemOut.log file, you see the java.io serializable error. You did not override the session management for the ISAMESSOIMS EAR file.

Workaround: Override session management. See "Overriding session management for the ISAMESSOIMS" in the *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*.

Cannot open the httpd.conf file

When you are enabling the SSL directive, the httpd.conf file cannot be opened. This issue occurs when the IBM HTTP Server is down or the nodes are not started.

Issue: An error message is displayed when you open the httpd.conf file and the text area is empty.

Workaround:

1. If the web server is created on a managed node, check whether the node agent for this node is available or started.
2. If the web server is created on an unmanaged node, check the credentials.
   a. In the administrator console, click **Servers** > **Server Types** > **Web servers**.
   b. Click the <*Web_server_name*>. For example: webserver1.
   c. In the **Additional Properties** section on the **Configuration** tab, click **Remote Web Server Management**.
   d. Enter the IBM HTTP Server administration server authentication user ID and password. For example: ihsadmin.
   e. Clear the **Use SSL** check box.
   f. Click **OK**.
   g. In the **Messages** box, click **Save**.
3. Start the IBM HTTP Server.

Cannot authenticate when a repository is down

If one or more of the configured repositories are down, you cannot authenticate or stop the WebSphere Application Server.

Issue: The following exception is displayed:

```
CWWIM4520E The 'javax.naming.CommunicationException:
Extdomain1.altext.ibm.com:389
[Root exception is java.net.ConnectException: Connection refused: connect]'
```

```
naming exception occurred during processing.
at  com.ibm.ws.wim.adapter.ldap.LdapConnection.reCreateDirContext
(LdapConnection.java:613)
at com.ibm.ws.wim.adapter.ldap.LdapConnection.search(LdapConnection.java:2419)
```

Workaround:

For more information about this problem and its possible solutions, see the following references:

- Unable to authenticate when a repository is down
- IdMgrRealmConfig command group for the AdminTask object

IMS Server cannot issue a certificate for an application

The IMS Server cannot issue SCR or CAPI certificates for an authentication service with ID that contains the underscore (_) character.

Subject fields of the IMS Server certificates cannot contain the underscore (_) character because it can cause problems at deployments that use certificate authentication for applications.

Remove all underscore (_) characters from the authentication services IDs that use certificate authentication.

Cannot single sign-on in a command prompt

When you install AccessAgent, the console application support is not enabled by default. As such, you cannot single sign-on to a command prompt.

To enable console application support, use `SetupHlp.ini` or run `InstallConsoleSupport.vbs`.

Enable console application support in `SetupHlp.ini`

Enable console application support in `SetupHlp.ini` during the AccessAgent installation.

1. In the AccessAgent installer, open the `Config` folder.
2. Double-click `SetupHlp.ini` to open the configuration settings file.
3. Under the Setup time only options category, set the value of `ConsoleAppSupportEnabled` to `1`.

Run `InstallConsoleSupport.vbs`

`InstallConsoleSupport.vbs` is automatically installed in the AccessAgent installation directory during the AccessAgent installation.

If you have AccessAgent installed and you want to enable console application support, complete the following procedure.

1. Run the `InstallConsoleSupport.vbs`.

   Note: Ensure that you have Administrator privileges before you run the script.
2. Restart the computer.

AccessProfile is not displayed in the properties pane

When you open an AccessProfile in AccessStudio, the content is supposed to be displayed on the properties pane.

This problem is intermittent.

Issue: Nothing is displayed on the properties pane when you open an AccessProfile in AccessStudio and you click the AccessProfile.

Workaround: Resize the **AccessStudio** window.

AccessStudio might stop working when you use the Convert to option

AccessStudio might stop working when you open an AccessProfile for a web application and use the **Convert to** option to convert a trigger. This problem occurs when the web application is running either on Microsoft Internet Explorer or on Mozilla Firefox.

Issue: In AccessStudio, when you right-click a trigger and select **Convert to** any other trigger, you are prompted that an unhandled exception occurred in your application.

Workaround: Instead of using the **Convert to** option, use this procedure.

1. Add a trigger.
2. Copy the trigger details from the existing trigger into the new trigger.
3. Delete the existing trigger.

OutOfMemory error when you open an AccessProfile

AccessStudio 8.2 cannot handle large sizes of AccessProfiles.

Issue: If you open an AccessProfile with a size of 9 MB or larger, a System Out of Memory Exception occurs.

Workaround: Reduce the AccessProfile file size.

Key pressed on a window trigger does not fire

The **Key pressed on a window** trigger does not fire when you use the **Enter** key to trigger the state transition.

Issue: If you use the AccessProfile trigger **Key pressed on a window** and you set its property **Fire trigger on key** to **Any key**, when you run the AccessProfile and use the **Enter** key to trigger the state transition, it does not fire.

Workaround: Create another **Key pressed on a window** trigger and set it's property **Fire trigger on key** to **Enter**. This trigger would be in parallel to the other **Key pressed on a window** trigger that fires for any other key.

Successful logon page might not be captured correctly when creating a profile in Mozilla Firefox

When you create an AccessProfile for a website in AccessStudio with Mozilla Firefox, the successful logon page might not be captured correctly.

Issue: In AccessStudio, when you create an AccessProfile for a website with Mozilla Firefox, capturing a successful logon page in the **Identify Successful Logon** page might fail to capture the page accurately.

Workaround: Use Microsoft Internet Explorer to create an AccessProfile for a web page.

Database slowdown because of buildup of unused cached Wallets

Unused cached Wallets in the IMS Server might slow down your database.

Issue: Cached Wallets of users that are not cleared in the IMS Server creates a buildup. This scenario causes the database to experience slow down and delay in operations.

Single sign-on does not work on Microsoft Internet Explorer

The user cannot single sign-on to a web application using Microsoft Internet Explorer.

Workaround:

1. Open Microsoft Internet Explorer.
2. Select **Tools** > **Internet Options**.
3. Click **Advanced**.
4. Under **Browsing**, select the **Enable third-party browser extensions** check box.
5. Restart Microsoft Internet Explorer.

Fields that are not functional in AccessAdmin

The `Is it a password field` and `Can it be empty` fields are not functional in AccessAdmin.

Issue: In AccessAdmin, navigate to **System Policies** > **Configurable Text Polices** > **Sign up Text Polices**. The user interface contains two fields: `Is it a password field` and `Can it be empty`. The changes made to these two fields are not effective.

Unexpected form validation when changing the SSL value in the IMS Configuration Wizard

The form fields in the **Repository information** page in the IMS Configuration Wizard are expected to be validated only when the **Save** button is clicked. However, the page is also validated when the values in the SSL dropdown are changed.

A message request that contains the character (`and`) fails

In Web API credential management, a message request that contains the character (`and`) fails.

Issue: An error occurs when you use the character (`and`) in any of the following Web API credential management tasks:

- Getting user credentials
- Deleting user credentials
- Setting user credentials

The (and) character is not a valid XML character. As such, the `rst.xml` file must not contain this character.

Non-ASCII characters cannot be used for application user name in IMS Server

Non-ASCII characters cannot be used for application user name in IMS Server when you use WebSphere Application Server, Version 8.5 and Microsoft SQL Server. Use the workaround to resolve this limitation.

Workaround: Set the **sendStringParametersAsUnicode** value to `true` by doing the following tasks:

1. On the WebSphere Application Server host, where IMS Server is installed, log on to the administrative console. For example: `https://localhost:9043/ibm/console/` .
2. In the navigation pane, select **Resources** > **JDBC** > **Data sources**.
3. Select the name of your data source.
4. In **Additional Properties**, select **Custom properties**.
5. In the custom properties window, select **sendStringParametersAsUnicode**.
6. In **General Properties**, set value to `true`.
7. Click **Apply**.
8. In the messages box, click **Save**.
9. Restart WebSphere Application Server.

Browser

You can encounter issues while using your browser. Learn more about these issues and their workaround.

Microsoft Internet Explorer stops working

Microsoft Internet Explorer stops working when you browse to any random website. The problem occurs on Microsoft Internet Explorer version 7.0 and later and on any random website.

Workaround: Create an AccessProfile for the website and specify whether to enable or not enable the Browser Helper Object.

Note: Make sure that you have Administrator privileges before you do the following steps to resolve this issue.

1. Open AccessStudio.
2. Create a basic AccessProfile for the website that displays this error.
3. Enable **state editing**.
4. Create a state. For example: `newstate1`.
5. Insert a trigger Fire immediately from the start state to `newstate1`.
6. Add an action `Run VBScript or JScript`.
7. Paste the following code in the script:
   ```
   dim objBHO     objBHO = runtime.getBrowserObject()     objBHO.enableBHO(false)
   ```
8. Create another state. For example: `newstate2`.
9. Insert a trigger Fire after specified time from `newstate1` to `newstate2`.
10. Set the trigger timeout to the time it takes to load the web page.

11. Add an action `Run VBScript or JScript`.
12. Paste the following code in the script:

```
dim objBHO     objBHO = runtime.getBrowserObject()     objBHO.enableBHO(true)
```

13. Upload the new AccessProfile to the IMS Server.

Mozilla Firefox interferes with the AccessAgent single sign-on feature

When you use Mozilla Firefox to log on to an application, Mozilla Firefox and AccessAgent both display a form to save the password.

By default, the **Remember passwords for sites** option is enabled in Mozilla Firefox. This feature captures your password so that every time you log on to a website, your password is automatically entered. When AccessAgent captures your logon credentials, Mozilla Firefox also displays another form to save the password.

During the AccessAgent installation, the installer automatically disables the **Remember passwords for sites** option in Mozilla Firefox. However, if you are not yet logged on to the Windows desktop and you did not use the Mozilla Firefox before, manually disable this option.

To disable this feature in Mozilla Firefox:

1. Open the Mozilla Firefox.
2. Navigate to **Tools** > **Options** > **Security** > **Passwords**.
3. Clear the **Remember passwords for sites** check box.

Alternately, go to `C:\Program Files\IBM\ISAM ESSO\AA` folder on your computer and double-click `InstallFirefoxXpCom.vbs`.

Single sign-on does not work in Mozilla Firefox

Mozilla Firefox must be installed before AccessAgent. Otherwise, single sign-on does not work on Mozilla Firefox.

Issue: Single sign-on does not work in Mozilla Firefox.

Workaround: If AccessAgent is installed before Mozilla Firefox, navigate to `C:\Program Files\IBM\ISAM ESSO\AA` and run the `InstallFirefoxXPCOM.vbs` batch script. This script enables Mozilla Firefox to support single sign-on.

Cannot capture logon credentials in Mozilla Firefox pop-up window

AccessAgent cannot capture the logon credentials in the Mozilla Firefox pop-up window.

Issue: In some Web page authentication, you are prompted to enter your user name and password in a pop-up window. If you are using Mozilla Firefox, AccessAgent cannot capture your input and detects the action trigger in the pop-up window.

Workaround: Use this procedure to capture your logon credentials.

1. Use the **Window is activated** trigger to detect the basic authentication window pop-up event.

2. Under this trigger, use the **Advanced Actions** > **Show a dialog to capture logon credentials**.

Cannot open web applications

You cannot open web applications in Microsoft Internet Explorer if your browser is set to work offline.

Issue: If you open a Microsoft Internet Explorer window and a network connection-related message is displayed, Microsoft Internet Explorer might be set to offline mode.

Workaround: Verify whether the Microsoft Internet Explorer is set to work offline by selecting the **File** menu from the Microsoft Internet Explorer. If the **Work Offline** option is selected, you cannot connect to the Internet. Clear the **Work Offline** option to resolve this issue.

Back button does not work

The **Back** button does not work for AccessAdmin and AccessAssistant.

You cannot use the **Back** button in a Web browser when you are using AccessAdmin and AccessAssistant.

AccessAssistant is designed this way because of security reasons, and AccessAdmin is designed this way because of certain implementation constraints.

Verifications

This section covers some tips on how to verify versions, modes, and the type of deployment used.

See the following topics:

- "Determining the type of IMS Server deployment"
- "Determining the Server AccessAgent mode" on page 33

Determining the type of IMS Server deployment

To know how the IMS Server is deployed, whether using the virtual appliance or the standard process, check the profile name and the operating system or check the Integrated Solutions Console.

Using the profile name and operating system.

Check the `System.Out` log file. This log file indicates the profile name and the operating system.

Within the environment variables that are printed at the beginning for each log file, locate:

```
user.install.root = /opt/IBM/WebSphere/Profiles/DefaultAppSrv01
```

For a virtual appliance deployment, the profile name is always **DefaultAppSrv01** and the operating system is SUSE Linux Enterprise Server.

Using the Integrated Solutions Console

For a virtual appliance deployment, click the Welcome link, and it shows an entry for both the WebSphere Application Server and WebSphere HyperVisor. Otherwise, it just shows WebSphere Application Server.

Verifying the IMS Server version

From the AccessAdmin navigation panel, select **System** > **Status** to view the system status, such as the server availability and version number.

Determining the Server AccessAgent mode

If you want to know whether the Server AccessAgent is running in standard or lightweight mode, check the logs.

To find out the lightweight mode setting on the server, use log level 3. Verify the log from TSVCServer.exe, with the following message:

```
Lightweight mode AccessAgent disabled or
Client AccessAgent has no V3 message support.
```

To determine whether the session is running on lightweight mode, verify the log from TSVCServer.exe, with the following message:

"Launch AATray success."
You are running in standard mode.

"Not launching AATray."
You are running in lightweight mode.

Chapter 5. Fixes

You can obtain fixes from the product support Web site and sign up for notifications of product support information, including fixes.

Obtaining fixes

A product fix might be available to resolve your problem. Check the product support site to determine what fixes are available for IBM Security Access Manager for Enterprise Single Sign-On.

Before you begin

You can determine what fixes are available for IBM Security Access Manager for Enterprise Single Sign-On by checking the product support Web site:

Procedure

1. Go to the IBM Software Support Web site for IBM Security Access Manager for Enterprise Single Sign-On: http://www.ibm.com/software/sysmgmt/products/support/index.html
2. Select **IBM Security Access Manager for Enterprise Single Sign-On** from the **Support for specific Tivoli products** drop-down list. A list of most recent fixes is listed in the Download section of the page.
3. Click the name of a fix to read the description. You can also download the fix.

Receiving fix notifications

Enable email notifications and subscriptions to receive notifications about any new fix packs and other news about IBM products.

Procedure

To receive email notifications about fixes and other news about IBM products, follow these steps:

1. Go to the IBM Software Support Web site for IBM Security Access Manager for Enterprise Single Sign-On: http://www.ibm.com/software/sysmgmt/products/support/index.html
2. Select **IBM Security Access Manager for Enterprise Single Sign-On** from the **Support for specific Tivoli products** drop-down list.
3. Click **My Support** in the upper-right corner of the page. A sign-in page is displayed.
4. If you have already registered, go to the next step. If you have not registered, click **Register now** to establish your user ID and password.
5. Sign in to **My support**.
6. Click the **Edit profile** tab.
7. Select **Software** > **Security** > **Access** in the fields that are displayed.
8. Select **IBM Security Access Manager for Enterprise Single Sign-On** from the list of products displayed.
9. Click **Add products**.

10. To enable email notification, click **Subscribe to email** at the top of the page.
11. From the list, click **Software**.
12. Select the check boxes that best describe the email notifications that you would like to receive.
13. Click **Update**.
14. Sign out of the session by clicking **Sign out** or click **Go to my personalized page** to see your personalized support page.

Chapter 6. Searching knowledge bases

IBM Support for IBM Security Access Manager for Enterprise Single Sign-On maintains a knowledge base of technical documentation, problems, and workarounds.

About this task

IBM Support Assistant includes a hierarchical search tool to help you focus your search for information related to a specific product, platform, or issue. See "IBM Support Assistant" on page 51 for more information.

The following procedure describes how to perform a manual search for information.

Procedure

1. Go to the IBM Software Support Web site for IBM Security Access Manager for Enterprise Single Sign-On: http://www.ibm.com/software/sysmgmt/products/support/index.html
2. Select **IBM Security Access Manager for Enterprise Single Sign-On** from the **Support for specific Tivoli products** drop-down list.
3. Under **Solve a problem**, click any of the following options:
   - **Technotes**, which lists information about the product by article title.
   - **APARs**, which lists known problems according to Authorized Program Analysis Report numbers.
4. Optionally, search for specific terms, error codes, or APARs by using the **Search** field on the product support page. You can also browse through the Technotes or APARs pages.

Chapter 7. Analyzing data

After you collect data from multiple sources, you must determine how that data can help you to resolve your problem.

To analyze the data, take the following actions:

- Determine which data sources are most likely to contain information about the problem, and start your analysis from those sources. For example, if the problem is related to installation, start your analysis with the installation log files, if any. This action helps narrow down the problem, instead of starting with the general product or operating system log files.
- Understand how the various pieces of data relate to each other. For example, if the data spans to more than one system, keep your data organized to know which pieces of data come from which sources.
- Use timestamps to confirm that each piece of diagnostic data is relevant to the timing of the problem.

  Note: Data from different sources can have different timestamp formats. Understand the sequence of the different elements in each timestamp format so you can tell when the different events occur.

The specific method of analysis is unique to each data source. One tip that is applicable to most traces and log files is to start by identifying the point in the data where the problem occurs. After you identify that point, go through the data to trace the root cause of the problem.

To investigate a problem for which you have comparative data for a working and non-working environment, start by comparing the operating system and product configuration details for each environment.

Chapter 8. Collecting data

There are other ways to solve a problem aside from troubleshooting the symptoms. Another way of solving a problem is collecting more diagnostic data.

Before you begin to collect data for a problem report, install and run the IBM Support Assistant. This troubleshooting tool includes a console where you can submit an online problem management record (PMR). As part of the process, information specific to your system, environment, and product is gathered into a file that is used by IBM Software Support. For more information about IBM Support Assistant, see "IBM Support Assistant" on page 51.

Collecting data early, even before you open a problem management record (PMR), can help you to answer the following questions:

1. Do the symptoms match any known problems?
2. If so, has a fix or workaround been published?
3. Is the problem a non-defect-oriented problem that can be identified and resolved without a code fix?
4. Where does the problem originate?

The diagnostic data that you need to collect and the sources from which you collect that data depend on the type of problem that you are investigating.

For help identifying the component from which the problem originates, follow the questions in the troubleshooting checklist for IBM Security Access Manager for Enterprise Single Sign-On.

Collecting general data

When you submit a problem to IBM Software Support, you typically must provide a base set of information about the affected system or systems, such as:

- Version of IBM Security Access Manager for Enterprise Single Sign-On and patch levels on affected systems.
- Operating system name and version.
- General details about the structure of your environment, such as number of servers and software installed, domains and federations configured.

Collecting problem-specific data

For specific symptoms, or for problems in a specific part of the product, you must collect more data, such as message and trace information. See "Message and trace logs." After you collect the appropriate diagnostic data, you can attempt to analyze the data yourself or you can provide it to IBM Software Support.

Message and trace logs

IBM Security Access Manager for Enterprise Single Sign-On message and trace logs are managed and stored by WebSphere Application Server.

See the troubleshooting topics in the WebSphere Application Server information center for detailed information about logs and logging.

Message logs

Message logs are text files in which the operations of the system are recorded.

The following types of messages are recorded by default:

Informational messages
Indicate conditions that are worthy of noting but that do not require you to take any precautions or perform an action.

Warning messages
Indicate that a condition has been detected that you must be aware of, but does not necessarily require any action.

Error messages
Indicate that a condition has occurred that requires an action.

Message log files

All IBM Security Access Manager for Enterprise Single Sign-On messages are logged in the following default WebSphere Application Server message logs.

Table 2. Message logs

Log	Default file name	Content
JVM Logs	SystemOut.log	Messages in text format for the application server instance.
IBM Service Log	activity.log	Messages in binary Common Base Event format for the application server installation. **Note:** Tools for viewing this format are provided with WebSphere Application Server. See the WebSphere Application Server documentation at http://www.ibm.com/software/webservers/appserv/was/library/ for more information.

You can use the WebSphere Application Server administrative consoleto configure the following log settings:

- location
- name
- maximum size of the log files
- levels of severity that you want to log, such as Warning and Severe

See "Configuring log settings" on page 44 for more information.

Message log locations

By default, the message logs are located in the following directories.

Table 3. Application server default message log locations

Log	Path
JVM Logs	**Windows:** `C:\Program Files\IBM\WebSphere\AppServer\profiles\` *`profile_name`*`\ logs\`*`server_name`*`\SystemOut.log`
IBM Service Log	**Windows:** `C:\Program Files\IBM\WebSphere\AppServer\profiles\` *`profile_name`*`\ logs\`*`server_name`*`\activity.log`
HTTP Server Log	`C:\Program Files\IBM\HTTPServer\logs`
ISAM ESSO Log	`C:\Program Files\IBM\ISAM ESSO\Logs`

Console message logs are saved in the message log directories of the WebSphere Application Server node where the administration console is installed.

Trace logs

Trace logging, or tracing, provides IBM Software Support personnel with additional information relating to the condition of the system at the time a problem occurred.

Trace logs capture transient information about the current operating environment when a component or application fails to operate as intended. Trace logs are different from message logs because message logs records only the occurrence of noteworthy events. Trace logs are available only in English.

Trace logging is not enabled by default. In some circumstances, trace logging might cause large amounts of data to be collected in a short amount of time which results in significant performance degradation. Therefore, enable the trace logging only at the direction of IBM Software Support personnel. See "Configuring log settings" on page 44 for more information.

Trace log entries can provide the following level of detail:

Fine Minimal detail.

Finer Moderate detail.

Finest Maximum (verbose) detail.

Trace log file

If tracing is enabled for an application server, IBM Security Access Manager for Enterprise Single Sign-On trace information is logged in the following default WebSphere Application Server trace log.

Table 4. Trace log

Default log name	Default file name	Content
Diagnostic Trace	trace.log	Trace information in text format for the application server instance.

Using the WebSphere Application Server administrative console, you can configure some settings of the logs, such as the location, name, maximum size of the log files and the level of detail that you want to log (such as Fine, Finer, Finest). For more information, refer to "Configuring log settings."

Trace log locations

By default, the trace log is located in the following directories.

Table 5. Application server default trace log locations

Log	Path

Diagnostic Trace	**UNIX and Linux:**
	`/opt/IBM/WebSphere/AppServer/profiles/`*profile_name*`/logs/`*server_name*`/trace.log`
	Windows:
	`C:\Program Files\IBM\WebSphere\AppServer\profiles\`*profile_name*`\logs\`*server_name*`\trace.log`

Console trace logs are saved in the trace log directories of the WebSphere Application Server node where the administration console is installed.

Configuring log settings

You can use the administration console to configure the settings for message and trace logs. Message logging is enabled by default. Trace logging must be enabled only at the direction of IBM Support personnel.

Configuring message logging

Message logging to the JVM log and the IBM Service log is enabled by default. Both logs are configured to log messages for all IBM Security Access Manager for Enterprise Single Sign-On components of all severity levels. You can modify the names, location, file size, and severity level to be logged.

Configuring the JVM log

You can modify the file name, location, file format, file size, logging start and stop times, number of logs to keep, and severity level to be logged in the JVM Log.

About this task

The JVM log, also called as SystemOut.log, is a standard WebSphere Application Server log used for messages. For detailed information, see the JVM log topics in the WebSphere Application Server information center.

Procedure

1. Start the WebSphere Application Server administrative console and log on, if necessary.
2. Click **Troubleshooting** > **Logs and Trace** to open the Logging and Tracing page.
3. Click the name of the server that you want to configure. For example, server1.
4. Click **JVM Logs** to view the configuration options.
5. Select the **Configuration** tab.

6. Scroll through the panel to show the attributes to configure.
7. Change the appropriate configuration attributes.
8. Click **Apply**.
9. Save your configuration changes.

Configuring the IBM Service log

The IBM Service log is enabled by default. You can change this setting or modify the names, location, file size, and severity level to be logged in the log.

About this task

The service log, also called as the activity.log, is a standard WebSphere Application Server log used for messages. For detailed information about the log, refer to the service log topics in the WebSphere Application Server information center.

Procedure

1. Start the WebSphere Application Server administrative console and log on, if necessary.
2. Click **Troubleshooting** > **Logs and Trace** to open the Logging and Tracing page.
3. Double-click the name of the server that you want to configure. For example, server1.
4. Click **IBM Service Logs** to view the configuration options.
5. Select or clear the **Enable service log** box to enable or disable logging. The service log is enabled by default.
6. Set the name for the service log in the **File Name** field. The default name is activity.log. If the name is changed, the runtime requires write access to the new file, and the file must use the .log extension.
7. Specify the number of megabytes to which the file can grow in the **Maximum File Size** field. When the file reaches this size, it wraps, replacing the oldest data with the newest data.
8. Click **Apply** to save the configuration changes.
9. Restart the server for the configuration changes to take effect.

Enabling trace logging

You can enable trace logging at server startup or on a running server. To maintain system performance, enable trace logging only at the direction of IBM Support personnel.

Enabling trace at server startup

Trace logging can be enabled at server startup.

About this task

The trace log is a standard WebSphere Application Server log used for trace information. For detailed information about the log, see the WebSphere Application Server information center.

Procedure

1. Start the WebSphere Application Server administrative console and log on, if necessary.

2. Click **Troubleshooting** > **Logs and Trace** to open the Logging and Tracing page.
3. Click the name of the server that you want to configure, for example, server1.
4. Click **Diagnostic Trace** to view the configuration options.
5. Click the **Configuration** tab.
6. Select or clear the **Enable log** box to enable or disable logging. The trace log is disabled by default.
7. Complete the configuration as instructed by IBM Support personnel. For additional information about the configuration settings, see the troubleshooting and trace log topics in the WebSphere Application Server information center.
8. Click **Apply** to save your configuration changes.
9. To enter a trace string to set the trace specification to the required state:
   a. Click **Troubleshooting** > **Logs and Trace** to open the Logging and Tracing page.
   b. Click the server you want to configure, for example, server1.
   c. Click **Change Log Detail Levels**.
   d. If the **All Components** option has been enabled, you turn it off and then enable specific components.
10. Click a component or group name.
11. Enter a trace string in the trace string box. For more information about trace strings, see the WebSphere Application Server information center.
12. Click **OK**.
13. Click **Save** to save your changes. You must restart WebSphere Application Server for the change to take effect.

Enabling trace on a running server

Trace logging can be enabled on a running server.

About this task

The trace log is a standard WebSphere Application Server log used for trace information. For detailed information about the log, see the WebSphere Application Server information center.

Procedure

1. Start the WebSphere Application Server administrative console and log on, if necessary.
2. Click **Troubleshooting** > **Logs and Trace** to open the Logging and Tracing page.
3. Click the name of the server that you want to configure, for example, server1.
4. Click **Diagnostic Trace**.
5. Click the **Runtime** tab.
6. Select the **Save runtime changes to configuration as well** box if you want to write your changes back to the server configuration.
7. Change the existing trace state by changing the trace specification to the required state.
8. Configure the trace output if you want to change the existing one.
9. Click **Apply**.

Viewing logs

The format of the logs determines how they can be viewed.

JVM logs

You can view the JVM logs with any of the following options:

- Use the WebSphere Application Server administrative console, which also supports viewing from a remote machine
- Use a text editor on the machine where the log files are stored.

See the **Viewing JVM logs** section in the WebSphere Application Server information center for more information.

Using IBM Support Assistant

The IBM Support Assistant tool helps troubleshoot IBM Security Access Manager for Enterprise Single Sign-On. Use the tool to automatically collect problem data.

You must install the IBM Security Access Manager for Enterprise Single Sign-On plug-in for IBM Support Assistant as part of the IBM Security Access Manager for Enterprise Single Sign-On installation. If you did not specify the IBM Support Assistant component when installing the product, install it now.

To use the tool, see the following topics:

- "Using the IBM Support Assistant in graphical mode"
- "Using the IBM Support Assistant in console mode" on page 48

Using the IBM Support Assistant in graphical mode

You can use a graphical user interface to collect data with IBM Support Assistant.

About this task

To access the graphical user interface, run a script from the command line.

Procedure

1. Ensure that your Java environment is configured correctly:
   a. Verify that your Java runtime environment is at level 1.4.2 or higher.
   b. Determine if the location of the Java runtime environment is included in your PATH environment setting. If the location is not included in your path, set the variable `JAVA_HOME` to point to the Java runtime environment.

Table 6. Specifying JAVA_HOME for your environment

Operating system	Sample command
Windows	For example, if you have a Java Development Kit installed at `c:\jre1.4.2`, use the command: `SET JAVA_HOME=c:\jre1.4.2`

2. Start the IBM Support Assistant tool:

   Open a command window, and change directory to the ISAlite installation directory. Enter the command `runISALite.bat`. The IBM Support Assistant now starts a graphical user interface.
3. In the Problem Type window, select a problem type.

Expand the folders to display all problem types. Find your problem type and select it.

4. Supply a filename for the data collection .zip file.

   You can use any filename. The tool automatically appends the .zip file extension. For example, if you enter the filename `Install_problem`, the file is named `Install_problem.zip`.
5. Click **Collect Data**.

   The collection script runs and prompts you for additional information. The information can include configuration information or, the sequence of events leading to the problem. The script might also prompt you for preferences for data collection.

   When the scripts finishes collecting the setup information, it collects the necessary data. The tool creates a .zip file that you can send to IBM Support.
6. When prompted, enter a filename in the **Output Filename/Path** box.

   The tool appends the server hostname and current timestamp to the filename that you entered.
7. Send the .zip file to IBM Support

   You can choose FTP or HTTPS for file transfer.

   Note: FTP is not encrypted and HTTPS is encrypted.

Using the IBM Support Assistant in console mode

You can collect data with IBM Support Assistant in console mode.

About this task

Console mode provides command-line control of the IBM Support Assistant Lite collection scripts. The tool lets you record your responses from a console-mode session in a response file. You can then use the response file to drive subsequent executions of the same collection script.

Procedure

1. Ensure that your Java environment is configured correctly:
   a. Verify that your Java runtime environment is at level 1.4.2 or higher.
   b. Determine if the location of the Java runtime environment is included in your PATH environment setting. If the location is not included in your path, set the variable `JAVA_HOME` to point to the Java runtime environment.

Table 7. Specifying JAVA_HOME for your environment

Operating system	**Sample command**
Windows	For example, if you have a Java Development Kit installed at `c:\jre1.4.2`, use the command: `SET JAVA_HOME=c:\jre1.4.2`

2. Start the IBM Support Assistant tool:

   Open a command window, and change directory to the ISAlite installation directory. The IBM Support Assistant now starts in console mode.
3. Create a response file by using the following command `runISALiteConsole.bat -record` *`response.txt`*.

   You can specify your own filename for *response.txt*.

When running in this mode, you supply data input during an interactive session. The tool records your responses into the file that you specify.

4. Run the tool by using the response file that you have created `runISALiteConsole.bat` *`response.txt`*.

   Notes®:

   - The response file is a plain text file. You can edit it to modify values as needed. For example, you can use the file on another computer after adjusting the response file values to reflect settings for the local computer.
   - Remember that sensitive information, such as user names and passwords, might be stored in the response file. Manage the file carefully, to prevent unauthorized access to important information.
   - Some data collection sessions require interaction with the user, and thus are not suitable for the silent collection option. For example, IBM Support might ask you to reproduce a problem during data collection, in order to collect log and trace files. In this case, silent collection cannot record and reproduce all steps.

Chapter 9. Contacting support

IBM Software Support provides assistance with product defects.

You can contact IBM Software Support in the following ways:

- **IBM Support Assistant:** You can search for information about a problem and collect the logged information required to troubleshoot a problem by using the IBM Support Assistant. You can use it to open a problem management report (PMR) online. It is also helpful to use the IBM Support Assistant to report a problem to IBM Software Support. You need your user account ID and password to submit a PMR through the IBM Support Assistant. The IBM Support Assistant client is included on your product CD and updates can be downloaded from the following website: http://www.ibm.com/software/support/isa/
- **Online:** Go to the **Submit** and **track problems** tab on the IBM Software Support site at http://www.ibm.com/software/support/probsub.html. Type your information into the appropriate problem-submission tool.
- **By phone:** For the phone number to call in your country, go to the Contacts page of the *IBM Software Support Handbook* at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/contacts.html, and click the name of your geographic region.

If the problem that you submit is for a software defect, missing content, or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the Software Support website daily, so that other users who experience the same problem can benefit from the same resolution.

Before you submit a problem to IBM Software support, answer these questions:

1. Do you have an active IBM software maintenance contract?
2. Do you understand the business effect of the problem?
3. Can you describe the problem?

IBM Support Assistant

IBM Support Assistant simplifies the process of researching and reporting on software problems.

IBM Support Assistant provides quick access to support-related information along with serviceability tools for problem determination. IBM Support Assistant consists of three tools:

Search
Use multiple filters to focus your search to access troubleshooting repository information quickly. The concurrent search tool spans the bulk of IBM documentation and returns results that are categorized by source for easy review.

Product information links
These self help links include:

- Product support pages

- Product home pages
- Product troubleshooting guides
- Product education road maps and the IBM Education Assistant
- Product updates
- Product news groups and forums

Service feature

The service feature is an automated system collector and symptom-based collector. The system collector gathers general information from your operating system, registry, and other sources. The symptom-based collector gathers specific product information relating to a particular problem that you are having. Use the service feature to automatically set tracing to help IBM support in the data gathering process.

The service feature also enables you to submit a problem online to IBM Software Support. Enter your entitlement information once, and save it for future sessions. You can then create a problem report for IBM and attach the gathered data in the collector file.

IBM Support Assistant provides a complete online user guide to assist you in the setup and use of the tool. The following steps describe the basic procedure for setting up your system to use IBM Support Assistant:

1. Install the IBM Support Assistant tool from your product CD, or from the following Web site:

   http://www.ibm.com/software/support/isa/
2. In an IBM software repository, locate the IBM Support Assistant plug-in for the version of WebSphere Application Server that you are running. The IBM Security Access Manager for Enterprise Single Sign-On plug-in uses the WebSphere Application Server plug-in as the base code.

   Note: Be patient downloading the WebSphere Application Server plug-in; it can take a long time depending on network traffic and the availability of system resources.
3. Install the WebSphere Application Server plug-in into the \plugin subdirectory of the IBM Support Assistant installation directory.
4. Locate the IBM Support Assistant plug-in for IBM Security Access Manager for Enterprise Single Sign-On on the product CD or in an IBM software repository.
5. Install the IBM Support Assistant plug-in into the \plugin subdirectory of the IBM Support Assistant installation directory.
6. Click your IBM Support Assistant desktop icon to start. Select the **User Guide** tab for information about performing the various available tasks.

IBM software maintenance contracts

Ensure that your company has an active maintenance contract before you submit a problem to IBM Software Support. Make sure that you are also authorized to submit problems to IBM.

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States. From other countries, go to the Contacts page of the *IBM Software Support Handbook* at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/contacts.html, and click the name of your geographic region for phone numbers of people who provide support for your location.

Determining the business impact

When you submit a problem to IBM, you are asked to supply a severity level. Therefore, you must understand and assess the business impact of the problem that you are reporting.

Use the following criteria:

Table 8. Severity levels

Severity 1	The problem has a *critical* business impact: You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.
Severity 2	This problem has a *significant* business impact: The program is usable, but it is severely limited.
Severity 3	The problem has *some* business impact: The program is usable, but less significant features (not critical to operations) are unavailable.
Severity 4	The problem has *minimal* business impact: The problem causes little impact on operations or a reasonable circumvention to the problem was implemented.

Describing a problem

When describing a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently.

To save time, know the answers to these questions:

- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms?
- Can you re-create the problem? If so, what steps do you perform to re-create the problem?
- Did you change anything in the system? For example, did you change anything in the hardware, operating system, networking software, or other system components?
- Are you currently using a workaround for the problem? If so, be prepared to describe the workaround when you report the problem.

Submitting data

You can send diagnostic data, such as log files and configuration files, to IBM Software Support.

Use one of the following methods:

- IBM Support Assistant
- FTP (EcuRep)
- ESR tool

IBM Support Assistant

IBM Support Assistant includes a service feature which has an automated system collector and a symptom-based collector. The system collector gathers general information from your operating system, registry, and other sources. The symptom-based collector gathers specific product information relating to a particular problem that you are having. The service feature also enables you to automatically set tracing to help IBM support in the data gathering process. See the "IBM Support Assistant" on page 51 for more information about IBM Support Assistant.

FTP (EcuRep)

Use the FTP service called EcuRep to submit data files to IBM. Package the data files that you collected into ZIP or TAR format, and name the package according to your Problem Management Record (PMR) identifier. Your file must use the following naming convention to be correctly associated with the PMR:

```
xxxxx.bbb.ccc.yyy.yyy
```

where:

Table 9. File naming convention

xxxxx	PMR number
bbb	Branch, from the PMR identifier
ccc	Country code, from the PMR identifier
yyy.yyy	File type (ZIP or TAR format)

Use FTP to transfer your files and follow these steps:

1. Using an FTP utility, connect to the emea.ibm.com server (for example, ftp.emea.ibm.com).
2. Log on as anonymous.
3. Enter your email address as your password.
4. Change directories to toibm (for example, cd toibm).
5. Change to one of the platform-specific subdirectories: aix, cae, hw, linux, lotus, mvs, os2, os400, swm, tivoli, unix, vm, vse, and windows.
6. Change to binary (bin) mode (for example, bin).
7. Put your file on the server. You can send but not update files on the FTP server. Therefore, any subsequent time that you must change the file, you create a file with a unique name.

For more information about the EcuRep service, see IBM EMEA Centralized Customer Data Store Service at http://www-05.ibm.com/de/support/ecurep/index.html.

ESR tool

Registered users who are on an authorized caller list can use the Electronic Service Request (ESR) tool to submit diagnostic data. Use the ESR tool to submit and manage Problem Management Records (PMRs) on demand, 24 hours a day, seven days a week, 365 days a year.

To submit data using ESR, complete these steps:

1. Sign onto ESR.
2. On the Welcome page, enter your PMR number in the **Enter a report number** field, and click **Go**.

3. Scroll down to the **Attach Relevant File** field.
4. Click **Browse** to locate the log, trace, or other diagnostic file that you want to submit to IBM Software Support.
5. Click **Submit**. Your file is transferred to IBM Software Support through FTP, and it is associated with your PMR.

Notices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

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

Trademarks

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

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

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

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

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

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

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

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

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

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

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

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

Privacy Policy Considerations

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

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

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

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

Glossary

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

The following cross-references are used in this glossary:

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

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

A

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

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

account data item
The user credentials required for logon.

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

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

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

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

Active Directory credential
The Active Directory user name and password.

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

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

active RFID
See active radio frequency identification.

AD
See Active Directory.

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

API
See application programming interface.

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

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

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

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

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

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

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

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

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

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

B

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

base image
A template for a virtual desktop.

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

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

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

C

CA See certificate authority.

CAPI See cryptographic application programming interface.

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

CCOW
See Clinical Context Object Workgroup.

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

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

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

CLI See command-line interface.

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

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

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

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

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

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

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

CSN See Card Serial Number.

CSP See cryptographic service provider.

D

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

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

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

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

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

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

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

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

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

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

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

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

DLL See dynamic link library.

DN See distinguished name.

DNS See domain name server.

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

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

E

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

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

ESSO See enterprise single sign-on.

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

F

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

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

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

FIPS See Federal Information Processing Standard.

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

FQDN
See fully qualified domain name.

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

G

GINA See graphical identification and authentication.

GPO See group policy object.

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

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

H

HA See high availability.

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

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

hot key
A key sequence used to shift operations

between different applications or between different functions of an application.

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

I

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

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

J

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

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

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

JMX See Java Management Extensions.

JRE See Java runtime environment.

JVM See Java virtual machine.

K

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

L

LDAP See Lightweight Directory Access Protocol.

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

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

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

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

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

M

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

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

N

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

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

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

O

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

OTP See one-time password.

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

P

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

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

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

PIN See personal identification number.

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

PKCS See Public Key Cryptography Standards.

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

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

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

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

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

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

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

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

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

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

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

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

R

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

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

RDP See remote desktop protocol.

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

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

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

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

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

RFID See radio frequency identification.

root CA
See root certificate authority.

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

S

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

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

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

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

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

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

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

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

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

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

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

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

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

sign up
To request a resource.

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

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

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

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

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

SMTP See Simple Mail Transfer Protocol.

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

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

SPI See service provider interface.

SSL See Secure Sockets Layer.

SSL VPN
See Secure Sockets Layer virtual private network.

SSO See single sign-on.

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

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

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

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

STS See Security Token Service.

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

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

T

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

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

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

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

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

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

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

tty See terminal type.

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

U

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

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

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

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

V

VB See Visual Basic.

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

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

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

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

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

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

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

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

VMM See Virtual Member Manager.

VPN See virtual private network.

W

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

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

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

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

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

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

Index

A

abends 8
AccessAdmin
  Back button not working 32
  connection issues 25
  fields not working 29
  logon issues 20, 21
  Service unavailable 26
AccessAgent
  application conflicts 13
  console application support 27
  IMS Server
    certificate 13
    connection 13
  installation issues 11, 13
  module registration 14
  Mozilla Firefox issues 31
  signup issues 16
  slow performance 23
  Wallet 24
AccessAssistant
  Back button not working 32
  logon issues 21
accessibility v
AccessProfile
  machine Wallet 24
  missing in properties pane 28
  OutOfMemory error 28
AccessStudio 28
activity.log file 42, 45
analyzing log data 39
APAR 37, 51
authentication device, lost 19
authentication factors 18

B

BIO-key verification UI 19

C

checklist for troubleshooting 1, 9
collecting data for a problem 41
connectivity 5
contacting IBM Software Support 51
contracts, software maintenance 52
Convert to option 28
crashes 8

D

data collection 41
directory server, configuration issues 15

E

EcuRep service 54
education v
Electronic Service Request 54
error messages 6
ESR tool 54

F

fixes 5, 35
  download 35
  fix pack 5
  receive notifications 35
  refresh pack 5
FTP EcuRep service 54

G

glossary 61

H

httpd.conf file, cannot open 26

I

IBM
  Software Support v
  Support Assistant v
IBM HTTP Server 14
IBM Service log
  activity.log file 43
  configuration 45
IBM Software Support 51
IBM Support Assistant 41, 47, 53
  console mode 48
  graphical mode 47
  search tool 51
  self-help links 51
  service feature 51
IMS Configuration Wizard 29
IMS Server
  cannot download certificate 13
  cannot issue certificate 27
  configuration issues 15
  connection issues 13
  database slowdown 29
  deployment issues 16
  deployment type 32
  installation issues 12
  logon issues 21
  slow performance 23
IMS Server version 32
Integrated Solutions Console 21

J

JVM logs
  configuration 44
  default filename 42
  path 43
  view 47

K

knowledge bases, searching 37
known issues
  authentication factors 18
  browser 30
  installation 11
  logon issues 20
  product components
    configuration 14
    installation 11
    operation 25
  Wallet 23

L

log settings 44
logon credentials 31
logs
  analyze data 39
  enable trace at server startup 45
  enable trace on a running server 46
  file names 42, 43
  locations 43, 44
  message 43
  message types 42
  trace 44
  view 47

M

maintenance contracts 52
message logs 41, 42, 44
messages 6
methods for submitting data to IBM
  ESR tool 53
  FTP EcuRep service 53
  IBM Support Assistant 53
Microsoft Internet Explorer
  cannot open web applications 32
  single sign-on issues 29
  stop when browsing 30
Mozilla Firefox
  single sign-on feature 31
  single sign-on issues 31
  successful logon page not captured 29

N

node federation 16

P

password problems 18
performance problems 6
problem management report 51
problem-determination v
problem-specific data 41

problems
  performance 6
  report 53
product fixes 5
publications
  statement of good security practices v

R

refresh pack 5

S

Server AccessAgent mode 33
severity levels, problems 53
signup issues
  ESSO GINA with smart card 20
  new user 21
smart card issues
  sign up from ESSO GINA 20
  slow recognition 20
software maintenance contracts 52
software support, contacting 51
submitting data to IBM, methods 53
SystemOut.log file 42

T

technotes 37
trace logs 41, 43, 45
training v
Transparent Screen Lock 25
traps 8
troubleshooting 3
  checklist 1, 9
  data collection 41
  log data analysis 39
  problem description 53
  problem identification 3
  process 1

U

updates to product 5

V

view logs 47

W

Wallet-related problems 24
Web API credential management 29
Web Workplace
  Back button not working 32
  logon issues 21
  signup issues 16
WebSphere Application Server 26

Printed in USA