Connector Administration

Oracle Consulting

Oracle® Identity Manager Connector Guide for Generic Web Service Release 1.0.0

Author: Dieter Steding

Creation Date: 27-10-2019

Latest Update: 08-08-2020

Control Number: OC\_DE/300194912/DO.081/001

Version: 1.0

**Approval:**

|  |  |
| --- | --- |
| Customer |  |
| Oracle Consulting |  |

logored Copy-No. \_\_\_\_\_

## Document Control

### Change Record

| Date | Author | Version | | Change Reference |
| --- | --- | --- | --- | --- |
|  |  |  |  | |
| 27-10-19 |  | 1.0 | No previous document | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |

### Reviewer

| Name | Position |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

### Distribution

| Copy No. | Name | Location |
| --- | --- | --- |
|  |  |  |
| 1 | Library Master | Project Library |
| 2 |  | Project Manager |
| 3 |  |  |
| 4 |  |  |

Table of Contents

[Document Control ii](#_Toc54931245)

[Change Record ii](#_Toc54931246)

[Reviewer ii](#_Toc54931247)

[Distribution ii](#_Toc54931248)

[Preface 1](#_Toc54931249)

[Audience 1](#_Toc54931250)

[Related Documents 1](#_Toc54931251)

[Confidentiality 1](#_Toc54931252)

[Typographical Conventions 1](#_Toc54931253)

[About the Connector 2](#_Toc54931254)

[Introduction to the Generic SCIM Connector 2](#_Toc54931255)

[Deployment Configurations 3](#_Toc54931256)

[Languages 3](#_Toc54931257)

[Architecture of the Generic SCIM Connector 3](#_Toc54931258)

[Use Cases Supported by the Generic SCIM Connector 4](#_Toc54931259)

[Features of the Generic SCIM Connector 5](#_Toc54931260)

[Support for Both Trusted Source and Target Resource Reconciliation 5](#_Toc54931261)

[Full and Incremental Reconciliation 6](#_Toc54931262)

[Limited (Filtered) Reconciliation 6](#_Toc54931263)

[Custom Authentication 6](#_Toc54931264)

[Custom Parsing 6](#_Toc54931265)

[Custom Payload 6](#_Toc54931266)

[Support for Additional HTTP Headers 6](#_Toc54931267)

[Support for Handling Multiple Endpoint URLs 7](#_Toc54931268)

[SSL Communication 7](#_Toc54931269)

[Roadmap for Generating and Using the Connector 7](#_Toc54931270)

[Installing and Configuring the Generic SCIM Connector 8](#_Toc54931271)

[Preinstallation 8](#_Toc54931272)

[Implementing Custom Authentication 8](#_Toc54931273)

[Implementing Custom Parsing 8](#_Toc54931274)

[Installing the Generic SCIM Connector 8](#_Toc54931275)

[Understanding Installation of the Generic SCIM Connector 9](#_Toc54931276)

[Running the Connector Installer 9](#_Toc54931277)

[Configuring the IT Resource for the Target System 10](#_Toc54931278)

[Post installation 14](#_Toc54931279)

[Configuring Oracle Identity Manager 14](#_Toc54931280)

[Localizing Field Labels in UI Forms 14](#_Toc54931281)

[Clearing Content Related to Connector Resource Bundles from the Server Cache 14](#_Toc54931282)

[Managing Logging for the Generic SCIM Connector 14](#_Toc54931283)

[Configuring SSL for the Generic SCIM Connector 14](#_Toc54931284)

[Deploying the Connector 15](#_Toc54931285)

[Configure Connector Server 15](#_Toc54931286)

[SCIM filter language 16](#_Toc54931287)

[Logical Operators 16](#_Toc54931288)

[Grouping Operators 16](#_Toc54931289)

[Attribute Operators 16](#_Toc54931290)

## Preface

### Audience

This guide is intended for resource administrators and target system integration teams.

### Related Documents

For information about installing and using Oracle Identity and Access Management, visit the following [Oracle Help Center](https://docs.oracle.com/cd/E52734_01/index.html) page:

* https://docs.oracle.com/en/middleware/idm/suite/12.2.1.3/index.html

For information about Oracle Identity Manager Connector’s documentation, visit the following Oracle Help Center page:

1. http://docs.oracle.com/cd/E52734\_01/index.html

### Confidentiality

The material contained in this documentation represents proprietary, confidential information pertaining to Oracle products and methods.

The audience agrees that the information in this documentation shall not be disclosed outside of Oracle, and shall not be duplicated, used, or disclosed for any purpose other than to evaluate this procedure.

### Typographical Conventions

The following typographical conventions are used in this document.

|  |  |
| --- | --- |
| **Convention** | **Meaning** |
| **boldface** | Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary. |
| *italic* | Italic type indicates book titles, emphasis, or. |
| monospace | Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter. |

## About the Connector

The Oracle Identity Manager Connector for Generic SCIM (Generic SCIM connector) integrates Oracle Identity Manager with SCIM -based target systems.

Oracle Identity Manager is a centralized identity management solution that provides self-service, compliance, provisioning and password management services for applications residing on-premise or on the Cloud. Oracle Identity Manager connects users to resources, and revokes and restricts unauthorized access to protect sensitive corporate information. Oracle Identity Manager Connectors are used to integrate Oracle Identity Manager with external and identity-aware applications such as PeopleSoft and MySQL.

The following topics introduce the Generic SCIM connector:

1. Introduction to the Generic SCIM Connector
2. Deployment Configurations
3. Languages
4. Architecture of the Generic SCIM Connector
5. Use Cases Supported by the Generic SCIM Connector
6. Features of the Generic SCIM Connector
7. Roadmap for Generating and Using the Connector

### Introduction to the Generic SCIM Connector

The Generic SCIM connector is a solution to integrate Oracle Identity Manager with SCIM-based identity-aware applications. A SCIM-based identity-aware application is any application that exposes its SCIM APIs or interfaces for identity management.

| D:\tt\icon-note-16.png | Note: |
| --- | --- |
| In this guide:   1. A SCIM-based identity-aware application has been referred to as the target system or SCIM-based target system. 2. RELEASE\_NUMBER has been used as a placeholder for the current release number of the connector. Therefore, replace all instances of RELEASE\_NUMBER with the release number of the connector. For example, 11.1.1. 3. The Oracle Identity Manager Connector for Generic SCIM has been referred to as the Generic SCIM connector. |

The Generic SCIM connector provides a centralized system to streamline delivery of services and assets to your company’s consumers, manage those services and assets in a simple, secure, and cost efficient manner by using automation. The Generic SCIM connector standardizes service processes and implements automation to replace manual tasks.

In order to connect with a SCIM-based target system, the Generic SCIM connector supports HTTP Basic Authentication and OAuth 2.0 authentication mechanisms. This connector also supports authenticating to the target system by using access token and refresh token as an input from the user. This authentication mechanism can be useful if your target system does not provide a programmatic approach to obtain access or refresh tokens.

The connector supports the following OAuth 2.0 grant types:

1. JWT
2. Client Credentials
3. Resource Owner Password

If your target system does not support any of the authentication types supported by this connector, then you can implement the custom authentication that your target system supports. You can connect this custom implementation to the connector by using the plug-ins exposed by this connector.

The Generic SCIM connector synchronizes data between Oracle Identity Manager and SCIM-based target systems by performing reconciliation and provisioning operations that parse data in the JSON format. If your target system does not support request or response payload in JSON format, then you can create your own implementation for parsing data. You can connect this custom implementation to the connector by using the plug-ins exposed by this connector.

The Generic SCIM connector is a connector for a discovered target system. This is because the schema of the SCIM-based target system with which the connector integrates is not known in advance. The Generic SCIM connector is not shipped with any artifacts. Instead, it is shipped with a set of deployment utilities that help in discovering the schema of the SCIM-based target system and generating the artifacts.

### Deployment Configurations

These are the software components and their versions required for integrating Oracle Identity Manager with a Generic SCIM connector.

| **System** | **Requirement** |
| --- | --- |
| **Oracle Identity Manager** | You can use one of the following releases of Oracle Identity Manager:  Oracle Identity Governance 12c (12.2.1.3.0) |
| **Target System** | Any target system that supports SCIM-based services. |
| **Connector Server** | 12.2.1.3.0 |
| **Connector Server JDK** | JDK 1.8 or later |

### Languages

The connector supports these languages.

1. English (US)
2. German

### Architecture of the Generic SCIM Connector

The Generic SCIM connector is implemented using the Identity Connector Framework (ICF).

The ICF is a component that provides basic reconciliation and provisioning operations that are common to all Oracle Identity Manager Connectors. In addition, ICF provides common features that developers would otherwise need to implement on their own, such as connection pooling, buffering, time outs, and filtering. The ICF is shipped along with Oracle Identity Manager.

The Generic SCIM connector is not shipped with any metadata, as it is a connector for target system that is not known in advance. Depending on the schema of your target system, the connector artifacts are generated during connector deployment.

The following is a high-level description of the stages into which the connector deployment and usage procedure is divided into:

1. **Generating the Connector**  
   The Generic SCIM connector includes a groovy file in which you can specify information about your target system. This information is used by the metadata generator, one of the deployment utilities shipped with the connector, to generate the connector based on the target system schema.  
     
   When you run the metadata generator on the groovy file, the connector package is generated. This package contains an XML file that contains definitions for connector components such as adapters, process tasks, scheduled tasks, lookup definitions, and IT resource. Connector operations such as provisioning and reconciliation are performed using these connector components. Along with the XML file, a schema file is included.
2. **Installing and configuring the connector**  
   In this stage, you install the generated connector by running the connector installer and then perform configuration tasks such as configuring the IT resource, enabling logging and so on.
3. **Using the Connector**  
   In this stage, you start using the connector to perform connector operations such as reconciliation and provisioning.

### Use Cases Supported by the Generic SCIM Connector

The Generic SCIM connector can be used to integrate OIM with any target system that supports SCIM services. This connector can be used to load identity data into OIM from a SCIM service and then efficiently manage identities in an integrated cycle with the rest of the identity-aware applications in your enterprise.

Oracle Identity Manager Connector for Generic SCIM, with a few simple configurations, provides a reusable framework that helps in integrating most of the SCIM-based target systems. This connector can be used to load identity data into Oracle Identity Manager from a SCIM service and then efficiently manage identities in an integrated cycle with the rest of the identity-aware applications in your enterprise.

As a business use case example, consider a leading logistics company that has 100+ cloud applications. Most of these cloud applications are now inefficient because data in these applications are manually entered and are managed using spreadsheets or custom-coded process flows. Therefore, this company wants to integrate its cloud applications with Oracle Identity Manager to streamline its operations, increase its organizational efficiency, and at the same time, lower its operational costs. There are two approaches for integrating these cloud applications with Oracle Identity Manager. One approach would be to deploy a point-to-point connector for each of these applications. The drawbacks of this approach are as follows:

1. Increased time and effort to identify and deploy a point-to-point connector for each application.
2. Increased administration and maintenance overheads for managing connectors for each application.
3. Unavailability of point-to-point connectors for all applications. In such a scenario, one needs to develop custom connectors that increases time and effort to develop, deploy and test the custom connector.

An alternative to this approach is to use the Generic SCIM connector that can be used to integrate all the cloud applications with Oracle Identity Manager. The Generic SCIM connector provides the ability to manage accounts across all cloud applications without spending additional resources and time on building custom connectors for each cloud application.

The Generic SCIM connector is a hybrid approach that helps enterprises leverage on-premise Oracle Identity Manager Deployment to integrate with target systems for identity governance. These targets systems include any application that exposes SCIM APIs such as SaaS, PaaS, and homegrown applications and so on.

The following are some example scenarios in which the Generic SCIM connector is used:

1. **User Management**  
   The Generic SCIM Connector manages individuals who can access Cloud service by defining them as users in the system and assigning them to groups. This connector allows new users to self-provision on a Generic SCIM Cloud Service, while having it be controlled by IT. Users can request and provision from a catalog of cloud-based resources that is established by Oracle Identity Manager Administrators. For example, to create a new user in the target system, fill in and submit the Oracle Identity Manager process form to trigger the provisioning operation. The connector executes the create operation against your target system and the user is created on successful execution of the operation. Similarly, operations such as delete and update can be performed.
2. **Entitlement Management**  
   The Generic SCIM Connector manages Cloud services objects (if exposed by the target system) as entitlements. Depending on the target system being used, this connector can be used to manage entitlements such as Groups, Roles, Licenses, Folders, Collaboration and so on. For example, you can use the Generic SCIM connector to automatically assign or revoke groups to users based on predefined access policies in Oracle Identity Manager. Similarly, you can use the Generic SCIM Connector to manage role memberships that provide selective access to certain Cloud Service functionality or groups. Therefore, as new users are added to a specific role, they automatically gain corresponding access in the applications. As an administrator, you can also use this connector to efficiently manage user licenses for all the available resources. By leveraging the auditing and reporting tools of Oracle Identity Manager, you can automate license allocation whenever a new account is created. In addition, license assignments and usage can be monitored through changing organization needs and unused licenses can be tracked for potential recycling.

### Features of the Generic SCIM Connector

The features of the connector include support for full and incremental reconciliation, limited reconciliation, custom authentication, custom parsing, custom payload, handling multiple endpoint URLs, and SSL communication.

The following are the features of the connector:

1. Support for Both Trusted Source and Target Resource Reconciliation
2. Full and Incremental Reconciliation
3. Limited (Filtered) Reconciliation
4. Custom Authentication
5. Custom Parsing
6. Custom Payload
7. Support for Additional HTTP Headers
8. Support for Handling Multiple Endpoint URLs
9. SSL Communication

#### Support for Both Trusted Source and Target Resource Reconciliation

The Generic SCIM connector includes a groovy file (a part of the metadata generator) that enables you to configure the connector to run either in the trusted source mode or target resource mode.

#### Full and Incremental Reconciliation

After you create the connector, you can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Manager. After the first full reconciliation run, you can configure your connector for incremental reconciliation. In incremental reconciliation, only records that are added or modified after the last reconciliation run are fetched into Oracle Identity Manager.

| D:\tt\icon-note-16.png | Note: |
| --- | --- |
| The connector supports incremental reconciliation if the target system contains an attribute that holds the timestamp at which an object is created or modified.  See Full Reconciliation and Incremental Reconciliation. |

You can perform a full reconciliation run at any time.

#### Limited (Filtered) Reconciliation

You can reconcile records from the target system based on a specified filter criterion. To limit or filter the records that are fetched into Oracle Identity Manager during a reconciliation run, you can specify the subset of added or modified target system records that must be reconciled.

You can set a reconciliation filter as the value of the Filter attribute of the scheduled jobs. This filter specifies the subset of newly added and modified target system records that must be reconciled.

See Limited Reconciliation for Generic SCIM Connector.

#### Custom Authentication

By default, the Generic SCIM connector supports HTTP Basic Authentication and OAuth 2.0 authentication mechanisms. The connector also supports an authentication mechanism in which the user provides access token and refresh tokens as an input. The supported grant types for OAuth 2.0 authentication mechanism are JWT, Client Credentials, and Resource Owner Password.

If your target system uses any of the authentication mechanisms that is not supported by the connector, then you can write your own implementation for custom authentication by using the plug-ins exposed by this connector. See Implementing Custom Authentication.

#### Custom Parsing

By default, the Generic SCIM connector supports request and response payloads only in the JSON format. If your target system does not support request or response payload in JSON format, then you can implement a custom parsing logic by using plug-ins exposed by this connector.

See Implementing Custom Parsing.

#### Custom Payload

The Generic SCIM connector provides support for handling custom formats for any attributes in the payload that do not adhere to the standard JSON format. This can be achieved by specifying a value for the customPayload IT resource parameter.

#### Support for Additional HTTP Headers

If your target system requires additional or custom HTTP headers in any SCIM call, then you can insert these HTTP headers as the value of the customAuthHeaders or customAuthHeaders IT resource parameters.

See Additional Configuration Parameters...

#### Support for Handling Multiple Endpoint URLs

The Generic SCIM connector allows you to handle attributes of an object class (for example, a User object class) that can be managed only through endpoints other than the base endpoint URL of the object class. For example, in certain target systems, there are attributes of the User object class that can be managed using the base endpoint URL. However, some attributes (for example, email alias) can be managed only through a different endpoint URL. The connector provides support for handling all endpoint URLs associated with an object class.

This can be achieved by providing endpoint URL details of such attributes in the relURIs IT resource parameter.

#### SSL Communication

You can configure SSL communication between Oracle Identity Manager and the SCIM-based target system.

See Configuring SSL for the Generic SCIM Connector for information about configuring secure communication.

### Roadmap for Generating and Using the Connector

This is the organization of information available in this guide for deploying and using the connector.

The rest of this guide is divided into the following chapters:

1. Installing and Configuring the Generic SCIM Connector describes those procedures that you must perform during each stage of connector installation.
2. Using the Generic SCIM Connector describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
3. Extending the Functionality of the Generic SCIM Connector describes procedures that you can perform if you want to extend the functionality of the connector.
4. Files and Directories of the Generic SCIM Connector lists the files and directories that comprise the connector installation media.

## Installing and Configuring the Generic SCIM Connector

You must install the connector in Oracle Identity Manager. If necessary, you can also deploy the connector in a Connector Server.

The following topics provide details to install and configure the Generic SCIM connector:

1. Preinstallation
2. Installing the Generic SCIM Connector
3. Post installation

### Preinstallation

Preinstallation for the Generic SCIM connector involves custom authentication implementation and custom parsing implementation. For the SCIM connector, the preinstallation steps are performed before the metadata generation.

The preinstallation steps include the following optional procedures:

1. Implementing Custom Authentication
2. Implementing Custom Parsing

#### Implementing Custom Authentication

If your target system uses an authentication mechanism that is not supported by this connector, then you must implement the authentication that your target system uses and then attach it to the connector by using the plug-ins exposed by this connector. Implementing custom authentication involves creating a Java class, overriding the Map<String, String> getAuthHeaders(Map<String, Object> authParams) method that returns the authorization header in the form of a map, and updating the connector installation media to include the new Java class. All the target system configuration and authentication details that may be required for obtaining the authorization header are passed to the Map<String, String> getAuthHeaders(Map<String, Object> authParams) method through specific IT resource parameters. All the configuration properties exposed by this connector are accessible within this method as a part of "authParams".

#### Implementing Custom Parsing

By default, the connector supports only JSON parsing during reconciliation runs. If the reconciliation data from your target system is not in JSON format, then you must write a custom parser implementation for your data format.

### Installing the Generic SCIM Connector

You must install the connector in Oracle Identity Manager. If necessary, you can also deploy the connector in a Connector Server.

The following topics provide details on installing the connector:

1. Understanding Installation of the Generic SCIM Connector
2. Running the Connector Installer
3. Configuring the IT Resource for the Target System

#### Understanding Installation of the Generic SCIM Connector

The procedure to understand installation of the Generic SCIM Connector is divided across two stages namely summary of steps to install the connector and about installing the Generic SCIM connector locally and remotely.

1. Summary of Steps to Install the Connector
2. About Installing the Generic SCIM Connector Locally and Remotely

##### Summary of Steps to Install the Connector

Installing this connector requires you to install the connector bundle that is included in the installation media and then install the connector package (specific to your target system) that you had generated while performing the procedure described in Generating the Generic SCIM Connector section.

The following is a summary of steps to install the Generic SCIM connector:

1. Run the connector installer to install the connector bundle included in the installation media. This procedure is described later in this chapter.
2. Run the connector installer to install the connector package (specific to your target system) that you had generated while performing the procedure described in Generating the Generic SCIM Connector. The procedure to install the connector package is described later in this guide.
3. Configure the IT resource. See Configuring the IT Resource for the Target System.

##### About Installing the Generic SCIM Connector Locally and Remotely

You can run the connector code either locally in Oracle Identity Manager or remotely in a Connector Server.

Depending on where you want to run the connector code (bundle), the connector provides the following installation options:

1. Run the connector code locally in Oracle Identity Manager.  
   In this scenario, you deploy the connector in Oracle Identity Manager. Deploying the connector in Oracle Identity Manager involves performing the procedures described in Running the Connector Installer and Configuring the IT Resource for the Target System.
2. Run the connector code remotely in a Connector Server.  
   In this scenario, you deploy the connector in Oracle Identity Manager, and then, deploy the connector bundle in a Connector Server. See Using an Identity Connector Server in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager for information about installing, configuring, and running the Connector Server, and then installing the connector in a Connector Server.

#### Running the Connector Installer

When you run the Connector Installer, it automatically copies the connector files to directories in Oracle Identity Manager, imports connector XML files, and compiles adapters used for provisioning.

As discussed in one of the earlier sections, you must first install the connector bundle that is included in the installation media and then install the connector bundle that is a part of the connector package that you generated. The procedure to install both connector bundles is the same except for the following differences:

1. Before running the connector installer to install the connector bundle from the installation media, you must copy the contents of the connector installation media to the OIM\_HOME/server/ConnectorDefaultDirectory directory.
2. Before running the connector installer to install the generated connector, you must copy the unzipped connector package (generated in Generating the Generic SCIM Connector) to the OIM\_HOME/server/ConnectorDefaultDirectory directory.

You must install the connector in Oracle Identity Manager by using the Connector Installer. To do so:

#### Configuring the IT Resource for the Target System

The IT resource for your target system is created after you install the connector. An IT resource is composed of parameters that store connection and other generic information about a target system. Oracle Identity Manager uses this information to connect to a specific installation or instance of your target system and perform reconciliation and provisioning operations.

The list of IT resource parameters for the Generic SCIM connector can be grouped into the following categories:

Connection-related parameters

Authentication parameters

Parser parameters

Additional configuration parameters

| D:\tt\icon-note-16.png | Note: |
| --- | --- |
| The list of parameters that are displayed on the IT resource page depends on the properties that you added to the Config entry of the SCIMConfiguration.groovy file. At any point in time, you can update the list of IT resource parameters by modifying the IT Resource Type definition using Oracle Identity Manager Design Console. There is no need to re-create and install the connector when you update the IT Resource Type definition. |

The following topics related to IT resource configuration are discussed in this section:

1. About IT Resource Parameter Categories
2. IT Resource Parameters
3. Specifying Values for the IT Resource Parameters

##### About IT Resource Parameter Categories

An IT resource is composed of parameters that store connection and other generic information about a target system. Oracle Identity Manager uses this information to connect to a specific installation or instance of your target system.

The list of IT resource parameters for this connector can be grouped into the following categories:

1. **Connection-related parameters**  
   Connection parameters are used by the connector to establish a connection between Oracle Identity Manager and your target system for exchange of identity information.
2. **Authentication parameters**  
   Authentication parameters are used by the target system to authenticate the application. The IT resource parameters for authentication vary depending on the value of the grantType parameter. The grantType parameter holds the type of authentication used by your target system. By default, the connector supports the following types of authentication:  
     
    Basic authentication  
    OAuth2.0 JWT  
    OAuth2.0 Client Credentials  
    OAuth2.0 Resource Owner password  
     
   Apart from the authentication types listed, if you target system uses any other authentication type, then you must write your own implementation which requires development effort. The following are the possible values for this parameter:  
   For HTTP Basic Authentication: basic  
     
    For OAuth 2.0 JWT: jwt  
    For OAuth 2.0 Client Credentials: client\_credentials  
    For OAuth 2.0 Resource Owner Password: password  
    For custom authentication implementation: custom
3. **Parser parameters**  
   By default, the connector supports only JSON parsing during reconciliation runs. If the reconciliation data from your target system is not in JSON format, then you must write a custom parser implementation for your data format. If the data from your target system is in JSON format, then the connector uses JSON parsing and you must provide a value for the jsonResourcesTag parameter. The jsonResourcesTag parameter must contain the json tag value that is used during reconciliation for parsing multiple entries in a single response payload. If you are using a custom parser implementation, then you must provide values for the parameters listed in table :::
4. **Additional Configuration parameters**  
   All additional configuration parameters are target system specific.

##### IT Resource Parameters

The IT resource for the target system contains connection information about the target system. Oracle Identity Manager uses this information during provisioning and reconciliation.

**Connection Parameters**

| **System** | **Requirement** |
| --- | --- |
| **Schema Descriptor** | Enter the name and relative path of the schema file that you want to use.  See Defining the Schema for information about the schema file that you created. |
| **Server Name** | Host name or IP address of the computer hosting the target system.  Sample value: www.example.com |
| **Server Port** | Port number at which the target system is listening.  Sample value: 80 |
| **Proxy Server Name** | Proxy host is the name of the proxy host used to connect to an external target system.  Sample value: www.example.com |
| **Proxy Server Port** | Proxy port number  Sample value: 80 |
| **Proxy Username** | Proxy user ID of the target system user account that Oracle Identity Manager uses to connect to the target system. |
| **Proxy Password** | Password of the proxy user ID of the target system user account that Oracle Identity Manager uses to connect to the target system. |
|  |  |
|  |  |
|  |  |

**Authentication Parameters**

As discussed in one of the earlier sections, IT resource parameters for authentication vary depending on the value that you specify for the grantType parameter.

*Basic Authentication*

Following table lists the set of IT resource parameters for which you must enter values when the grantType parameter is set to basic.

| **System** | **Requirement** |
| --- | --- |
| **Principal Username** | User name or User ID of the account that Oracle Identity Manager must use to connect to and access the target system during reconciliation and provisioning operations.  Sample value: scottiger |
| **Principal Password** | Password of the account that Oracle Identity Manager must use to connect to and access the target system during reconciliation and provisioning operations.  Sample value: password |

*Client Credential Authentication*

Following table lists the set of IT resource parameters for which you must enter values when the grantType parameter is set to client\_credentials.

| **System** | **Requirement** |
| --- | --- |
| **Client Identifier** | User name or User ID of the account that Oracle Identity Manager must use to connect to and access the target system during reconciliation and provisioning operations.  Sample value: scottiger |
| **Principal Username** | User name or User ID of the account that Oracle Identity Manager must use to connect to and access the target system during reconciliation and provisioning operations.  Sample value: scottiger |
| **Principal Password** | Password of the account that Oracle Identity Manager must use to obtain a authentication token.  Sample value: password |
| **Authentication Server** | Enter the URL of the authorization server that authenticates the client (by validating the client ID and client secret), and if valid, issues an access token.  Sample value: https://api.example.com/oauth2/token |

*Resource Owner Authentication*

Following table lists the set of IT resource parameters for which you must enter values when the grantType parameter is set to password.

| **System** | **Requirement** |
| --- | --- |
| **Principal Username** | User name or User ID of the account that Oracle Identity Manager must use to connect to and access the target system during reconciliation and provisioning operations.  Sample value: scottiger |
| **Principal Password** | Password of the account that Oracle Identity Manager must use to connect to and access the target system during reconciliation and provisioning operations.  Sample value: password |
| **Client Identifier** | Enter the client identifier issued to the client during the registration process. |
| **Principal Client Secret** | Enter the client secret used to authenticate the identity of the client application. |
| **Authentication Server URL** | Enter the URL of the authorization server (token endpoint) that authenticates the client (by validating client ID and client secret) and the resource owner credentials, if valid, issues an access token.  Sample value: https://api.example.com/oauth2/token |

**Additional Configuration parameters**

| **System** | **Requirement** |
| --- | --- |
| **Secure Socket** | Specifies whether SSL communication is enabled between Oracle Identity Manager and your target system.  Enter yes, if SSL is configured. Otherwise, enter no. |
|  |  |

##### Specifying Values for the IT Resource Parameters

The IT resource for the target system contains connection information about the target system. Oracle Identity Manager uses this information during provisioning and reconciliation.

When you run the metadata generator, the IT resource corresponding to this connector is automatically created in Oracle Identity Manager. You must specify values for the parameters of this IT resource as follows:

1. Log in to Oracle Identity System Administration.
2. In the left pane, under Configuration, click **IT Resource**.
3. In the IT Resource Name field on the Manage IT Resource page, enter the name of the IT resource, and then click **Search**. The name of the IT resource is the value of the itResourceName property in the GenericScimConfiguration.groovy file.
4. Click the edit icon for the IT resource.
5. From the list at the top of the page, select **Details and Parameters**.
6. Specify values for the parameters of the IT resource.  
     
   See the Configuring the IT Resource for the Target System section for information about IT resource parameters.
7. To save the values, click **Update**.

### Post installation

Post installation for the connector involves configuring Oracle Identity Manager, enabling logging to track information about all connector events, and configuring SSL. It also involves performing some optional configurations such as localizing the user interface.

This topic discusses the following post installation procedures:

1. Configuring Oracle Identity Manager
2. Localizing Field Labels in UI Forms
3. Clearing Content Related to Connector Resource Bundles from the Server Cache
4. Managing Logging for the Generic SCIM Connector
5. Configuring SSL for the Generic SCIM Connector

#### Configuring Oracle Identity Manager

You must create a UI form and an application instance for the resource against which you want to perform reconciliation and provisioning operations. In addition, you must run entitlement and catalog synchronization jobs.

|  | Important: |
| --- | --- |
| Perform the procedures described in this section only if you are using the connector in the target resource mode. |

You must create a UI form and an application instance for the resource against which you want to perform reconciliation and provisioning operations. In addition, you must run entitlement and catalog synchronization jobs. These procedures are described in the following sections:

#### Localizing Field Labels in UI Forms

#### Clearing Content Related to Connector Resource Bundles from the Server Cache

#### Managing Logging for the Generic SCIM Connector

#### Configuring SSL for the Generic SCIM Connector

## Deploying the Connector

The procedure to deploy the connector can divided into the following stages:

### Configure Connector Server

If the

| **System** | **Requirement** |
| --- | --- |
|  | javax.inject.javax.inject.jar |
|  | javax.ws.rs.javax.ws.rs-api.jar |
|  | com.sun.jersey.jersey-core.jar |
|  | org.glassfish.hk2.hk2-api.jar |
|  | org.glassfish.hk2.hk2-utils.jar |
|  | org.glassfish.hk2.hk2-locator.jar |
|  | org.glassfish.jersey.core.jersey-common.jar |
|  | org.glassfish.jersey.core.jersey-client.jar |
|  | org.glassfish.jersey.bundles.repackaged.jersey-guava.jar |
|  | org.glassfish.javax.json.jar |

## SCIM filter language

The System for Cross-domain Identity Management (SCIM) is an open standard for managing user identity information across applications or identity domains. You can use the SCIM filter language to build a user query.

### Logical Operators

| **Operator** | **Definition** | **Description** |
| --- | --- | --- |
| **and** | logical AND | Logical AND for building compound expressions in which both expressions are true. |
| **or** | logical OR | Logical OR for building compound expressions in which either expression is true. |
| **not** |  | Logical NEGATE in which expressions evaluates to false. |

### Grouping Operators

| **Operator** | **Definition** | **Description** |
| --- | --- | --- |
| **( )** | Precedence | Boolean expressions may be grouped using parentheses to change the standard order of operations, i.e., to evaluate logical "or" operators before logical "and" operators. |
| **[ ]** | Complex | The expression within square brackets ("[" and "]") must be a valid filter expression based upon sub-attributes of the parent attribute. Nested expressions may be used |

### Attribute Operators

| **Operator** | **Definition** | **Description** |
| --- | --- | --- |
| **pr** | present (has value) | If the attribute has a non-empty value, or if it contains a non-empty node for complex attributes there is a match.  Supported attributes: |
| **eq** | equals | The attribute and operator values are identical.  Supported attributes: |
| **ne** | not equal | The attribute and operator values are not identical.  Supported attributes: |
| **sw** | starts with | The entire operator value is a substring of the attribute value, starting at the beginning of the attribute value.  This criterion is satisfied if the two strings are identical.  Supported attributes: |
| **ew** | ends with | The entire operator value must be a substring of the attribute value, matching at the end of the attribute value.  This criterion is satisfied if the two strings are identical.  Supported attributes: |
| **co** | contains | The entire operator value must be a substring of the attribute value for a match.  Supported attributes: |
| **gt** | greater than | If the attribute value is greater than the operator value, there is a match.  The actual comparison is dependent on the attribute type. For string attribute types, this is a lexicographical comparison, and for DateTime types, it is a chronological comparison. For integer attributes, it is a comparison by numeric value. Boolean and Binary attributes fails with an *invalidFilter* message.  Supported attributes: |
| **ge** | greater than or equal | If the attribute value is greater than or equal to the operator value, there is a match.  The actual comparison is dependent on the attribute type. For string attribute types, this is a lexicographical comparison, and for DateTime types, it is a chronological comparison. For integer attributes, it is a comparison by numeric value. Boolean and Binary attributes fails with an *invalidFilter* message.  Supported attributes: |
| **lt** | less than | If the attribute value is less than operator value, there is a match.  The actual comparison is dependent on the attribute type. For string attribute types, this is a lexicographical comparison, and for DateTime types, it is a chronological comparison. For integer attributes, it is a comparison by numeric value. Boolean and Binary attributes fails with an *invalidFilter* message.  Supported attributes: |
| **lt** | less than or equal | If the attribute value is less than or equal to the operator value, there is a match.  The actual comparison is dependent on the attribute type. For string attribute types, this is a lexicographical comparison, and for DateTime types, it is a chronological comparison. For integer attributes, it is a comparison by numeric value. Boolean and Binary attributes fails with an *invalidFilter* message.  Supported attributes: |

A simple example to find a user by username:

| D:\tt\icon-tip-16.png | Tip: |
| --- | --- |
| username eq "mmusterfrau" |

You can join filter expressions by using the "and" and "or" operators and grouping them in parentheses. For example, to find all users who have a family name of "Mustermann" and a first name that starts with the letter "A", use the filter:

| D:\tt\icon-tip-16.png | Tip: |
| --- | --- |
| (name.familyName eq "Mustermann") and (name.givenName sw "A") |

| D:\tt\icon-note-16.png | Note: |
| --- | --- |
|  |

| D:\tt\icon-restrict-16.png | Restrict: |
| --- | --- |
|  |

|  | Important: |
| --- | --- |
|  |

| D:\tt\icon-caution-16.png | Caution: |
| --- | --- |
|  |

| D:\tt\icon-warning-16.png | Warning |
| --- | --- |
|  |

| D:\tt\icon-tip-16.png | Tip: |
| --- | --- |
|  |