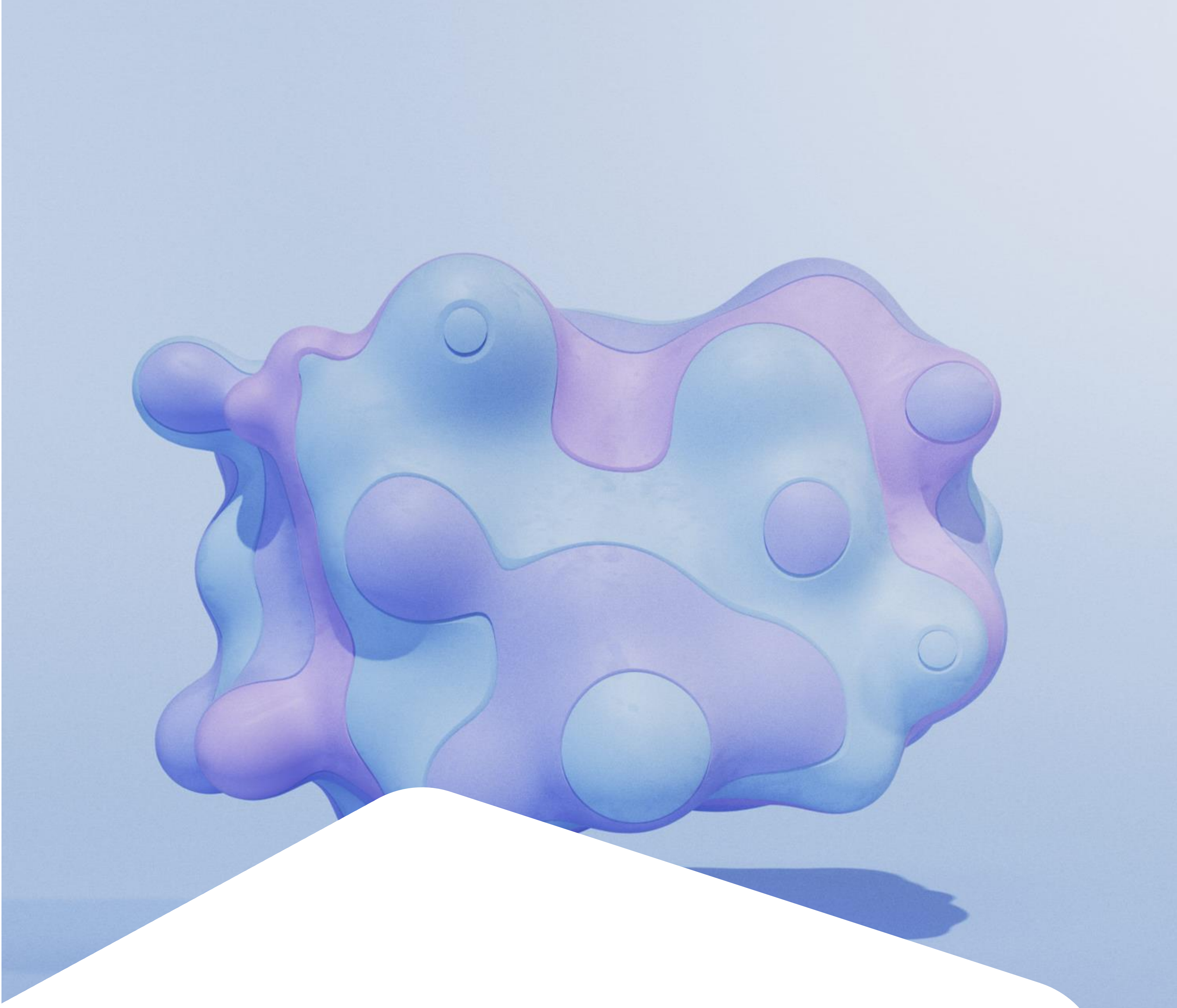


ONETRUST TO EQS DATASYNC MIGRATION

Guide on how to send HR Data to Compliance Cockpit

Table of Contents

1. Important Context: Connection to a New System and Vendor

As part of the migration process, your organization will be connected to a **new system** provided by a **new vendor (EQS)**. This marks a transition away from your existing setup in **Convercent** and/or **OneTrust**, where user and system data was previously sent and managed.

Going forward, data will be sent to the **EQS Compliance Platform** using **DataSync**, EQS's integration framework for user provisioning. This represents a new technical connection, configuration, and maintenance process - distinct from your previous vendor integrations.

It's important that technical teams involved in the migration understand this change, as new credentials, connection endpoints, and data mappings will need to be established and validated within EQS. This guide has been designed specifically to support migration customers through that setup, providing step-by-step instructions and mapping details to ensure a smooth transition.

2. Migration

All existing accounts in OneTrust will be created in EQS via the migration tooling. Employee ID will be a unique identifier for each user record, and this will be used for updating the user records in the future with DataSync or other user data imports. If you have Convercent Helpline along with OneTrust modules, Employee ID will be the unique identifier for the tooling so that it does not create duplicate records for users that exist in Convercent and in OneTrust.

After the migration tooling is completed, it is important to review the newly created users in EQS. We recommend validating email addresses and Employee IDs to ensure accuracy. This step helps guarantee that the DataSync connector can update these accounts correctly and avoids creating duplicate user records.

3. Flat File Integration

The first option we will review is flat file integration. This process is an automated process for ingesting a Microsoft Worksheet into the Compliance Platform. User records and their permissions can be managed by EQS retrieving files via SFTP actions. It is the customer's responsibility to host the FTP server and generate the file following the guidelines listed below.

- Customers will be responsible for maintaining their own FTP server.
- Clients will create an account for their EQS data synchronization.
- The file type will need to be converted from csv to XLSX

3.1. Attribute Mapping

Now let's compare the mandatory fields in OneTrust to EQS

OneTrust

Header	Accepted Values	Sample Values
First Name	String Text	Dorian
Last Name	String Text	Irvine
Employee Email Address	Valid Email Format	dorian.irvine@eqs.com
Employee ID	String Text	123
Is Active	True or False	True

EQS

Header	Accepted Values	Sample Values
First Name	String Text	Dorian
Last Name	String Text	Irvine
Email	Valid Email Format	dorian.irvine@eqs.com
Employee ID	String Text	123
Profile Status	Active or Inactive	Active

These attributes and their values will need to be updated in the new file format. The remaining supported fields in the EQS platform are listed below. Take the additional attributes from your OneTrust file template and map them to a corresponding EQS attribute.

Header	Accepted Values	Sample Values	Notes
Title	'Mr' 'Mrs'	Mr.	Any other values will cause errors in the upload.
Middle Name	String Text	Owen	
Academic Title	String Text	Dr.	

Job	String Text	Technical Consultant	
Department	String Text	Professional Services	If there are existing Locations present in Data Center, that value is displayed here. You cannot add a new Location. You can only add an existing Location name to the user. If you want to add a new value, then that should be done via the Attributes tab on Data Center or bulk upload via the Organization Attribute excel.
External Company	String Text	OneTrust	This column must be filled in the case of an external staff. For the internal staff, this column must be left empty.
Company Relationship	Employee, Freelancer, Consultant, Vendor, Contractor, or left empty	Employee	If the employee is an internal staff, this field can be empty, or 'Employee' should be added An external staff can be described as 'Freelancer', 'Consultant', 'Vendor', 'Contractor', etc.
Phone	Numbers, Parentheses, Dashes, and Addition sign	+1 (719) 240-8679	
Mobile	Numbers, Parentheses, Dashes, and Addition sign	+1 (719) 240-8679	
Supervisor's Email	Valid Email Format	ryan.mcneal@eqs.com	
Tags	String Text	Cast; TeamLife; HR	Please, ensure each tag is delimited by semicolon (;)
Business Unit	String Text	Ethics	If there are existing Locations present in Data Center, that value is displayed here. You cannot add a new Location. You can only add an existing Location name to the user. If you want to add a new value, then that should be done via the Attributes tab on Data Center or bulk upload via the Organization Attribute excel.

Location	String Text	Denver	If there are existing Locations present in Data Center, that value is displayed here. You cannot add a new Location. You can only add an existing Location name to the user. If you want to add a new value, then that should be done via the Attributes tab on Data Center or bulk upload via the Organization Attribute excel.
Country	ISO 3166-1 alpha-2 format	DE	Please, use the two-letter country codes as per ISO 3166-1: https://en.wikipedia.org/wiki/ISO_3166-1_alpha-2
Preferred Language	See section 3.2	en	Empty fields will be set to your company language.
Hire Date	ISO 8601 format	2021-09-30	
*Roles	Roles that are already set in Data Center	it-manager	All users are automatically added to the employee role - this does not need to be entered here. If a user should have another role in addition to the employee role, then enter it here. Please, only use role identification of roles that are already set in Data Center. The role identification can be found on the bottom left corner of the role cards in the permissions overview of Data Center. See example below. Multiple roles are separated by a semicolon (;).

3.1.1. Additional Guidance on Role Assignment

Role column is optional in DataSync. If Role is included, the values will override any existing role assignments, including those migrated via tooling. Adding a role column increases complexity and may result in incorrect access permissions.

We recommend omitting the role column unless:

- You have three (3) or fewer roles (e.g., Admin, Supervisor, Employee).

- You are 100% confident your team can assign roles accurately on a user-by-user basis.

If uncertain, it's safer to manage roles manually post-migration to avoid wiping or misassigning access.

3.1.2. Custom User Attributes

Currently, only the Default Attributes above are supported for user provisioning via SCIM. Support for Custom User Attributes (CUA) is scheduled for Spring 2026. CUA are supported by Manual Bulk Imports and SFTP connections. This allows organizations to define and manage their own user profile fields—going beyond the system-defined Default User Attributes currently supported on our platform.

Attribute types that are supported for CUA are the following:

- String Text
- Numerical
- Date (YYYY-MM-DD)

3.1.3. PGP Encryption

EQS will provide the public key that is generated in the DataSync Connector. *Customer can* use the generated key to encrypt files from their SFTP server. Key can be updated or turned off at any time.

3.1.4. SSH Authentication

EQS supports multiple authentication methods into SFTP servers including SSH keys. The client is required to generate the key pair and seed the private key in the data sync connector. The public key will be installed on the SFTP server for the EQS user account.

3.2. Preferred Language Attribute Values

'en' for English	'zh_TW' for Chinese Traditional
'ar' for Arabic	'zh_CN' for Chinese Simplified
'de' for German	'cs' for Czech
'de-ch' for Swiss German	'ko' for Korean
'nl' for Dutch	'th' for Thai
'fr' for French	'mg' for Malagasy
'ru' for Russian	'ro' for Romanian
'it' for Italian	'pl' for Polish

'es' for Spanish	'sv' for Swedish
'pt' for Portuguese	'ja' for Japanese
'pt_BR' for Portuguese (BR)	'hu' for Hungarian

3.3. Step-by-Step Configuration Process

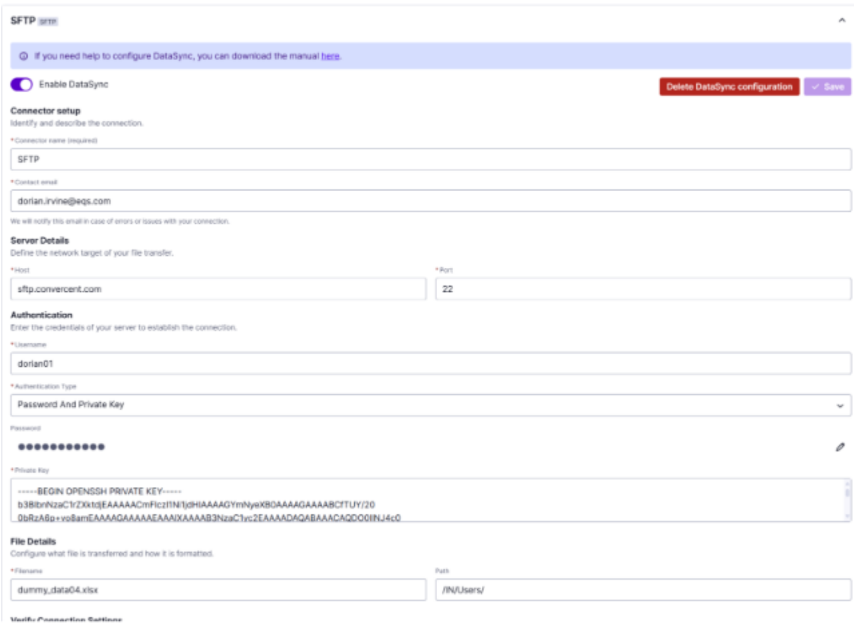
01. Log into EQS Compliance Cockpit with your user credentials.

02. Click the gear icon on the top-right to open the sidebar settings.

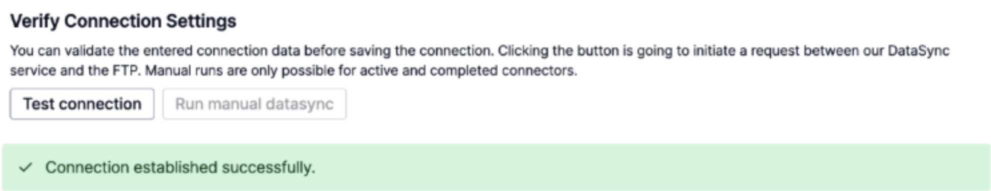
03. Select "DataSync Configuration," then click the "Add DataSync" button to open the connector creation dialog.

04. Make sure the "SFTP/FTPS" connector is selected in the dropdown and enter a name for your connector with the connection configuration, then click the "Create" button.

05. A new connector configuration panel is shown in the "DataSync Configuration" section. It displays connection configuration as well specifics like the file name and type. Authentication types that are supported are username and password or username and SSH private keys. Be sure to add the file under a folder and to add a "slash" (/) before and after the folder name in the Path input. The connector is disabled by default, which means EQS Data Center will not execute the Automatic Sync.



06. A test connection button is available to test the configuration.



07. Review the roles & permissions in the Data Center. By default, the below two roles will be present within the Roles & Permissions tab. These two roles cannot be deleted.

- Employee: All the employees within the organization have access to the Integrity Hub with Approvals, Policies and Policy Buddy.
- Admin: All admins who will have access to EQS Compliance COCKPIT, Approvals and Data Center and all other active modules.

08. Customized roles and permissions can be created via the Roles & Permissions tab. Create any new roles necessary for the implementation. Additional information on the scope of permissions for roles can be found here: https://support-center.eqs.com/s/article/Default-Roles

09. All roles must be created as an app role in the enterprise application of the identity provider. Remember that the value must be the same as the Role slug name in EQS Compliance Cockpit Data Center module.

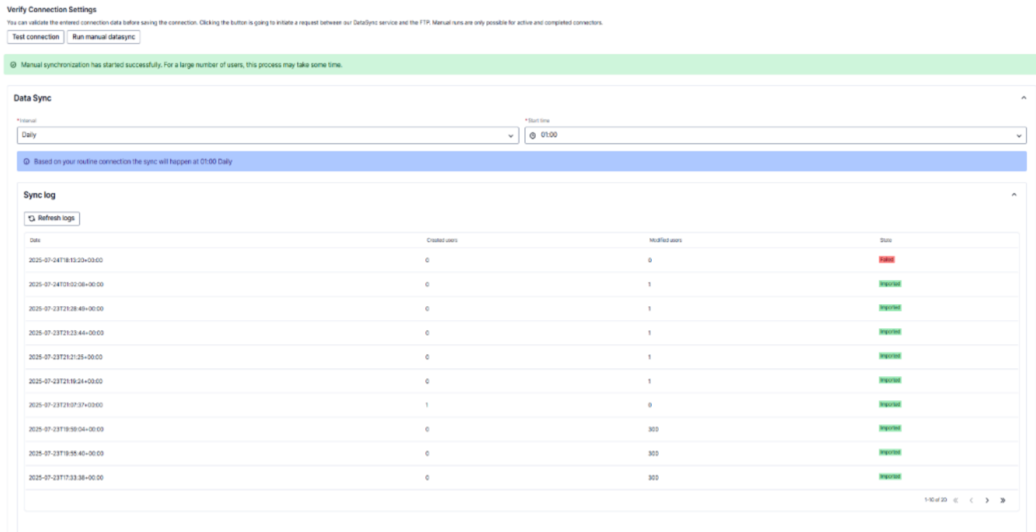
3.4. Data Testing & Production Configuration

01. Generate a test file containing minimum employees and deliver to the SFTP site. It is recommended to only list project employees in the file.

02. Select Run Manual DataSync button

03. A notification will appear stating "Manual synchronization has started successfully. For a large number of users, this process may take some time.

04. Select the 'Refresh Logs' button and the file import's processing results will be available via XLSX downloadable error log or viewable JSON payload.



Payload

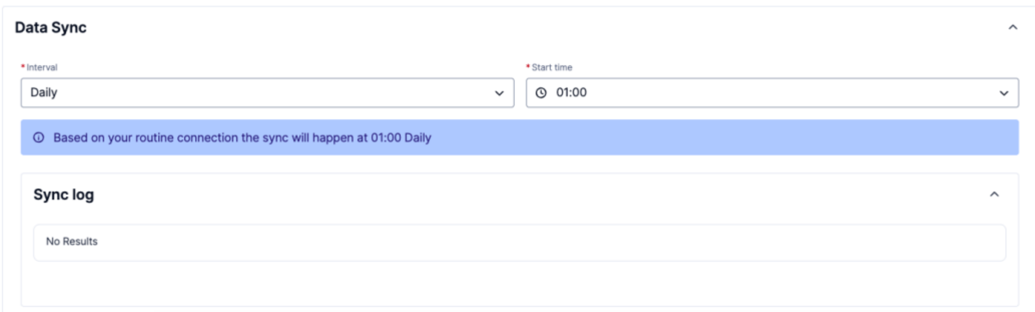
```
{
 "BulaTest02@sjjg7.onmicrosoft.com": [
  null,
  null,
  null,
  null,
  "BulaTest02@sjjg7.onmicrosoft.com",
  null,
  null,
  "666666666666666",
  "TCA",
  null,
  null,
  null,
  null,
  null,
  null,
  [],
  null,
  null,
  "Active",
  [
   "admin"
  ],
  null
 ]
}
```

Errors

```
[
 "firstName: This value should not be blank.",
 "lastName: This value should not be blank."
]
```


05. Review the provisioning log and make necessary updates to the HR data file based on error messages. Additionally, check newly created employees and validate that attribute mapping & role synchronization is as expected.

06. Once testing is approved for production ready imports you can define the frequency for which the provisioning will execute. For that we have the Data Sync panel with all executed synchronizations, manual or automatic. (don't forget to save using the top right button in the panel). If selecting monthly or weekly intervals, then synchronization will occur on the first day of the month or week.



07. Now we can enable Data Synchronization with this toggle (don't forget to save using the top right button in the panel):

08. Once the Data Synchronization is enabled the automatic data synchronization will take place in the next opportunity. A manual trigger for synchronization is also available.

4. System for Cross-domain Identity Management (SCIM)

4.1. Overview and Comparison between OneTrust and EQS

SCIM implementation on the EQS platform is largely the same as it was with OneTrust. Both platforms utilize the open-standard 2.0 version protocol. EQS supports a wider range of attributes that can be assigned to user accounts. A JSON-Schema definition of all employee objects which can be sent to EQS Data Center can be found at this link: api-compliance.eqscockpit.com/data-center/api/datasync/scim/Schemas

The main difference between the two platforms is management of role synchronization. OT managed role assignments by utilization of user groups that assigned roles via membership. On EQS, roles are assigned on the account level during the provisioning process. An important callout to make is that with role synchronization enabled the system will de-assign the roles in Compliance Cockpit that your users do not have assigned via the SCIM configuration.

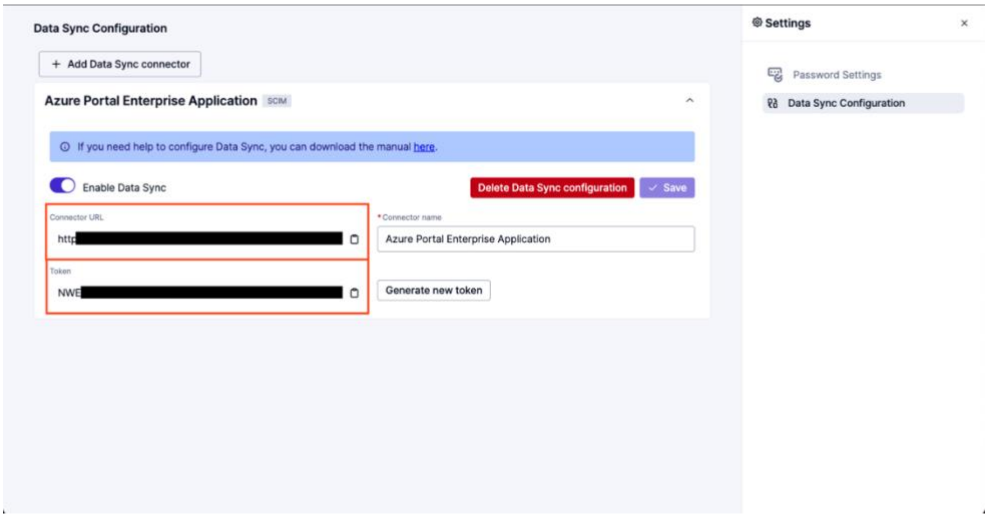
4.2. DataSync Configuration

01. Log into EQS Compliance Cockpit with your user credentials.

02. Click the gear icon on the top-right to open the sidebar settings.

03. Select "DataSync Configuration," then click the "Add DataSync" button to open the connector creation dialog.

04. Make sure the "SCIM" connector is selected in the dropdown and enter a name for your connector, then click the "Create" button.



05. A new connector configuration panel is shown in the "DataSync Configuration" section. It displays two important fields: the connector URL and the token. Please save the displayed token value. The token is sensitive information and should be kept in a safe space. You are not going to be able to view the token again. If you lose your token, you must generate a new one, invalidating the previous one. You can do this via the "Generate new token" button. This displayed connector URL, and token is going to be configured in your identity provider in the next steps. The connector is enabled by default. If you disable it, every request made to this connector is going to be rejected by the EQS Data Center.

06. Open the enterprise application in your identity provider for EQS and enter the credentials generated from DataCenter.

07. Test if the connection is successful

08. Now we need to configure the attribute mapping, so which user information that you want to send to the EQS Data Center for each user using the SCIM schema hyperlink in section 2.1

4.3. Attribute Mapping

01. Required attributes for user provisioning are the following fields:

- Id
- userName (the email used for login)
- familyName
- GivenName

02. "employeeNumber" is not a required field but is strongly recommended and set as the highest priority for matching precedence. This will allow for updating migrated accounts with lowest risk of duplication of user accounts.

03. Set “userName” as second priority for matching precedence.

04. An important callout is the attribute “emails” solely exists as compatibility with SCIMs default mapping, as our platform does not have support for multiple e-mails and the single e-mail that employee may have is “userName”. Therefore, this is marked as read-only field.

05. Complete mappings for remaining system attributes that are wanted to display in Data Center.

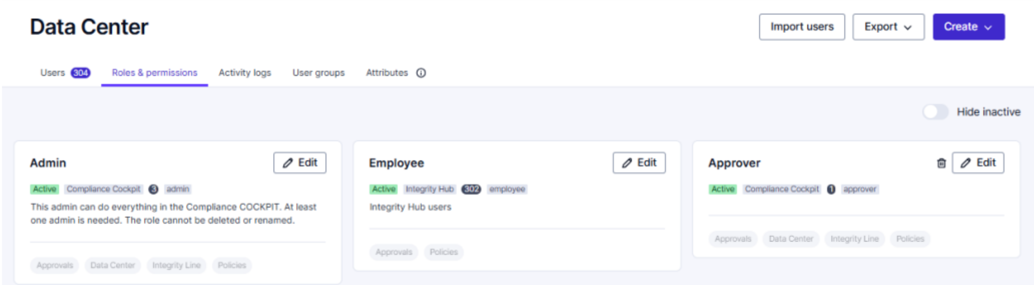
4.4. Role Synchronization

01. Now you must add a feature flag by adding query parameter **aadOptscim062020** to SCIM URL. This is to make de-assignments work.

- A new attribute mapping must be defined for role assignment. This attribute requires **Expression** mapping type equal to **AssertiveAppRoleAssignmentsComplex([appRoleAssignments])** to the target attribute roles.

02. Login to Compliance Cockpit and review the roles & permissions in the Data Center. By default, the below two roles will be present within the Roles & Permissions tab. These two roles cannot be deleted.

- Employee: All the employees within the organization have access to Integrity Hub with Approvals, Policies and Policy Buddy.
- Admin: All admins who will have access to EQS Compliance COCKPIT, Approvals and Data Center and all other active modules.



03. Customized roles and permissions can be created via the Roles & Permissions tab. Create any new roles necessary for the implementation. Additional information on the scope of permissions for roles can be found here: https://support-center.eqs.com/s/article/Default-Roles

04. All roles must be created as an app role in the enterprise application of the identity provider. Remember that the value must be the same as the Role slug name in EQS Compliance Cockpit Data Center module.

4.5. *Data Testing & Automatic Provisioning*

01. Assign a single user or small group of employees that are aware of project implementation to the enterprise application with their desired role.

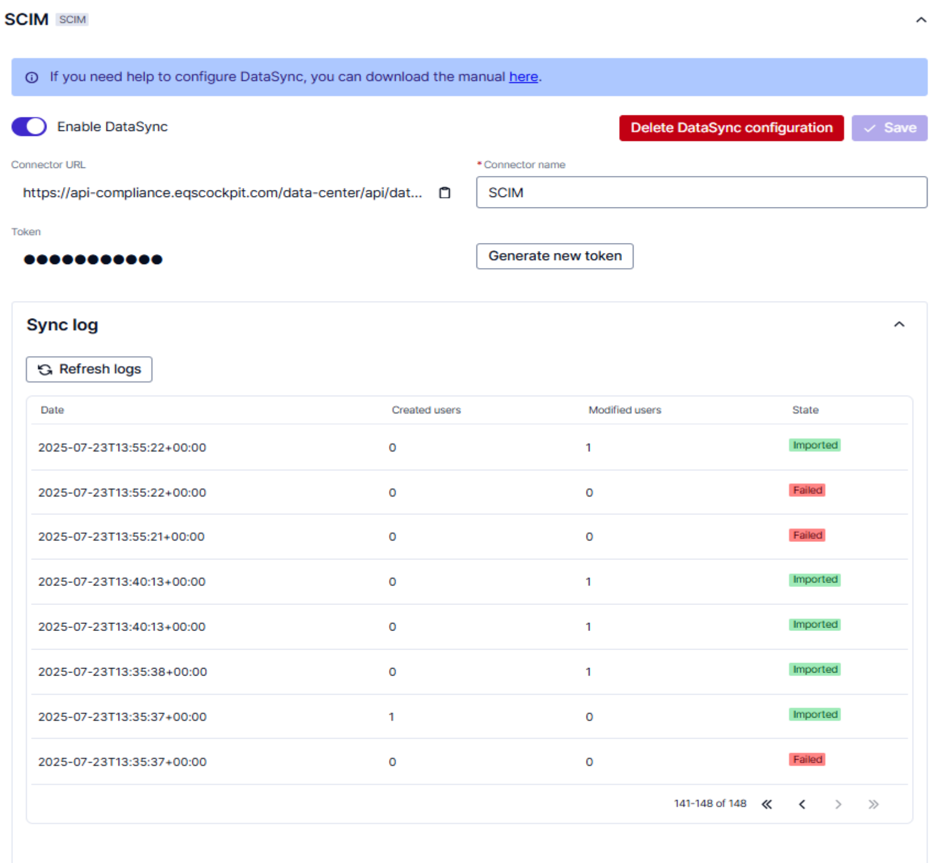
02. Review the provisioning logs from the identity provider for record errors.

03. Compare the provisioning logs to the Sync Log in EQS and validate that user or group creation is functioning as expected. The sync log allows a downloadable JSON file and viewable JSON payload.

Example Payload:


```
{
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:User",
    "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
    "urn:ietf:params:scim:schemas:eqs:datacenter:1.0:User"
  ],
  "meta": {
    "resourceType": "User"
  },
  "userName": "dorian.irvine@noemail.com",
  "displayName": "Dorian Irvine",
  "active": "true",
  "locale": "en-US",
  "preferredLanguage": "en-US",
  "userType": "Internal",
  "title": "Technical Consultant",
  "hireDate": "2027-01-01",
  "name": {
    "honorificPrefix": "Mr",
    "givenName": "Dorian",
    "middleName": "Nathanial Owen",
    "familyName": "irvine"
  },
  "emails": [
    {
      "type": "work",
      "value": "dorian.irvine@noemail.com",
      "primary": true
    }
  ],
  "phoneNumbers": [
    {
      "type": "work",
      "value": "+1-512-522-5468",
      "primary": true
    },
    {
      "type": "mobile",
      "value": "303-970-9867"
    }
```

```
  ],
  "roles": [
    {
      "type": "Postman",
      "value": "Admin",
      "display": "Admin"
    },
    {
      "type": "Postman",
      "value": "Employee",
      "display": "Employee"
    },
    {
      "type": "Postman",
      "value": "approver",
      "display": "Approver"
    }
  ],
  "addresses": [
    {
      "type": "work",
      "country": "US"
    },
    {
      "type": "home",
      "region": "Colorado",
      "country": "US",
      "locality": "Colorado Springs",
      "formatted": "Colorado Springs",
      "postalCode": "80218",
      "streetAddress": "321 Fake Street"
    }
  ],
  "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User": {
    "employeeNumber": "X201",
    "department": "Professional Services",
    "manager": {
      "value": "8d131acd-5341-4219-824d-98fe5913b381",
      "$ref": "https://api-compliance.eqscockpit.com/data-center/api/datasync/scim/56297f2c-bcd3-403b-870f-1dfd2948f4a6/Users/8d131acd-5341-4219-824d-98fe5913b381"
    }
  },
  "urn:ietf:params:scim:schemas:eqs:datacenter:1.0:User": {
    "academicTitle": "Professor",
    "tags": [
      "Postman",
      "API"
    ],
    "businessUnitName": "Development",
    "preferredCurrencyCode": "USD"
  }
}
```



04. Troubleshoot any errors or unexpected results from provisioning.

05. Once data synchronization has been validated and signed off by primary stakeholders all users & groups that need access to the application need to be assigned to the enterprise application with their desired roles.

06. If users need several roles they can be assigned multiple times in the enterprise application under different roles.

07. Enable automatic provisioning in the identity provider.