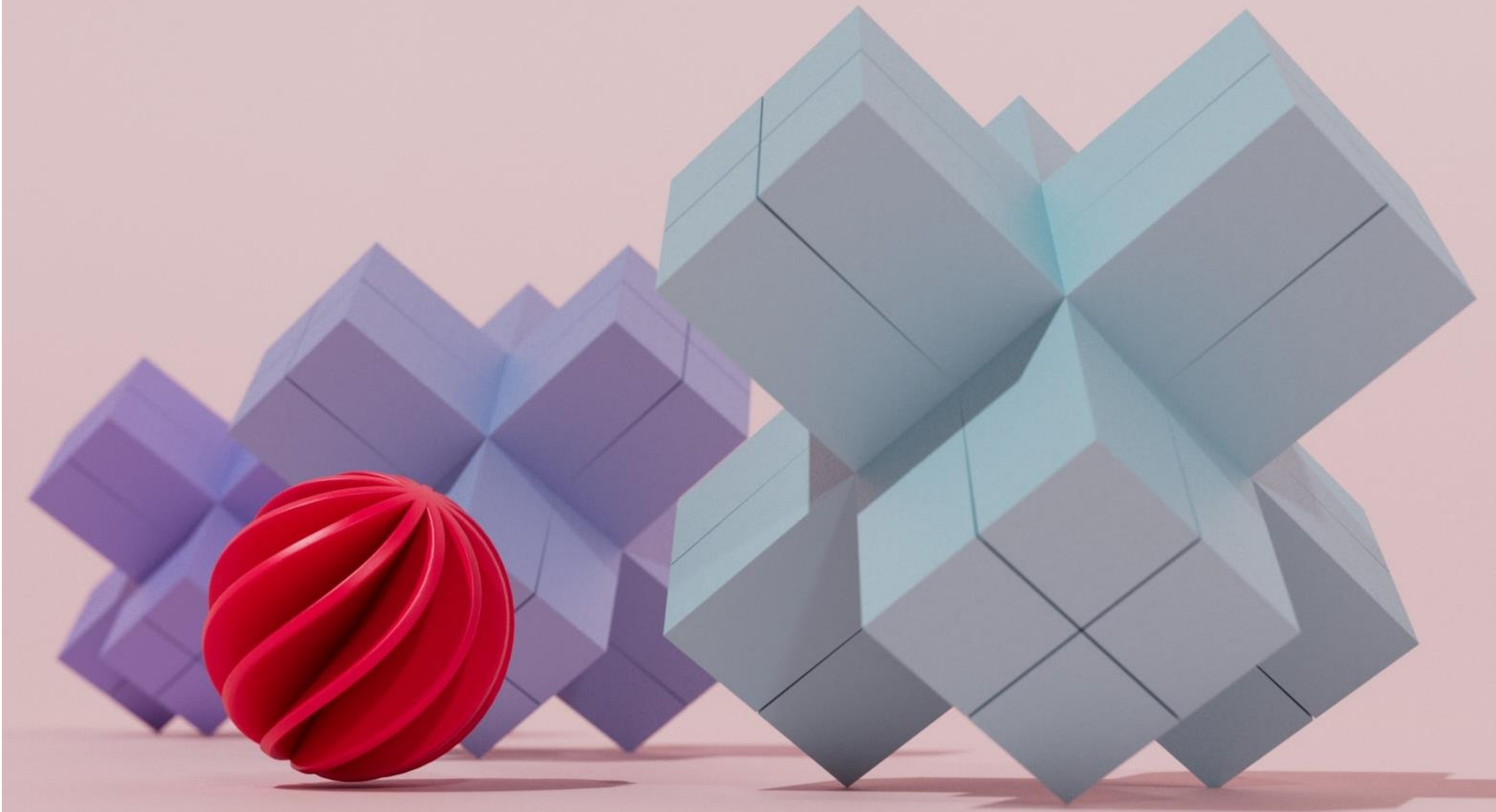


EQS GROUP

SSO USER MANUAL

Setup Single Sign-On with Compliance Platform

Table of contents

1. Introduction

Single Sign-On (SSO) is a feature of the EQS Compliance Platform to identify and authenticate user accounts between your central user management provider and the EQS Compliance Platform to automize the identity lifecycle management. With Single Sign-On you avoid the password management trouble for your users.

In order to configure SSO for Compliance COCKPIT, you will need a user there. Usually, a user should already have been created for you. Please check your mails for an email with the subject "Welcome to EQS Compliance COCKPIT!" and activate your account by choosing a password.

If you didn't receive this email, please contact your product responsible and request creation of a user for you.

In case, there is any issue with your SSO, EQS can deactivate it for you. Then, you will be able to log in with your password again to check the configuration and fix any issues

2. Protocols

EQS Compliance Platform integrates any identity provider that supports the SAML or OpenID Connect protocols.

The SSO implementation doesn't include any permission management or user provisioning. All users will need to be created in Compliance COCKPIT separately and their permissions within the COCKPIT will be managed there as well.

2.1 SAML

SAML is an acronym used to describe the Security Assertion Markup Language (SAML). Its primary role in online security is that it enables you to access multiple web applications using one set of login credentials. It works by passing authentication information in a particular format between two parties, usually an identity provider (IdP) and a web application.

2.1.1 Microsoft Entra

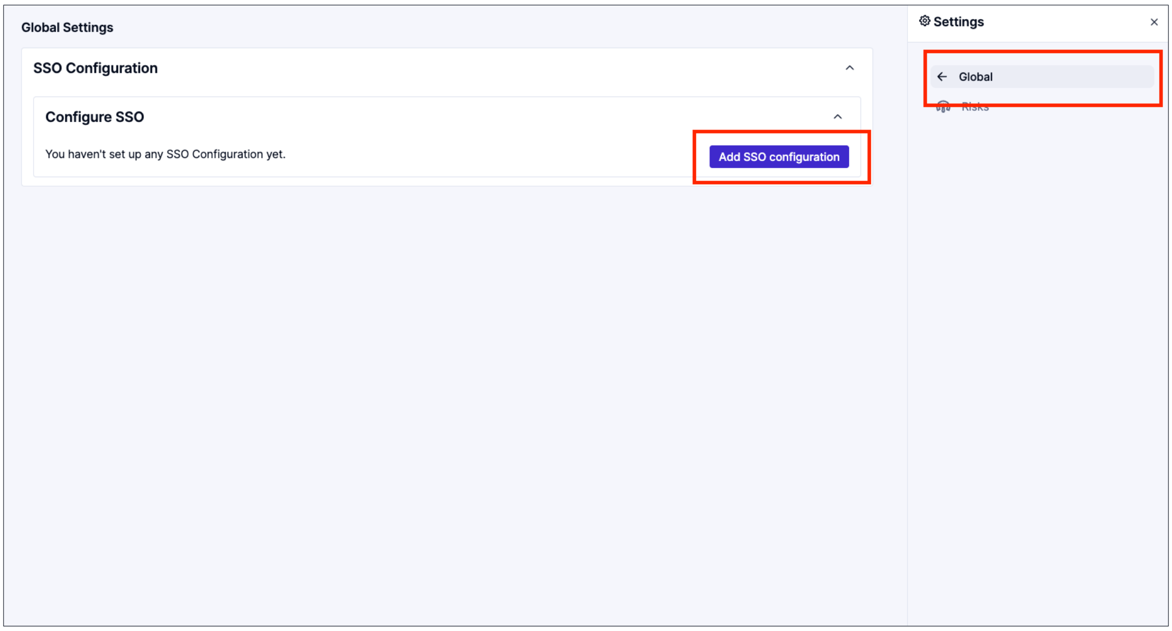
In this section we are going to setup SSO with **Microsoft Entra**, Microsoft's application to automate identity lifecycle management.

This is done via the following steps:

1. Create an enterprise application in your Azure portal at https://portal.azure.com.
2. Create and configure a new SAML connector within EQS Compliance Cockpit.
3. Configure the Azure enterprise application with EQS Compliance Cockpit Service Provider.
4. Activate and start using Single Sign-On.

2.1.1.1 Step-by-Step Process

1. Log into EQS Compliance Cockpit with your user credentials.
2. Click the gear icon on the top-right to open the settings sidebar.
3. Select "Global" and expand the SSO Configuration section, then click the "Add SSO configuration" button to open the connector creation dialog.



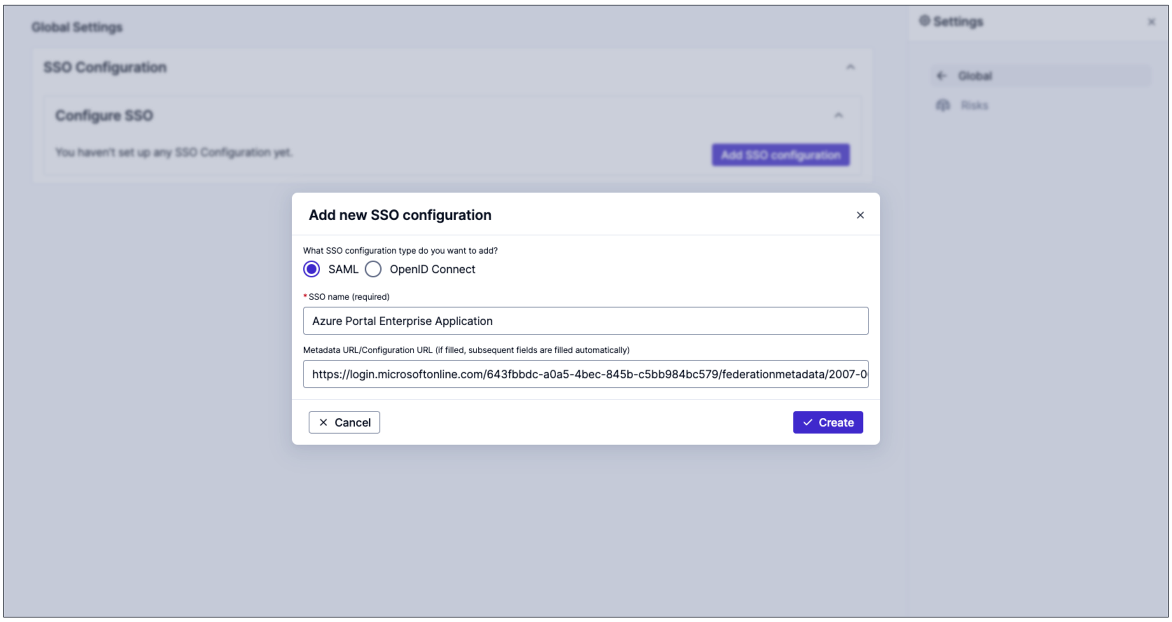
Global Settings

SSO Configuration

Configure SSO

You haven't set up any SSO Configuration yet.

4. Enter a name for your SAML connector and the Metadata URL from your Enterprise Application, if available, then click the “Create” button.



Add new SSO configuration

What SSO configuration type do you want to add?

● SAML ○ OpenID Connect

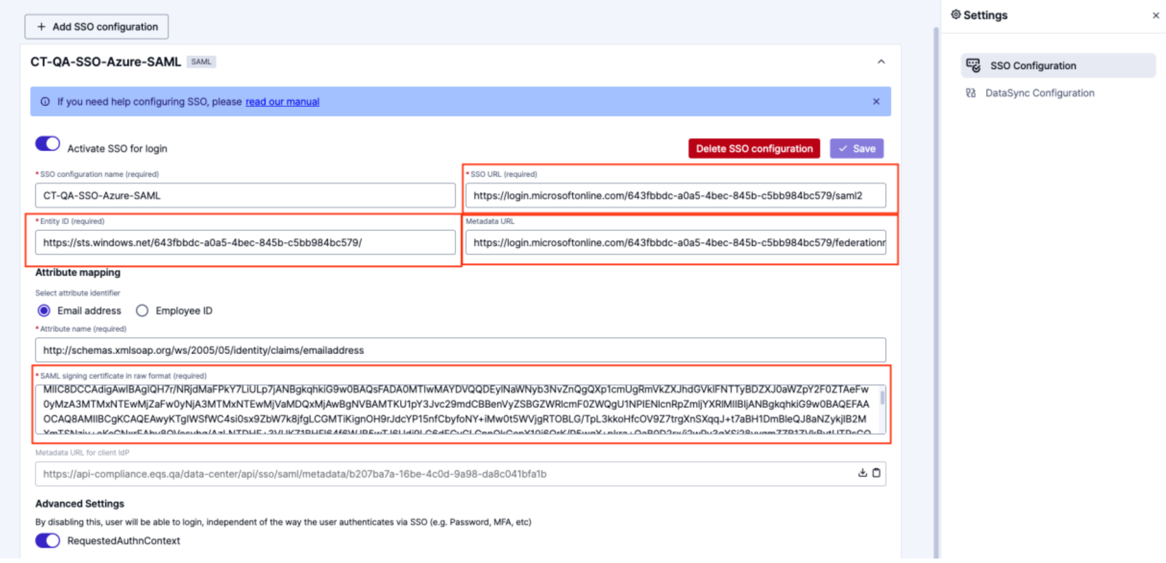
* SSO name (required)

Azure Portal Enterprise Application

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

https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984bc579/federationmetadata/2007-0

5. A new connector configuration panel is shown in the "SSO Configuration" section. If you entered a valid Metadata URL in the creation process, the red marked fields **SSO URL**, **Entity ID**, **SAML Signing Certificate**, should be automatically filled, if not please fill them with the information from your Enterprise Application. **Do not worry about the Attribute mapping for now (Steps 12 and 13)**.



CT-QA-SSO-Azure-SAML

If you need help configuring SSO, please read our manual

Activate SSO for login

* SSO configuration name (required): CT-QA-SSO-Azure-SAML

* SSO URL (required): https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984bc579/saml2

* Entity ID (required): https://sts.windows.net/643fbbdc-a0a5-4bec-845b-c5bb984bc579/

Metadata URL: https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984bc579/federationr

Attribute mapping

Select attribute identifier

● Email address ○ Employee ID

* Attribute name (required): http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

* SAML signing certificate in raw format (required)

```
MIIC8DCCAdigAwIBAgIQH7r/NRjdMaFPkY7LiULp7jANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEyINaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw
0yMzA3MTMxNTEwMjZaFw0yNjA3MTMxNTEwMjVaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQgU1NPIENlcnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAA
OCAQ8AMIIBCgKCAQEAwyKTgIWSfWC4si0sx9ZbW7k8jfgLCGMTiKignOH9rJdcYP15nfCbyfoNY+iMw0t5WVjgRTOBLG/TpL3kkoHfcOV9Z7trgXnSXqqJ+t7aBH1DmBleQJ8aNZykjlB2M
```

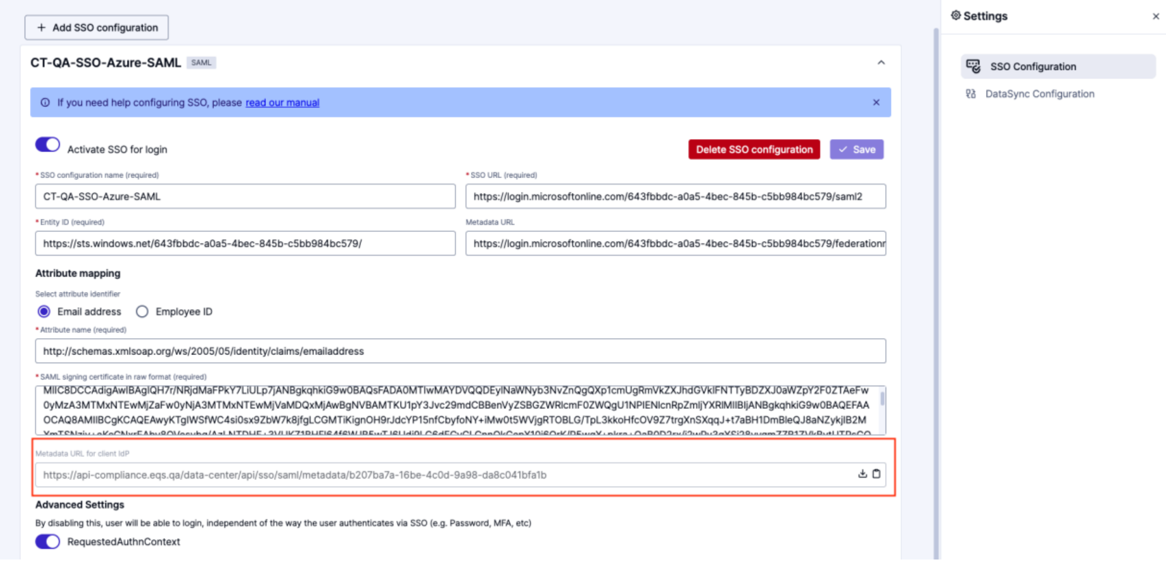
Metadata URL for client IdP: https://api-compliance.eqs.qa/data-center/api/sso/saml/metadata/b207ba7a-16be-4c0d-9a98-da8c041bfa1b

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

6. It also displays the **Service Provider Metadata URL**, which contains the **Entity ID** and the **Assertion Consumer Service URL**. This data is going to be configured in your Azure enterprise application.



CT-QA-SSO-Azure-SAML

If you need help configuring SSO, please read our manual

Activate SSO for login

* SSO configuration name (required): CT-QA-SSO-Azure-SAML

* SSO URL (required): https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984bc579/saml2

* Entity ID (required): https://sts.windows.net/643fbbdc-a0a5-4bec-845b-c5bb984bc579/

Metadata URL: https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984bc579/federationr

Attribute mapping

Select attribute identifier

● Email address ○ Employee ID

* Attribute name (required): http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

* SAML signing certificate in raw format (required)

MIIC8DCCAdigAwIBAgIQH7r/NRjdMaFPkY7LiULp7jANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEyINaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw
0yMzA3MTMxNTEwMjZaFw0yNjA3MTMxNTEwMjVaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQgU1NPIENlcnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAA
OCAQ8AMIIBCgKCAQEAwyKTgIWSfWC4si0sx9ZbW7k8jfgLCGMTiKignOH9rJdcYP15nfCbyfoNY+iMw0t5WVjgRTOBLG/TpL3kkoHfcOV9Z7trgXnSXqqJ+t7aBH1DmBleQJ8aNZykjlB2M

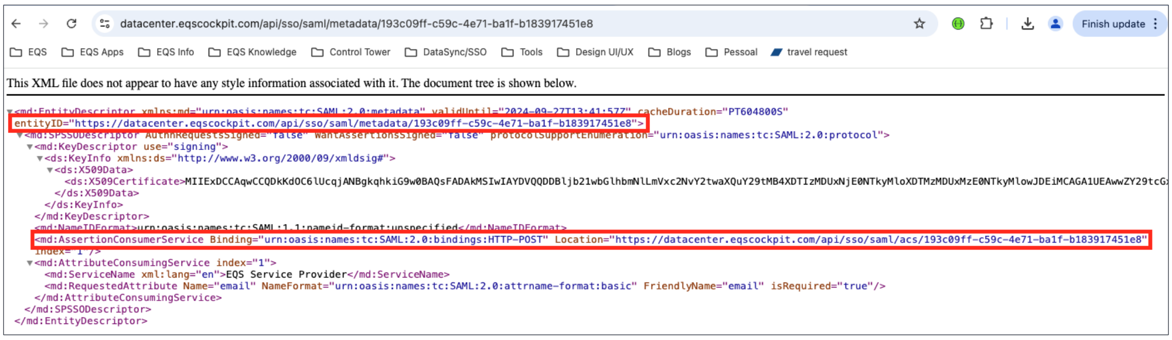
Metadata URL for client IdP: https://api-compliance.eqs.qa/data-center/api/sso/saml/metadata/b207ba7a-16be-4c0d-9a98-da8c041bfa1b

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

7. You can copy the URL and open it on a browser or just download it as an XML file, in order to find the **Entity ID** and **Assertion Consumer Service URL** information.

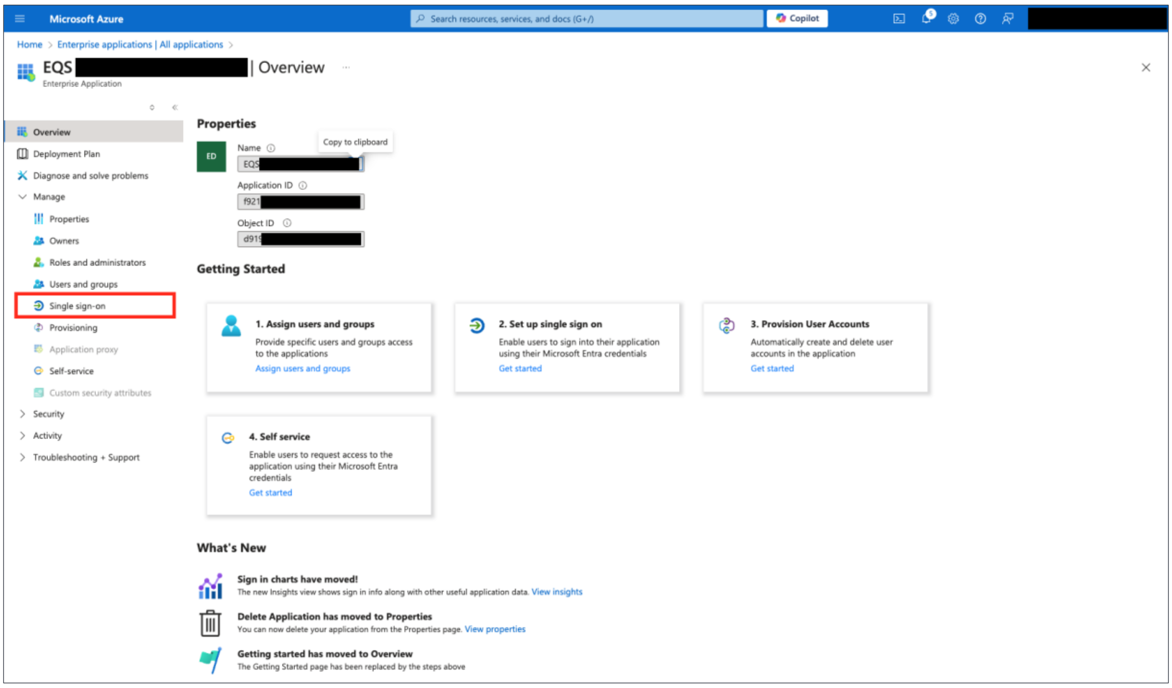


datacenter.eqscockpit.com/api/sso/saml/metadata/193c09ff-c59c-4e71-ba1f-b183917451e8

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2024-09-27T13:41:57Z" cacheDuration="PT604800S"
entityID="https://datacenter.eqscockpit.com/api/sso/saml/metadata/193c09ff-c59c-4e71-ba1f-b183917451e8">
 ▼<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>MIIExDCCAqwCCQDkKdOC6lUcqjANBgkqhkiG9w0BAQsFADAkMSIwIAYDVQQDDBljb21wbGlhbmNlLmVxc2NvY2twaXQuY29tMB4XDTIzMDUxNjE0NTkyMloXDTMzMDUxMzE0NTkyMlowJDEiMCAGA1UEAwwZY29tcG
     </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://datacenter.eqscockpit.com/api/sso/saml/acs/193c09ff-c59c-4e71-ba1f-b183917451e8"
  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:AttributeConsumingService>
 </md:SPSSODescriptor>
</md:EntityDescriptor>
```

8. Open https://portal.azure.com and find your enterprise application, your IT department may want to create a new one. The enterprise application has user groups assigned to it and manages the user provisioning. Once you have your enterprise application open, you can configure it by clicking on “Single sign-on”.



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
[redacted]
Home > Enterprise applications | All applications >

EQS [redacted] | Overview

Enterprise Application

Properties

Name: EQS[redacted]

Copy to clipboard

Application ID: f921[redacted]

Object ID: d91[redacted]

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Microsoft Entra credentials
Get started

3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

4. Self service
Enable users to request access to the application using their Microsoft Entra credentials
Get started

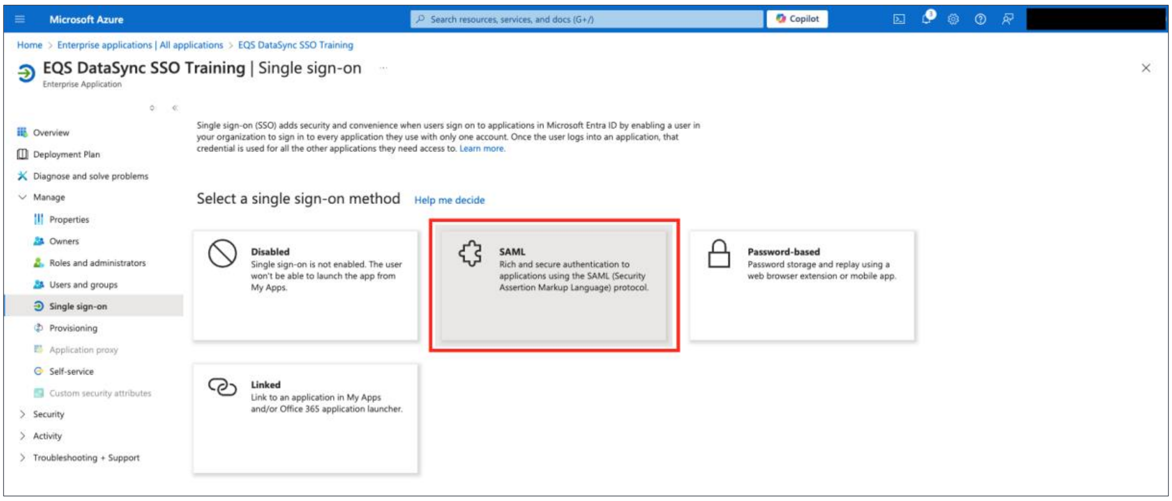
What's New

Sign in charts have moved!
The new Insights view shows sign in info along with other useful application data. View insights

Delete Application has moved to Properties
You can now delete your application from the Properties page. View properties

Getting started has moved to Overview
The Getting Started page has been replaced by the steps above

9. On the onboarding page, select "SAML" to start configuring the Single sign-on.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Enterprise applications | All applications > EQS DataSync SSO Training
Overview
Deployment Plan
Diagnose and solve problems
Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Custom security attributes
Security
Activity
Troubleshooting + Support
Help me decide

[redacted]

EQS DataSync SSO Training | Single sign-on

Enterprise Application

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

Select a single sign-on method

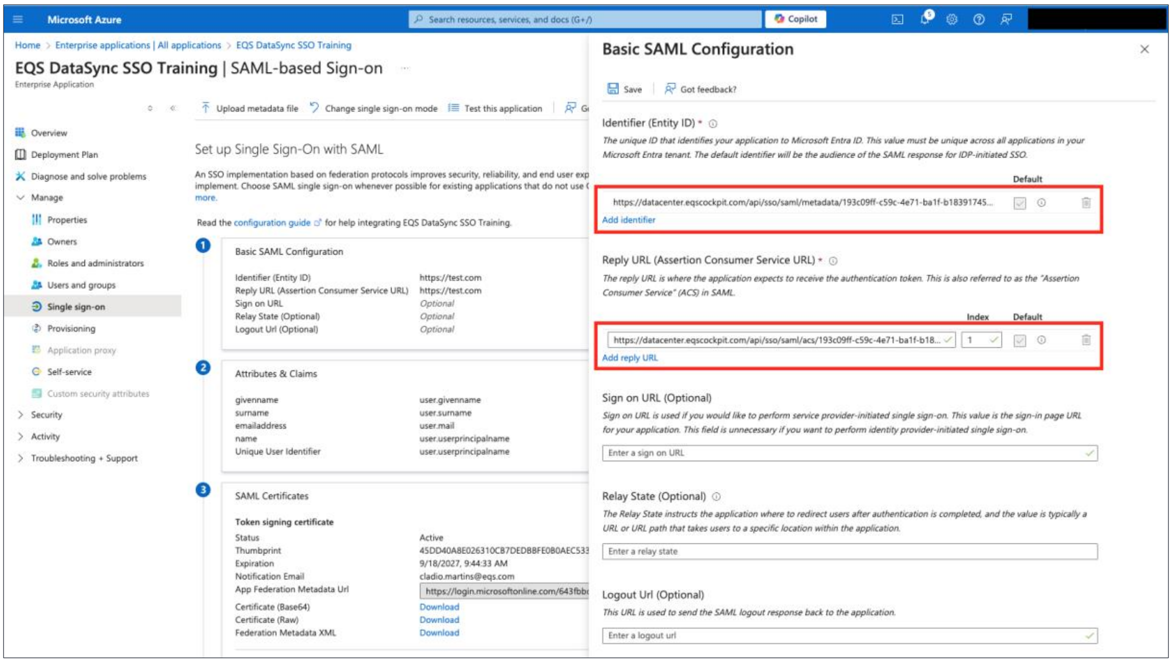
Disabled Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based Password storage and replay using a web browser extension or mobile app.

Linked Link to an application in My Apps and/or Office 365 application launcher.

10. Now enter the Entity ID and Assertion Consumer Service URL *(refer Step 7 to know where to get this)* by clicking on Edit in the Step 1 or by uploading the downloaded XML file.



[redacted]

EQS DataSync SSO Training | SAML-based Sign-on

Enterprise Application

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user exp implement. Choose SAML single sign-on whenever possible for existing applications that do not use (more.

Read the configuration guide for help integrating EQS DataSync SSO Training.

1 Basic SAML Configuration

Identifier (Entity ID)	https://test.com
Reply URL (Assertion Consumer Service URL)	https://test.com
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

2 Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Certificates

Token signing certificate

Status	Active
Thumbprint	45DD40A8E026310CB7DEDBBFE0B0AEC533
Expiration	9/18/2027, 9:44:33 AM
Notification Email	cladio.martins@eqs.com
App Federation Metadata Url	https://login.microsoftonline.com/643fbb
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Basic SAML Configuration

Identifier (Entity ID) *

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

https://datacenter.eqscockpit.com/api/sso/saml/metadata/193c09ff-c59c-4e71-ba1f-b18391745...

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

https://datacenter.eqscockpit.com/api/sso/saml/acs/193c09ff-c59c-4e71-ba1f-b18... ✓ | 1 ✓

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

Enter a sign on URL

Relay State (Optional)

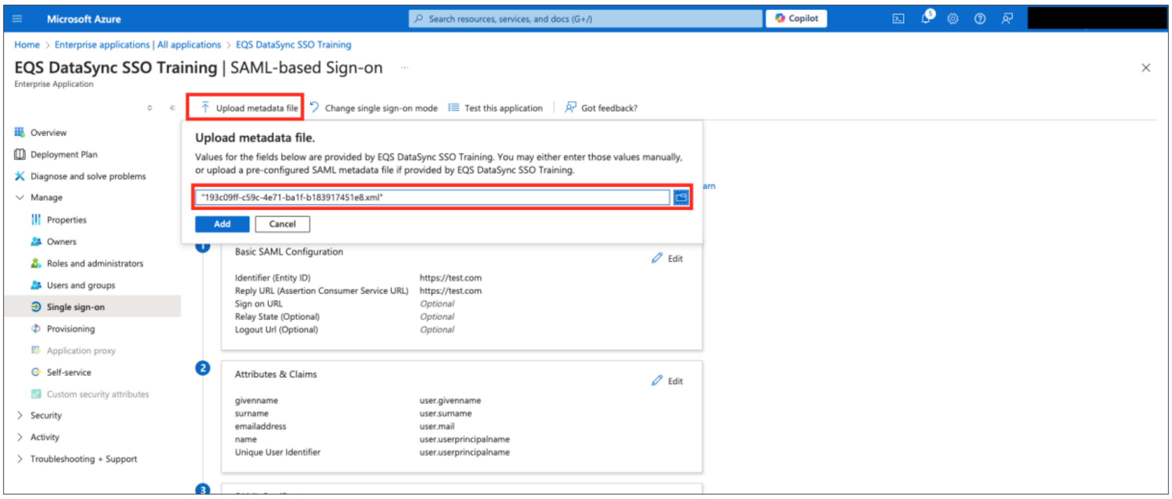
The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Enter a relay state

Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.

Enter a logout url



EQS DataSync SSO Training | SAML-based Sign-on

Enterprise Application

Upload metadata file.

Values for the fields below are provided by EQS DataSync SSO Training. You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by EQS DataSync SSO Training.

"193c09ff-c59c-4e71-ba1f-b183917451e8.xml"

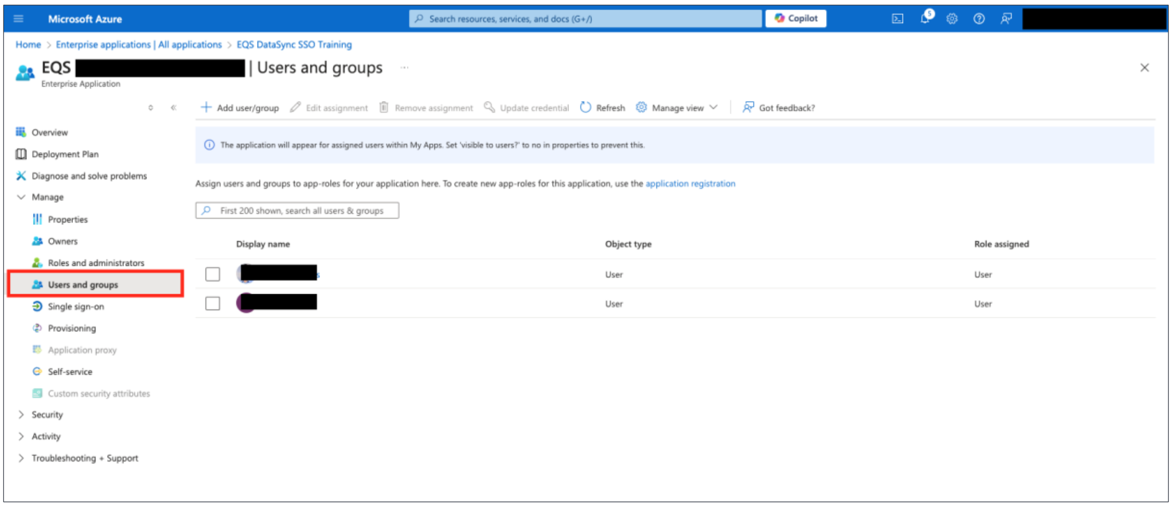
Basic SAML Configuration

Identifier (Entity ID)	https://test.com
Reply URL (Assertion Consumer Service URL)	https://test.com
Sign on URL	*Optional*
Relay State (Optional)	*Optional*
Logout Url (Optional)	*Optional*

Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

11. Inside the "Users and Groups" section of your enterprise application, assign all users and/or groups which should have access to the EQS Compliance Platform. Be sure the current logged in user in Compliance Cockpit is added here, so you can test the SSO when activating it in Compliance Cockpit.



EQS [redacted] | Users and groups

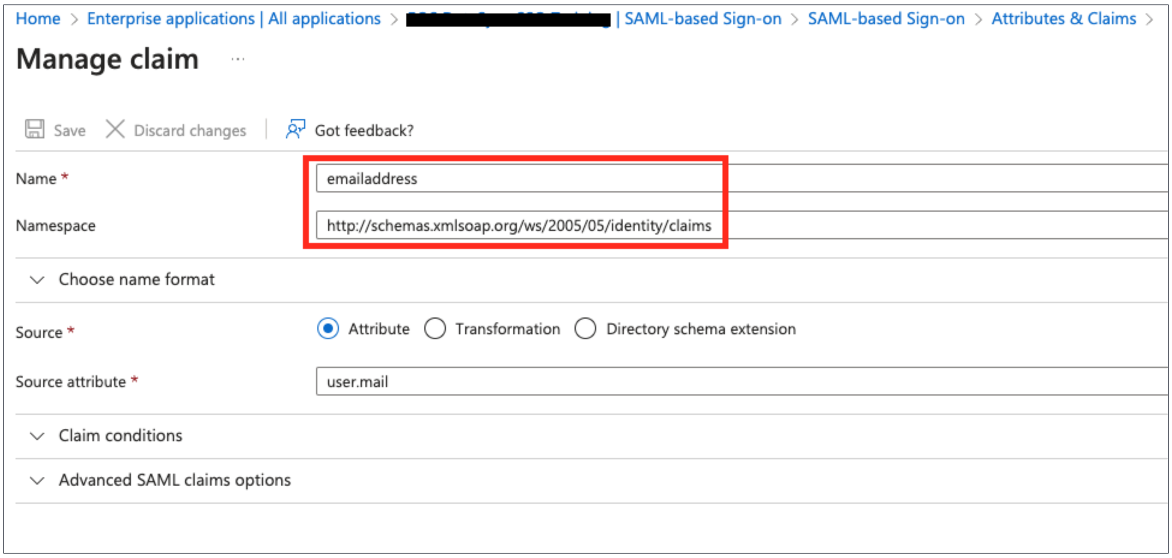
Enterprise Application

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this.

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration

	Display name	Object type	Role assigned
□	[redacted]	User	User
□	[redacted]	User	User

12. Also check the attribute mapping, by clicking on Edit in the Step 2 (*Attributes & Claims*) under *Single sign-on*, to match the Employee email address or Employee ID attribute from your Enterprise Application in the EQS Compliance Cockpit SSO Configuration.



Home > Enterprise applications | All applications > [redacted] | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >

Manage claim ...

Save   Discard changes   Got feedback?

Name *: emailaddress

Namespace: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

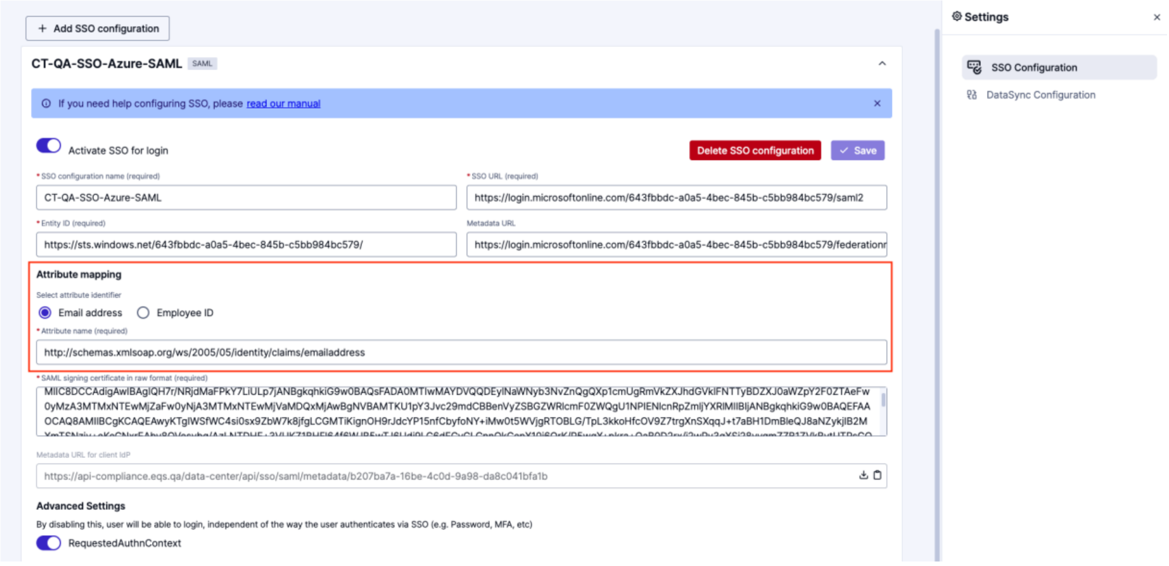
Choose name format

Source *: ● Attribute ○ Transformation ○ Directory schema extension

Source attribute *: user.mail

Claim conditions

Advanced SAML claims options



+ Add SSO configuration

CT-QA-SSO-Azure-SAML SAML

If you need help configuring SSO, please read our manual

Activate SSO for login

Delete SSO configuration   ✓ Save

* SSO configuration name (required): CT-QA-SSO-Azure-SAML

* SSO URL (required): https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984bc579/saml2

* Entity ID (required): https://sts.windows.net/643fbbdc-a0a5-4bec-845b-c5bb984bc579/

Metadata URL: https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984bc579/federationr

Attribute mapping

Select attribute identifier

● Email address ○ Employee ID

* Attribute name (required): http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

* SAML signing certificate in raw format (required)

MIIC8DCCAdigAwIBAgIQH7r/NRjdMaFPkY7LiULp7jANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw
0yMzA3MTMxNTEwMjZaFw0yNjA3MTMxNTEwMjVaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQgU1NPIENlcnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAA
OCAQ8AMIIBCgKCAQEAwyKTglWSfWC4si0sx9ZbW7k8jfgLCGMTiKignOH9rJdcYP15nfCbyfoNY+iMw0t5WVjgRTOBLG/TpL3kkoHfcOV9Z7trgXnSXqqJ+t7aBH1DmBleQJ8aNZykjlB2M

Metadata URL for client IdP: https://api-compliance.eqs.qa/data-center/api/sso/saml/metadata/b207ba7a-16be-4c0d-9a98-da8c041bfa1b

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)

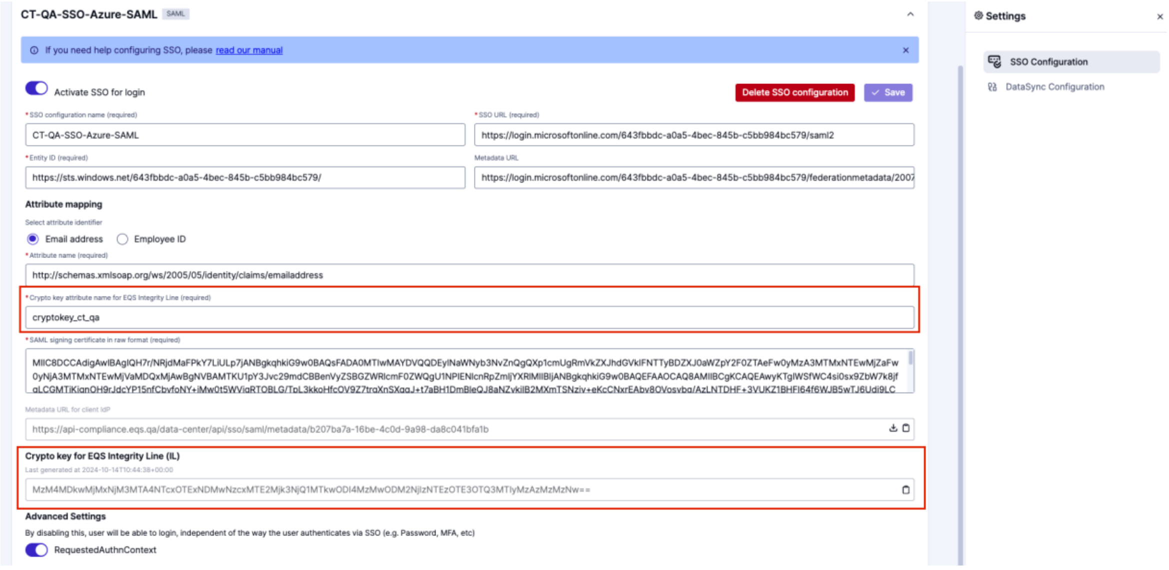
RequestedAuthnContext

Settings

SSO Configuration

DataSync Configuration

13. **In case your license contains Integrity Line**, you must also add a new attribute from EQS Compliance Cockpit SSO Configuration into your Enterprise Application. **If not, you can skip to Step 14.**



CT-QA-SSO-Azure-SAML SAML

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

● Activate SSO for login

* SSO configuration name (required): CT-QA-SSO-Azure-SAML

* SSO URL (required): https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984bc579/saml2

* Entity ID (required): https://sts.windows.net/643fbbdc-a0a5-4bec-845b-c5bb984bc579/

Metadata URL: https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984bc579/federationmetadata/2007

Attribute mapping

Select attribute identifier

● Email address ○ Employee ID

* Attribute name (required): http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

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

* SAML signing certificate in raw format (required):

```
MIIC8DCCAdigAwIBAgIQH7r/NRjdMaFPkY7LiULp7jANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMzA3MTMxNTEwMjZaFw
0yNjA3MTMxNTEwMjVaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQgU1NPIENlcnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwyKTglWSfWC4si0sx9ZbW7k8jf
gLCGMTiKiqnOH9rJdcYP15nfCbvfoNY+iMw0t5WVigRTOBLG/TpL3kkoHfcOV9Z7trgXnSXgqJ+t7aBH1DmBleQJ8aNZvkilB2MXmTSNziv+eKcCNxrEAbv8OVosvbq/AzLNTDHF+3VUKZ1BHFI64f6WJB5wTJ6Udi9LC
```

Metadata URL for client IdP: https://api-compliance.eqs.qa/data-center/api/sso/saml/metadata/b207ba7a-16be-4c0d-9a98-da8c041bfa1b

Crypto key for EQS Integrity Line (IL)

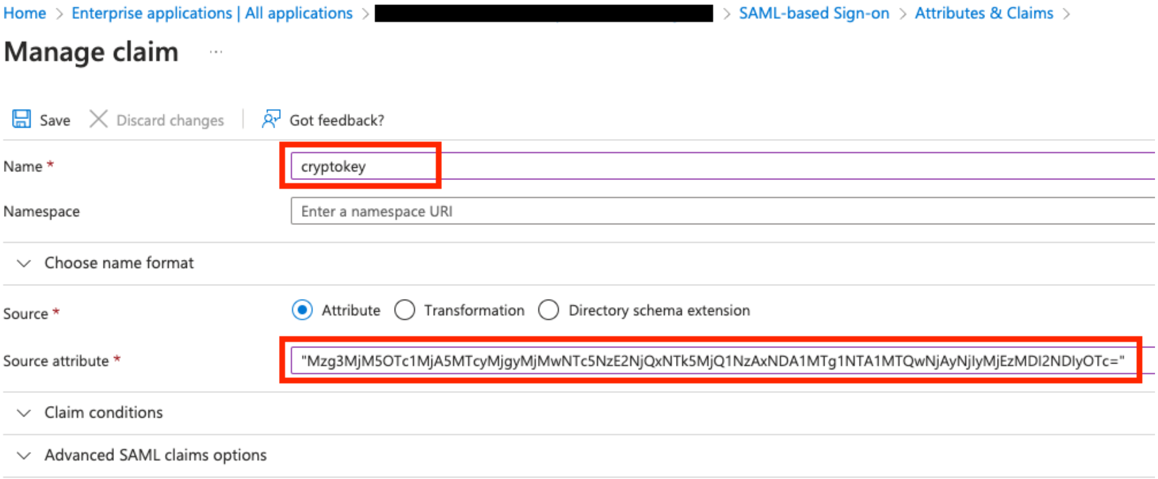
Last generated at 2024-10-14T10:44:38+00:00

MzM4MDkwMjMxNjM3MTA4NTcxOTExNDMwNzcxMTE2Mjk3NjQ1MTkwODI4MzMwODM2NjIzNTEzOTE3OTQ3MTIyMzAzMzMzNw==

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



Home > Enterprise applications | All applications > [redacted] > SAML-based Sign-on > Attributes & Claims >

Manage claim

Name *: cryptokey

Namespace: Enter a namespace URI

Choose name format

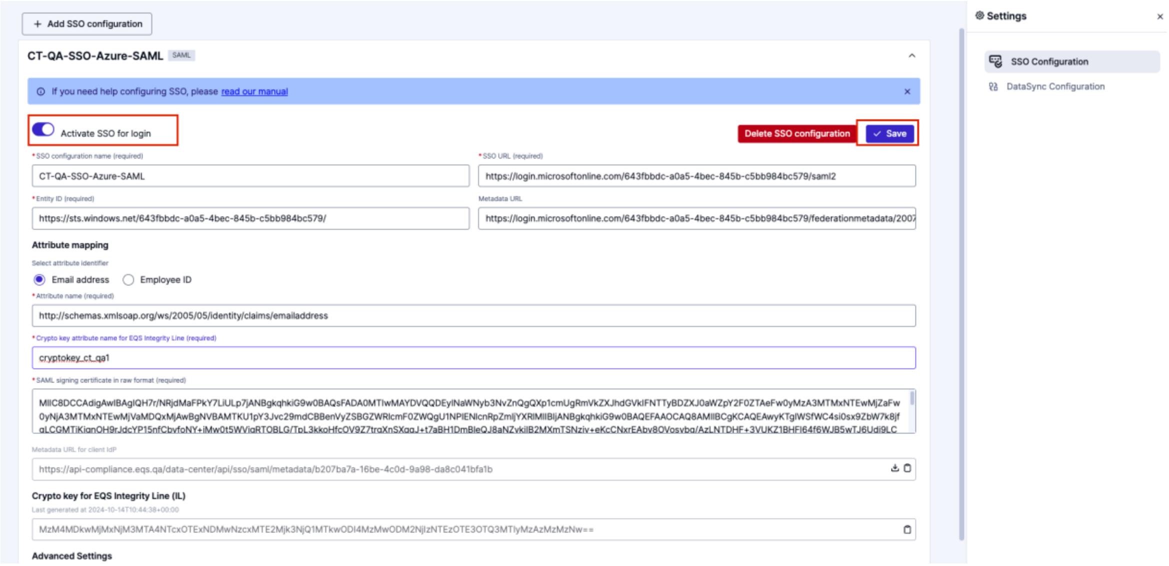
Source *: ● Attribute ○ Transformation ○ Directory schema extension

Source attribute *: "Mzg3MjM5OTc1MjA5MTcyMjgyMjMwNTc5NzE2NjQxNTk5MjQ1NzAxNDA1MTg1NTA1MTQwNjAyNjIyMjEzMDI2NDIyOTc="

Claim conditions

Advanced SAML claims options

14. Now activate and Save the SSO configuration.



+ Add SSO configuration

CT-QA-SSO-Azure-SAML SAML

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

Activate SSO for login

Delete SSO configuration ✓ Save

* SSO configuration name (required): CT-QA-SSO-Azure-SAML

* SSO URL (required): https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984bc579/saml2

* Entity ID (required): https://sts.windows.net/643fbbdc-a0a5-4bec-845b-c5bb984bc579/

Metadata URL: https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984bc579/federationmetadata/2007

Attribute mapping

Select attribute identifier

● Email address ○ Employee ID

* Attribute name (required): http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

* Crypto key attribute name for EQS Integrity Line (required): cryptokey_ct_qa1

* SAML signing certificate in raw format (required):

```
MIIC8DCCAdigAwIBAgIQH7r/NRjdMaFPkY7LiULp7jANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEyINaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMzA3MTMxNTEwMjZaFw
0yNjA3MTMxNTEwMjVaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQgU1NPIENlcnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwyKTglWSfWC4si0sx9ZbW7k8jf
qLCGMTiKiqnOH9rJdcYP15nfCbvfoNY+iMw0t5WViqRTOBLG/TpL3kkoHfcOV9Z7traXnSXqqJ+t7aBH1DmBleQJ8aNZvkiIB2MXmTSNziv+eKcCNxrEAbv8OVosvbq/AzLNTDHF+3VUKZ1BHFI64f6WJB5wTJ6Udi9LC
```

Metadata URL for client IdP: https://api-compliance.eqs.qa/data-center/api/sso/saml/metadata/b207ba7a-16be-4c0d-9a98-da8c041bfa1b

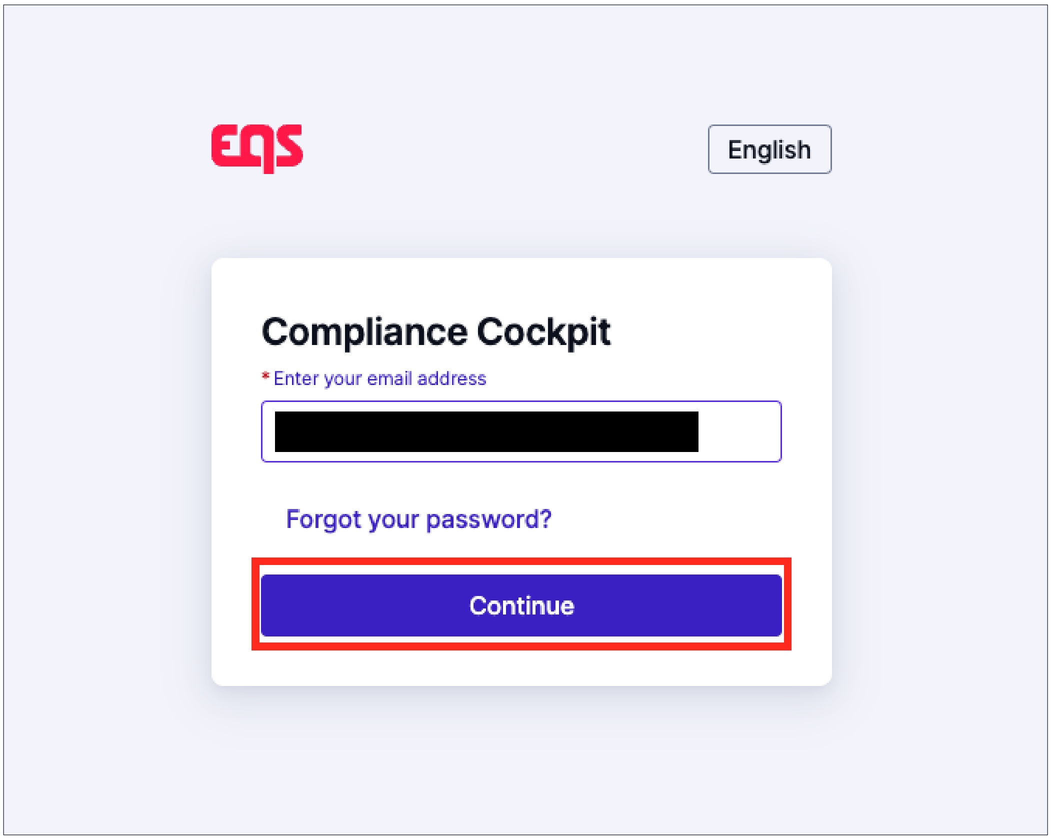
Crypto key for EQS Integrity Line (IL)

Last generated at 2024-10-14T10:44:38+00:00

MzM4MDkwMjMxNjM3MTA4NTcxOTExNDMwNzcxMTE2Mjk3NjQ1MTkwODI4MzMwODM2NjIzNTEzOTE3OTQ3MTIyMzAzMzMzNw==

Advanced Settings

15. Log out and log in again, this time with SSO by typing your e-mail address.



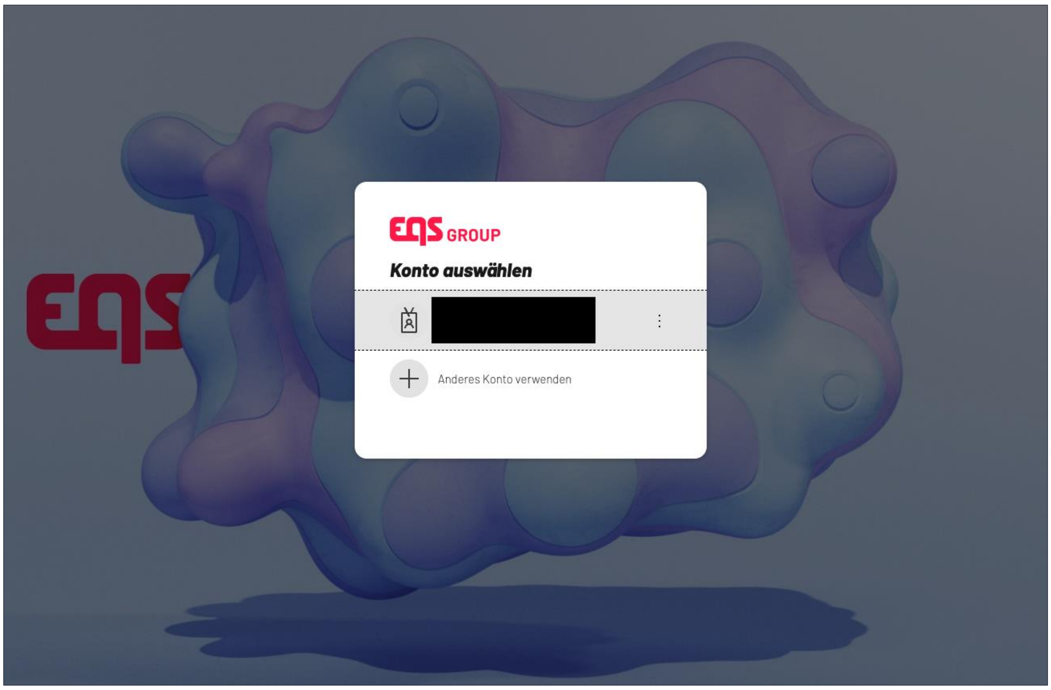
Compliance Cockpit

* Enter your email address

[redacted]

Forgot your password?

Continue



Konto auswählen

[redacted]

Anderes Konto verwenden

After activating the SSO, all users and groups assigned to the enterprise application are going to be able to log in into the Compliance Platform.

2.2 OpenID Connect

OpenID Connect (OIDC) is a protocol to verify user identities and get user profile information. OIDC enables devices to verify identities based on authentication done by an authentication server.

2.2.1 Microsoft Entra

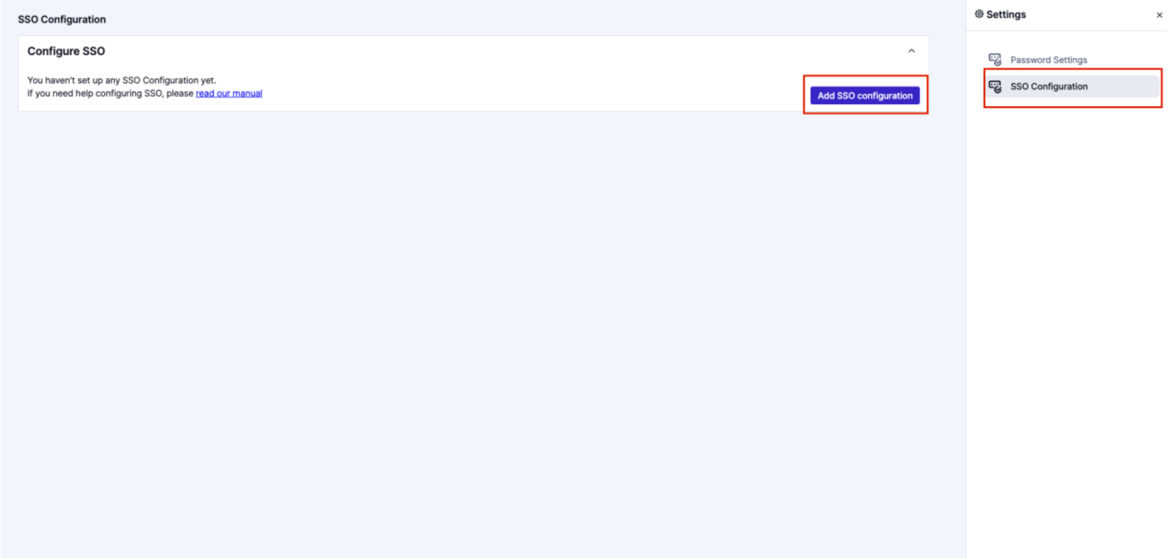
In this section we are going to setup SSO with **Microsoft Entra**, Microsoft's application to automate identity lifecycle management.

This is done via the following steps:

1. Create an enterprise application in your Azure portal at https://portal.azure.com.
2. Create and configure a new OIDC connector within EQS Compliance Cockpit.
3. Configure the Azure enterprise application with EQS Compliance Cockpit Service Provider.
4. Activate and start using Single Sign-On.

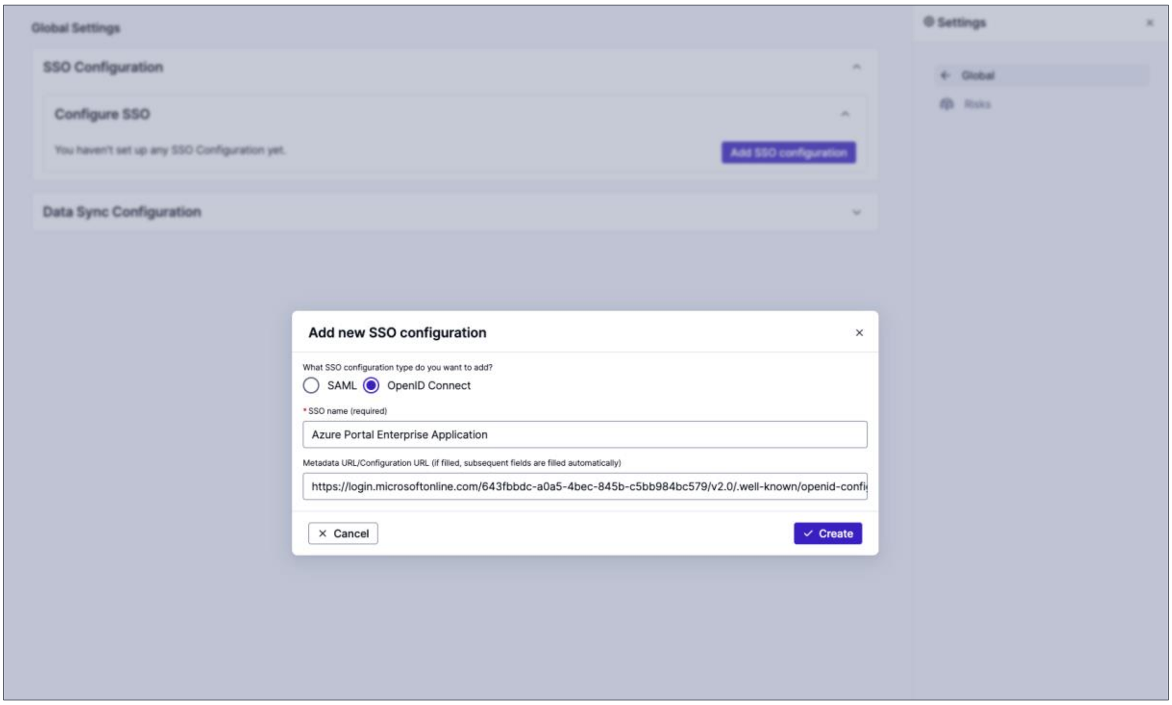
2.2.1.1 Step-by-Step Process

1. Log into EQS Compliance Cockpit with your user credentials.
2. Click the gear icon on the top-right to open the settings sidebar.
3. Select "Global" and expand the SSO Configuration section, then click the "Add SSO configuration" button to open the connector creation dialog.



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

4. Enter a name for your OIDC connector and the Configuration URL from your Enterprise Application, if available, then click the "Create" button.



Add new SSO configuration

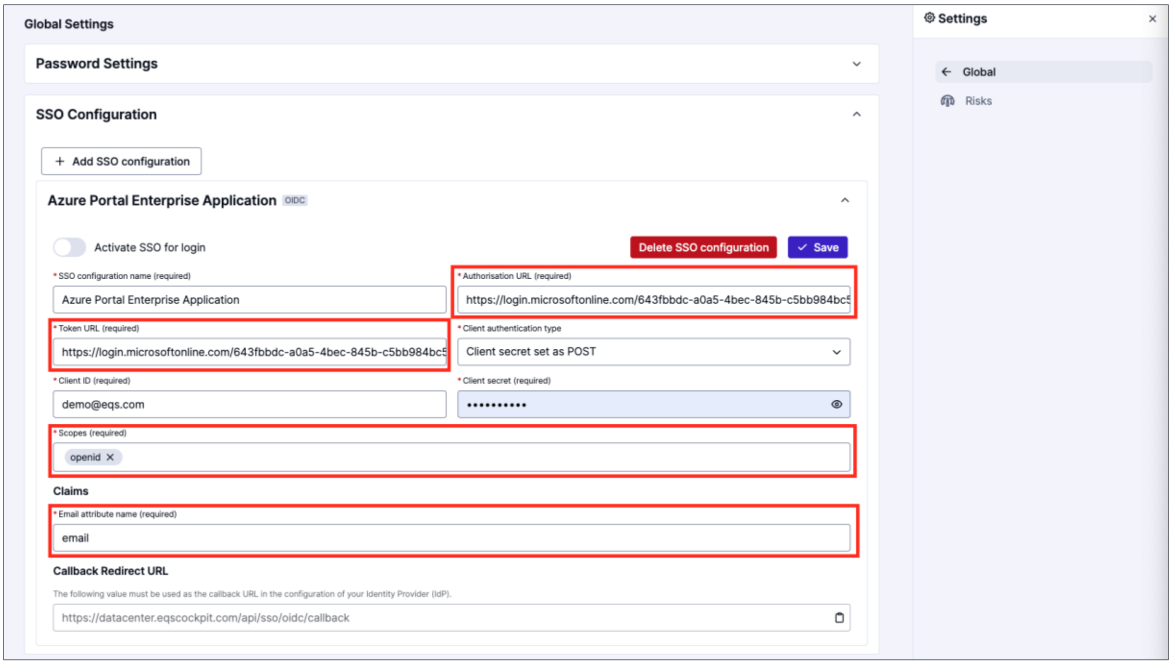
What SSO configuration type do you want to add?

○ SAML ● OpenID Connect

* SSO name (required): Azure Portal Enterprise Application

Metadata URL/Configuration URL (if filled, subsequent fields are filled automatically): https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984bc579/v2.0/.well-known/openid-confi

5. A new connector configuration panel is shown in the “SSO Configuration” section. If you entered a valid Configuration URL in the creation process, the red marked fields **Authorisation URL**, **Token URL**, **Scopes** and **Claims** should be automatically filled, if not please fill them with the information from your Enterprise Application. Ignore the automatic added data for Client ID and Client secret, they will be configured in the next step.



Azure Portal Enterprise Application OIDC

Activate SSO for login

* SSO configuration name (required): Azure Portal Enterprise Application

* Authorisation URL (required): https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984bc5

* Token URL (required): https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984bc5

* Client authentication type: Client secret set as POST

* Client ID (required): demo@eqs.com

* Client secret (required): ••••••••••

* Scopes (required): openid ×

Claims

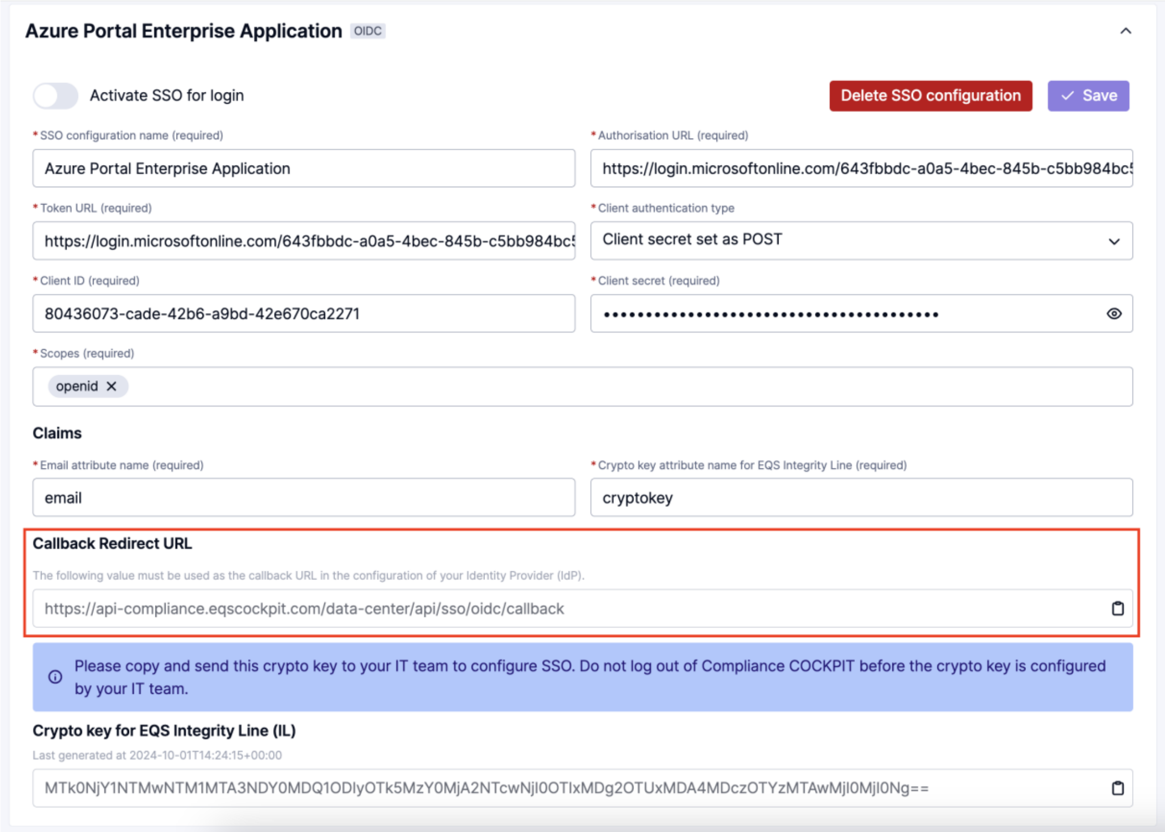
* Email attribute name (required): email

Callback Redirect URL

The following value must be used as the callback URL in the configuration of your Identity Provider (IdP).

https://datacenter.eqscockpit.com/api/sso/oidc/callback

6. It also displays the **Callback Redirect URL**, which is going to be configured in your Azure enterprise application.



Azure Portal Enterprise Application OIDC

Activate SSO for login

* SSO configuration name (required): Azure Portal Enterprise Application

* Authorisation URL (required): https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984bc

* Token URL (required): https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984bc5

* Client authentication type: Client secret set as POST

* Client ID (required): 80436073-cade-42b6-a9bd-42e670ca2271

* Client secret (required): ••

* Scopes (required): openid ✕

Claims

* Email attribute name (required): email

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

Callback Redirect URL

The following value must be used as the callback URL in the configuration of your Identity Provider (IdP).

https://api-compliance.eqscockpit.com/data-center/api/sso/oidc/callback

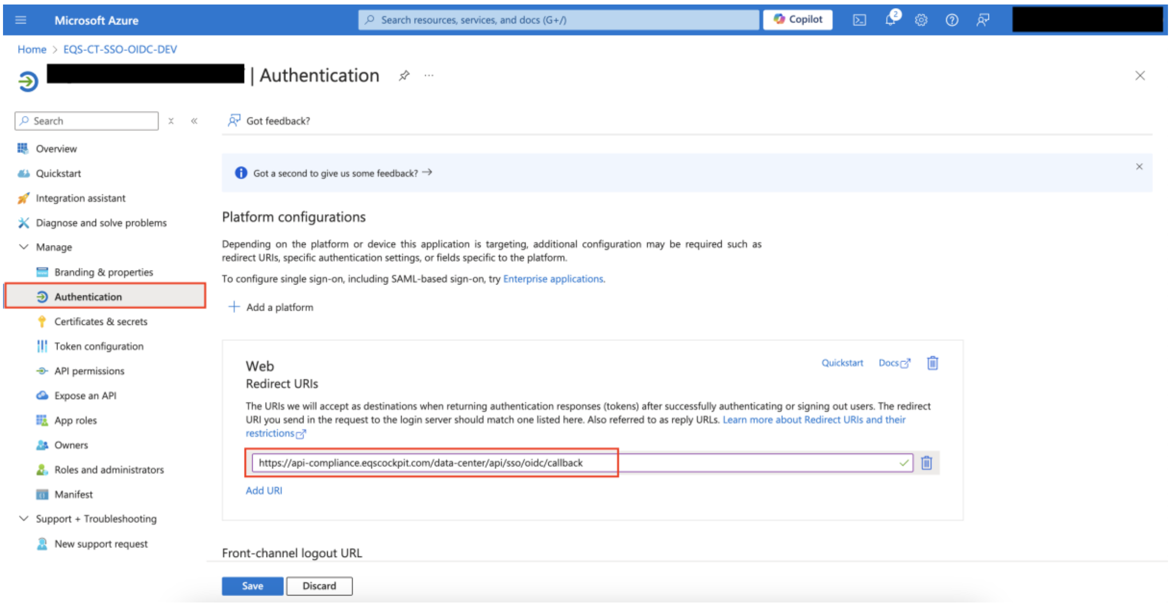
ⓘ Please copy and send this crypto key to your IT team to configure SSO. Do not log out of Compliance COCKPIT before the crypto key is configured by your IT team.

Crypto key for EQS Integrity Line (IL)

Last generated at 2024-10-01T14:24:15+00:00

MTk0NjY1NTMwNTM1MTA3NDY0MDQ1ODIyOTk5MzY0MjA2NTcwNjI0OTIxMDg2OTUxMDA4MDczOTYzMTAwMjI0MjI0Ng==

7. Open https://portal.azure.com and find your enterprise application, your IT department may want to create a new one. Once you have your enterprise application, go to "Authentication" and add a Web Redirect URI with the Callback Redirect URL value from the EQS Compliance Cockpit SSO configuration:



[redacted]

Home > EQS-CT-SSO-OIDC-DEV

[redacted] | Authentication

Got a second to give us some feedback? →

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

To configure single sign-on, including SAML-based sign-on, try Enterprise applications.

Web

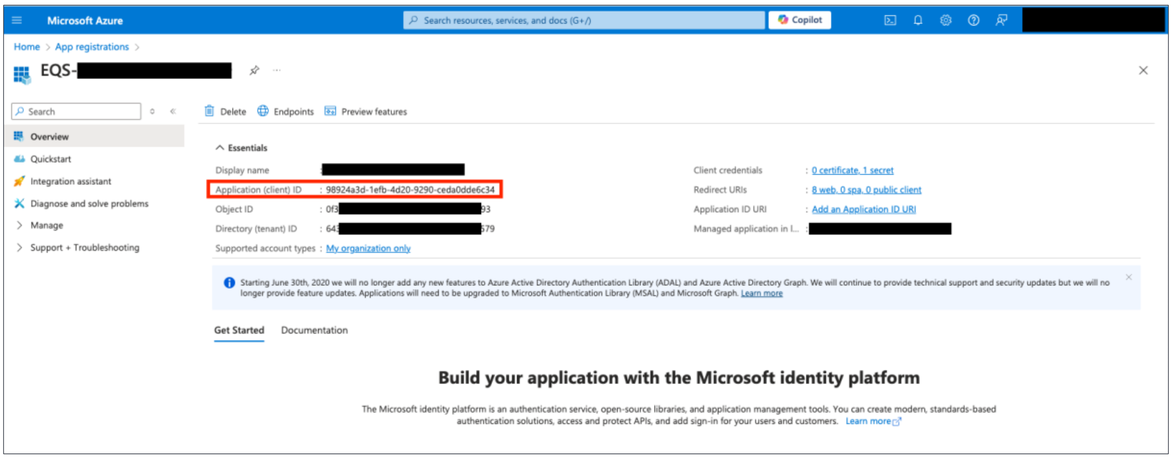
Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

https://api-compliance.eqscockpit.com/data-center/api/sso/oidc/callback

Front-channel logout URL

8. Also in the overview, copy the Client ID into the EQS Compliance Cockpit SSO configuration.



[redacted]

EQS-[redacted]

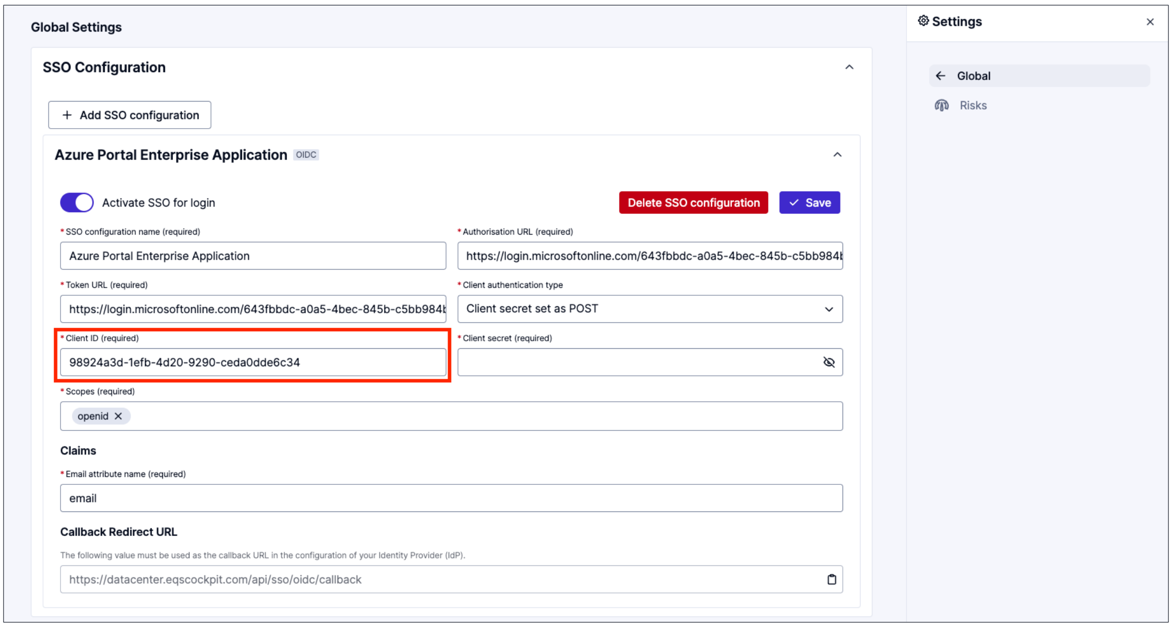
Essentials

Display name : [redacted]
Application (client) ID : 98924a3d-1efb-4d20-9290-ceda0dde6c34
Object ID : 0f3[redacted]93
Directory (tenant) ID : 643[redacted]579
Supported account types : My organization only
Client credentials : 0 certificate, 1 secret
Redirect URIs : 8 web, 0 spa, 0 public client
Application ID URI : Add an Application ID URI
Managed application in l... : [redacted]

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more



Azure Portal Enterprise Application OIDC

Activate SSO for login

* SSO configuration name (required): Azure Portal Enterprise Application
* Authorisation URL (required): https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984t
* Token URL (required): https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984t
* Client authentication type: Client secret set as POST
* Client ID (required): 98924a3d-1efb-4d20-9290-ceda0dde6c34
* Client secret (required):
* Scopes (required): openid ✕

Claims

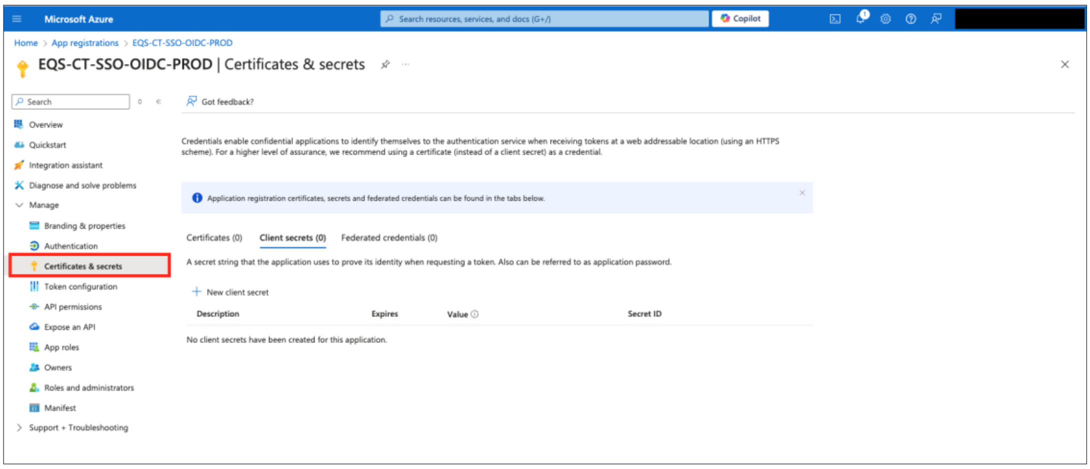
* Email attribute name (required): email

Callback Redirect URL

The following value must be used as the callback URL in the configuration of your Identity Provider (IdP).

https://datacenter.eqscockpit.com/api/sso/oidc/callback

9. Now go to “Certificates & secrets”.



EQS-CT-SSO-OIDC-PROD | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

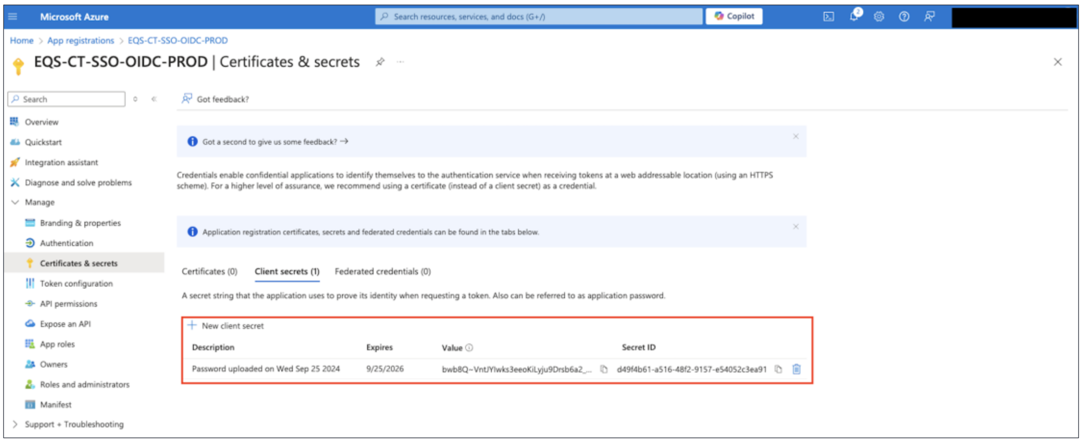
Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID

No client secrets have been created for this application.

10. Create a new secret and copy the Value into the EQS Compliance Cockpit SSO configuration.



EQS-CT-SSO-OIDC-PROD | Certificates & secrets

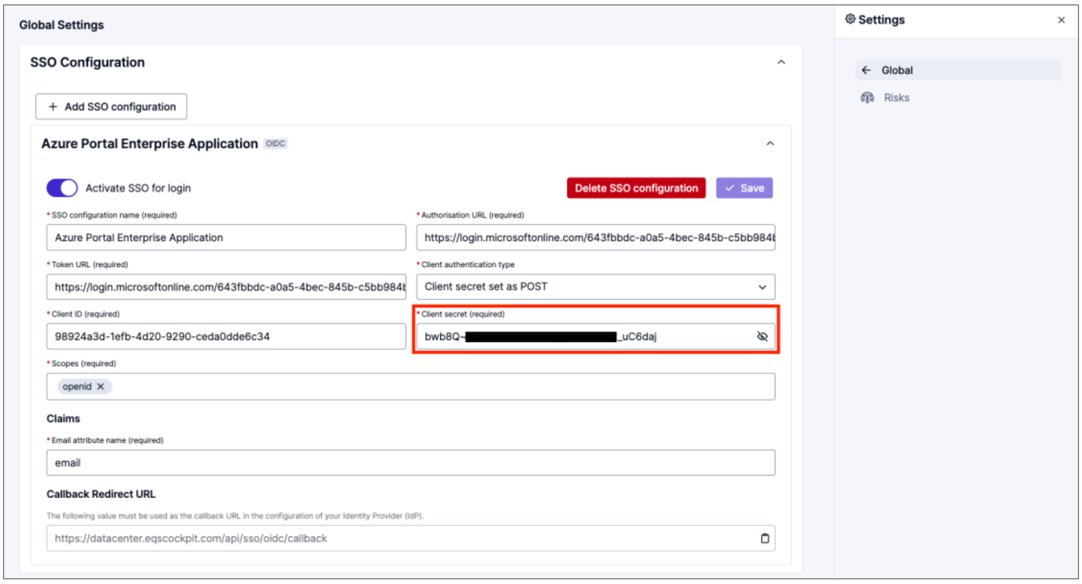
Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
Password uploaded on Wed Sep 25 2024	9/25/2026	bwb8Q~VntJYlwks3eeoKiLyju9Drsb6a2_...	d49f4b61-a516-48f2-9157-e54052c3ea91



SSO Configuration

Azure Portal Enterprise Application

Activate SSO for login

* SSO configuration name (required) Azure Portal Enterprise Application	* Authorisation URL (required) https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984t
* Token URL (required) https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984t	* Client authentication type Client secret set as POST
* Client ID (required) 98924a3d-1efb-4d20-9290-ceda0dde6c34	* Client secret (required) bwb8Q~[redacted]_uC6daj

* Scopes (required)
openid ✕

Claims

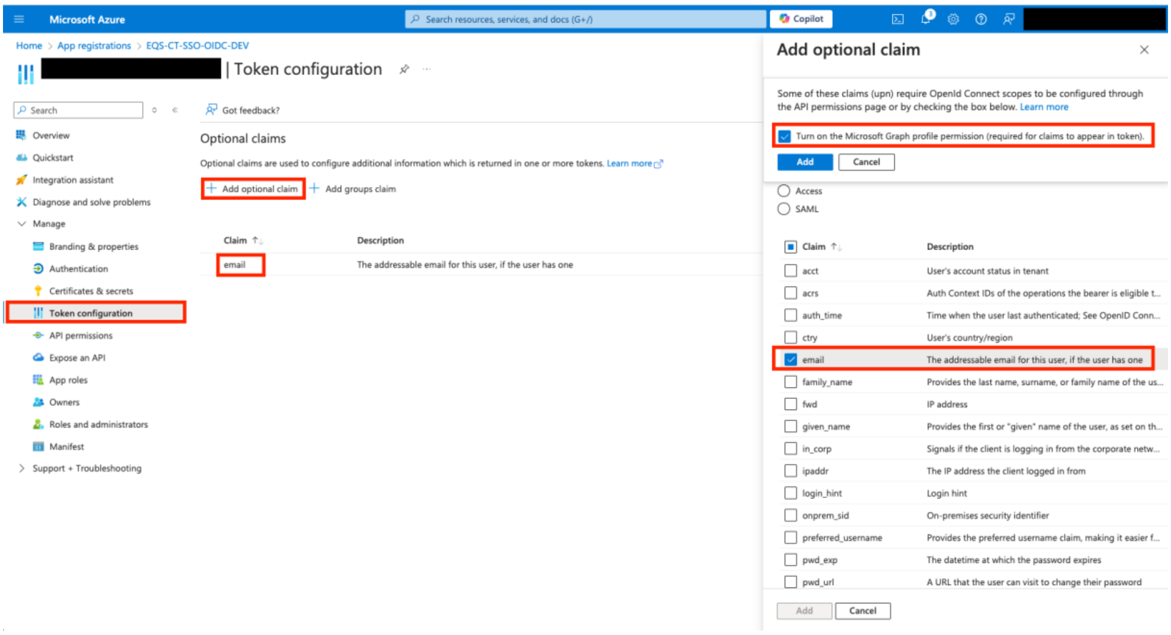
* Email attribute name (required)
email

Callback Redirect URL

The following value must be used as the callback URL in the configuration of your Identity Provider (IdP).

https://datacenter.eqscockpit.com/api/sso/oidc/callback

11. Go to "Token configuration" and create a new optional **email** claim of type ID, while checking the checkbox for Graph API. Then, copy the Claim name into the EQS Compliance Cockpit SSO configuration.



[redacted]

Home > App registrations > EQS-CT-SSO-OIDC-DEV

[redacted] | Token configuration

Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

Claim	Description
email	The addressable email for this user, if the user has one

Add optional claim

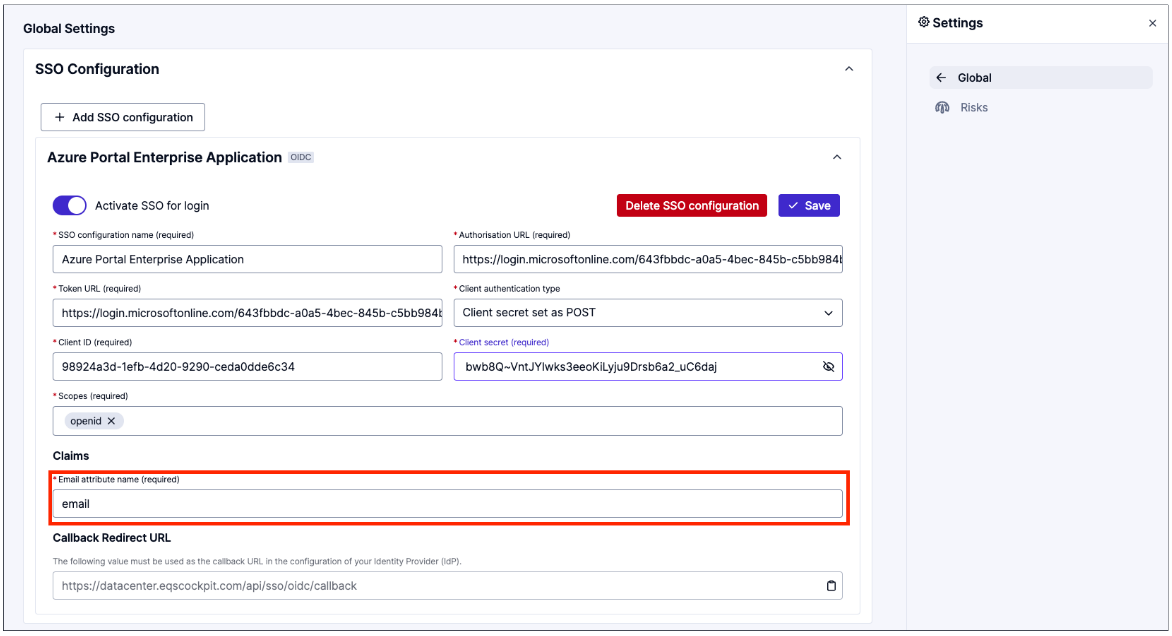
Some of these claims (upn) require OpenId Connect scopes to be configured through the API permissions page or by checking the box below. Learn more

☑ Turn on the Microsoft Graph profile permission (required for claims to appear in token).

○ Access

○ SAML

☐ Claim	Description
☐ acct	User's account status in tenant
☐ acrs	Auth Context IDs of the operations the bearer is eligible t...
☐ auth_time	Time when the user last authenticated; See OpenID Conn...
☐ ctry	User's country/region
☑ email	The addressable email for this user, if the user has one
☐ family_name	Provides the last name, surname, or family name of the us...
☐ fwd	IP address
☐ given_name	Provides the first or "given" name of the user, as set on th...
☐ in_corp	Signals if the client is logging in from the corporate netw...
☐ ipaddr	The IP address the client logged in from
☐ login_hint	Login hint
☐ onprem_sid	On-premises security identifier
☐ preferred_username	Provides the preferred username claim, making it easier f...
☐ pwd_exp	The datetime at which the password expires
☐ pwd_url	A URL that the user can visit to change their password



Global Settings

SSO Configuration

Azure Portal Enterprise Application OIDC

Activate SSO for login

* SSO configuration name (required): Azure Portal Enterprise Application

* Authorisation URL (required): https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984

* Token URL (required): https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984

* Client authentication type: Client secret set as POST

* Client ID (required): 98924a3d-1efb-4d20-9290-ceda0dde6c34

* Client secret (required): bwb8Q~VntJYIwks3eeoKiLyju9Drsb6a2_uC6daj

* Scopes (required): openid ✕

Claims

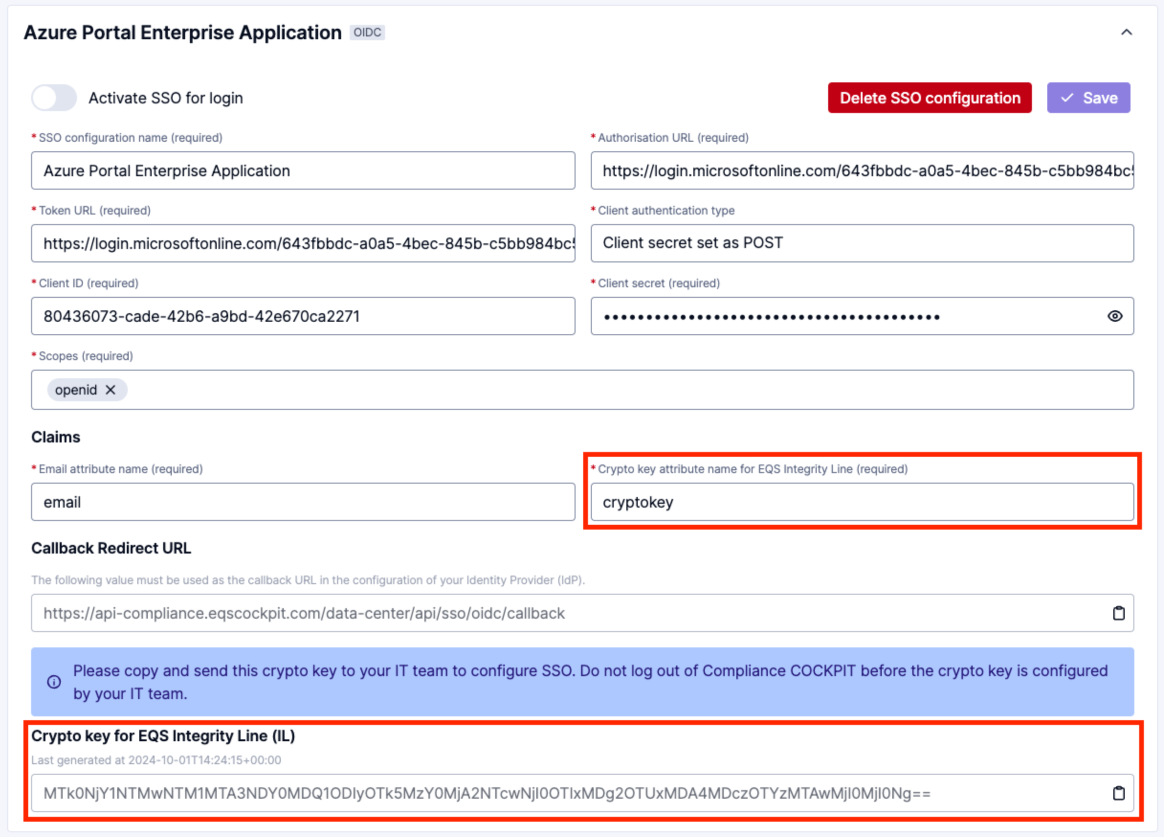
* Email attribute name (required): email

Callback Redirect URL

The following value must be used as the callback URL in the configuration of your Identity Provider (IdP).

https://datacenter.eqscockpit.com/api/sso/oidc/callback

12. **In case your license contains Integrity Line**, you must also add a new custom claim from EQS Compliance Cockpit SSO Configuration into your Enterprise Application. **If not, you can skip to Step 11.**



Azure Portal Enterprise Application OIDC

* SSO configuration name (required): Azure Portal Enterprise Application

* Authorisation URL (required): https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984bc

* Token URL (required): https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984bc

* Client authentication type: Client secret set as POST

* Client ID (required): 80436073-cade-42b6-a9bd-42e670ca2271

* Client secret (required): ••••••••••••••••••••••••••••••••••••••

* Scopes (required): openid ✕

Claims

* Email attribute name (required): email

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

Callback Redirect URL

The following value must be used as the callback URL in the configuration of your Identity Provider (IdP).

https://api-compliance.eqscockpit.com/data-center/api/sso/oidc/callback

ⓘ Please copy and send this crypto key to your IT team to configure SSO. Do not log out of Compliance COCKPIT before the crypto key is configured by your IT team.

Crypto key for EQS Integrity Line (IL)

Last generated at 2024-10-01T14:24:15+00:00

MTk0NjY1NTMwNTM1MTA3NDY0MDQ1ODIyOTk5MzY0MjA2NTcwNjI0OTIxMDg2OTUxMDA4MDczOTYzMTAwMjI0MjI0Ng==

12.1. To add a custom claim, make sure you have **AzureADPreview** module installed, before running below commands in your **PowerShell**:

```
Connect-AzureAD

New-AzureADPolicy -Definition @('
{
  "ClaimsMappingPolicy":
  {
    "Version":1,"IncludeBasicClaimSet":"true",
    "ClaimsSchema":
[{"Source":"user","ID":"extensionattribute1","SamlClaimType":"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/cryptokey","JwtClaimType":"cryptokey"}]
  }
}') -DisplayName "CryptokeyExtraClaim" -Type "ClaimsMappingPolicy"
```

12.2. Note the **ID** of the policy and assign it to your service principal using below command:

```
Add-AzureADServicePrincipalPolicy -Id serviceprincipal_ObjectID -RefObjectId policy_ID
```

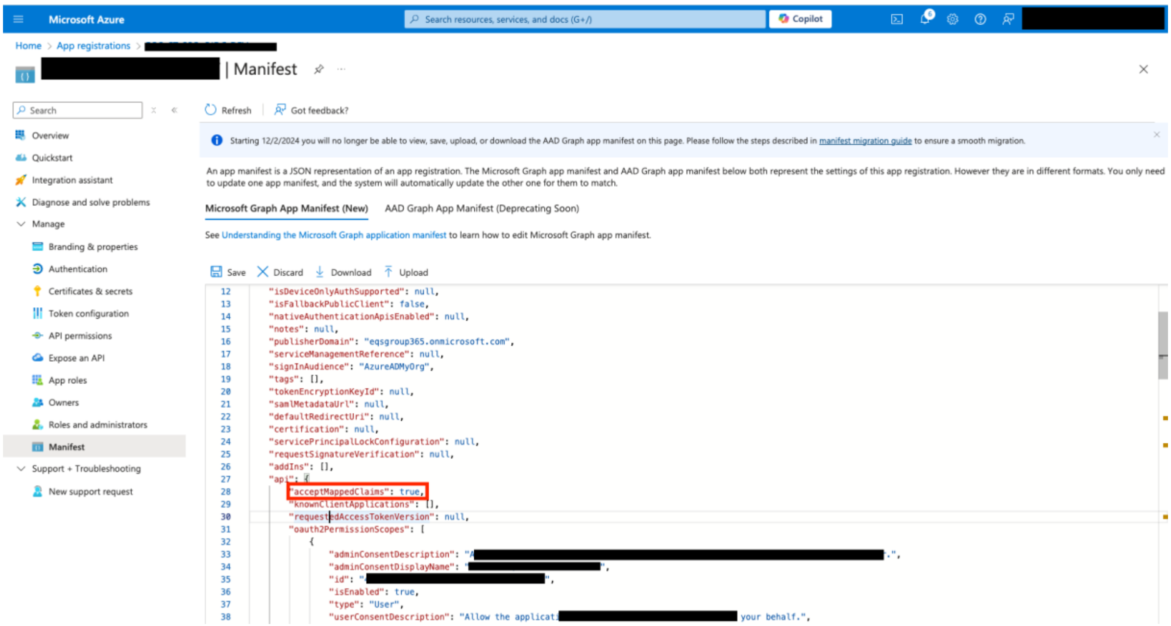
12.3. To confirm whether the policy is assigned or not, run below command:

Get-AzureADServicePrincipalPolicy -Id ***serviceprincipal_ObjectID***

12.4. To assign a **value** to that claim, sign in as admin to **Microsoft Graph Explorer** and run the below query, where the value is the value seem in the EQS Compliance Cockpit SSO Configuration under Cryptokey for EQS Integrity Line (IL) label:

```
PATCH https://graph.microsoft.com/beta/me
{
"onPremisesExtensionAttributes":
  {
    "extensionAttribute1":
"MTk0NjY1NTMwNTM1MTA3NDY0MDQ1ODIyOTk5MzY0MjA2NTcwNjI0OTIxMDg2OTUxMDA4MDczOTYzMTAwMjI0MjI0Ng=="
  }
}
```

12.5. Go to the Azure Portal in your Registered Enterprise Application and make sure to set **"acceptMappedClaims": true** in the applications' Manifest like below:



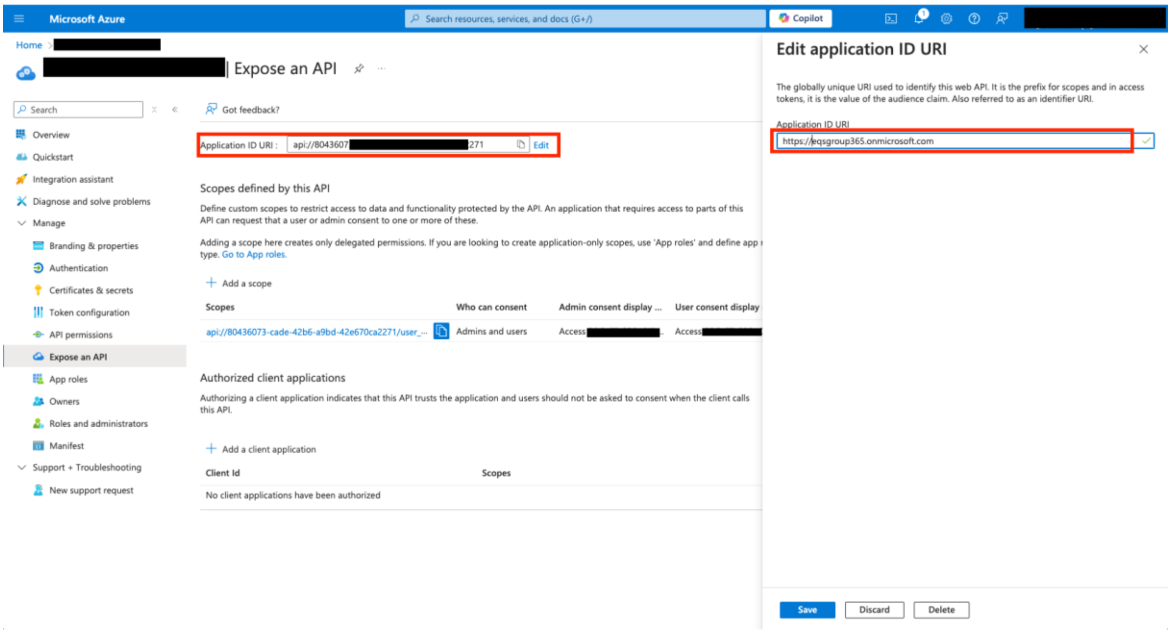
Starting 12/2/2024 you will no longer be able to view, save, upload, or download the AAD Graph app manifest on this page. Please follow the steps described in manifest migration guide to ensure a smooth migration.

An app manifest is a JSON representation of an app registration. The Microsoft Graph app manifest and AAD Graph app manifest below both represent the settings of this app registration. However they are in different formats. You only need to update one app manifest, and the system will automatically update the other one for them to match.

See Understanding the Microsoft Graph application manifest to learn how to edit Microsoft Graph app manifest.

```
    "isDeviceOnlyAuthSupported": null,
    "isFallbackPublicClient": false,
    "nativeAuthenticationApisEnabled": null,
    "notes": null,
    "publisherDomain": "eqsgroup365.onmicrosoft.com",
    "serviceManagementReference": null,
    "signInAudience": "AzureADMyOrg",
    "tags": [],
    "tokenEncryptionKeyId": null,
    "samlMetadataUrl": null,
    "defaultRedirectUri": null,
    "certification": null,
    "servicePrincipalLockConfiguration": null,
    "requestSignatureVerification": null,
    "addIns": [],
    "api": {
        "acceptMappedClaims": true,
        "knownClientApplications": [],
        "requestedAccessTokenVersion": null,
        "oauth2PermissionScopes": [
            {
                "adminConsentDescription": "A[redacted].",
                "adminConsentDisplayName": "[redacted]",
                "id": "[redacted]",
                "isEnabled": true,
                "type": "User",
                "userConsentDescription": "Allow the applicat[redacted] your behalf.",
```

12.6. Then go to Expose an API, under Application ID URI, if your value is using the pattern *api://<GUID>*, you must change to *https://<yourTenantDomain>*. i.e: https://contoso.onmicrosoft.com:



Home > [redacted]

[redacted] | Expose an API

Application ID URI : api://8043607[redacted]271 Edit

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'App roles' and define app type. Go to App roles.

Scopes	Who can consent	Admin consent display ...	User consent display
api://80436073-cade-42b6-a9bd-42e670ca2271/user_...	Admins and users	Access [redacted]	Access [redacted]

Authorized client applications

Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.

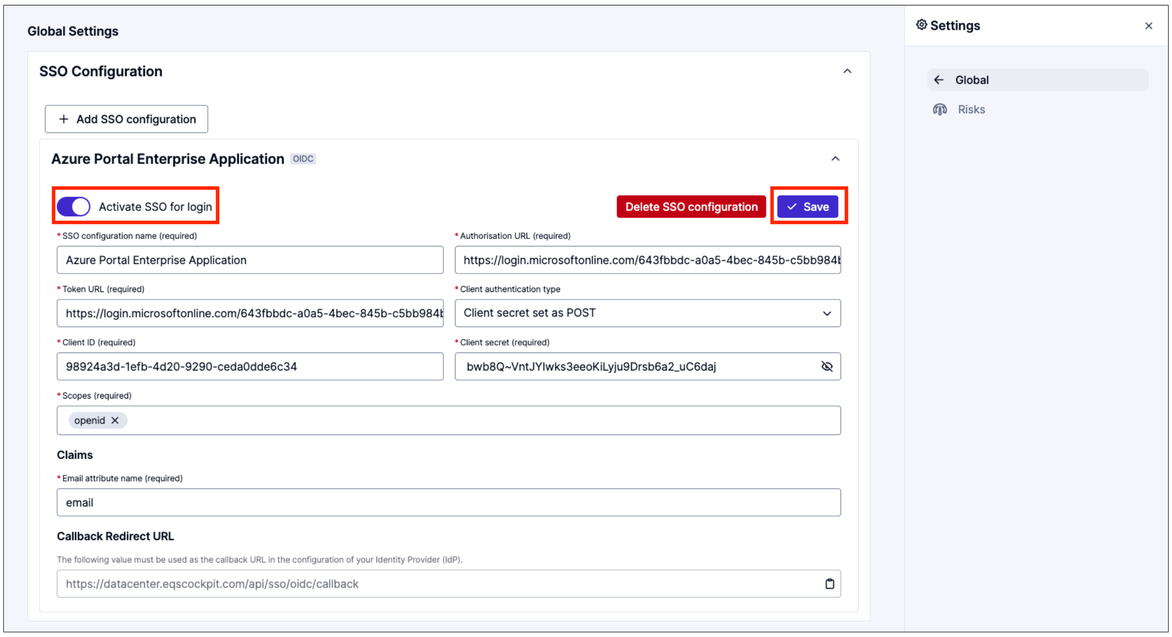
Client Id	Scopes
No client applications have been authorized	

Edit application ID URI

The globally unique URI used to identify this web API. It is the prefix for scopes and in access tokens, it is the value of the audience claim. Also referred to as an identifier URI.

Application ID URI: https://eqsgroup365.onmicrosoft.com ✓

13. Now activate and Save the SSO configuration.



Global Settings

SSO Configuration

+ Add SSO configuration

Azure Portal Enterprise Application OIDC

Activate SSO for login

Delete SSO configuration

✓ Save

* SSO configuration name (required): Azure Portal Enterprise Application

* Authorisation URL (required): https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984

* Token URL (required): https://login.microsoftonline.com/643fbbdc-a0a5-4bec-845b-c5bb984

* Client authentication type: Client secret set as POST

* Client ID (required): 98924a3d-1efb-4d20-9290-ceda0dde6c34

* Client secret (required): bwb8Q~VntJYIwks3eeoKiLyju9Drsb6a2_uC6daj

* Scopes (required): openid ✕

Claims

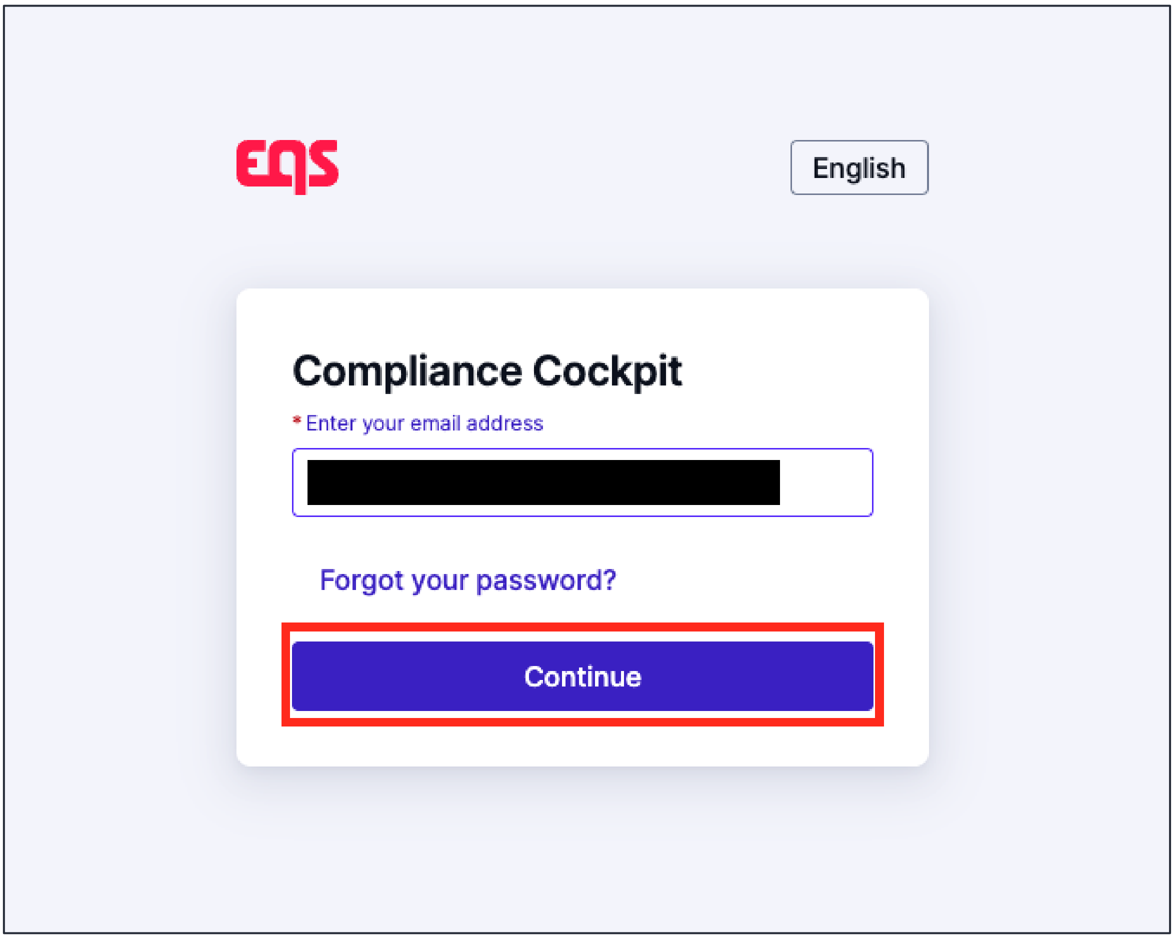
* Email attribute name (required): email

Callback Redirect URL

The following value must be used as the callback URL in the configuration of your Identity Provider (IdP).

https://datacenter.eqscockpit.com/api/sso/oidc/callback

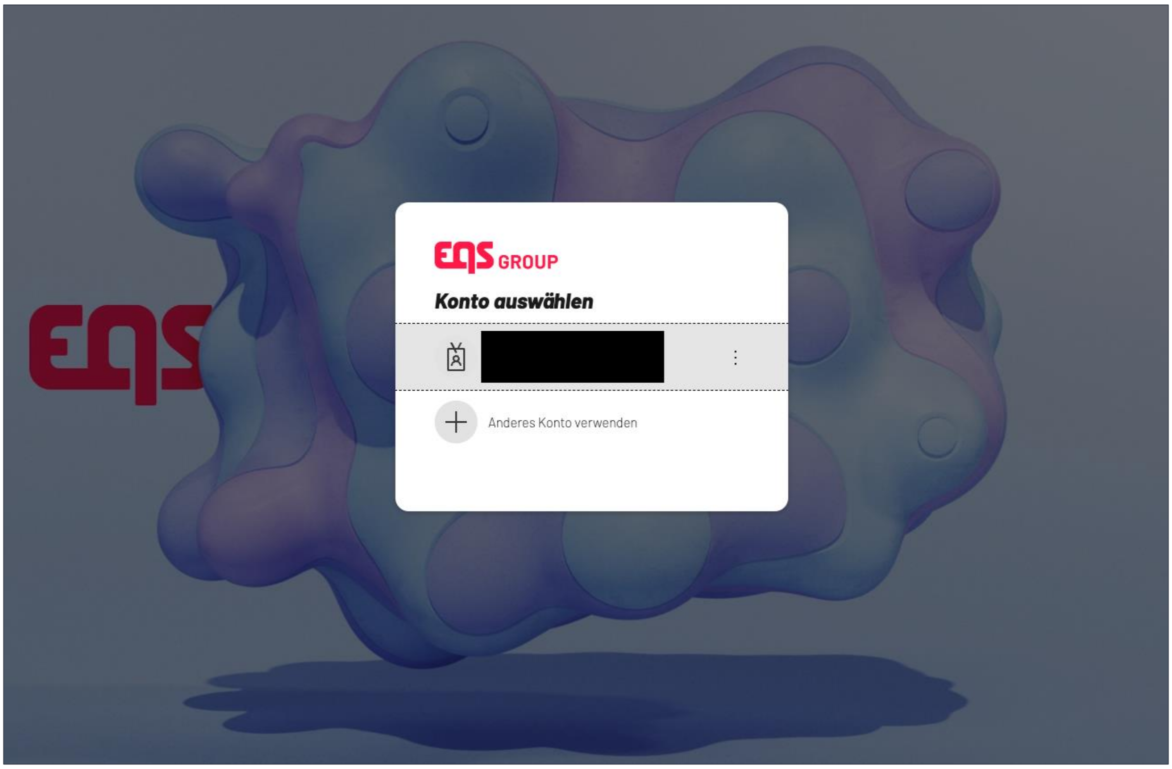
14. Log out and log in again, this time with SSO by typing your e-mail address.



Compliance Cockpit

* Enter your email address

[redacted]



Konto auswählen

[redacted]

After activating the SSO, all users and groups assigned to the enterprise application are going to be able to log in into the Compliance Platform.

2.3 Frequently Asked Questions

Welcome to our Frequently Asked Questions (FAQ) section. Here, you'll find answers to some of the most common inquiries about our Single Sign-on. If you don't find what you're looking for, feel free to reach out to our customer support team for further assistance.

2.3.1 Is it possible to have IDP-Initiated Login?

Yes, we do offer this capability.

2.3.2 Is it possible to have Just-In-Time provisioning via SSO?

No, we do not offer this capability. Please give a look in our DataSync documents, we offer SCIM as a solution for this.

2.3.3 Can a client in Demo Status test/configure SSO?

Yes, but the demo user will not be able to login anymore. Also, if the license contains IL, be aware, when going Live, the client will have to re-set the crypto key in the client's IdP.

2.3.4 Can user e-mails have multiple different domains?

Yes, the only requirement is the user's email have to exist in client's IdP.

2.3.5 What is cryptokey?

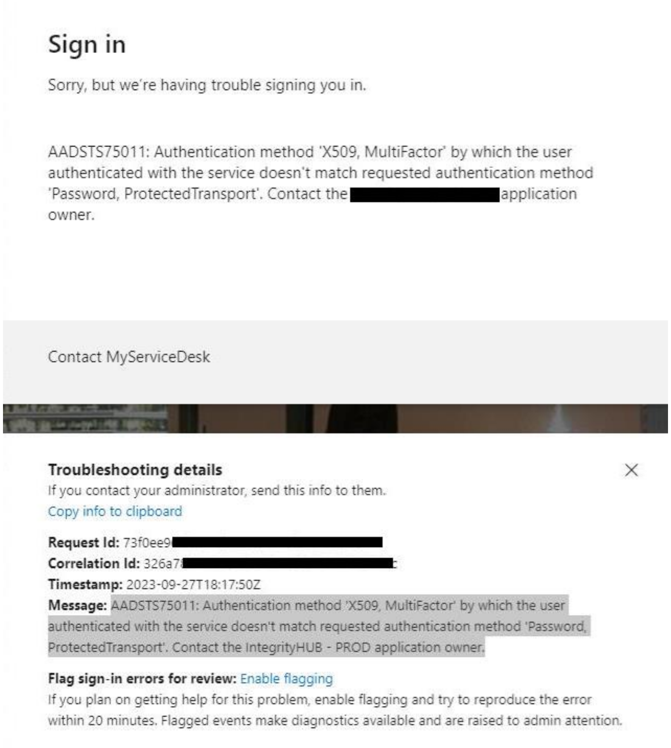
Cryptokey is specific related to Integrity Line module, this key is used to encrypt all cases created and only you have access to this key. Why do we need to add this key as an attribute? Because users, with the correct permissions, need to be able to open cases.

2.4 Troubleshooting

Welcome to our Troubleshooting. Here, you'll find step-by-step guidance to help you resolve common issues you may encounter while using Single Sign-on with our product. We've compiled a list of typical problems along with practical solutions to get you back on track quickly. If you need further assistance, don't hesitate to reach our customer support team for further assistance.

2.4.1 Authentication method error (SAML)

If you have issues related to the Authentication Method, like the image below:



Sign in

Sorry, but we're having trouble signing you in.

AADSTS75011: Authentication method 'X509, MultiFactor' by which the user authenticated with the service doesn't match requested authentication method 'Password, ProtectedTransport'. Contact the [redacted] application owner.

Contact MyServiceDesk

Troubleshooting details

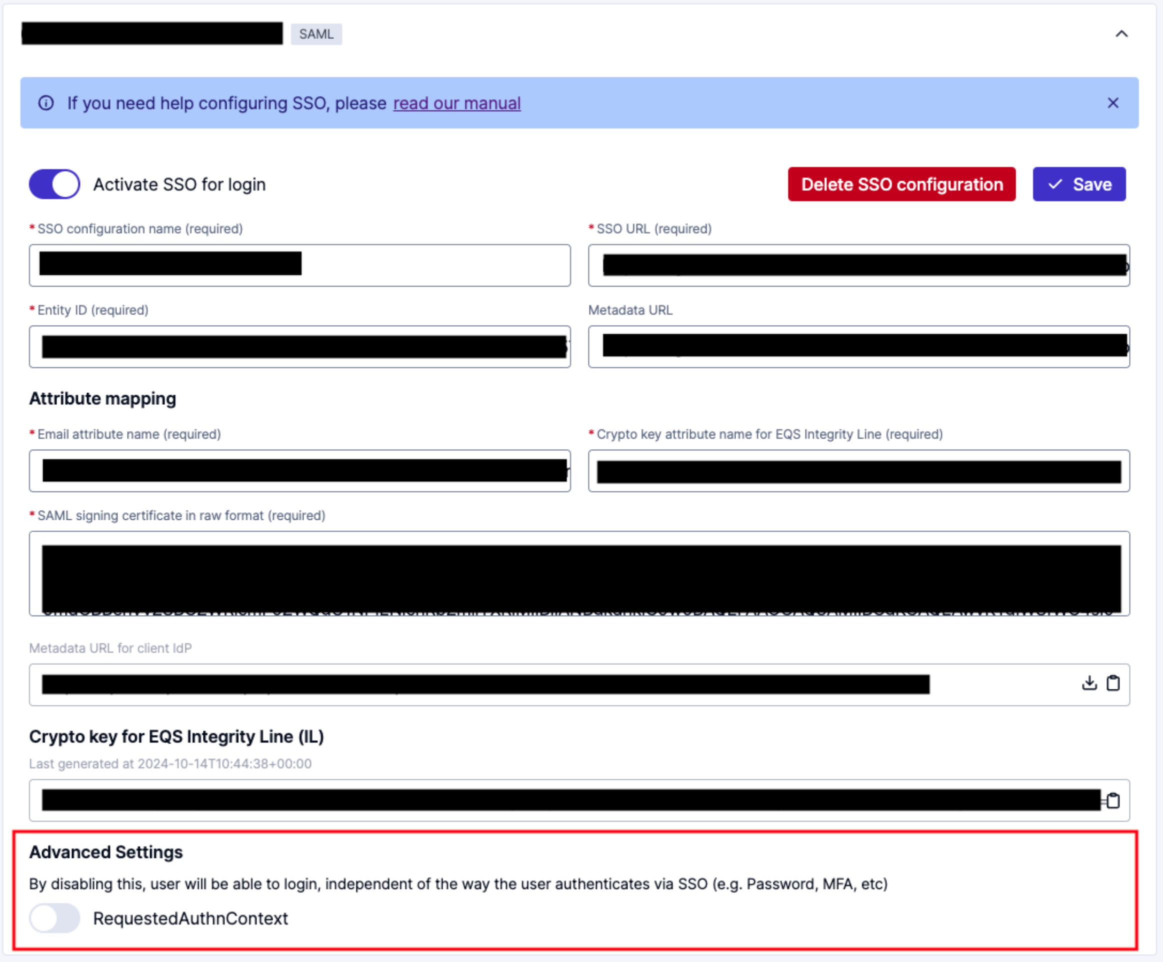
If you contact your administrator, send this info to them.

Copy info to clipboard

Request Id: 73f0ee9[redacted]
Correlation Id: 326a7[redacted]
Timestamp: 2023-09-27T18:17:50Z
Message: AADSTS75011: Authentication method 'X509, MultiFactor' by which the user authenticated with the service doesn't match requested authentication method 'Password, ProtectedTransport'. Contact the IntegrityHUB - PROD application owner.

Flag sign-in errors for review: Enable flagging
If you plan on getting help for this problem, enable flagging and try to reproduce the error within 20 minutes. Flagged events make diagnostics available and are raised to admin attention.

You can **turn OFF** the **RequestAuthnContext** option in the Advanced Settings of the SSO configuration in Compliance Cockpit.



[redacted] SAML

ⓘ If you need help configuring SSO, please read our manual ✕

● Activate SSO for login

* SSO configuration name (required)

[redacted]

* SSO URL (required)

[redacted]

* Entity ID (required)

[redacted]

Metadata URL

[redacted]

Attribute mapping

* Email attribute name (required)

[redacted]

* Crypto key attribute name for EQS Integrity Line (required)

[redacted]

* SAML signing certificate in raw format (required)

[redacted]

Metadata URL for client IdP

[redacted]

Crypto key for EQS Integrity Line (IL)

Last generated at 2024-10-14T10:44:38+00:00

[redacted]

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