Eagle Eye Application Note - AN022

Configuring SSO in the Eagle Eye Cloud VMS Enhanced Web Interface

2025-08-27 Revision 3.0

Target Audience

This guide is intended for Eagle Eye Cloud VMS users, 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 VMS editions can log in with Microsoft or Google as an IdP, but Standard Edition users are limited to 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 without SSO configured. Administrators will always have the ability to log in directly.

Contents

What is Single Sign On - SSO?

SSO (Single Sign-On) enables you to log in to multiple applications or services using a single set of login credentials. Instead of needing a separate username and password for each service, SSO allows you to use a single identity to access all services. 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.
- You use the same account you have for Gmail or Outlook, for example, to log in to other apps that support SSO.
- It's mainly used for individual services, personal accounts, or smaller setups, where using a Google or Microsoft login adds convenience.

Corporate SSO (Okta/Azure):

- **Corporate SSO** solutions, such as Okta or Microsoft Azure Active Directory (Azure AD), are designed specifically for businesses.
- They enable companies to manage employee logins to various internal systems, apps, and cloud services from a single, centralized location.
- Okta and Azure AD offer more control, security, and integration options. Companies can enforce policies like multi-factor authentication (MFA) and easily manage who has access to which services.
- These systems are designed for large organizations where security, compliance, and scalability are crucial.

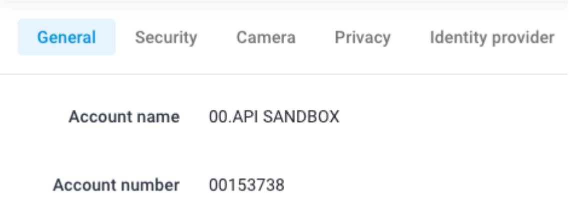
Key Differences:

- **Personal SSO** (Google/Microsoft): Great for convenience, more for individuals or small-scale users.
- **Corporate SSO** (Okta/Azure): Designed for businesses, providing higher security, access control, and scalability for large teams.

Prerequisites

Before setting up SSO, you will need the following items. Some of these items depend on the method being used, such as Google, Okta, or Microsoft.

- Administrator privileges within the Eagle Eye Cloud VMS.
- Obtain your Eagle Eye account ID (Account number) via **Admin > Account settings > General**



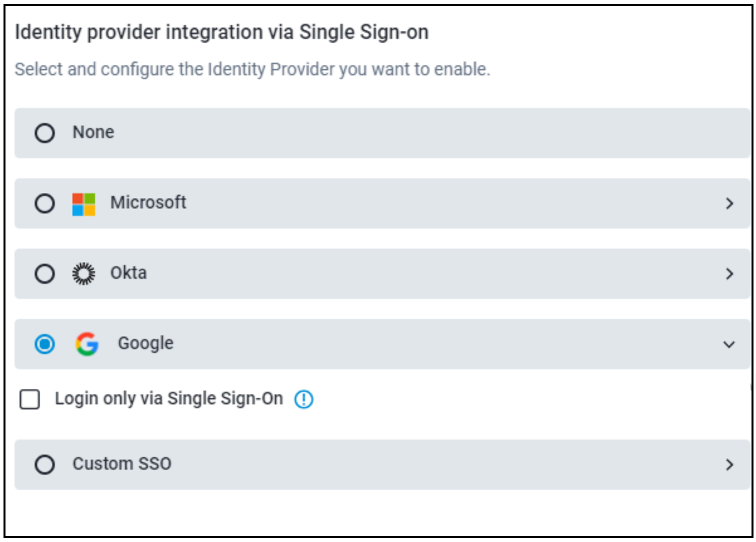
General | Security | Camera | Privacy | Identity provider

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 ensure they are URL-encoded).
- Obtain the redirectUri for the account: **https://auth.eagleeyenetworks.com/login/oauth2/code/**
- If you do not have an account in Azure AD, register for a free account at https://azure.micrsoft.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

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

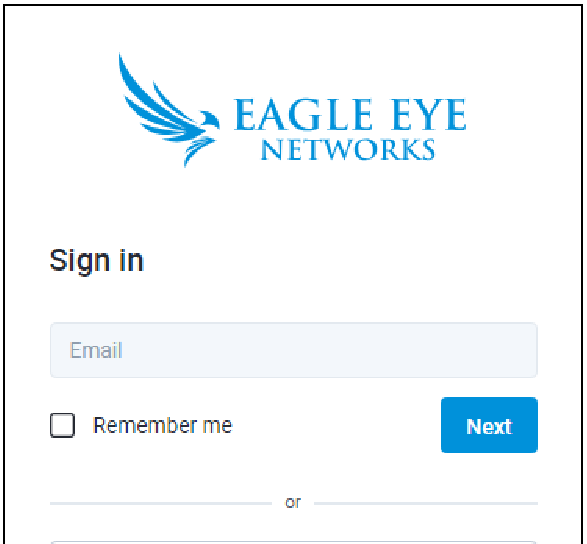
○ Microsoft ›

○ Okta ›

● Google ⌄

□ Login only via Single Sign-On ⓘ

○ Custom SSO ›



EAGLE EYE NETWORKS

Sign in

Email

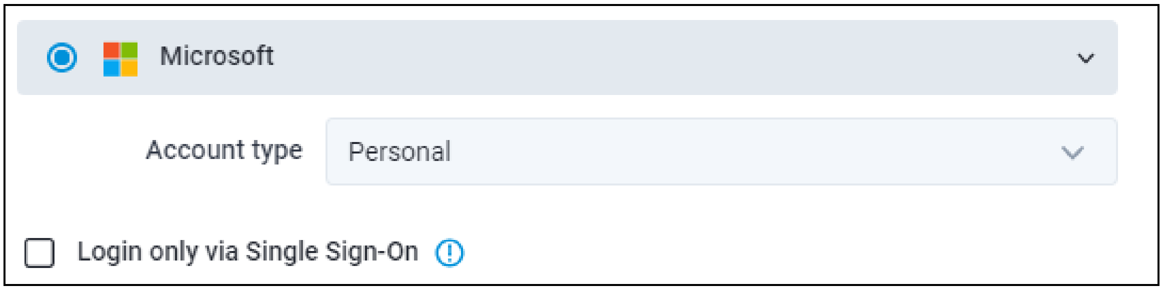
□ Remember me

2. Leave the '**Login Only via Single Sign-on'** checkbox unchecked to allow non-administrator users the option to log on with a direct password or by clicking '**Continue with Google'** to log in via SSO.

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

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

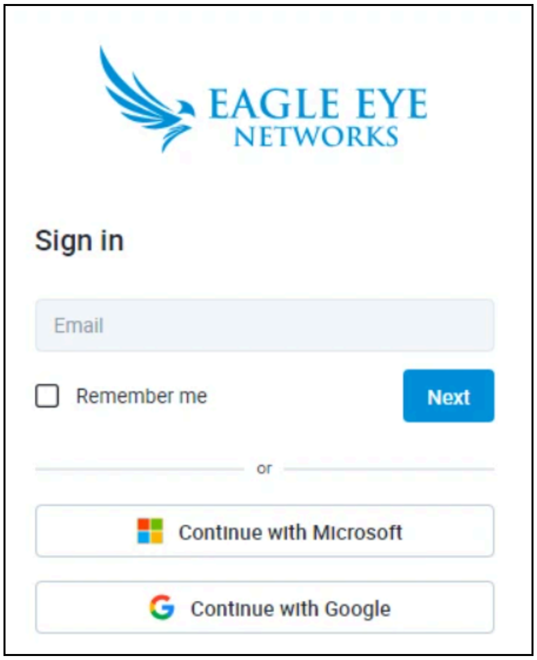


● Microsoft

Account type: Personal

☐ Login only via Single Sign-On

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.

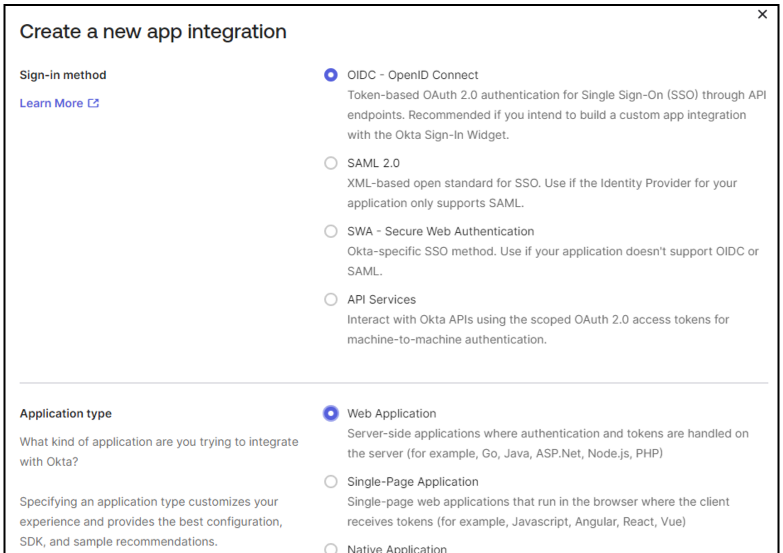


3. Check the **Login only via Single-Sign-On** box to prohibit non-administrator users from logging into the VMS with a direct password. By entering a non-administrator username and clicking Next, the user is automatically redirected to the Microsoft IdP for authentication. Additionally, users can log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

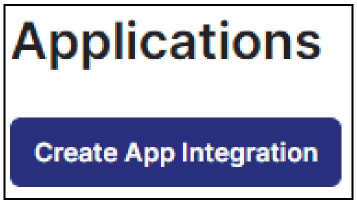
What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

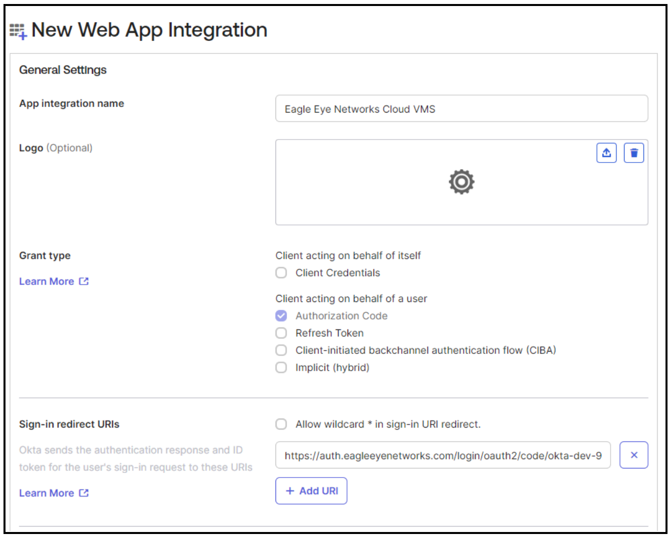
● Web Application
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)

○ 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



3. On the New **Web App Integration** screen, enter the name for your app integration and the URL for the sign-in redirect URL: **https://auth.eagleeyenetworks.com/login/oauth2/code/**



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

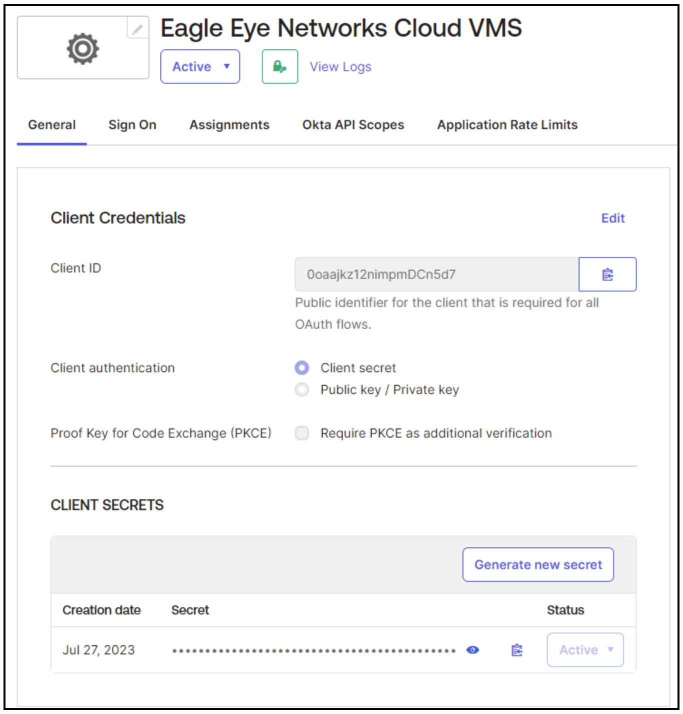
Client acting on behalf of a user
☑ Authorization Code
□ Refresh Token
□ Client-initiated backchannel authentication flow (CIBA)
□ Implicit (hybrid)

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

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



Eagle Eye Networks Cloud VMS

Client Credentials

Client ID: 0oaajkz12nimpmDCn5d7
Public identifier for the client that is required for all OAuth flows.

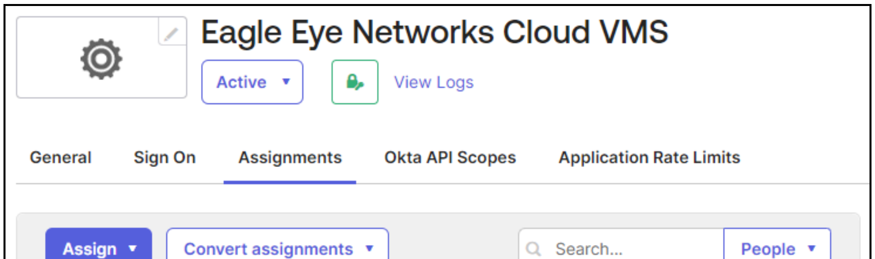
Client authentication
● Client secret
○ Public key / Private key

Proof Key for Code Exchange (PKCE)
□ Require PKCE as additional verification

CLIENT SECRETS

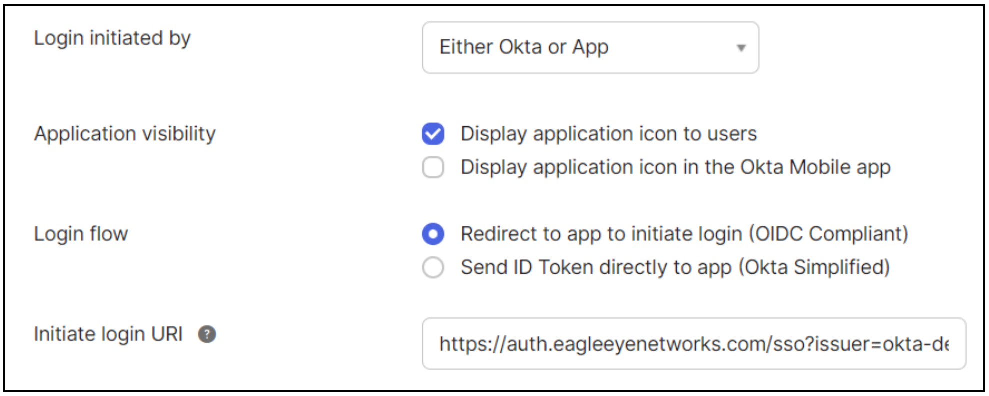
Creation date	Secret	Status
Jul 27, 2023	••	Active

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



Eagle Eye Networks Cloud VMS

6. To use IdP-initiated login, make the following configurations on the **Application > General** tab.



Login initiated by: Either Okta or App

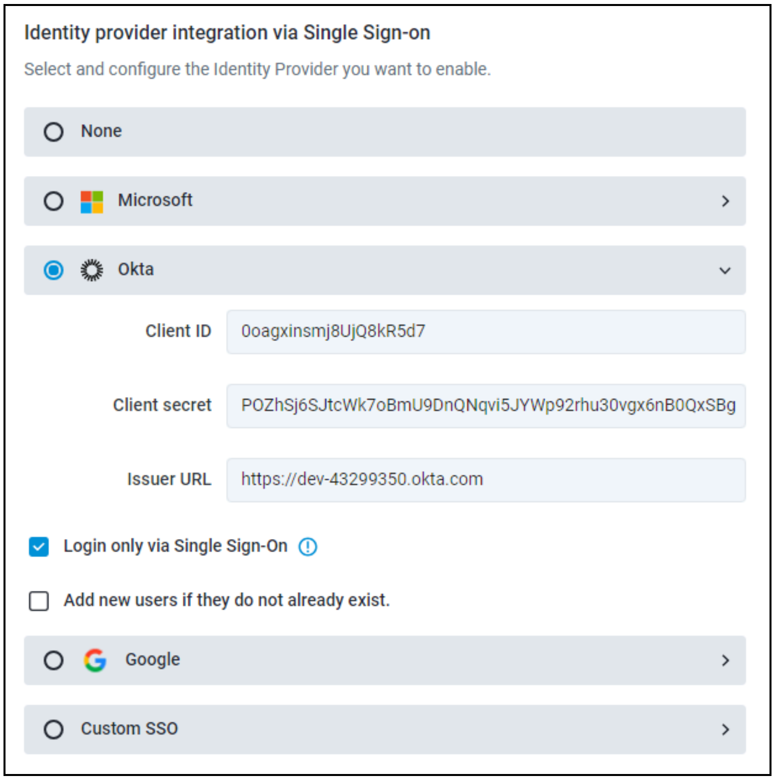
Application visibility:
- ☑ Display application icon to users
- □ Display application icon in the Okta Mobile app

Login flow:
- ● Redirect to app to initiate login (OIDC Compliant)
- ○ Send ID Token directly to app (Okta Simplified)

Initiate login URI: https://auth.eagleeyenetworks.com/sso?issuer=okta-de

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
  - 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

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 the SSO flow

Log in to the application,

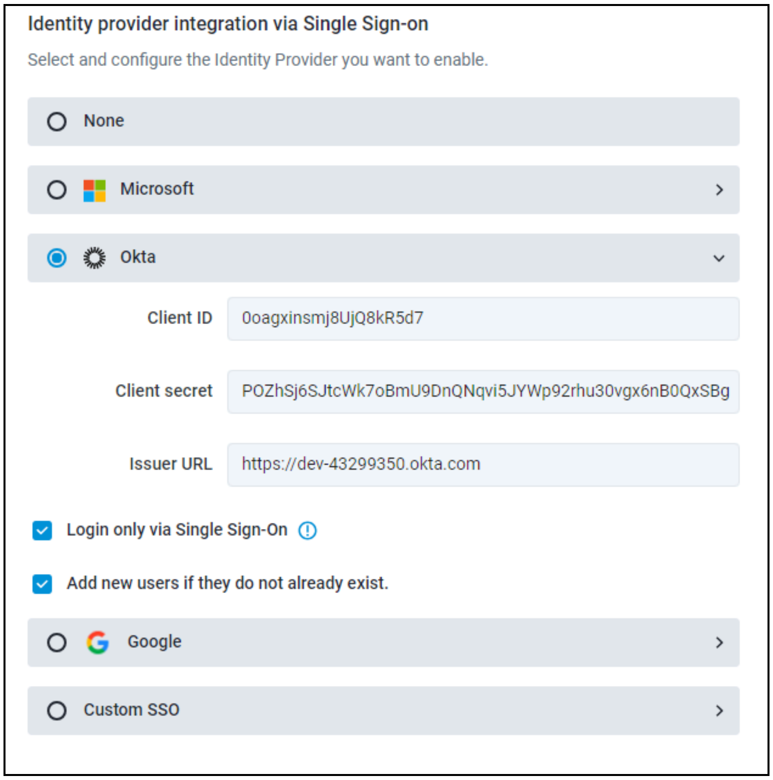
1. Provide a non-administrator user account at the identifier's first page.
2. Login with Okta and provide consent.

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 and has the same email address.
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

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

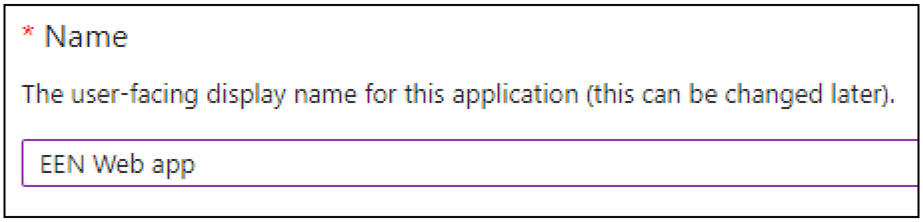
○ Custom SSO

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 EEN account using the same email address.
4. Click the Application you created, and you will be redirected to the application, where it will be auto-provisioned.

Configuring Azure Active Directory as the IdP

Configuring a new application 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.

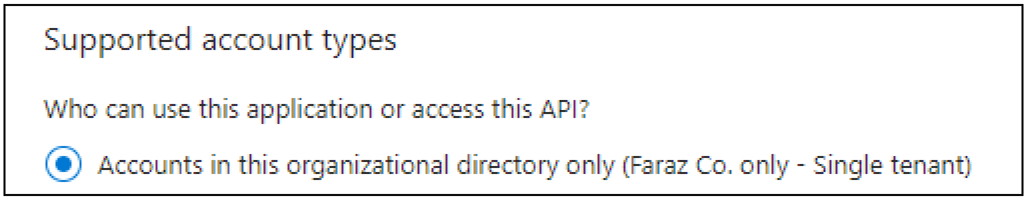


* Name

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

EEN Web app

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

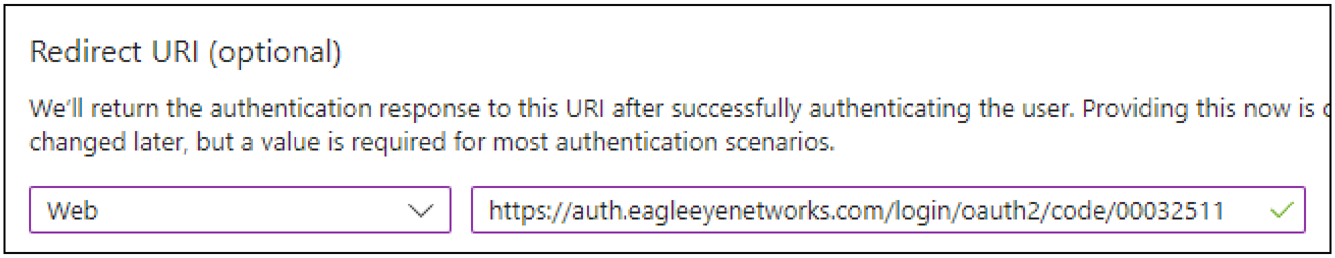


Supported account types

Who can use this application or access this API?

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

    c. Use the redirect URI as obtained in **the Prerequisites**.
    d. New installations should have a redirect url (without the accountId): **https://auth.eagleeyenetworks.com/login/oauth2/code/**



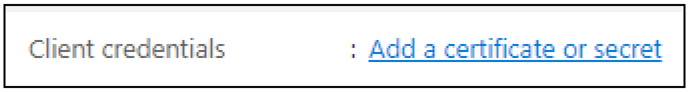
Redirect URI (optional)

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

Web

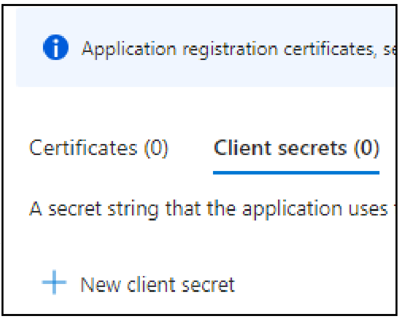
https://auth.eagleeyenetworks.com/login/oauth2/code/00032511 ✓

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

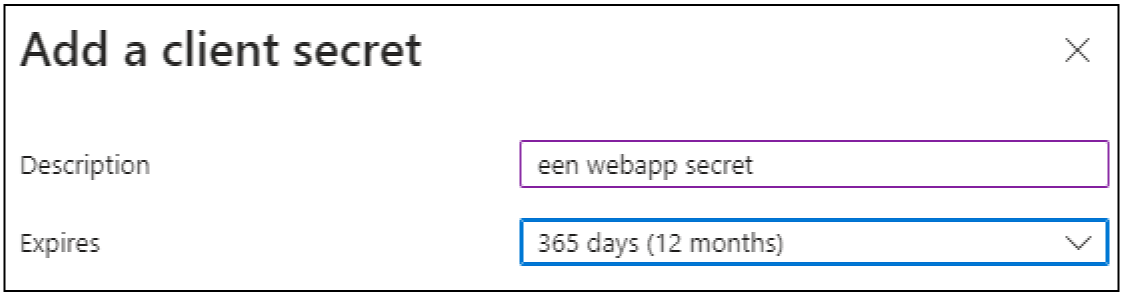
5. Click **New Client Secret**.



Application registration certificates, se

A secret string that the application uses

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



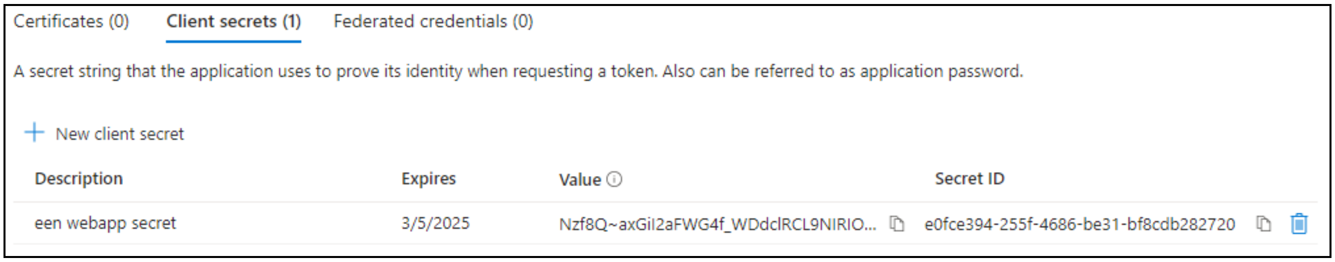
Add a client secret

Description: een webapp secret

Expires: 365 days (12 months)

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

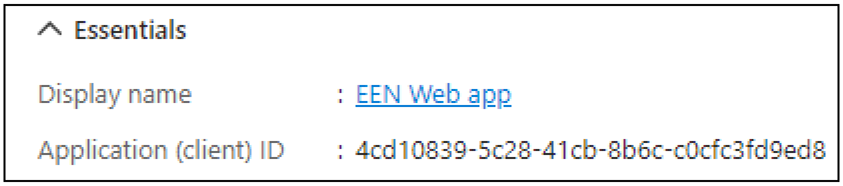
IMPORTANT: This is the **Client Secret** **<u>cannot</u>** be retrieved again after leaving the screen.



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
een webapp secret	3/5/2025	Nzf8Q~axGil2aFWG4f_WDdclRCL9NIRIO...	e0fce394-255f-4686-be31-bf8cdb282720

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

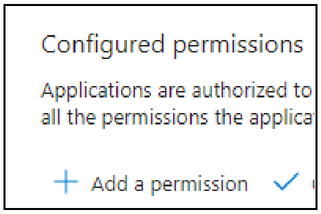


Essentials

Display name : EEN Web app

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

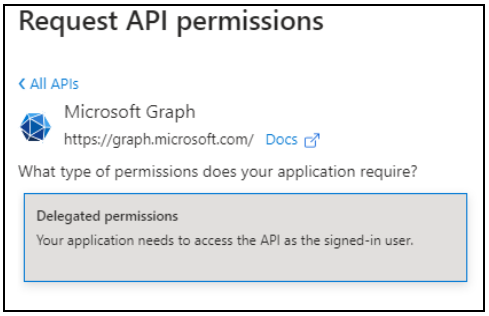
8. Navigate to the **API Permissions** on the left panel and select **Add a Permission**.



Configured permissions

Applications are authorized to all the permissions the applica

Select the **Microsoft Graph API**.



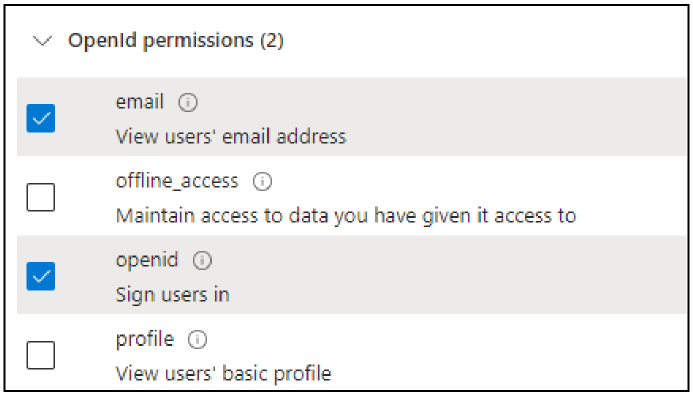
Request API permissions

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.

9. Add **Email** and **OpenID** permissions.



OpenId permissions (2)

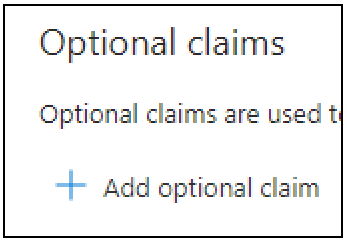
☑ email ⓘ
View users' email address

□ offline_access ⓘ
Maintain access to data you have given it access to

☑ openid ⓘ
Sign users in

□ profile ⓘ
View users' basic profile

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

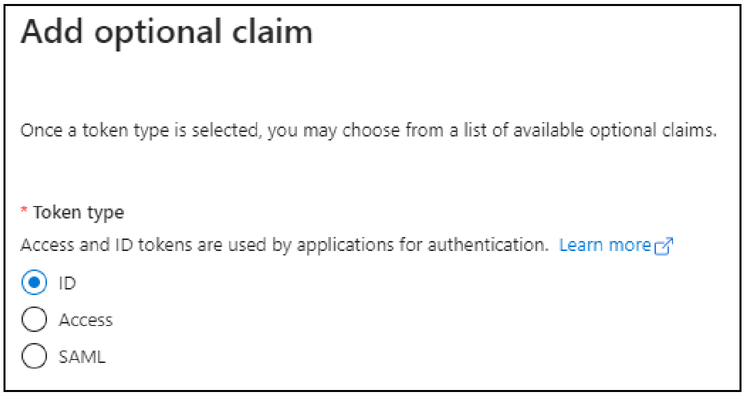


Optional claims

Optional claims are used t

+ Add optional claim

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

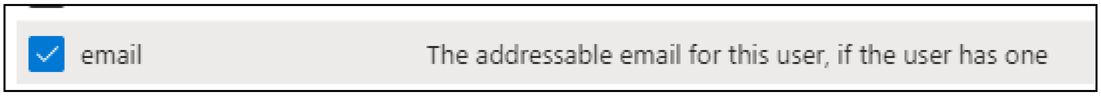


Add optional claim

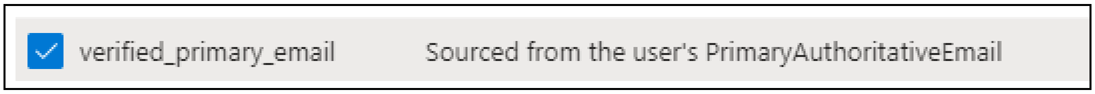
Once a token type is selected, you may choose from a list of available optional claims.

* Token type
Access and ID tokens are used by applications for authentication. Learn more

● ID
○ Access
○ SAML



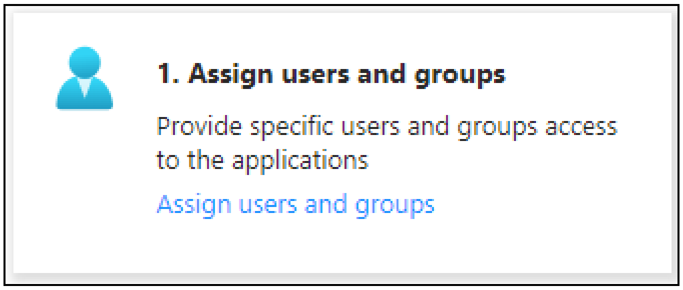
☑ email The addressable email for this user, if the user has one



☑ verified_primary_email Sourced from the user's PrimaryAuthoritativeEmail

12. You can also update the consent page using the **"Branding & Properties"** tab in the left panel.

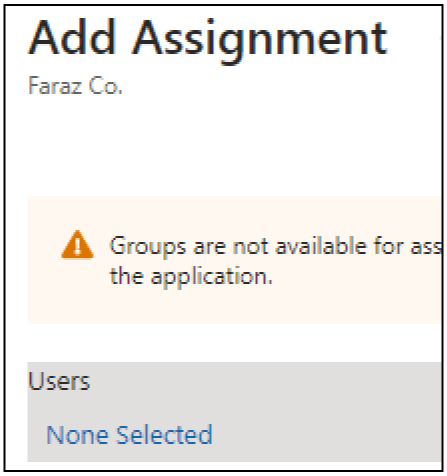
13. Assign users to the application. Navigate to **”Home > Manage Microsoft Entra ID > Enterprise Applications”** and select your application. Go to **"Assign Users and Groups"** and assign users as shown below to the application.



1. Assign users and groups

Provide specific users and groups access to the applications

Assign users and groups



Add Assignment

Faraz Co.

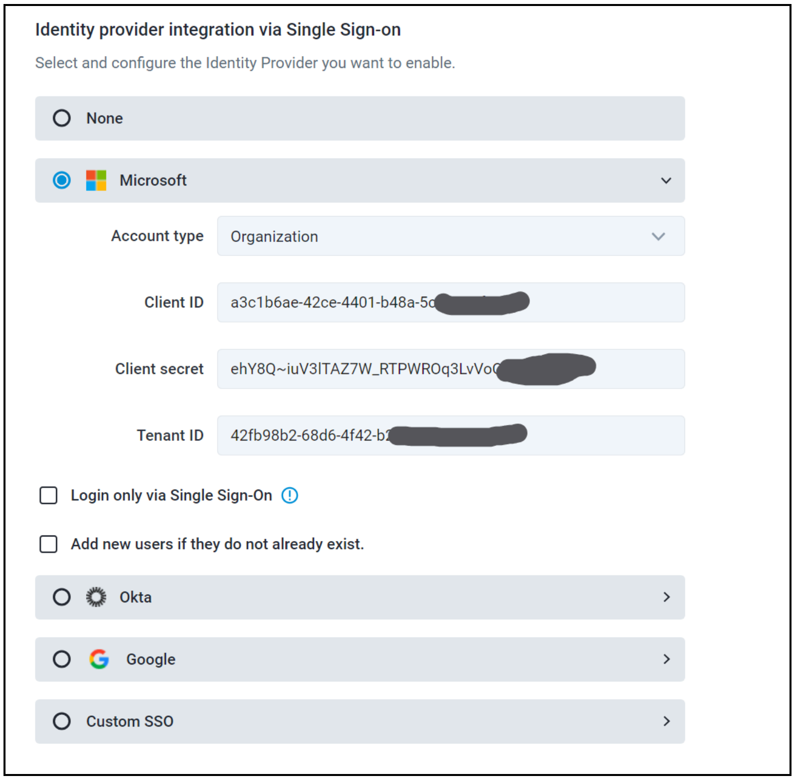
Groups are not available for ass
the application.

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-5d[redacted]

Client secret: ehY8Q~iuV3lTAZ7W_RTPWROq3LvVoC[redacted]

Tenant ID: 42fb98b2-68d6-4f42-b2[redacted]

☐ Login only via Single Sign-On

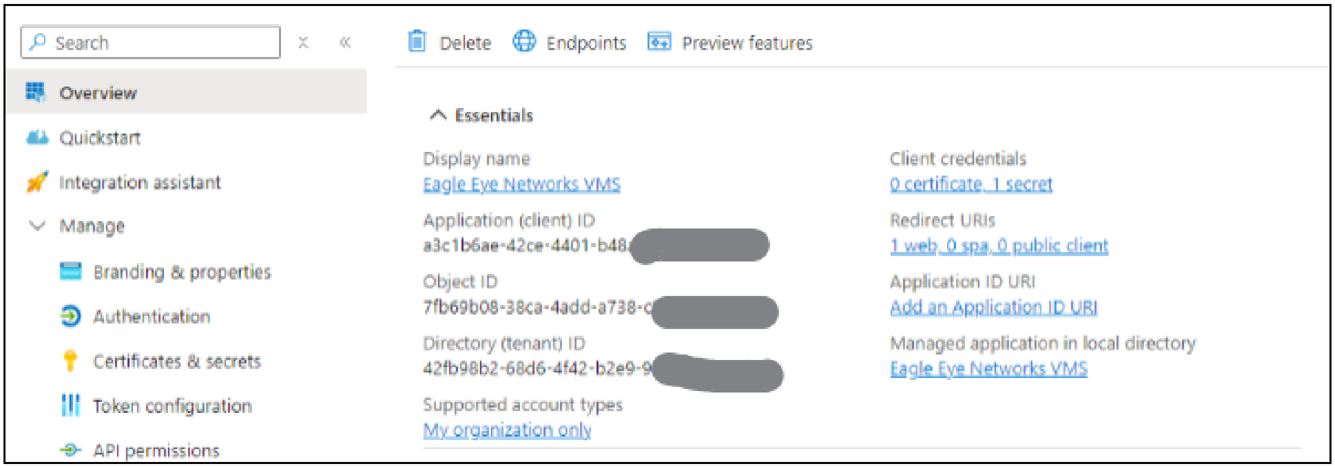
☐ Add new users if they do not already exist.

○ 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**.



Essentials

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

Client credentials: 0 certificate, 1 secret

Redirect URIs: 1 web, 0 spa, 0 public client

Application ID URI: 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

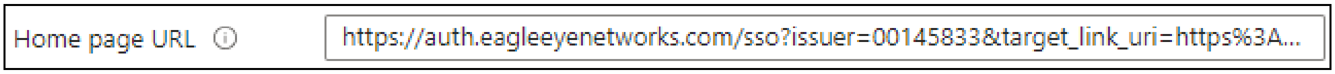
You should now be able to log in to the application.

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

Note: Ensure that the same user is 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.eagleeyenetworks.com/sso?issuer=00145833&target_link_uri=https%3A...

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%3A//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**.

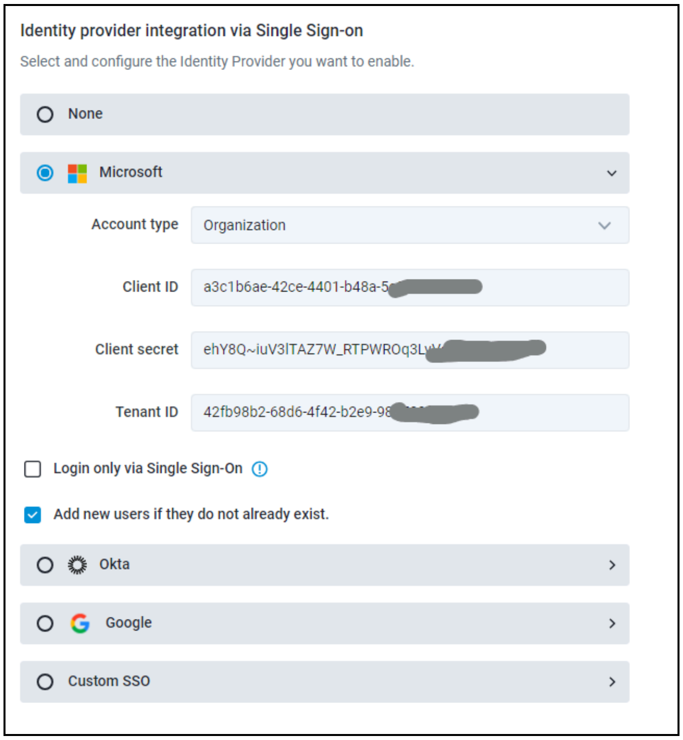
Visible to users? [✓ Yes] No

Setting up IdP-initiated SSO flow

1. Go to **https://myapplications.microsoft.com?tenantId=<tenant-id>.**
2. Log in with a user who exists in your Eagle Eye Networks account and has the same email address.
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[redacted]

Client secret: ehY8Q~iuV3lTAZ7W_RTPWROq3L[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. 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 and has the same email address.
3. Click the Application you created, and you will be redirected to the application.

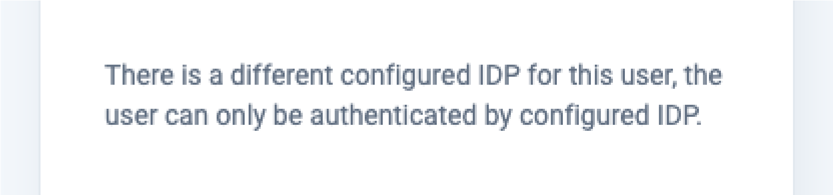
Troubleshooting

Troubleshooting SSO

Several error messages may occur when setting up SSO. Below is an overview of the most common ones. If you encounter any new or different errors, please report them to **support@een.com** so we can add them to this document for future reference.

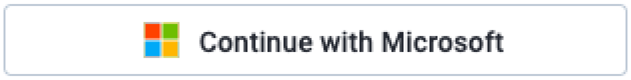
Known errors:

1. **Microsoft Error:** A different configured IDP is set for this user, and the user can only be authenticated by the configured IDP.

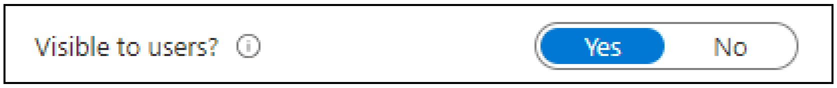


There is a different configured IDP for this user, the user can only be authenticated by configured IDP.

Solution: Users are trying to use the 'Continue with Microsoft' button when they should log in via https://myapplications.microsoft.com. This button is only for **personal** accounts.

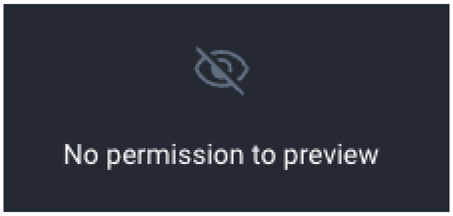


2. **Microsoft Error**: Newly created app doesn't show on my application page:
    a. Make sure the user is added to the enterprise application.
    b. Make sure to make the application visible:



Visible to users? ⓘ [✓ Yes] No

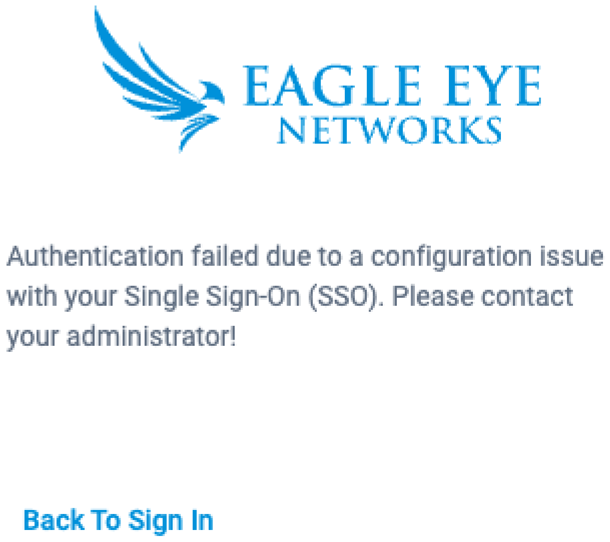
3. **Microsoft Error:** Newly created users see **No permissions to preview**.



No permission to preview

    a. New users don't have any default permissions added; these need to be granted by the admin from within the Enhanced Web Interface.

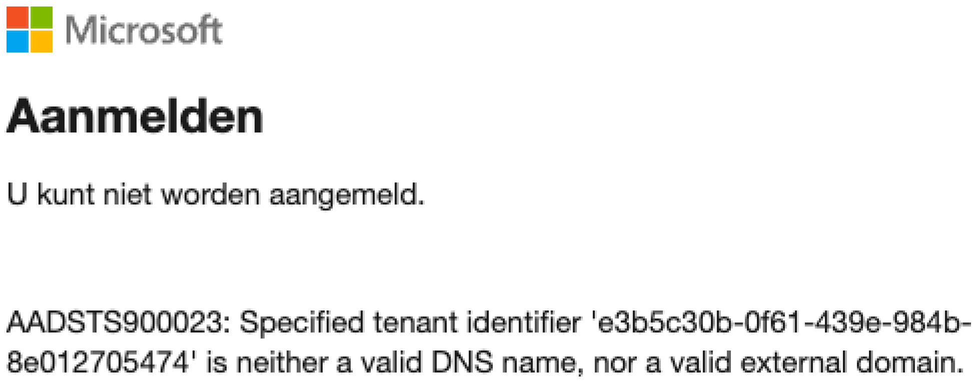
4. **Microsoft Error:** Authentication failed due to a configuration issue with your Single Sign-On (SSO). Please contact your administrator!



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

   a. Please verify the **Client ID** and the **Client Secret** entered on the Enhanced Web Interface.

5. **Microsoft Error:** Unable to log in, tenant identifier is invalid:



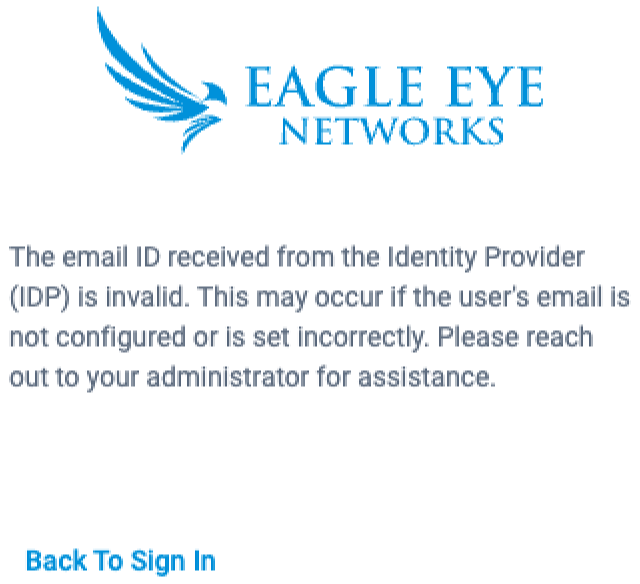
Aanmelden

U kunt niet worden aangemeld.

AADSTS900023: Specified tenant identifier 'e3b5c30b-0f61-439e-984b-8e012705474' is neither a valid DNS name, nor a valid external domain.

   a. Please verify that the **Tenant ID** is entered correctly with a valid ID

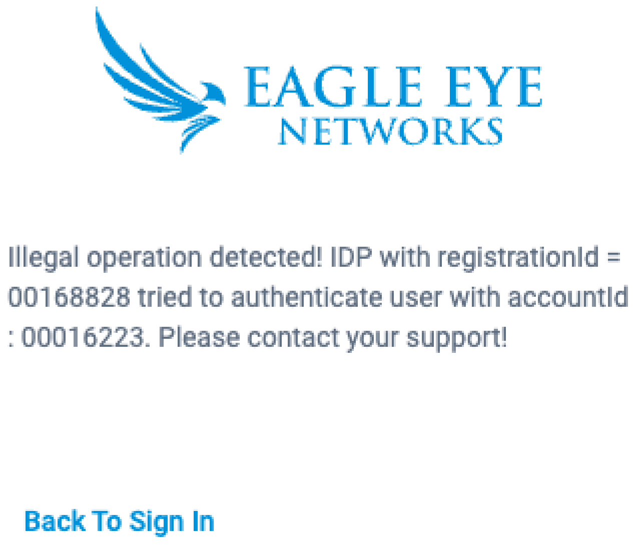
6. **Microsoft Error**: The email ID received from the Identity Provider (IDP) is invalid:



The email ID received from the Identity Provider (IDP) is invalid. This may occur if the user's email is not configured or is set incorrectly. Please reach out to your administrator for assistance.

   a. A user is not configured with a valid email address on the Azure portal.

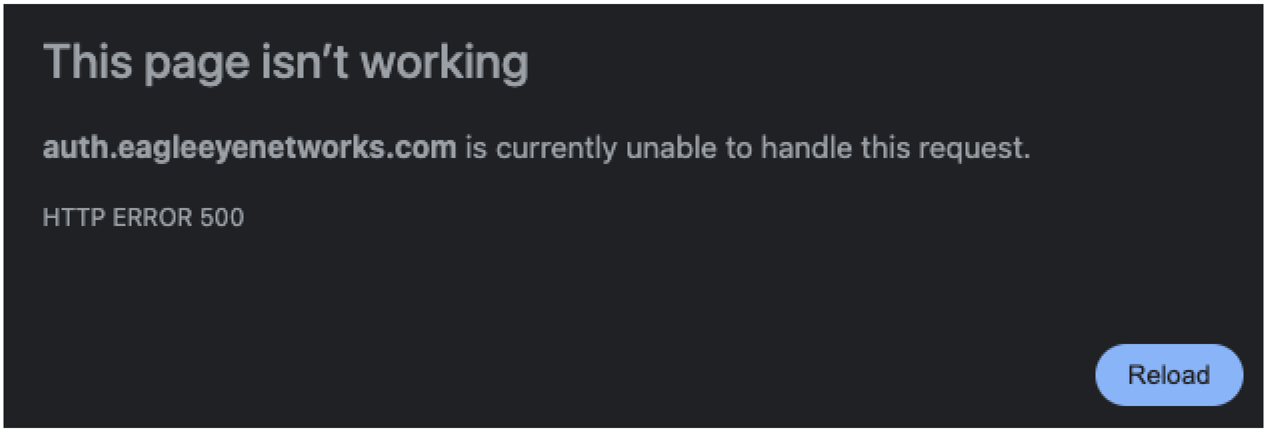
7. **Microsoft Error**: Illegal operation detected! Wrong registrationId.



Illegal operation detected! IDP with registrationId = 00168828 tried to authenticate user with accountId : 00016223. Please contact your support!

   a. A user attempting to sign in is already listed under a different account within our VMS.
   b. Create a separate account or remove the old one to log in.

8. **Microsoft Error**: HTTP ERROR 500:



This page isn't working

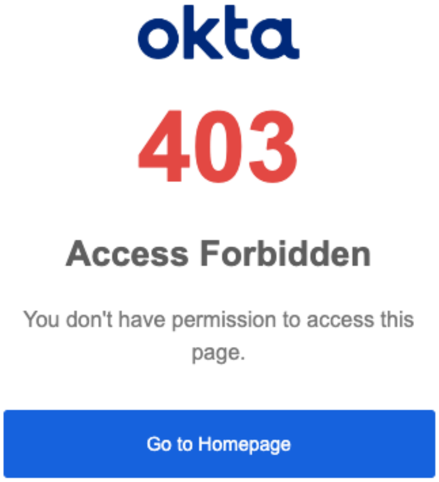
auth.eagleeyenetworks.com is currently unable to handle this request.

HTTP ERROR 500

   a. Verify the redirectURI; it should resemble this, where the issues are the account ID and the target_link_uri is **webapp.eagleeyenetworks.com** or **<branding>.webapp.eagleeyenetworks.com** :

https://auth.eagleeyenetworks.com/sso?issuer=00032511&target_link_uri=https%3A//webapp.eagleeyenetworks.com

9. **Okta Error**: 403 Access forbidden



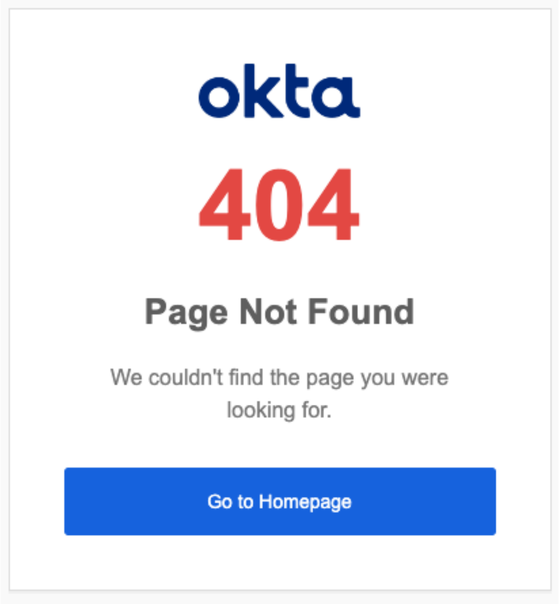
403

Access Forbidden

You don't have permission to access this page.

   a. Verify if settings are correct in our Enhanced Web Interface:
      i. Make sure Okta is selected as the Identity provider
      ii. Client id
      iii. Client Secret
      iv. **Issuer URL** *(example Okta url: https://<subdomain>.okta.com)*

10. Okta Error: 404 Page not found:



okta

404

Page Not Found

We couldn't find the page you were looking for.

a. **Verify the issuer URL; this is probably wrong:**
   i. **https://trial-7462771.okta.com/** < correct one (example)
   ii. **https://trial-7462771-admin.okta.com/** < wrong one (example
   ^ This is a link to the Okta admin panel instead of the Okta user dashboard.

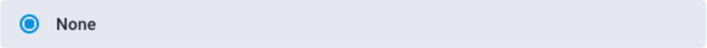
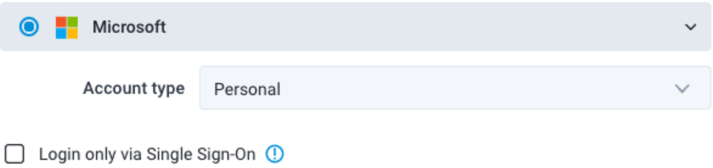
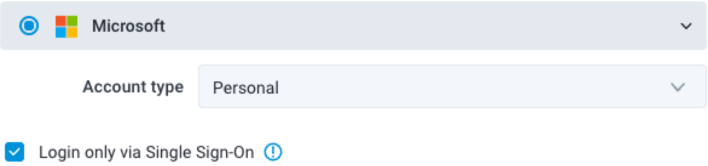
11. Unable to authenticate the user:

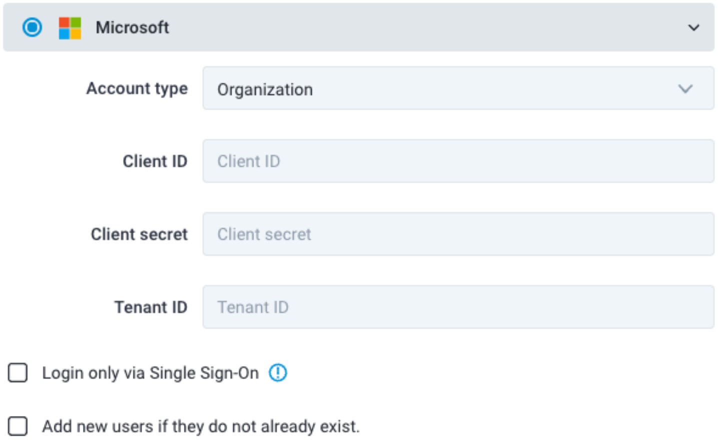
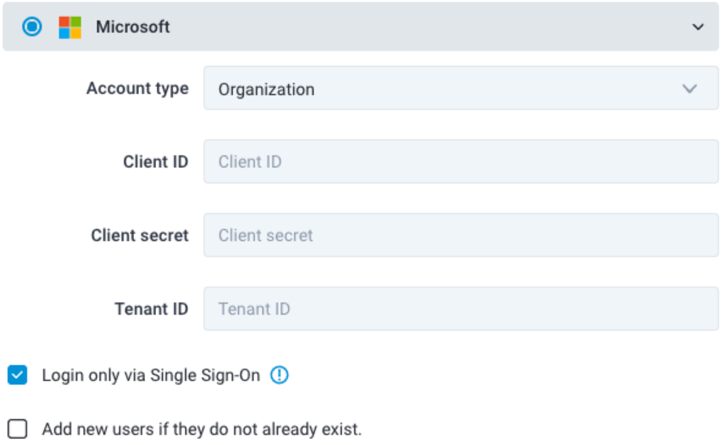
a. **Unable to authenticate the user.**
   i. Redirect URI is wrong: **https://auth.eagleeyenetworks.com/sso?issuer=00170929&target_link_uri=webapp.eagleeyenetworks.com**
   Instead of: **https://auth.eagleeyenetworks.com/sso?issuer=00170929&target_link_uri=https%3A//webapp.eagleeyenetworks.com**
   ii. 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

 ● None	**No SSO selected** • 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 ❌
 ● Microsoft Account type Personal ☐ Login only via Single Sign-On	**Microsoft, Personal** • 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 ❌
 ● Microsoft Account type Personal ☑ Login only via Single Sign-On	**Microsoft, Personal, only SSO** • 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 ❌

 ● Microsoft Account type: Organization Client ID: Client ID Client secret: Client secret Tenant ID: Tenant ID ☐ Login only via Single Sign-On ☐ Add new users if they do not already exist.	**Microsoft, Organization** ● 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 ❌
 ● Microsoft Account type: Organization Client ID: Client ID Client secret: Client secret Tenant ID: Tenant ID ☑ Login only via Single Sign-On ☐ Add new users if they do not already exist.	**Microsoft, Organization, SSO Only** ● 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 ❌