IBM Security Verify Identity
7.0

Privileged Identity Manager Adapter Installation and Configuration Guide

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server. The IBM Security Privileged Identity Manager Adapter enables communication between the Identity server and the IBM Security Privileged Identity Manager.

Features of the IBM Security Privileged Identity Manager Adapter

The IBM Security Privileged Identity Manager Adapter automates the management of user accounts and different service groups such as ISPIM roles, ISPIM groups, and ISPIM administrative domains.

The IBM Security Privileged Identity Manager Adapter automates the following tasks:

User account management

- Adding user accounts
- Changing user account passwords
- Modifying user account attributes
- Suspending and restoring user accounts
- Retrieving user accounts for the first time
- Deleting user accounts
- Reconciliation of modified user accounts

Service group management on the IBM Security Privileged Identity Manager server

- Adding groups
- Modifying group attributes, including adding and removing members
- Deleting groups
- Adding roles
- Modifying role attributes, including adding and removing members
- Deleting roles
- Adding and deleting administrative domain business units
- Modifying administrative domain attributes, including adding and removing administrators
- Reconciliation of other support data from the IBM Security Privileged Identity Manager server to IBM® Security Verify Identity

Related concepts

Architecture of the adapter
The adapter is pre-installed on the IBM Security Verify Identity virtual appliance.

Supported configurations
The adapter supports both single server and multiple server configurations. However, on the virtual appliance, there is only one configuration since the adapter is pre-installed.

Architecture of the adapter

The adapter is pre-installed on the IBM Security Verify Identity virtual appliance.

The adapter communicates with the IBM Security Privileged Identity Manager through the IBM Security Privileged Identity Manager REST API interface.

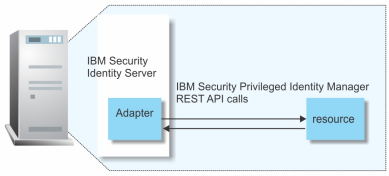

Figure 1. The architecture of the IBM Security Privileged Identity Manager Adapter

Related concepts

Features of the IBM Security Privileged Identity Manager Adapter
The IBM Security Privileged Identity Manager Adapter automates the management of user accounts and different service groups such as ISPIM roles, ISPIM groups, and ISPIM administrative domains.

Supported configurations
The adapter supports both single server and multiple server configurations. However, on the virtual appliance, there is only one configuration since the adapter is pre-installed.

Supported configurations

The adapter supports both single server and multiple server configurations. However, on the virtual appliance, there is only one configuration since the adapter is pre-installed.

There are fundamental components in each environment.

- The Identity server
- The IBM Security Privileged Identity Manager Adapter
- The managed resource

Related concepts

Features of the IBM Security Privileged Identity Manager Adapter
The IBM Security Privileged Identity Manager Adapter automates the management of user accounts and different service groups such as ISPIM roles, ISPIM groups, and ISPIM administrative domains.

Architecture of the adapter
The adapter is pre-installed on the IBM Security Verify Identity virtual appliance.

Chapter 2. Planning

The adapter comes pre-installed on the IBM Security Verify Identity appliance. You can download the appliance software package for profile updates and the latest release notes.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 7.x

Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Pre-installation

Complete these tasks.

1. Verify that your environment meets the software and hardware requirements for the adapter. See *Prerequisites*.
2. Obtain the installation software. See *Software downloads*.
3. Obtain the necessary information for the installation and configuration. See *Installation worksheet*.

Installation

Complete these tasks.

1. Install the dispatcher.
2. Install the adapter binaries or connector.
3. Install 3rd party client libraries.
4. Set up the adapter environment.
5. Restart the adapter service.
6. Import the adapter profile.
7. Create an adapter service/target.
8. Install the adapter language package.
9. Verify that the adapter is working correctly.

Upgrade

To upgrade the adapter, do a full installation of the adapter. Follow the *Installation roadmap*.

Configuration

Complete these tasks.

1. Configure secure communication between the Identity server and the adapter.
    a. Configure 1-way authentication.
    b. Configure 2-way authentication.
2. Configure secure communication between the adapter and the managed target.
    a. Configure 1-way authentication.
    b. Configure 2-way authentication.
3. Configure the adapter.
4. Modify the adapter profiles.
5. Customize the adapter.

Troubleshooting

See the following topics.

- Techniques for troubleshooting problems
- Configure debugging
- Logs
- Error messages and problem solving

Uninstallation

Complete these tasks.

1. Stop the adapter service.
2. Remove the adapter binaries or connector.
3. Remove 3rd party client libraries.
4. Delete the adapter service/target.
5. Delete the adapter profile.

Reference

See the following topics.

- Adapter attributes and object classes
- Adapter attributes by operations
- Special attributes

Related concepts

Prerequisites
The IBM Security Verify Identity appliance requires you to have system administrator authority.

Software downloads
Use your account at the IBM Passport Advantage website to get adapter profile updates and the latest release notes.

Prerequisites

The IBM Security Verify Identity appliance requires you to have system administrator authority.

See the Release Notes bundled with this adapter package for the most current information about supported versions and minimum fix pack levels.

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 7.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Software downloads
Use your account at the IBM Passport Advantage website to get adapter profile updates and the latest release notes.

Software downloads

Use your account at the IBM Passport Advantage website to get adapter profile updates and the latest release notes.

The profile is needed if there are updates to the profile that is pre-installed on the IBM Security Verify Identity appliance. You also need the profile if you want to customize it. See “Customizing the adapter profile” on page 15.

Go to IBM Passport Advantage.

See the *IBM Security Verify Identity Download Document* for instructions.

Note: You can also obtain additional adapter information from IBM Support. See https://www.ibm.com/support/pages/node/709115.

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 7.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Prerequisites
The IBM Security Verify Identity appliance requires you to have system administrator authority.

Chapter 3. Configuring

The adapter comes pre-installed on the IBM Security Verify Identity appliance. However, other tasks are involved to completely set it up.

Restarting the adapter service

The IBM Security Privileged Identity Manager Adapter runs as a shared library within the IBM Security Verify Identity application. To start, stop or restart the adapter, you must start, stop, or restart the IBM Security Verify Identity server.

Importing the adapter profile

An adapter profile defines the types of resources that the Identity server can manage. It is packaged with the IBM Security Verify Adapter. Use the adapter profile to create an adapter service on Identity server and establish communication with the adapter.

Before you begin

- You have root or administrator authority on the Identity server.
- The file to be imported must be a Java™ archive (JAR) file. The *<Adapter>*`Profile.jar` file includes all the files that are required to define the adapter schema, account form, service/target form, and profile properties. If necessary, you can extract the files from the JAR file, modify the files, and repackage the JAR file with the updated files.The JAR file for IBM Security Identity Manager is located in the top level folder of the installation package.

About this task

Service definition files are also called adapter profile files.

If the adapter profile is not installed correctly, the adapter cannot function correctly. You cannot create a service with the adapter profile or open an account on the service. You must import the adapter profile again.

Procedure

1. Log on to the Identity server by using an account that has the authority to perform administrative tasks.
2. From the navigation tree, select **Configure System** > **Manage Service Types**.
   The **Manage Service Types** page is displayed.
3. On the **Manage Service Types** page, click **Import**.
   The **Import Service Type** page is displayed.
4. On the **Import Service Type** page, complete these steps:
   a) In the **Service Definition File** field, type the directory location of the *<Adapter>*`Profile.jar` file, or click **Browse** to locate the file.
   For example, if you are installing the IBM Security Verify Adapter for a Windows server that runs Active Directory, locate and import the `ADProfileJAR` file.
   b) Click **OK** to import the file.

Results

A message indicates that you successfully submitted a request to import a service type.

What to do next

- The import occurs asynchronously, which means it might take some time for the service type to load into the Identity server from the properties files and to be available in other pages. On the **Manage Service Types** page, click **Refresh** to see the new service type. If the service type status is `Failed`, check the log files to determine why the import failed.
- If you receive a schema-related error, see the `trace.log` file for information about it. The `trace.log` file location is specified by the **`handler.file.fileDir`** property that is defined in the `enRoleLogging.properties` file. The `enRoleLogging.properties` file is in the Identity server*HOME*`\data` directory. .

Configuring the adapter as a startup service

The IBM Security Privileged Identity Manager Adapter is not enabled for the IBM Security Verify Identity virtual appliance. You must configure the adapter. The IBM Security Privileged Identity Manager Adapter creates and uses a database table. To start the adapter thread that maintains the table, configure the IBM Security Privileged Identity Manager Adapter as a startup service.

Procedure

1. Navigate to the **Configure** > **Update Property**.
2. Add the `PIMAdapterService`.
   a) Select the `enroleStartup.properties` file from the **Identity server property files** menu.
   b) Locate and select the `enrole.startup.names` property from the list of property names.
   c) Click **Edit**.
   d) Add `PIMAdapterService` at the end of the property value.
   For example

```
Scheduler,PasswordExpiration,
DataServices,PostOffice,
ReconcilerCleanup,RemotePending,
PolicyAnalysis,PasswordSynchStore,
Monitoring,WebServices,PIMAdapterService
```

   e) Click **Save Configuration**.
3. Verify that the `enroleStartup.properties` file contains the following property name and value. Otherwise, create and save this configuration.

Table 1. enroleStartup required property name and value

Field	Value
Property name	`enrole.startup.PIMAdapterService.attributes`
Property value	`class=com.ibm.itim.pim.serviceprovider.db.PIMDBManager`

4. Restart the IBM Security Verify Identity server from the dashboard server control.
   a) Click **Home**.
   b) Select **Security Identity Manager server** in the **Server Control** menu.
   c) Click **Restart**.

Enabling SSL between the adapter and the IBM Security Privileged Identity Manager server

Enable SSL to restrict the interaction with the IBM Security Privileged Identity Manager REST API server. Import the IBM Security Privileged Identity Manager server SSL signer certificate into the IBM Security Verify Identity appliance.

About this task

See the IBM Security Verify Identity appliance documentation for instructions on how to configure the SSL between the appliance and external entities.

Procedure

1. Export the certificate of the managed IBM Security Privileged Identity Manager to a file. The certificate must be DER-encoded or PEM-encoded.

   One way to do this is with a web browser. The procedure for using Internet Explorer 8 is as follows:

   a) Browse to the IBM Security Privileged Identity Manager virtual appliance using the HTTPS protocol. For example, `https://ispim.acme.com`.

      A page with the message “There is a problem with this website's security certificate.” is displayed.

   b) Click the **Continue to this website (not recommended).** link.

   c) Click the **Certificate Error** link in the address bar.

   d) Click the **View Certificates** link.

   e) Select the **Details** tab.

   f) Click the **Copy to file** button.

   g) Follow the instructions in the Certificate Export Wizard. Ensure to select **DER encoded binary X.509 (.CER)** on the **Export File Format** page.

   Note: The export procedure varies depending on the type and version of browser you are using. See your browser documentation for instructions on how to install and export a server certificate.
2. Log in to the IBM Security Verify Identity appliance as an administrator.
3. Select **Configure** > **SSL Certificate Management**.
4. Click **New**.
5. In the **Import Certificate** window, specify an alias for the certificate and browse to the file that holds the exported certificate from step 1.
6. Click **Save Configuration**.

   Note: If you get an error box with the message `System Error The network encountered a problem. Contact IBM Software Support if this issue continues to occur.`, then wait for a few seconds and click the **Save Configuration** button again.

   - You must enable SSL between the adapter and the managed resource before performing any adapter operation, including **Test Connection**.
   - After a Test Connection operation, the **Adapter version** field on the service **Status and information** page might show a version of 6.0.x.x and not match the value of the **Profile version** field, depending on the virtual appliance release. This is not an error.

Creating an adapter service/target

After you import the adapter profile on the Identity server, create a service/target so that Identity server can communicate with the managed resource.

Before you begin

Complete “Importing the adapter profile” on page 7.

About this task

You must create an administrative user account for the adapter on the managed resource. You can provide the account information such as administrator name and password when you create the adapter service. Ensure that the account has sufficient privileges to administer the users. For information about creating an administrative account, see the documentation for the managed resource.

To create or change a service, you must use the service form to provide information for the service. Service forms might vary depending on the adapter. The service name and description that you provide for each service are displayed on the console. Therefore, it is important to provide values that make sense to your users and administrators.

Procedure

1. From the navigation tree, click **Manage Services**.
   The **Select a Service** page is displayed.
2. On the **Select a Service** page, click **Create**.
   The **Create a Service** wizard is displayed.
3. On the **Select the Type of Service** page, click **Search** to locate a business unit.
   The **Business Unit** page is displayed.
4. On the **Business Unit** page, complete these steps:
   a) Type information about the business unit in the **Search information** field.
   b) Select a business type from the **Search by** list, and then click **Search**.
      A list of business units that matches the search criteria is displayed.
      If the table contains multiple pages, you can do the following tasks:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
   c) In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**.
      The **Select the Type of Service** page is displayed, and the business unit that you specified is displayed in the **Business unit** field.
5. On the **Select the Type of Service** page, select a service type, and then click **Next**.
   If the table contains multiple pages, you can do the following tasks:
   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.
6. On either the **Service Information** or **General Information** page, specify the appropriate values for the service instance.
   The content of the **General Information** page depends on the type of service that you are creating. The creation of some services might require more steps.
7. To create a service with NTLM authentication, the administrator login is in the following format:

   ```
   <Domain Name>\<Login Name>
   ```

8. For NLTM authentication, select **Authentication** mode as 'Claims-Based Authentication.

9. On the **Dispatcher Attributes** page, specify information about the dispatcher attributes, and then click **Next** or **OK**.

   The **Dispatcher Attributes** page is displayed only for IBM Security Directory Integrator based services.
10. Optional: On the **Access Information** page, select the **Define an Access** check box to activate the access definition fields. Select the type of access you want to enable.

    Specify the expected access information and any other optional information such as description, search terms, more information, or badges.
11. On the **Status and Information** page, view information about the adapter and managed resource, and then click **Next** or **Finish**.

    The adapter must be running to obtain the information.
12. On the **Configure Policy** page, select a provisioning policy option, and then click **Next** or **Finish**.

    The provisioning policy determines the ownership types available for accounts. The default provisioning policy enables only Individual ownership type accounts. Additional ownership types can be added by creating entitlements on the provisioning policy.

    Note: If you are creating a service for an identity feed, the **Configure Policy** page is not displayed.
13. Optional: On the **Reconcile Supporting Data** page, either do an immediate reconciliation for the service, or schedule a supporting data reconciliation, and then click **Finish**.

    The **Reconcile Supporting Data** page is displayed for all services except for identity feed services.

    The **supporting data only** reconciliation option retrieves only the supporting data for accounts. The supporting data includes groups that are defined on the service. The type of supporting data is defined in the adapter guide.
14. Optional: On the **Service Information** or **General Information** page, click **Test Connection** to validate that the data in the fields is correct, and then click **Next** or **Finish**.

    If the connection fails, contact the analyst who is responsible for the computer on which the managed resource runs.

Results

A message is displayed, indicating that you successfully created the service instance for a specific service type.

Service/Target form details

Complete the service/target form fields.

On the General Information tab:

Service Name
Specify a name that defines the adapter service on the Identity server.

Note: Do not use forward (/) or backward slashes (\) in the service name.

Description
(Optional) Specify a description that identifies the service for your environment.

Server URL
Specify the base URL for the IBM Security Privileged Identity Manager, `https://<PIM server host>`. By default, IBM Security Privileged Identity Manager virtual appliance restricts interaction with the IBM Security Privileged Identity Manager REST API server through the standard SSL port. See “Enabling SSL between the adapter and the IBM Security Privileged Identity Manager server” on page 9.

Owner
(Optional) Specify a user as a service owner.

Service Prerequisite
(Optional) Specify a service that is a prerequisite to this service.

On the Authentication tab:

Administrator name
Specify the name of a user with administrative privileges on the IBM Security Privileged Identity Manager server.

Password
Specify the password for the administrator.

On the Status and information tab
Contains read only information about the adapter and managed resource. These fields are examples. The actual fields vary depending on the type of adapter and how the service form is configured. The adapter must be running to obtain the information. Click **Test Connection** to populate the fields.

Last status update: Date
Specifies the most recent date when the Status and information tab was updated.

Last status update: Time
Specifies the most recent time of the date when the Status and information tab was updated.

Managed resource status
Specifies the status of the managed resource where the adapter is connected.

Managed resource version
Specifies the version of the managed resource where the adapter is connected.

Adapter version
Specifies the version of the adapter that the service uses to send requests to the managed resource.

Profile version
Specifies the version of the profile that is installed in the Identity server.

Installation platform
Specifies summary information about the operating system where the adapter is installed.

Adapter account
Specifies the account that executes the administrative commands on the managed resource.

Adapter up time: Date
Specifies the date when the adapter started.

Adapter up time: Time
Specifies the time of the date when the adapter started.

Adapter memory usage
Specifies the memory usage for running the adapter.

If the connection fails, follow the instructions in the error message. Also

- Verify the adapter log to ensure that the test request was successfully sent to the adapter.
- Verify the adapter configuration information.
- Verify the server URL, administrator name, and password parameters that are used when creating the service.
- Verify that SSL is set up correctly between the managed resource and the virtual appliance.
- Verify that the administrative user has adequate permission to contact the managed resource.
- Verify that the managed resource is running and can be reached on the network.

Installing the adapter language package

The adapters use a separate language package from IBM Security Verify Identity.

See *Installing the adapter language pack* from the IBM Security Verify Identity product documentation.

Verifying that the adapter is working correctly

After you install and configure the adapter, verify that the installation and configuration are correct.

Procedure

1. Test the connection for the service that you created on the Identity server.
2. Run a full reconciliation from the Identity server.
3. Run all supported operations such as add, modify, and delete on one user account.
4. Verify the `ibmdi.log` file after each operation to ensure that no errors are reported.
5. Verify the `trace.log` file to ensure that no errors are reported when you run an adapter operation.

Related concepts

Password management for account restoration
When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must change the adapter profile JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms by using the Form Designer or the `CustomLabels.properties` file. Each adapter has a `CustomLabels.properties` file.

Configuring property files for runtime behavior
You can change the runtime behavior of the IBM Security Verify Identity appliance by configuring the properties.

Chapter 4. Customizing

Configure the adapter to function correctly and based on your requirements or preference.

Customizing the adapter profile

To customize the adapter profile, you must change the adapter profile JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms by using the Form Designer or the `CustomLabels.properties` file. Each adapter has a `CustomLabels.properties` file.

About this task

The adapter profile JAR file is included in the adapter compressed file that you downloaded from the IBM website. The JAR file and the files that are contained in the JAR file vary depending on your operating system and the adapter.

Note: You cannot modify the schemas for this adapter. Attributes cannot be added to or deleted from the schema.

Procedure

1. Edit the profile JAR file.
   a) Log in to the system where the IBM Security Privileged Identity Manager Adapter is installed.
   b) Copy the JAR file into a temporary directory.
   c) Extract the contents of the JAR file into the temporary directory.
      Run the following command. Type the name of the JAR file for your operating system.

      ```
      #cd /tmp
      #jar -xvf PIMProfile.jar
      ```

      The **`jar`** command extracts the files into the PIMProfile directory.
   d) Edit the file that you want to change.
   e) Save the file.
2. Import the file.
   a) Create a JAR file by using the files in the `/tmp` directory
      Run the following command:

      ```
      #cd /tmp
      #jar -cvf PIMProfile.jar PIMProfile
      ```

   b) Import the JAR file into the IBM Security Verify Identity application server.
   c) Stop and start the Identity server
   d) Restart the adapter service.

Related concepts

Password management for account restoration
When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

Related tasks

Configuring property files for runtime behavior

You can change the runtime behavior of the IBM Security Verify Identity appliance by configuring the properties.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Configuring property files for runtime behavior

You can change the runtime behavior of the IBM Security Verify Identity appliance by configuring the properties.

About this task

Property	Description	Values
`com.ibm.itim.pim.serviceprovider.reconbatchsize`	Controls the number of objects that are returned in a single call to the IBM Security Privileged Identity Manager server during a reconciliation operation. The default number is 1000. For environments where there are large numbers of accounts, roles, groups, or administrative domains, returning all objects in a single call might cause network transmission errors. If that happens, set this property to some integer value. The adapter makes iterative calls to the IBM Security Privileged Identity Manager server. Each call returns the limit number of objects until all objects are retrieved.	Integer values greater than 0. Default is 1000.
`com.ibm.itim.pim.serviceprovider.dbpollinterval`	Controls the interval time before the adapter queries for results of outstanding asynchronous requests. The IBM Security Privileged Identity Manager REST API calls to add, modify, or delete accounts are asynchronous. The adapter makes an initial call and then polls the IBM Security Privileged Identity Manager server periodically to see whether the request is complete and to retrieve results. The default time interval between polling is 1 minute (60000 ms). To shorten or lengthen this interval, set the property to a value greater than or equal to 10 seconds (10000 ms).	Integer values (in millisecond) not less than 10000. Default is 60000 (one minute).

Procedure

1. Log in to the IBM Security Verify Identity appliance as an administrator.
2. Select **Configure** > **Update Property**.
3. Select the **enRole.properties** file.
4. Take any of the following action:
   - To add a property listed in the preceding table, complete the following steps:
     a. Click **New**.
     b. In the **Add property** pop-up window, enter the property name and a valid value.
     c. Click **Save Configuration**.
   - To modify a property listed in the preceding table, complete the following steps:
     a. Select the property from the list of displayed property names, and click **Edit**.
     b. In the **Update property** pop-up window, enter a new valid property value.
     c. Click **Save Configuration**.

Related concepts

Password management for account restoration
When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must change the adapter profile JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms by using the Form Designer or the `CustomLabels.properties` file. Each adapter has a `CustomLabels.properties` file.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Password management for account restoration

When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

However, in some cases you might not want to be prompted for a password. The password requirement to restore an account falls into two categories: allowed and required.

How each restore action interacts with its corresponding managed resource depends on either the managed resource, or the business processes that you implement. Certain resources reject a password when a request is made to restore an account. In this case, you can configure IBM Security Verify Identity to forego the new password requirement. You can set the adapter to require a new password if your company requires that passwords are reset when accounts are restored.

The adapter profile contains a `resource.def` file. In the `resource.def` file, you can define the option for handling password, whether it is required or not allowed on restore. When you import the adapter profile, if an option is not specified, the adapter profile importer determines the correct restoration password behavior from the `schema.dsml` file. Adapter profile components enable remote services to determine whether you discard a password that the user entered while multiple accounts on disparate resources are being restored. In this scenario, only some of the accounts that are being restored might require a password. Remote services discard the password from the restore action for those managed resources that do not require them.

Edit the `<properties>...</properties>` section of the `resource.def` file to add the new protocol options, for example:

```
<property name = "com.ibm.itim.remoteservices.ResourceProperties.
                        PASSWORD_NOT_REQUIRED_ON_RESTORE"><value>true</value>
```

```
</property>
<property name = "com.ibm.itim.remoteservices.ResourceProperties.
                        PASSWORD_NOT_ALLOWED_ON_RESTORE"><value>false</value>
</property>
```

By adding the two options in the preceding example, you are ensuring that you are not prompted for a password when an account is restored.

Note: Before you set the property **PASSWORD_NOT_REQUIRED_ON_RESTORE** to `true`, ensure that the managed resource supports restoring of an account without a password.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must change the adapter profile JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms by using the Form Designer or the `CustomLabels.properties` file. Each adapter has a `CustomLabels.properties` file.

Configuring property files for runtime behavior
You can change the runtime behavior of the IBM Security Verify Identity appliance by configuring the properties.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly

After you install and configure the adapter, verify that the installation and configuration are correct.

Procedure

1. Test the connection for the service that you created on the Identity server.
2. Run a full reconciliation from the Identity server.
3. Run all supported operations such as add, modify, and delete on one user account.
4. Verify the `ibmdi.log` file after each operation to ensure that no errors are reported.
5. Verify the `trace.log` file to ensure that no errors are reported when you run an adapter operation.

Related concepts

Password management for account restoration
When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must change the adapter profile JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms by using the Form Designer or the `CustomLabels.properties` file. Each adapter has a `CustomLabels.properties` file.

Configuring property files for runtime behavior
You can change the runtime behavior of the IBM Security Verify Identity appliance by configuring the properties.

Chapter 5. Troubleshooting

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. This topic provides information and techniques for identifying and resolving problems that are related to the adapter, including troubleshooting errors that might occur during the adapter installation.

Techniques for troubleshooting problems

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 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 you start 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 operating system, or is it common across multiple operating systems?
- Is the current environment and configuration supported?
- Do all users have the problem?
- (For multi-site 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 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 are not fully tested together.

When does the problem occur?

Develop a detailed timeline of events that lead 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 use 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 done?
- Is a certain sequence of events required 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 occur 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. 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?
- Do multiple users or applications have the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

Server tracing

The trace output for the IBM Security Privileged Identity Manager Adapter is controlled by the `logger.trace.com.ibm.itim.pim.level` property.

The following properties values are the defaults:

`logger.trace.level=DEBUG_MIN`
Specifies the trace log level.

`DEBUG_MIN`
Records the least amount of information. (Default)

DEBUG_MID
Records a greater amount of trace information for debugging.

DEBUG_MAX
Records the maximum amount of trace information. This level has the greatest impact on server performance. Use this level only to narrow down a problem to a specific component. Then, reset this parameter back to DEBUG_MIN or DEBUG_MID.

logger.trace.com.ibm.itim.component_name
Defines the IBM Security Verify Identity component that you want to trace.

Specifying trace contents

The trace output for the IBM Security Privileged Identity Manager Adapter is controlled by the logger.trace.com.ibm.itim.pim.level property.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Manage** > **Maintenance** > **Log Retrieval and Configuration**.

   The **Log Retrieval and Configuration** page consists of two tabs.

   - **Appliance**
   - **Identity**

   To work with these tabs, see "Retrieving logs" on page 22.
2. On the **Log Retrieval and Configuration** page, do one of these actions.

   - Click **Appliance** to open the **Appliance** tab.
   - Click **Identity** to open the **Identity** tab.

   For example, click **Appliance**.
3. Click **Configure** to display the **Log Roll Over Configuration** window.
4. Click **Configure**.
   The **Logging Configuration** window consists of these tabs.

   General
   This tab contains information about log rollover settings, such as maximum log file rotation size and maximum number of historical log files.

   Provide the following details:

   Maximum size for log file rotation
   The maximum size in megabytes of the log file.

   Maximum number of historical log files
   The maximum number of historical log files.

   To edit the existing log details, specify new values.

   Identity Manager
   This tab contains information about identity-specific logging details, such as date format, time format, package, and trace levels.

   Provide the following details:

   Date Format
   Specify a format for that date that you want to assign for the logs.

   Time Format
   Specify a format for the time that you want to assign for the logs.

   New
   Do these steps:

a. Click **New** to add a package name.

b. In the **Package Name** column, select a package name from the list and assign it to the Identity log.

c. In the **Trace Level** column, select a trace level from the list and assign it to the Identity log.

Delete
Select a record and click **Delete**.

To edit an existing package name, you can take any of the following actions.

a. Select another package name from the list.

b. Select another trace level from the list.

5. Provide the following details:

Maximum size for log file rotation
The size of the log file in megabytes that you want to assign. For example, specify 2.

Maximum number of historical log files
The maximum number of historical log files that you want to assign. For example, specify 101.

6. Click **Save Configuration**.

Note: Depending on the changes that you made on any of these tabs, a message indicates to restart the server in the **Notifications** widget.

Retrieving logs

Use the **Log Retrieval and Configuration** page to view, save, or clear the log files. You can also use the page to configure the server log settings for the virtual appliance.

About this task

See Table 2 on page 22 for a list of available logs, which can help you to diagnose or troubleshoot the logs from the **Log Retrieval and Configuration** page.

Table 2. Available logs to help you diagnose or troubleshoot

Tab	Tab description	Log file name	Log file name description
Appliance	The files debug any configuration failures that occur in the virtual appliance.	Identity data store configuration	It is the Identity data store configuration log file.
		Directory server information	It is the Tivoli® Directory Server user registry configuration log file.
		Server System out	It is the Appliance system output log file.
		Server Message	It is the Appliance server message log file.

Table 2. Available logs to help you diagnose or troubleshoot (continued)			
Tab	**Tab description**	**Log file name**	**Log file name description**
Identity	Identifies issues in the Identity applications.	Cluster manager system out and Cluster manager system error	They are the Cluster manager system out and system error log files.
		Application server system out and Application server system error	They are the Identity Application server system out and system error log files.
		Message server system out and Message server system error	They are the Identity Message server system out and system error log files.
		Application message	It is the Identity virtual appliance message log file.
		Application trace	It is the Identity virtual appliance trace log file.
		Application access	It is the Identity virtual appliance access log file.
	Identifies issues in the cluster manager of the Identity virtual appliance.	Cluster manager system out and Cluster manager system error	They are the Identity cluster manager system out and system error log files.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Manage** > **Maintenance** > **Log Retrieval and Configuration**.
2. On the **Log Retrieval and Configuration** page, do one of the following actions.
   - Click **Appliance** to open the **Appliance** tab.
   - Click **Identity** to open the **Identity** tab.
3. From the **Log Retrieval and Configuration** table of the **Appliance** tab, select a log file.
   For more information about the **Appliance** and the **Identity** log files, see Table 2 on page 22.
4. Do one of the following actions:
   - Click **View** to display the contents of the selected log file in the **Log file** field of the **Log Content** window.
   - Click **Download** to save or download a copy of the log file.
   - Click **Clear** and confirm the action to remove the contents from the selected log file.
   - Click **Refresh** to display the most recent version of the log files, including changes that were made to the data since it was last refreshed.

Known adapter issues

Learn about the known adapter issues.

IBM Security Privileged Identity Manager requests hang

If a IBM Security Privileged Identity Manager service request seems to hang in pending state, there are different actions that you can take:

- Continue to wait for the IBM Security Privileged Identity Manager server to complete the request.

- Cancel the request from the IBM Security Privileged Identity Manager server.
- Cancel the request by using the IBM Security Verify Identity admin console.

If you choose the first two options, there are no additional actions needed. If you choose the last option, there are manual cleanup steps that you might need to perform, depending on the type of operation canceled.

The operations that require manual cleanup are as follows:

- account add
- account modify (including adding an account user as a role member or a group member, or adding an account user as a domain administrator)
- account delete
- account suspend
- account restore
- change account password

The preceding operations are asynchronous - the IBM Security Privileged Identity Manager adapter makes an initial request to the IBM Security Privileged Identity Manager server. The IBM Security Privileged Identity Manager adapter then polls periodically for status until the IBM Security Privileged Identity Manager server responds that the request is complete. The IBM Security Privileged Identity Manager adapter maintains a database table that is named PIM_ASYNC_REQUESTS to manage asynchronous requests. Each row of the table contains information about one request, including the IBM Security Verify Identity request ID in column ISIM_REQID.

If you use IBM Security Verify Identity to cancel a request of one of the preceding types, you must note the IBM Security Verify Identity request ID. Use the administrative tool of your choice to access the IBM Security Verify Identity database and look up the entry that has the IBM Security Verify Identity request ID in the PIM_ASYNC_REQUESTS table. Delete the entry and commit the change. Then, restart the IBM Security Verify Identity server so that the IBM Security Privileged Identity Manager adapter reads the database table again and will not poll for that request's status.

If the IBM Security Privileged Identity Manager server completes the request and responds after you cancel the operation but before you clean up the database table, the request entry will already have been removed from the table and no further action is needed.

Chapter 6. Uninstalling

To remove an adapter from the Identity server for any reason, you must remove all the components that were added during installation. The adapter runtime is built into the IBM Security Verify Identity virtual appliance. Uninstalling the adapter involves disabling the adapter and removing the adapter profile.

Disabling the adapter

Disabling the adapter is a multitask process.

Procedure

1. Remove the service definition.
   a) Delete any existing IBM Security Privileged Identity Manager services.
   b) Uninstall the service definition.
2. Remove the adapter configuration items.
   a. Remove or restore the values of any adapter runtime properties that you added or set, including logging properties.
      - To remove an added property, complete the following steps:
        i) Log in to the IBM Security Verify appliance as an administrator.
        ii) Click **Configure** > **Update Property**.
        iii) Select the appropriate properties file.
        iv) Click the **Modified properties** tab.
        v) Select the property that you want to remove and click **Delete**.
        vi) In the **Confirm delete** pop-up window, click **Yes**.
      - To restore the value of a modified property, complete the following steps:
        i) Log in to the IBM Security Verify appliance as an administrator.
        ii) Click **Configure** > **Update Property**.
        iii) Select the appropriate properties file.
        iv) Select the property from the list of displayed property names and click **Edit**.
        v) In the **Update Property** pop-up window, enter the original property value.
        vi) Click **Save Configuration**.
   b. Remove the **PIMAdapterService** from the startup services.
      i) Log in to the IBM Security Verify appliance as an administrator.
      ii) Click **Configure** > **Update Property**.
      iii) Select the **enRoleStartup.properties** file.
      iv) Select the **enrole.startup.names** property and click **Edit**.
      v) In the **Update Property** pop-up window, remove **PIMAdapterService** from the property value.
      vi) Click **Save Configuration**.
   c. Remove the adapter database tables and indexes from the database. Manually remove the database tables that the IBM Security Privileged Identity Manager Adapter created. Use the administrative interface for the IBM Security Verify Identity database to delete the following table and indexes:
      - `PIM_ASYNC_REQUESTS` table in the `ENROLE_DATA` table space
      - `PIM_ASYNCREQS_REQTIME_X` index

- PIM_ASYNCREQS_ISIMID_X index

Removing the adapter profile

Before you remove the adapter profile, ensure that no objects exist on your IBM Security Verify Identity server that reference the adapter profile.

The following are examples of objects on the IBM Security Verify Identity server that can reference the adapter profile.

- Adapter service instances
- Policies referencing an adapter instance or the profile
- Accounts

For specific information about removing the adapter profile, see the IBM Security Verify Identity product documentation.

Chapter 7. Reference

Reference information is organized to help you locate particular facts quickly, such as adapter attributes, registry settings, and environment variables.

Adapter attributes

The IBM Security Verify Identity server communicates with the adapter by using attributes that are sent from the IBM Security Verify Identity user console to the adapter shared library.

The combination of attributes, depends on the type of action that the IBM Security Verify Identity server requests from the adapter.

erPIMService object class

Table 3. Attributes, descriptions, data types, and permissions

Attribute	Description	Data Type	Single-valued?	Permissions	Required
erServiceName	The display name of the service	String	Yes	RW	Yes
description	The service description	String	Yes	RW	No
erURL	The URL to the IBM Security Privileged Identity Manager server	String	Yes	RW	Yes
erServiceUid	The IBM Security Privileged Identity Manager administrative user's name	String	Yes	RW	Yes
erPassword	The IBM Security Privileged Identity Manager administrative user's password	Binary	Yes	RW	Yes
erAdapterLast StatusTime*	The date and time of the last status response	String	Yes	R	No
erAdapterResourc e Status*	The managed resource status	String	Yes	R	No
erAdapterResourc e StatusMsg*	A status message returned from the managed resource	String	Yes	R	No
erAdapterResourc e Version*	The managed resource version	String	Yes	R	No
erAdapterVersion *	The adapter version	String	Yes	R	No
erAdapterProfile Version*	The adapter profile version	String	Yes	R	No
erAdapter Platform*	The adapter installation platform	String	Yes	R	No

Table 3. Attributes, descriptions, data types, and permissions (continued)					
Attribute	**Description**	**Data Type**	**Single-valued?**	**Permissions**	**Required**
erAdapterAccount*	The administrative user account that the adapter runs as	String	Yes	R	No
erAdapterUpTime*	The date and time the adapter was last started	String	Yes	R	No
erAdapterMemory*	Adapter memory usage	String	No	R	No

Note: * - These attributes are applicable to adapters running on IBM Security Verify Identity 6.0 or later only.

erPIMAccount object class

Table 4. Attributes, descriptions, data types, and permissions					
Attribute	**Description**	**Data Type**	**Single-valued?**	**Permissions**	**Required**
erPIMParent BusinessUnit	The business unit under which the user account is defined	String	Yes	AR	Yes
erUid	A unique identifier for the user with respect to the ISIM service	String	Yes	RW	Yes
erPIMChange Password	Indicates whether the PIM user must change his password at next logon	Boolean	Yes	RW	No
erPIMLastName	The user's last name	String	Yes	RW	Yes
erPIMFullName	The user's full name	String	Yes	RW	Yes
erPIMFirstName	The user's first name	String	Yes	RW	No
erPIMInitials	The user's initials	String	Yes	RW	No
erPIMHomeAddress	The user's home address	String	Yes	RW	No
erPIMSharedSecret	A token used for password pickup	String	Yes	RW	No
erPIMOrgRoles	The roles that the user is a member of	String	No	RW	No
erPIMOfficeNumber	The user's office number	String	Yes	RW	No
erPIMEmployee Number	The user's employee number	String	Yes	RW	No
erPIMTitle	The user's personal title	String	Yes	RW	No
erPIMManager	The user's manager	String	Yes	RW	No
erPIMPostal Address	The user's mailing address	String	Yes	RW	No

Table 4. Attributes, descriptions, data types, and permissions (continued)					
Attribute	**Description**	**Data Type**	**Single-valued?**	**Permissions**	**Required**
erPIMAdmin Assistant	The user's administrative assistant	String	Yes	RW	No
erPIMEmailAddres s	The user's email address	String	Yes	RW	No
erPIMPhoneNumber	The user's preferred phone number	String in telephone number syntax	Yes	RW	No
erPIMMobileNumbe r	The user's mobile or cellular phone number	String in telephone number syntax	Yes	RW	No
erPIMPager	The user's pager number	String in telephone number syntax	Yes	RW	No
erPIMHomePhone Number	The user's home phone number	String in telephone number syntax	Yes	RW	No
erPIMGroups	The system groups to which the user belongs	String	No	RW	No
erPIMAdminDomain s	The domains the user administers	String	No	RW	No
erAccountStatus	Indicates whether the user account is active (0) or inactive (1)	Integer	Yes	R	No
erPassword	The user's password	Binary	Yes	RW	No
erPIMGlobalID	The unique identifier for the user account on the IBM Security Privileged Identity Manager server	String	Yes	R	No

erPIMRole object class

Table 5. Attributes, descriptions, data types, and permissions					
Attribute	**Description**	**Data Type**	**Single-valued?**	**Permissions**	**Required**
erPIMFullNam e	The fully-qualified role name, including its organizational hierarchy	String	Yes	R	No
erPIMName	The simple role name which does not include its organizational hierarchy	String	Yes	RW	Yes
description	The role description	String	Yes	RW	No

Table 5. Attributes, descriptions, data types, and permissions (continued)

Attribute	Description	Data Type	Single-valued?	Permissions	Required
erPIMRoleType	The type of role. Currently, only static roles are supported.	String	Yes	R	No
erPIMRole Classification	The role classification	String	Yes	R	No
erPIMParent BusinessUnit	The business unit under which the role is defined	String	Yes	AR	Yes
erPIMRoleRole Owners	The role's role owners	String	No	RW	No
erPIMRoleUser Owners	The role's user owners	String	No	RW	No
erPIMRoleAccess Option	The role's access option: disabled (“0”), enabled but not shown as common access (“1”), or enabled and shown as common access (“2”)	String	Yes	RW	No
erPIMRoleAccess Type	The role's access type	String	Yes	RW	No
erPIMRoleSystem Groups	The groups that are associated with the role	String	No	RW	No
erPIMRolePIM Work flow	The identifier for the PIM workflow that is associated with the role	String	Yes	R	No
erPIMGlobalID	The unique identifier for the role on the IBM Security Privileged Identity Manager server	String	Yes	R	No

erPIMGroup object class

Table 6. Attributes, descriptions, data types, and permissions

Attribute	Description	Data Type	Single-valued?	Permissions	Required
erPIMFullName	The fully-qualified group name, including its organizational hierarchy	String	Yes	R	No
erPIMName	The simple group name which does not include its organizational hierarchy	String	Yes	AR	Yes
description	The group description	String	Yes	RW	No
erPIMParentBusinessUnit	The business unit under which the group is defined	String	Yes	AR	Yes
erPIMGroupView	View that users in the group can see	String	Yes	RW	No
erPIMGlobalID	The unique identifier for the group on the IBM Security Privileged Identity Manager server	String	Yes	R	No

erPIMDomain object class

Table 7. Attributes, descriptions, data types, and permissions

Attribute	Description	Data Type	Single-valued?	Permissions	Required
erPIMFullName	The fully-qualified administrative domain name, including its organizational hierarchy	String	Yes	R	No

Table 7. Attributes, descriptions, data types, and permissions (continued)					
Attribute	**Description**	**Data Type**	**Single-valued?**	**Permissions**	**Required**
erPIMName	The simple administrative domain name which does not include its organizational hierarchy	String	Yes	RW	Yes
description	The administrative domain description	String	Yes	RW	No
erPIMParent BusinessUnit	The business unit under which the administrative domain is defined	String	Yes	AR	Yes
erPIMGlobalID	The unique identifier for the administrative domain on the IBM Security Privileged Identity Manager server	String	Yes	R	No

erPIMBusinessUnit object class

Table 8. Attributes, descriptions, data types, and permissions				
Attribute	**Description**	**Data Type**	**Single-valued?**	**Required**
erPIMFullName	The fully-qualified business unit name, including its organizational hierarchy	String	Yes	No
erPIMName	The simple business unit name which does not include its organizational hierarchy	String	Yes	Yes
description	The business unit description	String	Yes	No

Table 8. Attributes, descriptions, data types, and permissions (continued)				
Attribute	**Description**	**Data Type**	**Single-valued?**	**Required**
erPIMParentBusiness Unit	The business unit under which this business unit is defined	String	Yes	Yes
erPIMGlobalID	The unique identifier for the business unit on the IBM Security Privileged Identity Manager server	String	Yes	No

erPIMAccessType object class

Table 9. Attributes, descriptions, data types, and permissions				
Attribute	**Description**	**Data Type**	**Single-valued?**	**Required**
erPIMName	The access type display name	String	Yes	Yes
erPIMGlobalID	The unique identifier for the access type on the IBM Security Privileged Identity Manager server	String	Yes	Yes

erPIMGroupView object class

Table 10. Attributes, descriptions, data types, and permissions				
Attribute	**Description**	**Data Type**	**Single-valued?**	**Required**
erPIMName	The group view display name	String	Yes	Yes
erPIMGlobalID	The unique identifier for the group view on the IBM Security Privileged Identity Manager server	String	Yes	Yes

erPIMRoleClassification object class

Table 11. Attributes, descriptions, data types, and permissions				
Attribute	**Description**	**Data Type**	**Single-valued?**	**Required**
erPIMName	The role classification display name	String	Yes	Yes

Table 11. Attributes, descriptions, data types, and permissions (continued)				
Attribute	**Description**	**Data Type**	**Single-valued?**	**Required**
erPIMGlobalID	The unique identifier for the role classification on the IBM Security Privileged Identity Manager server	String	Yes	Yes

Attributes by IBM Security Privileged Identity Manager Adapter actions

Typical adapter actions can be listed by their functional transaction group.

The following lists include more information about required and optional attributes that are sent to the adapter to complete that action.

System Login Add

A System Login Add is a request to create a user account with the specified attributes.

Table 12. Add request attributes	
Required attribute	**Optional attribute**
erPIMParentBusinessUnit erUid erPIMLastName erPIMFullName	erPIMChangePassword erPIMFirstName erPIMInitials erPIMHomeAddress erPIMSharedSecret erPIMOrgRoles erPIMOfficeNumber erPIMEmployeeNumber erPIMTitle erPIMManager erPIMPostalAddress erPIMAdminAssistant erPIMEmailAddress erPIMPhoneNumber erPIMMobileNumber erPIMPager erPIMHomePhoneNumber erPIMGroups erPIMAdminDomains erAccountStatus erPassword

Related concepts

System Login Change
A System Login Change is a request to change one or more attributes for the specified user.

System Login Delete
A System Login Delete is a request to remove the specified user from the managed resource.

System Login Suspend
A System Login Suspend is a request to disable a user account. The user is not removed and the account attributes are not modified.

System Login Restore
A System Login Restore is a request to activate a user account that was previously suspended. After an account is restored, the user can access the system with the same attributes as the ones before the Suspend function was called.

System Login Reconcile
The Reconciliation request synchronizes user account information between IBM Security Verify Identity and the managed resource.

System Login Group Modify
Group change is a request to modify group attributes for an ISPIM role, ISPIM group, or ISPIM administrative domain with the specified attribute.

System Login Group Delete
Group delete is a request to delete an ISPIM role, ISPIM group, or ISPIM administrative domain with the specified attribute.

System Login Change

A System Login Change is a request to change one or more attributes for the specified user.

Table 13. Change request attributes

Required attribute	Optional attribute
erUid	Any supported account attribute except those with Read only (R) permission. See "Adapter attributes" on page 27.

Related concepts

System Login Add
A System Login Add is a request to create a user account with the specified attributes.

System Login Delete
A System Login Delete is a request to remove the specified user from the managed resource.

System Login Suspend
A System Login Suspend is a request to disable a user account. The user is not removed and the account attributes are not modified.

System Login Restore
A System Login Restore is a request to activate a user account that was previously suspended. After an account is restored, the user can access the system with the same attributes as the ones before the Suspend function was called.

System Login Reconcile
The Reconciliation request synchronizes user account information between IBM Security Verify Identity and the managed resource.

System Login Group Modify
Group change is a request to modify group attributes for an ISPIM role, ISPIM group, or ISPIM administrative domain with the specified attribute.

System Login Group Delete

Group delete is a request to delete an ISPIM role, ISPIM group, or ISPIM administrative domain with the specified attribute.

System Login Delete

A System Login Delete is a request to remove the specified user from the managed resource.

Table 14. Delete request attributes	
Required attribute	**Optional attribute**
erUid	None

Related concepts

System Login Add
A System Login Add is a request to create a user account with the specified attributes.

System Login Change
A System Login Change is a request to change one or more attributes for the specified user.

System Login Suspend
A System Login Suspend is a request to disable a user account. The user is not removed and the account attributes are not modified.

System Login Restore
A System Login Restore is a request to activate a user account that was previously suspended. After an account is restored, the user can access the system with the same attributes as the ones before the Suspend function was called.

System Login Reconcile
The Reconciliation request synchronizes user account information between IBM Security Verify Identity and the managed resource.

System Login Group Modify
Group change is a request to modify group attributes for an ISPIM role, ISPIM group, or ISPIM administrative domain with the specified attribute.

System Login Group Delete
Group delete is a request to delete an ISPIM role, ISPIM group, or ISPIM administrative domain with the specified attribute.

System Login Suspend

A System Login Suspend is a request to disable a user account. The user is not removed and the account attributes are not modified.

Table 15. Suspend request attributes	
Required attribute	**Optional attribute**
erUid erAccountStatus	None

Related concepts

System Login Add
A System Login Add is a request to create a user account with the specified attributes.

System Login Change
A System Login Change is a request to change one or more attributes for the specified user.

System Login Delete
A System Login Delete is a request to remove the specified user from the managed resource.

System Login Restore

A System Login Restore is a request to activate a user account that was previously suspended. After an account is restored, the user can access the system with the same attributes as the ones before the Suspend function was called.

System Login Reconcile
The Reconciliation request synchronizes user account information between IBM Security Verify Identity and the managed resource.

System Login Group Modify
Group change is a request to modify group attributes for an ISPIM role, ISPIM group, or ISPIM administrative domain with the specified attribute.

System Login Group Delete
Group delete is a request to delete an ISPIM role, ISPIM group, or ISPIM administrative domain with the specified attribute.

System Login Restore

A System Login Restore is a request to activate a user account that was previously suspended. After an account is restored, the user can access the system with the same attributes as the ones before the Suspend function was called.

Table 16. Restore request attributes

Required attribute	**Optional attribute**
erUid erAccountStatus	erPassword

Related concepts

System Login Add
A System Login Add is a request to create a user account with the specified attributes.

System Login Change
A System Login Change is a request to change one or more attributes for the specified user.

System Login Delete
A System Login Delete is a request to remove the specified user from the managed resource.

System Login Suspend
A System Login Suspend is a request to disable a user account. The user is not removed and the account attributes are not modified.

System Login Reconcile
The Reconciliation request synchronizes user account information between IBM Security Verify Identity and the managed resource.

System Login Group Modify
Group change is a request to modify group attributes for an ISPIM role, ISPIM group, or ISPIM administrative domain with the specified attribute.

System Login Group Delete

Group delete is a request to delete an ISPIM role, ISPIM group, or ISPIM administrative domain with the specified attribute.

System Login Reconcile

The Reconciliation request synchronizes user account information between IBM Security Verify Identity and the managed resource.

Table 17. Reconciliation request attributes

Required attribute	Optional attribute
None	None. All supported attributes are returned.

Related concepts

System Login Add
A System Login Add is a request to create a user account with the specified attributes.

System Login Change
A System Login Change is a request to change one or more attributes for the specified user.

System Login Delete
A System Login Delete is a request to remove the specified user from the managed resource.

System Login Suspend
A System Login Suspend is a request to disable a user account. The user is not removed and the account attributes are not modified.

System Login Restore
A System Login Restore is a request to activate a user account that was previously suspended. After an account is restored, the user can access the system with the same attributes as the ones before the Suspend function was called.

System Login Group Modify
Group change is a request to modify group attributes for an ISPIM role, ISPIM group, or ISPIM administrative domain with the specified attribute.

System Login Group Delete
Group delete is a request to delete an ISPIM role, ISPIM group, or ISPIM administrative domain with the specified attribute.

System Login Group Modify

Group change is a request to modify group attributes for an ISPIM role, ISPIM group, or ISPIM administrative domain with the specified attribute.

Table 18. Group change request attribute

Required attribute	Optional attribute
erPIMGlobalId	Any supported role attribute except those attributes with Read only (R) permission. See “Adapter attributes” on page 27.

Related concepts

System Login Add
A System Login Add is a request to create a user account with the specified attributes.

System Login Change
A System Login Change is a request to change one or more attributes for the specified user.

System Login Delete

A System Login Delete is a request to remove the specified user from the managed resource.

System Login Suspend
A System Login Suspend is a request to disable a user account. The user is not removed and the account attributes are not modified.

System Login Restore
A System Login Restore is a request to activate a user account that was previously suspended. After an account is restored, the user can access the system with the same attributes as the ones before the Suspend function was called.

System Login Reconcile
The Reconciliation request synchronizes user account information between IBM Security Verify Identity and the managed resource.

System Login Group Delete
Group delete is a request to delete an ISPIM role, ISPIM group, or ISPIM administrative domain with the specified attribute.

System Login Group Delete

Group delete is a request to delete an ISPIM role, ISPIM group, or ISPIM administrative domain with the specified attribute.

Table 19. Group delete request attribute

Required attribute	**Optional attribute**
erPIMGlobalId	None

Related concepts

System Login Add
A System Login Add is a request to create a user account with the specified attributes.

System Login Change
A System Login Change is a request to change one or more attributes for the specified user.

System Login Delete
A System Login Delete is a request to remove the specified user from the managed resource.

System Login Suspend
A System Login Suspend is a request to disable a user account. The user is not removed and the account attributes are not modified.

System Login Restore
A System Login Restore is a request to activate a user account that was previously suspended. After an account is restored, the user can access the system with the same attributes as the ones before the Suspend function was called.

System Login Reconcile
The Reconciliation request synchronizes user account information between IBM Security Verify Identity and the managed resource.

System Login Group Modify
Group change is a request to modify group attributes for an ISPIM role, ISPIM group, or ISPIM administrative domain with the specified attribute.

Index

S

T

U

V