

Eagle Eye Application Note - AN022

Configuring SSO in the Eagle Eye Cloud VMS Enhanced Web Interface

2025-01-30 Revision 2.0

Target Audience

This Application Note is intended for users of the Eagle Eye Cloud VMS, particularly those using the Enhanced Web Interface, who want to leverage the convenience and security of single sign-on (SSO) with common or custom Identity Providers (IdPs). Resellers can also configure SSO for their end users. Users of all Eagle Eye Cloud VMS Editions can log in with Microsoft or Google as an IdP, but Standard Edition users are limited to the following domains: [msn.com](https://www.msn.com), [live.com](https://www.live.com), [hotmail.com](https://www.hotmail.com), [outlook.com](https://www.outlook.com), [gmail.com](https://www.gmail.com), [een.com](https://www.een.com). Professional and Enterprise Edition users can log in via the IdP buttons even without SSO configured. Administrators always have the ability to log in directly.

Introduction

SSO (Single Sign-On) allows you to log in to multiple applications or services using just one set of login credentials. Instead of needing a separate username and password for each service, SSO lets you use a single identity to access everything. It simplifies login and increases security because you're managing fewer passwords.

Personal SSO (Google/Microsoft):

- Personal accounts like Google and Microsoft work as Identity Providers (IdPs) for SSO.
- Gmail or Outlook personal accounts are used to log in to other apps that support SSO.
- Personal SSO is mainly used for individual services, personal accounts, or smaller setups, where using a Google or Microsoft login adds convenience.

Corporate SSO Solutions (Okta/Azure):

- Okta or Microsoft Azure Active Directory (Azure AD) are designed for businesses.
- Okta or Azure AD allow companies to manage employee logins to various internal systems, apps, and cloud services from a central location.
- Okta and Azure AD offer more control, security, and integration options. Companies can enforce policies like multi-factor authentication (MFA) and easily manage services access.

- These systems are designed for large organizations where security, compliance, and scalability are crucial.

Key Differences:

- Personal SSO (Google/Microsoft): Great for convenience; designed for individuals or small-scale organizations.
- Corporate SSO (Okta/Azure): Designed for businesses, provides higher security, access control, and scalability for large teams.

Prerequisites

Before setting up SSO, you will need the following information depending on what method is being used (Google, Okta, Microsoft):

- Administrator privileges within the Eagle Eye Cloud VMS.
- Your Eagle Eye account ID (Account Number). Go to **Admin > Account Settings > General**.

General	Security	Camera	Privacy	Identity provider
Account name	00.API SANDBOX			
Account number	00153738			

- <registration-id> is the Eagle Eye Account ID.
- <domain-branding> can be eagleeyenetworks.com, mobotixcloud.com, etc.
- <webapp-url> can be "<https://webapp.eagleeyenetworks.com>" (Based on the domain branding you can use different values for this and make sure values are URL encoded).
- The redirectUrl for the account by adding your account ID at the end of this redirectUrl:
<https://auth.eagleeyenetworks.com/login/oauth2/code/<account ID>>

Note: If you do not have an account in Azure AD, register for a free account at <https://azure.microsoft.com>. If you do not have an account in Okta, register for a free account at <https://www.okta.com>

Configuring Google IdP via SSO

Follow the steps in this section to configure Google SSO authentication in the Cloud VMS enhanced web interface.

1. Go to **Admin > Account Settings > Identity Provider** and select Google.

Identity provider integration via Single Sign-on

Select and configure the Identity Provider you want to enable.

None

 Microsoft >

 Okta >

 Google v

Login only via Single Sign-On ⓘ

Custom SSO >



Sign in

Email

Remember me

_____ or _____

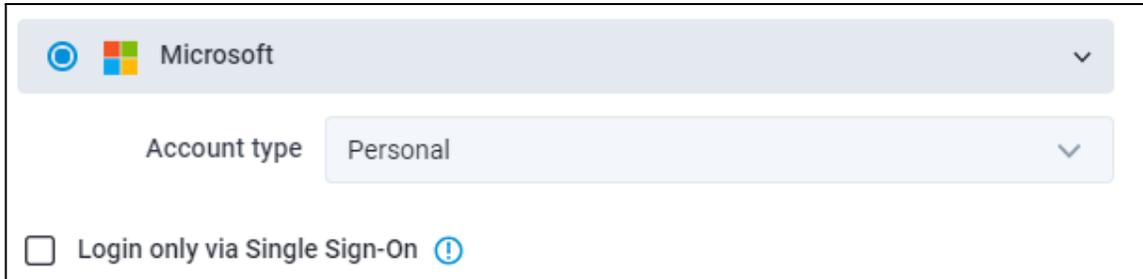
 Continue with Microsoft

 Continue with Google

2. Leave the **Login Only via Single Sign-on** checkbox unchecked to allow non-administrator users to have the option to log on with a direct password or by clicking **Continue with Google** to login via SSO.
3. Check the **Login only via Single-Sign-On** box to prohibit non-administrator users from logging into the Cloud VMS with a direct password. By entering a non-administrator username and clicking **Next**, the user is automatically redirected to the Google IdP for authentication. Additionally, users can log in using the **Continue with Google** button in the login interface.

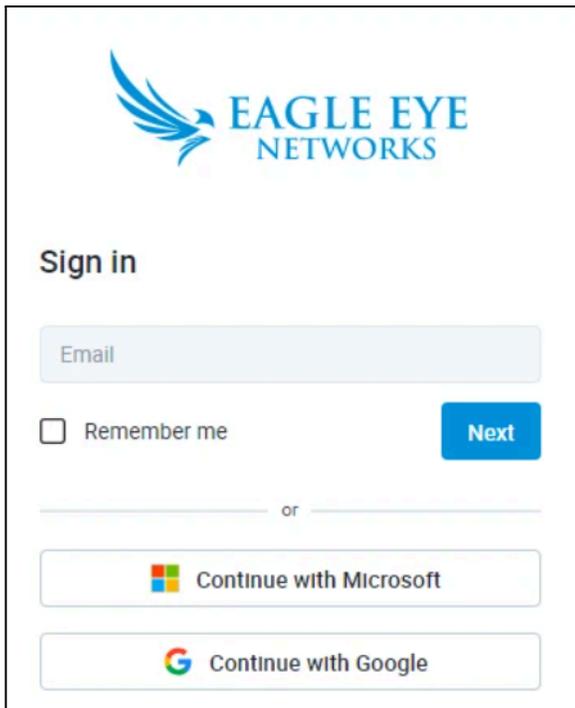
Configuring Microsoft IdP via SSO

1. Go to **Admin > Account Settings > Identity Provider** and select Microsoft.



The screenshot shows the configuration interface for the Microsoft Identity Provider. At the top, there is a dropdown menu with the Microsoft logo and the text "Microsoft". Below this is another dropdown menu labeled "Account type" with "Personal" selected. At the bottom, there is a checkbox labeled "Login only via Single Sign-On" which is currently unchecked, followed by a blue information icon.

2. Leave the **Login only via Single Sign-On** box unchecked to allow non-administrator users the option to log in with a direct password. They will also have the option to log in by clicking the **Continue with Microsoft** button in the login interface.



The screenshot shows the login interface for Eagle Eye Networks. At the top is the Eagle Eye Networks logo. Below the logo is the text "Sign in". There is an input field for "Email". Below the email field is a checkbox labeled "Remember me" and a blue button labeled "Next". Below the "Next" button is a horizontal line with the word "or" in the center. Below the line are two buttons: "Continue with Microsoft" and "Continue with Google".

3. Check the **Login only via Single-Sign-On** box to prohibit non-administrator users from logging into the VMS with a direct password. By entering a non-administrator username and clicking **Next**, the user is automatically redirected to the Microsoft IdP for authentication. Additionally, users can log in using the **Continue with Microsoft** button in the login interface.

Configuring Okta IdP for Eagle Eye SSO

Obtaining a redirectUrl from Okta

1. Open your Okta administrator dashboard and select **Applications > Applications** from the left navigation menu. Click **Create App Integration**.
2. On the **Create a New App Integration** screen, select **OIDC** for Sign-in Method and **Web Application** for Application Type. Click **Next**.

Create a new app integration

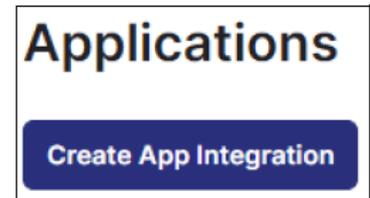
Sign-in method
[Learn More](#)

- OIDC - OpenID Connect**
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type
What kind of application are you trying to integrate with Okta?
Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

- Web Application**
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)
- Single-Page Application**
Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)
- Native Application**
Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

[Cancel](#) [Next](#)



3. On the **New Web App Integration** screen, enter the name for your app integration name and the URL for Sign-in redirect URLs.

New Web App Integration

General Settings

App integration name
Eagle Eye Networks Cloud VMS

Logo (Optional)

Grant type
[Learn More](#)

- Client acting on behalf of itself
 - Client Credentials
- Client acting on behalf of a user
 - Authorization Code
 - Refresh Token
 - Client-initiated backchannel authentication flow (CIBA)
 - Implicit (hybrid)

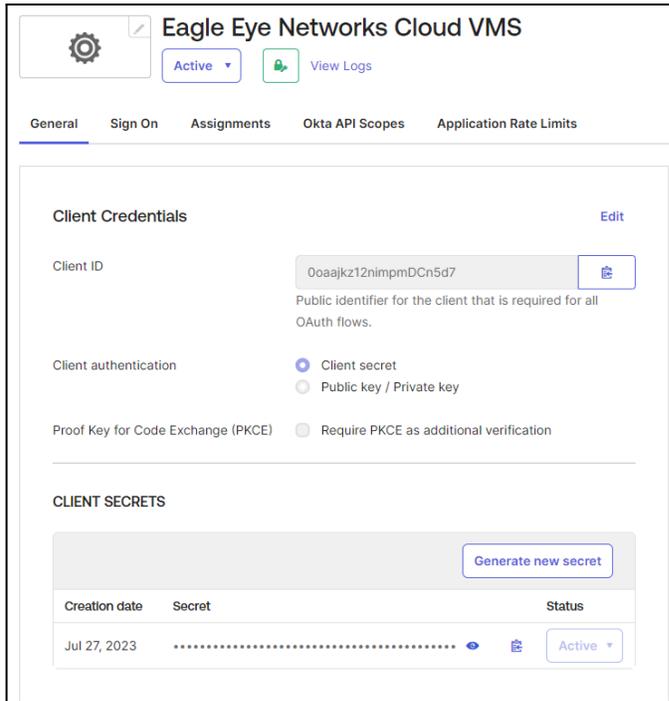
Sign-in redirect URIs
Okta sends the authentication response and ID token for the user's sign-in request to these URIs
[Learn More](#)

Allow wildcard * in sign-in URI redirect.

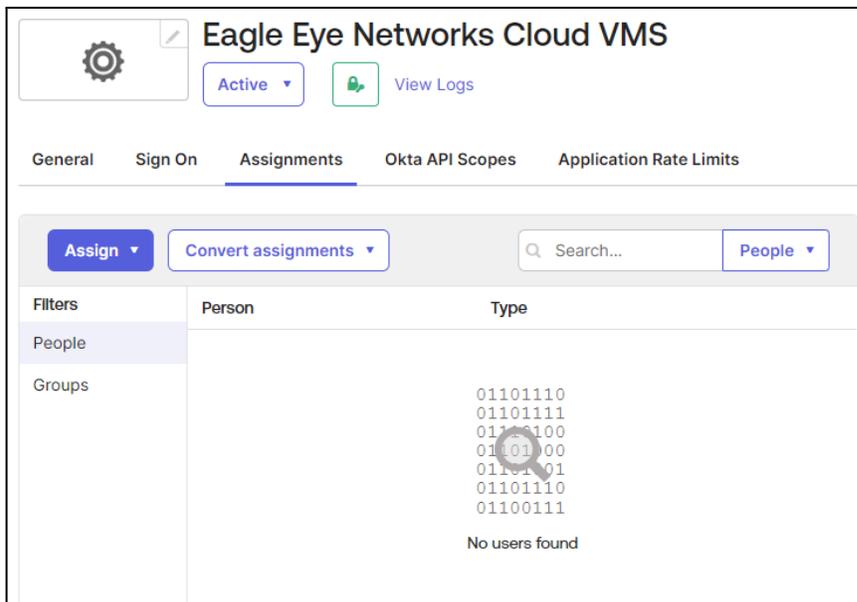
https://auth.eagleeyenetworks.com/login/oauth2/code/okta-dev-9 [×](#)

[+ Add URI](#)

- The Application Integration Information appears on the next screen. The **Client ID** and **Client Secret** information needed for configuring the Cloud VMS are found here.



- On the **Assignments** tab, choose the people who can use this login option for the Cloud VMS.



- In order to use IdP-initiated login, make the following configurations on the **Application > General** tab.

Login initiated by	<input type="text" value="Either Okta or App"/>
Application visibility	<input checked="" type="checkbox"/> Display application icon to users <input type="checkbox"/> Display application icon in the Okta Mobile app
Login flow	<input checked="" type="radio"/> Redirect to app to initiate login (OIDC Compliant) <input type="radio"/> Send ID Token directly to app (Okta Simplified)
Initiate login URI	<input type="text" value="https://auth.eagleeyenetworks.com/sso?issuer=okta-d"/>

In the **Initiate Login URL** box, enter:

https://auth.eagleeyenetworks.com/sso?issuer={registrationId}&target_link_uri={webapp_url}

The registrationId is your Eagle Eye account ID. Your login URL will be:

https://auth.eagleeyenetworks.com/sso?issuer=00000011&target_link_uri=https%3A//webapp.eagleeyenetworks.com

Configuring SP-initiated SSO settings for Okta

Note: Okta does not have a login link in the Cloud VMS.

The Okta settings are shown below:

Identity provider integration via Single Sign-on

Select and configure the Identity Provider you want to enable.

- None
- Microsoft >
- Okta v

Client ID

Client secret

Issuer URL

Login only via Single Sign-On ⓘ

Add new users if they do not already exist.

- Google >
- Custom SSO >

Update the Client ID and Client Secret with the values from the Okta application created. For the Issuer URL, you can use the actual Okta domain **https://<your-okta-domain>**. (Do not include "/" at the end.).

SP initiated SSO flow

Log in to the application,

1. Provide a non-administrator user account at the identifier first page.
2. Log in with Okta and provide consent.

IdP initiated SSO flow

1. Go to **https://<your-okta-domain>/app/UserHome**.
2. Log in with a user who exists in your Eagle Eye Networks account with the same email.
3. Click the Application you created to be redirected to the application.

Configuring automated user provisioning for Okta

1. Check the **Add new users if they do not already exist** box in the **Identity Provider Integration via Single Sign-on** screen in the Cloud VMS.

Identity provider integration via Single Sign-on

Select and configure the Identity Provider you want to enable.

None

Microsoft >

Okta v

Client ID: 0oagxinsmj8UjQ8kR5d7

Client secret: POZhSj6SJtcWk7oBmU9DnQNqvi5JYWp92rhu30vgx6nB0QxSBg

Issuer URL: https://dev-43299350.okta.com

Login only via Single Sign-On ⓘ

Add new users if they do not already exist.

Google >

Custom SSO >

2. Log in to the application. Go to **https://<your-okta-domain>/app/UserHome**.
3. Log in with a user who does not exist in your Eagle Eye account with the same email.
4. Click the Application you created and you will be redirected to the application and auto-provisioned.

Configuring Azure Active Directory as the IdP

Configuring a new applications in Azure AD

1. Log in to the Azure console (<https://portal.azure.com/#home>) and navigate to **Manage Microsoft Entra ID** (previously known as Azure ID).
2. Go to **App Registrations** in the left panel and create a new registration.
3. Provide the following information under the **Register an Application** wizard:
 - a. Name the application.

* Name

The user-facing display name for this application (this can be changed later).

- b. Set the Supported Account Type to **Accounts in this Organizational Directory Only**.

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (Faraz Co. only - Single tenant)

- c. Use the redirectURI as obtained in Prerequisites.

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional, but a value is required for most authentication scenarios.

Web

4. On the **Application Overview** screen, create a client credential using the **Add a Certificate or Secret** option.

Client credentials : [Add a certificate or secret](#)

5. Click **New Client Secret**.

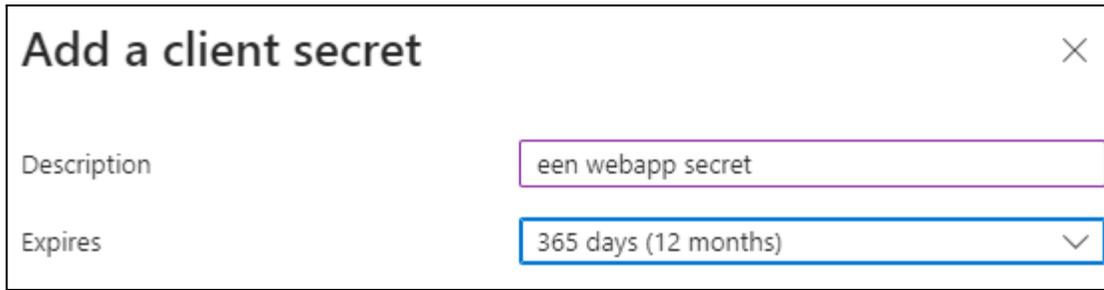
Application registration certificates, secrets, and keys

Certificates (0) Client secrets (0)

A secret string that the application uses

+ New client secret

6. Enter a description of the secret and an expiration date.



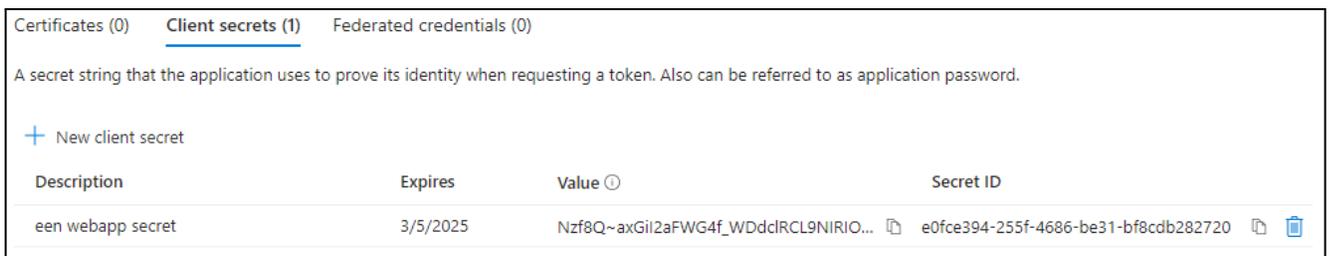
Add a client secret [X]

Description: een webapp secret

Expires: 365 days (12 months) [v]

7. Copy the Value field to a text file and save it.

IMPORTANT: This is the Client Secret cannot be retrieved again after leaving the screen.



Certificates (0) Client secrets (1) Federated credentials (0)

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

+ New client secret

Description	Expires	Value ⓘ	Secret ID
een webapp secret	3/5/2025	Nzf8Q~axGil2aFWG4f_WDdclRCL9NIRIO...	e0fce394-255f-4686-be31-bf8cdb282720

You can find the **Application (Client) ID** on this screen as well.

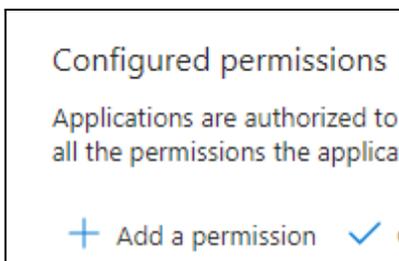


^ Essentials

Display name : [EEN Web app](#)

Application (client) ID : 4cd10839-5c28-41cb-8b6c-c0cfc3fd9ed8

8. Navigate to the API Permissions on the left panel and select **Add a Permission**.

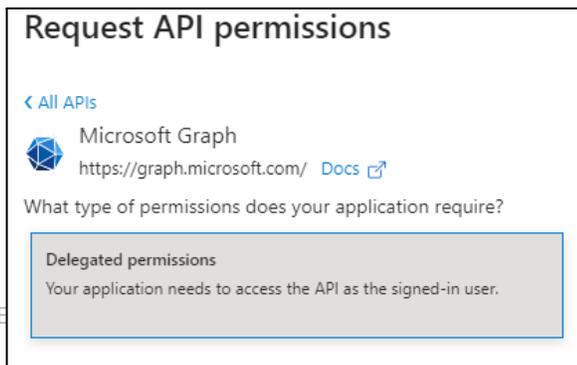


Configured permissions

Applications are authorized to all the permissions the applica

+ Add a permission ✓

9. Select the Microsoft Graph API.



Request API permissions

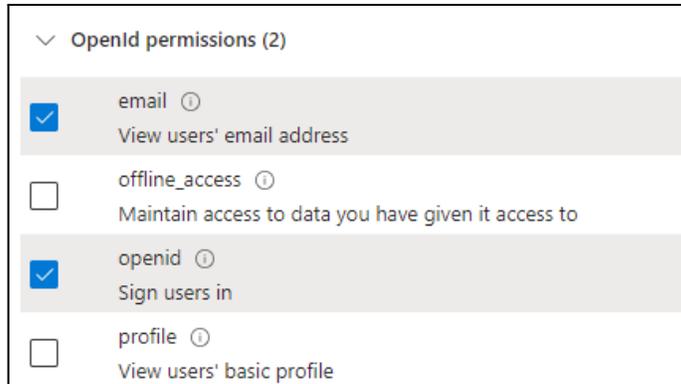
< All APIs

Microsoft Graph
<https://graph.microsoft.com/> Docs

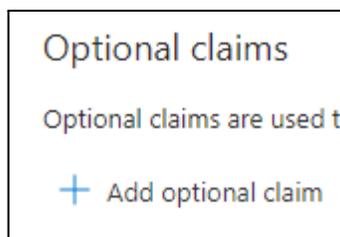
What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

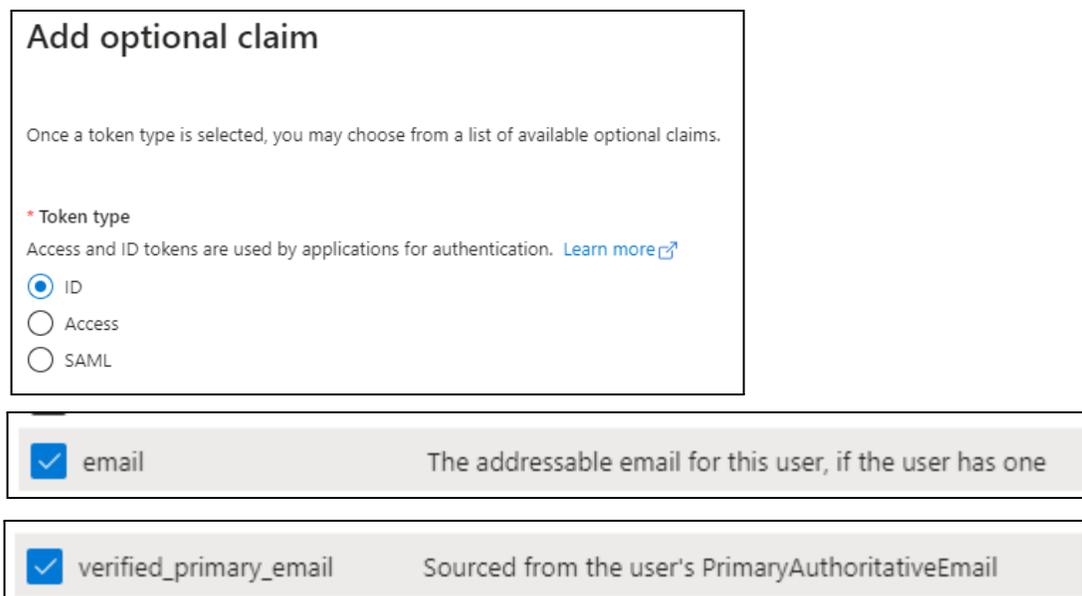
10. Add **Email** and **OpenId** permissions.



11. Navigate to **Token Configuration** from the left panel and click **Add Optional Claim**.



12. In the **Add Optional Claim** wizard, select **Adding verified_primary_email is optional**.



13. (Optional) Update the consent page using the **Branding & Properties** tab in the left panel.

14. Assign users to the application. Navigate to **Home > Manage Microsoft Entra ID > Enterprise Applications** and select your application. Go to **Assign Users and Groups** and assign users as shown below to the application.



1. Assign users and groups
Provide specific users and groups access to the applications
[Assign users and groups](#)

Add Assignment

Faraz Co.

 Groups are not available for assignment to the application.

Users

None Selected

Configuring SP-initiated SSO settings for Azure Active Directory

Use the instructions in this section to configure the organizational Microsoft SSO.

Identity provider integration via Single Sign-on

Select and configure the Identity Provider you want to enable.

None

 Microsoft v

Account type: v

Client ID:

Client secret:

Tenant ID:

Login only via Single Sign-On ⓘ

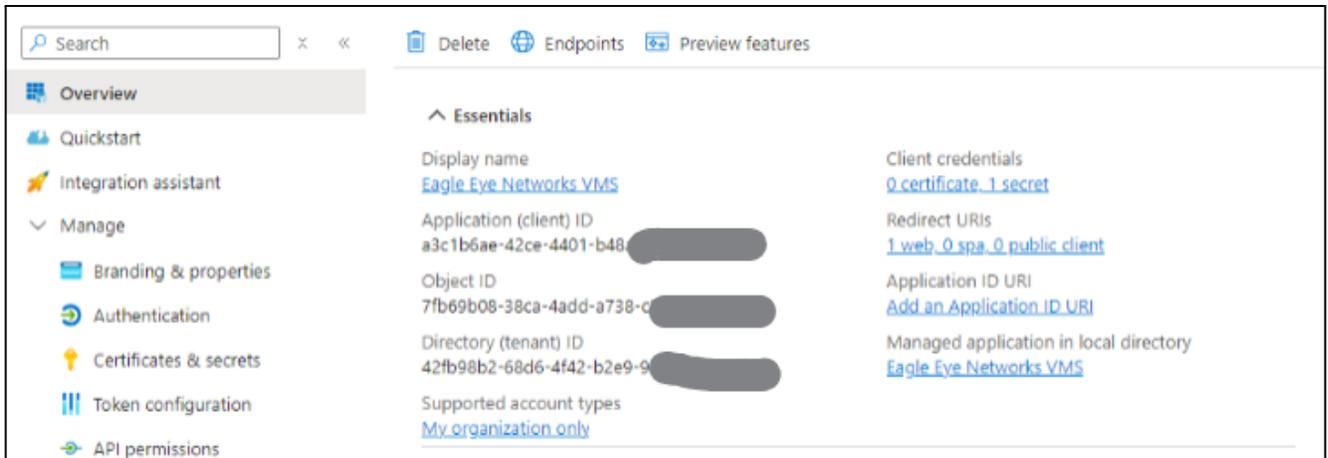
Add new users if they do not already exist.

 Okta >

 Google >

Custom SSO >

1. Update the **Client ID** (Application (client) ID) and **Client Secret** with values you got from the Azure AD application created in Prerequisites.



2. Enter the <tenant-id> found on the **Overview** page.

SP-initiated SSO flow

You should now be able to login to the application.

1. Provide a non-administrator user account at the identifier home page.
2. Log in with Azure AD and provide the consent.

Note: Be sure you have the same user created on the Azure AD side.

IdP-initiated SSO flow:

1. Update the homepage URL in the **Branding & Properties** section of the application as follows:

Home page URL ⓘ

https://auth.<domain-branding>/sso?issuer=<registration-id>&target_link_uri=<webapp-url>.

Example:

https://auth.eagleeyenetworks.com/sso?issuer=00032511&target_link_uri=https://webapp.eagleeyenetworks.com

2. Navigate to the **Enterprise Application** tab and select your application. In the left panel select **Manage > Properties**. Set **Visible to Users** to **Yes**.

Visible to users? ⓘ Yes No

Setting up IdP-initiated SSO flow:

1. Go to <https://myapplications.microsoft.com?tenantId=<tenant-id>>.
2. Login with a user who exists in your Eagle Eye Networks account with the same email.
3. Click the Application you created and you will be redirected to the application.

Configuring auto user provisioning for Azure AD

1. Check the **Add new users if they do not already exist** checkbox in the Identity Provider Integration via Single Sign-on screen in the Cloud VMS interface and click **Save**.

Identity provider integration via Single Sign-on

Select and configure the Identity Provider you want to enable.

None

Microsoft

Account type: Organization

Client ID: a3c1b6ae-42ce-4401-b48a-5[REDACTED]

Client secret: ehY8Q~iuV3ITAZ7W_RTPWROq3LW[REDACTED]

Tenant ID: 42fb98b2-68d6-4f42-b2e9-98[REDACTED]

Login only via Single Sign-On

Add new users if they do not already exist.

Okta

Google

Custom SSO

IdP-initiated SSO with auto user provisioning flow:

1. Login to the application. Go to <https://myapplications.microsoft.com?tenantId=<tenant-id>>.
2. Login with a user who exists in your Eagle Eye Networks account with the same email.
3. Click the Application you created and you will be redirected to the application.

Troubleshooting

Various error messages may appear when setting up SSO. This section provides an overview of the most common ones and suggests solutions. If you encounter any new errors, please report them to api_support@een.com so we can add them to this document for reference.

Known errors:

1. Microsoft Error: There is a different configured IDP for this user, the user can only be authenticated by configured IDP.

There is a different configured IDP for this user, the user can only be authenticated by configured IDP.

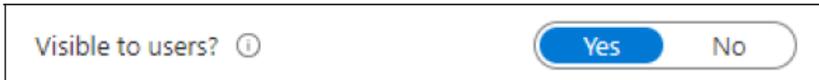
Solution: Users are trying to use the **Continue with Microsoft** button while they should login via <https://myapplications.microsoft.com>. This button is only for personal accounts.



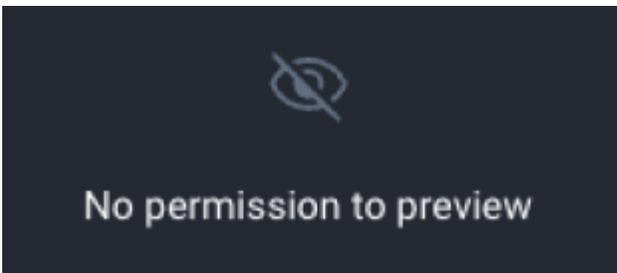
2. Microsoft Error: Newly created app does not show on my application page:

Solutions:

- a. Ensure the user is added to the enterprise application.
- b. Ensure the application is visible:

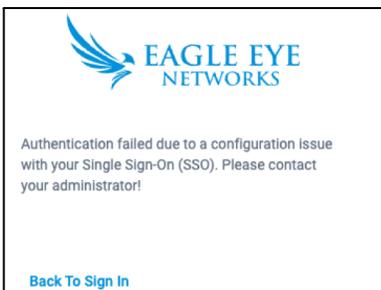


3. Microsoft Error: Newly created users see : "No permissions to preview"



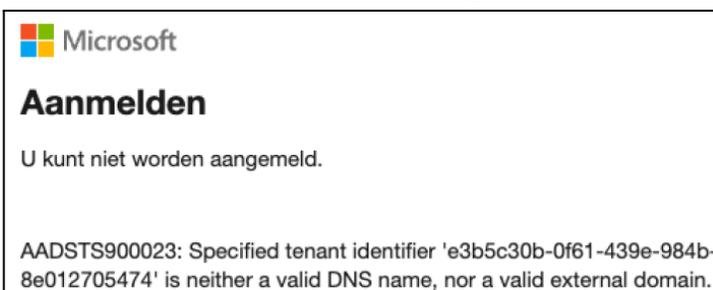
Solution: New users do not have any default permissions added. These must be granted by the admin from within the Cloud VMS.

4. Microsoft Error: Authentication failed due to a configuration issue with your Single Sign-On (SSO). Please contact your administrator!



Solution: Verify the Client ID and the Client Secret entered the Cloud VMS.

5. Microsoft Error: Unable to login, tenant identifier is invalid:



Solution: Verify the Tenant ID is entered correctly with a valid id.

6. Microsoft Error: The email ID received from the Identity Provider (IDP) is invalid:



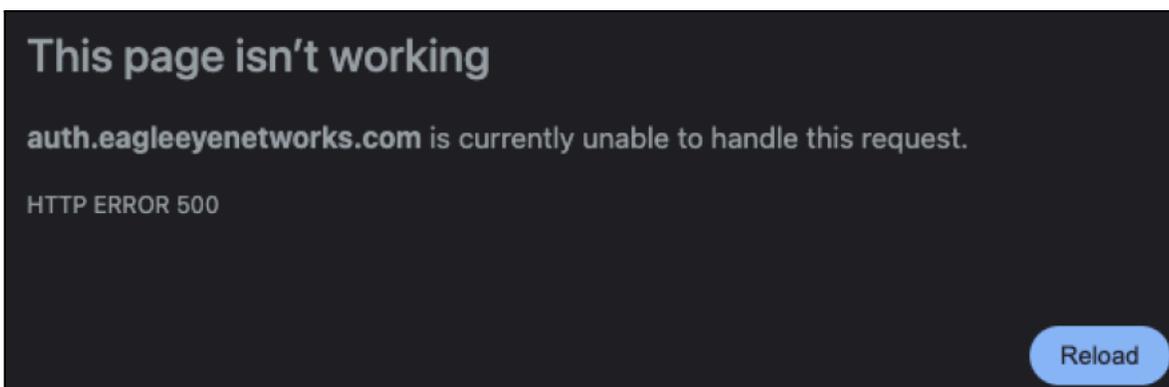
Solution: Configure the user with a valid email address on the Azure portal.

7. Microsoft Error: Illegal operation detected! Wrong registrationId:



Solution: The user trying to sign in is already added under a different Cloud VMS account. Create a separate account, or remove the old one in order to login.

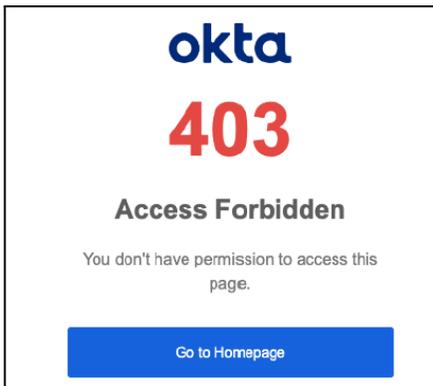
8. Microsoft Error: HTTP ERROR 500:



Solution: Verify the redirectURI this should be looking like this where the issues = account id and the target_link_uri = webapp.eagleeyenetworks.com or <branding>.webapp.eagleeyenetworks.com : https://auth.eagleeyenetworks.com/sso?issuer=00032511&target_link_uri=https%3A//web

app.eagleeyenetworks.com

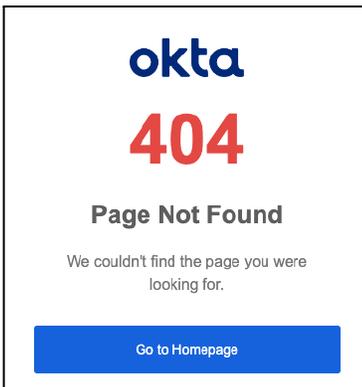
9. Okta Error: 403 Access forbidden



Solution: Verify the following settings are correct in the Cloud VMS:

- a. Okta is the selected Identity Provider
- b. Client ID
- c. Client Secret
- d. Issuer URL (example Okta url: <https://<subdomain>.okta.com>)

10. Okta Error : 404 Page not found:



Solution: Verify the issuer URL is correct:

- a. <https://trial-7462771.okta.com/> < correct one (example)
- b. <https://trial-7462771-admin.okta.com/> < wrong one (example)
^ This is a link to the Okta admin panel instead of the Okta user dashboard.

11. Unable to authenticate the user:

Solution: Check the redirect uri.

- a. Redirect uri is wrong:

https://auth.eagleeyenetworks.com/sso?issuer=00170929&target_link_uri=webapp.eagleeyenetworks.com

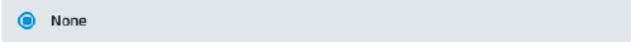
Instead of:

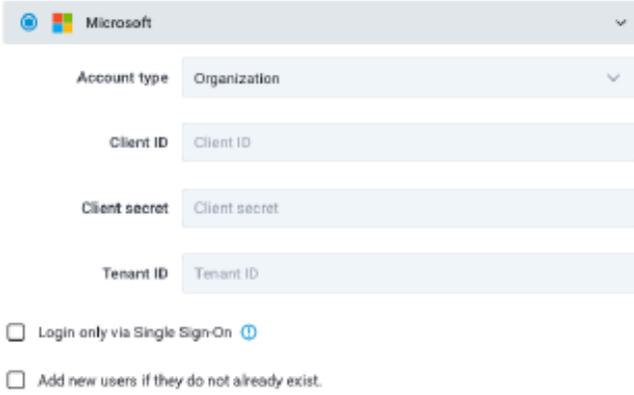
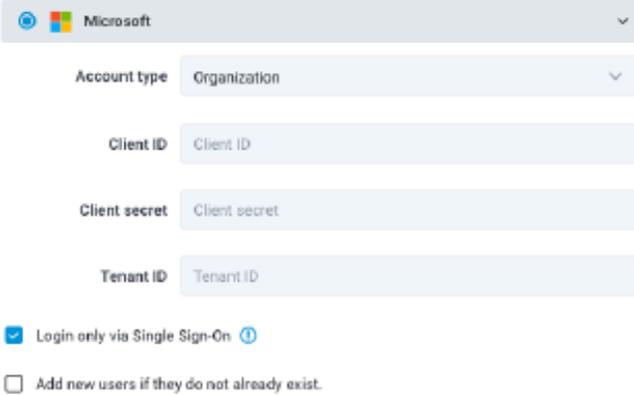
https://auth.eagleeyenetworks.com/sso?issuer=00170929&target_link_uri=https%3A//webapp.eagleeyenetworks.com

- b. Make sure the target link is formatted correctly with `https%3A//` instead of `https://`

Troubleshooting: SSO Configurations

This overview shows all possible SSO configurations and the available options that accompany them:

SSO Configuration	Available options
 <p>A screenshot of a configuration interface showing a single option labeled "None" with a blue radio button selected.</p>	<p>No SSO selected</p> <ul style="list-style-type: none"> • Login via Username and password <input checked="" type="checkbox"/> • SSO login by entering Email ID <input type="checkbox"/> • Login via Microsoft button <input checked="" type="checkbox"/> • Login via Google button <input checked="" type="checkbox"/> • Login via IDP-initiated flow <input type="checkbox"/> • SSO user provisioning <input type="checkbox"/>
 <p>A screenshot of a configuration interface showing "Microsoft" selected in a dropdown menu. Below it, "Account type" is set to "Personal". There is also a checkbox for "Login only via Single Sign-On" which is currently unchecked.</p>	<p>Microsoft, Personal</p> <ul style="list-style-type: none"> • Login via Username and password <input checked="" type="checkbox"/> • SSO login by entering Email ID <input type="checkbox"/> • Login via Microsoft button <input checked="" type="checkbox"/> • Login via Google button <input type="checkbox"/> • Login via IDP-initiated flow <input type="checkbox"/> • SSO user provisioning <input type="checkbox"/>

	<p>Microsoft, Personal, only SSO</p> <ul style="list-style-type: none"> • Login via username and password ❌ • SSO login by entering Email ID ✔️ • Login via Microsoft button ✔️ • Login via Google button ❌ • Login via IDP-initiated flow ❌ • SSO user provisioning ❌
	<p>Microsoft, Organization</p> <ul style="list-style-type: none"> • Login via username and password ✔️ • SSO login by entering Email ID ❌ • Login via Microsoft button ❌ • Login via Google button ❌ • Login via IDP-initiated flow ✔️ • SSO user provisioning ❌
	<p>Microsoft, Organization, SSO Only</p> <ul style="list-style-type: none"> • Login via username and password ❌ • SSO login by entering Email ID ✔️ • Login via Microsoft button ❌ • Login via Google button ❌ • Login via IDP-initiated flow ✔️ • SSO user provisioning ❌