

# Eagle Eye Application Note - AN022

## Configuring SSO in the Eagle Eye Cloud VMS Enhanced Web Interface

2024-06-20 Revision 1.0

### Target Audience

This application note is intended for users of the Eagle Eye Cloud VMS, and specifically those using the Enhanced Web Interface, that want to utilize the convenience and security offered by single sign-on (SSO) through common or custom Identity Providers (IdPs). Resellers can also configure SSO for all their end users of the VMS. Users of all Editions of the VMS can log in using Microsoft or Google as an IdP, but Standard Edition users can only log in via the following domains:

- msn.com
- live.com
- hotmail.com
- outlook.com
- gmail.com
- een.com

Professional and Enterprise Edition users can log in via the IdP buttons even if SSO is not configured. Administrators will always be able to log in directly.

### Introduction

Eagle Eye Networks allows users to log in using single sign-on via an identity provider that supports OIDC. This application note provides instructions for setting up IdPs for SSO with the Eagle Eye Cloud VMS for the three most common IdPs for SSO: Microsoft Azure Active Directory, Okta, and Google Cloud Platform. This application note also includes instructions for setting up Custom SSO. Resellers can set up SSO for all end users of the Cloud VMS as well. Note: Both the Classic Interface and the Standard Edition with SAML can be set up and can operate simultaneously.

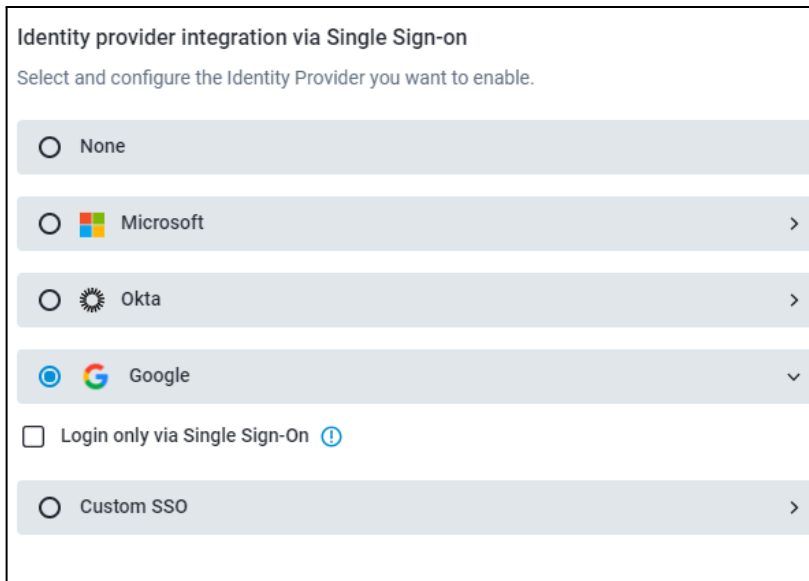
### Prerequisites

Before setting up SSO, you will need administrator privileges within the Eagle Eye Cloud VMS.

# 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.

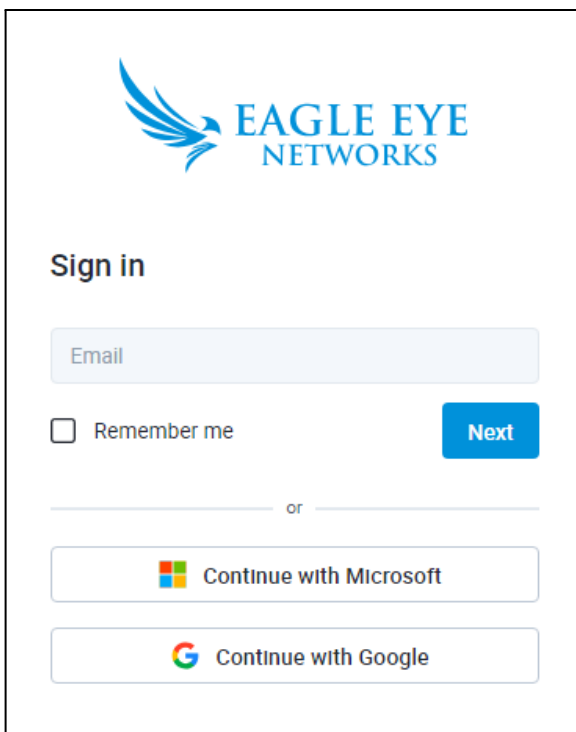



Identity provider integration via Single Sign-on

Select and configure the Identity Provider you want to enable.

- None
-  Microsoft >
-  Okta >
-  Google v
- Login only via Single Sign-On ⓘ
- Custom SSO >

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.





Sign in

Email

Remember me

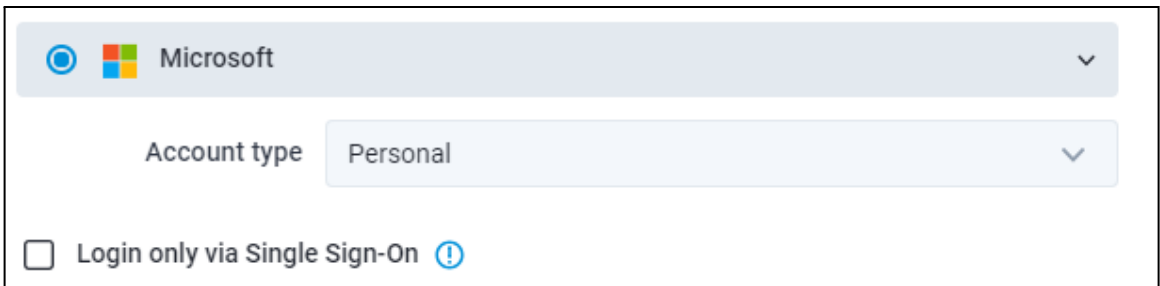
\_\_\_\_\_ or \_\_\_\_\_

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 Google IdP for authentication. Additionally, users can log in using the **Continue with Google** button in the login interface.

## Configuring Microsoft IdP via SSO

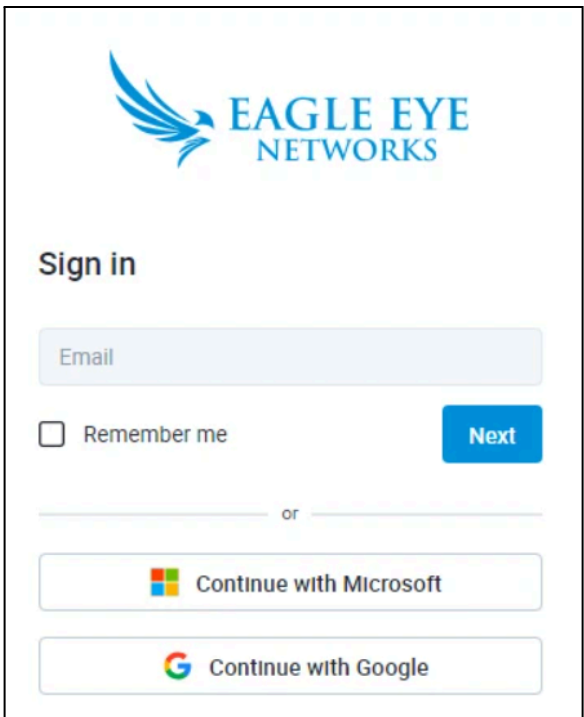
Follow the steps in this section to configure Microsoft SSO authentication in the Cloud VMS enhanced web interface.

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 left 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 "Next" button. Below the "Next" button is a horizontal line with "or" in the center. Below the line are two buttons: "Continue with Microsoft" (with the Microsoft logo) and "Continue with Google" (with the Google logo).

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

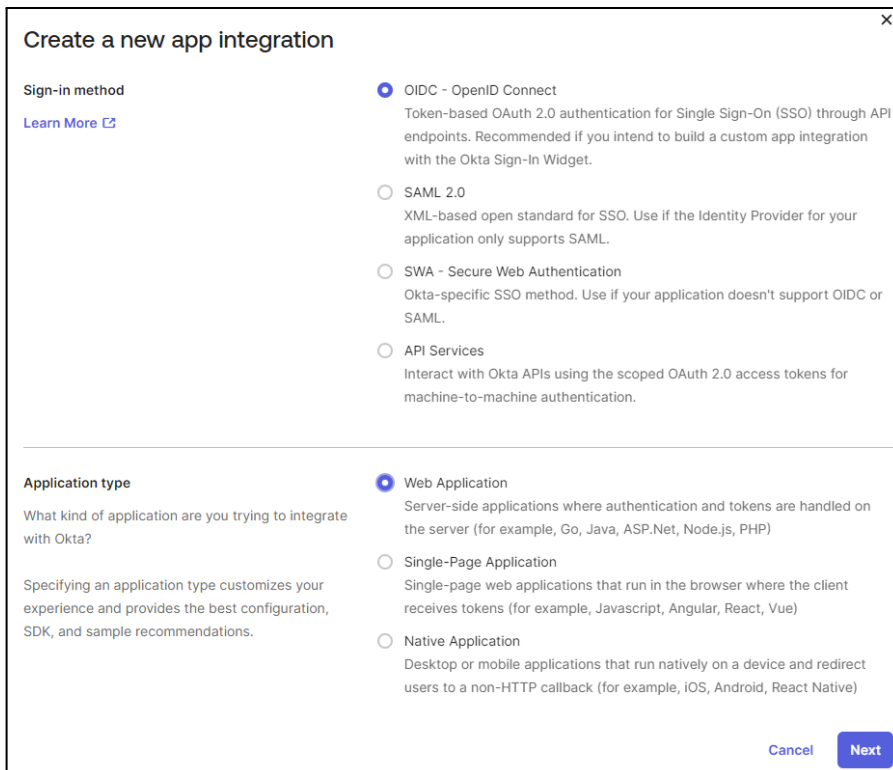
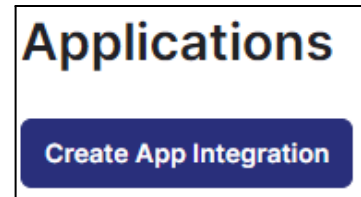
Follow the steps in this section to configure Okta SSO authentication in the Cloud VMS enhanced web interface.

### Prerequisites

- Create an account in Okta if you do not already have one.
- Obtain your Eagle Eye account ID.

### Obtaining a redirectUri 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**.



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

To get the redirect URI, call:

`{baseUrl}/api/v3.0/accounts/self/ssoAuthSettings?include=ssoOidcIidpConfigUrls`

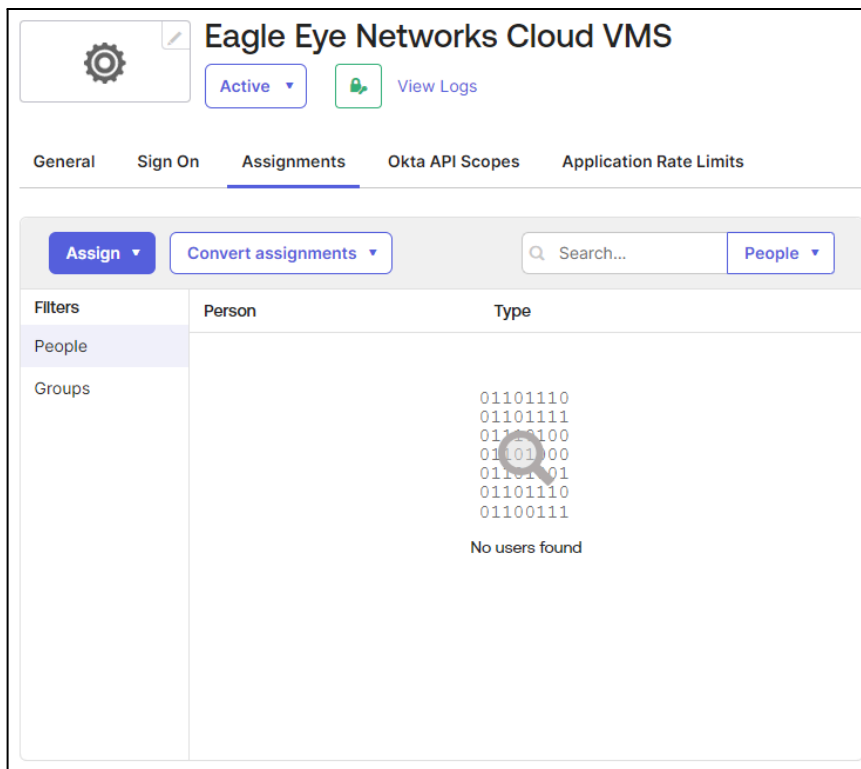
Example baseUrl: [api.c013.eagleeyenetworks.com](https://api.c013.eagleeyenetworks.com)

This call returns the redirectUri for your account.

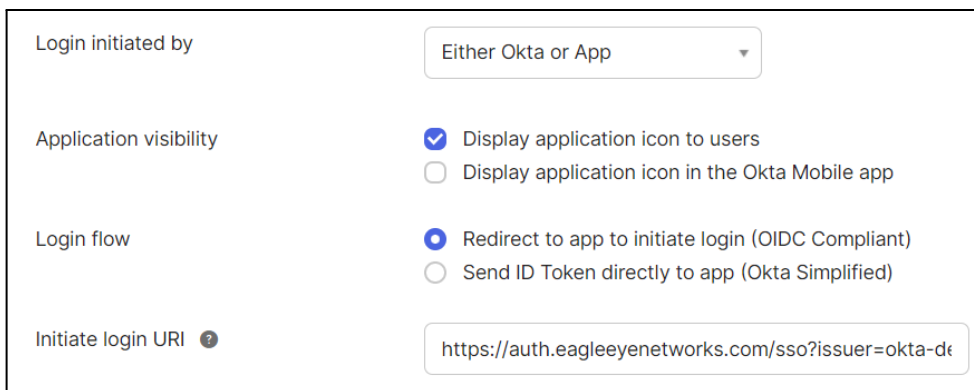
4. The Application Integration Information appears on the next screen. The **Client ID** and **Client Secret Information** needed for configuring the VMS Cloud are found here.

Creation date	Secret	Status
Jul 27, 2023	.....	Active

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



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



7. In the **Initiate Login URI** box, enter:

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

The registrationId is the last part of the redirectUri retrieved from. Get

**`{baseURL}/api/v3.0/accounts/self/ssoAuthSettings?include=ssoOidcIdpConfigUrls`**

For example, if you get

```
1 "ssoOidcIdpConfigUrls": {
2   "redirectUri": "https://auth.test.eagleeyenetworks.com/login/oauth2/code/00000011"
3 }
```

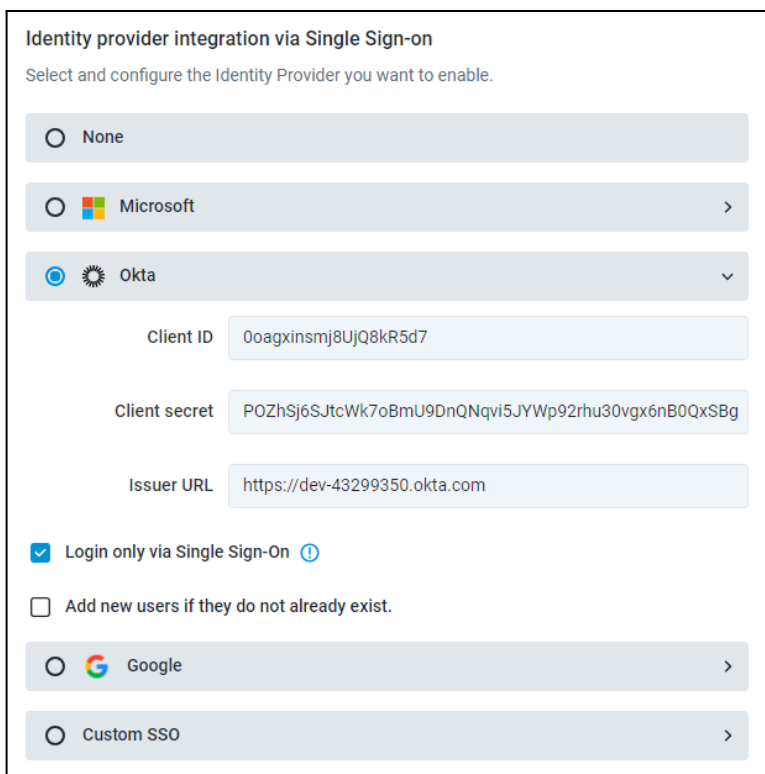
As a response, your registrationId is 00000011. The redirectionId is actually your Eagle Eye account ID. Your login URI will be:

**[https://auth.eagleeyenetworks.com/sso?issuer=00000011&target\\_link\\_uri=webapp\\_eagleeyenetworks.com](https://auth.eagleeyenetworks.com/sso?issuer=00000011&target_link_uri=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 in the prerequisites section. 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. Login 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 on 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 interface.

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 >

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

## Enabling Azure Active Directory as the IdP

If Microsoft is the IdP, use the instructions in this section to enable Azure Active Directory (AD).



## Prerequisites

1. If you do not have an account in Azure AD, register for a free account at <https://azure.microsoft.com>.
2. Obtain the redirectUri for the account by adding your account ID at the end of this redirectUri: **<https://auth.eagleeyenetworks.com/login/oauth2/code/<account ID>>**.

## 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 [Configuring Microsoft Azure OIDC](#).

Redirect URI (optional)

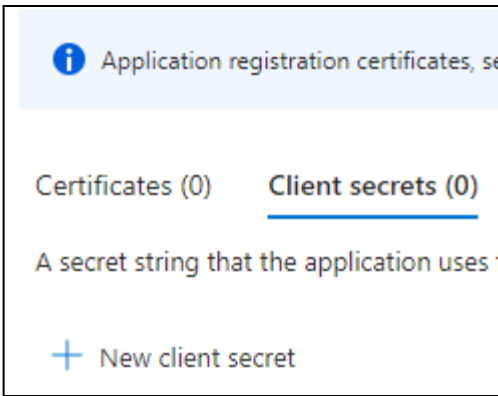
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional, but a value is required for most authentication scenarios.

Web

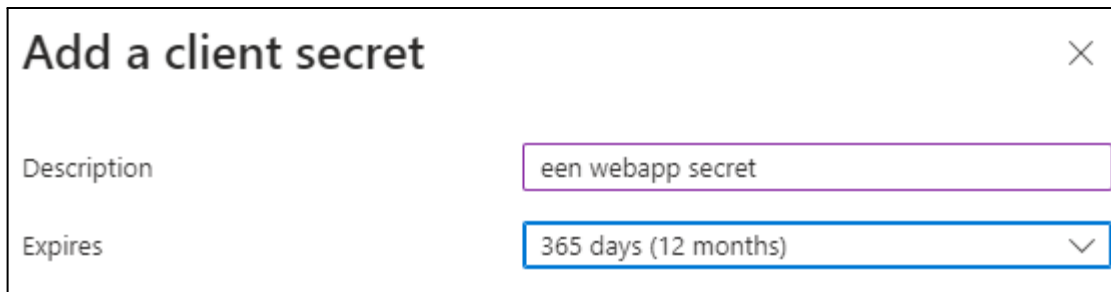
4. On the Application Overview screen, create a client credential using the **Add a Certificate or Secret** option.

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

5. Click **New Client Secret**.

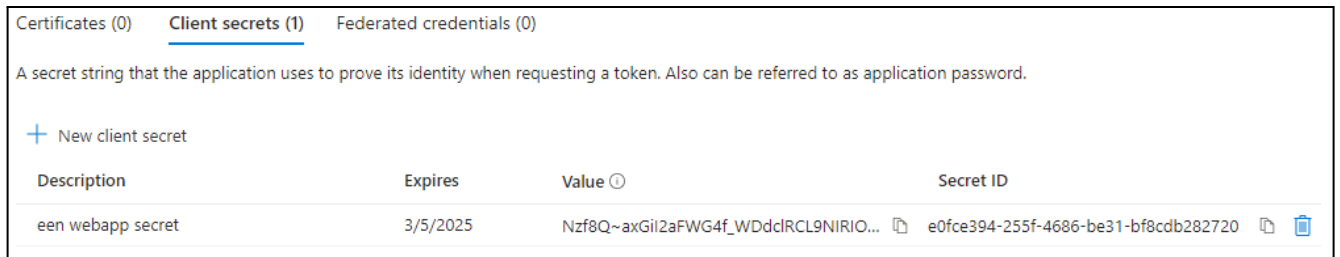


6. Enter a description of the secret and an expiration date.



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

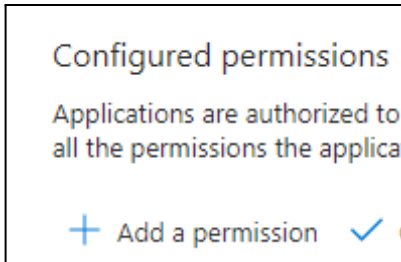
**IMPORTANT:** This is the Client Secret and cannot be viewed again.



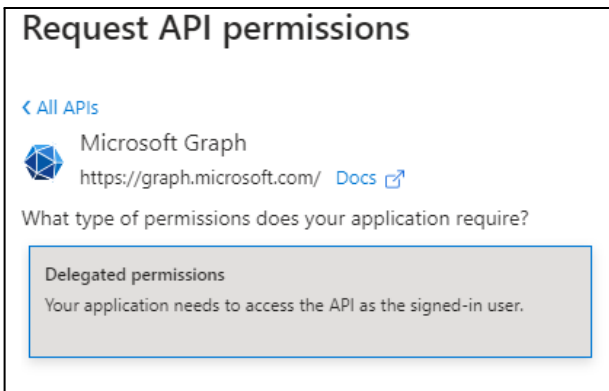
You can find the **Application (Client) ID** on this screen as well.



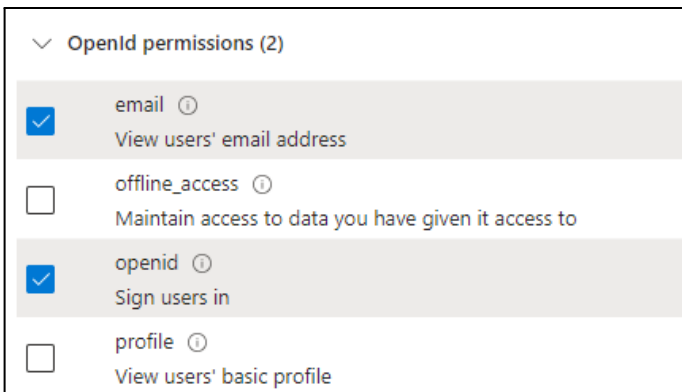
8. Navigate to the API Permissions on the left panel and select **Add a Permission**.



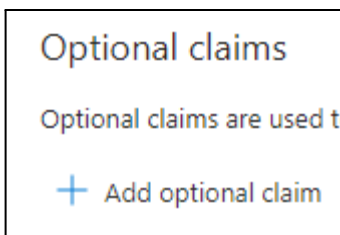
9. Select the Microsoft Graph API.



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.

### Add optional claim

Once a token type is selected, you may choose from a list of available optional claims.

\* Token type  
Access and ID tokens are used by applications for authentication. [Learn more](#)


ID  
 Access  
 SAML

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

verified\_primary\_email      Sourced from the user's PrimaryAuthoritativeEmail

13. You can also 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 assigning users 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

Account type: Organization

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

Client secret: ehY8Q~iuV3ITAZ7W\_RTPWROq3LVoC[REDACTED]

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

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.

The screenshot shows the 'Overview' page for an application named 'Eagle Eye Networks VMS'. The 'Essentials' section displays the following information:

- Display name: [Eagle Eye Networks VMS](#)
- Application (client) ID: a3c1b6ae-42ce-4401-b48[REDACTED]
- Object ID: 7fb69b08-38ca-4add-a738-c[REDACTED]
- Directory (tenant) ID: 42fb98b2-68d6-4f42-b2e9-9[REDACTED]
- Supported account types: [My organization only](#)

On the right side, under 'Client credentials', there are links for:

- [0 certificate\\_1 secret](#)
- [1 web\\_0 spa\\_0 public client](#)
- [Add an Application ID URI](#)
- [Managed application in local directory](#)
- [Eagle Eye Networks VMS](#)

2. You can find the **<tenant-id>** on the **Overview** page.

### SP-initiated SSO flow

You should now be able to log in 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.

## Prerequisites for the IdP-initiated SSO flow

1. Update the homepage URL in the **Branding & Properties** section of the application as follows:  
**https://auth.<domain-branding>/sso?issuer=<registration-id>&target\_link\_uri=<webapp-url>**.
  - **domain-branding** can be eagleeyenetworks.com, mobotixcloud.com, etc.
  - The registration-id is your account id. This Can be found at the end of redirectUri found in **Prerequisites**.
  - The **<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).

Home page URL ⓘ	https://auth.eagleeyenetworks.com/sso?issuer=00145833&target_link_uri=https%3A...
-----------------	---

- An example is:  
**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? ⓘ	<input checked="" type="radio"/> Yes	<input type="radio"/> No
---------------------	--------------------------------------	--------------------------

## Setting up IdP-initiated SSO flow

1. Go to **https://myapplications.microsoft.com?tenantId=<tenant-id>**.
2. Log in 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** box 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...

Client secret: ehY8Q~iuV3ITAZ7W\_RTPWROq3Lw...

Tenant ID: 42fb98b2-68d6-4f42-b2e9-96...

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. Log in to the application. Go to <https://myapplications.microsoft.com?tenantId=<tenant-id>>.
2. Log in 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.