Eagle Eye Application Note - AN014

Implementing Single Sign-On (SSO) in the Eagle Eye Cloud VMS

2023-05-16 Revision 1.0

Target Audience

This Application Note is intended for Resellers of the Eagle Eye Cloud VMS whose customers wish to utilize the convenience and security offered by Single Sign-On, as well as those End Users wishing to set it up for themselves. Note that SSO is included with both Professional and Enterprise editions.

Introduction

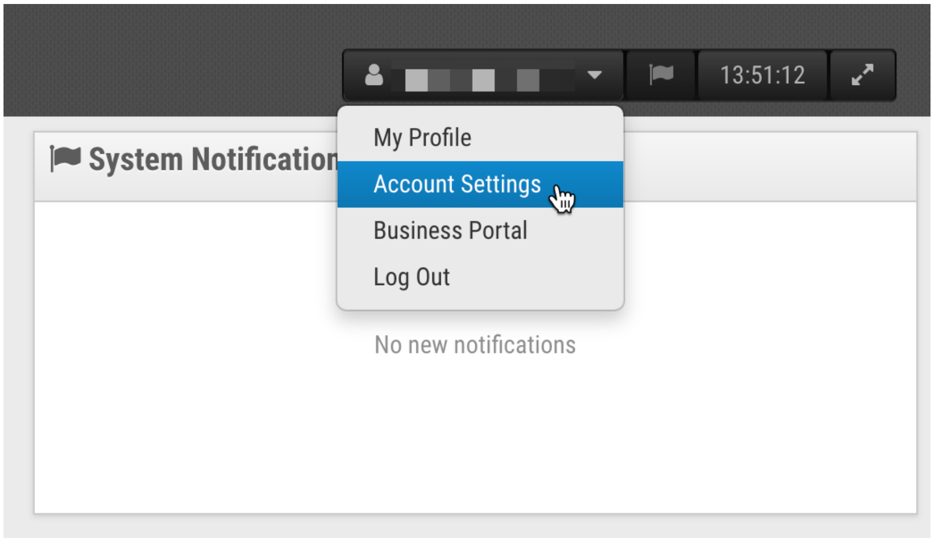
Eagle Eye Networks allows users to log in using single sign-on via an identity provider that supports SAML v2.0 (Security Assertion Markup Language). This document provides the information required to set up the Identity Provider (IdP) for Single Sign-On (SSO) with the Eagle Eye Networks Cloud VMS. Common systems used for SSO are Microsoft Azure Active Directory, Okta, and Google Cloud Platform. Users can login with their corporate emails, which offers the following benefits:

- Easier login experience for the user.
- Increased security because there are fewer passwords to remember.
- Higher productivity because people spend less time logging in to their system.
- Easier IT administration. If an employee departs the company, access can be revoked for multiple applications at once.

Prerequisites

In order to configure SSO, the following requirements should be met:

- You must be a Professional or Enterprise Edition user as SSO support is only available in the Professional and Enterprise Editions of the Eagle Eye Cloud VMS.
- You must enable Branding. To do this, log in to your Reseller account, then click your profile name and Account Settings. If Branding has already been enabled, it will be the default tab shown in Account Settings. If you do not see the Branding tab, please contact your sales engineer to have this enabled.



- Single Sign-On options must have been enabled for you by Eagle Eye Networks. Contact your sales engineer if you need to have this enabled.

The person configuring SSO in the VMS must have the following knowledge and access:

- Basic knowledge of SAML 2.0.
- Access to the Eagle Eye Networks Cloud VMS account with administrator privileges.
- Administrator access to the desired Identity Provider (IdP).

Limitations

- SSO in the Eagle Eye Cloud VMS is limited to being set at either the Reseller level **or** the End User account level. It cannot be set up at both. So, if a Reseller sets up SSO for a specific end user account, they cannot use SSO for their own Reseller account.
- If you choose to enable SSO at the End User account level, login must be initiated within the identity provider (Azure, Okta, etc.).
- The mobile app does not support SSO at this time so it cannot be used if SSO is enabled.

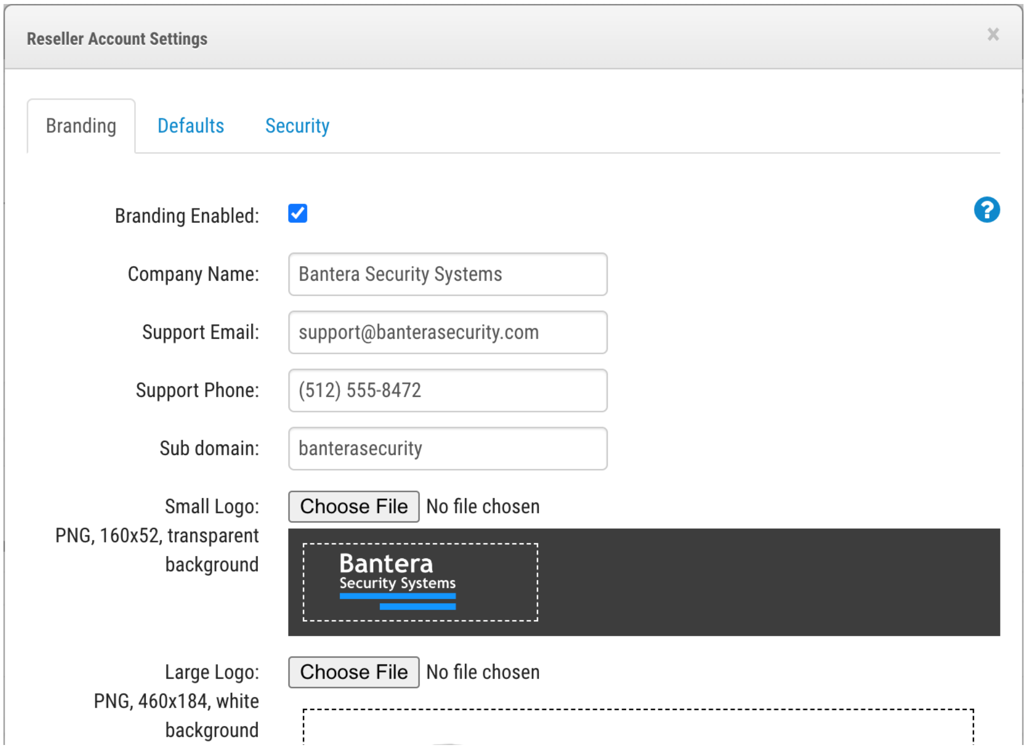
Configuration

As mentioned above, SSO configuration can be done at either the Reseller account level or the End User account level. Both methods are detailed in the section below.

Reseller Account

1. Enable Branding

To enable SSO, the Reseller must first enable branding by going to Account Settings, then Branding as shown below to enable branding.



Reseller Account Settings

Branding | Defaults | Security

Branding Enabled: ☑

Company Name: Bantera Security Systems

Support Email: support@banterasecurity.com

Support Phone: (512) 555-8472

Sub domain: banterasecurity

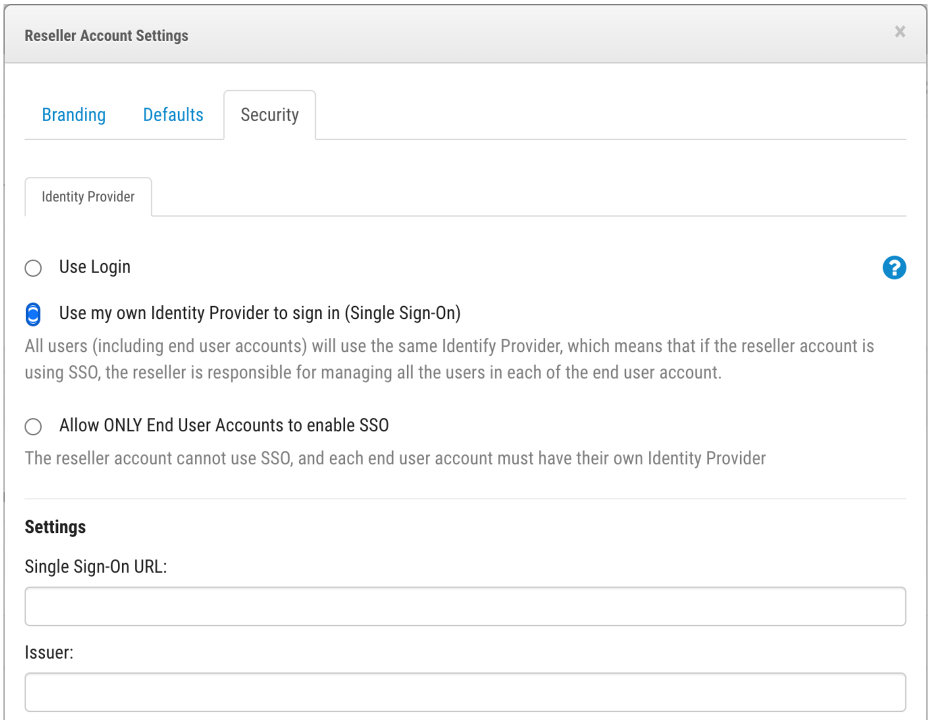
Small Logo: PNG, 160x52, transparent background — No file chosen

Large Logo: PNG, 460x184, white background — No file chosen

The sub domain field will be used to then create a unique URL which will be used for SSO. For example, if the sub domain used is “banterasecurity” then the unique URL will be banterasecurity.eagleeyenetworks.com. The other required fields are Company Name, Small Logo, and Large Logo. After setting up the brand details, click Save.

2. Enable Identity Provider

Once branding is configured and the page is refreshed, a tab labeled Security is available in Account Settings. Using the Identity Provider tab under this, an Identity provider can be set up.



○ Use Login

● Use my own Identity Provider to sign in (Single Sign-On)

All users (including end user accounts) will use the same Identify Provider, which means that if the reseller account is using SSO, the reseller is responsible for managing all the users in each of the end user account.

○ Allow ONLY End User Accounts to enable SSO

The reseller account cannot use SSO, and each end user account must have their own Identity Provider

Settings

Single Sign-On URL:

Issuer:

You will use this tab to select "Use my own Identity Provider to sign in (Single Sign-On)". In this option there will be one IdP to set up for all end user accounts. As the Reseller, you are responsible for setting up the SSO, and users will use the same identity provider.

3. Configure Identity Provider

Jump to Configure Identity Provider via SAML to continue with the setup.

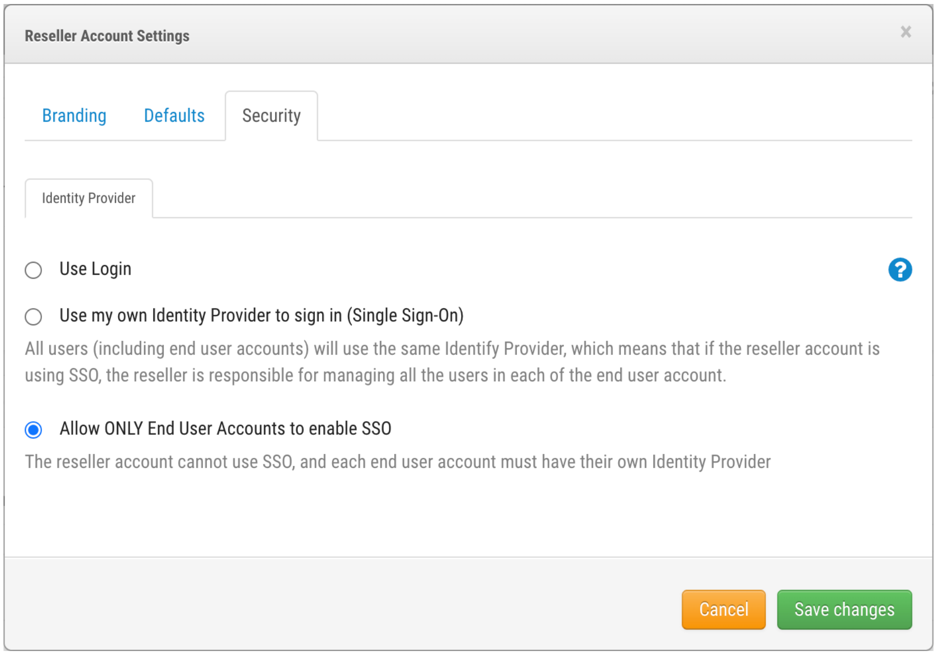
End User Account

1. Enable Branding

Enable branding using the same procedure covered in Step 1 of the Reseller Account. Once that is completed, continue to Step 2 of this section.

2. Enable Identity Provider

Once branding is configured and the page is refreshed, a tab labeled Security is available in Account Settings. Use the Identity Provider tab to set up an Identity provider.



Reseller Account Settings

○ Use Login

○ Use my own Identity Provider to sign in (Single Sign-On)

All users (including end user accounts) will use the same Identify Provider, which means that if the reseller account is using SSO, the reseller is responsible for managing all the users in each of the end user account.

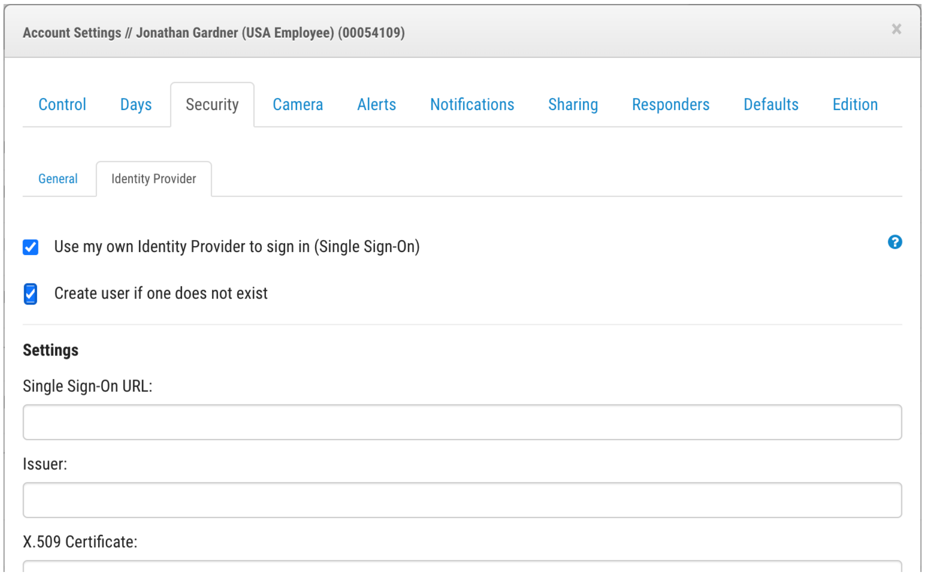
● Allow ONLY End User Accounts to enable SSO

The reseller account cannot use SSO, and each end user account must have their own Identity Provider

You will use this tab to select “Allow ONLY End User Accounts to enable SSO.” Setup must then be continued in the end user account. Click **Save changes,** then log out.

3. Log in to the End User Account and Enable SSO

Log in to the Eagle Eye Cloud VMS End User Account and navigate to Account Settings → Security → Identity Provider. Enable SSO by selecting “Use my own identity provider to sign in.” The settings required to activate SSO will appear after selecting that option.



Account Settings // Jonathan Gardner (USA Employee) (00054109)

☑ Use my own Identity Provider to sign in (Single Sign-On)

☑ Create user if one does not exist

Settings

Single Sign-On URL:

Issuer:

X.509 Certificate:

When setting up the IdP, there is an additional option to “Create user if one does not exist.” If this is enabled, anyone authenticated by the IdP will automatically have a VMS account created without permissions.

Configure Identity Provider via SAML

Now that SSO has been enabled either at the Reseller or End User Account level, the remaining steps are identical. You need to set up the identity provider and VMS to work together and these basic concepts are covered in this section. Some specific examples of IdPs will then be covered in the following section.

To set up the identity provider, there are configurations that need to be shared between the service provider (Eagle Eye Networks) and the account IdP. Below is the Eagle Eye Networks SAML information that needs to be added in the IdP:

Field	Value
Identifier	eagleeyenetworks.com
Reply URL (Assertion Consumer Service URL)	https://<brandsubdomain>.eagleeyenetworks.com/g/aaa/sso/SAML2/Authenticate
Logout URL	https://login.eagleeyenetworks.com/g/aaa/sso/SAML2/LogOut

Below are the required claims that are needed in the assertion:

Field	Value	Required
NameId	User email	Yes
firstName	User first name	No
lastName	User last name	No

Once this is added in the IdP, you will also need to save the IdP secrets in the Eagle Eye Cloud VMS Identity provider settings (Account Settings → Security → Identity Provider). The IdP will provide the following information that you need to enter into the appropriate fields here:

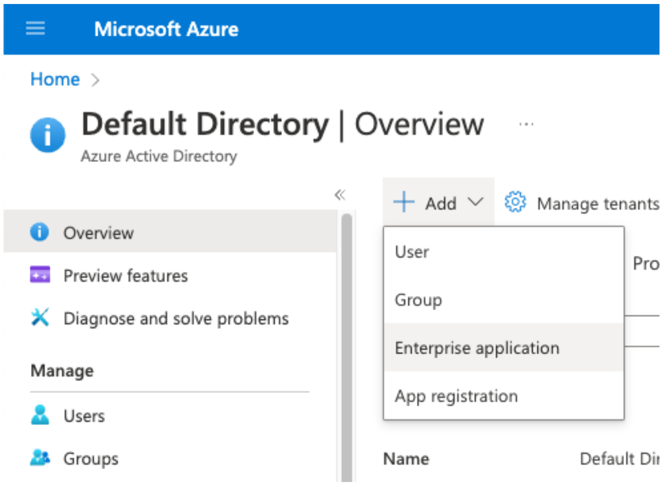
Field	Description
Single Sign-On URL	The URL to which Eagle Eye Networks will redirect the user to login
Issuer	The unique name for the identity provider
X.509 Certificate	The certificate to set up secure communication

After saving the changes, SSO is successfully configured.

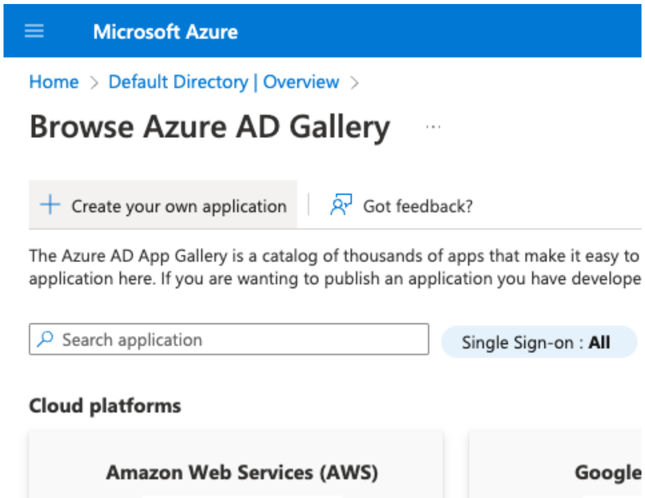
Microsoft Azure Setup

Create a New Application

1. Log in to the Azure Portal at https://portal.azure.com.
2. Click **Azure Active Directory**.
3. Click the **+ Add** dropdown and then **Enterprise application**.

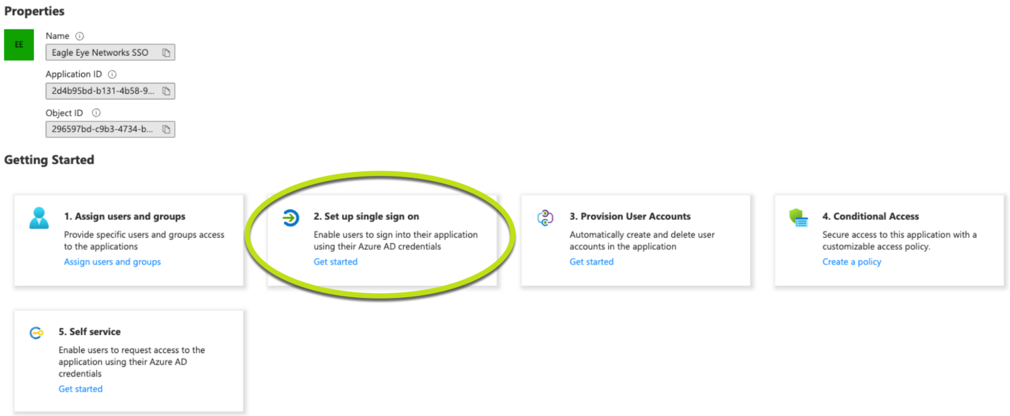


4. Then select **+ Create your own application**.



The Azure AD App Gallery is a catalog of thousands of apps that make it easy to application here. If you are wanting to publish an application you have develope

5. Enter an application name, such as "Eagle Eye Cloud VMS Login," select the option to **Integrate any other application you don't find in the gallery (Non-gallery)**, and click **Create**.
6. Find "Set up Single Sign On" and click **Get Started**.



Properties

Name: Eagle Eye Networks SSO

Application ID: 2d4b95bd-b131-4b58-9...

Object ID: 296597bd-c9b3-4734-b...

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 Azure AD credentials
Get started

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

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

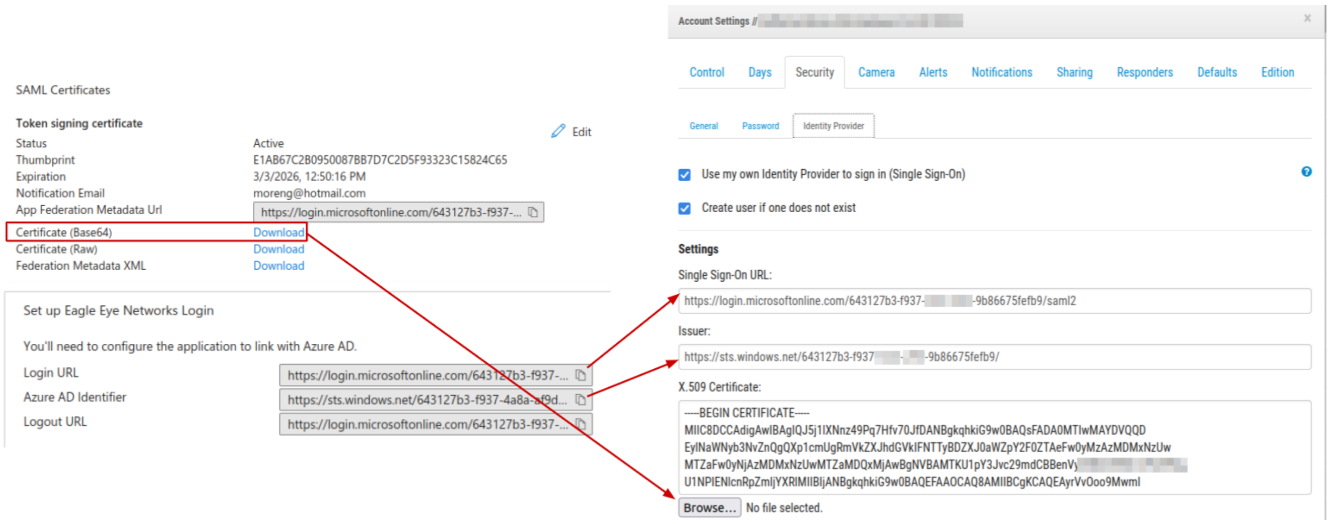
5. Self service
Enable users to request access to the application using their Azure AD credentials
Get started

7. Choose SAML as the SSO method.
8. Use the SAML configuration values provided in the "Configure Identity Provider via SAML" section.
9. Enter the following values in the "User Attributes & Claims":
    a. Please note that some user attributes will be created by default so these need to be deleted.

Claim Name	Claim Value
Unique User Identifier (Name ID)	user.mail [nameid-format:emailAddress]
firstName	user.givenname
lastName	user.surname

10. Enter the following values in the "SAML Signing Certificate" section:
    a. **Signing Option** – Sign SAML assertion
    b. **Signing Algorithm** – SHA-1
11. The "Set up <application name>" section then provides you with the values you need to configure the Eagle Eye Cloud VMS, and the SAML Signing Certificate section provides you with the certificate needed in the VMS. The table below shows how the values relate:

Azure Value	VMS Entry
Login URL	Single Sign-On URL
Azure AD Identifier	Issuer
Certificate (Base64) (Download)	X.509 Certificate (Choose File)



SAML Certificates

Token signing certificate

Status	Active
Thumbprint	E1AB67C2B0950087BB7D7C2D5F93323C15824C65
Expiration	3/3/2026, 12:50:16 PM
Notification Email	moreng@hotmail.com
App Federation Metadata Url	https://login.microsoftonline.com/643127b3-f937-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Set up Eagle Eye Networks Login

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/643127b3-f937-...
Azure AD Identifier	https://sts.windows.net/643127b3-f937-4a8a-af9d...
Logout URL	https://login.microsoftonline.com/643127b3-f937-...

Account Settings // [redacted]

☑ Use my own Identity Provider to sign in (Single Sign-On)

☑ Create user if one does not exist

Settings

Single Sign-On URL:

https://login.microsoftonline.com/643127b3-f937-[redacted]-9b86675fefb9/saml2

Issuer:

https://sts.windows.net/643127b3-f937[redacted]-9b86675fefb9/

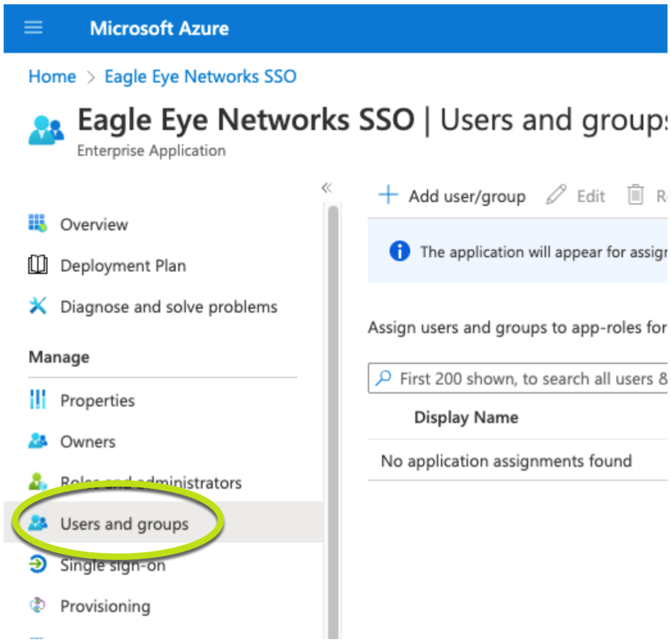
X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIC8DCCAdigAwIBAgIQJ5j1IXNnz49Pq7Hfv70JfDANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQD
EylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMzAzMDMxNzUw
MTZaFw0yNjAzMDMxNzUwMTZaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVy[redacted]
U1NPIENlcnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyrVvOoo9Mwml
```

No file selected.

Set Up Users

1. On the new application's Azure landing page, click **Users and groups**.



Eagle Eye Networks SSO | Users and group:

Enterprise Application

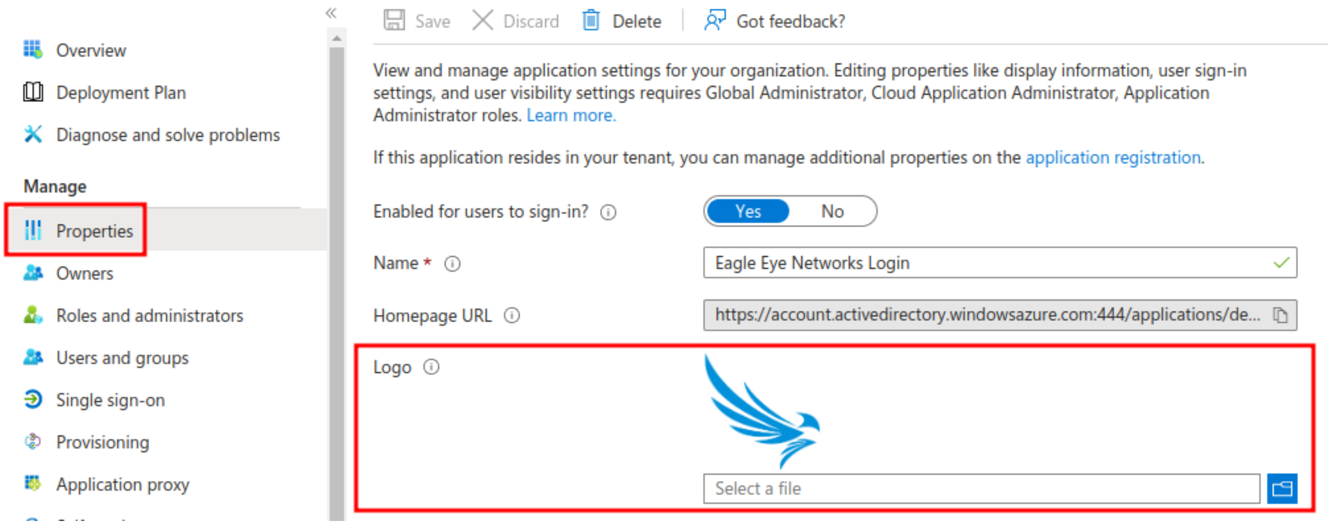
The application will appear for assigr

Assign users and groups to app-roles for

First 200 shown, to search all users &

Display Name
No application assignments found

2. Click **+ Add user/group**.
3. Choose the users you want to add to the SSO application, then click **Select** to confirm.
4. As an optional step, customize the logo being utilized by going to Properties and browsing for a file. If you skip this type, the Microsoft Azure logo will be the default logo.



View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. Learn more.

If this application resides in your tenant, you can manage additional properties on the application registration.

Enabled for users to sign-in? Yes No

Name * Eagle Eye Networks Login

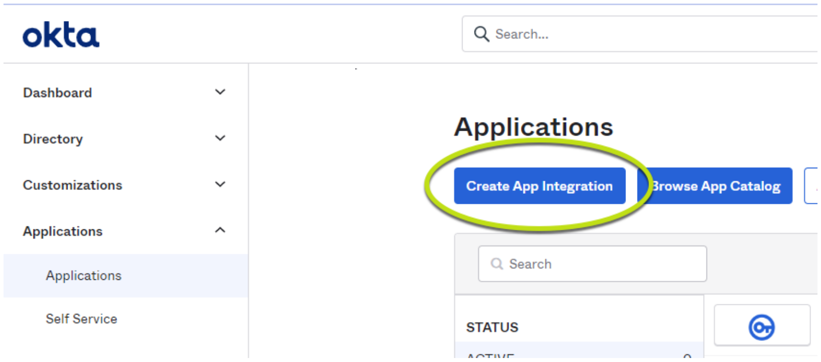
Homepage URL https://account.activedirectory.windowsazure.com:444/applications/de...

Logo

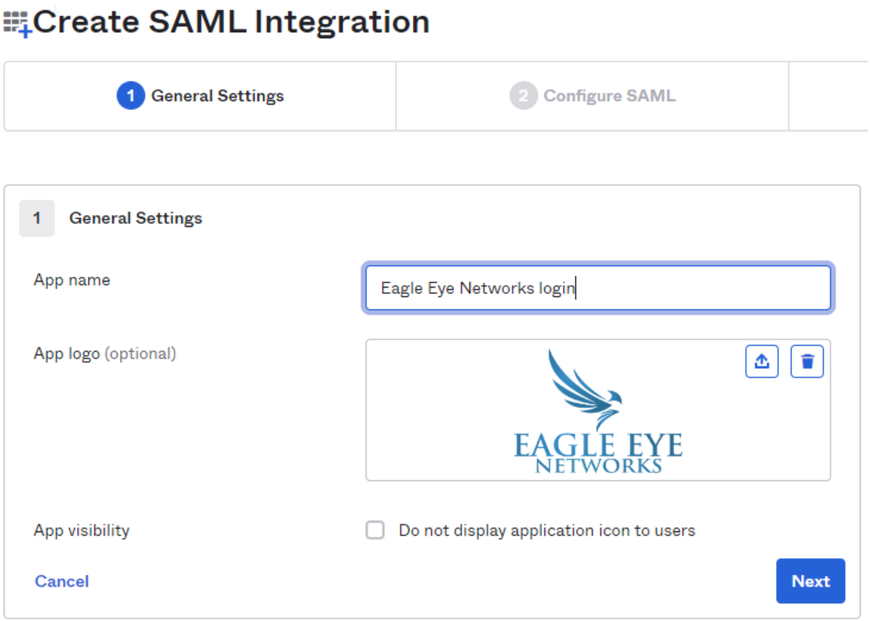
Select a file

Okta Setup

1. Log in to Okta as an admin and click **Create App Integration**.



2. Choose SAML 2.0
3. Give your App a name and a logo.



Create SAML Integration

1 General Settings

2 Configure SAML

1 General Settings

App name: Eagle Eye Networks login

App logo (optional)

App visibility: □ Do not display application icon to users

4. Fill in the details as shown in the table below:

General Settings	
Single sign-on URL	https://<brand>.eagleeyenetworks.com/g/aaa/sso/SAML2/Authenticate **or** https://<custom domain>/g/aaa/sso/SAML2/Authenticate Where **<brand>** and **<custom domain>** are specific to your VMS account.
Audience URI (SP Entity ID)	https://<brand>.eagleeyenetworks.com/saml/metadata **or** https://<customdomain>.eagleeyenetworks.com/saml/metadata
Default RelayState	<leave blank>
Name ID format	EmailAddress
Application username	Email

5. Click the link to show the Advanced Settings, then populate them as shown below:

Advanced Settings	
Response	Signed
Assertion Signature	Signed

Signature Algorithm	RSA-SHA1
Digest Algorithm	SHA1
Assertion Encryption	
Enable Single Logout	Unchecked
Authentication context class	X.509 Certificate
Honor Force Authentication	Yes
SAML Issuer ID	http://www.okta.com/${org.externalKey}

6. Add the following attributes to the Attribute Statements:

Attribute Statements	
firstName	user.firstName
lastName	user.lastName

7. Locate the SAML Signing Certificates section and click **View SAML setup instructions** to find the information that you need to add to the VMS.
8. Add the information to the VMS WebApp as described above.
9. Return to Okta and go to Applications.
10. Click **Assign Users to App**.
11. Select the users you want to assign to the app (enabling SSO for them), then click **Next** and confirm. SSO should now be working for your users.
12. You can test the app by logging in to Okta as a user and clicking the tile to log into the VMS.