IBM Security Verify Identity
7.0

SoftLayer 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 SoftLayer Adapter uses the Security Directory Integrator functions to facilitate communication between the Identity server and SoftLayer.

Adapters can be installed on the managed resource. The Identity server manages access to the resource by using the security system. Adapters function as trusted virtual administrators on the target operating system. The adapter creates, suspends, restores user accounts, and other functions that administrators run manually. The adapter runs as a service, independently of whether you are logged on to the Identity server.

Features of the adapter

The adapter automates several administrative and management tasks.

You can use the adapter to automate the following tasks:

- Create, modify, suspend, restore, change password, and delete a user.
- Reconcile user and user attributes.

Architecture of the adapter

Several components are involved in running and using the adapter. Install all these components so that the adapter can function correctly.

The adapter requires the following components:

- The Dispatcher
- The IBM Security Directory Integrator connector
- The IBM® Security Verify Adapter profile

You must install the Dispatcher and the adapter profile; however, the Security Directory Integrator connector might already be installed with the base Security Directory Integrator product.

The SoftLayer Adapter consists of IBM Security Directory Integrator Assembly Lines. When an initial request is made by IBM Security Verify Identity to the SoftLayer Adapter, the assembly lines are loaded into the Security Directory Integrator server. Subsequent service requests do not require those same assembly lines to be reloaded.

The assembly lines use the Security Directory Integrator components to undertake user management-related tasks on the SoftLayer domain. They perform these tasks remotely by using the ID and API key of a master account.

The following diagram shows the various components that work together to complete user management tasks in a Security Directory Integrator environment.

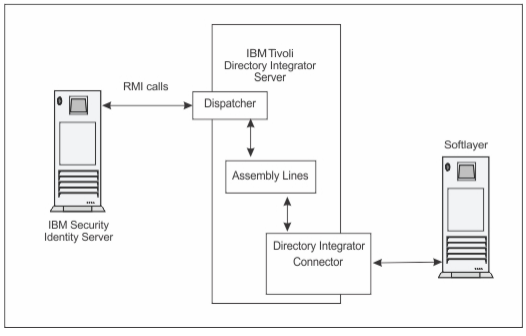

Figure 1. The architecture of the SoftLayer Adapter

Supported configurations

The adapter supports both single and multiple server configurations.

The following components are the fundamental components of a SoftLayer Adapter environment:

- An Identity server
- An IBM Security Directory Integrator server
- The SoftLayer Adapter

As part of each configuration, the SoftLayer Adapter must be installed on the computer that is running the IBM Security Directory Integrator server.

For a single server configuration, you must install the Identity server, IBM Security Directory Integrator server, and the SoftLayer Adapter on one server. That server communicates with the SoftLayer server.

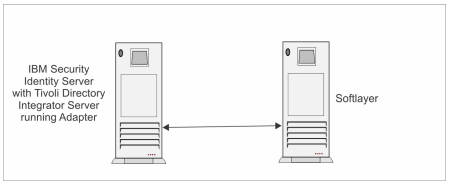

Figure 2. Single server configuration

Chapter 2. Planning

Installing and configuring the adapter involves several steps that you must complete in a specific sequence. Follow the roadmap for the main tasks.

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

Prerequisites

Verify that your environment meets the software and hardware requirements for the adapter.

The following table identifies the software and operating system prerequisites for the adapter installation.

Ensure that you install the adapter on the same workstation as the Security Directory Integrator server.

Table 1. Prerequisites to install the adapter

Prerequisite	Description
Operating system	The SoftLayer Adapter can be used on any operating system that is supported by Security Directory Integrator.
Network Connectivity	Internet Protocol network
System Administrator authority	To complete the adapter installation procedure, you must have system administrator authority.

Table 1. Prerequisites to install the adapter (continued)	
Prerequisite	**Description**
Directory Integrator	• IBM Security Directory Integrator Version 7.1.1 + 7.1.1-TIV-TDI-FP0004 + 7.2.0-ISS-SDI-LA0008 • IBM Security Directory Integrator Version 7.2 + FP0002 + 7.2.0-ISS-SDI-LA0008 **Note:** • Earlier versions of IBM Security Directory Integrator that are still supported might function properly. However, to resolve any communication errors, you must upgrade your Directory Integrator release to the versions that the adapter officially supports. • The adapter supports IBM Security Directory Integrator 7.2, which is available only to customers who have the correct entitlement. Contact your IBM representative to find out whether you have the entitlement to download IBM Security Directory Integrator 7.2.
Identity server	The following servers are supported: • Identity server Version 10.0 • Identity server Version 10.0 • IBM Security Privileged Identity Manager Version 2.0 • Identity server Version 10.0
Dispatcher	Obtain the dispatcher installer from the IBM Passport Advantage website.
Security Directory Integrator adapters solution directory	A Security Directory Integrator adapters solution directory is a Security Directory Integrator work directory for adapters. For more information, see the *Dispatcher Installation and Configuration Guide*.

For information about the prerequisites and supported operating systems for Security Directory Integrator, see the *IBM Security Directory Integrator 7.1.1: Administrator Guide*.

Software downloads

Download the software through your account at the IBM Passport Advantage® website.

Go to IBM Passport Advantage.

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

Note:

You can also obtain additional adapter information from IBM Support.

Installation worksheet

The installation worksheet lists the information that is required to install and configure the adapter. Complete this worksheet before you start the installation procedure for ease of reference. Make a copy of the worksheet for each adapter instance you install.

Table 2. Required information to install the adapter

Required information	Description	Value
Administrator account ID and password	An administrator account ID and password on the managed resource that has administrative rights for running the SoftLayer Adapter.	
Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the jars/connectors subdirectory that contains adapter JAR files. For example, the `jars/connectors` subdirectory contains the JAR file for the UNIX adapter.	If Security Directory Integrator is automatically installed with your IBM Security Verify Identity product, the default directory path for Security Directory Integrator is as follows: Windows: • for version 7.1.1: *drive*`\Program Files\IBM\TDI\V7.1.1` UNIX: • for version 7.1.1: `/opt/IBM/TDI/7.1.1`
Adapters solution directory	When you install the dispatcher, the installer prompts you to specify a file path for the solution directory. For more information about the solution directory, see the *Dispatcher Installation and Configuration Guide*.	The default solution directory is at: Windows: • for version 7.1.1: *drive*`\Program Files\IBM\TDI\7.1.1\`*timsol* UNIX: • for version 7.1.1: `/opt/IBM/TDI/V7.1.1/`*timsol*

Chapter 3. Installing

Installing the adapter mainly involves importing the adapter profile and creating an adapter service. Depending on the adapter, several other tasks can be involved to completely install it.

All IBM Security Directory Integrator based adapters require the Dispatcher for the adapters to function correctly. If the Dispatcher is installed from a previous installation, do not reinstall it unless the Dispatcher is upgraded. See Installing the dispatcher.

Depending on your adapter, the Security Directory Integrator connector might already be installed as part of the Security Directory Integrator product and no further action is required. If the connector is not pre-installed, install it after the Dispatcher.

Installing the dispatcher

If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

If you already installed the RMI Dispatcher for another adapter, you do not need to reinstall it.

If you have not yet installed the RMI Dispatcher in the Security Directory Integrator environment, download the Dispatcher installer from the IBM Passport Advantage website. For more information about the installation, see the *Dispatcher Installation and Configuration Guide*.

Updating the directory integrator binaries

Update the directory integrator binaries to install the required fixes for Security Directory Integrator. Complete this task only if you are using IBM Security Directory Integrator 7.2 or 7.2 with fix pack 1.

About this task

The adapter installation involves installing the Security Directory Integrator connector. Before you install the adapter, make sure that the Dispatcher is installed. See Installing the dispatcher.

Procedure

1. Stop the Security Directory Integrator dispatcher service.
2. Replace the following files from Security Directory Integrator with the corresponding files in the resource folder of the installation package.
   - `<ITDI_HOME>\jars\connectors\httpClientConnector.jar`
   - `<ITDI_HOME>\jars\parsers\HTTPParsers.jar`
   - `<ITDI_HOME>\jars\parsers\JSONParsers.jar`
3. Restart the Security Directory Integrator dispatcher service.

Restarting the adapter service

Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

The adapter does not exist as an independent service or a process. The adapter is added to the Dispatcher instance, which runs all the adapters that are installed on the same Security Directory Integrator instance.

See the topic about starting, stopping, and restarting the Dispatcher service in the *Dispatcher Installation and Configuration Guide*.

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 AD`ProfileJAR` 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. .

Attribute mapping

Attribute mapping is required to define which target attributes correspond to the Verify Governance Identity Manager account attributes.

About this task

This task involves an account attribute mapping definition file, which is included in the adapter package.

The file consists of Verify Governance Identity Manager account attributes and their equivalent attributes in the managed target. The file is structured as *<IGI_attribute> = <target_attribute>*.

The *<IGI_attribute>* is fixed and must not be modified. Edit only the *<target_attribute>*. Some *<IGI_attribute>* already has a fixed equivalent *<target_attribute>* of `eraccount`.

Some *<IGI_attribute>* do not have a defined *<target_attribute>* and you can assign the mapping. For example:

```
USER_TYPE=USER_TYPE
ATTR1=ATTR1
```

Note:

- The default mapping is already included out-of-the box. If there are no changes to the attribute mapping, there is no need to import the attribute mapping files.
- It might take up to 10 minutes for the attribute mapping changes to take effect once the file is imported.

Procedure

1. Open the mapping definition file by using any text editor.
2. Edit the mapping.
3. If the target attribute has a list of predefined values, use the following syntax to convert its values to the corresponding Verify Governance Identity Manager attribute values.

   ```
   [conversion].<target_attribute>.<IGI_attribute> =
   [<target_attribute_value1>=<IGI_attribute_value1>;...;
   <target_attribute_valuen>=<IGI_attribute_valuen>]
   ```

4. For attributes that contains date and time, use the following syntax to convert its values.
   For example:

   ```
   [conversion.date].erbirthDate.BIRTHDAY=[yyyyMMdd=dd/MM/yyyy HH:mm:ss]
   [conversion.date].ACCOUNT_EXPIRY_DATE.ACCOUNT_EXPIRY_DATE=
   [dd/MM/yyyy HH:mm:ss=dd/MM/yyyy HH:mm:ss]
   ```

5. Import the updated mapping definition file through the Target Administration module. For more information, see *Attribute-to-permission mapping service* in the IBM Security Verify Governance Identity Manager product documentation.

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 8.

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.

Adapter Details

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
Specify a description that identifies the service for your environment.

Security Directory Integrator location

Specify the URL for the IBM Security Directory Integrator instance. The valid syntax for the URL is `rmi://`*`ip-address`*`:`*`port`*`/ITDIDispatcher`, where *ip-address* is the IBM Security Directory Integrator host and *port* is the port number for the RMI Dispatcher.

The default URL for the default SDI1 instance is `rmi://localhost:1099/ITDIDispatcher`.

SoftLayer Service URL

Specify the URL which the adapter can use to communicate with SoftLayer. For the current SoftLayer release, use **https://api.softlayer.com**.

API User
Specify the user name of the user with the API key. Use the master account for full adapter functionality.

API Key
Specify the API key for the user specified in the **API User** field.

Sync VPN password to account (portal) password

Select the check box to synchronize the SoftLayer VPN password to the portal password. When password synchronization is enabled:

- The VPN password for the created accounts is set to be the same as the account (portal) password. The value specified for the VPN password in the account form is ignored.
- Every time the account password is changed, the VPN password is also updated accordingly.

Note: This option must be selected if the SoftLayer Adapter is running in the IBM Security Privileged Identity Manager virtual appliance

Dispatcher Attributes

AL FileSystem Path
Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines that are received from Identity server. You can specify a file path to load the assembly lines from the `profiles` directory of the Windows operating system such as: *`drive`*`:\Program Files\IBM\TDI\V7.1\profiles`. You can also specify the following file path to load the assembly lines from the `profiles` directory of the UNIX and Linux® operating system: `/opt/IBM/TDI/V7.1/profiles`

Max Connection Count
Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. Enter `10` when you want the dispatcher to run a maximum of 10 assembly lines simultaneously for the service. If you enter `0` in the **Max Connection Count** field, the dispatcher does not limit the number of assembly lines that are run simultaneously for the service.

Disable AL Caching
Select the check box to disable the assembly line caching in the dispatcher for the service. The assembly lines for the `add`, `modify`, `delete`, and `test` operations are not cached.

Status and information
The page 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 that the adapter is connected to.

Adapter version
Specifies the version of the adapter that the service uses to provision request to the managed resource.

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

TDI version
Specifies the version of the Security Directory Integrator on which the adapter is deployed.

Dispatcher version
Specifies the version of the Dispatcher.

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

Adapter account
Specifies the account that running the adapter binary file.

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 sent successfully to the adapter.

- Verify the adapter configuration information.
- Verify service parameters for the adapter profile. Verify parameters such as the work station name or the IP address of the managed resource and the port.

Creating an adapter user account

After a full reconciliation is completed, user accounts can be created on the SoftLayer service.

Complete the following fields to create an account.

User ID
Identifies the account in IBM Security Verify Identity and is used as the user name in SoftLayer.

First Name
First name of the account being created.

Last Name
Last name of the account being created.

Company Name
Company name of the account being created.

Address
Address of the account being created.

Address (continue)
Second line for the address (if applicable) of the account being created.

City
City of the account being created.

State/Province Code
Two letter ISO state or province code corresponding to the address of the account being created. Required for countries that use these codes.

Country
Two letter ISO country code corresponding to the address of the account being created.

Postal Code
Postal code corresponding to the address of the account being created.

Email Address
Email address of the account being created.

Office Phone
Office phone of the account being created.

Parent Account
Parent account of the account being created. The parent account can view the accounts that are created in its list of users.

Time Zone
Time zone of the account being created.

VPN Password
VPN Password of the account being created. VPN password is only applicable if VPN permission is granted for the account, and is ignore if 'Sync to portal password' option is enabled in the service form

Permissions
See the SoftLayer documentation for the list of permissions managed by the adapter and their corresponding descriptions.

Configuring the SSL connection between the dispatcher and the SoftLayer server

To enable communication between the adapter and the SoftLayer server, you must configure keystores for the Dispatcher.

About this task

For more information about SSL configuration, see the *Dispatcher Installation and Configuration Guide*.

Procedure

1. On a web browser, go to `https://api.softlayer.com`.
2. View its certificate.
   - Click the **SSL lock** icon from the browser.
   - If your browser reports that revocation information is not available, click **View Certificates**.
3. On the Certificate window, open the **Certification Path** tab and select the **api.softlayer.com** certificate.
4. Open the **Details** tab and click **Copy to File**.
5. In the Certificate Export Wizard, select the **Base-64 encoded X.509 (.CER)** format.
6. Take one of the following actions:
   - If the RMI Dispatcher already has a configured keystore, use the **`keytool.exe`** program to import the Softlayer Server certificate.
   - If the keystore is not yet configured, create it by running the following command from a command prompt. Type the command on a single line.

     ```
     keytool -import -alias softlayer -file c:\softlayer.cer
     -keystore c:\truststore.jks -storepass passw0rd
     ```
7. After you modify the `solution.properties` file, restart the Dispatcher.

   For information about SSL configuration, see the *Dispatcher Installation and Configuration Guide*.

Configuring the server to encrypt VPN password

If the SoftLayer VPN password is not synchronized with the portal password, you can configure the server to encrypt the VPN password.

About this task

If you do not select **Sync VPN password to account (portal) password** check box, the VPN password is stored in the directory server. For information on **Sync VPN password to account (portal) password**, see Creating an adapter service/target.

By default, the VPN password is stored as clear text. To store it in encrypted form in the server, perform the following task:

Procedure

Update the `enRole.properties` file that is located under the `isim_server_home\data` directory. Append the attribute `erSFloginPassword` to the list of attributes of the `password.attribute` property.

```
password.attributes=ersynchpassword
erServicePassword erServicePwd1 erServicePwd2 erServicePwd3 erServicePwd4
erADDomainPassword erPersonPassword hi erNotesPasswdAddCert
eritamcred erep6umds erposixpassphrase erSoftLayer-vpnPassword
```

Configuring the password policy

Password rules in SoftLayer are stronger than the default rules in IBM Security Verify Identity. You must create a password policy for the adapter that is at least as strong as the SoftLayer password rules before you use the adapter. SoftLayer's password rules can be found in SoftLayer portal when you create a user or on the SoftLayer's website.

Retrieving an API key for the master account in Softlayer

To create a service for the SoftLayer Adapter, you need an API key.

Procedure

1. Log in to the Softlayer Console (https://control.softlayer.com/) with the master account.
2. Select **Account** > **Users**.
3. Click **Generate** if the API key is not yet available for the account master.

   If the API key is already generated, click **View**.
4. Copy the API key for the account master.

Results

You are ready to delegate the domain-wide authority to your service account.

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.

Chapter 4. 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?

Related concepts

Error messages and problem solving
You might encounter some problems at run time. Use this information to resolve some of these common runtime problems.

Error messages and problem solving

You might encounter some problems at run time. Use this information to resolve some of these common runtime problems.

Runtime problems and corrective actions are described in the following table.

Table 3. Runtime problems	
Problem	**Corrective Action**
Reconciliation does not return all SoftLayeraccounts. Reconciliation is successful but some accounts are missing.	For the adapter to reconcile many accounts successfully, you might need to increase the WebSphere JVM memory. The complete the following steps on the WebSphere host computer: **Note:** Do not increase the JVM memory to a value higher than the system memory. 1. Log in to the administrative console. 2. Expand **Servers** in the left menu and select **Application Servers**. 3. A table displays the names of known application servers on your system. Click the link for your primary application server. 4. Select **Process Definition** from the **Configuration** tab. 5. Select the **Java Virtual Machine** property. 6. Enter a new value for the **Maximum Heap Size**. The default value is 256 MB. If the allocated JVM memory is not large enough, an attempt to reconcile many accounts with the adapter results in log file errors. The reconciliation process fails. The adapter log files contain entries that state `ErmPduAddEntry failed`. The *`WebSphere_install_dir`*`/logs/itim.log` file contains **`java.lang.OutOfMemoryError`** exceptions.

Related concepts

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.

Chapter 5. Uninstalling

To remove an adapter from the Identity server for any reason, you must remove all the components that were added during installation. Uninstalling an IBM Security Directory Integrator based adapter mainly involves removing the connector file, and the adapter profile from the Identity server. Depending on the adapter, some of these tasks might not be applicable, or there can be other tasks.

Deleting the adapter profile

Remove the adapter service/target type from the Identity server. Before you delete the adapter profile, ensure that no objects exist on the Identity server that reference the adapter profile.

Objects on the Identity server that can reference the adapter profile:

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

Note: The Dispatcher component must be installed on your system for adapters to function correctly in a Security Directory Integrator environment. When you delete the adapter profile, do not uninstall the Dispatcher.

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

Chapter 6. Reference

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

Adapter attributes and object classes

Adapter attributes and object classes are required for customization, creating provisioning rules, and understanding what service/target attributes are supported by the adapter. The Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network.This topic is not applicable for this adapter.

User attributes

The following tables show the standard attributes and object classes that are supported by the SoftLayer Adapter.

Table 4. Supported user attributes

IBM Security Verify Identity name	Attribute name in schema	Data type
API Key	erSoftLayerapikey	String
API User	erSoftLayerapiuser	String
SoftLayer Service Url	erSoftLayerurl	String
AL File System Path	erSoftLayeralfilesystempath	String
Max Connection Count	erSoftLayermaxconnectioncnt	Integer
Disable AL Cache	erSoftLayerdisablealcache	Boolean
Sync VPN password to account (portal) password	erSoftLayersyncvpnpassword	String
ID	erSoftLayer-id	Integer
Address	erSoftLayer-address1	String
Address (continue)	erSoftLayer-address2	String
City	erSoftLayer-city	String
Country (2 letters code)	erSoftLayer-country	String
State/Province Code (2 letters code)	erSoftLayer-state	String
Email Address	erSoftLayer-email	String
Postal Code	erSoftLayer-postalcode	String
Office Phone	erSoftLayer-officephone	String
First Name	erSoftLayer-firstname	String
Last Name	erSoftLayer-lastname	String
Company Name	erSoftLayer-companyname	String

Table 4. Supported user attributes (continued)

IBM Security Verify Identity name	Attribute name in schema	Data type
Daylight Savings Time	erSoftLayer-daylightsavingstimeflag	String
Restrict Access to IP	erSoftLayer-ipaddressrestriction	String
User Status	erSoftLayer-userstatusid	Integer
Password Expiry Date	erSoftLayer-passwordexpiredate	String
Allow SSL VPN	erSoftLayer-sslvpnallowedflag	String
Allow PPTP VPN	erSoftLayer-pptpvpnallowedflag	String
Time Zone	erSoftLayer-timezoneid	Integer
Parent User	erSoftLayer-parentid	Integer
Display Name	erSoftLayer-displayname	String
VPN Password	erSoftLayer-vpnpassword	String
Require Security Question	erSoftLayer-secondaryloginrequiredflag	String
Status	erSoftLayerUserStatus-name	String
StatusId	erSoftLayerUserStatus-id	Integer
Time Zone	erSoftLayerTimezone-longname	String
Manage DNS	erSoftLayerPerm-dns-manage	String
Hardware Firewall	erSoftLayerPerm-firewall-manage	String
Forum Access	erSoftLayerPerm-forum-access	String
View Hardware	erSoftLayerPerm-hardware-view	String
Edit Hostname/Domain	erSoftLayerPerm-hostname-edit	String
Add/Upgrade Cloud Instances	erSoftLayerPerm-instance-upgrade	String
Add IP Addresses	erSoftLayerPerm-ip-add	String
View licenses	erSoftLayerPerm-license-view	String
Manage Notification Subscribers	erSoftLayerPerm-ntf-subscriber-manage	String
Manage Port Control	erSoftLayerPerm-port-control	String
Upgrade Port	erSoftLayerPerm-port-upgrade	String
Request Compliance Report	erSoftLayerPerm-request-compliance-report	String
View Tickets	erSoftLayerPerm-ticket-view	String
View Event Log	erSoftLayerPerm-user-event-log-view	String

Table 4. Supported user attributes (continued)		
IBM Security Verify Identity name	**Attribute name in schema**	**Data type**
View Virtual Server Details	erSoftLayerPerm-virtual-guest-view	String
Edit Tickets	erSoftLayerPerm-ticket-edit	String
Manage Certificates (SSL)	erSoftLayerPerm-security-certificate-manage	String
View Certificates (SSL)	erSoftLayerPerm-security-certificate-view	String
Manage Security	erSoftLayerPerm-security-manage	String
Add Server	erSoftLayerPerm-server-add	String
Cancel Server	erSoftLayerPerm-server-cancel	String
OS Reloads	erSoftLayerPerm-server-reload	String
Upgrade Server	erSoftLayerPerm-server-upgrade	String
Add Services	erSoftLayerPerm-service-add	String
Cancel Services	erSoftLayerPerm-service-cancel	String
Upgrade Services	erSoftLayerPerm-service-upgrade	String
Software Firewall	erSoftLayerPerm-software-firewall-manage	String
SSL VPN Allowed	erSoftLayerPerm-ssl-vpn-enabled	String
Add Tickets	erSoftLayerPerm-ticket-add	String
View Account Summary	erSoftLayerPerm-account-summary-view	String
Add Storage (StorageLayer)	erSoftLayerPerm-add-service-storage	String
View Bandwidth Statistics	erSoftLayerPerm-bandwidth-manage	String
Manage SSH Keys	erSoftLayerPerm-customer-ssh-key-management	String

Object classes

Table 5. Supported object classes		
Description	**Object class name in schema**	**Superior**
Service class	ergoogappsservice	Top
Account class	ergoogappsaccount	Top
Time zone	erSoftLayer-timezone	Top
Account Status	erSoftLayer-accountStatus	Top

Adapter Configuration Properties

For information about setting Security Directory Integrator configuration properties for the operation of the SoftLayer Adapter, see the *Dispatcher Installation and Configuration Guide*.

Adapter attributes by operations

Adapter attributes by operations refer to adapter actions by their functional transaction group. They are required for customization, creating provisioning rules, and understanding what service/target attributes are supported by the adapter.This topic is not applicable for this adapter.

Special attributes

Certain attributes have special syntax and meaning that customers needs to be aware off. This information will be used to help the customer in how to supply the attribute value.This topic is not applicable for this adapter.

Index