IBM Security Verify Identity
7.0

Siebel JDB Adapter Installation and Configuration Guide

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server.

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.

The adapter automates the following tasks:

- Reconciling user accounts and support data
- Adding, suspending, restoring, and deleting user accounts
- Modifying user account 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
- IBM® Security Verify Adapter profile

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

Figure 1 on page 1 describes the components that work together to complete the user account management tasks in a Security Directory Integrator environment.

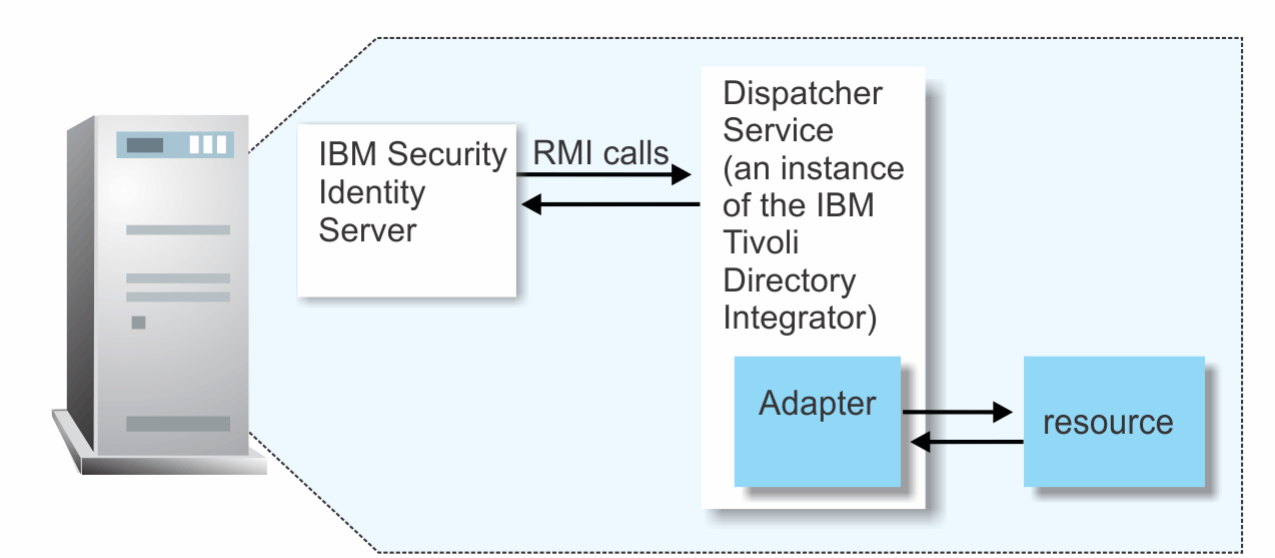

Figure 1. The architecture of the Siebel JDB Adapter

Supported configurations

The adapter supports both single and multiple server configurations.

The fundamental components in each environment are:

- The Identity server
- The Security Directory Integrator
- The managed resource
- The adapter

The adapter must reside directly on the server running the Security Directory Integrator.

Single server configuration

In a single server configuration, install the Identity server, the Security Directory Integrator, and the Siebel JDB Adapter on one server to establish communication with the Siebel server.

The Siebel server is installed on a different server as described in Figure 2 on page 2.

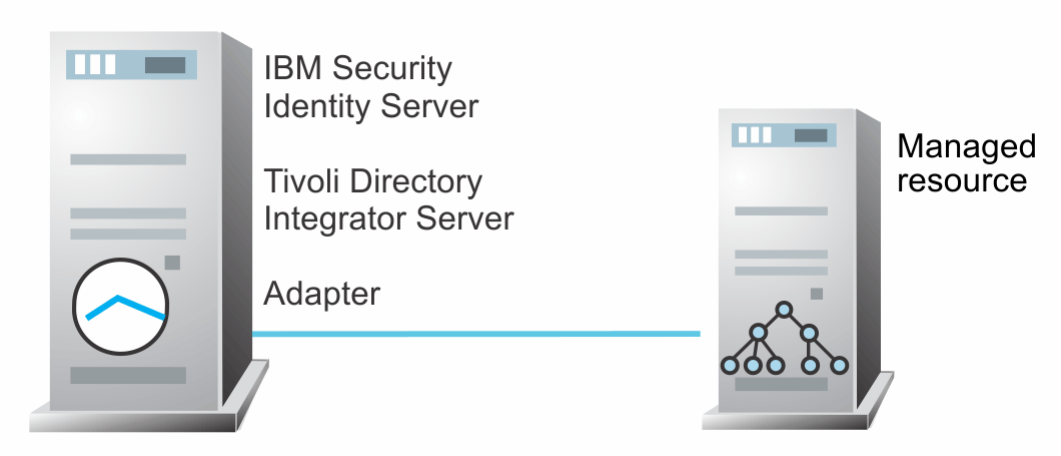

Figure 2. Example of a single server configuration

Multiple server configuration

In a multiple server configuration, the Security Directory Integrator server, the Security Directory Integrator, the Siebel JDB Adapter, and the Siebel server are installed on different servers.

Install the Security Directory Integrator and the Siebel JDB Adapter on the same server as described in Figure 3 on page 3.

Figure 3. Example of a multiple 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

Related concepts

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

Prerequisites to use the adapter
You must meet the following Java Data Beans requirement to run the Siebel JDB Adapter.

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

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.

Prerequisites

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

Ensure that you install the adapter on the same workstation as the Security Directory Integrator server. Table 1 on page 7 identifies the software and operating system prerequisites for the adapter installation.

Table 1. Prerequisites to install the adapter	
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 **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
Siebel server	7.7, 7.8, 8.0
System Administrator Authority	To complete the adapter installation procedure, you must have system administrator authority.
Security Directory Integrator adapters solution directory	A Security Directory Integrator adapters solution directory is a Security Directory Integrator work directory for adapters. See the *Dispatcher Installation and Configuration Guide*.

You must install the adapter on those IBM Tivoli® Directory Integrator platforms that support the managed resource libraries or jars that the adapter uses. For information about the prerequisites and supported operating systems, see the *IBM Tivoli Directory Integrator 7.1: Administrator Guide*.

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 to use the adapter
You must meet the following Java Data Beans requirement to run the Siebel JDB Adapter.

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

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.

Prerequisites to use the adapter

You must meet the following Java Data Beans requirement to run the Siebel JDB Adapter.

The Siebel JDB connector communicates with the Siebel Enterprise server by using the Java Data Beans (JDB). The Java Data Beans is an integration method exposed by Siebel to communicate with external Java applications. The Java Data Bean code in the Siebel JDB connector has dependency on the following JAR files on the managed resource:

- Siebel.jar
- SiebelJI_*lang*.jar. (where *lang* is the installed language pack; for example, SiebelJI_enu.jar for English or SiebelJI_jpn.jar for Japanese).

These JAR files must be copied from *SiebelInstall*\siebsrvr\CLASSES" on the managed resource to the Security Directory Integrator workstation, so that the adapter can access them. Copy the JAR files to *ITDI_HOME*`/jars/3rdparty/others` directory.

The JAR files corresponding to the JDBC driver that is used for communicating with the database must be copied to the *ITDI_HOME*`/jars/3rdparty/others` directory.

For example, if you are using the Microsoft SQL Server driver to connect to MS-SQL, copy the following driver JAR files:

- Msbase.jar
- Msutil.jar
- Mssqlserver.jar

These JAR files are available as part of the Microsoft SQL Server driver for JDBC.

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

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

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.

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.

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

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

Prerequisites to use the adapter
You must meet the following Java Data Beans requirement to run the Siebel JDB Adapter.

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.

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 on page 9 identifies the information that you need before installing the adapter.

Table 2. Required information to install the adapter

Required information	Description	Value

Security Directory Integrator Home Directory (*ITDI_HOME*)	The *ITDI_HOME* directory contains the jars/connectors subdirectory that contains adapter jars. For example, the jars/connectors subdirectory contains the jar 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:
		`drive\Program Files\IBM\TDI\V7.1`
		UNIX:
		• for version 7.1:
		`/opt/IBM/TDI/V7.1`

Solution Directory (*ADAPTER_SOLDIR*)	When you install the dispatcher, the adapter 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:
		Windows:
		• for version 7.1
		`drive\Program Files\IBM\TDI\V7.1\timsol`
		UNIX:
		• for version 7.1:
		`/opt/IBM/TDI/V7.1/timsol`

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

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

Prerequisites to use the adapter
You must meet the following Java Data Beans requirement to run the Siebel JDB Adapter.

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

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*.

Related concepts

Verifying the adapter installation
When the adapter is installed correctly, you can find the adapter components on IBM Security Directory Integrator.

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.

Service/Target form details
Complete the service/target form fields.

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

Related tasks

Installing the adapter binaries or connector
The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

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.

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

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.

Verifying that the adapter is working correctly

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

Installing the adapter binaries or connector

The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

Before you begin

- The Dispatcher must be installed.

Procedure

1. Create a temporary directory on the workstation where you want to install the adapter.
2. Extract the contents of the compressed file in the temporary directory.
3. Copy the `SiebelJDBConnector.jar` file to the *ITDI_HOME*`/jars/connectors` directory.
4. Copy all XML files from resource directory in the installation package to the *ADAPTER_SOLDIR*`/SiebelCustomXMLs` directory.
5. Restart the adapter service.

Related concepts

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.

Verifying the adapter installation
When the adapter is installed correctly, you can find the adapter components on IBM Security Directory Integrator.

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.

Service/Target form details
Complete the service/target form fields.

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

Related tasks

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.

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

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.

Verifying that the adapter is working correctly

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

Verifying the adapter installation

When the adapter is installed correctly, you can find the adapter components on IBM Security Directory Integrator.

Table 3. Adapter components

Directory	Adapter component
On the Windows operating system: *ITDI_HOME*\jars\connectors\ **On the UNIX operating system:** *ITDI_HOME*/jars/connectors/	SiebelJDBConnector.jar
On the Windows operating system: ADAPTER_SOLDIR\SiebelCustomXmls **On the UNIX operating system:** ADAPTER_SOLDIR/SiebelCustomXmls	• AvailStatusTypes.xml • Employee.xml • NotificationTypes.xml • Organization.xml • PersonalTitle.xml • Positions.xml • Responsibility.xml • TimeZone.xml • UserList.xml • Validator.dtd

If this installation is to upgrade a connector, send a request from IBM Security Verify Identity and verify that the version number in the `ibmdi.log` matches the version of the connector.

Related concepts

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.

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.

Service/Target form details
Complete the service/target form fields.

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

Related tasks

Installing the adapter binaries or connector
The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

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.

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

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.

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

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*.

Related concepts

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.

Verifying the adapter installation
When the adapter is installed correctly, you can find the adapter components on IBM Security Directory Integrator.

Service/Target form details
Complete the service/target form fields.

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

Related tasks

Installing the adapter binaries or connector
The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

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.

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

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.

Verifying that the adapter is working correctly

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

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. .

Related concepts

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.

Verifying the adapter installation
When the adapter is installed correctly, you can find the adapter components on IBM Security Directory Integrator.

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.

Service/Target form details
Complete the service/target form fields.

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

Related tasks

Installing the adapter binaries or connector
The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

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

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.

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

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.

Related concepts

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.

Verifying the adapter installation
When the adapter is installed correctly, you can find the adapter components on IBM Security Directory Integrator.

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.

Service/Target form details
Complete the service/target form fields.

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

Related tasks

Installing the adapter binaries or connector
The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

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.

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.

Verifying that the adapter is working correctly

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

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 15.

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.

Related concepts

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.

Verifying the adapter installation
When the adapter is installed correctly, you can find the adapter components on IBM Security Directory Integrator.

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.

Service/Target form details
Complete the service/target form fields.

Installing the adapter language package

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

Related tasks

Installing the adapter binaries or connector
The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

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.

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

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

Service/Target form details

Complete the service/target form fields.

ITIM Siebel JDB Service

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.

IBM 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`.

Owner
Optional: Specify a user as a service owner.

Service prerequisite
Optional: Specify the service that is a prerequisite to this service.

Siebel JDB connection

Connect string
Specify the web address that contains the information to connect to any Siebel server component. The generic form of the syntax for the connect string is:

```
siebel[[.transport][.[encryption][.[compression]]]]:
//host:port/EnterpriseServer/AppObjMgr
```

transport
Specify the network protocol used for communication between the Siebel JDB connector and the Siebel server. Typical values are `TCP/IP` or `HTTP`.

encryption
Specify the type of encryption used for communication between the Siebel JDB connector and the Siebel server. Typical values are `none` or `mscrypto`.

compression
Specify the type of data compression used for communication between the Siebel JDB connector and the Siebel server. Typical values are `none` or `zlib`.

host
The value used for the host portion of the connect string depends on Siebel system configuration:

- If the Siebel system configuration contains only one Siebel server, specify the host name or IP address of the computer where the Siebel server is running.
- If the Siebel system configuration contains multiple Siebel servers and uses third-party load balancing, specify the virtual IP address of the third-party load balancer.
- If the Siebel system configuration contains multiple Siebel servers and uses Siebel native load balancing, specify the host name or IP address of any computer where a Siebel server is running.

port
The value used for the port portion of the connect string depends on Siebel system configuration:

- If the Siebel system configuration contains only one Siebel server, specify the port number for SCBroker on that server. The default port for SCBroker is *2321*.
- If the Siebel system configuration contains multiple Siebel servers and uses third-party load balancing, specify the virtual port number in the third-party load balancer that maps to the physical workstations running the Siebel server.
- If the Siebel system configuration contains multiple Siebel servers and uses Siebel native load balancing, specify the port number that SCBroker uses on the Siebel server that you specified for the host portion of the connect string.

EnterpriseServer
Specify the name of the Siebel enterprise.

AppObjMgr
Specify the Application Object Manager.

Note: For Java Data Beans, the Siebel JDB Adapter must connect to the EAIObjMgr_<lang>.

The specific connect string can be found in the file *Siebel installation home*\ SWEApp \BIN\eapps.cfg, under the heading [eai_*lang*]>], where *lang* is the language pack installed.

Administrator name
Specify the Siebel administrator. This user must have sufficient permissions to perform User Provisioning operations on the managed resource.

Administrator Password
Specify the password of the Siebel administrator.

Language
Specify the installed language pack. Select the appropriate language from the drop-down menu of all languages supported by the Siebel server.

Authentication Type
Siebel resource can be configured to use different authentication mechanisms at various levels namely. Enterprise, Siebel server, or components on the Siebel server. Specify the Siebel authentication mechanism in use for the EAI Object Manager (EAIObjMgr) component. Depending on the choice given here, either database connection related or LDAP connection-related parameters given in the next two tabs are used. If authentication type is DB Authentication, then fill parameters on the **Siebel database connection** tab. If authentication type is LDAP Authentication, then fill parameters on the **Siebel LDAP connection** tab.

Siebel database connection
If authentication type is DB Authentication, then fill parameters on the **Siebel database connection** tab, otherwise you might ignore this tab.

Database type
Specify the type of database that the adapter uses. For example, MS-SQL or Oracle.

JDBC URL For Database
Specify the JDBC web address to connect to the database.

JDBC driver to be used
Specify the JDBC driver class name.

Database name
Specify the instance name of the database that Siebel uses.

Database user name
Specify the user name to connect to the database. The user must have privileges to add, delete, and modify logins and users to the specified database instance.

Database user password
Specify the password for the database user.

Siebel LDAP connection
If authentication type is LDAP Authentication, then fill parameters on the **Siebel LDAP connection** tab, otherwise you might ignore this tab.

Directory Server Location
Specify the LDAP web address in `ldap://host:port` format. The default value is `ldap://localhost:389`

Administrator Name
Specify the full distinguished name (DN) for the LDAP administrator that is stored in the directory.

Administrator Password
Specify the password for the specified administrator.

User Base DN
Specify the base DN under which users are stored.

Responsibilities Attribute
Specify the LDAP attribute in which user responsibilities are stored. You can configure the Siebel server to use any attribute from the iNetOrgPerson objectclass to store responsibilities. This attribute must be multi-valued to store more than one responsibility because Siebel-supported security adapters cannot read more than one responsibility from a single-value attribute. User can select one of the attributes from the dropdown list which lists of all multi-valued attributes from LDAP objectclass iNetOrgPerson.

Remove LDAP User on Delete?
Specify whether to remove the LDAP user on user delete operation. The Siebel server does not remove the LDAP user from directory. The adapter can remove it by using the LDAP connector.

Dispatcher Attributes

Disable AL Caching
Select the check box to disable the assembly line (test, add, modify, delete) caching in the dispatcher for the service.

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 received from Identity server. For example, you can specify the following file path to load the assembly lines from the `profiles` directory of the Windows operating system: `c:\Files\IBM\TDI\V7.1\profiles` or you can specify the following file path to load the assembly lines from the `profiles` directory of the UNIX and Linux® operating systems:`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. For example, enter `10` when you want the dispatcher to run maximum 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 run simultaneously for the service.

On the Status and information tab
This 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 successfully sent to the adapter.
- Verify the adapter configuration information.
- Verify service parameters for the adapter profile. For example, verify the work station name or the IP address of the managed resource and the port.

Note: If the following fields on the service form are changed for an existing service, the adapter service on the Security Directory Integrator server must be restarted.

SIEBEL JDB CONNECTION tab:

- **Administrator Password**
- **Language**
- **Authentication Type**

SIEBEL DATABASE CONNECTION tab:

- **Database Type**
- **JDBC URL for the database**
- **JDBC Driver to be used**
- **Database Name**
- **Database User Name**
- **Database User Password**

SIEBEL LDAP CONNECTION tab:

- **Directory Server Location**
- **Administrator Name**
- **Administrator Password**
- **User Base DN**
- **Responsibilities Attribute**
- **Remove LDAP User on Delete?**

DISPATCHER ATTRIBUTE tab:

- **AL FileSystem Path**
- **Max Connection Count**

Related concepts

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.

Verifying the adapter installation
When the adapter is installed correctly, you can find the adapter components on IBM Security Directory Integrator.

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.

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

Related tasks

Installing the adapter binaries or connector
The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

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.

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

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.

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

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.

Related concepts

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.

Verifying the adapter installation
When the adapter is installed correctly, you can find the adapter components on IBM Security Directory Integrator.

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.

Service/Target form details
Complete the service/target form fields.

Related tasks

Installing the adapter binaries or connector
The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

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.

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

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.

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

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.

Verifying the adapter installation
When the adapter is installed correctly, you can find the adapter components on IBM Security Directory Integrator.

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.

Service/Target form details
Complete the service/target form fields.

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

Configuring the business components view mode
The Siebel JDB connector uses custom XML files that specify which user attributes to set or get and which support data attributes to get.

Configuration properties of the dispatcher
The `solution.properties` file and the `itim_listener.properties` file contain the configuration properties for the Dispatcher.

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

Related tasks

Installing the adapter binaries or connector
The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

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.

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

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.

Customizing the adapter profile
To customize the adapter profile, you must modify the Siebel JDB Adapter JAR file.

Removing the Responsibilities in LDAP attribute from the account form for database authentication
If the authentication type used by the Siebel server is database authentication, then account form attribute **`Responsibilities in LDAP`** can be removed. It is not needed because all responsibilities are stored in a database for database authentication.

Chapter 4. Upgrading

Upgrading an IBM Security Directory Integrator-based adapter involves tasks such as upgrading the dispatcher, the connector, and the adapter profile. Depending on the adapter, some of these tasks might not be applicable. Other tasks might also be required to complete the upgrade.

To verify the required version of these adapter components, see the adapter release notes.

Upgrading the connector

The new adapter package might require you to upgrade the connector.

Before you upgrade the connector, verify the version of the connector.

- If the connector version mentioned in the release notes is later than the existing version on your workstation, install the connector.
- If the connector version mentioned in the release notes is the same or earlier than the existing version, do not install the connector.

Related concepts

Upgrading the dispatcher
The new adapter package might require you to upgrade the Dispatcher.

Upgrading the adapter profile
Read the adapter Release Notes for any specific instructions before you import a new adapter profile.

Upgrading the dispatcher

The new adapter package might require you to upgrade the Dispatcher.

Before you upgrade the dispatcher, verify the version of the dispatcher.

- If the dispatcher version mentioned in the release notes is later than the existing version on your workstation, install the dispatcher.
- If the dispatcher version mentioned in the release notes is the same or earlier than the existing version, do not install the dispatcher.

Note: The dispatcher installer stops the dispatcher service before the upgrade and restarts it after the upgrade is complete.

Related concepts

Upgrading the connector
The new adapter package might require you to upgrade the connector.

Upgrading the adapter profile
Read the adapter Release Notes for any specific instructions before you import a new adapter profile.

Upgrading the adapter profile

Read the adapter Release Notes for any specific instructions before you import a new adapter profile.

Note: Restart the Dispatcher service after importing the profile. Restarting the Dispatcher clears the assembly lines cache and ensures that the dispatcher runs the assembly lines from the updated adapter profile.

Related concepts

Upgrading the connector
The new adapter package might require you to upgrade the connector.

Upgrading the dispatcher

The new adapter package might require you to upgrade the Dispatcher.

Chapter 5. Configuring

After you install the adapter, configure it to function correctly. Configuration is based on your requirements or preference.

You can change the configuration options for the Siebel JDB Adapter.

See the *Dispatcher Installation and Configuration Guide* for additional configuration options such as:

- JVM properties
- Dispatcher filtering
- Dispatcher properties
- Dispatcher port number
- Logging configurations
- Secure Sockets Layer (SSL) communication

Customizing the adapter profile

To customize the adapter profile, you must modify the Siebel JDB Adapter JAR file.

About this task

You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms using the Form Designer or `CustomLabels.properties`. Each adapter has a `CustomLabels.properties` file for that adapter.

The JAR file is included in the Siebel JDB Adapter compressed file that you downloaded from the IBM website.

Note: The adapter supports a set of ready-to-use attributes. To customize the set of attributes that the adapter supports, see the *Directory Integrator-Based Siebel JDB Adapter User Guide*.

The following files are included in the SiebelJDBProfile JAR file:

- CustomLabels.properties
- erTDISblJDBAccount.xml
- erTDISblJDBRMIService.xml
- SiebelJDBAdapter.xml
- siebelJDBAdd.xml
- siebelJDBDelete.xml
- siebelJDBModify.xml
- siebelJDBSearch.xml
- siebelJDBTest.xml
- schema.dsml
- service.def

After you edit the file, you must import the file into the Identity server for the changes to take effect.

Procedure

1. Edit the JAR file.
   a) Log on to the workstation where the Siebel JDB 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. The following example applies to the Siebel JDB Adapter profile. Type the name of the JAR file for your operating system.

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

The jar command extracts the files into the SiebelJDBProfile directory.

d) Edit the file that you want to change.

2. Import the file.

a) Create a JAR file using the files in the `/tmp` directory

Run the following command:

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

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

Configuring the business components view mode
The Siebel JDB connector uses custom XML files that specify which user attributes to set or get and which support data attributes to get.

Configuration properties of the dispatcher
The `solution.properties` file and the `itim_listener.properties` file contain the configuration properties for the Dispatcher.

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

Related tasks

Removing the Responsibilities in LDAP attribute from the account form for database authentication
If the authentication type used by the Siebel server is database authentication, then account form attribute **`Responsibilities in LDAP`** can be removed. It is not needed because all responsibilities are stored in a database for database authentication.

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

LDAP Password attribute change for LDAP authentication

To manage users on Siebel Server having LDAP authentication, Siebel JDB Adapter needs the LDAP password attribute name for the LDAP user, which is **`userPassword`** by default.

The LDAP password attribute **`LDAPPwdAttribute`** is a dispatcher parameter and is defined in the `service.def` file as:

```
<dispatcherParameter name="LDAPPwdAttribute">
        <default>userPassword</default>
</dispatcherParameter>
```

You can change default value by editing the `service.def` file. See the Siebel JDB Adapter white paper for more details on modifying Siebel JDB Profile.

Note: The dispatcher parameter **`LDAPPwdAttribute`** is ignored, if the Siebel server is using database authentication.

Related tasks

Editing Siebel JDB adapter profiles on the UNIX or Linux operating system

The adapter profile `.jar` file might contain ASCII files that are created by using the MS-DOS ASCII format.

Editing Siebel JDB adapter profiles on the UNIX or Linux operating system

The adapter profile `.jar` file might contain ASCII files that are created by using the MS-DOS ASCII format.

About this task

If you edit an MS-DOS ASCII file on the UNIX operating system, you might see a character `^M` at the end of each line. These characters indicate new lines of text in MS-DOS. The characters can interfere with the running of the file on UNIX or Linux systems. You can use tools, such as **dos2unix**, to remove the `^M` characters. You can also use text editors, such as the **vi** editor, to remove the characters manually.

Example

You can use the **vi** editor to remove the `^M` characters. From the **vi** command mode, run the following command and press Enter:

```
:%s/^M//g
```

When you use this command, enter `^M` or `Ctrl-M` by pressing **^v^M** or **Ctrl V Ctrl M** sequentially. The **^v** instructs the **vi** editor to use the next keystroke instead of issuing it as a command.

Related concepts

LDAP Password attribute change for LDAP authentication
To manage users on Siebel Server having LDAP authentication, Siebel JDB Adapter needs the LDAP password attribute name for the LDAP user, which is **userPassword** by default.

Configuring the business components view mode

The Siebel JDB connector uses custom XML files that specify which user attributes to set or get and which support data attributes to get.

You can edit these XML files or create a new one to change the business object, the business component, and the set of attributes under that business component. These XML files for the ready-to-use attributes that the adapter supports are shipped along with the Siebel JDB Adapter, and are in the *Adapter_solution_directory*/SiebelCustomXMLs/ directory.

See "View Mode specification in XML file" on page 32.

Related concepts

Configuration properties of the dispatcher
The `solution.properties` file and the `itim_listener.properties` file contain the configuration properties for the Dispatcher.

Password management when restoring accounts
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 modify the Siebel JDB Adapter JAR file.

Removing the Responsibilities in LDAP attribute from the account form for database authentication
If the authentication type used by the Siebel server is database authentication, then account form attribute **Responsibilities in LDAP** can be removed. It is not needed because all responsibilities are stored in a database for database authentication.

Verifying that the adapter is working correctly

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

View mode

The view modes of a business component determine the allowable access control mechanisms that can be applied to the business component in any view.

When a view is based on a particular business component, the view must use one of the view modes specified for the business component. For example, the Responsibility business component can only be used in Organization view mode. Each view mode also determines how data is associated with a user to determine whether the user has access. For example, a business component that allows personal access control might connect the data to the person by comparing the data Owner Id field to the person's user ID. Another business component might apply personal access control through the data Created by field.

Use Siebel Tools to work with properties of business components.

Note: If a business component has no listed view modes, then no access control based on the business component exist for views that are based on that business component.

Related concepts

View Mode specification in XML file
The adapter supports various ready-to- use attributes for view mode.

Related tasks

Viewing the view mode and visibility fields of a business component
You can use Siebel Tools to see the view mode details of a particular business component.

Viewing the view mode and visibility fields of a business component

You can use Siebel Tools to see the view mode details of a particular business component.

Procedure

1. Launch Siebel Tools.
2. In the Siebel Objects Object folder, click **+** (the plus sign) next to Business Component to expand the Business Component object type. The Business Component sub-tree is displayed.
3. Select the required Business Component and click the **BusComp View Mode** icon. The business component view mode details are displayed. A record in Business Component View Modes represents one view mode the business component can assume.

Related concepts

View mode
The view modes of a business component determine the allowable access control mechanisms that can be applied to the business component in any view.

View Mode specification in XML file
The adapter supports various ready-to- use attributes for view mode.

View Mode specification in XML file

The adapter supports various ready-to- use attributes for view mode.

This table shows the XML files for the ready-to-use attributes that the adapter supports.

Table 4. XML files used for user management and for various support data attributes

Used for	Business object: business component	XML file name	Default view mode of business component	Default view modes of MVBBusComoponets and PicklistBusComponents
User management	User List: User	UserList.xml	5	**MVGBusComponent** • name="Employee Organization" viewMode="9" • name="Responsibility" viewMode="9" • name="Position" viewMode="9" **PicklistBusComponent** • name="Time Zone" viewMode="9" • name="Personal Title" viewMode="9" • name="Availability Status" viewMode="9" • name="Standard Notification" viewMode="9" • name="Emergency Notification" viewMode="9"

Table 4. XML files used for user management and for various support data attributes (continued)

Used for	Business object: business component	XML file name	Default view mode of business component	Default view modes of MVBBusComoponets and PicklistBusComponents
User management	Employee: Employee	Employee.xml	5	**MVGBusComponent** • name="Employee Organization" viewMode="9" • name="Responsibility" viewMode="9" • name="Position" viewMode="9" **PicklistBusComponent** • name="Time Zone" viewMode="9" • name="Personal Title" viewMode="9" • name="Availability Status" viewMode="9" • name="Standard Notification" viewMode="9" • name="Emergency Notification" viewMode="9"
Support data - Availability	List Of Values: List Of Values	AvailStatusTypes.xml	9 (not used)	Not applicable
Support data - Standard/ Emergency Notification	List Of Values: List Of Values	NotificationTypes.xml	9 (not used)	Not applicable
Support data - Organization	Organizations: Organization	Organization.xml	9	Not applicable
Support data - Personal title (Mr./ Mrs.)	List Of Values: List Of Values	PersonalTitle.xml	9 (not used)	Not applicable
Support data - Position	Employee: Position	Positions.xml	9	Not applicable
Support data - Responsibility	Employee: Responsibility	Responsibility.xml	9	Not applicable
Support data - Time Zone	Time Zone: Time Zone	TimeZone.xml	9	Not applicable

This table lists the integer values allowed in the definition of the business component for viewMode and their meaning:

Table 5. Values for business components in viewMode		
Value	**View name**	**Meaning**
0	SalesRepView	Users can access records owned by them or can access records whose team contains their position.
1	ManagerView	Users can access records associated with their own position and positions that report directly to them.
2	PersonalView	Users can access records with which their person records are associated.
3	AllView	Users can access all records, except those with a missing or an invalid owner.
5	OrganizationView	Users can access records that are associated with a single organization or with multiple organizations to which their position is linked.
6	ContactView	Users can access records that are associated with a single organization to which their position is linked.
7	GroupView	Users can access categories of master data that are associated with any of the access groups with which they are associated. Users are associated with an access group if during the current session, they are associated with a position, organization, account, household, or a user list that is a member of the access group.
8	CatalogView	Users can access a flat (uncategorized) list of data in all of the categories across catalogs to which all of the user's access groups have access. Users are associated with an access group if during the current session, they are associated with a position, organization, account, household, or a user list that is a member of the access group.
9	SubOrganizationView	Users can access records associated with their active organization or a descendant organization.

You can edit the XML file and set the required view mode accordingly. The viewMode is redundant in those XML files that have searchSpecificationAttribute or searchSpecificationValue specified for the business component. These XML files are PersonalTitle.xml, NotificationTypes.xml, and AvailStatusTypes.xml. But viewMode cannot be removed due to redundancy, because it is a required attribute in the definition of BusinessComponent.

The following sample of the Responsibility.xml file specifies view mode as **9**, SubOrganizationView for business component Responsibility:

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE BusinessObject SYSTEM "Validator.dtd">
<BusinessObject name="Employee">

    <BusinessComponent name = "Responsibility"  viewMode = "9">

        <Attribute name = "Name" isUnique = "true" isRequired = "true"> </Attribute>
        <Attribute name = "Primary Organization Id"> </Attribute>
        <Attribute name = "Description"> </Attribute>
    </BusinessComponent>
</BusinessObject>
```

Related concepts

View mode

The view modes of a business component determine the allowable access control mechanisms that can be applied to the business component in any view.

Related tasks

Viewing the view mode and visibility fields of a business component
You can use Siebel Tools to see the view mode details of a particular business component.

Removing the Responsibilities in LDAP attribute from the account form for database authentication

If the authentication type used by the Siebel server is database authentication, then account form attribute **Responsibilities in LDAP** can be removed. It is not needed because all responsibilities are stored in a database for database authentication.

About this task

This attribute can be removed from the profile manually. It can also be removed from IBM Security Verify Identity by using form customization, after the Siebel JDB profile is imported to the Identity server.

Note: Even if this attribute is present, it is ignored by the adapter if the authentication type is database authentication.

Procedure

1. Log on to IBM Security Verify Identity with an account that has administrative authority.
2. Click **Configure System**.
3. Click **Design Forms**.
4. Double-click **Account**.
   A list of existing account class definitions is displayed.
5. Double-click **SiebelJDBAccount**.
   Various account form tabs are displayed. Attributes are displayed on each tab.
6. Click **$ertdisblaccesscontrol**.
   The attributes for access control are displayed.
7. Delete the attribute **ertdisblldaprelresponsibilit**.
   a) Click **ertdisblldaprelresponsibilit**.
   b) Click **Attribute**.
   c) Click **Delete Attribute**.
   The **ertdisblldaprelresponsibilit** attribute is removed from the list of attributes.
8. Click **Close**.

Related concepts

Configuring the business components view mode
The Siebel JDB connector uses custom XML files that specify which user attributes to set or get and which support data attributes to get.

Configuration properties of the dispatcher
The `solution.properties` file and the `itim_listener.properties` file contain the configuration properties for the Dispatcher.

Password management when restoring accounts
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 modify the Siebel JDB Adapter JAR file.

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

Configuration properties of the dispatcher

The `solution.properties` file and the `itim_listener.properties` file contain the configuration properties for the Dispatcher.

To configure the dispatcher properties, follow the configuration instructions included in the dispatcher download package.

Related concepts

Configuring the business components view mode
The Siebel JDB connector uses custom XML files that specify which user attributes to set or get and which support data attributes to get.

Password management when restoring accounts
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 modify the Siebel JDB Adapter JAR file.

Removing the Responsibilities in LDAP attribute from the account form for database authentication
If the authentication type used by the Siebel server is database authentication, then account form attribute **`Responsibilities in LDAP`** can be removed. It is not needed because all responsibilities are stored in a database for database authentication.

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

Password management when restoring accounts

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.

Note: A password is required for the restore operation, if the authentication is LDAP authentication.

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 Siebel JDB Adapter to require a new password when the account is restored, if your company has a business process in place that dictates that the account restoration process must be accompanied by resetting the password.

In the service.def file, you can define whether a password is required as a new protocol option. 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 also enable remote services to determine if you discard a password that is entered by the user in a situation where multiple accounts on disparate resources are being restored. In this situation, only some of the accounts 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 service.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 example above, 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 operating system supports restoring of an account without a password.

Related concepts

Configuring the business components view mode
The Siebel JDB connector uses custom XML files that specify which user attributes to set or get and which support data attributes to get.

Configuration properties of the dispatcher
The `solution.properties` file and the `itim_listener.properties` file contain the configuration properties for the Dispatcher.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must modify the Siebel JDB Adapter JAR file.

Removing the Responsibilities in LDAP attribute from the account form for database authentication
If the authentication type used by the Siebel server is database authentication, then account form attribute **`Responsibilities in LDAP`** can be removed. It is not needed because all responsibilities are stored in a database for database authentication.

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

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.

Verifying the adapter installation
When the adapter is installed correctly, you can find the adapter components on IBM Security Directory Integrator.

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.

Service/Target form details
Complete the service/target form fields.

Installing the adapter language package

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

Configuring the business components view mode
The Siebel JDB connector uses custom XML files that specify which user attributes to set or get and which support data attributes to get.

Configuration properties of the dispatcher
The `solution.properties` file and the `itim_listener.properties` file contain the configuration properties for the Dispatcher.

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

Related tasks

Installing the adapter binaries or connector
The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

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.

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

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.

Customizing the adapter profile
To customize the adapter profile, you must modify the Siebel JDB Adapter JAR file.

Removing the Responsibilities in LDAP attribute from the account form for database authentication
If the authentication type used by the Siebel server is database authentication, then account form attribute **`Responsibilities in LDAP`** can be removed. It is not needed because all responsibilities are stored in a database for database authentication.

Chapter 6. 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
A warning or error message might be displayed in the user interface to provide information about the adapter or when an error occurs.

Error messages and problem solving

A warning or error message might be displayed in the user interface to provide information about the adapter or when an error occurs.

Table 6 on page 43 contains warnings or errors which might be displayed in the user interface when the Siebel JDB Adapter is installed on your system.

Table 6. Messages and actions

Message number	Message	Action
CTGIMT600E	An error occurred while establishing communication with the Security Directory Integrator server.	• Verify that the Security Directory Integrator-Based Adapter Service is running. • Verify that the URL specified on the service form for Security Directory Integrator is correct.
CTGIMT001E	The following error occurred. Error: Error communicating with Siebel Server using Java Data Beans. Could not open a session in 4 attempts. {1} (SBL-JCA-200) OR Code Page "UTF-8" is not supported. Use "-encoding" option to change the file encoding. (SBL-JCA-328)	• Verify that the Siebel server is running. • Verify that the port specified in connect string can be reached from Security Directory Integrator workstation and that no firewall or other security product prevents communication between them. • Verify that the dispatcher JVM is *not* using the UTF-8 code page (which is by default on Linux). The code page for JVM can be changed using -Dfile.encoding option.
CTGIMT001E	The following error occurred. Error: NoClassDefFoundError for class: com.siebel.data.SiebelException	Ensure that Siebel.jar and SiebelJI_*lang*.jar files are placed in the *ITDI_HOME*/jars/3rdparty/others directory.
CTGIMT001E	The following error occurred. Error: [JavaPackage com.ibm.di. utils. SiebelJDBAdapterUtils. Get[LDAP/JDBC]Connector] is not a function.	Ensure that the correct dispatcher is installed.
CTGIMT001E	The following error occurred. Error: SBL-SVR-00040: Internal: Informational, encrypted parameter. OR The following error occurred. Error: Siebel authentication error.	Verify that the Siebel Administrator name and password are correct.
CTGIMT001E	The following error occurred. Error: null	Verify that port number is specified in connect string.
CTGIMT001E	The following error occurred. Error: [error message]	Verify that the required parameter specified in the error message is given correctly.
CTGIMT003E	The account already exists.	The user has already been added to the resource. This error might occur if you are attempting to add a user to the managed resource and IBM Security Verify Identity is not synchronized with the resource. To fix this problem, schedule a reconciliation between IBM Security Verify Identity and the resource. See the online help for information about scheduling a reconciliation. For Siebel server using LDAP authentication this error might occur if the Siebel user is not present but the corresponding LDAP user exists.

Table 6. Messages and actions (continued)

Message number	Message	Action
CTGIMT015E	An error occurred while deleting the *username* account because the account does not exist.	This error might occur when you attempt to delete a user. This error might also occur if you attempt to change the password for a user. To fix the problem, ensure that: • The location specified for the managed resource is correct. • The user was created on the resource. • The user was not deleted from the resource. • If the user does not exist on the resource, create the user on the resource and then schedule a reconciliation. See the online help for information about scheduling a reconciliation.
CTGIMT009E	The account *username* cannot be modified because it does not exist.	This error might occur when you attempt to modify a user. This error might also occur if you attempt to change the password for a user. To fix the problem, ensure that: • The location specified for the managed resource is correct. • The user was created on the resource. • The user was not deleted from the resource. • If the user does not exist on the resource, create the user on the resource and then schedule a reconciliation. See the online help for information about scheduling a reconciliation.
CTGIMT211E	The account was not added/ modified/deleted due to a system error: An end of file error has occurred. Please continue or ask your systems administrator to check your application configuration if the problem persists.(SBL-DAT-00393).	Verify that the `Siebel.jar` and `SiebelJI_enu.jar` files in *`ITDI_HOME`*`/jars/3rdparty/others` directory are copied from the same Siebel server being used to manage the users.
CTGIMT222W	The account is already suspended.	This error might occur if you attempt to suspend an account that was already suspended.
CTGIMT224W	The account is already restored.	This error might occur if you attempt to restore an account that was already restored.

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 7. 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.

If you take the server offline, completed adapter requests might not be recovered when the server is back online.

Removing the adapter binaries or connector

Use this task to remove the connector file for the Siebel JDB Adapter.

Before you begin

Before you remove the adapter, inform your users that the Siebel JDB Adapter is going to be unavailable. If the server is taken offline, adapter requests that were completed might not be recovered when the server is back online.

About this task

Note: The Dispatcher is required for all IBM Security Directory Integrator adapters. If you uninstall the Dispatcher, none of the other installed adapters work. To uninstall the Dispatcher, see the *Dispatcher Installation and Configuration Guide*.

Procedure

1. Stop the adapter service.
2. Remove `SiebelJDBConnector.jar` from the *`ITDI_HOME`*`\jars\connectors` directory.
3. Remove the directory: *`ADAPTER_SOLDIR`*`\SiebelCustomXMLs`.

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 8. 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

The Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network.

This list describes the attributes used by the Siebel JDB Adapter account object class **erTDISblJDBAccount** and the corresponding counterparts in the User business component on Siebel.

*Table 7. Attributes, descriptions, and corresponding Siebel attributes for **erTDISblJDBAccount***

Attribute name	Description	Required	Siebel attribute
erUid	User ID	Yes	Login Name
erPassword	Password for the user ID	No	LDAP auth.: Password and Verify Password DB auth.:<In database>
erAccountStatus	Status of the account (suspended/restored)	No	LDAP auth.: <In LDAP> DB auth.: <In database>
erTDISblIsEmployee	Type of account (Employee/Contact user)	No	Employee Flag
erTDISblFirstName	Given name	Yes	First Name
erTDISblLastName	Surname	Yes	Last Name
erTDISblMiddleName	Middle initial	No	Middle Name
erTDISblJobTitle	Job title	No	Job Title
erTDISblAlias	Alias	No	Alias
erTDISblTZone	Time zone	No	Time Zone
erTDISblWorkPhone	Work telephone number	No	Phone #
erTDISblHomePhone	Home telephone number	No	Home Phone #
erTDISblFaxNo	Fax number	No	Fax #
erTDISblEmail	Email address	No	Email Addr
erTDISblEmpNo	Employee number	No	EMP #
erTDISblCellPhone	Cell telephone number	No	Cell Phone #
erTDISblShortName	Short name	No	Nick Name
erTDISblPagerNo	Pager number	No	Pager Phone #
erTDISblPagerPin	Pager PIN	No	Pager PIN

*Table 7. Attributes, descriptions, and corresponding Siebel attributes for **erTDISblJDBAccount** (continued)*			
Attribute name	**Description**	**Required**	**Siebel attribute**
erTDISblEmergencyNtfy	Emergency notification	No	Emergency Notification
erTDISblStndNotify	Standard notification	No	Standard Notification
erTDISblAvail	Availability	No	Availability Status
erTDISblAvailUntil	Overtime availability	No	Availability Status Until
erTDISblRelPositions	Positions	No	Position
erTDISblRelResponsibility	Responsibilities	No	Responsibility
erTDISblPersonalTitle	Name title (Mr./Mrs.)	No	Personal Title
erTDISblBUnits	Employee organizations	No	Employee Organization
erTDISblPrimBUnit	Primary employee organization	No	Primary Employee Organization
erTDISblPrimPosition	Primary position ID	No	Primary Position
erTDISblLDAPRelResponsibility	Responsibilities in LDAP	No	Responsibility in LDAP (Available for only LDAP authentication.)
erLastAccessDate	Last Access Date	No	erLastAccessDate

This list describes the attributes used by the Siebel JDB Adapter responsibility support DataObject class **erTDISblResponsibility** and the corresponding counterparts in the Responsibility business component on Siebel.

*Table 8. Attributes, descriptions, and corresponding Siebel attributes for **erTDISblResponsibility***			
Object class attribute	**Description**	**Required**	**Siebel attribute**
erTDISblRespName	Name of the responsibility	Yes	Name
erTDISblRespDisplayName	Display name on the IBM Security Verify Identity user interface	Yes	Name + Primary Organization ID + Description
erTDISblRespOrgName	Responsibility name and the primary organization ID it belongs to	Yes	Name + Primary Organization ID

This list describes the attributes used by the Siebel JDB Adapter position support DataObject class **erTDISblPosition** and the corresponding counterparts in the Position business component on Siebel.

*Table 9. Attributes, descriptions, and corresponding Siebel attributes for **erTDISblPosition***			
Object class attribute	**Description**	**Required**	**Siebel attribute**
erTDISblPostnId	ID of position on resource	Yes	Position ID
erTDISblPostnName	Name of the position	Yes	Name + Division + Position ID + Description

This list describes the attribute used by the Siebel JDB Adapter time zone support DataObject class **erTDISblTZones** and the corresponding counterpart in the Time Zone business component on Siebel.

*Table 10. Attribute, description, and corresponding Siebel attribute for **erTDISblTZones***			
Object class attribute	**Description**	**Required**	**Siebel attribute**
erTDISblTZName	Name of time zone	Yes	Name

This list describes the attribute used by the Siebel JDB Adapter personal title support DataObject class **erTDISblTitles** and the corresponding counterpart in the List of Values business component on Siebel.

*Table 11. Attribute, description, and corresponding Siebel attribute for **erTDISblTitles***			
Object class attribute	**Description**	**Required**	**Siebel attribute**
erTDISblTitle	Name of title on resource	Yes	Value

This list describes the attribute used by the Siebel JDB Adapter notification type support DataObject class **erTDISblEmpNotify** and the corresponding counterpart in the List of Values business component on Siebel.

*Table 12. Attribute, description, and corresponding Siebel attribute for **erTDISblEmpNotify***			
Object class attribute	**Description**	**Required**	**Siebel attribute**
erTDISblNotifyType	Type of employee notification	Yes	Value

This list describes the attribute used by the Siebel JDB Adapter availability type support DataObject class **erTDISblEmpAvail** and the corresponding counterpart in the List of Values business component on Siebel.

*Table 13. Attribute, description, and corresponding Siebel attribute for **erTDISblEmpAvail***			
Object class attribute	**Description**	**Required**	**Siebel attribute**
erTDISblAvailType	Type of employee availability	Yes	Value

This list describes the attributes used by the Siebel JDB Adapter employee organization support DataObject class **erTDISblBU** and the corresponding counterparts in the Organization business component on Siebel.

*Table 14. Attributes, descriptions, and corresponding Siebel attributes for **erTDISblBU***			
Object class attribute	**Description**	**Required**	**Siebel attribute**
erTDISblBUnit	Name of organization	Yes	Name
erTDISblBUnitId	ID of organization	Yes	Organization ID

Custom XML details

The Siebel JDB connector uses custom XML files to specify objects, components, and attributes for the set and get operations.

The following example is a sample of the Custom XML file used by the Siebel JDB connector. It specifies the business object, business component, and attributes that the connector sets or gets.

```
<!-Start of file->
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE BusinessObject SYSTEM "Validator.dtd">
<BusinessObject name="User List">
    <BusinessComponent name = "User" viewMode = "9" >
        <Attribute name = "Employee Flag"> </Attribute>
        <Attribute name = "Login Name" isUnique = "true" forceCase = "Upper"
        isRequired = "true"></Attribute>
```

```
        <Attribute name = "Password"> </Attribute>
        <Attribute name = "Verify Password"> </Attribute>
        <Attribute name = "Last Name" isRequired = "true"></Attribute>
        <Attribute name = "First Name" isRequired = "true"></Attribute>
        <Attribute name = "Middle Name"></Attribute>
        <Attribute name = "Job Title"></Attribute>
        <Attribute name = "Alias"></Attribute>

        <PicklistBusComponent name="Time Zone">
            <Attribute name = "Name" isUnique = "true"
            isRequired = "true"></Attribute>
        </PicklistBusComponent>

        <MVGBusComponent name="Responsibility">
            <Attribute name = "Name"  isUnique = "true" isRequired = "true"></Attribute>
            <Attribute name = "Primary Organization Id" isUnique = "true"
           isRequired = "true"> </Attribute>
        </MVGBusComponent>
    </BusinessComponent>
</BusinessObject>
<!-End of file->
```

Supported attributes for the custom XML file

You can use attributes to customize the XML files that define the set and get operations for the Siebel JDB connector.

Table 15. Attribute information for the custom XML file

Node type	Attribute	Description	Req
BusinessObject	Name	Name of the business object	Yes
BusinessComponent	Name	Name of the business component	Yes
	searchSpecificationAttribute	Name of the search specification attribute that specifies the value to be matched in **searchSpecificationValue**. Only records that satisfy this condition are retrieved.	No
	searchSpecificationValue	searchSpecificationAttribute value	No
	viewMode	View mode to search records Possible values and their meaning are: 0 - SalesRepView 1 - ManagerView 2 - PersonalView 3 - AllView 5 - OrganizationView 6 - ContactView 7 - GroupView 8 - CatalogView 9 - SubOrganizationView	Yes
MVGBusComponent	Name	Name of the MVG Business Component	Yes
	viewMode	View mode to search records	Yes
PicklistBusComponent	Name	Name of the Picklist Business Component	Yes
	viewMode	View mode to search records	Yes
Attribute	Name	Name of the Attribute	Yes

Table 15. Attribute information for the custom XML file (continued)

Node type	Attribute	Description	Req
	isUnique	Specifies whether the attribute value is unique in the business component. Allowed values are: true | false | TRUE | FALSE	No
	isRequired	Specifies whether the attribute value is required for adding the business component. Allowed values are: true | false | TRUE | FALSE	No
	forceCase	Specifies whether the attribute value needs to be forced to a particular case. Allowed values are: upper | lower | Upper | Lower | UPPER | LOWER	No

Index

S

T

U

V

W

X