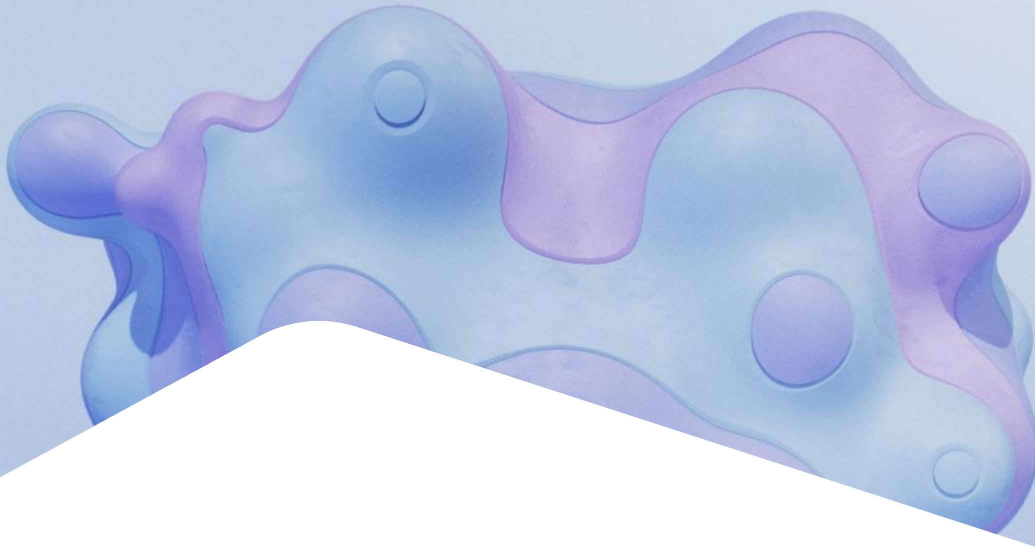


HR DATA – ONETRUST TO EQS MIGRATION

Introduction to Data Center

Table of Contents

1. Flat File Integration

- Customer will be responsible for maintaining their own FTP server.
- Clients will create an account for their EQS data synchronization. Account must have username and password credentials.
- The file type will need to be converted from csv to XLSX
- An important callout to make is the system will de-assign the roles in Compliance Cockpit that users do not have assigned via the flat file integration.

1.1. 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
Status	Active/Inactive	Active
Roles	Roles that are already set in Data Center	Site Admin

- 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 attributes.

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.	
Preferred Language	Noted Below Table	en	Empty fields will be set to your company language. Please note that some languages may not be available depending on the options you have subscribed to.

Employee ID	String Text	123	Primary Key of Account
Job Title	String Text	Technical Consultant	
Department	String Text	Professional Services	
Company	String Text	Convercent	This column must be filled in the case of 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 only	1231231234	
Mobile	Numbers only	1231231234	
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	
Country	Two letter country codes	DE	Please, use the two-letter country codes as per ISO 3166-1: https://en.wikipedia.org/wiki/ISO_3166-1_alpha-2
*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 (;).

1.2. Upcoming features (targeting September)

*1.2.1. *Additional Guidance on Role Assignment*

Role column is optional in DataSync for SCIM but mandatory for SFTP until future product features are released. Expecting September release. If Role is included, the values will override any existing role assignments, including those migrated via tooling. Adding a role column increases complexity and introduces risk of misassignment.

We recommend omitting the role column unless:

- You have three 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.

1.2.2. Future Enhancement: Custom User Attributes

Currently, only the Default Attributes above are supported for user provisioning via DataSync. Custom User Attribute (CUA) support is slated for release in September and will allow organizations to define and manage their own user profile fields—going beyond the system-defined Default User Attributes currently supported in our platform.

1.2.3. Future Enhancement: SSH Authentication and PGP Encryption

SSH Authentication and PGP Encryption are not yet available for the SFTP DataSync Connector. Support for these is slated to be released in late September / early October.

1.3. Preferred Language Attribute Values

'en' for English
'ar' for Arabic
'de' for German
'de-ch' for Swiss German
'nl' for Dutch
'fr' for French
'ru' for Russian
'it' for Italian

'es' for Spanish
'pt' for Portuguese
'pt_BR' for Portuguese (BR)
'zh_TW' for Chinese Traditional
'zh_CN' for Chinese Simplified
'cs' for Czech
'ko' for Korean
'th' for Thai
'mg' for Malagasy
'ro' for Romanian
'pl' for Polish
'sv' for Swedish
'ja' for Japanese
'hu' for Hungarian

1.4. Step-by-Step Configuration Process

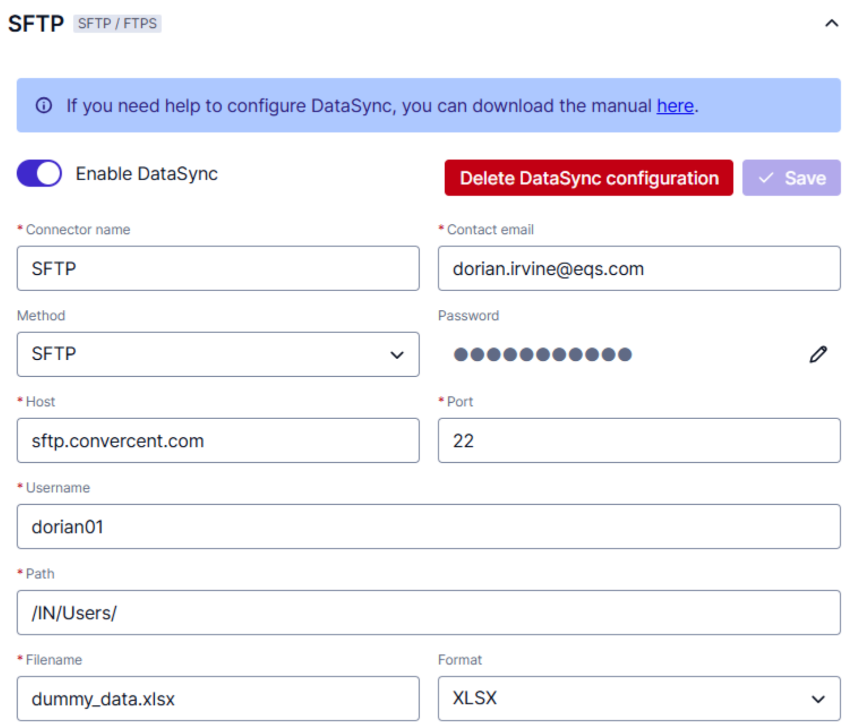
01. Log into EQS Compliance Cockpit with your user credentials.

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

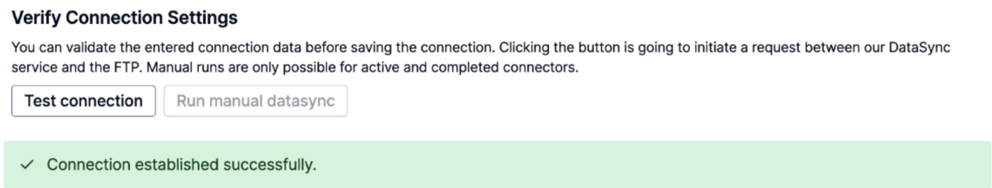
03. Select “DataSync Configuration,” then click the “Add DataSync” button to open the connector creation dialog.

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. 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 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.

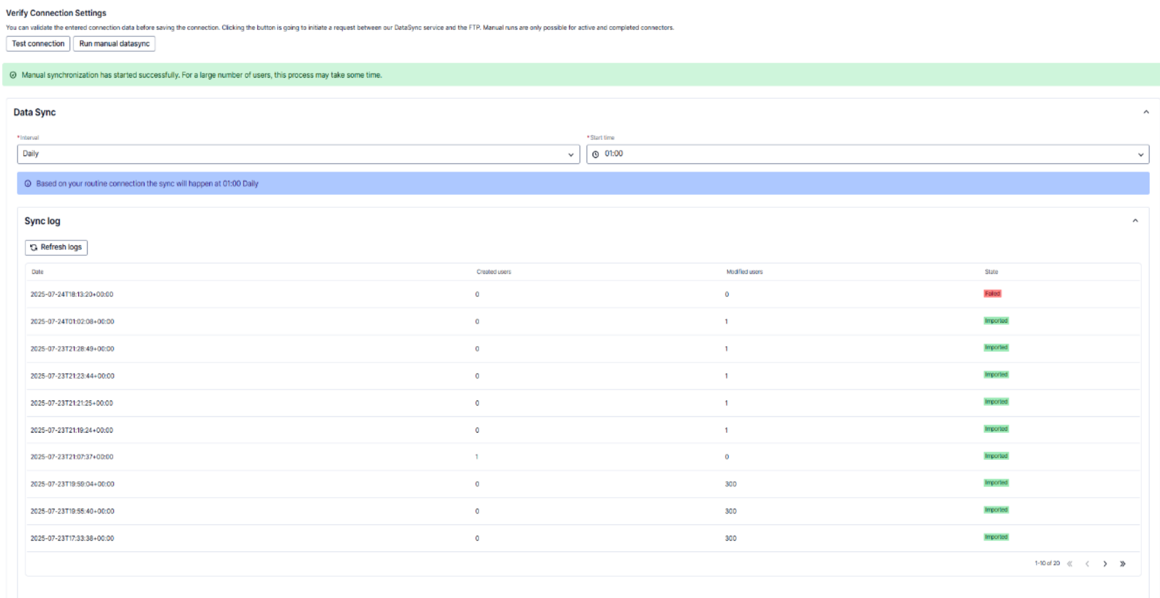
1.5. Data Testing & Production Configuration

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 downloadable error log or viewable JSON payload.



Payload

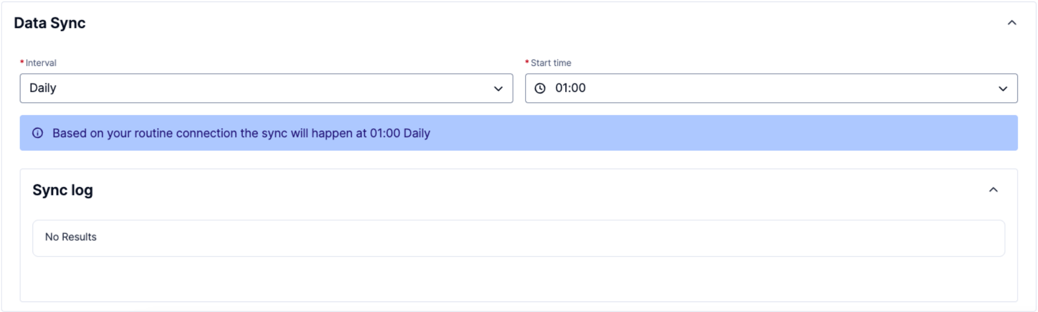

```
{
 "BulaTest02@sjjg7.onmicrosoft.com": [
  null,
  null,
  null,
  null,
  "BulaTest02@sjjg7.onmicrosoft.com",
  null,
  null,
  "666666666666666",
  "TCA",
  null,
  null,
  null,
  null,
  null,
  null,
  [],
  null,
  null,
  "Active",
  [
   "admin"
  ],
  null
 ]
}
```


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 of the synchronization is also available.

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

2.1. Overview and product 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: https://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. Assignment of roles via SCIM is mandatory in the implementation. 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.

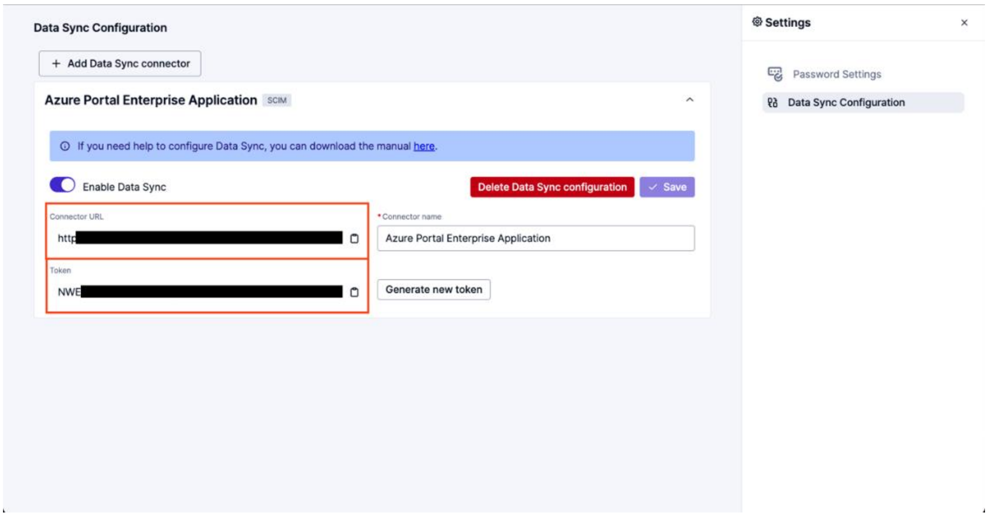
2.2. DataSync Configuration

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 Azure enterprise application 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

2.3. Role Synchronization

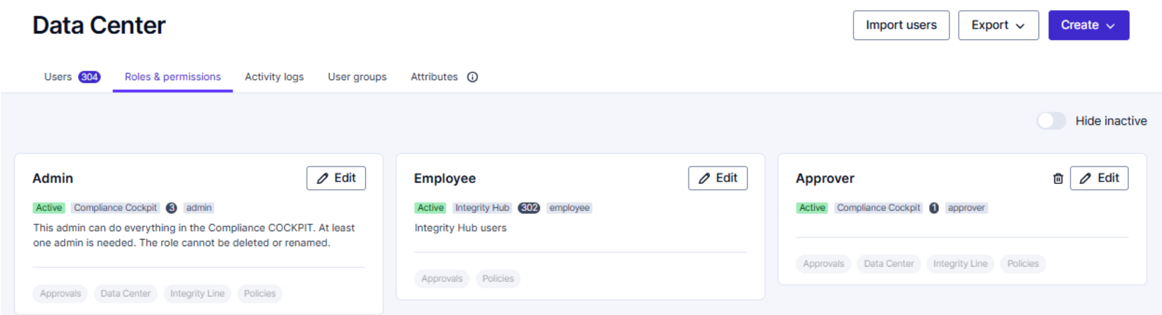
01. Now you must add a feature flag by adding query parameter aadOptscim062020 to SCIM URL. This is to make de-assignments work.

02. 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***.

03. 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.



04. 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

05. 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.

2.4. Data Testing & Automatic Provisioning

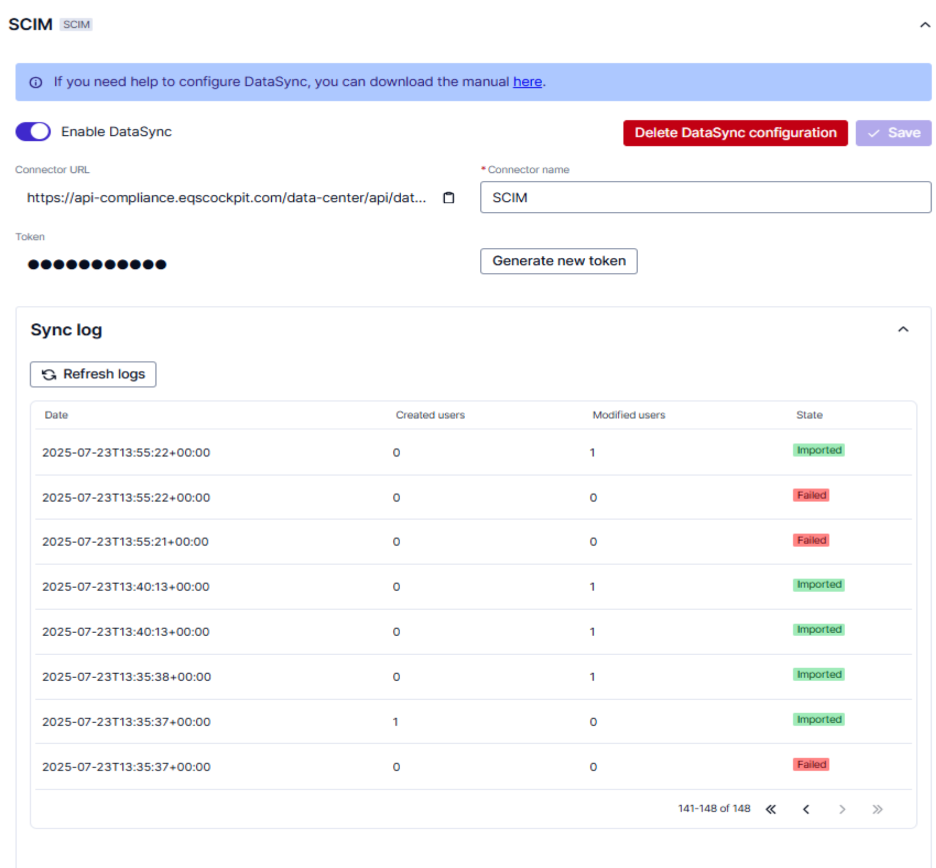
01. Assign a single user or small group of employees that are aware of project implementation to the enterprise application with their desired role.

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:


```
{
 "meta": {
  "resourceType": "User"
 },
 "name": {
  "givenName": "Dorian",
  "familyName": "Irvine"
 },
 "roles": [
  {
   "type": "WindowsAzureActiveDirectoryRole",
   "value": "admin",
   "display": "Admin",
   "primary": false
  }
 ],
 "title": "Technical Implementation Consultant",
 "active": true,
 "emails": [
  {
   "type": "work",
   "value": "dorian.irvine@sjjg7.onmicrosoft.com",
   "primary": true
  }
 ],
 "schemas": [
  "urn:ietf:params:scim:schemas:core:2.0:User",
  "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User"
 ],
 "userName": "dorian.irvine@sjjg7.onmicrosoft.com",
 "addresses": [
  {
   "type": "work",
   "region": null,
   "country": "FI",
   "primary": false,
   "locality": null,
   "formatted": null,
   "postalCode": null,
   "streetAddress": null
  }
 ],
 "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User": {
  "department": "Professional Services",
  "employeeNumber": "15612"
 }
}
```



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