



One Identity Manager 9.2

Administration Guide for Connecting to Starling Connect Using Starling Connect Connector

Copyright 2023 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

 **WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.**

 **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

Contents

| | |
|---|-----------|
| Starling Connect Connector module | 4 |
| Technical overview | 4 |
| Prerequisites | 4 |
| Installing Starling Connect Connector module | 5 |
| Configuring a Synchronization project using Starling Connect Connector | 6 |
| Creating a synchronization project | 6 |
| Troubleshooting | 10 |
| About us | 11 |
| Contacting us | 11 |
| Technical support resources | 11 |

Starling Connect Connector module

This document describes the details of the Starling Connect Connector Module.

Technical overview

This section provides an overview of the technical aspects of the Starling Connect Connector Module.

The synchronization of a cloud application with the One Identity Manager database and the provisioning of object changes from the One Identity Manager database to the cloud application is performed by the SCIM connector of One Identity Manager. While creating a synchronization project for Starling Connect connectors, the user has to manually enter the SCIM URL, Authentication endpoint, Authentication type, Client secret and Application/Client ID.

To access cloud applications, the SCIM connector must be installed on a synchronization server. The SCIM connector can communicate with cloud applications that understand the System for Cross-Domain Identity Management (SCIM) specification. The synchronization server ensures that data is compared between the One Identity Manager database and the cloud application. For more details on SCIM, see [SCIM Administration Guide for Connecting to Cloud Applications](#).

Starling Connect Connector makes the configuration simpler and less prone to errors caused by wrongly entered configuration values. The SCC Connector uses Starling Hybrid Subscription credentials and auto discovers all the Connectors registered with the Connect subscription. It integrates the SCIM capabilities with the Starling Hybrid Subscription in order to create a synchronization project for the connector.

Prerequisites

The below mentioned prerequisites must be in place before configuring a synchronization project using the Starling Connect Connector.

- Enable SCIM server function for the job server.
- Configure the Starling Hybrid Subscription using a Starling account.

For more information on configuring Starling Hybrid Subscription, see [Multi-factor authentication in One Identity Manager](#).

Installing Starling Connect Connector module

The Starling Connect Connector module installation procedure is similar to installation procedures of other One Identity Manager modules. To install the Starling Connect Connector module, 9.2 or a later version of One Identity Manager is required.

For information on installing Starling Connect Connector module, refer to the *Installing One Identity Manager Components* section of the *One Identity Manager Installation Guide*.

Configuring a Synchronization project using Starling Connect Connector

This section provides details about creating a synchronization project using Starling Connect Connector module.

Creating a synchronization project

To create a synchronization project:

1. Ensure that all the prerequisites for SCC are configured.
2. Open the **Synchronization Editor**.
3. Click **Start a new synchronization project**.
4. Choose **Starling Connect Connector** as the **Target system**.
5. Click **Next** until the **Connect to System wizard** page.
6. Enter the credentials for the system user.
7. Click **Connect**.
8. Click **Next**.
9. Click **Test** to validate the Starling Hybrid Subscription credentials.
10. Select the appropriate connector from the drop down list. Click **Next**.
11. In the **Endpoint configuration** section, enter the URLs for the SCIM end points.

| **NOTE:** The SCIM default is used as there is no URL.

Table 1: End Point Configuration

| Property | Description |
|---------------------------|--|
| Schema | End point for accessing the schema information for the cloud application. |
| Resources | End point for accessing resource information for the cloud application, for example groups or user accounts. |
| Supported service options | End point for accessing the service provider information for the cloud application |

To test the connection at the specified end points, click **Test**. The connection will be automatically validated against the default endpoints.

NOTE:

- The Endpoints can be modified if required.
- On successful endpoint validation, the **Next** button is enabled.

12. Click **Next**.
13. Enter a unique display name for the cloud application on the **Display name** page.
NOTE: You can use display names to differentiate between the cloud application in One Identity Manager tools. Display names cannot be changed later..
14. On the last page of the system connection wizard, you can save the connection data locally and finish the system connection configuration.
 - Set the **Save connection data** on local computer option to save the connection data. This can be reused when you set up other synchronization projects.
 - Click **Finish** to end the system connection wizard and return to the project wizard.
15. On the **One Identity Manager Connection** tab, test the data for connecting to the One Identity Manager database. The data is loaded from the connected database. Reenter the password.

NOTE: If you use an unencrypted One Identity Manager database and have not yet saved any synchronization projects to the database, you need to enter all connection data again. This page is not displayed if a synchronization project already exists.

16. The wizard loads the target system schema. This may take a few minutes depending on the type of target system access and the size of the target system.
17. Select a project template on the **Select project template** page that you want to use for setting up the synchronization configuration.

NOTE: A default project template ensures that all required information is added in One Identity Manager. This includes mappings, workflows and the synchronization base object. If you do not use a default project template you must declare the synchronization base object in One Identity Manager yourself. Use a default project

template for initially setting up the synchronization project. For custom implementations, you can extend the synchronization project with the Synchronization Editor.

18. On the **Restrict target system access** page, you can specify how the system access must work. You have the following options:

Table 2: Specify target system access

| Project template | Description |
|---|--|
| Read-only access to target system. | <p>Specifies whether a synchronization workflow is only to be set up for the initial loading of the target system into the One Identity Manager database.</p> <p>The synchronization workflow has the following characteristics:</p> <ul style="list-style-type: none"> • Synchronization is in the direction of One Identity Manager. • Processing methods in the synchronization steps are only defined for synchronization in the direction of One Identity Manager. |
| Read/write access to target system. Provisioning available. | <p>Specifies whether a provisioning workflow is to be set up in addition to the synchronization workflow for the initial loading of the target system.</p> <p>The provisioning workflow displays the following characteristics:</p> <ul style="list-style-type: none"> • Synchronization is in the direction of the Target system. • Processing methods are only defined in the synchronization steps for synchronization in the direction of the Target system. • Synchronization steps are only created for such schema classes whose schema types have write access. |

19. Select the synchronization server to execute synchronization on the **Synchronization server** page.

If the synchronization server is not declared as a Job server in the One Identity Manager database yet, you can add a new Job server.

- a. Click **+** to add a new Job server.
- b. Enter a name for the Job server and the full server name conforming to DNS syntax.
- c. Click **OK**.

The synchronization server is declared as Job server for the target system in the One Identity Manager- database.

NOTE: After you save the synchronization project, ensure that this server is set up as a synchronization server.

20. To close the project wizard, click **Finish**.

This creates and allocates a default schedule for regular synchronization. Enable the schedule for regular synchronization.

The synchronization project is created, saved and enabled immediately.

NOTE: If you do not want the synchronization project to be activated immediately, disable the **Activate and save the new synchronization project automatically** option. In this case, save the synchronization project manually before closing the **Synchronization Editor**.

NOTE: The connection data for the target system is saved in a variable set and can be modified under **Configuration | Variables** in Synchronization Editor.

Troubleshooting

This section describes the troubleshooting procedure for Starling Connect Connector module.

Starling Connect Connector uses the Starling Hybrid Subscription integrated with SCIM Connector capabilities to validate Starling Connect Subscription and the connector endpoints. In case of any failures during the configuration, follow the below steps to troubleshoot.

To trouble the Starling Connect Connector:

1. Check if the starling hybrid subscription is configured properly.

NOTE: If you have not committed the changes to the One Identity Manager Database via the designer tool when you reconfigured or updated the Starling Hybrid Subscription, it will result in a connection failure. This is because the old configuration would still exist in the database. You must reconfigure the Starling Hybrid Subscription and commit the changes to the One Identity Manager Database via the designer tool.

2. Check if SCIM is enabled in the job server function.
3. Check the Synchronization Editor Logs in the client machine for detailed error.

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit <https://www.oneidentity.com/company/contact-us.aspx>.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at <https://support.oneidentity.com/>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product