IBM Security Verify Identity
7.0

Box Adapter Installation and Configuration Guide

Contents

Tables... v

Chapter 1. Overview... 1

Chapter 2. Planning.. 3
Roadmap... 3
Prerequisites.. 4
Software downloads.. 6
Installation worksheet.. 6

Chapter 3. Installing.. 9
Installing the dispatcher.. 9
Exporting and importing the Box SSL certificate..................................... 9
Installing the adapter binaries or connector... 10
Verifying the adapter installation.. 10
Restarting the adapter service.. 11
Importing the adapter profile.. 11
Attribute mapping... 12
Registering the API key... 13
Creating an adapter service/target... 13
Service/Target form details.. 15
Permissions for the `/tmp` directory... 18
Managing suspend, restore operations, and Box account statuses.......... 18
Installing the web application... 18
Installing the web application on WebSphere Application Server........... 18
Adding the Box certificate to WebSphere Application Server................. 19
Configuring subform... 20
Generating Box tokens.. 20
Installing the adapter language package.. 20
Verifying that the adapter is working correctly...................................... 20

Chapter 4. Upgrading.. 23
Upgrading the adapter binaries or connector... 23
Upgrading the adapter profile... 23

Chapter 5. Configuring.. 25
Customizing the adapter to support custom attributes........................... 25
Schema extensions and custom attributes.. 25
Copying the `BoxProfile.jar` file and extracting the files........................ 26
Modifying the assembly lines... 27
Updating the `schema.dsml` file... 29
Modifying the `CustomLabels.properties` file....................................... 30
Creating a JAR file and installing the new attributes.............................. 31
Adapter form modification (optional)... 31
Editing Box adapter profiles on the UNIX or Linux operating system........ 32
Modifying the maximum length of the account form attributes................ 33
Creating a JAR file and importing the profile.. 33

Chapter 6. Uninstalling... 35

Removing the adapter binaries or connector....35
Deleting the adapter profile....35

Chapter 7. Reference.... 37
Adapter-specific files....37
The `schema.dsml` file....37
`CustomLabels.properties` file....39
Adapter attributes....40
Attribute descriptions....40

Index.... 41

Tables

1. Prerequisites to install the adapter....................5

2. Box connector prerequisites.................... 6

3. Required information to install the adapter....................6

4. Adapter component.................... 10

5. Syntax tag data types and values.................... 39

6. Attributes for the erBoxAccount object class....................40

Chapter 1. Overview

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

Adapters can be on the managed resource. The Identity server manages access to the resource by using your security system.

Adapters function as trusted virtual administrators on the target operating system. They do tasks such as creating, suspending, and restoring user accounts, and other administrative functions that are done manually. The adapter runs as a service, independently of whether you are logged on to the Identity server.

The Box Adapter enables communication between the Identity server and the Box server.

Chapter 2. Planning

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

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

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

Pre-installation

Complete these tasks.

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

Installation

Complete these tasks.

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

Upgrade

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

Configuration

Complete these tasks.

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

Troubleshooting

See the following topics.

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

Uninstallation

Complete these tasks.

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

Reference

See the following topics.

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

Prerequisites

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

Table 1 on page 5 identifies the software and operating system prerequisites for the adapter installation.

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

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
Box API	Version 2.0
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. For more information, see the *Dispatcher Installation and Configuration Guide*.
A Box API user	A user must have admin privileges and a Box content application to generate valid tokens those are used to access the Box APIs. For more information about creating a Box application and generating the tokens, see the “OAuth2.0” section of the Box documentation online page.

The following table lists the requirements to run the Box connector.

Table 2. Box connector prerequisites

Requirement	Description	Task
Export and Import the SSL certificate	Export the SSL certificate from the managed resource and import it to the certificate authority (CA) certificates of the Security Directory Integrator Java virtual machine (JVM).	See "Exporting and importing the Box SSL certificate" on page 9.

Note: Set the environmental variable CLASSPATH to Java version 1.5 or later that is required for the adapter installation or upgrade.

For information about the prerequisites and supported operating systems for Security Directory Integrator, see the *IBM Security Directory Integrator 7.0: Administrator Guide*.

Software downloads

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

Go to IBM Passport Advantage.

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

Note:

You can also obtain additional adapter information from IBM Support.

Installation worksheet

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

Table 3. Required information to install the adapter

Required information	Description	Value

Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the `jars/connectors` subdirectory that contains adapter JAR files. For example, the `jars/connectors` subdirectory contains the JAR file for the UNIX adapter.	If Security Directory Integrator is automatically installed with your Identity server product, the default directory path for Security Directory Integrator is as follows:
		Windows:
		• For version 7.1.1:
		`*drive*\Program Files \IBM\TDI\V7.1.1`
		UNIX:
		• For version 7.1.1:
		`/opt/IBM/TDI/V7.1.1`

Table 3. Required information to install the adapter (continued)

Required information	Description	Value

Adapters solution directory	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 at:
		Windows:
		• For version 7.1.1:
		`drive\Program Files \IBM\TDI\V7.1.1\timsol`
		UNIX:
		• For version 7.1.1:
		`/opt/IBM/TDI/V7.1.1/timsol`

Chapter 3. Installing

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

All IBM Security Directory Integrator based adapters require the Dispatcher for the adapters to function correctly. If the Dispatcher is installed from a previous installation, do not reinstall it unless the Dispatcher is upgraded. See "Installing the dispatcher" on page 9.

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 installation is the first adapter installation that is based on the Security Directory Integrator, you must install the RMI Dispatcher before you install the adapter.

You must install the dispatcher on the same Security Directory Integrator server where you want to install the adapter.

Obtain the dispatcher installer from the IBM Passport Advantage website, http://ww.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm. For information about Dispatcher installation, see the *Dispatcher Installation and Configuration Guide*.

Exporting and importing the Box SSL certificate

To enable communication between the Box Adapter and the Box server, keystores must be configured for the RMI Dispatcher.

Procedure

1. Create a keystore that contains the Box SSL certificates as trusted certificate entries.

   Use Internet Explorer to download the Box server SSL certificate into the Windows certificate store from `https://app.box.com/`. View the certificate by double-clicking the **SSL lock** icon. If your browser reports that revocation information is not available, double-click **View Certificate**.
2. Click **Certification Path** and select the **CA Root** certificate.

   The Java™ keytool displays a confirmation that the certificate is added to the keystore.
3. Click **View Certificate**.
4. Click the **Details** tab and navigate to **Copy to File using the Base-64 encoded X.509 (.CER) format**.

   - If the RMI Dispatcher has the configured keystore, use the **`keytool.exe`** program to import the Box server certificate.
   - If the keystore is not configured, create a keystore. Issue the following command (as one line) from a command prompt:

     ```
     keytool -import -alias box -file
     c:\box.cer -keystore c:\truststore.jks -storepass passw0rd
     ```
5. Edit the *IDI_HOME*`/timsol/solution.properties` file to specify truststore and keystore information.

   In the current release, only `jks-type` is supported:

   ```
   # Keystore file information for the server authentication.
   # It is used to verify the server's public key.
   # example
   javax.net.ssl.trustStore=truststore.jks
   ```

```
javax.net.ssl.trustStorePassword=passw0rd
javax.net.ssl.trustStoreType=jks
```

Note: If these key properties are not configured, you can set the truststore to the same value that contains the Box server certificate. Otherwise, you must import the Box server certificate to the truststore specified in `javax.net.ssl.trustStore`.

6. Restart the adapter service.

What to do next

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

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.

About this task

If you are updating a previous installation, the adapter you want to update must exist. If it does not exist, the software generates the following message:

```
Adapter is not found at specified location.
Cannot perform Update Installation. Correct
the path of installed adapter or select Full Installation.
```

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 `BoxConnector.jar` file to the *ITDI_HOME*`/jars/connectors` directory.
4. Copy the `httpclient-4.0.1.jar` file to the *ITDI_HOME*`/jars/3rdparty/others` directory.
5. Restart the adapter service.

Verifying the adapter installation

If the adapter is installed correctly, adapter components exist in the specified directory.

Table 4. Adapter component

Adapter component	Directory
`BoxConnector.jar`	**On the Windows operating system** *drive*`:\Program Files\IBM\TDI\V7.1.1\jars\connectors\` **On the UNIX operating system** `/opt/IBM/TDI/V7.1.1/jars/connectors/`

Table 4. Adapter component (continued)

Adapter component	Directory
`httpclient-4.0.1.jar`	**On the Windows operating system** *drive*:\Program Files\IBM\TDI \V7.1.1\jars\3rdparty\others\ **On the UNIX operating system** /opt/IBM/TDI/V7.1.1/3rdparty/ others/

Review the installer log file, `Box_Installer.log`, that is in the adapter installer directory for any errors.

If this installation is to upgrade a connector, then send a request from IBM Security Verify Identity. Verify that the version number in the `ibmdi.log` matches the version of the connector that you installed. The `ibmdi.log` file is in the *ITDI_Home**adapter solution directory*\logs directory.

Restarting the adapter service

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

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

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

Importing the adapter profile

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

Before you begin

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

About this task

Service definition files are also called adapter profile files.

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

Procedure

1. Log on to the Identity server by using an account that has the authority to perform administrative tasks.
2. From the navigation tree, select **Configure System** > **Manage Service Types**.

   The **Manage Service Types** page is displayed.

3. On the **Manage Service Types** page, click **Import**.

   The **Import Service Type** page is displayed.

4. On the **Import Service Type** page, complete these steps:

   a) In the **Service Definition File** field, type the directory location of the *<Adapter>*`Profile.jar` file, or click **Browse** to locate the file.
   For example, if you are installing the IBM Security Verify Adapter for a Windows server that runs Active Directory, locate and import the `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. .

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.

Registering the API key

Register an API key by creating a content application for the adapter on the managed resource.

Note:

While you are configuring the Box content app, select the **Manage an enterprise** scope to perform enterprise management on users and groups by Box Adapter.

After you register, you must generate security tokens with client ID and client secret which can be obtained from the OAuth parameters section of the content application.

For more information about creating a Box application and generating tokens, see the "OAuth2.0" section of the Box documentation online page.

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 11.

About this task

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

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

Procedure

1. From the navigation tree, click **Manage Services**.

   The **Select a Service** page is displayed.
2. On the **Select a Service** page, click **Create**.

   The **Create a Service** wizard is displayed.
3. On the **Select the Type of Service** page, click **Search** to locate a business unit.

   The **Business Unit** page is displayed.
4. On the **Business Unit** page, complete these steps:

a) Type information about the business unit in the **Search information** field.

b) Select a business type from the **Search by** list, and then click **Search**.

A list of business units that matches the search criteria is displayed.

If the table contains multiple pages, you can do the following tasks:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

c) In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**.

The **Select the Type of Service** page is displayed, and the business unit that you specified is displayed in the **Business unit** field.

5. On the **Select the Type of Service** page, select a service type, and then click **Next**.

   If the table contains multiple pages, you can do the following tasks:

   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.
6. On either the **Service Information** or **General Information** page, specify the appropriate values for the service instance.

   The content of the **General Information** page depends on the type of service that you are creating. The creation of some services might require more steps.
7. To create a service with NTLM authentication, the administrator login is in the following format:

   ```
   <Domain Name>\<Login Name>
   ```
8. For NLTM authentication, select **Authentication** mode as 'Claims-Based Authentication.
9. On the **Dispatcher Attributes** page, specify information about the dispatcher attributes, and then click **Next** or **OK**.

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

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

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

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

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

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

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

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

Results

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

Service/Target form details

Complete the service/target form fields.

Connector Profile

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
Optionally, specify a description that identifies the service for your environment.

Security Directory Integrator location

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

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

Account Operations Settings
Define the behavior of account deletion and enable or disable the Suspend Account and Restore Account operations:

- Enable Suspend/Restore (Deleted accounts are reconciled as orphan accounts.)

  Select this option to enable the Suspend and Restore account operations. Suspended users are marked as “Inactive” on Box. At account deletion, the user is marked “Inactive” on Box; however, the adapter reconciles the user back as an Orphan Account.
- Disable Suspend/Restore (Accounts can be reactivated)

  Select this option to disable Suspend and Restore account operations. An error is returned when an account under the Box Service is submitted for restoration or suspension. Deleted accounts are not reconciled. If the account is deleted and is later re-created in the Identity server, it is restored from the Box by marking it as “Active” again.
- Disable Suspend/Restore (Accounts cannot be reactivated)

  This default option has behavior that is compatible with previous versions of the adapter. Accounts that are deleted cannot be restored. If the account is re-created later, it fails.

Owner
Optionally, specify a user as a service owner.

Service Prerequisite
Optionally, specify a service that is prerequisite to this service.

Connection

Box API URL

Specify the URL to access the Box API.

Specify `https://api.box.com/2.0` as the login URL.

Box API Login Email
Specify the login email that is used to log in to the resource and perform user management operations on the organization. Ensure that the user has API access privilege on Box.

Client ID

Specify the client ID of the Box Content Application that is associated with the login email.

Obtain the **`client_id`** from the OAuth2 parameters section of the Box Content Application.

Client Secret

Specify the client secret of the Box Content Application that is associated with the login email.

Obtain the **`client_secret`** from the OAuth2 parameters section of the Box Content Application.

Redirect URI

Specify the Redirect URI of the Box Content Application. The redirect URI is the URL within your application that receives the OAuth2 credentials.

Obtain the **`redirect_uri`** from the OAuth2 parameters section of the Box Content Application.

Note: For more information about Client ID, Client Secret, and Redirect URI, see the *"OAuth2.0"* section of the Box documentation online page.

Access Token

Specify the access token that is associate d with the Box Content Application.

To make Box API requests, a valid access token must be generated for the Box application.

Refresh Token

Specify the refresh token that is associated with the Box Content Application.

To regenerate an access token upon its expiration, a valid refresh token must be generated for the Box Application.

Note: For more information about generating an access token and refreshing a token, see the *"OAuth2.0"* section of the Box documentation online page.

Connector Filter Parameters

Limit

Optionally, specify a limit for the number of accounts to return for reconciliation. The minimum value is 0.

Note: Do not use characters or negative integers.

Offset

Optionally, specify the number corresponding to the position of an account. During reconciliation, the adapter retrieves the accounts from the specified position until the total number of accounts or until the account limit you specified. The minimum value is 0.

Note:

- Do not use characters or negative integers.
- Accounts are sorted by their creation date and time.

Filter Term

Optionally, specify one or more terms to filter the accounts to be processed for reconciliation. You can use the initial part of the username or login email as filter terms, to retrieve those criteria.

For multiple entries, separate the values with a comma. For example: `boxuser, adapteruser, example@box.com`

Dispatcher Attributes:

Disable AL Caching

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

AL FileSystem Path

Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines that are received from Identity server. For example, you can specify the following file path to load the assembly lines from the `profiles` directory of the Windows operating system: `c:\Program Files\IBM\TDI\V7.1.1\profiles` or you can specify the following file path to load the assembly lines from the `profiles` directory of the UNIX and Linux® operating: `system:/opt/IBM/TDI/V7.1.1/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 are run simultaneously for the service.

Status and information
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 to which the adapter is connected.

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 is 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.

Permissions for the /tmp directory

The permissions for the /tmp directory on the managed resource must be set to 777 when you do the reconciliation operation by using the sudo user.

Managing suspend, restore operations, and Box account statuses

This version of the adapter supports suspension and restoration of Box accounts.

About this task

Box has two additional account statues other than suspend and restore operations. The adapter supports the management of Box statuses but only when the account is active. If the account is suspended or inactive, you have to restore the account first to manage the rest of the statuses of the account.

If you update the account status while the account is in suspended or inactive state, the update is not reflected and warning messages are shown.

Procedure

1. Suspend and restore the account.

   Note: For more information, see the "Account Management" section of the IBM Security Verify Identity product documentation.
2. Select one of the following statuses in the **Account Status** menu to manage the Box account statuses:
   - **Cannot delete and edit**
   - **Cannot delete, edit, and upload**

   Note: Changes are not reflected when the account is in an inactive state.

Installing the web application

You must install the web application on the WebSphere® Application Server if you want to configure the application. This task involves adding the Box certificate to the server trustore, configuring a subform, and generating Box tokens.

Important: These set of tasks are:

- Not applicable in a virtual appliance deployment.
- Not required if you generated the tokens by using the information provided in *OAuth2.0* of the Box documentation at https://box-content.readme.io/docs/oauth-20

Installing the web application on WebSphere Application Server

Install the application on the WebSphere Application Server to associate libraries or configure the application properties file.

Before you begin

- Install the application on the WebSphere Application Server before you associate libraries or configure the application properties file.
- The **redirect_uri** of the Box content application must be the host name of the web application that is installed on the WebSphere Application Server.

Extract the content of the Box Adapter Installation package into a temporary directory.

Note: The extracted file name is `Adapter-Box-6.0.1-AI.zip`. Extract the zip file to obtain `BoxTokenGenerator.war`.

Procedure

1. Log on to the administrative console.
2. Click **Application** > **New Application**.
3. Select **New Enterprise Application** as the application type.
4. Specify the full path to the `BoxTokenGeneratorversion.war` file.
5. Click **Next**.
6. Select **Fast Path** installation.
7. Click **Next**.

   Note: Do **not** change the application name field. The name includes the version number. For example: `BoxTokenGenerator-6.0.1.war`
8. On the **Select Installation Options** page, accept all the default values.
9. On the **Map Modules to Server** page, accept all the default values.
10. On the **Map Context Roots for Web Modules** page, type **`/generatetokens`** as the context root.
11. Click **Next**.
12. Review the configuration summary and click **Finish** to begin the installation.

    Application BoxTokenGeneratorversion_war is displayed upon successful installation.
13. Click the **Save directly to master configuration** link.

What to do next

1. Add the Box signer certificate to the WebSphere Application Server keystores and certificates. See "Adding the Box certificate to WebSphere Application Server" on page 19
2. Configure the subform in Identity server. See "Configuring subform" on page 20
3. Generate Box tokens. See "Generating Box tokens" on page 20

Adding the Box certificate to WebSphere Application Server

Add the Box certificate to the truststore of the WebSphere Application Server to enable communication between the web component and the Box server.

Procedure

1. Log on to the WebSphere Application Server with an administrator account.
2. On the left pane, expand **Security** and click **SSL certificate and key management**.
3. On the **SSL certificate and key management** page, under **Related Items**, click **Keystores and certificates**.
4. On the **Keystores and certificates** page, click **NodeDefaultTrustStore**.
5. On the **NodeDefaultTrustStore** page, under **Additional Properties**, click **Signer certificates**.
6. On the **Signer certificates** page, click **Add** to add the Box certificate.
7. Specify box as the alias name.
8. Specify the path where `box.cer` is located. For example: `C:\Program Files\IBM\TDI\V7.1.1\timsol\serverapi\box.cer`
9. Specify `Base64-encoded ASCII data` as the data type.
10. Click **OK**.
11. Restart the WebSphere Application Server for the changes to take effect.

Configuring subform

Add a subform on the Boxservice form to communicate with the web application that is installed on WebSphere Application Server

Procedure

1. Extract the `subforms.zip` archive from the adapter package into temporary folder.
2. Copy the folder and the files in `subforms\box` to the `WEBSPHERE_HOME\AppServer \profiles \SERVER_NAME\installedApps\NODE_NAME\ITIM.ear\itim_console.war \subforms \box directory`.
3. Log on to the Identity server with an administrator account.
4. Click **Configure System** > **Design Forms**.
5. Double-click **Service** and then double-click the specific service.
6. Navigate to the **Connection** tab.
7. From the **Attribute List**, double-click `erboxgeneratortokens`.

   The attribute is displayed in the **Service** tab field on the design form.
8. Click **erboxgeneratortokens**.
9. Click **Attributes** > **Change to** > **Subform**.
10. In the **customServletURI** field, type `box/boxtokenmanage.jsp`.
11. Click **OK**.
12. Save the form template.

Generating Box tokens

Generate the Box tokens to access the Box API.

Procedure

1. In the Box Service form, navigate to the **Connection** tab.
2. Click on the **Generate Box Tokens Details** button.
3. Enter the Box administrator username and password.
4. Click **Authorize**.
5. On the **Grant Access** page, click on the **Grant access to Box** button.
6. On the **Generate Access Code** page, click on the **Generate** button within 30 seconds.
7. Click on **Copy Tokens** or take note of the token and enter it into the Box Service form.

Installing the adapter language package

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

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

Verifying that the adapter is working correctly

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

Procedure

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

5. Verify the `trace.log` file to ensure that no errors are reported when you run an adapter operation.

Chapter 4. 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 adapter binaries or connector

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

- If the connector version is higher or same as the previous version, the installer installs the new connector.
- If the connector version is lower than the existing connector version, the installer does not install the connector. A message is displayed indicating that no upgrade is required.

Note: Stop the dispatcher service before the upgrading the connector and start it again after the upgrade is complete.

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.

Chapter 5. Configuring

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

See the *IBM Security Dispatcher Installation and Configuration Guide* for more configuration options such as:

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

Customizing the adapter to support custom attributes

Use these tasks to configure the Box Adapter to support customized Box attributes.

Box supports custom fields for the user object. However, the Box Adapter supports only the standard set of attributes.

You can customize the adapter to support custom attributes. Complete the following tasks to customize the Box Adapter to support custom fields in Box.

Related concepts

Modifying the maximum length of the account form attributes
When you want to modify the maximum length of the attributes on the account form, modify the `schema.dsml` file with their required length.

Related tasks

Editing Box 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.

Creating a JAR file and importing the profile
After you modify the `schema.dsml` or any other profile files, you must import these files, into the Identity server for the changes to take effect.

Schema extensions and custom attributes

Use the interface and tools that are provided by Box to extend the Box User schema and add the custom attributes.

For more information about adding new attributes to the Box User schema, see the Box documentation.

The Box Adapter supports the following types of custom attributes:

- Boolean
- Integer
- Case-sensitive string
- Not case-sensitive string
- Coordinated Universal Time (UTC) coded time

Prefix the attribute names with `erBox` to easily identify the attributes that are used with IBM Security Verify Identity.

Note:

- If Security Directory Server is being used as the directory server application, the name of the attribute must be unique within the first 16 characters.
- The Box Adapter supports a multi-line value for custom attributes with string syntax.
- The custom attributes are supported for User account class only.

Related concepts

Adapter form modification (optional)
After the changes are available in the Identity server, you can modify the Box Adapter forms to use the new custom attributes.

Related tasks

Copying the BoxProfile.jar file and extracting the files
Use these tasks to customize your environment.

Modifying the assembly lines
Use this task to add new mappings to the assembly lines for custom attributes.

Updating the schema.dsml file
The Box Adapter `schema.dsml` file identifies all of the standard User account attributes. Modify this file to identify new custom attributes.

Modifying the CustomLabels.properties file
After you add the custom attributes to the `schema.dsml` file, the attributes are available for use on the Box Adapter form.

Creating a JAR file and installing the new attributes
You must import the modified assembly lines, `schema.dsml`, `CustomLabels.properties`, and any other files in the profile that were modified for the adapter. The changes do not take effect until after the files are imported into the Identity server.

Copying the `BoxProfile.jar` file and extracting the files

Use these tasks to customize your environment.

About this task

The profile JAR file, `BoxProfile.jar`, is included in the Box Adapter compressed file that you downloaded from the IBM website. The `BoxProfile.jar` file contains a folder named **BoxProfile** with the following files:

- `CustomLabels.properties`
- `erBoxAccount.xml`
- `erBoxService.xml`
- `schema.dsml`
- `service.def`
- `erBoxGroups.xml`
- `boxTest.xml`
- `boxRecon.xml`
- `boxAccountAdd.xml`
- `boxAccountModify.xml`
- `boxAccountDelete.xml`
- `boxAccountSuspend.xml`
- `boxAccountRestore.xml`
- `boxGroupModify.xml`
- `boxGroupDelete.xml`
- `boxGroupAdd.xml`

You can modify these files to customize your environment. When you finish updating the profile JAR file, rebuild the JAR file and install it on the IBM Security Verify Identity server.

Procedure

1. Log in to the system where the Box Adapter is installed.
2. On the **Start** menu, click **Programs** > **Accessories** > **Command Prompt**.
3. Copy the `BoxProfile.jar` file into a temporary directory.
4. Extract the contents of` the `BoxProfile.jar` file into the temporary directory.

   Run the following commands:

   ```
   cd c:\temp
   jar -xvf BoxProfile.jar
   ```

   The **`jar`** command creates the `c:\temp\BoxProfile` directory.

What to do next

Edit the appropriate files by completing the following tasks.

Related concepts

Schema extensions and custom attributes
Use the interface and tools that are provided by Box to extend the Box User schema and add the custom attributes.

Adapter form modification (optional)
After the changes are available in the Identity server, you can modify the Box Adapter forms to use the new custom attributes.

Related tasks

Modifying the assembly lines
Use this task to add new mappings to the assembly lines for custom attributes.

Updating the schema.dsml file
The Box Adapter `schema.dsml` file identifies all of the standard User account attributes. Modify this file to identify new custom attributes.

Modifying the CustomLabels.properties file
After you add the custom attributes to the `schema.dsml` file, the attributes are available for use on the Box Adapter form.

Creating a JAR file and installing the new attributes
You must import the modified assembly lines, `schema.dsml`, `CustomLabels.properties`, and any other files in the profile that were modified for the adapter. The changes do not take effect until after the files are imported into the Identity server.

Modifying the assembly lines

Use this task to add new mappings to the assembly lines for custom attributes.

About this task

The Box Adapter uses Security Directory Integrator to process requests before you submit them to Box.

The Box assembly lines contain mapping instructions from a IBM Security Verify Identity request to Box. Modify the assembly lines to add new mappings for custom attributes.

Procedure

1. Start the Security Directory Integrator Configuration Editor.
2. Open the `boxAdd.xml` file. Click **File** > **Open** Security Directory Integrator **Configuration File...**.
   a) Browse to the `BoxProfile` directory.

   b) Select the `boxAdd.xml` file.
3. Optional: If previously edited, assign this configuration file to an existing project. Otherwise, proceed to the next screen to create a project and name it `BoxProfile`.
4. After the file is imported, expand the project to display the **AssemblyLines** tree in the Navigator pane.
5. Right click **boxAccountAdd assemblyline** and select **Open**. The **Add assemblyline** configuration is displayed in the main panel.
6. Click **Show Mapping** in the main panel. The mapping table for the assembly line is displayed in the main panel.
7. Locate the **AddUser** section and left click to select it in the table.
8. Click **Map** to display the Add attribute dialog.
9. Enter the name of the custom field exactly as displayed in the API Name on Box.
   For example, `Custom1__c`.
10. After the field is added, locate it in the mapping table and double-click the corresponding row to display an edit dialog.
11. Change the default value of `work.[custom field name]` to `work.[custom attribute name]`.
    For example, change `work.Custom1__c` to `work.erBoxCustom1__c`.
12. Save the changes. Click **File** > **Save**.
13. Right click the project in the Navigator pane and select the **Export...** option to export the new assembly line.
14. In the first screen of the **Export** dialog, expand the IBM Security Directory Integrator folder and select **Runtime Configuration**.
15. Click **Next**.
16. In the file path field, browse to the `BoxProfile` directory and select the file with the same name from step 2 to overwrite it.
17. Click **Finish**.
18. Repeat the steps 5 through 17 for the Modify assembly line.
19. Repeat steps 5 through 17 for the Recon assembly line and do the following steps instead of steps 10 and 11:

    a) Locate the field in the mapping table and click the **Work Attribute** cell corresponding to the custom field to rename it.

    b) Enter the attribute name that is specified previously in step 11.
    For example, `erBoxCustom1__c`.

Related concepts

Schema extensions and custom attributes
Use the interface and tools that are provided by Box to extend the Box User schema and add the custom attributes.

Adapter form modification (optional)
After the changes are available in the Identity server, you can modify the Box Adapter forms to use the new custom attributes.

Related tasks

Copying the BoxProfile.jar file and extracting the files
Use these tasks to customize your environment.

Updating the schema.dsml file
The Box Adapter `schema.dsml` file identifies all of the standard User account attributes. Modify this file to identify new custom attributes.

Modifying the CustomLabels.properties file
After you add the custom attributes to the `schema.dsml` file, the attributes are available for use on the Box Adapter form.

Creating a JAR file and installing the new attributes

You must import the modified assembly lines, `schema.dsml`, `CustomLabels.properties`, and any other files in the profile that were modified for the adapter. The changes do not take effect until after the files are imported into the Identity server.

Updating the `schema.dsml` file

The Box Adapter `schema.dsml` file identifies all of the standard User account attributes. Modify this file to identify new custom attributes.

About this task

For more information about the attributes in this file, see "The schema.dsml file" on page 37.

Procedure

1. Locate the `schema.dsml` file in the `\BoxProfile` directory.
2. Edit the `schema.dsml` file to add an attribute definition for each custom attribute.

   The Object Identifier (OID) is increased by 1, based on the last entry in the file.

   For example, if the last attribute in the file uses the OID 1.3.6.1.4.1.6054.3.176.2.47, the first new attribute uses the OID 1.3.6.1.4.1.6054.3.176.2.48.

   You might want to start a new range of numbers for your custom attributes. For example, start custom attributes with OID 11.3.6.1.4.1.6054.3.176.2.1000. This range prevents duplicate OIDs if the adapter is upgraded to support new attributes that are standard for newer versions of Box API.
3. Add each of the new attributes to the account class.
   For example, add the following attribute definition under the erBoxAccount section of the `schema.dsml` file:

   ```
   <attribute ref="erBoxCustom1__c" required="false"/>
   ```
4. Save the file when you are finished.

Related concepts

Schema extensions and custom attributes
Use the interface and tools that are provided by Box to extend the Box User schema and add the custom attributes.

Adapter form modification (optional)
After the changes are available in the Identity server, you can modify the Box Adapter forms to use the new custom attributes.

Related tasks

Copying the BoxProfile.jar file and extracting the files
Use these tasks to customize your environment.

Modifying the assembly lines
Use this task to add new mappings to the assembly lines for custom attributes.

Modifying the CustomLabels.properties file
After you add the custom attributes to the `schema.dsml` file, the attributes are available for use on the Box Adapter form.

Creating a JAR file and installing the new attributes

You must import the modified assembly lines, `schema.dsml`, `CustomLabels.properties`, and any other files in the profile that were modified for the adapter. The changes do not take effect until after the files are imported into the Identity server.

Modifying the `CustomLabels.properties` file

After you add the custom attributes to the `schema.dsml` file, the attributes are available for use on the Box Adapter form.

About this task

The attributes are displayed in the attribute list for the account form. You can modify the attribute names that are in the attribute list. See "CustomLabels.properties file" on page 39.

To add the attribute and its corresponding label to the `CustomLabels.properties` file, complete the following steps:

Procedure

1. Locate the `CustomLabels.properties` file in the `\BoxProfile` directory.
2. Edit the `CustomLabels.properties` file to add the attribute and its corresponding label.

   Use the following format:

   ```
   attribute=label
   ```

   Note: The attribute name must be in lowercase. For example:

   ```
   #
   Adapter Labels definitions
   #
   erboxcustom1__c=Custom Field One
   erboxcustom2__c=Custom Attribute Field Two
   ```
3. Save the file when you are finished.

Related concepts

Schema extensions and custom attributes
Use the interface and tools that are provided by Box to extend the Box User schema and add the custom attributes.

Adapter form modification (optional)
After the changes are available in the Identity server, you can modify the Box Adapter forms to use the new custom attributes.

Related tasks

Copying the BoxProfile.jar file and extracting the files
Use these tasks to customize your environment.

Modifying the assembly lines
Use this task to add new mappings to the assembly lines for custom attributes.

Updating the schema.dsml file
The Box Adapter `schema.dsml` file identifies all of the standard User account attributes. Modify this file to identify new custom attributes.

Creating a JAR file and installing the new attributes

You must import the modified assembly lines, schema.dsml, CustomLabels.properties, and any other files in the profile that were modified for the adapter. The changes do not take effect until after the files are imported into the Identity server.

Creating a JAR file and installing the new attributes

You must import the modified assembly lines, schema.dsml, CustomLabels.properties, and any other files in the profile that were modified for the adapter. The changes do not take effect until after the files are imported into the Identity server.

Procedure

1. Create a JAR file by using the files in the \temp directory.

   Run the following commands:

   ```
   cd c:\temp
   jar -cvf BoxProfile.jar BoxProfile
   ```

2. Import the BoxProfile.jar file into the Identity server.
3. Start and stop the Identity server.

   Note: If you are upgrading an existing adapter profile, the new adapter profile schema is not reflected immediately. You must stop and start the IBM Security Verify Identity server to refresh the cache and the adapter schema. See Chapter 4, “Upgrading,” on page 23.

Related concepts

Schema extensions and custom attributes
Use the interface and tools that are provided by Box to extend the Box User schema and add the custom attributes.

Adapter form modification (optional)
After the changes are available in the Identity server, you can modify the Box Adapter forms to use the new custom attributes.

Related tasks

Copying the BoxProfile.jar file and extracting the files
Use these tasks to customize your environment.

Modifying the assembly lines
Use this task to add new mappings to the assembly lines for custom attributes.

Updating the schema.dsml file
The Box Adapter schema.dsml file identifies all of the standard User account attributes. Modify this file to identify new custom attributes.

Modifying the CustomLabels.properties file
After you add the custom attributes to the schema.dsml file, the attributes are available for use on the Box Adapter form.

Adapter form modification (optional)

After the changes are available in the Identity server, you can modify the Box Adapter forms to use the new custom attributes.

You do not have to add the attributes to the Box Adapter form unless you want them to be available. The attributes are returned during reconciliations unless you explicitly exclude them.

For more information about modifying the adapter form, see the IBM Security Verify Identity product documentation.

Related concepts

Schema extensions and custom attributes

Use the interface and tools that are provided by Box to extend the Box User schema and add the custom attributes.

Related tasks

Copying the BoxProfile.jar file and extracting the files
Use these tasks to customize your environment.

Modifying the assembly lines
Use this task to add new mappings to the assembly lines for custom attributes.

Updating the schema.dsml file
The Box Adapter `schema.dsml` file identifies all of the standard User account attributes. Modify this file to identify new custom attributes.

Modifying the CustomLabels.properties file
After you add the custom attributes to the `schema.dsml` file, the attributes are available for use on the Box Adapter form.

Creating a JAR file and installing the new attributes
You must import the modified assembly lines, `schema.dsml`, `CustomLabels.properties`, and any other files in the profile that were modified for the adapter. The changes do not take effect until after the files are imported into the Identity server.

Editing Box 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

Customizing the adapter to support custom attributes
Use these tasks to configure the Box Adapter to support customized Box attributes.

Modifying the maximum length of the account form attributes
When you want to modify the maximum length of the attributes on the account form, modify the `schema.dsml` file with their required length.

Related tasks

Creating a JAR file and importing the profile

After you modify the schema.dsml or any other profile files, you must import these files, into the Identity server for the changes to take effect.

Modifying the maximum length of the account form attributes

When you want to modify the maximum length of the attributes on the account form, modify the schema.dsml file with their required length.

For example, when you want 2048 as the maximum length of the **First Name** attribute, modify the schema.dsml file as:

```
Old profile:

<!-- ******************************************************** -->
<!-- erRsaAmFirstName -->
<!-- ******************************************************** -->
<attribute-type single-value = "true" >
    <name>erRsaAmFirstName</name>
    <description>First Name</description>
    <object-identifier>1.3.6.1.4.1.6054.3.150.2.1</object-identifier>
    <syntax>1.3.6.1.4.1.1466.115.121.1.15{1024}</syntax>
</attribute-type>

Modified profile:

<!-- ******************************************************** -->
<!-- erRsaAmFirstName -->
<!-- ******************************************************** -->
<attribute-type single-value = "true" >
    <name>erRsaAmFirstName</name>
    <description>First Name</description>
    <object-identifier>1.3.6.1.4.1.6054.3.150.2.1</object-identifier>
    <syntax>1.3.6.1.4.1.1466.115.121.1.15{2048}</syntax>
</attribute-type>
```

Related concepts

Customizing the adapter to support custom attributes
Use these tasks to configure the Box Adapter to support customized Box attributes.

Related tasks

Editing Box 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.

Creating a JAR file and importing the profile
After you modify the schema.dsml or any other profile files, you must import these files, into the Identity server for the changes to take effect.

Creating a JAR file and importing the profile

After you modify the schema.dsml or any other profile files, you must import these files, into the Identity server for the changes to take effect.

About this task

Note: If you are upgrading an existing adapter profile, the new adapter profile schema is not reflected immediately. You must stop and start the Identity server to refresh the cache and the adapter schema. For more information about upgrading an existing adapter, see Chapter 4, “Upgrading,” on page 23.

Procedure

1. Extract the contents of the BoxProfile.jar file into the temporary directory by running the following command:

   ```
   cd c:\temp
   jar -xvf BoxProfile.jar
   ```

The **jar** command creates the `c:\temp\BoxProfile` directory.

2. Update the profile files.
3. Create a JAR file with the files in the `\temp` directory by running the following commands:

```
cd c:\temp
jar -cvf BoxProfile.jar BoxProfile
```

4. Import the `BoxProfile.jar` file into the Identity server.
5. Stop and start the Identity server.

Related concepts

Customizing the adapter to support custom attributes
Use these tasks to configure the Box Adapter to support customized Box attributes.

Modifying the maximum length of the account form attributes
When you want to modify the maximum length of the attributes on the account form, modify the `schema.dsml` file with their required length.

Related tasks

Editing Box 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.

Chapter 6. Uninstalling

To remove an adapter from the Identity server for any reason, you must remove all the components that were added during installation. 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.

Removing the adapter binaries or connector

The Box Adapter installation installs the Security Directory Integrator Box connector.

About this task

To uninstall the Dispatcher, see the *Dispatcher Installation and Configuration Guide*.

Procedure

1. Stop the Dispatcher service.
2. Remove the `BoxConnector.jar` file from *`ITDI_HOME`*`/jars/connectors` directory.
3. Remove the Box folder which contains the `boxConfig.properties` file from `ITDI_HOME/timsol/`
4. Start the Dispatcher service.

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 7. Reference

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

Files

You can configure several adapter-specific files that are associated with the Box Adapter.

- “The schema.dsml file” on page 37
- “CustomLabels.properties file” on page 39

The `schema.dsml` file

The `schema.dsml` file contains all of the attributes that are common to all adapters. This common file also contains IBM Security Verify Identity server attributes that can be used by any adapter. The `schema.dsml` file defines all of the classes that are used by the adapter. The classes are used to declare accounts, services, and supporting data.

The `schema.dsml` file defines the attributes and objects that the adapter supports and uses to communicate with the IBM Security Verify Identity server. All attributes must be unique. Therefore, they are assigned an object identifier (OID).

The OID is defined with the `<object-identifier>...</object-identifier>`

The `schema.dsml` file has the following format:

```
SCHEMA.DSML File<?xml version="1.0" encoding="UTF-8"?>
<dsml>
<!-- ******************************************************** -->
<!-- Schema supported by the Box Adapter. -->
<!-- ******************************************************** -->
<directory-schema> ...
<!-- ******************************************************** -->
<!-- erBoxString1-->
<!-- ******************************************************** -->
<attribute-type single-value="true">
<name>erBoxString1</name>
<description/>
<object-identifier>1.3.6.1.4.1.6054.3.176.2.100</object-identifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
</attribute-type>
<!-- ******************************************************** -->
<!-- erBoxInteger-->
<!-- ******************************************************** -->
<attribute-type single-value="true">
<name>erBoxInteger</name>
<description/>
<object-identifier>1.3.6.1.4.1.6054.3.176.2.101</object-identifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.27</syntax>
</attribute-type>
<!-- ******************************************************** -->
<!-- erBoxDate-->
<!-- ******************************************************** -->
<attribute-type single-value="true">
<name>erBoxDate</name>
<description/>
<object-identifier>1.3.6.1.4.1.6054.3.176.2.102</object-identifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.24</syntax>
</attribute-type>
<!-- ******************************************************** -->
<!-- erBoxBoolean-->
<!-- ******************************************************** -->
<attribute-type single-value="true">
<name>erBoxBoolean</name>
<description/>
<object-identifier>1.3.6.1.4.1.6054.3.176.2.103</object-identifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.7</syntax>
</attribute-type>
```

```
<!-- ******************************************************** -->
<!-- erBoxMultiValueString-->
<!-- ******************************************************** -->
<attribute-type>
<name>erBoxMultiValueString</name>
<description>List of string values</description>
<object-identifier>1.3.6.1.4.1.6054.3.176.2.104</object-identifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
</attribute-type> ...
<!-- ******************************************************** -->
<!-- erBoxUserAccount Class -->
<!-- ******************************************************** -->
<class superior="top">
<name>erBoxUserAccount</name>
<description>Class representing a Box account.</description> ...
<object-identifier>1.3.6.1.4.1.6054.3.176.1.1</object-identifier>
<attribute ref="erBoxBoolean" required="false"/>
<attribute ref="erBoxDate" required="false"/>
<attribute ref="erBoxInteger" required="false"/>
<attribute ref="erBoxMultiValueString" required="false"/>
<attribute ref="erBoxString1" required="false"/>
</class> ...
</directory-schema>
</dsml>
```

Object identifier

The Identity server uses LDAP directory services to add, delete, modify, and search IBM Security Verify Identity data. Each data item in an LDAP directory server must have a unique object identifier (OID). Therefore, each attribute and class that is defined in the `schema.dsml` file in IBM Security Verify Identity has an OID.

OIDs have the following syntax:

```
enterprise ID.product ID.adapter ID.object ID.instance ID
```

- The *enterprise ID* is always 1.3.6.1.4.1.6054 for IBM.
- The *product ID* is always 3 because these `schema.dsml` files are used with adapters.
- The *adapter ID* is 176 for the Box Adapter.
- The *object ID* is 2. An attribute uses 2 as the object ID.
- The *instance ID* is a sequential number of the object.

Attribute definition

Before you define unique attributes for the adapter, ensure that the attribute does not exist in the common `schema.dsml` file.

The following example defines an attribute:

```
<!-- *********************************************** -->
<!-- erSampleHome -->
<!-- *********************************************** -->
<attribute-type single-value = "true" >
<name>erSampleHome</name>
<description>User home directory</description>
<object-identifier>1.3.6.1.4.1.6054.3.125.2.100</object-identifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
</attribute-type>
```

Comment lines are denoted by the `<!-- ... -->` markers

The attribute type is defined as single-value or multi-value. A single-value attribute is denoted by the line: `<attribute-type single-value ="true">`. To denote a multi-valued attribute, change the `true` value to `false`.

The name of the attribute that is used by the Identity server is defined in the schema. To simplify the tracking of new Box Adapter attributes, use `erBox` as the preface for all new attributes.

The description of the attribute is denoted by the line: `<description>...</description>` tag.

The OID is defined by the `<object-identifier>...</object-identifier>` tag. Because OIDs are already assigned to the existing, standard attributes, the OID can be copied from the last attribute in the list. However, the last number must be incremented by one for each new attribute that you add to the `schema.dsml` file.

The data type is defined with the `<syntax>...</syntax>` tag. The following table lists various data types and the value you specify in the syntax tags.

Table 5. Syntax tag data types and values

Data type	Value
Bit string	1.3.6.1.4.1.1466.115.121.1.6
Boolean	1.3.6.1.4.1.1466.115.121.1.7
Directory string	1.3.6.1.4.1.1466.115.121.1.15
UTC coded time	1.3.6.1.4.1.1466.115.121.1.24
Integer	1.3.6.1.4.1.1466.115.121.1.27

Classes

At least one account class and one service class must be defined in the `schema.dsml` file.

Each class requires at least one attribute to identify the class: a name attribute. More attributes might be required depending on the class that is defined.

The following syntax defines a class:

```
<class superior="top">
<name> ... </name>
<description> ... </description>
<object-identifier> ... </object-identifier>
<attribute ref = "..." required = "true" />
<attribute ref = "..." required = "true" />
</class>
```

To make an attribute optional for a class, change `required = "true"` to `required = "false"` in the <attribute ref> tag.

An account class defines the attributes that are used to describe an account. An account class must be defined in the `schema.dsml` file.

The following example defines an account class:

```
<class superior="top" >
<name>erSampleAccount</name>
<description>Sample Account</description>
<object-identifier>1.3.6.1.4.1.6054.3.125.1.101</object-identifier>
<attribute ref = "eruid" required = "true" />
<attribute ref = "erAccountStatus" required = "false" />
<attribute ref = "erSampleGroups" required = "false" />
<attribute ref = "erSampleHome" required = "false" />
<attribute ref = "erSampleDesc" required = "false" />
<attribute ref = "erPassword" required = "false" />
</class>
```

In the preceding example, the class name is erSampleAccount and the only required attribute is eruid. However, erAccountStatus is a required attribute to suspend or restore accounts.

`CustomLabels.properties` file

The `CustomLabels.properties` file is a text file that defines the labels on the form for the adapter.

Use this syntax for the information in the file:

```
attribute=text
```

where:

- *attribute* is the same attribute that is defined in the `schema.dsml` file.
- *text* is the label that is on the form in the IBM Security Verify Identity user interface for the account.

The value of *attribute* must be in lowercase. This requirement is from the Identity server.

Adapter attributes

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

As part of the adapter implementation, a dedicated account for IBM Security Verify Identity to access the Box is created on the Box. The adapter consists of files and directories that are owned by the IBM Security Verify Identity account. These files establish communication with the Identity server.

Attribute descriptions

The Identity server communicates with the Box Adapter with attributes that are included in transmission packets that are sent over a network.

The combination of attributes, included in the packets, depends on the type of action that the Identity server requests from the Box Adapter.

Table 6 on page 40 lists the attributes that are used by the Box Adapter. The table provides a description and the corresponding values of the attribute.

Use this key for the permissions column.

```
R = Read only
RW = Add, read, modify, write
AR = Add, Read
```

Table 6. Attributes for the erBoxAccount object class

Attribute name and definition	Data type	Single-valued	Permissions	Required
erBoxAddress	String	Yes	RW	No
erBoxAvatarUrl	String	Yes	RW	No
erBoxCanSeeManagedUsers	Boolean	Yes	RW	No
erBoxGroupId	String	No	RW	No
erBoxGroupMemberId	String	No	RW	No
erBoxIsExemptFromDeviceLimits	Boolean	Yes	RW	No
erBoxIsExternalCollabRestricted	Boolean	Yes	RW	No
erBoxIsSyncEnabled	Boolean	Yes	RW	No
erBoxLanguage	Picklist	Yes	RW	No
erBoxPhone	String	Yes	RW	No
erBoxSpaceAmount	Integer	Yes	RW	No
erBoxSpaceUsed	Integer	Yes	R	No
erBoxStatus	Picklist	Yes	RW	No
erBoxUserId	String	Yes	R	Yes
erBoxUserName	String	Yes	RW	Yes
eruid	String	Yes	R	Yes

Index

A

adapter
  attributes
    descriptions 40
  installation
    verifying 20
  installation worksheet 6
  profile
    upgrading 23
  uninstall 35
adapter form
  modifying 31
adapter installation
  verifying 10
adapter overview 1
adapters
  removing profiles 35
attribute
  classes 39
attributes
  customizing 25
  defining 38
  definitions
    attributes 38
  descriptions 40
  installing on server 31
  modifying the adapter form 31
  names and descriptions 40
  object identifier 38

B

box SSL certificate
  exporting 9
  importing 9

C

classes
  attributes 39
connector
  installing 10
connectors
  upgrading 23
custom attributes
  modifying CustomLabels.properties 30
  updating schema.dsml file 29
customizing attributes 25
CustomLabels.properties
  modifying 30

D

download, software 6

F

files
  BoxProfile.jar 26
  CustomLabels.properties 30, 39
  JAR 31
  schema.dsml 29, 37

I

installation
  adapter 9
  connector 10
  language pack 20
  uninstall 35
  verification
    adapter 20
  verify 10
  worksheet 6

J

JAR files
  creating 31
  extracting files 26

L

language pack
  installation 20
  same for adapters and server 20

M

MS-DOS ASCII characters 32

O

object identifier 38
OID 38
operating system prerequisites 4
overview
  adapter 1

P

profile
  editing on UNIX or Linux 32

R

removing
  adapter profiles 35

S

schema.dsml
- updating 29

service
- restart 11
- start 11
- stop 11

software
- download 6
- website 6

software requirements 4

SSL certificate
- box 9

U

uninstallation 35

uninstalling the adapter 35

upgrade
- connectors 23

upgrades
- adapter profiles 23

V

verification
- installation 20
- operating system prerequisites 4
- operating system requirements 4
- software prerequisites 4
- software requirements 4

vi command 32

IBM®