IBM Security Privileged Identity Manager
Version 2.0.2

Troubleshooting Guide

IBM Security Privileged Identity Manager
Version 2.0.2

Troubleshooting Guide

Note

Before using this information and the product it supports, read the information in Notices.

Edition notice

Note: This edition applies to Version 2.0.2 of *IBM Security Privileged Identity Manager* **(product number 5725-H30) and to all subsequent releases and modifications until otherwise indicated in new editions.**

Contents

Figures

Tables

Chapter 1. General information

To get started with troubleshooting, familiarize yourself with the basic techniques for troubleshooting and on how to contact and exchange information with IBM Support. You can also use tools such as IBM knowledge base, Fix Central, and Support Portal.

Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. Certain common techniques can help with the task of troubleshooting.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- 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, which can then lead you to a problem resolution.

What are the symptoms of the problem?

When starting to describe a problem, the most obvious question is "What is the problem?" This 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, crash, performance degradation, or incorrect result?

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 of the components to consider when you are investigating problems.

The following questions 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?

- Do all users have the problem?
- (For multisite installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in 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 and version, all corresponding software and versions, and hardware information. Confirm that you are running in 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 develop a 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 need to look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, 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 these types of questions can give you a frame of reference in which to investigate the problem.

Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These 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 need to happen for the problem to occur?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might have occurred around the same time, the problems are not necessarily related.

Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem 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 is of significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

About this task

You can find useful information by searching the IBM® Security Privileged Identity Manager documentation. However, sometimes you need to look beyond the documentation to answer your questions or resolve problems.

Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

- Search for content by using the IBM Support Assistant (ISA).

  ISA is a no-charge software serviceability workbench that helps you answer questions and resolve problems with IBM software products. You can find instructions for downloading and installing ISA on the ISA website.
- Find the content that you need by using the IBM Support Portal.

  The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the demo videos about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.
- Search for content about IBM Security Privileged Identity Manager by using one of the following additional technical resources:
  - IBM Security Privileged Identity Manager Support website.
  - IBM support communities (forums and newsgroups).
- Search for content by using the IBM masthead search. You can use the IBM masthead search by typing your search string into the **Search** field at the top of any ibm.com® page.
- Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

  Tip: Include "IBM" and the name of the product in your search if you are looking for information about an IBM product.

Getting fixes from Fix Central

You can use Fix Central to find the fixes that are provided by IBM Support for various products, including IBM Security Privileged Identity Manager. With Fix Central, you can search, select, order, and download fixes for your system with a choice of delivery options. A IBM Security Privileged Identity Manager product fix might be available to resolve your problem.

Procedure

To find and install fixes:

1. Obtain the tools that are required to get the fix. If it is not installed, obtain your product update installer. You can download the installer from Fix Central. This site provides download, installation, and configuration instructions for the update installer.
2. Select IBM Security Privileged Identity Manager as the product, and select one or more check boxes that are relevant to the problem that you want to resolve. For details, see: http://www.ibm.com/systems/support/fixes/en/fixcentral/help/faq_sw.html.
3. Identify and select the fix that is required.
4. Download the fix.
   a. Open the download document and follow the link in the “Download Package” section.
   b. When you download the file, ensure that the name of the maintenance file is not changed. This change might be intentional, or it might be an inadvertent change that is caused by certain web browsers or download utilities.
5. Apply the fix.
   a. Follow the instructions in the “Installation Instructions” section of the download document.
   b. For more information, see the “Installing a fix pack” topic in the product documentation.
6. Optional: Subscribe to receive weekly email notifications about fixes and other IBM Support updates. See “Subscribing to Support updates” on page 6.

Contacting IBM Support

IBM Support provides assistance with product defects, answers FAQs, and helps users resolve problems with the product.

Before you begin

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company or organization must have an active IBM *maintenance contract name*, and you must be authorized to submit problems to IBM. For information about the types of available support, see the Support portfolio topic in the “*Software Support Handbook*”.

For information about the types of available support, see the Support portfolio topic in the *Software Support Handbook*.

Procedure

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem. See the Contacting IBM Support topic in the *Software Support Handbook*. For more information, see the Getting IBM support topic in the *Software Support Handbook*.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
   - Using IBM Support Assistant (ISA):
     a. Download and install the ISA tool from the ISA website. See www.ibm.com/software/support/isa/.
     b. Open ISA.
     c. Click **Collection and Send Data**.
     d. Click the **Service Requests** tab.
     e. Click **Open a New Service Request**.

     Using ISA in this way can expedite the analysis and reduce the time to resolution.
   - Online through the IBM Support Portal: You can open, update, and view all of your service requests from the **Service Request** portlet on the Service Request page.
   - By telephone for critical, system down, or severity 1 issues: For the telephone number to call in your region, see the Directory of worldwide contacts web page. You can also see the Contacts page in the *Software Support Handbook*.

Results

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

Exchanging information with IBM

To diagnose or identify a problem, you might need to provide IBM Support with data and information from your system. In other cases, IBM Support might provide you with tools or utilities to use for problem determination.

Sending information to IBM Support

To reduce the time that is required to resolve your problem, you can send trace and diagnostic information to IBM Support.

Procedure

To submit diagnostic information to IBM Support:

1. Open a problem management record (PMR).
2. Collect the diagnostic data that you need. Diagnostic data helps reduce the time that it takes to resolve your PMR. You can collect the diagnostic data manually or automatically:

- Collect the data manually.
- Collect the data automatically.

3. Compress the files by using the `.zip` or `.tar` file format.
4. Transfer the files to IBM. You can use one of the following methods to transfer the files to IBM:
   - IBM Support Assistant
   - The Service Request tool
   - Standard data upload methods: FTP, HTTP
   - Secure data upload methods: FTPS, SFTP, HTTPS
   - Email

   All of these data exchange methods are explained on the IBM Support website.

Receiving information from IBM Support

Occasionally an IBM technical-support representative might ask you to download diagnostic tools or other files. You can use FTP to download these files.

Before you begin

Ensure that your IBM technical-support representative provided you with the preferred server to use for downloading the files and the exact directory and file names to access.

Procedure

To download files from IBM Support:

1. Use FTP to connect to the site that your IBM technical-support representative provided and log in as `anonymous`. Use your email address as the password.
2. Change to the appropriate directory:
   a. Change to the `/fromibm` directory.
   ```
   cd fromibm
   ```
   b. Change to the directory that your IBM technical-support representative provided.
   ```
   cd nameofdirectory
   ```
3. Enable binary mode for your session.
   ```
   binary
   ```
4. Use the **`get`** command to download the file that your IBM technical-support representative specified.
   ```
   get filename.extension
   ```
5. End your FTP session.
   ```
   quit
   ```

Subscribing to Support updates

To stay informed of important information about the IBM products that you use, you can subscribe to updates.

About this task

By subscribing to receive updates about IBM Security Privileged Identity Manager, you can receive important technical information and updates for specific IBM Support tools and resources. You can subscribe to updates by using one of two approaches:

RSS feeds

For information about RSS, including steps for getting started and a list of RSS-enabled IBM web pages, visit the IBM Software Support RSS feeds site.

My Notifications

With **My Notifications**, you can subscribe to Support updates for any IBM product. **My Notifications** replaces **My Support**, which is a similar tool that you might have used in the past. With **My Notifications**, you can specify that you want to receive daily or weekly email announcements. You can specify what type of information you want to receive (such as publications, hints and tips, product flashes (also known as alerts), downloads, and drivers). **My Notifications** enables you to customize and categorize the products about which you want to be informed and the delivery methods that best suit your needs.

Procedure

To subscribe to Support updates:

1. Subscribe to My Notifications by going to the IBM Support Portal and click **My Notifications** in the **Notifications** portlet.
2. Sign in using your IBM ID and password, and click **Submit**.
3. Identify what and how you want to receive updates.
   a. Click the **Subscribe** tab.
   b. Select the appropriate software brand or type of hardware.
   c. Select one or more products by name and click **Continue**.
   d. Select your preferences for how to receive updates, whether by email, online in a designated folder, or as an RSS or Atom feed.
   e. Select the types of documentation updates that you want to receive, for example, new information about product downloads and discussion group comments.
   f. Click **Submit**.

Results

Until you modify your **RSS feeds** and **My Notifications** preferences, you receive notifications of updates that you have requested. You can modify your preferences when needed (for example, if you stop using one product and begin using another product).

Related information

IBM Software Support RSS feeds

Subscribe to My Notifications support content updates

My Notifications for IBM technical support

My Notifications for IBM technical support overview

Chapter 2. Common problems and solutions

Find possible solutions to common problems.

Table 1. Lists some of the common problems and possible solutions.

Problem	Solutions
AccessAgent throws a Privileged Credential Manager error about an invalid password during check-in and check-out.	IBM Security Privileged Identity Manager password has expired. Reset the password for the credential in Service Center.
Cannot log in to IBM Security Privileged Identity Manager consoles. You keep getting password invalid or a password expired error. Data tier was restarted while the virtual appliance was running.	Restart the virtual appliance.
AccessProfile is loaded, but no check-in or check out or recording occurs.	You are using a standard single sign-on profile, not one that is enhanced for check-in, check-out, and session recording.
Virtual appliance response is slow or unstable.	Causes: • Virtual appliance is deployed on a non-supported VMware platform or version. Solution: Install a supported version of VMware. • Insufficient RAM. Solution: Increase RAM allocation.
Problem with certificates in a virtual appliance cluster.	Causes: • AccessAgent is not configured to communicate with the load balancer. • Load balancers CA certificate is not imported properly. • The load balancers certificate host name does not match. Solution Deploy the CA certificate with the AccessAgent installer. If AccessAgent is already installed, copy the certificate into the AccessAgent folder and then restart.

Table 1. Lists some of the common problems and possible solutions. (continued)

Problem	Solutions
Check in and check out throws an error. Check in and check out works but nothing is recorded.	Causes: • Mismatched host name in certificate. • DNS or host file is not set up correctly to resolve target URL. Solution: Deploy the CA certificate with the AccessAgent installer. If AccessAgent is already installed, copy the certificate into the AccessAgent folder and then restart.
When the IBM Security Privileged Identity Manager Server is not available.	• Check the network connection. • Check that the user registry or directory server is operational.
The managed resource is not configured for shared access for IBM Security Privileged Identity Manager.	• Configure the managed resource for shared access with IBM Security Privileged Identity Manager. • Avoid logging with shared access credentials.
All the available shared access credentials are checked out.	• Wait for a few minutes until there are available shared access credentials. • Find out the identity of the checked out credentials from the IBM Security Privileged Identity Manager. Ask the credential owner to check in their credentials.
There are no IBM Security Privileged Identity Manager Server credentials in the Wallet.	Follow the instructions on the screen to enter the credentials. The credentials must have privileges to check out shared access credentials.
The account that is used to log on to the managed resource does not have correct entitlements on IBM Security Privileged Identity Manager.	Use IBM Security Privileged Identity Manager to ensure that the account used to log on has correct permissions for the available shared access accounts.
Client application is not responding to keyboard or mouse input. For example: you cannot resize or move the window for the client application.	Verify that the Session Recorder service is: • Started on the client workstation. • Accessible from the client. The behaviour of the client application is determined by the privileged identity management policies in AccessAdmin.
Client application is closed unexpectedly.	• Verify that the Session Recorder service on the client workstation is started. • Verify that the Privileged Session Recorder Server is running and reachable from the client. The behaviour of the client application is determined by the privileged identity management policies in AccessAdmin.

Table 1. Lists some of the common problems and possible solutions. (continued)

Problem	Solutions
IBM Security Access Manager for Enterprise Single Sign-On ends the active process but does not check in the shared access credential when the following conditions occur: • A shared access credential is checked out from IBM Security Privileged Identity Manager through IBM Security Access Manager for Enterprise Single Sign-On. • The shared access credential is used by the user until the lease expires. Since the shared access credential is not checked in, users cannot use the shared access credential unless IBM Security Privileged Identity Manager is configured to check in the shared access credential.	If you want users to use the shared access credential again: 1. Open the **IBM Security Privileged Identity Manager Console**. 2. Click **Manage Shared Access** > **Configure Credential Default Settings**. 3. Select **Notify violation and check in**.

Chapter 3. Troubleshooting the virtual appliance

This section describes the solutions for potential IBM Security Privileged Identity Manager virtual appliance problems.

Troubleshooting dashboard panel widget display issues on Microsoft Internet Explorer 10

The dashboard panel widget might not display while viewing it in the Microsoft Internet Explorer 10 browser.

About this task

An attempt to view the IBM Security Privileged Identity Manager virtual appliance console or activation wizard in a Microsoft Internet Explorer, version 10 browser does not display the panel widget.

To solve the issue, complete these steps as a workaround:

Procedure

1. Open the Microsoft Internet Explorer 10 browser.
2. After the activation steps are completed, change the browser setting:
   a. Click **Tools**.
   b. Deselect **Compatibility View**.
   c. Open **Compatibility View Settings**.
   d. Deselect the **Download updated compatibility lists from Microsoft** option.
3. Access the IBM Security Privileged Identity Manager virtual appliance console.

Troubleshooting Logon to Session Replay Console

The Logon to Session Replay Console fails if the virtual appliance console and Session Replay Console are opened in the same browser window.

About this task

An attempt to do the Logon to Session Replay Console opened in the same browser window where the virtual appliance console is open fails. To solve the issue, complete these steps as a workaround:

Procedure

1. Clear the browser cache before you access the Session Replay Console.
2. Open a new browser window to access the Session Replay Console.

Value for a property is not retained if update_syslog command is executed without any value for other properties

If a user does not enter any value for a property before running the `update_syslog` command, default values are set for the property.

The default value of the following parameters is `false` if a user does not specify any value.

```
logSystemManagementActivity: false
logUserAdminActivity: false
logUserService: false
logUserActivity: false
```

For the syslog CLI utility, the default values for the IBM Security Privileged Identity Manager entries are:

```
rwrangler.example.com:ispim> list_syslog
  Enable syslog
    logSystemManagementActivity: false
    logUserAdminActivity: false
    logUserService: false
    logUserActivity: false
  Syslog server port: 514
  Syslog server hostname: localhost
  Syslog logging facility: 20
  Syslog field-separator: \n
```

Startup problems with the IBM Security Privileged Identity Manager virtual appliance Dashboard

You might encounter some problems when you start the IBM Security Privileged Identity Manager virtual appliance Dashboard.

The possible startup problems are as follows:

- Startup or loading delays for several seconds or minutes.
- A notification prompts for a required restart.
- A component status prompts as started, but is not available.

Symptom

You might experience some delays or other startup problems with the IBM Security Privileged Identity Manager virtual appliance Dashboard due to these conditions:

- The virtual appliance dashboard starts for the first time after configuration.
- All the widgets are not loaded.

Resolving the problem

Wait for some time and refresh the widget to check the latest status of the virtual appliance.

Virtual appliance dashboard displays notifications about snapshots

The IBM Security Privileged Identity Manager virtual appliance Dashboard displays notifications that a snapshot is being applied.

Symptom

Notifications about snapshots that are being applied are displayed by the IBM Security Privileged Identity Manager virtual appliance Dashboard.

Resolving the problem

Snapshots might also change the network settings of the virtual appliance. When you apply a snapshot from the management interface of the virtual appliance, you are directed to a pop-up window. The window notifies you to go to the virtual appliance by using the IP or the host name that is specified in the snapshot.

If you log on to the virtual appliance while the snapshot process is in progress, in the Notification widget, you might see a notification such as `'Snapshot is getting applied'`. Since the snapshot process takes some time, wait until the process completes. Refresh the Notification widget to retrieve the recent notifications.

LDAP Server must run when IBM Security Privileged Identity Manager virtual appliance servers are restarted after LDAP configuration

The LDAP Server must be running when you restart the IBM Security Privileged Identity Manager virtual appliance servers after an LDAP configuration.

Symptom

When the IBM Security Privileged Identity Manager virtual appliance servers are restarted after an LDAP configuration, the LDAP Server must be in a running state.

Resolving the problem

Some of the post-configuration tasks start running after an LDAP configuration and when you start the IBM Security Privileged Identity Manager virtual appliance server. This task requires the LDAP Server to be in running state. Therefore, it is required that the LDAP Server is running.

Restrict operations for a Member node

The IBM Security Privileged Identity Manager virtual appliance cluster is composed of one `Primary node` and other nodes that are called as `Member` nodes. To configure a virtual appliance, you must work from a `Primary node`.

The **Configure** menu contains the following configuration options:

- `Directory Server Configuration`
- `Database Server Configuration`
- `E-mail Server Configuration`
- `Upload Feed File`
- `Update property`
- `Load Balancer configuration`
- `Session Recording activation`
- `Administrator settings`
- Other CLI configuration options such as:
  - Service properties
  - Syslog properties
  - Set password

The operations for any of these configuration options are restricted for a `Member node`.

If you open any Configuration page from the **Configure** menu on the `Member node` to modify any configuration information, a warning message is displayed.

If you ignore the warning message and continue to modify any of the configuration information from the **Configure** menu, a warning message indicates that you cannot complete the operation.

The restriction exists because the IBM Security Privileged Identity Manager virtual appliance is a member of a cluster, which does not contain the role of a `Primary node`.

Handling password synchronization issues

You encounter administrator password synchronization issues when you undo or redo a configuration for the Single Sign-On data store. The synchronization issues are between the Identity and Credential Vault Administration console, the Single Sign-On and Session Recorder Administration console, and the Session Replay Console.

About this task

The administrator password is not synchronized with each of the following consoles when you undo and redo the configuration for the Single Sign-On data store:

- Identity and Credential Vault Administration console
- Single Sign-On and Session Recorder Administration console
- Session Replay Console

Procedure

1. Log on to Administrative console with the `pim manager` credentials.
2. From the navigation tree, click **Manage Users** to display the Select a User page.
3. In the **Users** table, click the twistie icon ▶ next to the user name whose password that you want to change.
4. Click **Accounts** to display the Accounts page.
5. On the Accounts page, click the twistie icon ▶ next to the user ID.
6. Click **Change Password**.
7. On the Change Passwords page, select **Allow me to type a password**.
8. In the **Password** field, enter a password.
9. In the **Confirm Password** field, retype the password.

Results

The password for the Administrative console, the Single Sign-On and Session Recorder Administration console, and the Session Replay Console is synchronized.

What to do next

Log on to the following consoles by using the new password to verify whether it is synchronized:

- Identity and Credential Vault Administration console
- Single Sign-On and Session Recorder Administration console
- Session Replay Console

Cluster bootstrap process

Bootstrapping refers to getting a cluster node up and running. When a cluster node recovers from failure, checks are made to keep the node state consistent with the rest of the nodes in the cluster.

When you encounter an unresponsive `Primary node` or `Member node`, take following actions:

- You remove it from the Load Balancer configuration, which stops user requests from being routed to the node.
- You troubleshoot or fix the errors by using the various methods that are documented in http://www-01.ibm.com/support/knowledgecenter/SSRQBP/welcome.
- Restart the `Primary node` or the `Member node` virtual appliance.
  - Reconnect the `Member node` with the new `Primary node` if the earlier role of the node was changed from `Primary` to `Member`.
  - Synchronize the `Member node` with the `Primary node` if the node continues to be a `Member node`, but missed a few virtual appliance configuration updates.
  - This node becomes a stand-alone node if this node is removed from the cluster definition.

The following actions are done by the cluster bootstrap process:

- When a `Primary node` recovers from a failure and detects that no other node is promoted to `Primary`, it continues to be as `Primary` in that cluster.
- When a `Member node` recovers from a failure and detects that it continues to be part of the original cluster, synchronization might be needed if the virtual appliance configuration changes were made.
- When a `Primary node` recovers from a failure and detects that another node is promoted to `Primary`, the role of the current node is changed to `Member` and a reconnect notification request is set.
- When a `Primary node` or a `Member node` recovers from a failure and cannot connect with any of the previously known cluster members because the virtual appliance password changed, the current node is made a stand-alone node. A reconnect notification is set.

Cluster monitor service

Cluster monitor service is a background process in the IBM Security Privileged Identity Manager virtual appliance that frequently checks for all business functions to be alive and running.

The cluster monitor service specifically checks for the following aspects:

- The three servers:
  - Identity
  - Single Sign-On
  - Session Recorder
- Data stores for the installed servers
- IBM Security Directory Server
- IBM Security Directory Integrator Service Connector

An administrator can check the status of the three servers by following the instructions that are provided in Monitoring URLs. The status of all the IBM

Security Privileged Identity Manager virtual appliance components is shown on the Middleware and Server Monitor widget of the IBM Security Privileged Identity Manager virtual appliance console. The IBM Security Directory Integrator Service Connector status is reflected in the availability status of the Identity Server.

The cluster monitor service checks the former function at a repeating and fixed interval of 4 seconds. When it finds that one or more of the services are not functional, the following actions are taken:

1. Automatically stops external access to the Identity, Single Sign-On, and the IBM Privileged Session Recorder functions. This action means that the business user requests for check-out or check-in of the shared credentials cannot be serviced by the IBM Security Privileged Identity Manager virtual appliance.
2. Sends an email notification to the IBM Security Privileged Identity Manager administrator with the URL for the IBM Security Privileged Identity Manager virtual appliance where one or some failures occurred.

Similarly, the cluster monitor service can detect service restoration when the failures are fixed. The following actions are taken:

1. Automatically enables external access to the Identity, Single Sign-On, and the IBM Privileged Session Recorder functions. This action means that the business user requests for check-out or check-in of the shared credentials can be serviced by the IBM Security Privileged Identity Manager virtual appliance.
2. Sends an email notification to the IBM Security Privileged Identity Manager administrator with the URL for the IBM Security Privileged Identity Manager virtual appliance where the service is restored after failures were fixed.

Checking logs

Use the Log Retrieval and Configuration page to view the log files. You can also use this page configure the server log settings for the IBM Security Privileged Identity Manager virtual appliance.

About this task

To learn more about the available log files, see Retrieving logs.

Procedure

From the top menu, click **Manage** > **Log Retrieval and Configuration**.

Common issues

You might encounter common issues during the deployment and usage of IBM Security Privileged Identity Manager in the IBM Security Privileged Identity Manager virtual appliance. For more information, see the following common issues and workaround sections.

Password policy noncompliance

IBM Security Privileged Identity Manager generated passwords do not comply with certain rule settings in the password policy.

Identity provider operations fails

Check that the password is provided to the identity provider from the Privileged Identity Manager Service Center. When updating any of the identity provider properties, reenter the password upon each update and test the connection before submitting the changes made to an identity provider.

Data store configuration fails

Check the configuration of the database system.

On the Log Retrieval and Configuration page, click the **Appliance** tab and check the Identity, Single Sign-On and Session Recording data store configuration, Server System Out, and Server Messages.

Directory Server Configuration fails

Check the configuration of the directory server.

On the Log Retrieval and Configuration page, click the **Appliance** tab and check the directory server configuration, Server System Out, and Server Messages.

Unable to access the virtual appliance console

Make sure that the network configuration link IP, Subnet Mast, DNS, and Gateway are correct.

High Disk Usage Notification on Dashboard

Reduce the setting for the **Maximum size for log file rotation** and **Maximum number of historical log files**.

Reduce the trace level from the command-line interface.

Clean the log files from **Manage** > **Maintenance** > **Log Retrieval and Configuration**.

Unable to access credentials by using AccessAgent on client system

Make sure that the virtual appliance host name is registered with DNS or updated in the client system hosts file.

Restart the client system.

Make sure that the time in the client system where AccessAgent is installed and the time in the IBM Security Privileged Identity Manager virtual appliance are synchronized.

Test connection or reconciliation operation failed by using Identity and Credential Vault administration console

Restart by using the **Server control dashboard** widget with the option **Others(Full restart)**. If the operation still fails, restart the virtual appliance.

Unable to access Identity and Credential Vault Administration console

Check the **Middleware and Server Monitor** dashboard widget to verify the status of the Identity server, Directory server, and Identity data store. Then, take the appropriate action.

See the log files for more details.

Unable to access Single Sign-on and Session Recorder Administration console

Check the **Middleware and Server Monitor** dashboard widget to verify the status of the Single Sign-On server and Single Sign-On data store. Then, take the appropriate action.

See the log files for more details.

Unable to access Session Recorder Replay console (if activated)

Check the **Middleware and Server Monitor** dashboard widget to verify the status of the Session Recording server and Session Recording data store. Then, take the appropriate action.

See the log files for more details.

For any other unrecoverable issues

Generate a support file by using the command-line interface or the virtual appliance console for the IBM Support Team.

CLI

```
ispimva.example.com> support
ispimva.example.com:support> create
ispimva.example.com:support> download
1: ispim_1.0.1.1_20130925-014609_ispimva.example.com.zip
2: ispim_1.0.1.1_20130925-015645_ispimva.example.com.zip
Enter index: 1
Insert a USB drive into the USB port on the appliance.
Enter 'YES' to confirm: YES
```

Console

1. Log on to the IBM Security Privileged Identity Manager virtual appliance console.
2. Select **Manage** > **System Settings** > **Support Files**.
3. Click **new** to create a new file.
4. Click **download** to save a copy of the support file.

Unable to connect the IBM Security Privileged Identity Manager Server even with the correct host name

To resolve this issue, add the certificate to the client.

1. Log on with Administrator privileges on the client computer.

2. Start a web browser and go to the HTTPS URL for the IBM Security Privileged Identity Manager Server `https://hostname` where host name is the name of the computer that has the IBM Security Privileged Identity Manager virtual appliance Server.
3. In the web browser, export the security certificates to a file.
4. Complete the following instructions:
   a. On the Microsoft Internet Explorer, click **File** > **Properties**.
   b. Click **Certificates**.
   c. Click the **Certification Path** tab.
   d. Click the **Details** tab.
   e. For each certificate marked with a red `X` in the certificate hierarchy, do the following actions.
      1) Click **View Certificate**.
      2) Click **Details**.
      3) Click **Copy to File**.
      4) Follow the instructions in the wizard with the following considerations:
         - When the Export format page is displayed, select the **DER encode binary x.509 (CER) format**.
         - Save the certificates on your local computer. For example: `webhost.cer`.
5. Copy the CER files to the following location: `*aa_home*\SessionRecorder`

   aa_home is the AccessAgent installation directory. For example: `C:\Program Files\IBM\ISAM ESSO\AA\`.
6. Restart the computer where AccessAgent is installed.

Limitations

Limitations in a prerequisite component can affect how the IBM Security Privileged Identity Manager virtual appliance capabilities work.

Virtual appliance limitations

- Characters other than English are not supported in the **Comment** fields of the following IBM Security Privileged Identity Manager virtual appliance panels:
  – Snapshot
  – Firmware Settings
  – Support Files
- The following file name display issues occur in several languages when a snapshot with a long file name is uploaded in the IBM Security Privileged Identity Manager virtual appliance:
  – The text in the **Comment** field is truncated.
  – The file name gets truncated in the **Snapshot** table.

IBM Security Privileged Identity Manager limitations

- Data Tier and Reporting components

  The Data Tier and Reporting components must be installed separately or outside the IBM Security Privileged Identity Manager virtual appliance.
  – IBM Cognos® reporting components are outside of the IBM Security Privileged Identity Manager virtual appliance.

  - Supports only DB2® and IBM Security Directory Server as the IBM Security Privileged Identity Manager data store on the external data tier.
- Limited IBM Security Privileged Identity Manager and IBM Security Access Manager for Enterprise Single Sign-On functions are supported.

  Customization is limited since there is no direct access to low-level IBM Security Privileged Identity Manager and IBM Security Access Manager for Enterprise Single Sign-On configuration files.
- Changing the IBM Security Privileged Identity Manager user logon ID on the IBM Security Privileged Identity Manager console and AccessAgent is not supported.
- Three network adapters can be used.
- Custom workflow extension configuration is not supported.
- Uploading of custom Java archive files, which implements IBM Security Privileged Identity Manager custom extensions, is not supported. For example, workflow.
- External adapters that work with an external IBM Security Directory Integrator are not supported.
- Multiple domains on Active Directory are not supported.
- Multiple Active Directory servers are not supported.

IBM Security Access Manager for Enterprise Single Sign-On limitations

- AccessAgent sign up

  Sign-up is not allowed from AccessAgent. Users are signed up through IBM Security Privileged Identity Manager.
- AccessAssistant/WebWorkplace

  This component is not required for IBM Security Privileged Identity Manager.
- Self-Service Sign-Up through IBM Security Access Manager for Enterprise Single Sign-On AccessAgent

  This feature is not supported because users are to be on-boarded through IBM Security Privileged Identity Manager.
- Self-Service Password Reset

  IBM Security Privileged Identity Manager virtual appliance users must use the equivalent feature in IBM Security Privileged Identity Manager instead.
- Change ISAM ESSO password

  Users must use the equivalent feature in the IBM Security Privileged Identity Manager Self-Service UI instead. You can change the password with AccessAgent with Active Directory configured.
- Biometric and smartcard second factor support with IBM Security Access Manager for Enterprise Single Sign-On Agent are not available in the IBM Security Privileged Identity Manager virtual appliance.
- Only the default User Policy Template is supported. User Policy Templates that are based on arbitrary directory attributes are not supported.
- Third-party Provisioning System to provision or manage IBM Security Access Manager for Enterprise Single Sign-On accounts or Wallets

  This component is not required in the IBM Security Privileged Identity Manager virtual appliance because the IBM Security Access Manager for

Enterprise Single Sign-On accounts are provisioned through IBM Security Privileged Identity Manager.

- IBM Security Access Manager for Enterprise Single Sign-On mobile

  This feature is not used with IBM Security Privileged Identity Manager.
- Mobile Active Code, One Time Password, or RADIUS are not supported
- AccessAgent Private and Shared Desktop modes are not supported.
- IMS Configuration wizard and single sign-on CLTs are not supported.

Bulkload command errors

When running the bulkload command, some errors might occur. The bulkload utility fails if any of the entries in the input LDIF file exist in LDAP.

This error might occur if the suffix you defined exists as an entry in the directory server. It might be necessary to delete all entries in the suffix (but leave the suffix) from LDAP before running the command. You can use the `ldapsearch` commands to check for existence of entries, and the `ldapdelete` command to remove these entries.

Error codes:

```
GLPCRY007E The directory key stash file is inconsistent with the associated
encrypted data.

GLPBLK071E Bulkload is unable to run because of an initialization error.

GLPBLK030E Run DB2CMD.EXE first, and then run bulkload within the "DB2 CMD"
command interpreter.
```

To correct these errors, you must know the encryption seed and salt values of the target instance. The target instance is the directory server instance where you are running the bulkload.

1. To determine the salt value of target instance, run the following command from `TDS_HOME/bin`:

   ```
   ldapsearch -D bind DN -w password -h hostname -p port -s base -b
   cn=crypto,cn=localhost cn=*
   ```

   where:

   `bind DN` is the distinguished name (DN) of the directory server.

   `password` is the DN password.

   `hostname` is the name of the computer where IBM Security Directory Server is installed.

   `port` is the port number on which IBM Security Directory Server is listening.
2. Replace the value of `ibm-slapdCryptoSync`, `ibm-slapdCryptoSalt` with the values returned by the **`ldapsearch`** command in the `ldap_output_file` file. This file is generated as output of the **`db2ldif`** command, for example `old_ldif_data.ldif`.
3. Run the **`bulkload`** command again.

Note: You can use the **`-W OUT_FILE_NAME`** option with the **`bulkload`** command. This option places the output from the command into the specified file. The bulkload command runs several instances of a DB2 command to load data. Each one has its own success, error, or warning messages. Without the **-W** option to save the output, it is difficult to check the result.

Chapter 4. Shared access

This section describes the solutions for potential privileged credential problems.

Getting access to a target resource when check-in fails or the adapter is not able to connect to the resource

If the IBM Security Privileged Identity Manager cannot establish a connection with the managed endpoint because a network adapter is not working, or the adapter is not configured correctly, for example, with a wrong password, the PIM Manager might want to view the password for the endpoint to regain control.

The following scenarios describe the possible workarounds that the PIM Manager can do to view the password for an endpoint.

Workaround for a scenario with a connection problem with a pending check-in

Scenario

1. As a privileged user, James, checks out a credential for a Linux host with the self-care interface.
2. To simulate a connection problem, as a PIM Manager, log in to the administrator console. Tamper with the Service profile for the host by changing the adapter password to an invalid password. IBM Security Privileged Identity Manager cannot connect to the host.
3. As privileged user James, checks in the account with the self-care interface.

   The `In Process` message is displayed.

   Under **View Requests**, there is a **Check-In** event with status **Pending** that is displayed for James.

   James can no longer see the credential when **View Password** is selected, and cannot check in the credential again.
4. As PIM Manager, in the administrator console, the credential is still checked-out to James, but the **Check-In** option is disabled.

Solution

1. As a PIM Manager, complete the following tasks:
   a. Go to **View Requests** to cancel the pending request from James.

      The **Check-In** command for the credential is enabled.
   b. Disconnect the credential from the resource.
   c. Click **Check-In** for the disconnected credential.
2. When James attempts to check out credentials, the credential is available for selection again.
3. James checks out the credential again, and can see the most recent password.

Workaround for a scenario with a configuration problem with a check-in that is completed with a warning

Scenario

1. As a privileged user, James, checks out a credential for a Linux host with the self-care interface.
2. To simulate a configuration problem, as a PIM Manager, log in to the administrator console. Tamper with the Service profile for the host by changing the IP address without providing a new password. IBM Security Privileged Identity Manager cannot connect to the host.
3. As a privileged user, James, checks in the account with the self-care interface. The message `Completed with warning` is displayed.

   There is a **Check-in** event with the **Warning** status for James under **View Requests**.

   Error message displays `Missing userPwd attribute in request`.

   James can still see the credential when **View Password** is selected, and can still try to check in again.
4. As PIM Manager, in the administrator console, the credential is still checked-out to James, and the **Check-In** command for the credential is enabled.
5. When the PIM Manager clicks **Check In**, the credential remains checked-out by James.

   Under **View Requests**, there is a check-in event with status `Warning` for PIM Manager.

   You cannot clear the requests, as the requests are presumably completed, although with a warning.

Solution

1. As PIM Manager, complete the following steps:
   a. Disconnect the credential from the resource.
   b. Check in the disconnected credential.
2. In the self-care interface, James notices that the credential is checked-in, but the credential is available for check-out again.
3. James checks out the credential again, and can see the most recent password.

An authorized credential does not show in the self-care user interface checkout page

The shared access policy entitlement preview shows that a credential is included by the entitlement. But that credential does not show up in the self-care user interface checkout page to a user who is entitled to the credential. This behavior indicates that the problem is most likely caused by inappropriate credential setting.

About this task

The IBM Security Privileged Identity Manager administrative console supports the addition of user credentials into a credential vault. When you add a credential to the vault, you can apply values for each of the credential settings. Use this task to fix the credential configuration settings.

Procedure

1. From the navigation tree, select **Manage Shared Access** > **Manage Credential Vault** > **Select a Credential**.
2. On the Select a Credential page, click **Refresh** under **Credentials**.
3. Click the credential from the results to open the Change Configuration Settings page.

4. Under **Credential Settings**, verify that you selected these settings:
   - The **Require the checkin and checkout process for the shared IDs** option to specify the checkin and checkout process for the accounts.
   - The **Enable checkout search** check box to enable the credentials for a checkout search. The accounts are searched for the checkout process on the Self Service user interface.
5. Click **Submit** to save the configuration settings.

What to do next

Log on to the self-care user interface to verify that the credential is listed under **My Shared Access** > **Check out Credential**.

Enabling cut and paste within ITIM applets

Follow the guidelines to enable cut and paste in IBM Security Privileged Identity Manager applets

Procedure

1. On your client box (windows), run:
   - Windows: `C:\Program Files\JavaSoft\JRE\ <version>\bin\policytool.exe`
   - Unix/Linux: `$JAVA_HOME/bin/policytool (ex: /usr/java/jre1.7.0_67/bin/policytool)`
2. Click **Add Policy Entry**.
3. In the CodeBase field, enter: `http://hostname/-`. If directly accessing IBM Security Privileged Identity Manager on a specific port, include the port number in the URL. For example: `http://itimserver:9080/-`
4. Click **Add Permission**.
5. In the field next to **Permission**, enter: `java.awt.AWTPermission`
6. In the filed next to **Target Name**, enter: `accessClipboard`.
7. Click **Ok** to return to the Policy Entry screen.
8. Click **Done**.
9. On the Policy Tool interface, select **File** > **Save As**.
10. Save the file as:
    - For Win2000/XP: `C:\Documents and Settings\Administrator\.java.policy`
    - For Win7/8: `C:\Users\<username>\.java.policy`
    - For Unix/Linux: `$USER_HOME/ (ex: /root/.java.policy)`
11. Add `deployment.security.use.user.home.java.policy=true` to:
    - Windows: `C:\Users\<username>\AppData\LocalLow\Sun\Java\Deployment\deployment.properties`
    - Unix/Linux: `$USER_HOME/.java/deployment/deployment.properties`
12. Save `deployment.properties` and reopen the browser.

    Note:

    The steps that are provided might not work for some of the newer releases of Java 7. In this case, `accessClipboard` may have to be granted directly in the `java.policy` file (`%JAVA_HOME%\jre\lib\security\java.policy`).

If the steps that are provided do not work, the Java Plugin version might not be compatible with the applets and need to be upgraded or downgraded.

Chapter 5. Privileged Session Recorder

This section describes the solutions for potential Privileged Session Recorder problems.

Limitations with session recordings

Some limitations exist with session recordings created with the Privileged Session Recorder.

- In session recordings with IBM Personal Communications, the status-bar is not recorded.
- The Privileged Session Recorder configuration utility is available in English language only.
- The Privileged Session Recorder configuration utility cannot start when there are non-ASCII characters in the installation path.
- For Arabic locales, the Privileged Session Recorder console does not use Arabic-Indic digits and does not use the correct date and time format.
- On a monitored application, when you complete actions with modifier keys, for example Ctrl+A, the Privileged Session Recorder on the client computer logs the action as two separate events. For example: Ctrl and Ctrl+A.
- Session recordings ignore Microsoft Windows accessibility settings for StickyKeys, ToggleKeys, FilterKeys, and MouseKeys.
- Other language characters are not displayed during playback.

Log files for the Privileged Session Recorder Client

You can use the generated log files to troubleshoot or diagnose potential deployment or configuration problems. The recorder log captures processing and recording activities.

Privileged Session Recorder Client log (Recorder.log)

The IBM Privileged Session Recorder Client stores log messages in the `Recorder.log` file in `<aa_home>\logs` on the client computer. For example: `C:\Program Files\IBM\ISAM ESSO\AA\logs`.

The log level is determined by the **`LogLevel`** value on the client computer.

To configure the log level on the client computer, start the Registry Editor. Browse to the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\DeploymentOptions
```

Locate the `LogLevel` value.

Note: Increasing the log level can reduce computer performance. Reduce the log level after troubleshooting is complete.

For more information about configuring log levels on the client computer, see the IBM Security Access Manager for Enterprise Single Sign-On product documentation and search for `pid_log_level`.

SSL related messages are specified in the following format:

```
[SSL] <error-description>
```

Table 2. Known error descriptions for SSL messages in the Recorder.log file.

Error description: <error-description>	Required Log Level	Known causes or solutions
`The CA issuing the server certificate is not trusted.`	2	Ensure that the client computer trusts the signer of the SSL certificate.
`Server certificate has invalid common name (host name field).`	2	Ensure that the IBM Privileged Session Recorder Server host name can be resolved.

WinHTTP event log messages are specified in the following format:

```
[WinHTTP]<method-name> failed, err=<error-code>,desc=<error-description>
```

Table 3. Known error descriptions for WinHTTP messages in the Recorder.log file.

Error description: <error-description>	Required Log Level	Known causes or solutions
`The operation timed out.`	2	Open the **Registry Editor**, and add the following optional HTTP timeout registry entries in `HKEY_LOCAL_MACHINE\Software\IBM\SessionRecorder`. These registry values are DWORD values and specified in milliseconds. **`ResolveTimeout`** Timeout for resolving host name. (default: 5000 = 5 sec) **`ConnectTimeout`** Timeout for making connection to the server. (default: 5000 = 5 sec) **`SendTimeout`** Timeout for sending data, for example, one screen capture to the server. (default: 60000 = 1 min) **`ReceiveTimeout`** Timeout for receiving response from the server. There is no large data to download from the Privileged Session Recorder Server. (default: 10000 = 10 sec)
`The server name or address could not be resolved.`	2	Verify that there is a DNS entry for the host name or add the name to the hosts file.
`A security error occurred.`	2	See troubleshooting causes or solutions for SSL type log events.

HTTP-Status related messages are specified in the following format:

```
[HTTP-Status] Status Code: <http-status-code>, Internal: <internal-status-code>
```

Table 4. Known causes for http-status codes in the Recorder.log file.

HTTP status codes: <http-status-code>	Required Log Level	Known causes or solutions
`500`	2	Internal server error. • Verify that WebSphere® Application Server profile is running and the **`ISPIMRecorder`** application is started. • Try restarting the WebSphere Application Server profile. • Look for exceptions in the server logs.
`404`	2	Page not found. • Ensure that the Privileged Session Recorder Server URL is in the following format: `https://<hostname>/recorder/collector`. • Verify that WebSphere Application Server profile is running and the **`ISPIMRecorder`** application is started. For more information, see the IBM Security Privileged Identity Manager product documentation and search for `pid_recorder_server`.

Table 4. Known causes for http-status codes in the Recorder.log file. (continued)

HTTP status codes: <http-status-code>	Required Log Level	Known causes or solutions
401	3	Unauthorized. If this message occurs every 30 minutes, this event indicates that the Privileged Session Recorder Server is authenticating with the Privileged Session Recorder Client. If this series of messages are accompanied by the following log message: `WARNING: This is attempt <number> for authorization.` Ensure that session affinity is configured properly.

Troubleshooting uploads to the Privileged Session Recorder Server

If the IBM Privileged Session Recorder Server is unavailable, the IBM Security Privileged Identity Manager Session Recorder service on the client computer stores the session recordings. The service resumes uploads of the recordings when the server is available.

Problems

The IBM Privileged Session Recorder Server is not available or cannot be contacted.

The monitored client application is either not responding to mouse or keyboard input or the window is no longer moveable.

Session recordings from client computers are not available on the IBM Privileged Session Recorder Server.

Causes

Some possible causes:

- The network connection is disconnected.
- The IBM Privileged Session Recorder Server is not configured.
- The IBM Privileged Session Recorder Server is not available.
- The IBM Privileged Session Recorder Server host name cannot be resolved.
- The IBM Privileged Session Recorder Server certificate has not been trusted.

To determine causes, see the message logs. For more information about the types of problems and possible solutions, see “Log files for the Privileged Session Recorder Client” on page 29.

Solutions

- Check the network connection and attempt to restore the connection on the IBM Privileged Session Recorder Server.
- If you are the Administrator, ensure that the IBM Privileged Session Recorder Server is started.
- Ensure that the session recording host name and port number is configured correctly and the host can be resolved by client workstations.
- Review the session recording policies to configure the action to take on the client computer when the IBM Privileged Session Recorder Server is not available.

Troubleshooting IBM Privileged Session Recorder console display issues on Microsoft Internet Explorer 9 and 10

The IBM Privileged Session Recorder console might not display correctly when you view the console in Microsoft Internet Explorer 9 and 10 with Compatibility View mode turned on.

Problem

The IBM Privileged Session Recorder console does not display correctly when viewed in Microsoft Internet Explorer 9 and 10.

Solution

Disable the Microsoft Internet Explorer Compatibility View mode for the IBM Privileged Session Recorder console web page. For more information, go to the Microsoft website at www.microsoft.com and search for `turn off Compatibility View Internet Explorer`.

SQL0480N error with sp_export_psr_partitionset during archival

Exporting to a non-existent directory or a directory with spaces or special characters throws an error.

The error occurs when you run `sp_export_psr_partitionset` Error Message : `Unexpected error occurred : SQL0480N The procedure "SYSPROC.ADMIN_CMD " has not yet been called. SQLSTATE=51030`

Chapter 6. Application identity management

This section describes the solutions for potential Application identity management problems.

Troubleshooting a Fingerprint Matching Failure

If you are a Privileged Identity Manager administrator, check the Identity application trace log file for information about a failed fingerprint matching attempt. The log entry starts with "Fingerprint match failed".

Consider the following possible causes of fingerprint matching failures:

Incorrect application type
The application instance may be registered as a different type. For example, a Java application may have been wrongly registered as a script.

Load balancer does not forward IP address
The load balancer for IBM Security Privileged Identity Manager virtual appliance needs to be configured to forward client IP address using the X-Forwarded-For header. If this is not set correctly, network interface matching will fail.

Changed network hardware
If the network card in the application instance host computer is changed, its MAC address will change and this will cause network interface matching to fail.

Different operating system user
The user who registers the application instance may be different from the user account used to run the application. Specify the operating system user during registration using the -o or `--os-user` switch. If there are multiple user accounts that may be used to run the application, each account needs to be registered as a separate application instance.

Updated application
If "Strict" fingerprint matching policy is used, an update to the application instance binary causes the fingerprint matching to fail.

Missing group name
If you specified a group name during application instance registration, the same group name must be specified to get managed credentials. For scripts, use the `-g` or `--group-id` switch when calling get-credential. For Java applications, call `.withGroupName()` when building the AppIdManager. For data sources, specify the "group" custom property.

The host IP is also recorded. If the IP address changes, it can also invalidate the fingerprint.

Chapter 7. AccessProfiles

This section describes the solutions for potential AccessProfile problems.

Multiple AccessProfiles for the same client application

Each application signature for an AccessProfile must be unique. Single sign-on cannot occur if there are multiple AccessProfiles with the same application signature on the IMS Server.

If you have more than one AccessProfile for the same application, consider deleting or modifying copies of the AccessProfile.

Note: Duplicate AccessProfiles with signature conflicts are also logged in the AccessAgent logs as errors.

For example, a Remote Desktop Connection (RDP) AccessProfile is already on the IMS Server.

- You might already have a custom Remote Desktop Connection (RDP) AccessProfile for logging on to remote desktops.
- If you upload a new privileged identity management AccessProfile with the same application signature, single sign-on does not trigger.
- Consider the actions that you can take to resolve the issue.
  - Delete the existing AccessProfile for the RDP application from the IMS Server if the AccessProfile is not in use.
  - Merge the AccessProfiles.

Important: Privileged identity management AccessProfiles work only with AccessAgent, Version 8.2.1

Identifying AccessProfile collision

You can use the AccessStudio message pane logs to determine whether there are multiple AccessProfiles for the same client application on the IMS Server.

Before deployment, complete these steps on a test computer with the AccessAgent installed:

1. Ensure that you are logged on to AccessProfiles.
2. Import data from the IMS Server with AccessStudio.
3. Start the client application that you are testing for AccessProfile collision.
4. From the AccessStudio real-time logs, look for the phrase:
   ```
   ...multiple AccessProfiles were found.
   ```

Merging AccessProfiles

If you want both the privileged identity management AccessProfiles and the AccessProfiles you already have, then you must consider advanced AccessProfile merging.

For help with advanced AccessProfile merging, contact IBM Services.

With multiple instances of RDP check out fails

When you open several instances of RDP, the **Allow me to save credentials** check box is not automatically selected. Check out of shared access credential fails.

Workaround

Select the check box **Allow me to save credentials** and click **Connect** to successfully check out the credential.

Credential injection fails

Credential injection fails even when you start any application. At the time of injection, the application is overlaid with another application, or with the lease expiry window.

Workaround

Ensure that you place focus on the application until application logon is complete.

Prompted to save shared credentials after credential injection in a Remote Desktop Connection

When using Remote Desktop Connection, AccessAgent offers to save the shared credentials after injecting the checked out user name and password. This issue occurs after the `PIM_Profiles.eas` AccessProfile is uploaded to the IMS Server.

Workaround

Disable the **sso_site_wnd_rdp6_with_options** AccessProfile.

1. Open AccessStudio.
2. Choose **File** > **Import data from local AccessAgent**.
3. From the list of AccessProfiles, select **sso_site_wnd_rdp6_with_options**.
4. Select the **General Properties** tab.
5. Under **Signatures identifying web-page or exe where this AccessProfile is to be loaded**, click **Remove**.
6. Right-click **sso_site_wnd_rdp6_with_options**.
7. Click **Upload to IMS**.

Password injection fails for resized PuTTY window

The password injection process does not start if you resized the PuTTY window to a width that is too small.

Workaround

This situation occurs if you resize the window to 24 columns wide, or a width where the user password prompt splits into a new line, as shown in the following example:

Table 5.

Actual output	Expected output

`login as: adminaccount`
`adminaccount@192.0.2.24's passw`
`ord`
	`login as: adminaccount`
	`adminaccount@192.0.2.24's password`

The password injection process with the bundled AccessProfile cannot find a match for the word, `password`, because the keyword `password` is split into separate lines. As a result, the password is not injected.

Resize the PuTTY window so that the line for the password does not split.

Limitations

The following limitations are known with AccessProfiles.

- The bundled IBM Security Privileged Identity Manager AccessProfiles are not designed for Microsoft Remote Desktop Connection clients with versions 6.1.76xx.
- The IBM Security Privileged Identity Manager AccessProfile for Microsoft Remote Desktop Connection RDP client does not support the injection of shared credentials at the RDP lock screen.
- Check-out and check-in of shared credentials cannot work for mainframe applications that run on z/OS® and i5 series, which have the following workflow:
  1. Inject user name.
  2. Press **Tab**.
  3. Inject password.
- Multiple IBM Security Privileged Identity Manager credentials for one AccessAgent user is not supported.
- When the user does not have an IBM Security Privileged Identity Manager credential in the user Wallet and simultaneously starts two applications, such as Remote Desktop Connection and VMware vSphere Client, checking out shared credentials only works for one application where the user enters the IBM Security Privileged Identity Manager credentials when prompted by AccessAgent.
- Shared access credential check-out in RDP only works when the **General** tab is selected.

Chapter 8. Cognos reports and audit logs

You might encounter some problems or limitations when you generate reports. This section describes the known problems and suggested solutions, including the known limitations of the Privileged Identity Manager Cognos-based reports. It also includes solutions for potential audit log problems.

Report problems and their solutions

Unable to view the Cognos drill through reports in Microsoft Internet Explorer version 10

If you are using the Microsoft Internet Explorer version 10 browser, the Cognos drill through reports might not work.

Solution

Complete the following steps:

1. Enable the compatibility view.
   a. In the Microsoft Internet Explorer 10 menu, go to **Tools**.
   b. Select **Compatibility View**.
2. Add the IBM Cognos website to the trusted sites list.
3. In the Microsoft Internet Explorer 10 menu, go to **Tools** > **Internet Options**.
4. On the **Security** tab, click the **Trusted sites** icon.
5. Click **Sites**.
6. In the **Add this website to the zone** box, add the IBM Cognos website address.
7. Click **Add**.
8. Click **Close**.

Long filter values are not shown completely on the prompt pages

See the technote at http://www-01.ibm.com/support/docview.wss?uid=swg21341018 to resolve this issue. The information in the technote also applies to IBM Cognos Business Intelligence, 10.2.1 Fix Pack 1.

Generating reports is slow and causes timeouts

You might encounter slow performance or transaction time-outs during report generation for certain reports against large data sets.

To improve performance and reduce time-outs, follow these best practices:

- When you run the large reports in PDF output format, specify the appropriate filters or parameters and avoid the usage of the default filter `'Any'` that fetches all the records.
- In a large data deployment, specify the HTML output format. HTML format supports the pagination, which renders one page at a time and provides the options to move to the next pages.
- Tune the database. See the *IBM Security Privileged Identity Manager Performance Tuning Guide* at http://www-01.ibm.com/support/docview.wss?uid=swg27036205 for suggested indexes to set on columns in Report DB tables.

Known limitations

The Prompt Page Summary table in the IBM Cognos Report shows "--" as the parameter value when more than 1000 filters per prompt is selected.

IBM Cognos Reports provide the option for multiple selection. You can select more than one value for each parameter in the prompt page. When you select several values to filter the report, text overflow can occur and '--' is displayed instead in the Prompt Page Summary table.

Solution

Avoid selecting too many values for each parameter in the prompt page.

Disabled Shared Access Policy credentials are not displayed in the Shared Access Entitlement Definition Report

This report does not include shared access credentials that belong to a disabled Shared Access Policy.

Audit of the disconnected credentials in the IBM Cognos shared access history report

A user can disconnect the shared access credentials in the credential vault. After the credentials are disconnected, they do not have a connection with an account.

IBM Cognos shared access history report does not include the check-out and check-in history of the credentials that are not connected to an account. The shared access history report does not show the disconnected credentials for check-out and check-in audit action.

Cannot truncate the length of the text in the pie charts

An option or a property that truncates the length of the text is not available for the pie charts.

Languages that are not supported by the IBM Cognos Business Intelligence 10.2.1 Fix Pack 1

IBM Cognos Business Intelligence 10.2.1 Fix Pack 1 does not support the following languages:

- ar=Arabic
- iw=Hebrew

Note: The unsupported languages are not in the **Product Language** list, although they are displayed in the **Content Language** list in the Cognos configuration of IBM Cognos Business Intelligence Server.

Audit log problems and their solutions

Event number mismatch in the audit logs.

Update the AccessProfile custom audit log action if you are defining custom audit codes.

The event code changes are not reflected on the client.

Synchronize the AccessAgent computer with the IMS Server.

Earlier records show even when only the current date is specified

Records from earlier dates appear in a Cognos report when records for only the current date are required.

Workaround

If you require only the records for the current date, specify a value for both the start date and end date.

Report data synchronization utility errors and their workarounds

The following topic describes how to troubleshoot the IBM Security Privileged Identity Manager report data synchronization utility errors.

The report data synchronization utility completes the data synchronization operation successfully, but with the following exception.

The following exception might get registered into the trace file:

```
Class com.ibm.websphere.cache.DistributedMap NOT FOUND
```

It might happen because the synchronization time exceeds the cache refresh timeout interval specified by the `enrole.profile.timeout` property. This exception does not affect the success of the data synchronization. You can ignore this exception message.

Workaround:

Increase the timeout interval value for the property `enrole.profile.timeout` in the `enRole.properties` property file.

The report data synchronization utility completes with a failure with log entries and indicates that the data synchronization cannot run because data synchronization is already running.

Follow the steps to end the data synchronization operation process and rerun the data synchronization utility. For more information about how to end the data synchronization operation, see http://www.ibm.com/support/docview.wss?uid=swg21303678.

The report data synchronization utility completes with a failure with log entries and indicates that the data synchronization failed with an `OutOfMemoryError` message.

`OutOfMemoryError` can occur if the Java™ virtual machine heap is too small.

Workaround:

Increase the Java virtual machine heap size by creating an operating system environment variable:

Microsoft Windows operating systems

```
set IBM_JAVA_OPTIONS=-Xms1024m -Xmx2048m
```

UNIX or Linux operating systems

```
export IBM_JAVA_OPTIONS='-Xms1024m -Xmx2048m'
```

where:

`-Xms1024m` specifies initial heap size of 1024 mb

`-Xmx2048m` specifies maximum heap size of 2048 mb

Note: The numbers mentioned in the instructions are examples only. The exact numbers that are required might vary.

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.

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.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

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

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability
These terms and conditions are in addition to any terms of use for the IBM website.

Personal use
You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use
You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

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 http://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.

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, usage tracking, or functional purposes. These technologies can be disabled, but disabling them will also eliminate the functionality they enable.

This Software Offering does not use cookies to collect personally identifiable information. The only information that is transmitted between the server and the browser through a cookie is the session ID, which has a limited lifetime. A session ID associates the session request with information stored on the server.

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”.

Printed in USA