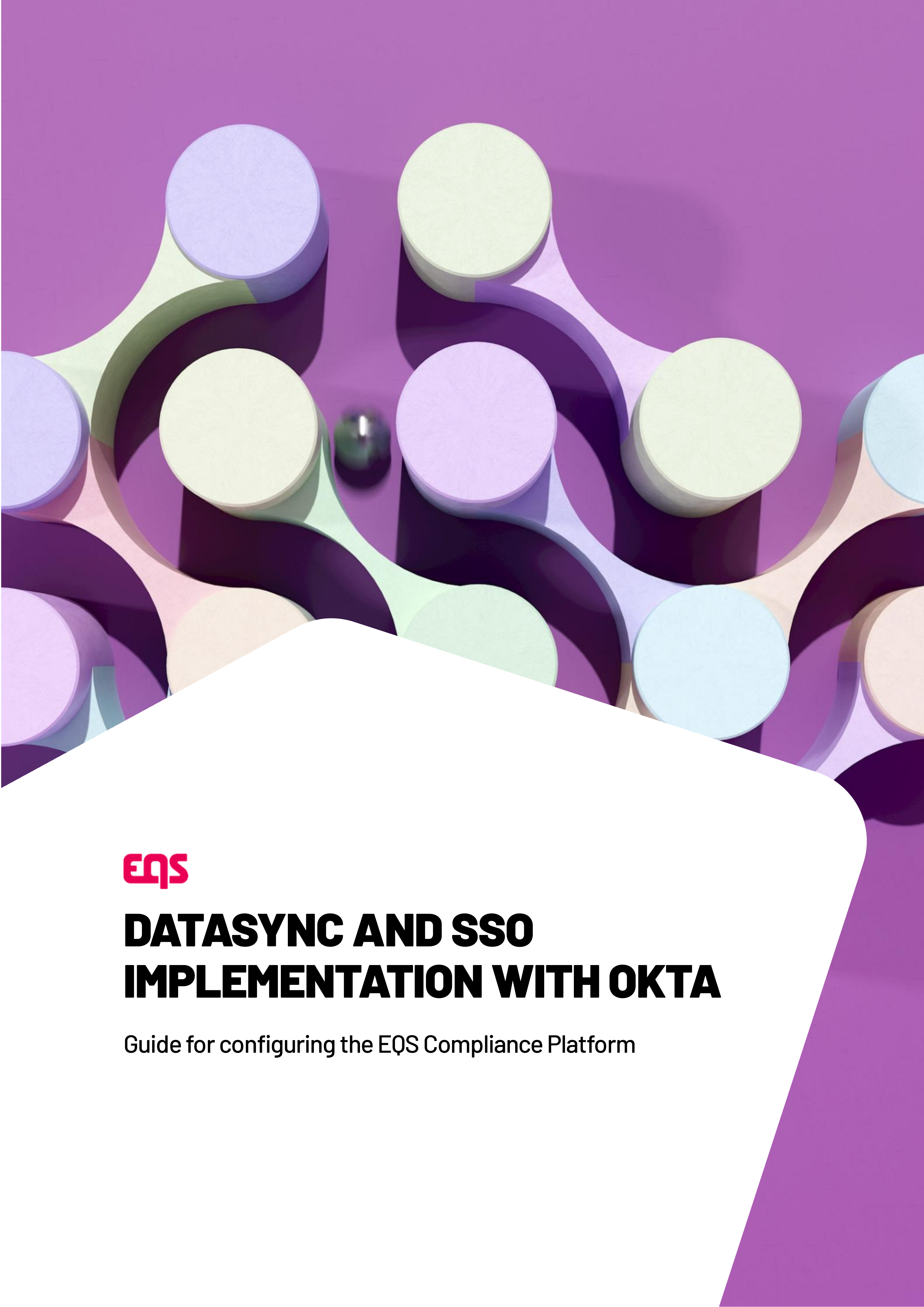


DATASYNC AND SSO IMPLEMENTATION WITH OKTA

Guide for configuring the EQS Compliance Platform

Table of Contents

1. SSO Configuration in Okta

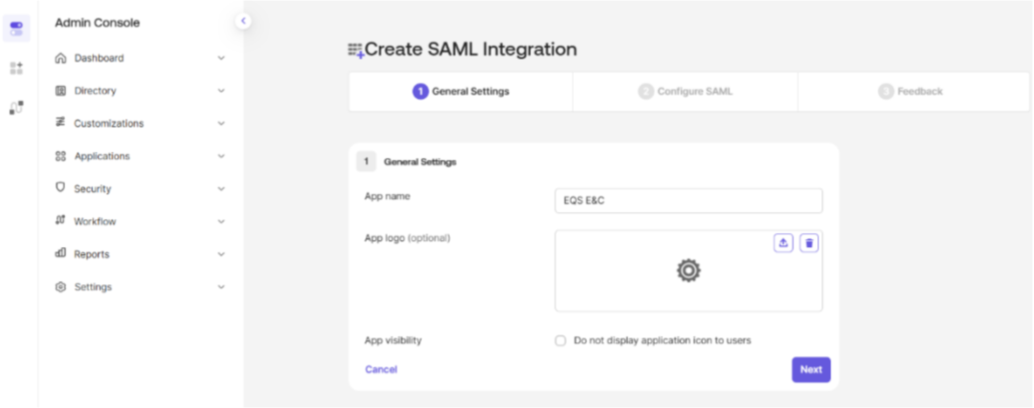
1.1. Create a new Application in your Okta portal.

01. Navigate to the Okta portal home page: https://login.okta.com

02. Select **Admin Console** and then **Applications.**

03. Create a new App Integration and select **SAML 2.0** based.

04. In the **App name** field, enter a name for your new web application then select **next.**



App name: EQS E&C

App logo (optional)

App visibility: □ Do not display application icon to users

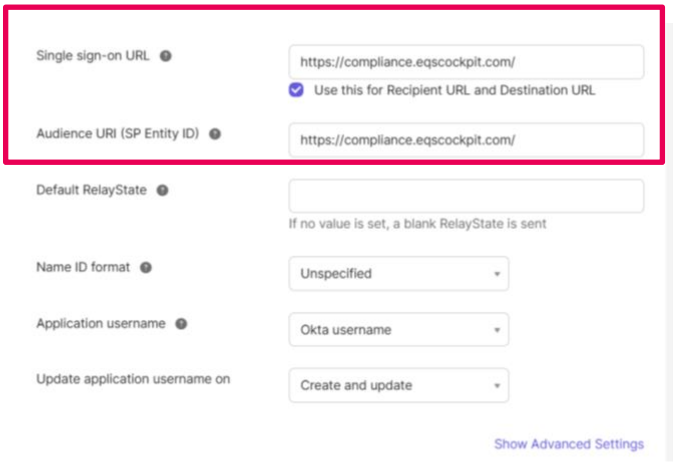
1.2. Create SAML Integration

Because SAML configuration between Okta and EQS Compliance COCKPIT is interdependent, it is not possible to fully configure either system in isolation. We recommend that you begin your configuration in Okta.

Okta requires placeholder values in the Single Sign-On URL (Recipient & Destination URL) and Audience URI (SP Entity ID) to complete the initial SAML configuration. These placeholder values will be replaced later, once you generate the required metadata in EQS Compliance COCKPIT.

01. Enter placeholder values for **Single Sign-On URL** and **Audience URI**

02. In this example, https://compliance.eqscockpit.com/ is used as a temporary placeholder for both fields. These values are not final. You will return to this configuration after setting up the Service Provider in EQS Compliance COCKPIT and obtaining the actual metadata.



Single sign-on URL: https://compliance.eqscockpit.com/

☑ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID): https://compliance.eqscockpit.com/

Default RelayState:

If no value is set, a blank RelayState is sent

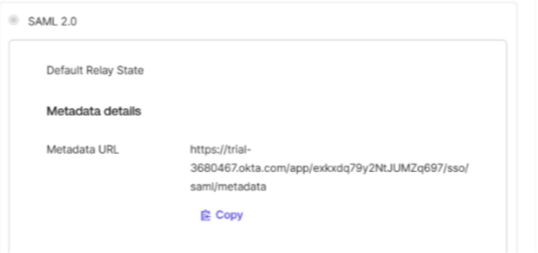
Name ID format: Unspecified

Application username: Okta username

Update application username on: Create and update

03. After selecting **next** a new tab will appear asking to fill out an Okta Support Questionnaire. This can be skipped by selecting **Finish.**

04. Copy the **Metadata URL** from your SAML configuration. You will use this to create a new SAML connector in EQS Compliance COCKPIT



SAML 2.0

Default Relay State

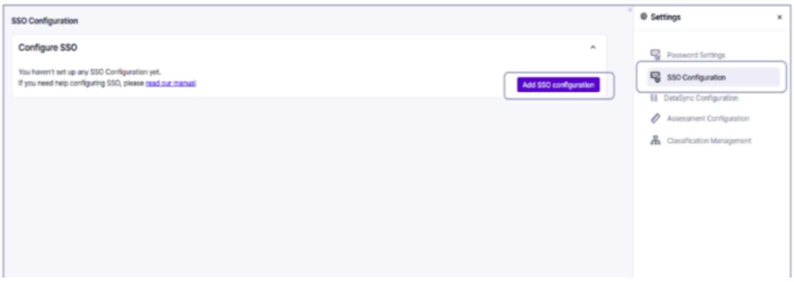
Metadata details

Metadata URL: https://trial-3680467.okta.com/app/exkxdq79y2NtJUMZq697/sso/saml/metadata

1.3. Create a new SAML connector in EQS Compliance COCKPIT

01. Login into EQS Compliance COCKPIT with your user credentials

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



SSO Configuration

Configure SSO

You haven't set up any SSO Configuration yet.
If you need help configuring SSO, please read our manual

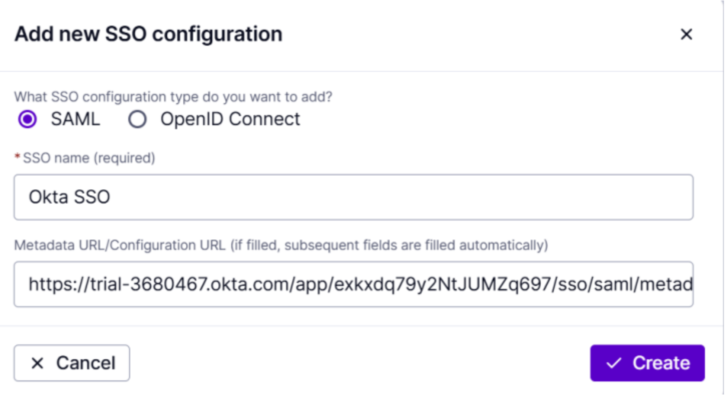
03. Select **SSO Configuration**, then click **Add SSO configuration** button to open the connector creation dialog.

04. Select the **SAML** radio button under **What SSO configuration type do you want to add?**

05. Enter an **SSO name** for your SAML connector (required)

06. In the **Metadata URL** field, add the **Application Metadata URL** that you pulled from your Okta Application in Section 1.2 Step 4

07. Click the **Create** button to create the new SSO configuration.



Add new SSO configuration ×

What SSO configuration type do you want to add?

● SAML ○ OpenID Connect

* SSO name (required)

Okta SSO

Metadata URL/Configuration URL (if filled, subsequent fields are filled automatically)

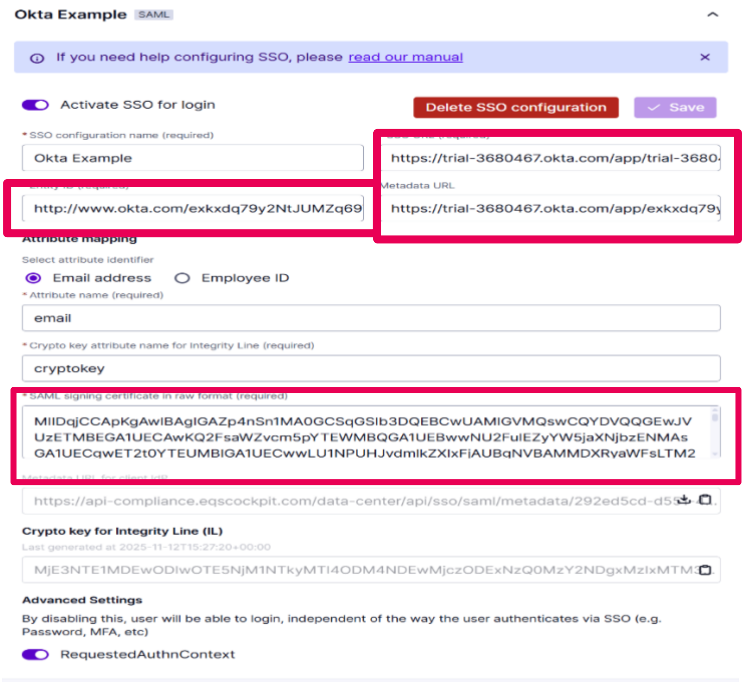
https://trial-3680467.okta.com/app/exkxdq79y2NtJUMZq697/sso/saml/metad

× Cancel ✓ Create

08. A new SAML connector configuration section is displayed on the **SSO Configuration** page. The application uses the **Metadata URL** to automatically populate the **SSO URL, Entity ID, Metadata URL** and the **SAML signing certificate in raw format** when the connector is created.

09. Select the **Email address** radio button under Attribute mapping.

10. Type **email** in the Attribute name (required) field.



Okta Example SAML

If you need help configuring SSO, please read our manual ×

Activate SSO for login

Delete SSO configuration ✓ Save

* SSO configuration name (required)

Okta Example

https://trial-3680467.okta.com/app/trial-3680

http://www.okta.com/exkxdq79y2NtJUMZq69

Metadata URL

https://trial-3680467.okta.com/app/exkxdq79y

Attribute mapping

Select attribute identifier

● Email address ○ Employee ID

* Attribute name (required)

email

* Crypto key attribute name for Integrity Line (required)

cryptokey

* SAML signing certificate in raw format (required)

MIIDqjCCApKgAwIBAgIGAZp4nSn1MA0GCSqGSIb3DQEBCwUAMIGVMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAs
GA1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXIxFjAUBgNVBAMMDXRyaWFsLTM2

Metadata URL for client IdP

https://api-compliance.eqscockpit.com/data-center/api/sso/saml/metadata/292ed5cd-d55

Crypto key for Integrity Line (IL)

Last generated at 2025-11-12T15:27:20+00:00

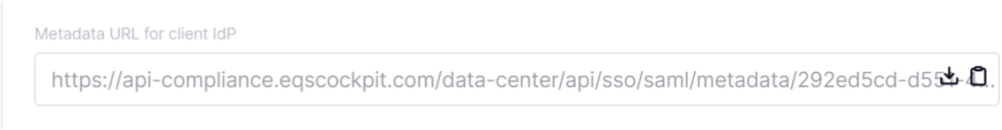
MjE3NTE1MDEwODIwOTE5NjM1NTkyMTI4ODM4NDEwMjczODExNzQ0MzY2NDgxMzIxMTM3

Advanced Settings

By disabling this, user will be able to login, independent of the way the user authenticates via SSO (e.g. Password, MFA, etc)

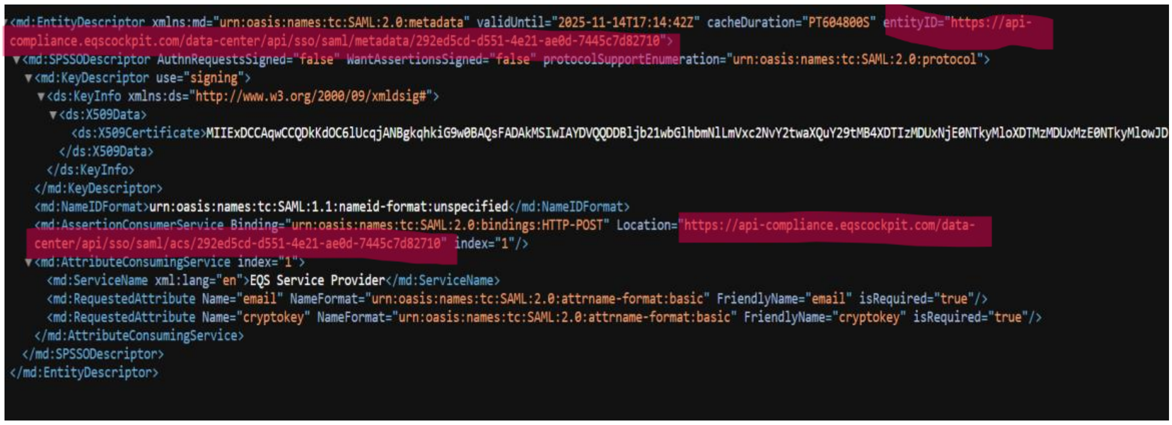
RequestedAuthnContext

11. Click the download icon next to the **Metadata URL for client IDP** to gather the **Entity ID and Assertion Consumer Service URL**



Metadata URL for client IdP

https://api-compliance.eqscockpit.com/data-center/api/sso/saml/metadata/292ed5cd-d55



```
▼<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2025-11-14T17:14:42Z" cacheDuration="PT604800S" entityID="https://api-
compliance.eqscockpit.com/data-center/api/sso/saml/metadata/292ed5cd-d551-4e21-ae0d-7445c7d82710">
 ▼<md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  ▼<md:KeyDescriptor use="signing">
   ▼<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    ▼<ds:X509Data>
       <ds:X509Certificate>MIIExDCCAqwCCQDkKdOC6lUcqjANBgkqhkiG9w0BAQsFADAkMSIwIAYDVQQDDBljb21wbGlhbmNlLmVxc2NvY2twaXQuY29tMB4XDTIzMDUxNjE0NTkyMloXDTMzMDUxMzE0NTkyMlowJD
     </ds:X509Data>
    </ds:KeyInfo>
  </md:KeyDescriptor>
  <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
  <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://api-compliance.eqscockpit.com/data-
  center/api/sso/saml/acs/292ed5cd-d551-4e21-ae0d-7445c7d82710" index="1"/>
 ▼<md:AttributeConsumingService index="1">
    <md:ServiceName xml:lang="en">EQS Service Provider</md:ServiceName>
    <md:RequestedAttribute Name="email" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="email" isRequired="true"/>
    <md:RequestedAttribute Name="cryptokey" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="cryptokey" isRequired="true"/>
  </md:AttributeConsumingService>
 </md:SPSSODescriptor>
</md:EntityDescriptor>
```

12. In the example above:

Entity ID: https://api-compliance.eqscockpit.com/data-center/api/sso/saml/metadata/292ed5cd-d551-4e21-ae0d-7445c7d82710

Assertion Consumer Service URL: https://api-compliance.eqscockpit.com/data-center/api/sso/saml/acs/292ed5cd-d551-4e21-ae0d-7445c7d82710

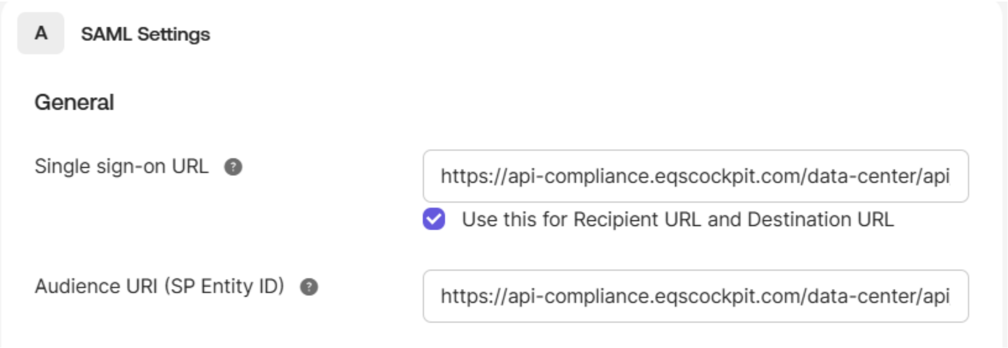
Important: If you delete the SSO configuration in EQS, or create a new SSO configuration in EQS, the Entity ID and ACS URL metadata values will change

EQS Attribute	Okta Attribute
entityID	Audience URI
AssertionConsumerService	Recipient & Destination URL

1.4. Add metadata & Attribute Statements into Okta SAML configuration.

01. In your Okta **SAML Settings**, click the **Edit** button.

02. Replace the placeholder values for **Single Sign-On URL** and **Audience URI** with the metadata from the EQS Compliance COCKPIT



A SAML Settings

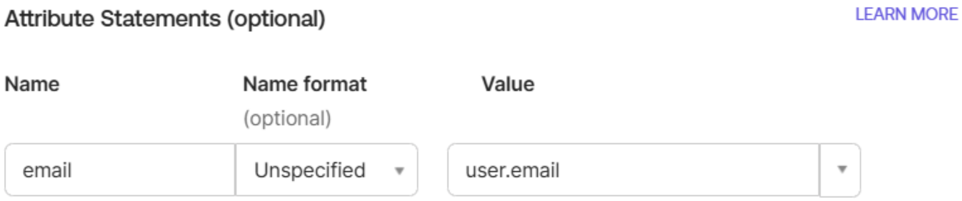
General

Single sign-on URL: https://api-compliance.eqscockpit.com/data-center/api

☑ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID): https://api-compliance.eqscockpit.com/data-center/api

03. Under Attribute Statements type **email** as the Name and select **user.email** as the Value



Attribute Statements (optional)

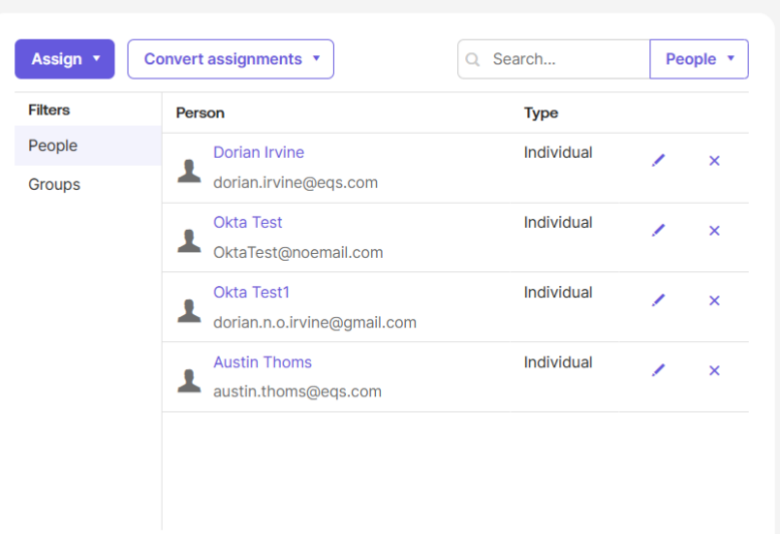
Name	Name format (optional)	Value
email	Unspecified	user.email

04. Select **Next** and then **Finish** to save the updated SAML configuration.

1.5. Assign Users or Groups in Okta Application

01. Access the **Assignments** tab in the navigation menu of the application.

02. Select the **Assign** button and then either **to People** or **to Groups** to assign the users and groups that should have access to EQS Compliance COCKPIT or Integrity Hub

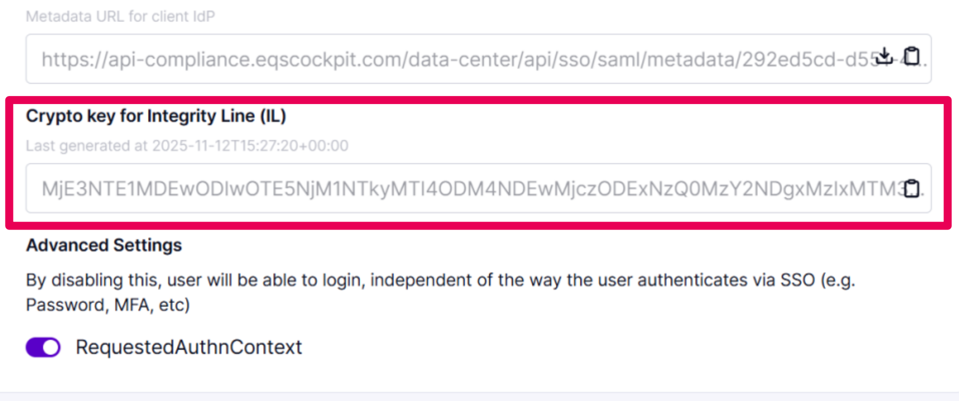


Person	Type
Dorian Irvine dorian.irvine@eqs.com	Individual
Okta Test OktaTest@noemail.com	Individual
Okta Test1 dorian.n.o.irvine@gmail.com	Individual
Austin Thoms austin.thoms@eqs.com	Individual

1.6. *Configure the cryptokey attribute for Integrity Line*

If your license contains *Integrity Line*, you must also add a new custom attribute statement in your Okta Application. If not, you can skip Section 1.7

01. To configure the new custom attribute statement in your Okta Application, first gather the **Cryptokey attribute name for Integrity Line** and the **Crypto Key for Integrity Line** from EQS Compliance COCKPIT in the SAML connector.



Metadata URL for client IdP

https://api-compliance.eqscockpit.com/data-center/api/sso/saml/metadata/292ed5cd-d55

Crypto key for Integrity Line (IL)

Last generated at 2025-11-12T15:27:20+00:00

MjE3NTE1MDEwODIwOTE5NjM1NTkyMTI4ODM4NDEwMjczODExNzQ0MzY2NDgxMzIxMTM3

Advanced Settings

By disabling this, user will be able to login, independent of the way the user authenticates via SSO (e.g. Password, MFA, etc)

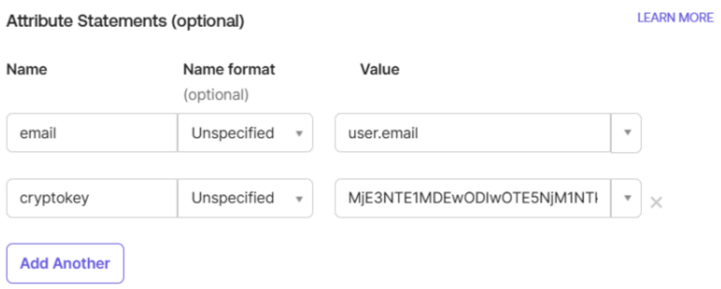
● RequestedAuthnContext

02. The crypto key is automatically generated when the SAML Connector is created.

03. Access your Okta Application and select **Edit** in the **SAML Settings**

04. In the Attribute Statements select **Add Another**

05. Type **cryptokey** in the Name field and paste the cryptokey in the Value field.



Attribute Statements (optional)

Name	Name format (optional)	Value
email	Unspecified	user.email
cryptokey	Unspecified	MjE3NTE1MDEwODIwOTE5NjM1NT

06. Select **Next** and then **Finish** to save the updated SAML configuration.

1.7. *Enable Authentication Context and Activate SSO*

When using SAML-based SSO in EQS Compliance Platform, the RequestedAuthnContext setting defines the required authentication level for the user session such as password-only or multi-factor authentication (MFA) at the Identity Provider (IdP).

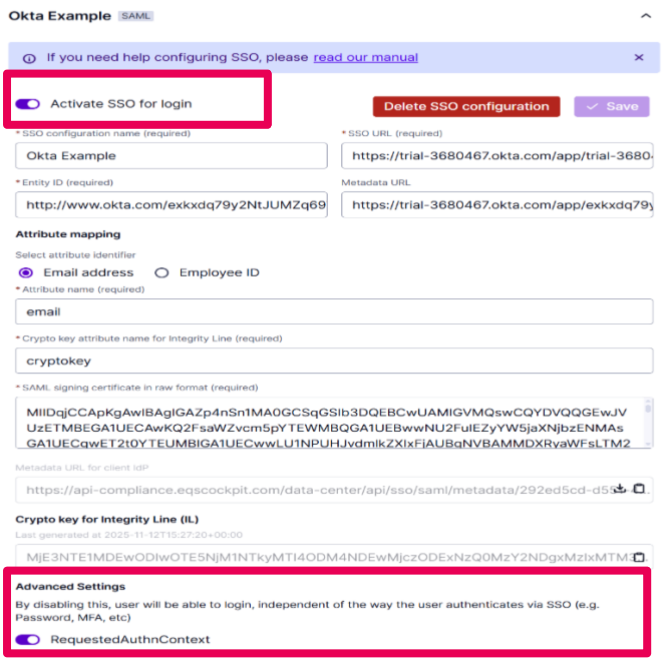
Enabling this setting enforces stricter access control. It requires users to authenticate using the specified method, even if they already have a valid SAML session from another application. Disabling this setting allows the system to accept any valid SAML assertion, regardless of how the user originally authenticated.

Configuring the RequestedAuthnContext appropriately ensures that the authentication process matches your security requirements and helps prevent login errors or failed assertion.

01. Toggle on **Activate SSO for Login** in the upper left corner of the configuration.

02. Under Advanced Settings, toggle on **RequestedAuthnContext** in the lower left corner of the configuration to enable Requested Authentication Context

03. Click **Save** in the upper right corner of the SAML Connector to save the SSO configuration.



Activate SSO for login

* SSO configuration name (required): Okta Example

* SSO URL (required): https://trial-3680467.okta.com/app/trial-3680

* Entity ID (required): http://www.okta.com/exkxdq79y2NtJUMZq69

Metadata URL: https://trial-3680467.okta.com/app/exkxdq79

Attribute mapping

Select attribute identifier

● Email address ○ Employee ID

* Attribute name (required): email

* Crypto key attribute name for Integrity Line (required): cryptokey

* SAML signing certificate in raw format (required):

```
MIIDqjCCApKgAwIBAgIGAZp4nSn1MA0GCSqGSIb3DQEBCwUAMIGVMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAs
GA1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXIxFjAUBgNVBAMMDXRyaWFsLTM2
```

Metadata URL for client IdP: https://api-compliance.eqscockpit.com/data-center/api/sso/saml/metadata/292ed5cd-d55

Crypto key for Integrity Line (IL)

Last generated at 2025-11-12T15:27:20+00:00

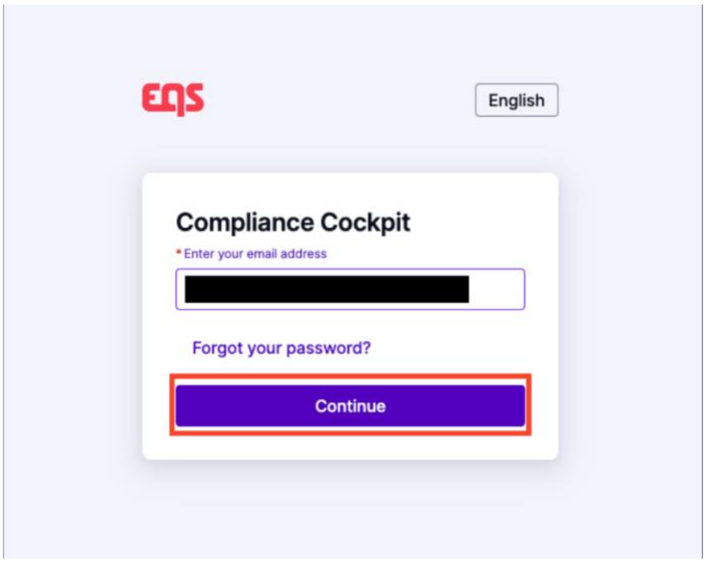
MjE3NTE1MDEwODIwOTE5NjM1NTkyMTI4ODM4NDEwMjczODExNzQ0MzY2NDgxMzIxMTM3

Advanced Settings

By disabling this, user will be able to login, independent of the way the user authenticates via SSO (e.g. Password, MFA, etc)

RequestedAuthnContext

04. Log out and then log in again. Type your email address and click **Continue**. You will be forwarded to the login screen of your central user management platform.



Compliance Cockpit

*Enter your email address

[redacted]

After activating SSO, all users and groups assigned to the enterprise application will be able to login to EQS Compliance COCKPIT and/or Integrity Hub depending on the permissions set up for them within Data Center in EQS Compliance COCKPIT

2. SCIM Configuration in Okta

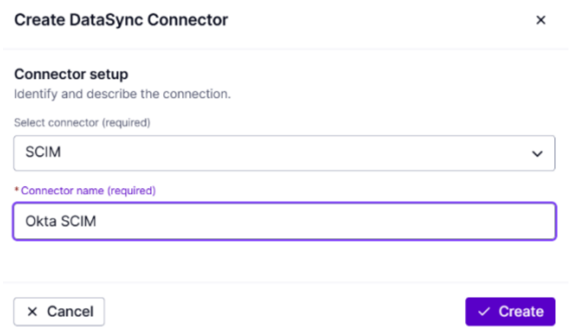
2.1. Create a SCIM Connector in EQS Compliance COCKPIT

01. Login to EQS Compliance COCKPIT with your user credentials

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

03. Select **DataSync Configuration**, then click **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.



Create DataSync Connector ×

Connector setup

Identify and describe the connection.

Select connector (required)

SCIM

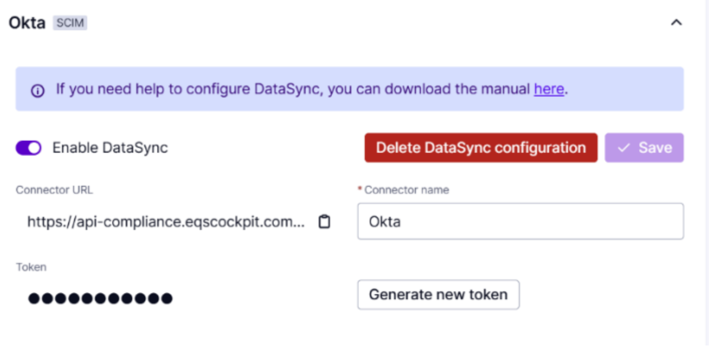
*Connector name (required)

Okta SCIM

× Cancel

✓ Create

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 Okta 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.



Okta SCIM

If you need help to configure DataSync, you can download the manual here.

Enable DataSync

Delete DataSync configuration

✓ Save

Connector URL

https://api-compliance.eqscockpit.com...

*Connector name

Okta

Token

●●●●●●●●●●●●

Generate new token

2.2. *Enable SCIM Provisioning in Okta*

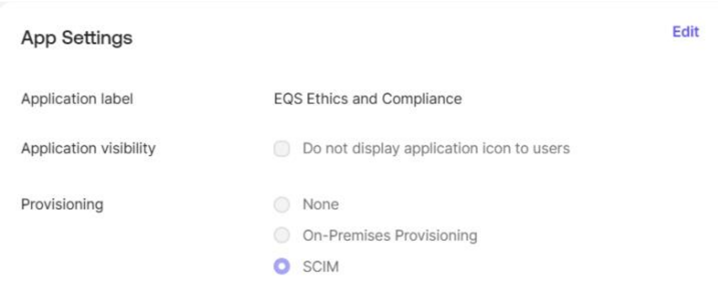
01. Navigate to the Okta portal home page: https://login.okta.com

02. Select **Admin Console** and then **Applications.**

03. Select your Application that you created in section 1.1 and switch to the **General** tab.

04. Select **Edit** in the **App Settings**

05. Select the **SCIM** radio button and then press **Save.**



App Settings Edit

Application label: EQS Ethics and Compliance

Application visibility: □ Do not display application icon to users

Provisioning: ○ None ○ On-Premises Provisioning ● SCIM

06. Navigate to the **Provisioning** tab and press **Edit.**

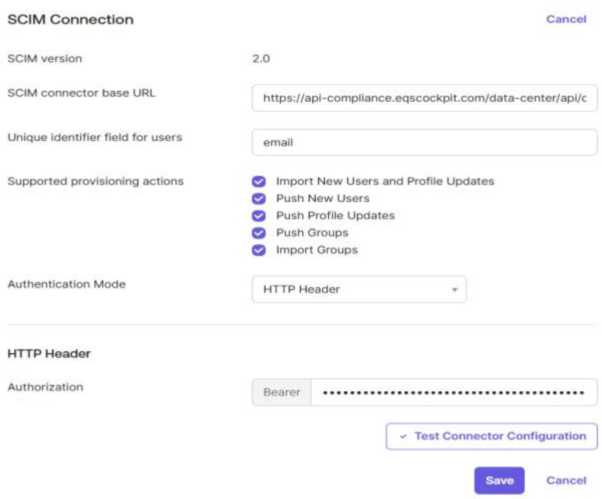
07. Paste the Connector URL into the **SCIM connector base URL.**

08. Type **email** as the **Unique identifier field for users.**

09. In the **Supported provisioning actions** select all of the radio buttons

10. Change **Authentication Mode** to **HTTP Header**

11. Paste the Token from EQS as the **Bearer Token**



SCIM Connection Cancel

SCIM version: 2.0

SCIM connector base URL: https://api-compliance.eqscockpit.com/data-center/api/c

Unique identifier field for users: email

Supported provisioning actions:
☑ Import New Users and Profile Updates
☑ Push New Users
☑ Push Profile Updates
☑ Push Groups
☑ Import Groups

Authentication Mode: HTTP Header

HTTP Header

Authorization: Bearer ••

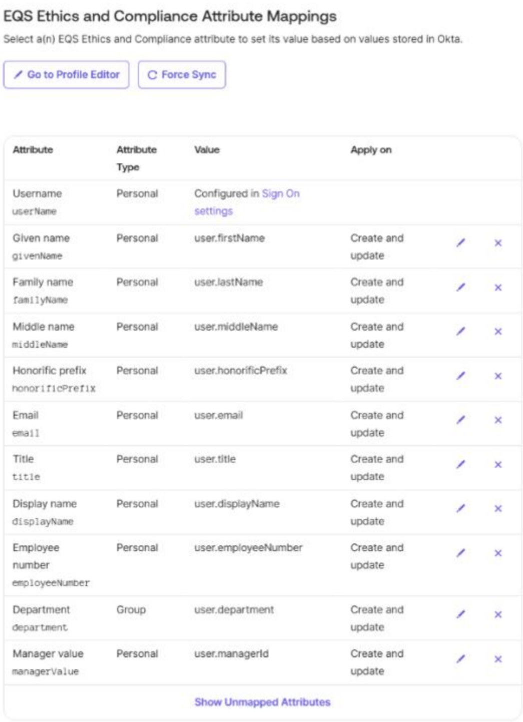
12. Pressing **Test Connector Configuration** will validate the credentials. If successful, select **Save.**

13. In the Provisioning to App settings enable Create Users, Update User Attributes, and Deactivate Users

14. Select **Mappings** and complete Attribute Mappings

- Required Attributes, "id," "userName" (the email used for login), "familyName" and "givenName."
- Emails attribute: The "emails" field exists only for compatibility with SCIM's default mapping. Our platform does not support multiple emails; the single email for an employee is "userName", so this field is read-only.

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



EQS Ethics and Compliance Attribute Mappings

Select a(n) EQS Ethics and Compliance attribute to set its value based on values stored in Okta.

Attribute	Attribute Type	Value	Apply on		
Username userName	Personal	Configured in Sign On settings			
Given name givenName	Personal	user.firstName	Create and update	✎	×
Family name familyName	Personal	user.lastName	Create and update	✎	×
Middle name middleName	Personal	user.middleName	Create and update	✎	×
Honorific prefix honorificPrefix	Personal	user.honorificPrefix	Create and update	✎	×
Email email	Personal	user.email	Create and update	✎	×
Title title	Personal	user.title	Create and update	✎	×
Display name displayName	Personal	user.displayName	Create and update	✎	×
Employee number employeeNumber	Personal	user.employeeNumber	Create and update	✎	×
Department department	Group	user.department	Create and update	✎	×
Manager value managerValue	Personal	user.managerId	Create and update	✎	×

2.3. *Data Testing & Automatic Provisioning*

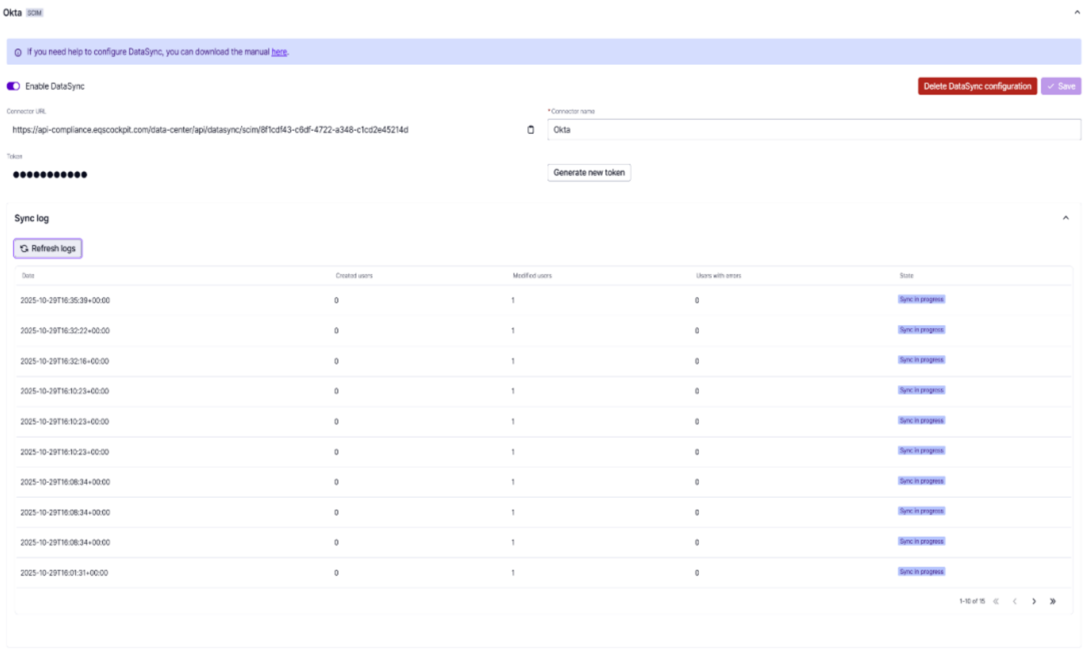
01. Assign a single user or small group of employees that are aware of project implementation to the enterprise application with their desired role.

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

```
{
 "id": "f08b43bf-c646-4bf0-b07c-d8f56c825a0c",
 "meta": {
  "created": "2025-10-23T16:14:28+00:00",
  "location": "https://api-compliance.eqscockpit.com/data-center/api/datasync/scim/8f1cdf43-c6df-4722-a348-c1cd2e45214d/Users/f08b43bf-c646-4bf0-b07c-d8f56c825a0c",
  "lastModified": "2025-10-29T16:32:22+00:00",
  "resourceType": "User"
 },
 "name": {
  "formatted": "Okta Test",
  "givenName": "Okta",
  "familyName": "Test"
 },
 "roles": [
  {
   "type": "COMPLIANCE_COCKPIT",
      "value": "admin",
      "display": "Admin",
      "primary": true
    },
    {
      "type": "INTEGRITY_HUB",
      "value": "employee",
      "display": "Employee",
      "primary": true
    }
  ],
  "active": true,
  "emails": [
    {
      "type": "work",
      "value": "OktaTest@noemail.com"
    },
    {
      "type": "work",
      "value": "OktaTest@noemail.com",
      "primary": true
    }
  ],
  "groups": [ ],
  "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"
  ],
  "userName": "OktaTest@noemail.com",
  "userType": "Employee",
  "externalId": "00uwo5i2uo0drKxan697",
  "displayName": "Okta Test",
  "preferredLanguage": "en",
  "urn:ietf:params:scim:schemas:eqs:datacenter:1.0:User": {
    "tags": [ ],
    "preferredCurrencyCode": "EUR"
  },
  "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User": {
    "manager": {
      "$ref": "https://api-compliance.eqscockpit.com/data-center/api/datasync/scim/8f1cdf43-c6df-4722-a348-c1cd2e45214d/Users/597a593e-c85f-45cd-be6d-8d60d32e8b48",
      "value": "1",
      "displayName": "austin.thoms@eqs.com"
    }
  }
}
```



ⓘ If you need help to configure DataSync, you can download the manual here.

● Enable DataSync

Connector URL: https://api-compliance.eqscockpit.com/data-center/api/datasync/scim/8f1cdf43-c6df-4722-a348-c1cd2e45214d

*Connector name: Okta

Token: ●●●●●●●●●●●

Sync log

Date	Created users	Modified users	Users with errors	State
2025-10-29T16:35:39+00:00	0	1	0	Sync in progress
2025-10-29T16:32:22+00:00	0	1	0	Sync in progress
2025-10-29T16:32:16+00:00	0	1	0	Sync in progress
2025-10-29T16:10:23+00:00	0	1	0	Sync in progress
2025-10-29T16:10:23+00:00	0	1	0	Sync in progress
2025-10-29T16:10:23+00:00	0	1	0	Sync in progress
2025-10-29T16:08:34+00:00	0	1	0	Sync in progress
2025-10-29T16:08:34+00:00	0	1	0	Sync in progress
2025-10-29T16:08:34+00:00	0	1	0	Sync in progress
2025-10-29T16:01:31+00:00	0	1	0	Sync in progress

04. Troubleshoot any errors or unexpected results from provisioning.

05. Once data synchronization is 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 separate roles.

07. Enable automatic provisioning in the identity provider.