Starling Connect

Troubleshooting Guide

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.

Starling Connect Troubleshooting Guide
Updated - January 2020

Contents

1

About this Guide

This document describes common issues related to Starling Connect connectors that may occur while connecting to different cloud applications using Starling Connect. It also defines how to diagnose and troubleshoot different issues concerning Starling Connect. This document will be revised by the Support team as and when information update happens.

Starling Connect errors

Different errors associated with Starling Connect are detailed in this section. This section also describes different procedures to be followed to verify the error and the scenario.

The errors related to Starling Connect are as follows:

Error 400

Different error scenarios associated with **Error 400** are listed below:

- Bad request when mandatory fields are missing
- Bad request when custom mapping is missing
- Bad request when there is an invalid input

The procedures to verify the above mentioned scenarios are detailed below.

Bad request when mandatory fields are missing

To verify that Starling endpoints are working

1. Copy the failed request body from One Identity Manager.
2. Paste the request body at a SCIM client (for example, Postman).
3. Perform a **POST/PUT** operation for the request on Starling Endpoints as required.
4. Observe the JSON response with the error description.
5. Correct the request body by adding or modifying the required fields and then, reinitiate.
6. Ensure that the core schema included in the request wrapper is accurate.
7. Apply the changes that were performed in steps 5 and 6, and send the request from One Identity Manager.
8. Check for the success of synchronization.

Bad request when custom mapping is missing

To verify that Starling endpoints are working

1. Copy the failed request body from One Identity Manager.
2. Paste the request body at a SCIM client (for example, Postman).
3. Perform a **POST/PUT** operation for the request on Starling endpoints as required.
4. Observe the JSON response with error description.
5. Identify the mapping that is missing.
6. Based on requirement of the connector, add or update a custom mapping in One Identity Manager.
7. Reinitiate the request from One Identity Manager
8. Check for the success of synchronization.

Bad request when there is an invalid input

To verify that Starling endpoints are working

1. Copy the failed request body from One Identity Manager.
2. Paste the request body at a SCIM client (for example, Postman).
3. Perform a **POST/PUT** operation for the request on Starling endpoints as required.
4. Observe the JSON response with error description.
5. Based on the error description, identify the root cause.
6. Correct the request body by adding or modifying the required fields.

The following table consists of error messages that are returned, if different request wrapper properties are missing.

Table 1: Error messages

Request wrapper property	Error message
Method	Required property missing in Request Wrapper
ClientRequest	Required property missing in Request Wrapper
Body	Required property missing in Request Body
targetURi	Required property missing in Request Wrapper
serviceCredentials	Required property missing in Request Wrapper
AuthenticationType	enum -0 (default)
ConfigProperties	Required property missing in Request Wrapper
credential information (username, password, clientID, and so on)	Credential information missing in Request Wrapper
ConfigProperties	Required property missing in Request Wrapper (from connector)

Error 401 Unauthorized

Different error scenarios associated with **Error 401 Unauthorized** are listed below:

- Invalid cloud application credentials
- Invalid Starling credentials
- Expired Starling Subscription
- Deleted Starling Connector connection

The procedures to rectify the error scenarios are detailed below.

Invalid cloud application credentials

To rectify the error

1. Log in to the cloud application and validate your credentials.
2. Log in to the Starling account.
3. Navigate to **My Connectors**.
4. Select the required connector.
5. Edit and update the connection parameters with accurate details.
6. Click **Save**.

Invalid Starling credentials

To rectify the error

1. Log in to the Starling account.
2. Navigate to **My Connectors**.
3. Select the required connector.
4. Use the Starling endpoints and credentials.

Expired Starling subscription

To rectify the error

1. Log in to the Starling account.
2. Navigate to **My Connectors**.
3. If the account is expired, get it activated.
4. Use the Starling endpoints and credentials.

Deleted Starling Connector connection

To rectify the error

1. Log in to the Starling account.
2. Navigate to **My Connectors**.
3. Ensure that the relevant connector is available.

Error 403 Forbidden

Error 403 occurs when the user does not have the required access privileges.

To rectify the error, ensure that the user has required access privileges.

Error 404 Not found

The error scenario associated with **Error 404 Not found** occurs when the Starling endpoints are not accessible.

To ensure that Starling endpoints are working

1. Open a SCIM Client (for example, Postman).
2. Perform a **GET** operation for endpoints mentioned below:
    - Schemas
    - ServiceProviderConfig
    - ResourceTypes
    - Users
    - Groups
3. Verify the JSON response, to check whether it is successful.

Error 406

The following error scenarios are associated with **Error 406** :

- Function Host Down
- Connector West US is stopped and the East US is up and running for MRF Archer

The procedures to verify the error scenarios are detailed below:

Function Host Down

To verify the scenario, check and ensure that the Function host is up and running.

Connector West US is stopped and the East US is up and running for MRF Archer

Error 406 is displayed for a short time when the connector West US is stopped and the East US is up and running for MRF Archer.

To verify the scenario, do the following:

1. Pass a request when both the West and East US connector are up and running.
2. Verify that a successful response is displayed.
3. Stop the West US app service.
4. Pass a request and verify the response.

NOTE:

- **Actual Result**: A 406 error is displayed for few seconds. The proper response is displayed a little later.
- **Expected Result**: There should not be any error because if a sync is running, the sync would fail in 1IM.

Error 409 Conflict

Error 409 Conflict occurs when duplicate values are used in unique fields of the application**.**

To rectify the error

1. Copy the failed request body from One Identity Manager.
2. Paste the request body at a SCIM client (for example, Postman).
3. Perform a **POST/PUT** operation for the request on Starling Endpoints as required.
4. Observe the JSON response with the error description.
5. Based on the error description, identify the unique fields that cause the conflict.
6. Correct the request body by adding or modifying the unique fields.

Error 422 Unprocessable Entity

Error 422 unprocessable Entity occurs when the number of resources limit on account has been exceeded.

To rectify the error

1. Ensure that the account has the ability to host additional user resources and group resources.
2. Repeat the steps of provision by providing values for all the mandatory fields.
3. Check and confirm that the resource has been provisioned.

Error 500 Generic Message

Different error scenarios associated with **Error 500 Generic Message** are listed below:

- Internal Server Error
- Unhandled Exception from Starling Connector
- RSA Archer cloud application returns code 500 for all errors except 401 Unauthorized

The procedures to verify the error scenarios are detailed below.

Internal Server Error

To ensure that Starling endpoints are working

1. Open a SCIM Client (for example, Postman).
2. Perform a **GET** operation for endpoints mentioned below:
    - Schemas
    - ServiceProviderConfig
    - ResourceTypes
    - Users
    - Groups
3. Verify the JSON response, to check whether it is successful.

Unhandled Exception from Starling connector

To ensure that Starling Endpoints are working

1. Open a SCIM Client (for example, Postman).
2. Perform a **GET** operation for endpoints mentioned below:
    - Schemas
    - ServiceProviderConfig
    - ResourceTypes
    - Users
    - Groups
3. Verify the JSON response, to check whether it is successful.

RSA Archer cloud application returns code 500 for all errors except 401 Unauthorized

To ensure that Starling endpoints are working

1. Open a SCIM Client (for example, Postman).
2. Perform a **GET** operation for endpoints mentioned below:
    - Schemas
    - ServiceProviderConfig
    - ResourceTypes
    - Users
    - Groups
3. Verify the JSON response, to check whether it is successful.

Error 502 Bad Gateway

The error scenario associated with **Error 502 Bad Gateway** occurs when the requests count is more than 730, and load balances are not available.

To ensure that Starling endpoints are working

1. Open a SCIM Client (for example, Postman).
2. Perform a **GET** operation for endpoints mentioned below:
    - Schemas
    - ServiceProviderConfig
    - ResourceTypes
    - Users
    - Groups
3. Verify the JSON response, to check whether it is successful.

Error 503 Service Unavailable

The error scenarios associated with **Error 503 Service Unavailable** are mentioned below:

- Cloud account instance not awake or active (for example, ServiceNow)
- FunctionHost Down

The procedures to rectify the mentioned error scenarios are detailed below.

Cloud account instance not awake or active (for example, ServiceNow)

To rectify the error

1. Log in to the cloud application instance.
2. Navigate through the steps to reactivate or enable.
3. Verify using the SCIM client (for example, Postman).
4. Perform a **GET** operation for the endpoints mentioned below:
    - Schemas
    - ServiceProviderConfig
    - ResourceTypes
    - Users
    - Groups
5. Validate the cloud application instance credentials.
6. Edit and update the connection parameters for the connector at Starling subscription.

Function Host Down

To rectify the error

1. Log in to the Azure portal with the available credentials.
2. Navigate to the specific Function host and ensure that it is working.
3. Start the Function host, if it has been stopped.

Error 507 Insufficient Storage

Error 507 Insufficient Storage

To rectify the error

1. Ensure that the account has the ability to host additional user resources and group resources.
2. Repeat the steps of provision by providing values for all the mandatory fields.
3. Check and confirm that the resource has been provisioned.

Error messages

The following table consists of error messages that are returned, if different request wrapper properties are missing.

Table 2: Error messages

Request wrapper property	Error Code	Error message
Method	400	Required property missing in Request Wrapper
ClientRequest	400	Required property missing in Request Wrapper
Body	400	Required property missing in Request Body
targetURi	400	Required property missing in Request Wrapper
serviceCredentials	400	Required property missing in Request Wrapper
AuthenticationType	412	Unsupported authentication type
ConfigProperties	400	Required property missing in Request Wrapper
credential information (username, password, clientID, and so on)	400	Credential information missing in Request Wrapper
ConfigProperties	400	Required property missing in Request Wrapper (from connector)

Other error scenarios

Table 3: Other error scenarios

Error scenario	Work item
One Identity Manager 7.1.4 does not return any users for expired Starling Supervisor accounts after the successful completion of synchronization on any connector.	170884

About us

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 or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

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