DEPLOYMENT GUIDE

BloxOne™ Threat Defense Access Authentication

Table of Contents

Introduction

BloxOne™ Threat Defense provides an Access Authentication service that you can use to authenticate users through a captive portal using third-party IdP (Identity Provider) federation and create security policies based on user groups. The Access Authentication feature allows you to integrate third-party IdP federations, using SAML, OpenID Connect or LDAP and create authentication profiles that you associate with BloxOne hosts. Using the Access Authentication service, you can synchronize user groups from your chosen IdP, so you can build security policies based on user groups from Microsoft Azure Active Directory, Okta, and OpenAM

Prerequisites

The following are prerequisites for the integration using the BloxOne Access Authentication feature:

- BloxOne:
  - BloxOne Threat Defense Business Cloud or Advanced subscription
  - BloxOne DFP (or DNS Forwarding Proxy) deployed as a VM or in a container. Please note that DFP deployed on NIOS are not supported
  - A CSP user account with B1TD administrator permissions
- A configured 3rd-party Identity Provider (One of the following):
  - Azure
  - Okta
  - Microsoft AD (Microsoft AD is not covered in this guide. Refer to BloxOne Documentation.)
  - OpenAM (OpenAM is not covered in this guide. Refer to BloxOne Documentation.)
  - For more information on supported IdPs see Managing Access Authentication - BloxOne Cloud - Infoblox Documentation Portal

Known Limitations

Please note that By enabling the Access Authentication service users connected to any existing DNS services may be interrupted. Once the Access Authentication service is enabled, users will be redirected to the Access Authentication page for authentication before DNS resolution is available.

Additionally, please note that you may only apply one Authentication Profile to a BloxOne host. This feature will also not work on a BloxOne host that is running BloxOne DNS. Currently this feature is not supported on NIOS.

Configuration

Workflow

1. Acquire Service Provider URLs from BloxOne.
2. Create an Application on the IdP.
3. Assign user groups to the IdP Application.
4. Acquire the associated IdP API keys, and URLs.
5. Input the IdP URLs into BloxOne and enable the Authentication Profile.
6. Enable the Access Authentication service on a BloxOne Host.
7. Apply the desired Access Authentication IdP configuration to the Access Authentication service.
8. Pull list of user groups from the IdP application.
9. Add Desired User Groups to one or many Security Policies.
10. Test the configuration.

Before You Get Started

Prepare BloxOne Host

The following sections do not cover how to deploy a BloxOne host and/or the BloxOne DFP service and only covers how to deploy the BloxOne Threat Defense Access Authentication service with Azure, and Okta. For the BloxOne Access Authentication service to work, you must have a BloxOne host with the DNS Forwarding Proxy and Access Authentication services enabled. For details on how to deploy a BloxOne host, or how to enable the DFP service, please visit the Infoblox Documentation portal.

Configure an IdP

The following sections cover how to acquire the tokens needed to configure BloxOne to work with the IdPs Azure and Okta. This document does not cover how to initially configure and set up each of the required components of an IdP.

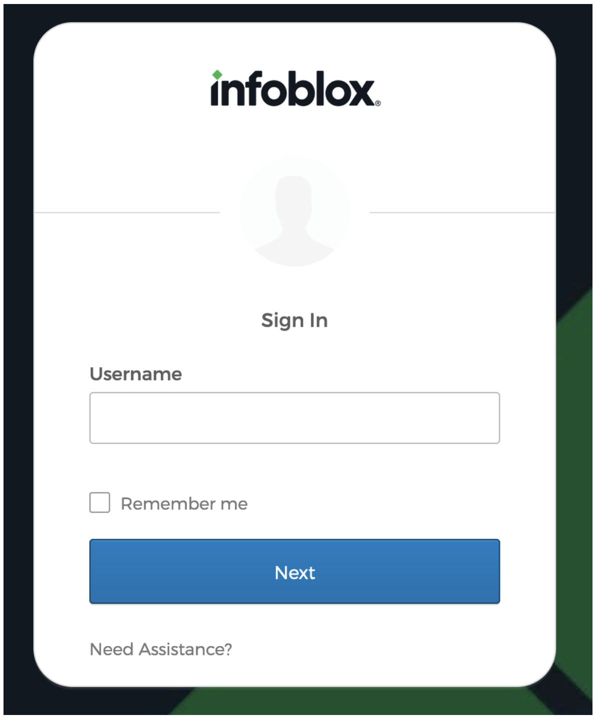
BloxOne Access Authentication with Azure

This portion of the guide covers how to configure BloxOne to work with AzureAD as an IdP.

Prepare the BloxOne Authentication Profile

To configure BloxOne to work with Azure as its IdP you must first create a SAML Authentication profile and acquire service provider URLs. To acquire these URLs, perform the following steps:

1. Access the Infoblox CSP at csp.infoblox.com, and log in with your credentials.



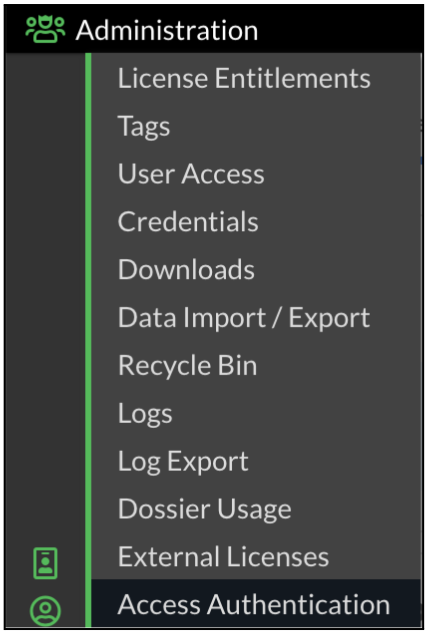
infoblox

Sign In

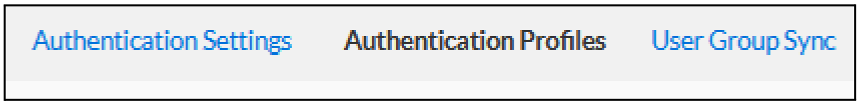
Username

□ Remember me

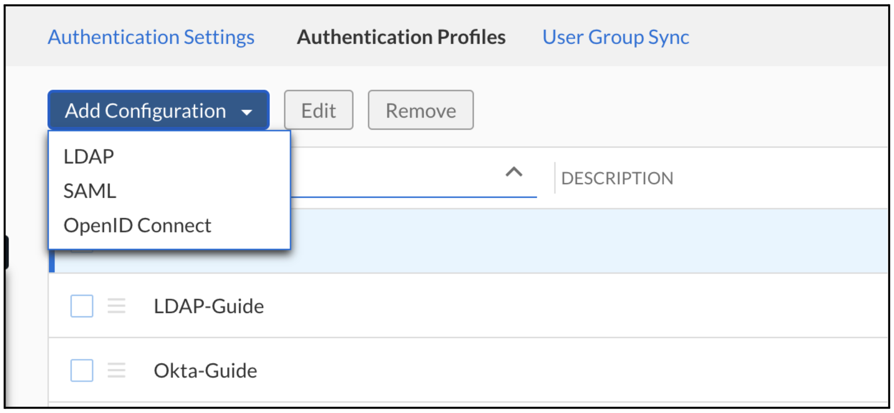
2. On the left navigation panel, highlight **Administration**. Then, click **Access Authentication** in the list that is revealed.



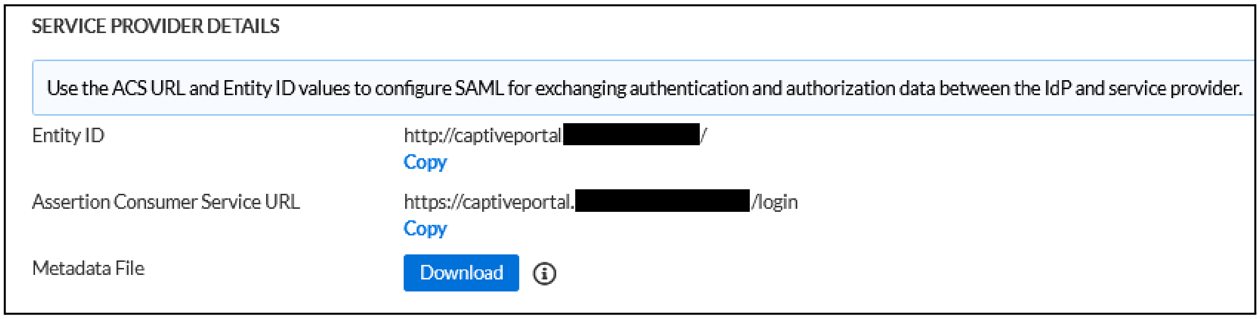
3. On the Access Authentication page, click the **Authentication Profiles** tab.



4. On the Authentication Profiles page, click **Add Configuration**. Then, click **SAML** in the list that is revealed.



5. On the Create Authentication Profile panel, copy and paste the two URLs located under the Service Provider Details header into a separate document so that they can be used later.



SERVICE PROVIDER DETAILS

Use the ACS URL and Entity ID values to configure SAML for exchanging authentication and authorization data between the IdP and service provider.

Entity ID: http://captiveportal[redacted]/
Copy

Assertion Consumer Service URL: https://captiveportal.[redacted]/login
Copy

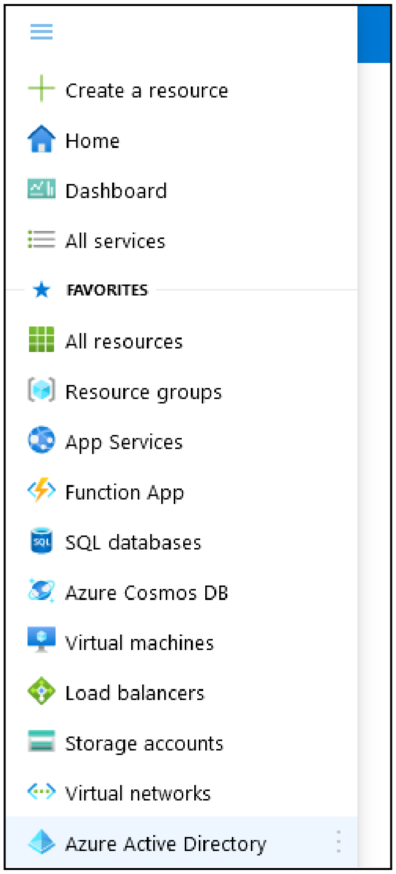
Metadata File: Download ⓘ

Create an Azure Application

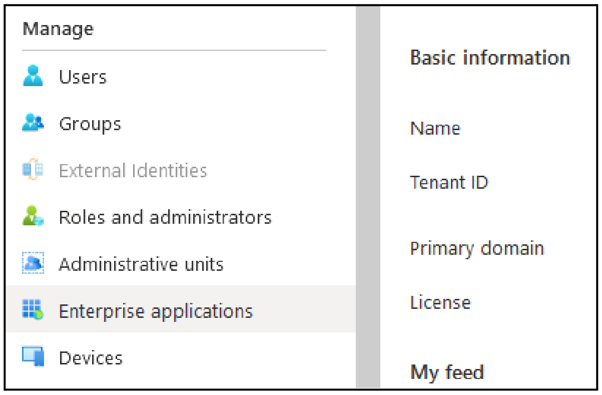
In order to allow Azure to sync groups with BloxOne you must create and configure an Azure application. Additionally, you must also acquire multiple URLs, and create a Groups Claim from the application. To create an Azure Application, acquire the needed URLs, and create the Groups claim, perform the following steps:

1. Keep the Infoblox CSP Authentication Profile page open, and open a new browser or browser tab. Then, access your organization's Azure Portal at portal.azure.com.

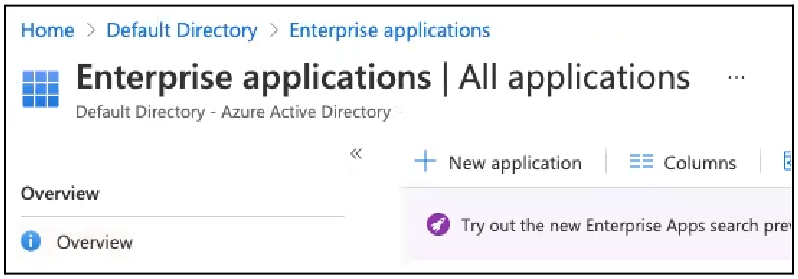
2. Click on the **hamburger** icon located on the top left of the Azure Portal to reveal the navigation panel. In the list that is revealed, click on **Azure Active Directory**.



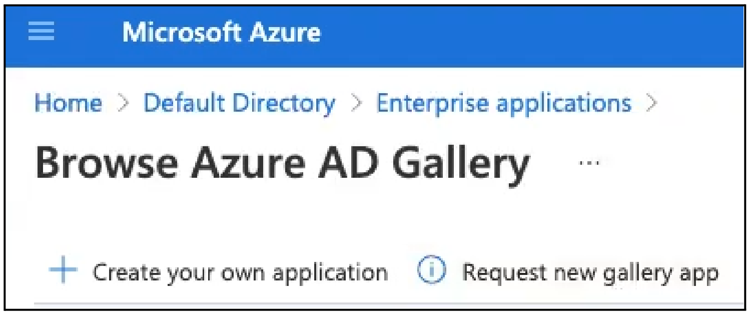
3. Click on **Enterprise applications** located under the manage header in the left navigation panel.



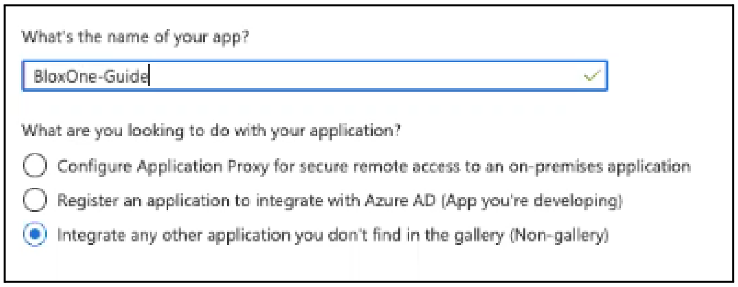
4. Above the list of existing applications, click on **New application**.


Home > Default Directory > Enterprise applications
Enterprise applications | All applications
Default Directory - Azure Active Directory
«
+ New application
Columns
Overview
Overview
Try out the new Enterprise Apps search pre

5. On the Azure AD Gallery page, click **Create your own application**.


Microsoft Azure
Home > Default Directory > Enterprise applications >
Browse Azure AD Gallery ...
+ Create your own application
Request new gallery app

6. In the Create your own application prompt, input a **name**, and keep all other settings as their **default**. Then click **Create** to confirm the creation of the App.



What's the name of your app?

BloxOne-Guide

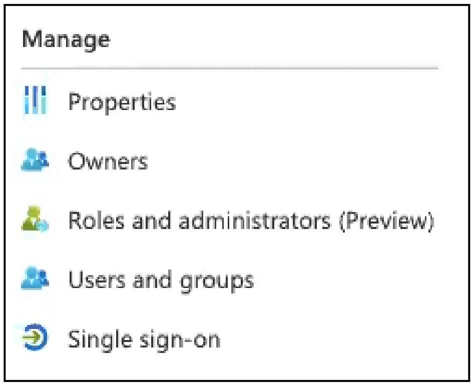
What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application

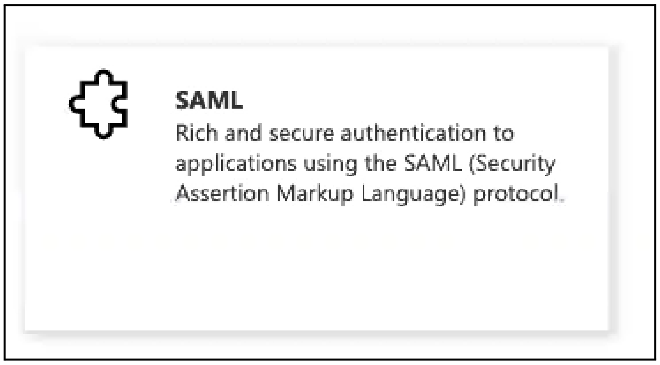
○ Register an application to integrate with Azure AD (App you're developing)

● Integrate any other application you don't find in the gallery (Non-gallery)

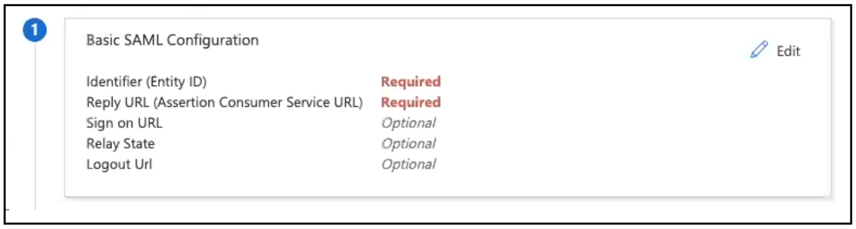
7. On the newly created app's page, click **Single sign-on** located in the left navigation panel.



8. On the Select a single sign-on method page, click **SAML**.


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

9. On the Enterprise Application page, click the **Edit** icon associated with the Basic SAML Configuration panel.



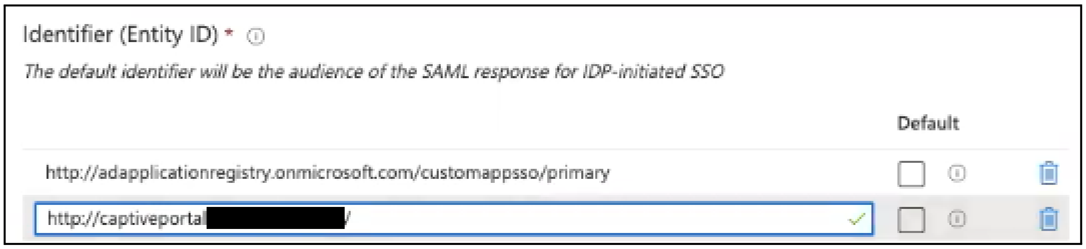
Basic SAML Configuration

Edit

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	*Optional*
Relay State	*Optional*
Logout Url	*Optional*

10. In the panel that is revealed, input the following information:

- In the text box titled **Identifier** (Entity ID), input the **URL** acquired from the Infoblox CSP Authentication Profile. This URL is titled as the Entity ID in the Infoblox CSP.

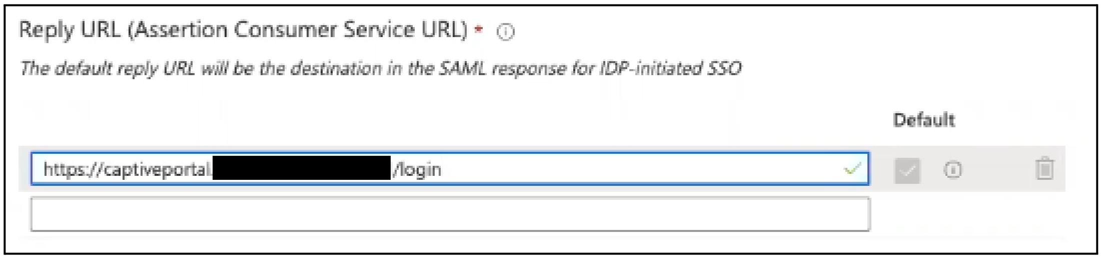


Identifier (Entity ID) *

The default identifier will be the audience of the SAML response for IDP-initiated SSO

	Default
http://adapplicationregistry.onmicrosoft.com/customappsso/primary	□
http://captiveportal[redacted]/	□

- In the text box titled Reply URL (Assertion Consumer Service URL), input the **URL** acquired from the Infoblox CSP Authentication Profile. Note: This URL ends with the text login and is titled as the Assertion Consumer Service URL in the Infoblox CSP.

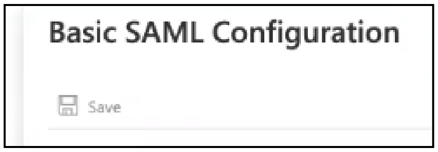


Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

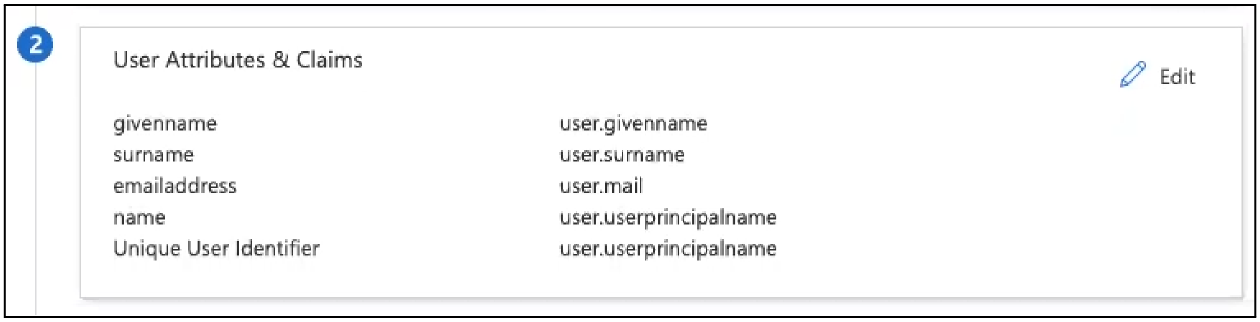
	Default
https://captiveportal[redacted]/login	☑

11. Click the **Save** icon located below the Basic SAML configuration header.



Basic SAML Configuration

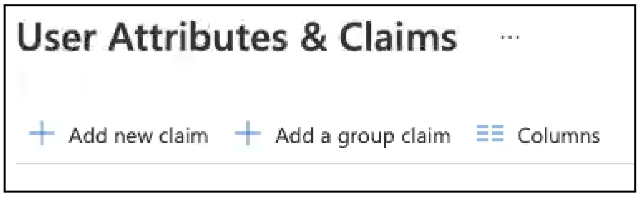
12. Click **Edit** on the User Attributes & Claims step.



User Attributes & Claims

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

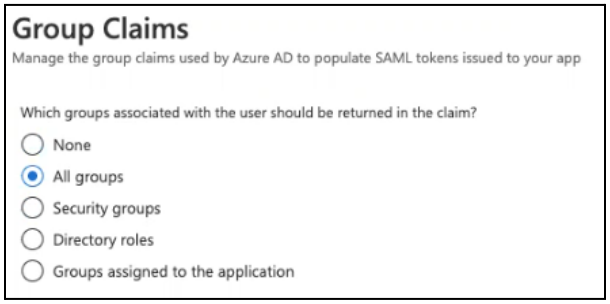
13. On the User Attributes & Claims page, click **Add a group claim**.



User Attributes & Claims

14. In the Group Claims panel configure the following settings:

   - Under the Which Groups associated with the user should be returned in the claim? header, select All groups.



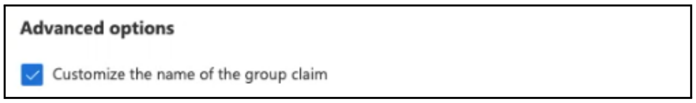
Group Claims

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

○ None
● All groups
○ Security groups
○ Directory roles
○ Groups assigned to the application

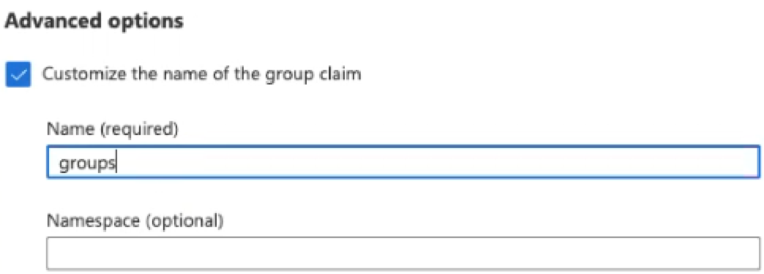
   - Under Advanced options ensure that the checkbox for Customize the name of the group claim is checked.



Advanced options

☑ Customize the name of the group claim

   - In the Name (required) textbox, input the **name** groups for the group claim.



Advanced options

☑ Customize the name of the group claim

Name (required)

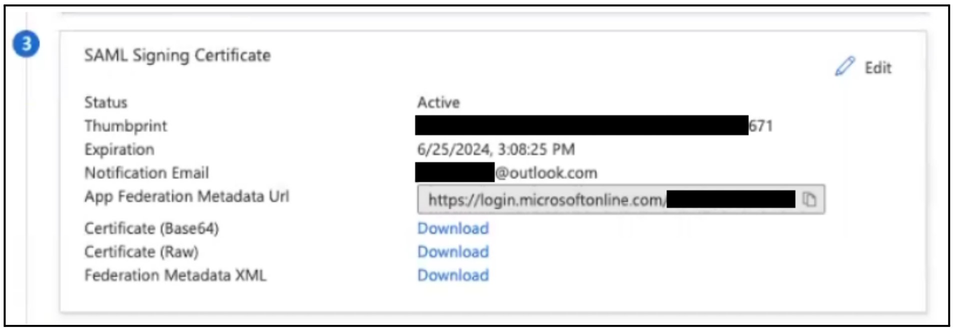
groups

Namespace (optional)

- Click **Save** to confirm the creation of the Group Claim.

15. Navigate back to App's main configuration page by clicking the **X** located on the top right of the Azure screen.

16. On step 3 of the Enterprise Application page, copy the App Federation Metadata Url by clicking the copy icon. Save this to a text file for use later. Note: this will be used as the Metadata URL in the Infoblox CSP.



SAML Signing Certificate

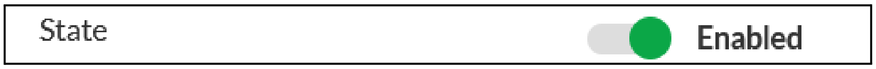
Status	Active
Thumbprint	[redacted]671
Expiration	6/25/2024, 3:08:25 PM
Notification Email	[redacted]@outlook.com
App Federation Metadata Url	https://login.microsoftonline.com/[redacted]
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Finalize the creation of the BloxOne Authentication Profile

To finalize the creation of the BloxOne Authentication Profile you must enable the profile, select the correct IdP and input a Metadata URL To accomplish this, perform the following steps:

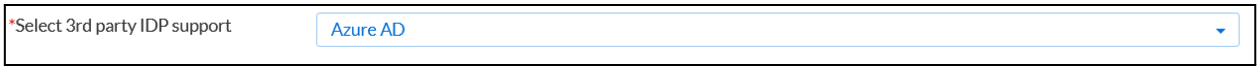
1. Navigate back to the Infoblox CSP and the Create Authentication Profile panel accessed on page 5, in steps 2-5.

2. Change the State of the Authentication profile to **Enabled** by clicking the toggle switch.



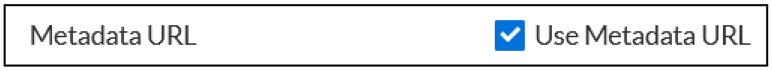
State ● Enabled

3. Under the Select 3rd party IDP support dropdown, select **Azure AD**.



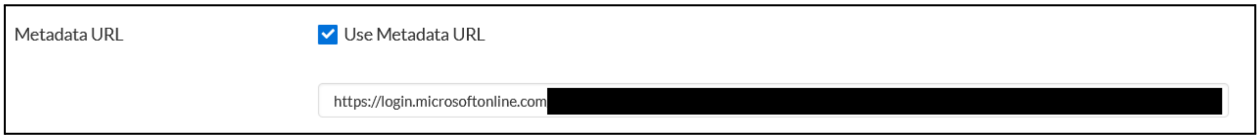
*Select 3rd party IDP support: Azure AD

4. Under the Identity Provider Details header, click the **checkbox** associated with Metadata URL.



Metadata URL ☑ Use Metadata URL

5. Paste the URL acquired from the SAML Signing Certificate on page 10.



Metadata URL ☑ Use Metadata URL

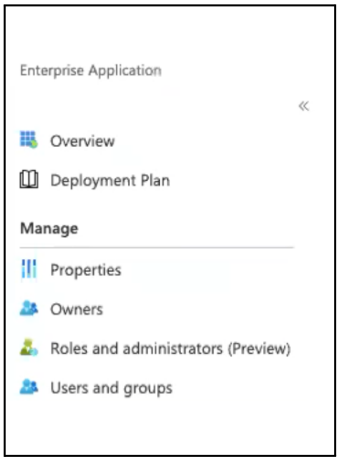
https://login.microsoftonline.com[redacted]

6. Click **Save & Close** to confirm the creation of the Authentication Profile.

Add Security Groups to the Azure Application

To allow users to login to the new application, you must first assign security groups to the application. To accomplish this, perform the following steps:

1. Access your Azure portal while keeping the Infoblox CSP open. From the Overview page of your new Enterprise Application, click **Users and groups** in the left navigation panel.



Enterprise Application

«

Overview

Deployment Plan

Manage

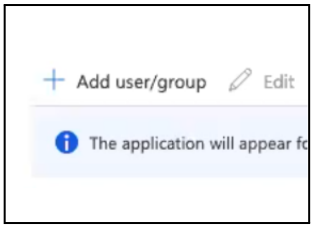
Properties

Owners

Roles and administrators (Preview)

Users and groups

2. On the Users and groups page, click **Add user/group**.

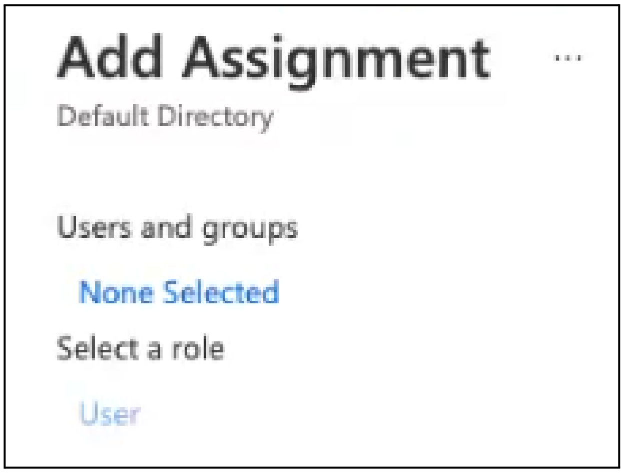


+ Add user/group

Edit

The application will appear fo

3. On the Add Assignment page, click the blue text **None Selected.**



Add Assignment ...

Default Directory

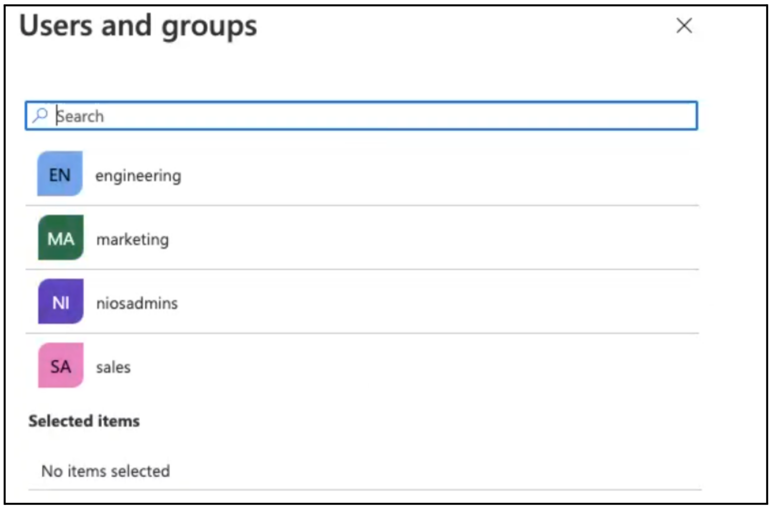
Users and groups

None Selected

Select a role

User

4. Select the desired groups you would like to be associated with the Access Authentication profile.



Users and groups

Search

EN engineering

MA marketing

NI niosadmins

SA sales

Selected items

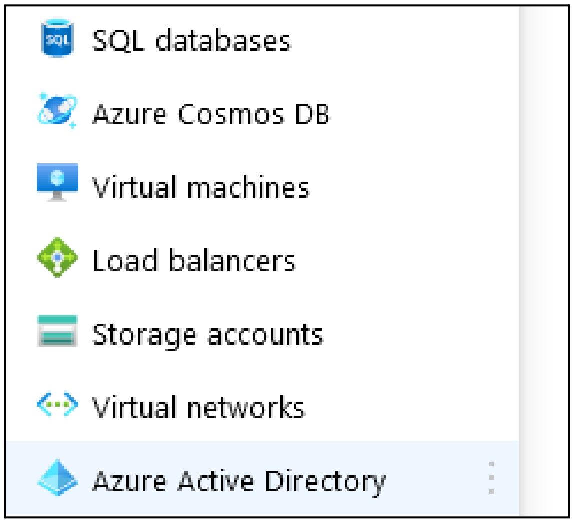
No items selected

5. Click **Save** to confirm the selection of groups.

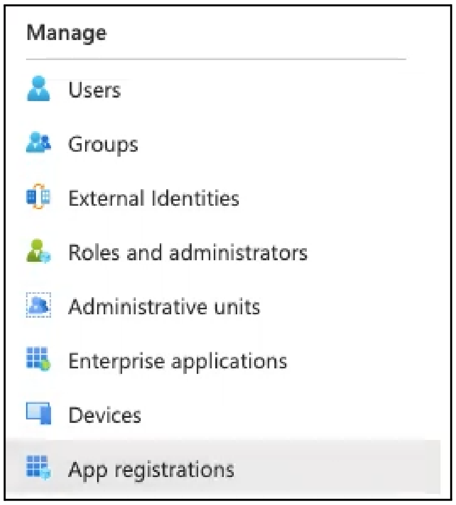
Acquire an Access token from Azure

Acquire an Admin token from Azure. This Admin token will be used to sync Azure Active Directory Groups into the CSP. To acquire the Access Token, perform the following steps:

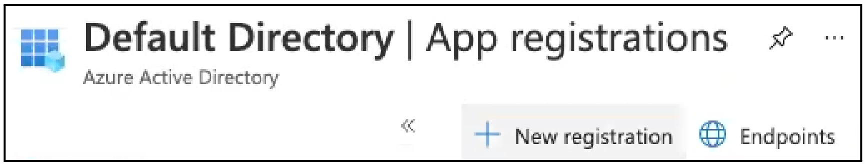
1. Access the Azure Active Directory. On the Azure Portal's homepage, click the hamburger icon located on the top left of the screen to reveal the navigation panel. In the list that is revealed, click on **Azure Active Directory**.



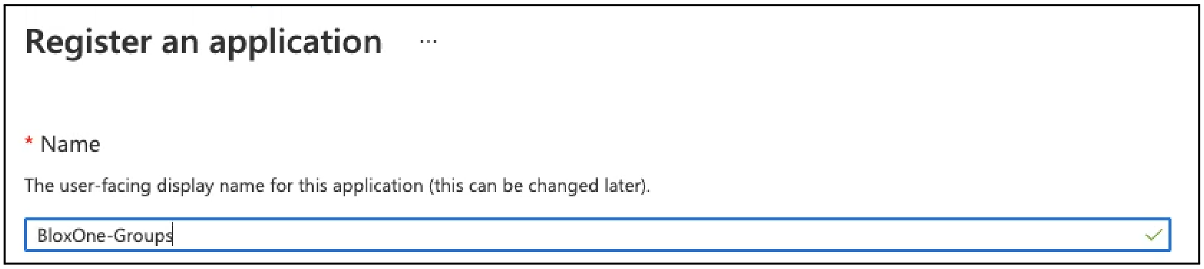
2. In the left navigation panel of the Azure Active Directory page, click **App registrations**.



3. Click **New registration**.



4. On the Register an application page, give the application a **Name**.

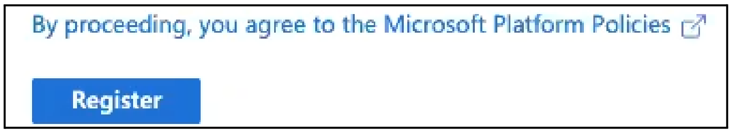


* Name

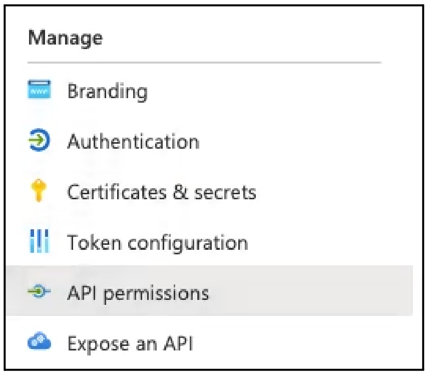
The user-facing display name for this application (this can be changed later).

BloxOne-Groups

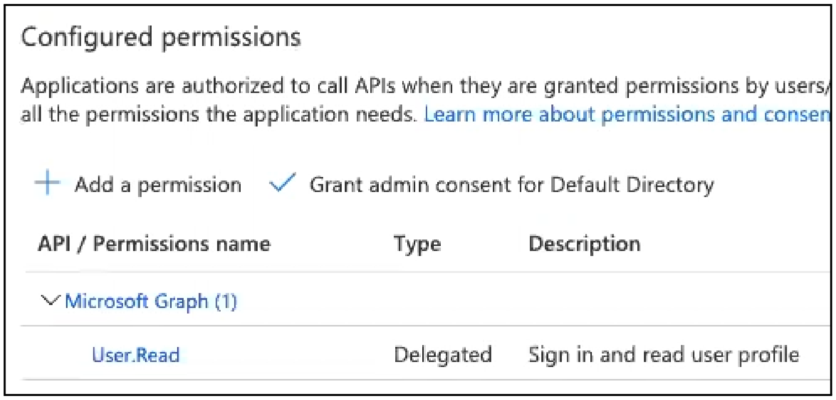
5. Keep all other settings as their default. Click **Register** to confirm the registration of the app.


By proceeding, you agree to the Microsoft Platform Policies

6. On the App’s page, click **API permissions** located in the left navigation panel.



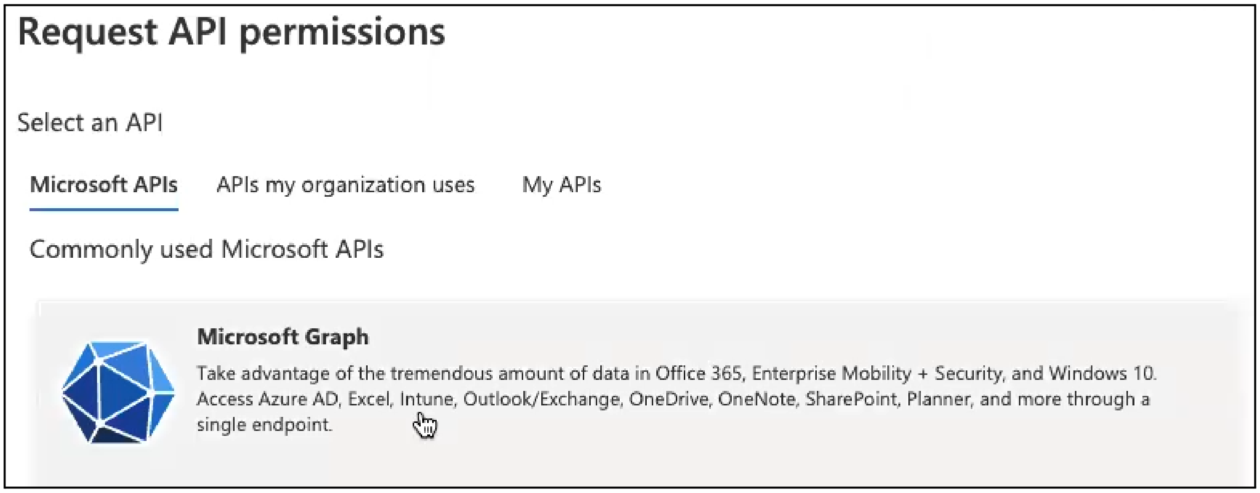
7. On the API permissions page, click **Add a permission**.


Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/ all the permissions the application needs. Learn more about permissions and consen

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

8. On the Request API permissions panel that is revealed, click **Microsoft Graph**.


Request API permissions

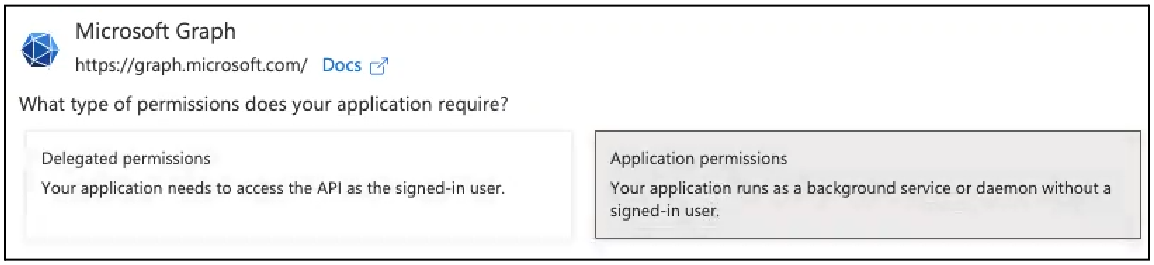
Select an API

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

9. Click **Application permissions.**



Microsoft Graph

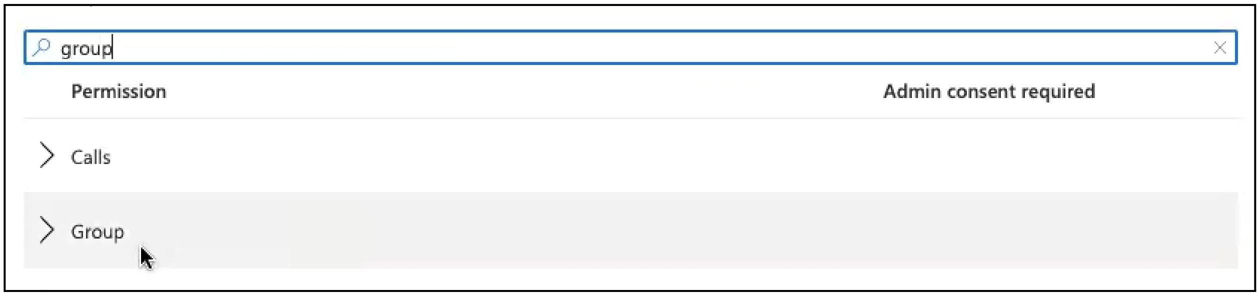
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

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

Application permissions
Your application runs as a background service or daemon without a signed-in user.

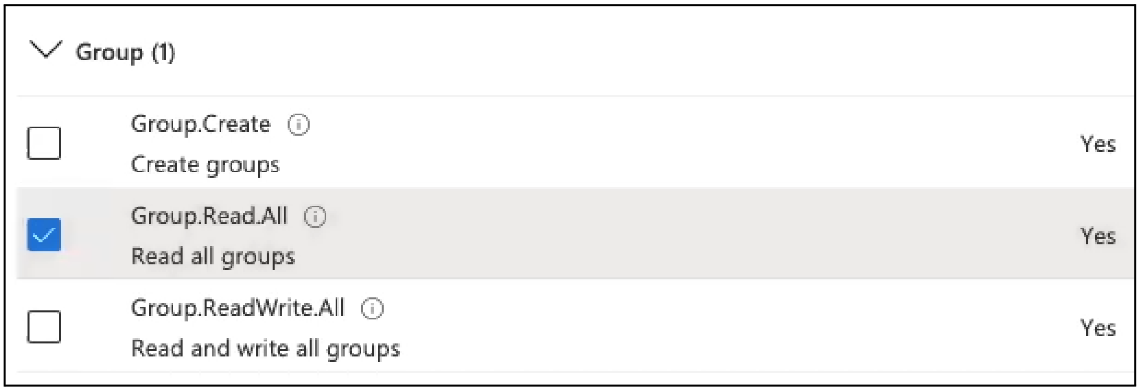
10. Use the search bar that is revealed and type in group. Then, click the **Group** dropdown.



group

Permission	Admin consent required
› Calls	
› Group	

11. In the list that is revealed, click the checkbox associated with **Group.Read.All**.

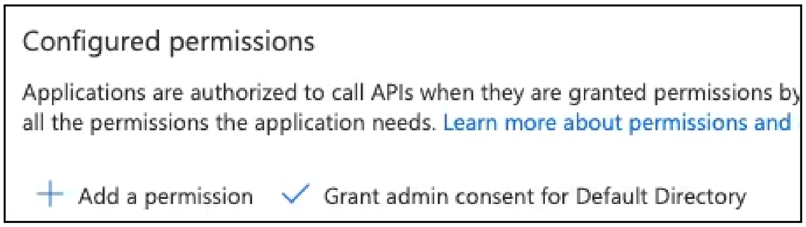


Group (1)

□	Group.Create ⓘ Create groups	Yes
☑	Group.Read.All ⓘ Read all groups	Yes
□	Group.ReadWrite.All ⓘ Read and write all groups	Yes

12. Click **Add permissions** to confirm the addition of the permission.

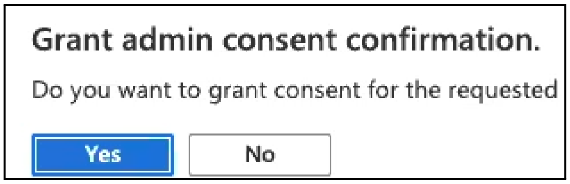
13. On the API Permissions page, click **Grant admin** consent for Default Directory. *Note: You must have administrator permissions to see and/or click this button.*



Configured permissions

Applications are authorized to call APIs when they are granted permissions by all the permissions the application needs. Learn more about permissions and

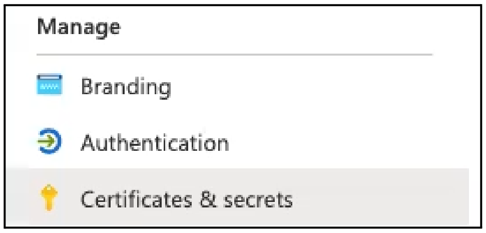
14. Click **Yes** in the confirmation panel that is revealed.



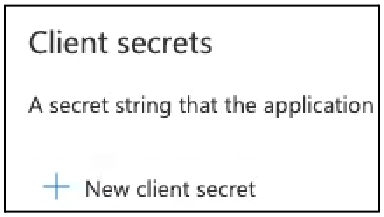
Grant admin consent confirmation.

Do you want to grant consent for the requested

15. After permission has been granted, click **Certificates & secrets** in the left navigation panel.



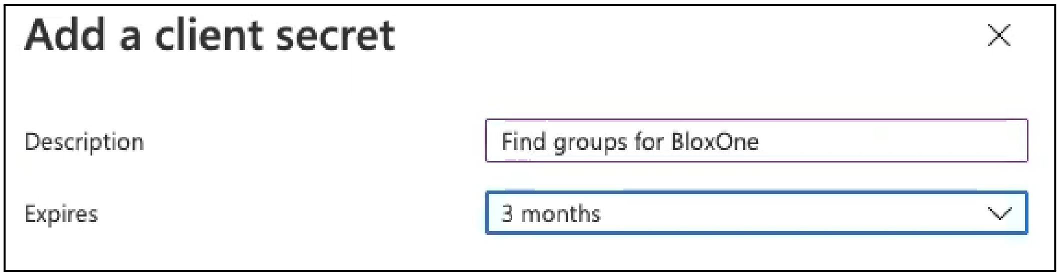
16. Click **New client secret** under the Client secrets header.



Client secrets

A secret string that the application

17. In the Add a client secret panel, add a Description and set an expiration date.



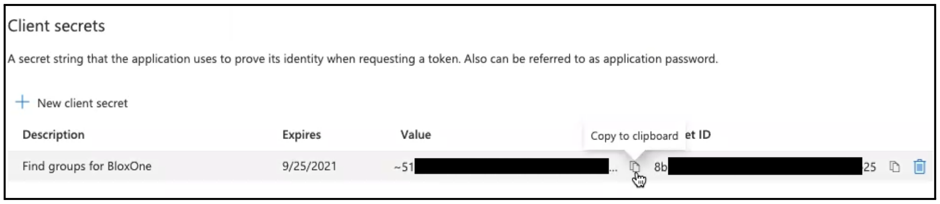
Add a client secret

Description: Find groups for BloxOne

Expires: 3 months

18. Click **Add** to confirm the creation of the new Client secret.

19. Copy the Value of the new Client secret, save this string in a text file for later.

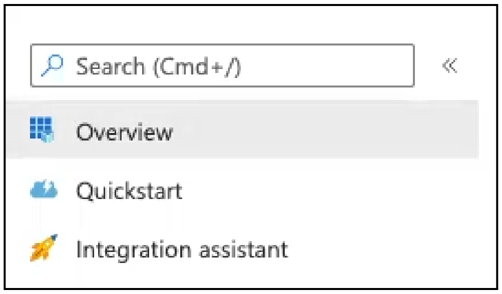


Client secrets

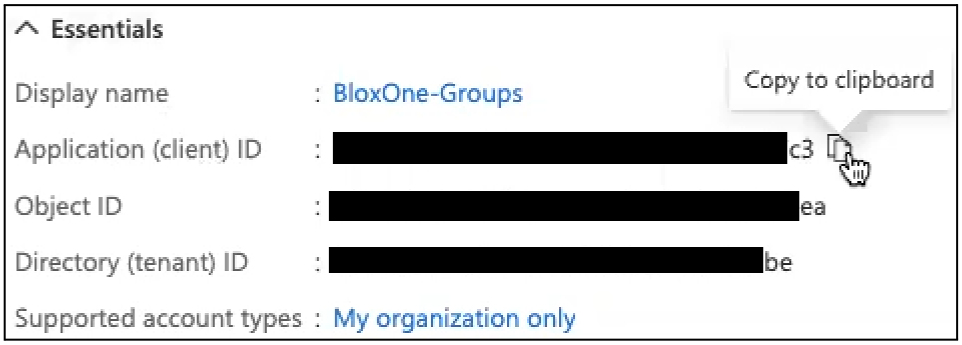
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	et ID
Find groups for BloxOne	9/25/2021	~51[redacted]...	8b[redacted]25

20. Click **Overview** in the left navigation panel.



21. On the Overview page, copy the **Application** (client) ID. Save this string to a text file.



Essentials

Display name : BloxOne-Groups

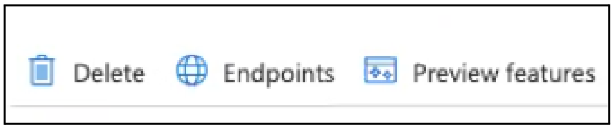
Application (client) ID : [redacted]c3

Object ID : [redacted]ea

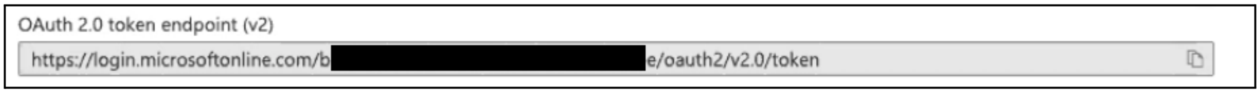
Directory (tenant) ID : [redacted]be

Supported account types : My organization only

22. On the Overview page, click **Endpoints**.



23. Then, copy the OAuth 2.0 token endpoint (v2) url located in the panel that is revealed. Save this URL to a text file for use later.



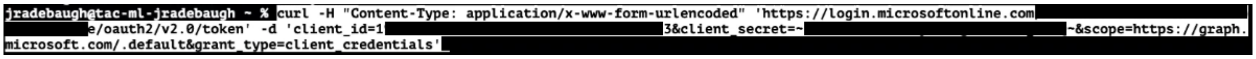
OAuth 2.0 token endpoint (v2)

https://login.microsoftonline.com/b[redacted]e/oauth2/v2.0/token

24. Construct a curl call with the Client secret id value (page 17, step 19), Application (client) ID (page 17, step 21), and the OAuth 2.0 token endpoint (v2) (Acquired on page 17, step 23). *Note: Replace all text contained within the < > characters, < > inclusive.*

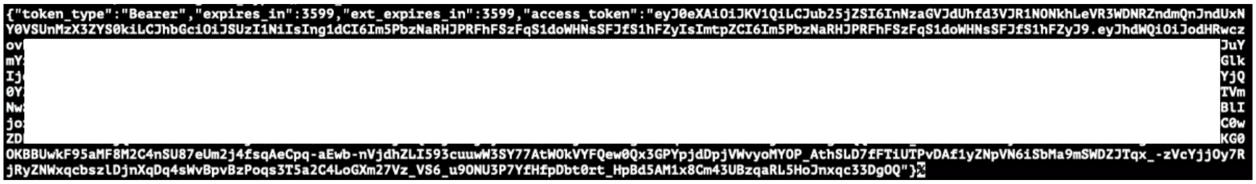
```
curl -H "Content-Type: application/x-www-form-urlencoded" '<OAuth 2.0 token endpoint (v2>' -d 'client_id=<Application (client) ID>&client_secret=<Client secret id value>&scope=https://graph.microsoft.com/.default&grant_type=client_credentials'
```

25. Access a command line interface with curl installed, then input the curl command.



```
jradebaugh@tac-ml-jradebaugh ~ % curl -H "Content-Type: application/x-www-form-urlencoded" 'https://login.microsoftonline.com[redacted]
e/oauth2/v2.0/token' -d 'client_id=1[redacted]3&client_secret=~[redacted]~&scope=https://graph.
microsoft.com/.default&grant_type=client_credentials'
```

26. Acquire the access_token from the output. *Note: Save this token to a text file for use later. Only copy the text after "access_token":" and remove the final quotation mark and curly bracket from the string. i.e. in the example screenshot the access token would start with eyJ0eX… and end with ...DgOQ.*

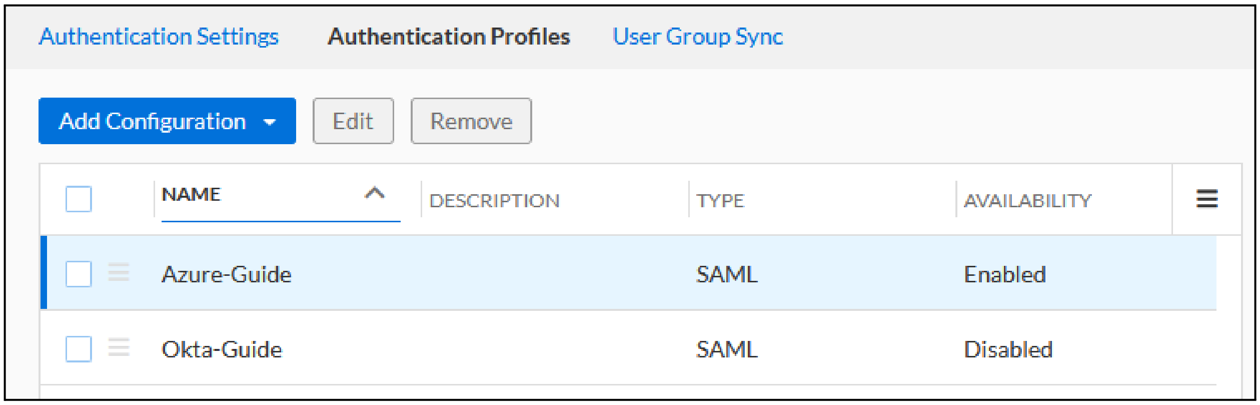


```
{"token_type":"Bearer","expires_in":3599,"ext_expires_in":3599,"access_token":"eyJ0eXAiOiJKV1QiLCJub25jZSI6InNzaGVJdUhfd3VJR1NONkhLeVR3WDNRZndmQnJndUxN
Y0VSUnMzX3ZYS0kiLCJhbGciOiJSUzI1NiIsIng1dCI6Im5PbzNaRHJPRFhFSzFqS1doWHNsSFJfS1hFZyIsImtpZCI6Im5PbzNaRHJPRFhFSzFqS1doWHNsSFJfS1hFZyJ9.eyJhdWQiOiJodHRwcz
ov [redacted]                                                                                                                                      JuY
mY                                                                                                                                                 Glk
Ij                                                                                                                                                 YjQ
0Y                                                                                                                                                 TVm
Nw                                                                                                                                                 BlI
jo                                                                                                                                                 C0w
ZD                                                                                                                                                 KG0
OKBBUwkF95aMF8M2C4nSU87eUm2j4fsqAeCpq-aEwb-nVjdhZLI593cuuwW3SY77AtWOkVYFQew0Qx3GPYpjdDpjVWvyoMYOP_AthSLD7fFTiUTPvDAf1yZNpVN6iSbMa9mSWDZJTqx_-zVcYjjOy7R
jRyZNWxqcbszlDjnXqDq4sWvBpvBzPoqs3T5a2C4LoGXm27Vz_VS6_u9ONU3P7YfHfpDbt0rt_HpBd5AM1x8Cm43UBzqaRL5HoJnxqc33DgOQ"}%
```

Sync Azure Active Directory Groups with BloxOne

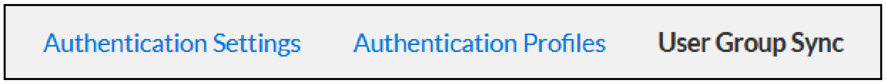
To sync the Azure Active Directory groups with BloxOne, perform the following steps:

1. Navigate to the Infoblox CSP's Access Authentication page that was accessed on page 11. *Note: Keep the Azure Portal open in another tab or browser.*

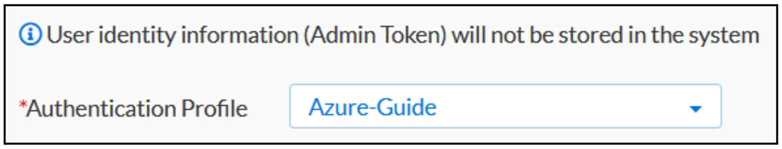


□	NAME	DESCRIPTION	TYPE	AVAILABILITY
□	Azure-Guide		SAML	Enabled
□	Okta-Guide		SAML	Disabled

2. On the Access Authentication page, click the **User Group Sync** tab.



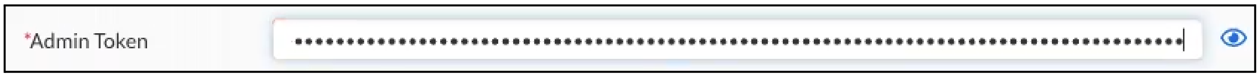
3. On the User Group Sync, select the Authentication Profile that was created earlier in this guide.



User identity information (Admin Token) will not be stored in the system

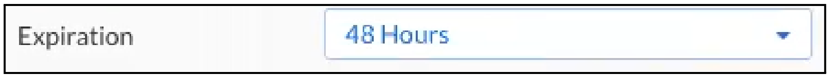
*Authentication Profile: Azure-Guide

4. In the Admin Token text field, input the **access_token acquired** in step 26 on page 18.



*Admin Token: ••

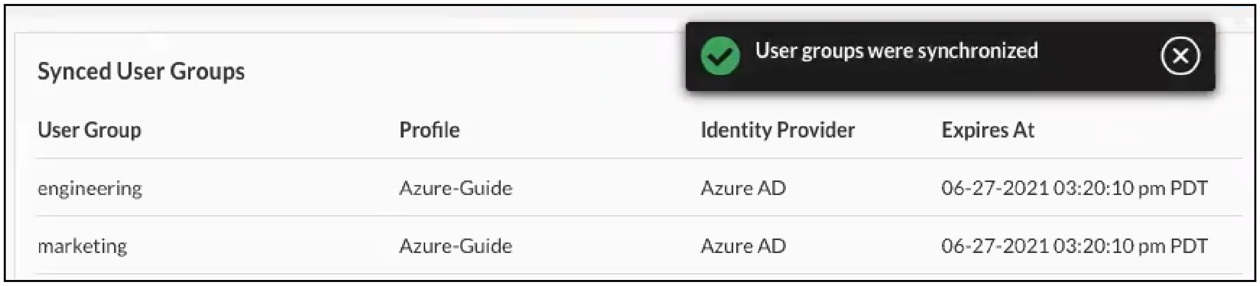
5. (Optional) If desired, change the Expiration for the sync. This setting designates the period of time the CSP holds the user group data. *Note: If the IdP in your authentication profile renames a user group or deletes one, you must resynchronize the user groups to get the latest Information. For more details on this setting, see the Synchronizing User Groups doc on the Infoblox Documentation portal.*



Expiration: 48 Hours

6. Click **Sync** to sync groups between Azure Active Directory and BloxOne.

7. After several seconds you will see groups from Azure Active Directory populate in the Synced User Groups panel.



Synced User Groups

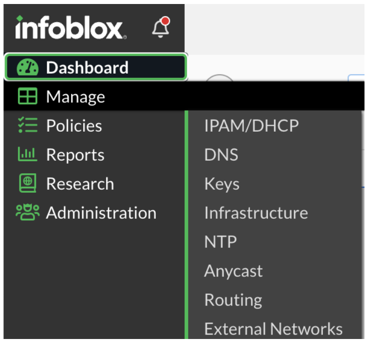
User groups were synchronized

User Group	Profile	Identity Provider	Expires At
engineering	Azure-Guide	Azure AD	06-27-2021 03:20:10 pm PDT
marketing	Azure-Guide	Azure AD	06-27-2021 03:20:10 pm PDT

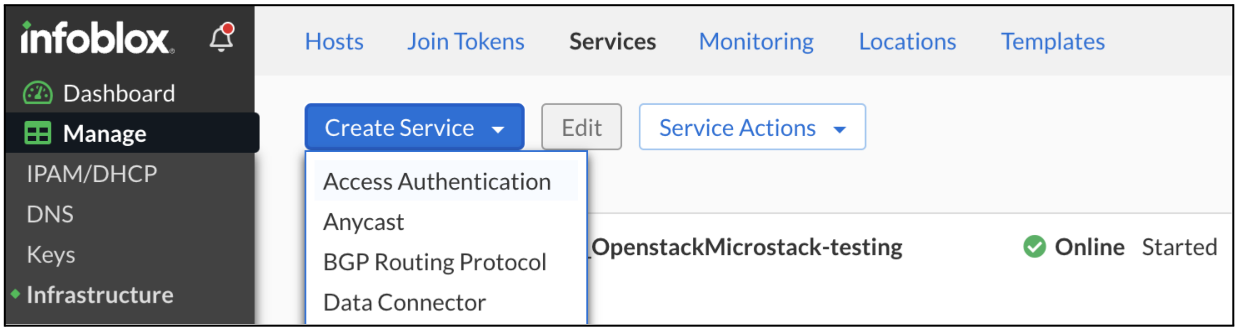
Create the Access Authentication Service

To create the Access Authentication service and attach it to a Host, perform the following steps:

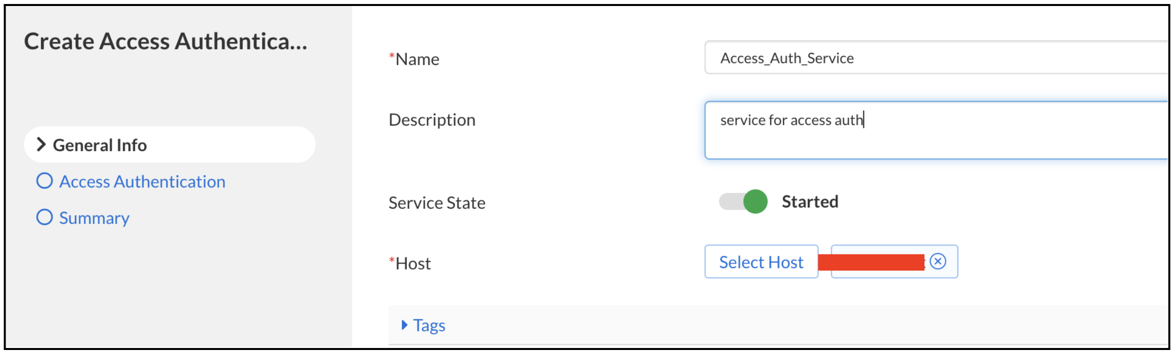
1. On the Infoblox CSP access the Infrastructure page. Highlight **Manage**, then click **Infrastructure**.



2. Navigate to **Services** tab, click **Create Service** and select **Access Authentication**.



3. Under General Info, enter the **Name**, **Description** and select a **Host** on which this service will be associated with. Click Next.



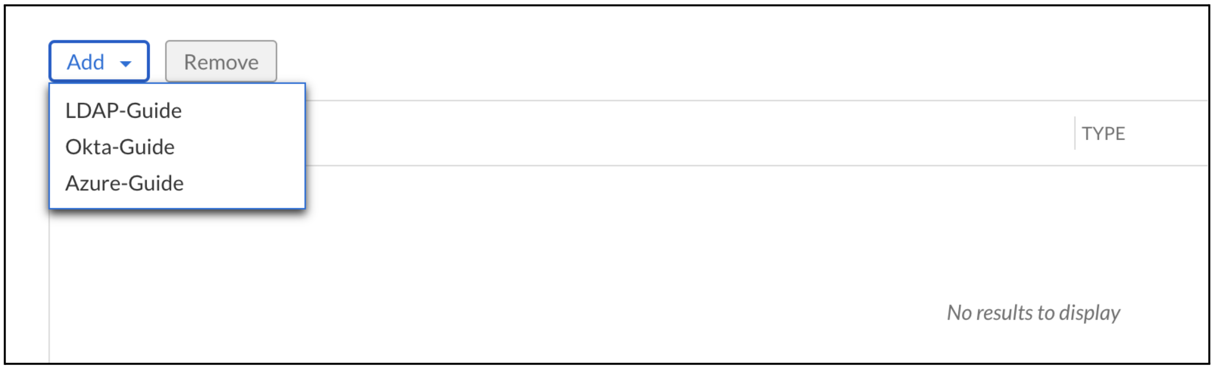
*Name: Access_Auth_Service

Description: service for access auth

Service State: Started

*Host: [redacted]

4. Under Access Authentication, click **Add** then click the configured Azure Access Authentication IdP in the list that is revealed.



No results to display

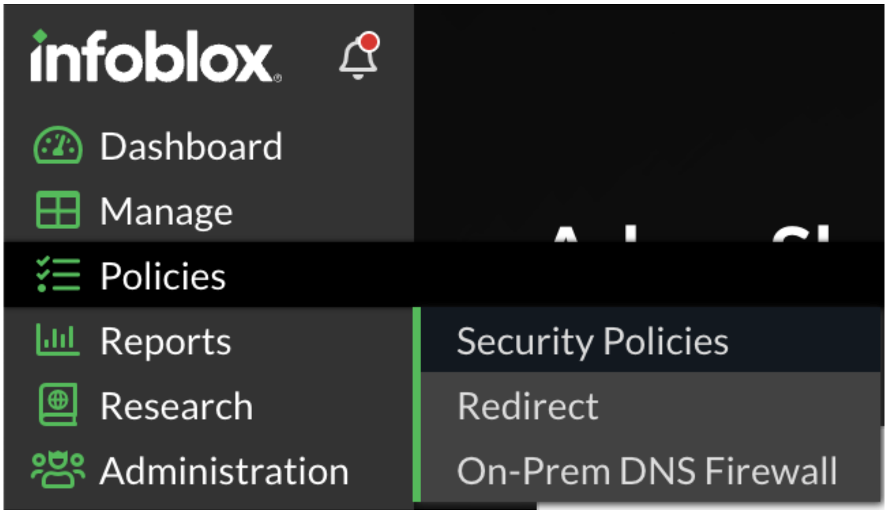
5. Click **Finish**.

6. Click **Save & Close** to confirm the changes to the Access Authentication service.

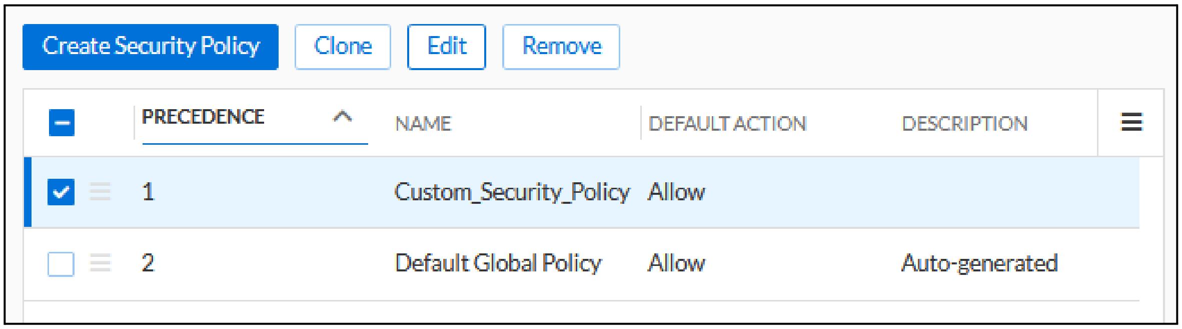
Add User Groups to a BloxOne Security Policy

Once User Groups are synced between BloxOne and the Azure Active Directory, you can apply security policies to a User Group. Perform the following steps to apply a security policy to a User Group.

1. On the Infoblox CSP access the Security Policies page. Highlight **Policies**, then click **Security Policies.**

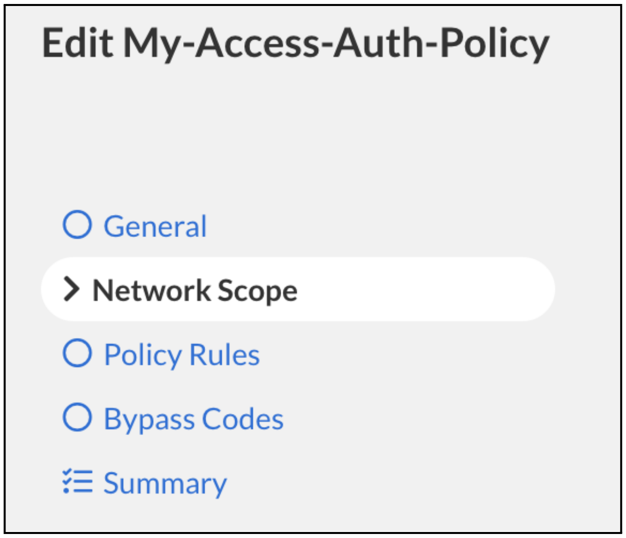


2. Click the checkbox associated with an existing Security Policy that you would like to assign an Azure Active Directory user group to. Then, click **Edit**. *Note: Create a new Security policy if desired.*

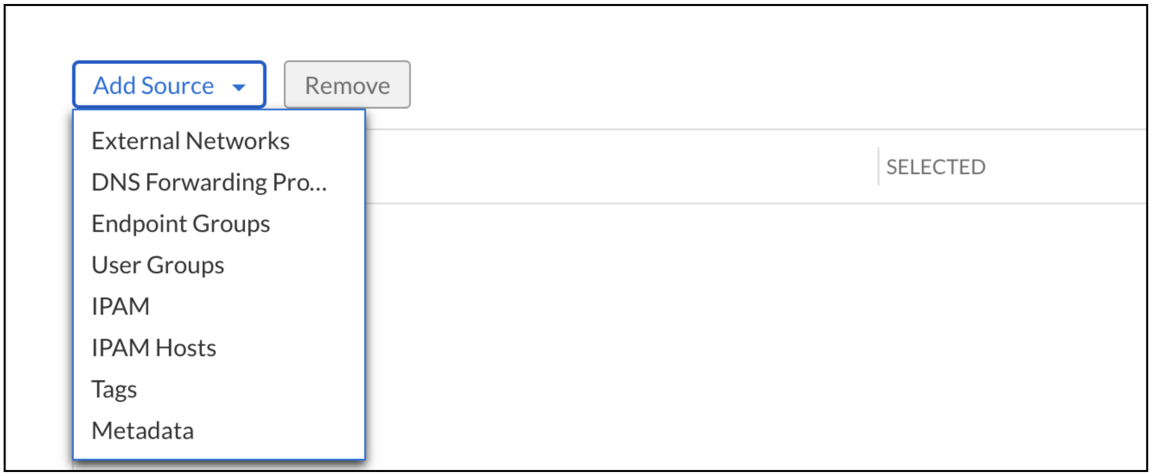


	PRECEDENCE	NAME	DEFAULT ACTION	DESCRIPTION
☑	1	Custom_Security_Policy	Allow	
□	2	Default Global Policy	Allow	Auto-generated

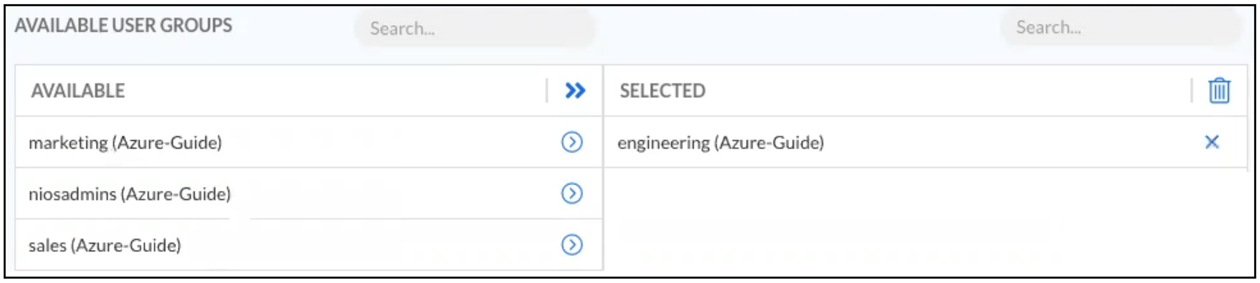
3. In the Edit Security Policy panel, click **Network Scope** located in the left navigation panel.



4. On the Network Scope panel, click the **Add Source** button. Then, click **User Groups** in the list that is revealed.



5. Select any desired User Groups to add to the Security Policy.



AVAILABLE	SELECTED
marketing (Azure-Guide)	engineering (Azure-Guide)
niosadmins (Azure-Guide)	
sales (Azure-Guide)	

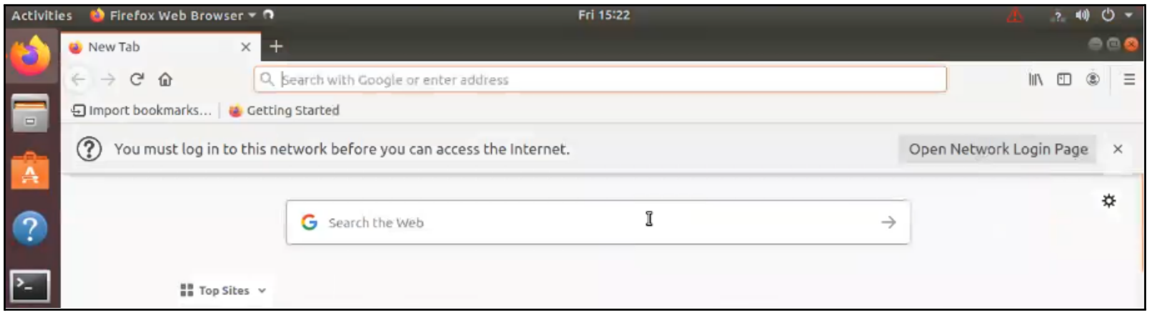
6. Click **Save** to confirm the addition of the User Groups.

7. Click **Finish** to confirm the changes to the Security Policy.

Test the Access Authentication with Azure Configuration

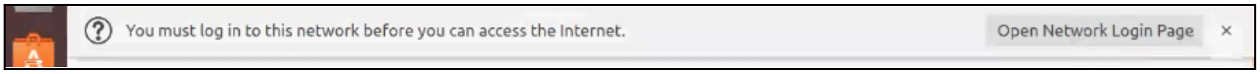
To test the configuration perform the following steps:

1. Access a device that is utilizing the previously configured BloxOne Host as its primary DNS. Open a Web browser on the client.



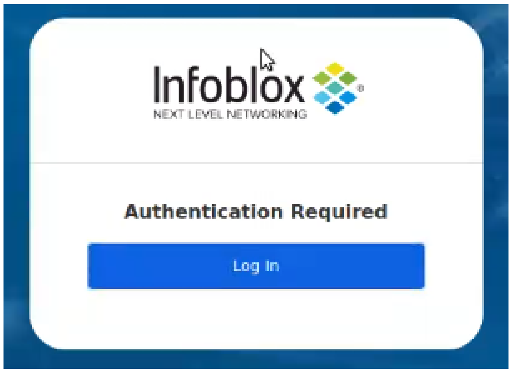
You must log in to this network before you can access the Internet.

- The web browser on the client will prompt the user to log in via IdP. Shown is Firefox's prompt.



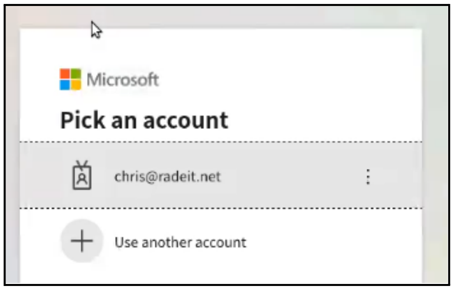
You must log in to this network before you can access the Internet.

2. By clicking the prompt the user will be redirected to a page requesting the user Log In. Click Log In to login.



Authentication Required

3. The user will be redirected to login via Azure's Microsoft Online portal. Add an account, or select the correct account if it is listed.

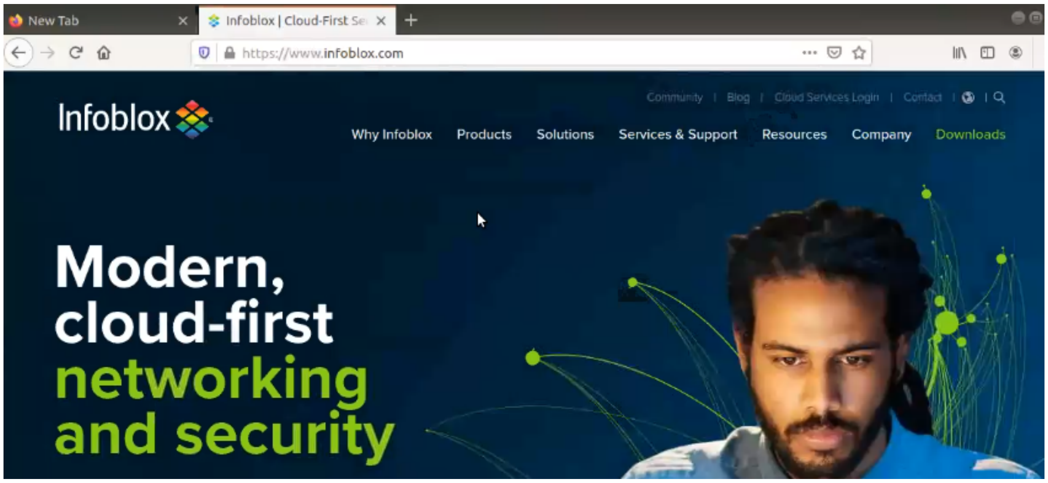


Pick an account

chris@radeit.net

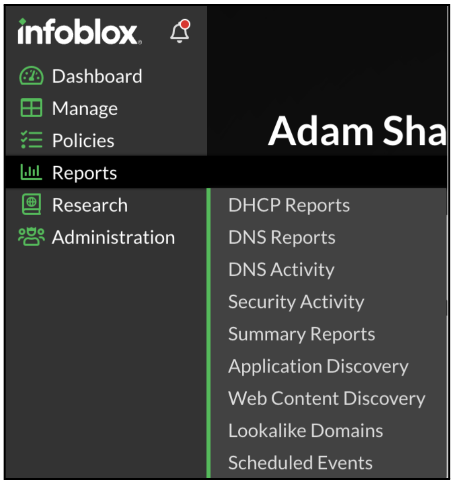
Use another account

- After a successful login, the user will be able to access the Internet.

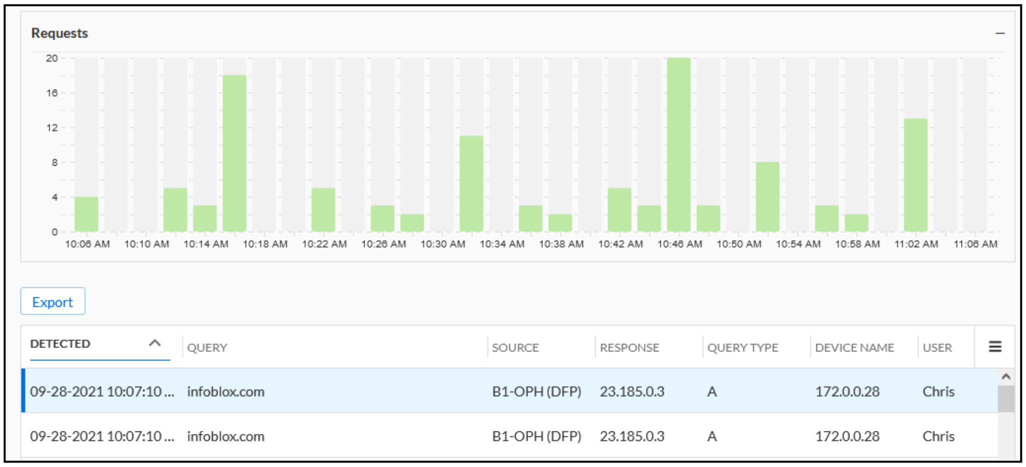


New Tab
Infoblox | Cloud-First Se
https://www.infoblox.com
Infoblox
Community | Blog | Cloud Services Login | Contact
Why Infoblox
Products
Solutions
Services & Support
Resources
Company
Downloads
Modern, cloud-first networking and security

4. To view the user's activity in the Infoblox CSP access BloxOne's Reporting.



- Shown are the DNS Activity reports. Observe the User Chris representing the user Chris that was synced with BloxOne from the Azure Active Directory. Note that the User field is visible in the DNS Activity, Security Activity, and the Security reports pages.



DETECTED	QUERY	SOURCE	RESPONSE	QUERY TYPE	DEVICE NAME	USER
09-28-2021 10:07:10 ...	infoblox.com	B1-OPH (DFP)	23.185.0.3	A	172.0.0.28	Chris
09-28-2021 10:07:10 ...	infoblox.com	B1-OPH (DFP)	23.185.0.3	A	172.0.0.28	Chris

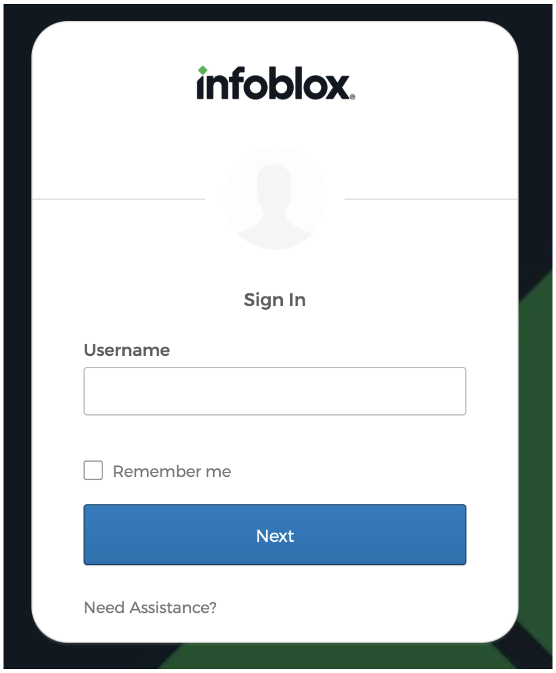
BloxOne Access Authentication with Okta

This portion of the deployment guide covers how to configure BloxOne to work with Okta as an IdP.

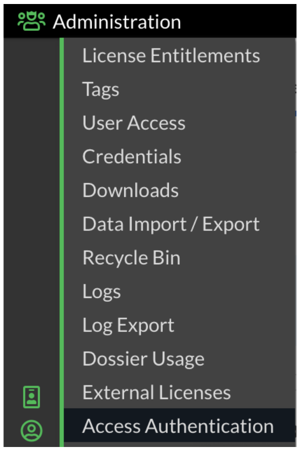
Prepare the BloxOne Authentication Profile

To configure BloxOne to work with Okta as its IdP you must first create a SAML Authentication profile and acquire service provider URLs. To acquire these URLs, perform the following steps:

1. Access the Infoblox CSP at csp.infoblox.com, and log in with your credentials.

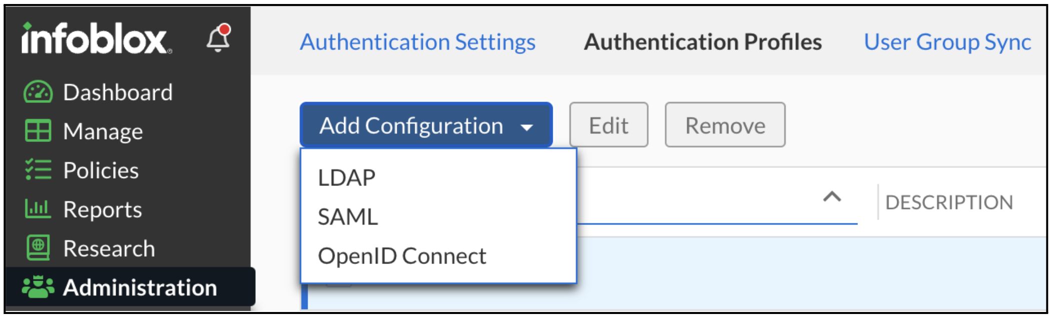


2. On the left navigation panel, highlight **Administration**. Then, click **Access Authentication** in the list that is revealed.



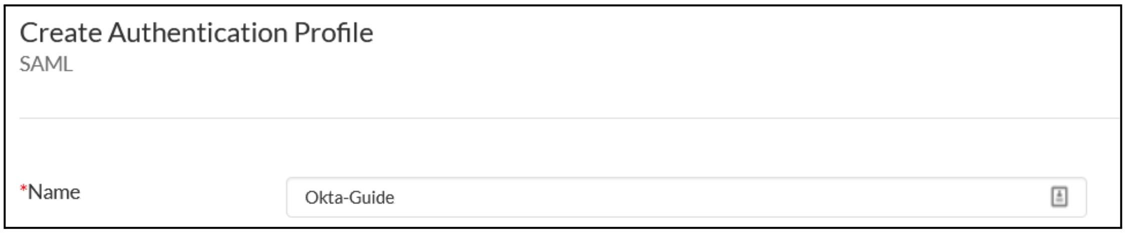
3. On the Access Authentication page, click the **Authentication Profiles** tab.

4. On the Authentication Profiles page click **Add Configuration**. Then, click **SAML** in the list that is revealed.



5. On the Create Authentication Profile panel perform the following steps:

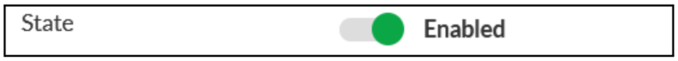
   - Give the new Authentication Profile a **Name**.



Create Authentication Profile
SAML

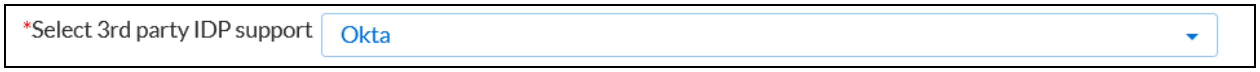
*Name Okta-Guide

   - Enable the Authentication profile by clicking the **State** toggle switch.



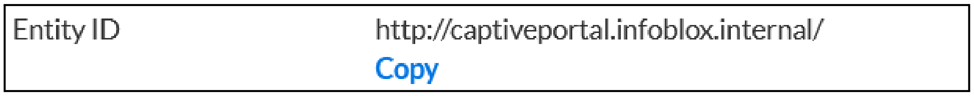
State Enabled

   - Select Okta for the **Select 3rd party IDP support** by using the dropdown.



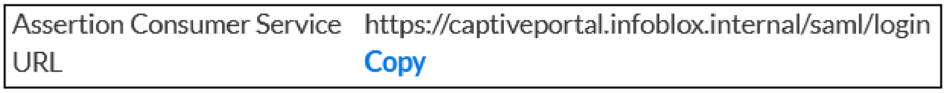
*Select 3rd party IDP support Okta

   - Copy the **Entity ID** and save it to a text file for use later.



Entity ID http://captiveportal.infoblox.internal/

   - Copy the **Assertion Consumer Service URL** and save it to a text file for use later.

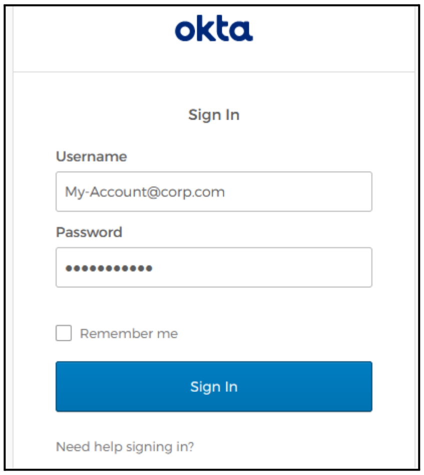


Assertion Consumer Service URL https://captiveportal.infoblox.internal/saml/login

Create an Okta Application and Finalize the Creation of the BloxOne Authentication Profile

In order to allow Okta to communicate with BloxOne you must create an application, acquire multiple URLs, and input this data into the BloxOne Authentication Profile. To create the Okta Application, acquire the associated URLs and finalize the creation of the BloxOne Authentication profile, perform the following steps:

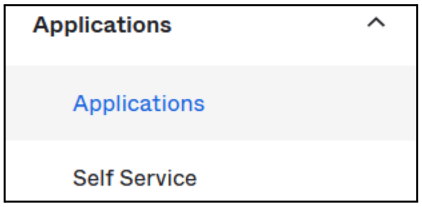
1. Access the admin web interface of Okta, and log in. *Note: Keep the Infoblox CSP and the Create Authentication Profile page open in another tab or browser*.



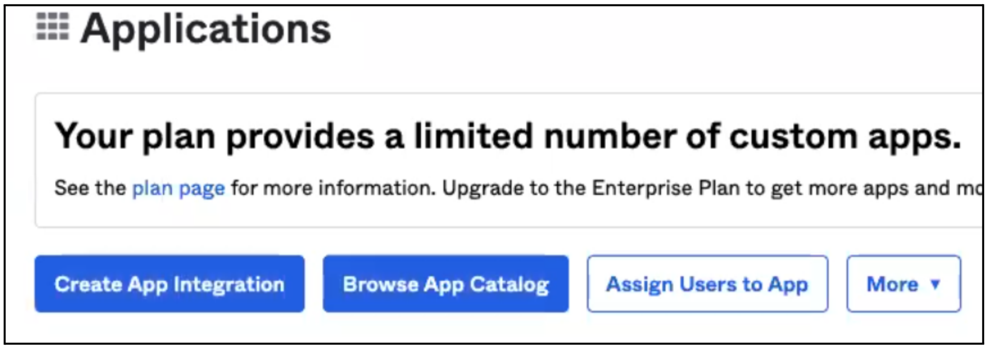
Username: My-Account@corp.com

Password: ••••••••••••

2. Once logged in to the Okta admin interface, expand Applications, then click Applications in the list that is revealed.



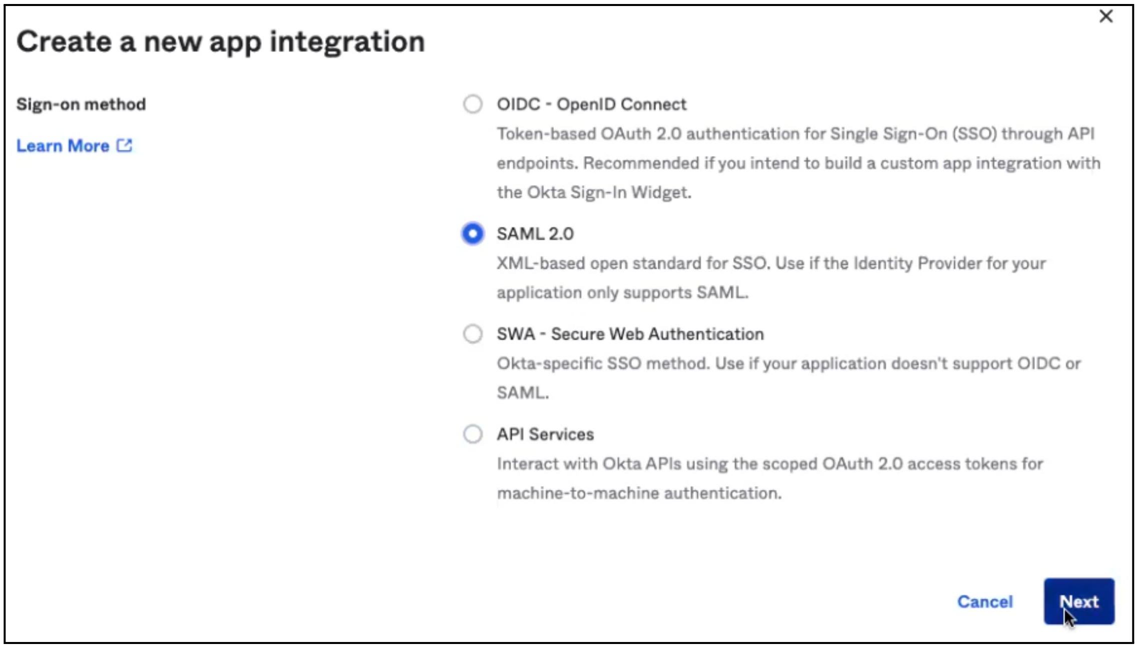
3. On the Applications page, click **Create App Integration**.



Your plan provides a limited number of custom apps.

See the plan page for more information. Upgrade to the Enterprise Plan to get more apps and mo

4. On the Create a new app integration panel, click the bubble associated with SAML 2.0, then click **Next**.



Create a new app integration

Sign-on method

Learn More

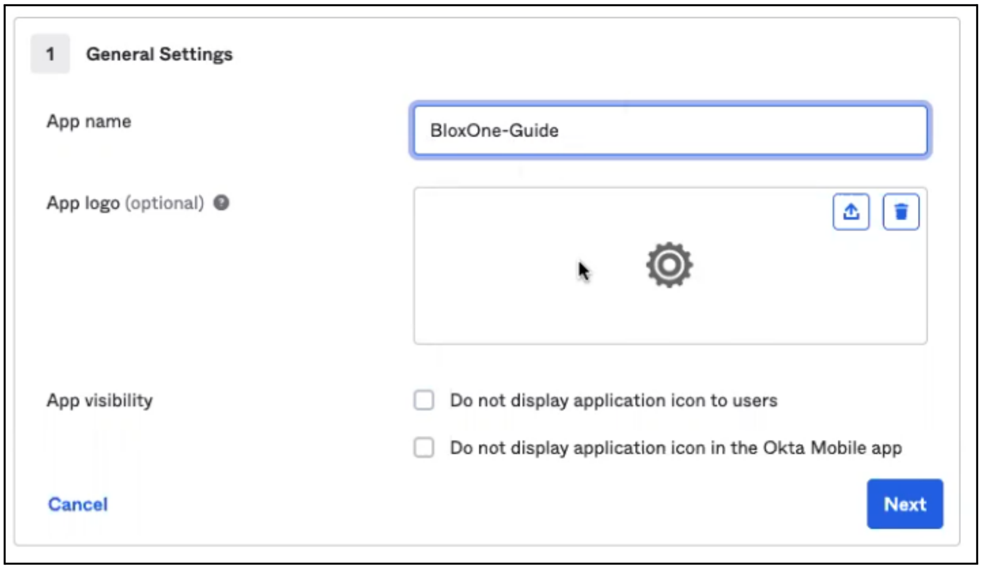
○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

● 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.

5. On the first step of the Create SAML Integration page, give the App a name by inputting a name in the App name text field. Then, click **Next**. *Note: If desired, you may also give the app a logo and adjust app visibility settings.*



1 General Settings

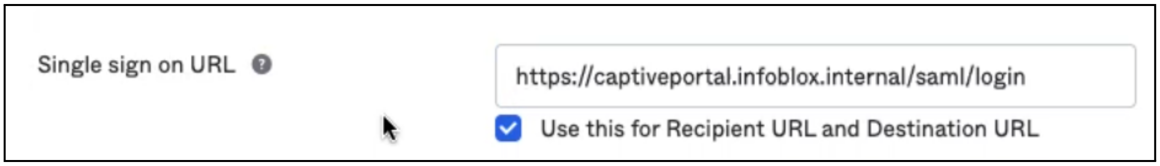
App name: BloxOne-Guide

App logo (optional)

App visibility
□ Do not display application icon to users
□ Do not display application icon in the Okta Mobile app

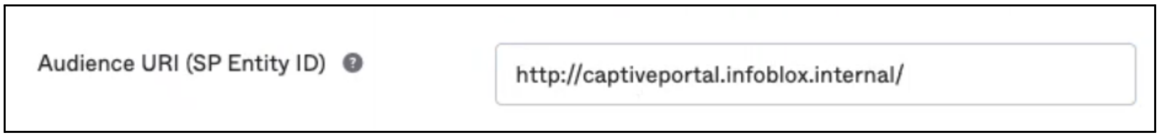
6. On step 2 of the Create SAML Integration panel perform the following steps:

   ○ Input the Single sign on URL acquired from the Infoblox CSP (see step 5 on page 27, named Assertion Consumer Service URL from the Create Authentication Profile panel on the Infoblox CSP).

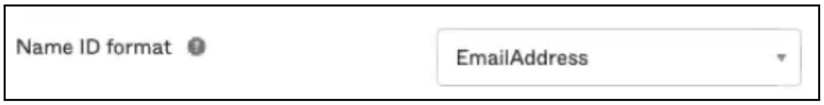

Single sign on URL: https://captiveportal.infoblox.internal/saml/login

☑ Use this for Recipient URL and Destination URL

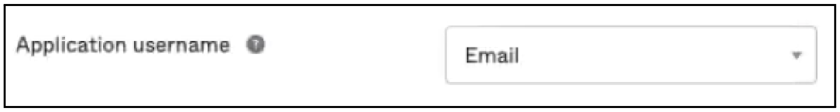
- Input the Audience URI (SP Entity ID) acquired from the Infoblox CSP (see step 5 on page 27, named Entity ID from the Create Authentication Profile panel on the Infoblox CSP).


Audience URI (SP Entity ID): http://captiveportal.infoblox.internal/

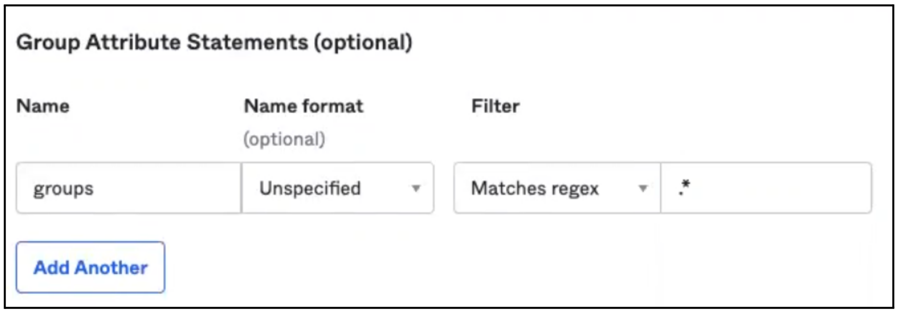
- Change the Name ID format to **EmailAddress**.


Name ID format: EmailAddress

- Change the Application username to **Email**.


Application username: Email

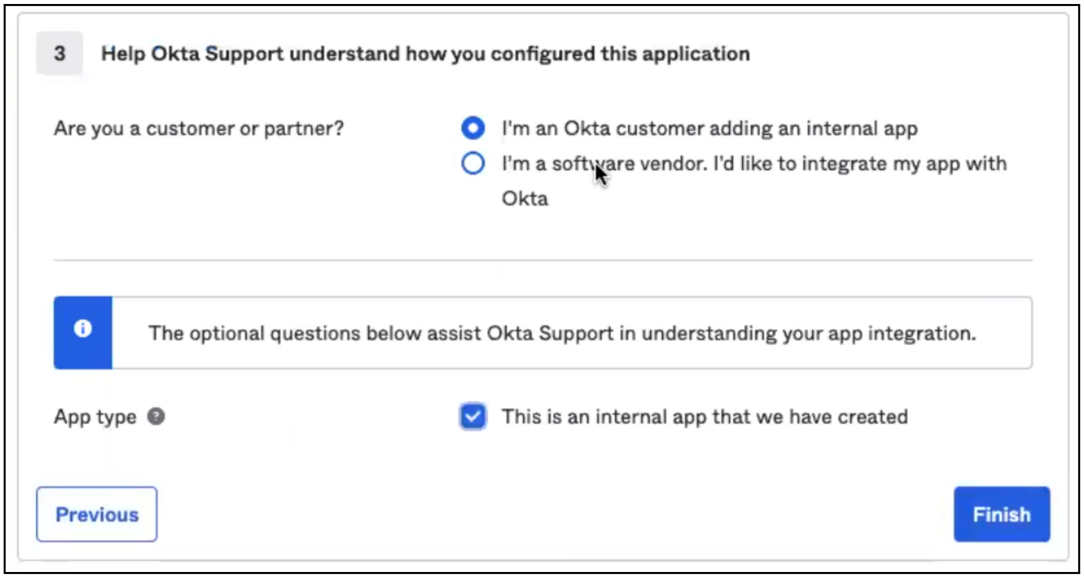
- For the Group Attribute Statements (optional) section, assign the Name as groups, and input the characters .* as the filter.


Group Attribute Statements (optional)

Name	Name format (optional)	Filter	
groups	Unspecified	Matches regex	.*

- Click **Next**.

7. Fill out the Feedback step if desired. Then. click **Finish** to confirm the creation of the application.



3 Help Okta Support understand how you configured this application

Are you a customer or partner?

● I'm an Okta customer adding an internal app

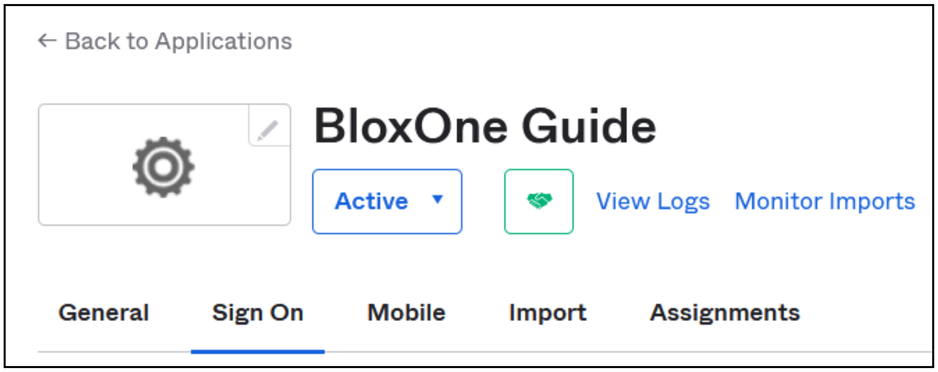
○ I'm a software vendor. I'd like to integrate my app with Okta

The optional questions below assist Okta Support in understanding your app integration.

App type

☑ This is an internal app that we have created

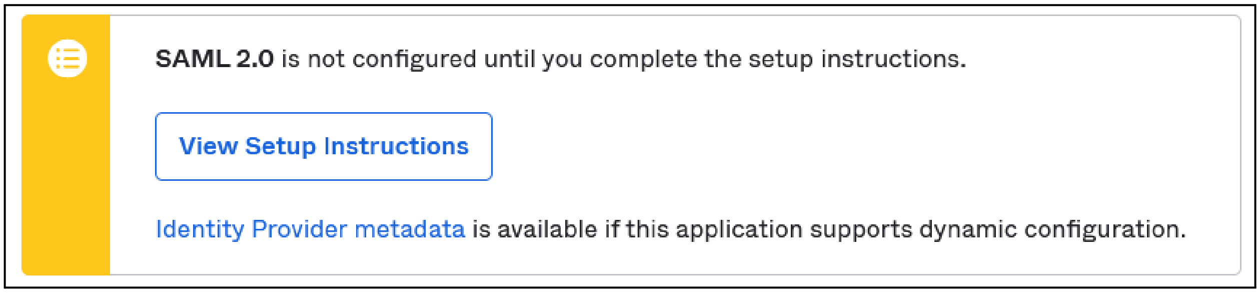
8. On the newly created application's page, navigate to the **Sign on** tab.



← Back to Applications

BloxOne Guide

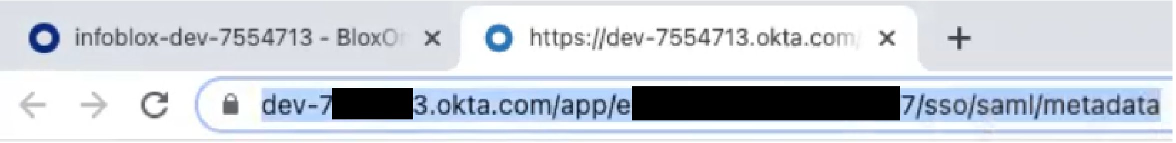
9. In the sections panel, click the **Identity Provider metadata** link.



SAML 2.0 is not configured until you complete the setup instructions.

Identity Provider metadata is available if this application supports dynamic configuration.

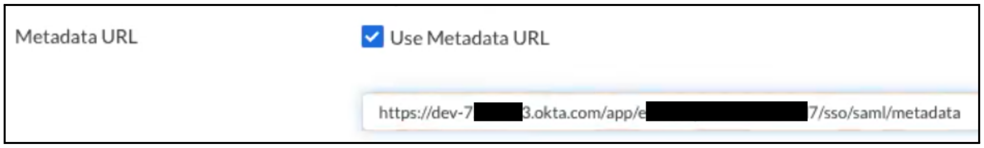
10. Copy the link that the previous step navigates to. Save this link to a text file for use later.



dev-7[redacted]3.okta.com/app/e[redacted]7/sso/saml/metadata

11. Navigate back to the Infoblox CSP and the **Create Authentication Profile** panel.

12. Under the Identity Provider Details header, input the Metadata URL by clicking the checkbox, and inputting the URL acquired in step 10.

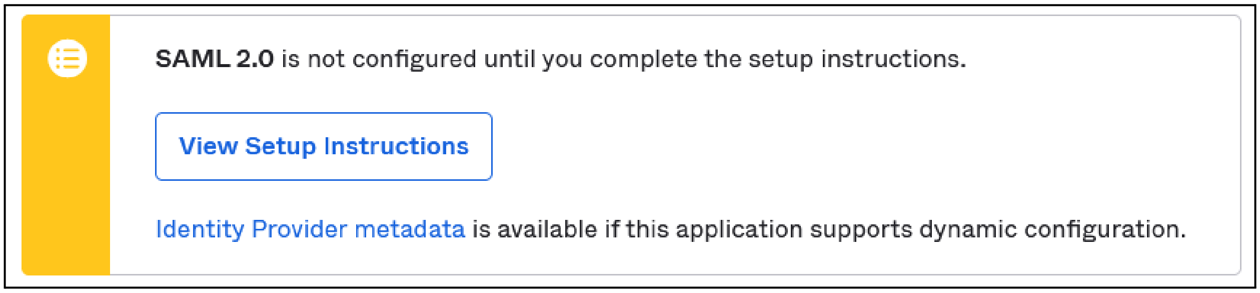


Metadata URL

☑ Use Metadata URL

https://dev-7[redacted]3.okta.com/app/e[redacted]7/sso/saml/metadata

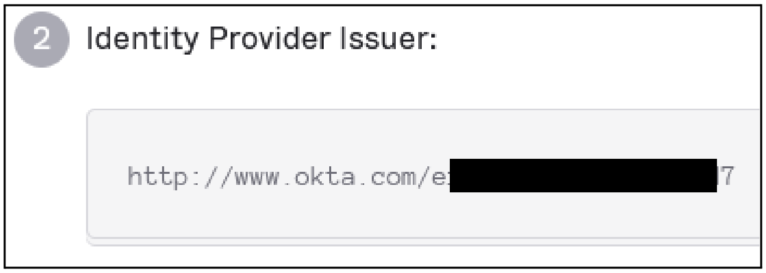
13. (Optional) If desired, you may use the IDP Issuer URI and IDP Single Sign-On URL instead of the Metadata URL. These can be acquired by clicking on View Setup Instructions on the application's page, in the Sign on methods panel. If you would prefer to use the Metadata URL, skip to step 19.



SAML 2.0 is not configured until you complete the setup instructions.

Identity Provider metadata is available if this application supports dynamic configuration.

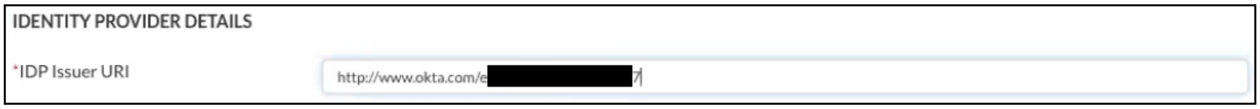
- On the How To Configure… page, copy the Identity Provider Issuer URL.



2 Identity Provider Issuer:

```
http://www.okta.com/e[redacted]7
```

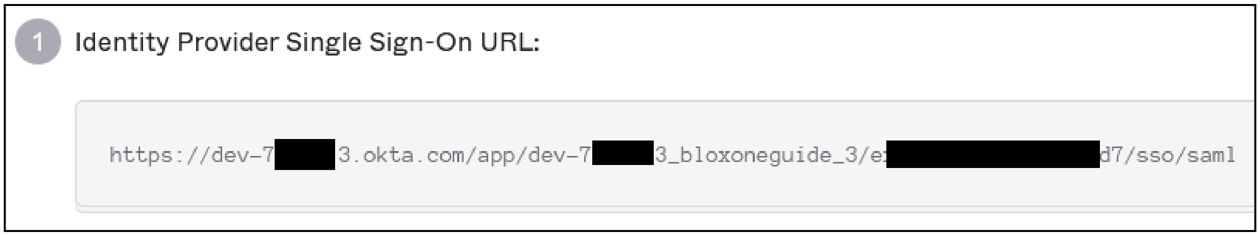
- On the Infoblox CSP, paste the URL into the IDP Issuer URI text box.



IDENTITY PROVIDER DETAILS

*IDP Issuer URI: http://www.okta.com/e[redacted]7

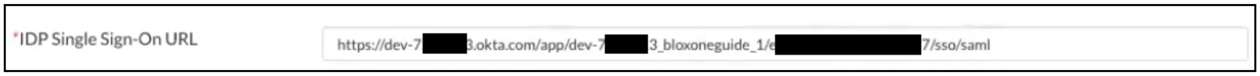
- On the How To Configure… page of Okta, copy the Identity Provider Single Sign-On URL.



1 Identity Provider Single Sign-On URL:

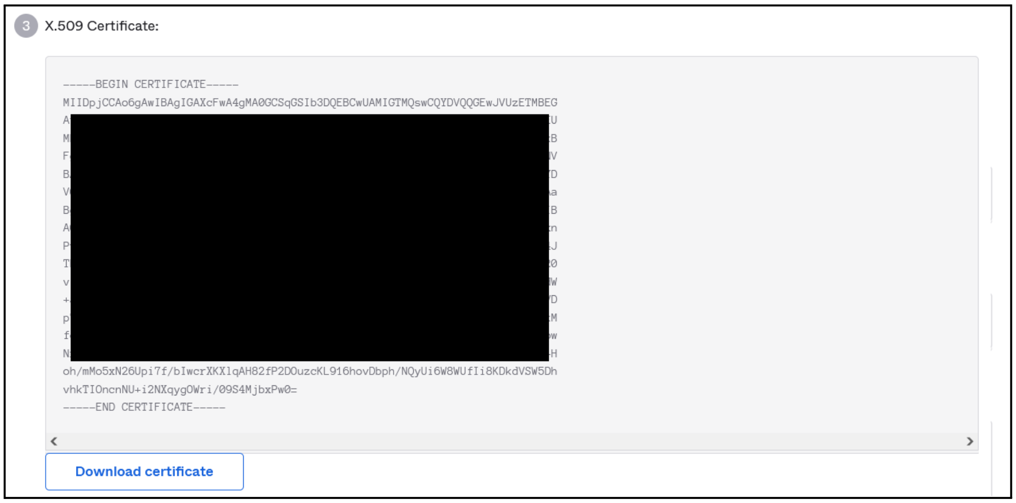
```
https://dev-7[redacted]3.okta.com/app/dev-7[redacted]3_bloxoneguide_3/e[redacted]d7/sso/saml
```

- On the Infoblox CSP, Paste the URL into the IDP Single Sign-On URL text box.



*IDP Single Sign-On URL: https://dev-7[redacted]3.okta.com/app/dev-7[redacted]3_bloxoneguide_1/e[redacted]7/sso/saml

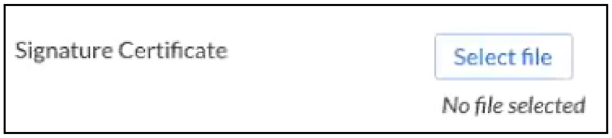
- Download the Certificate from Okta by clicking the **Download certificate** button. Save the certificate to a place you will remember.



3 X.509 Certificate:

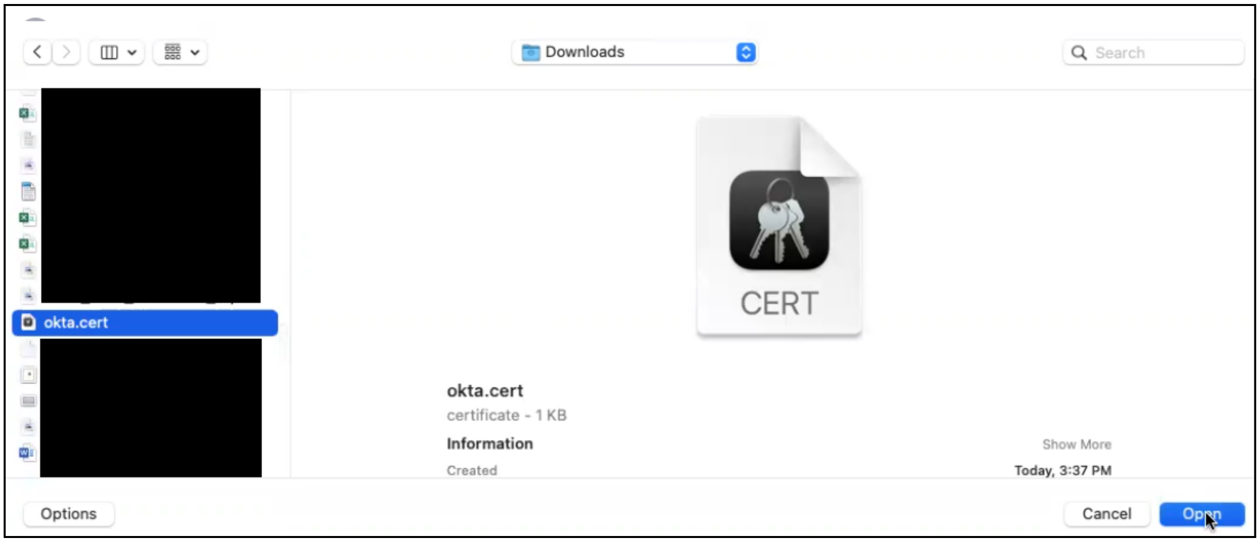
```
-----BEGIN CERTIFICATE-----
MIIDpjCCAo6gAwIBAgIGAXcFwA4gMA0GCSqGSIb3DQEBCwUAMIGTMQswCQYDVQQGEwJVUzETMBEG
[redacted]
oh/mMo5xN26Upi7f/bIwcrXKXlqAH82fP2DOuzcKL916hovDbph/NQyUi6W8WUfIi8KDkdVSW5Dh
vhkTIOncnNU+i2NXqygOWri/09S4MjbxPw0=
-----END CERTIFICATE-----
```

- On the Infoblox CSP, Click the **Select file** button that is associated with the Signature Certificate.



Signature Certificate: No file selected

- Locate and select the certificate that was acquired in step 18e.



[redacted]

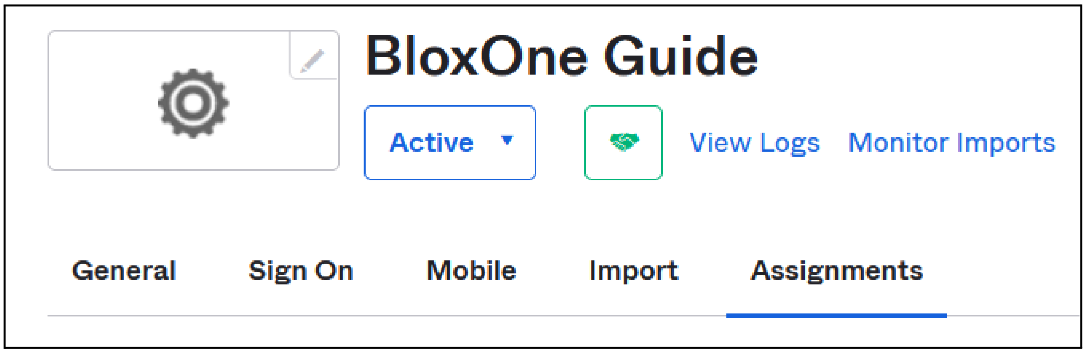
[redacted]

14. Finally, click **Save & Close** to confirm the creation of the Authentication Profile.

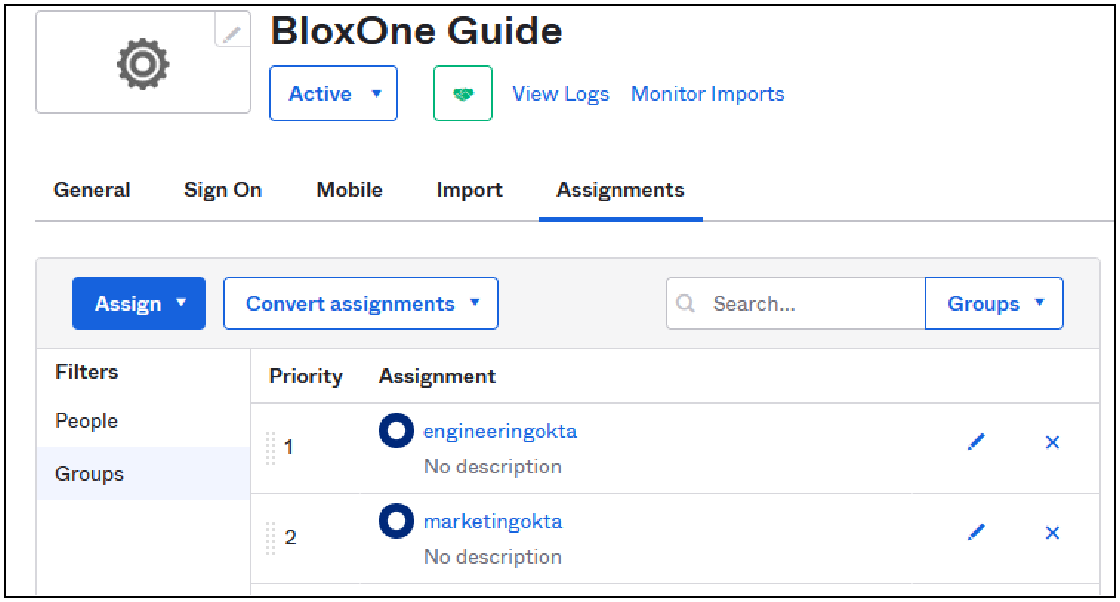
Assign Groups to the Okta Application

To allow users to login to the new application, you must first assign groups to your application. To accomplish this, perform the following steps:

1. Access your Okta Admin portal while keeping the Infoblox CSP open. On the App that was created steps 3-7 on pages 28-31, click the Assignments tab.

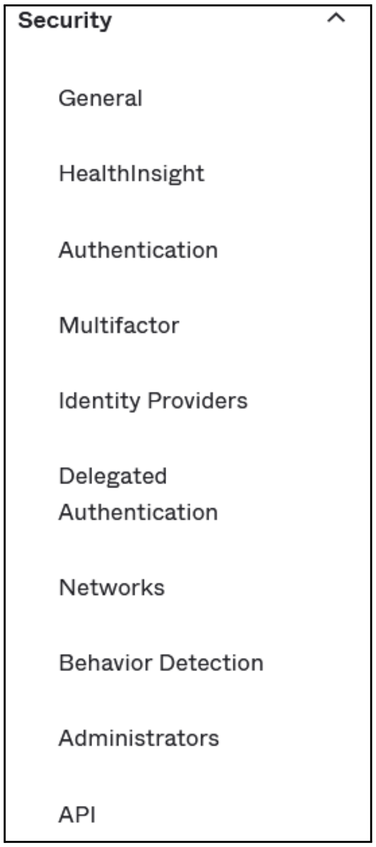


2. Click on **Groups** in the application's left hand navigation panel. Here you may assign any desired Groups to this application.

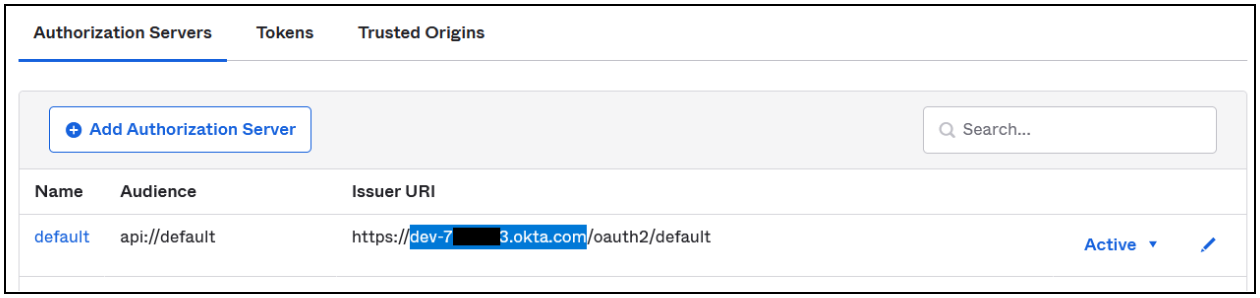


Priority	Assignment
1	engineeringokta No description
2	marketingokta No description

3. To Sync the people and/or groups to BloxOne you must acquire an API key and an IdP Domain. Click Security in the left navigation panel. Then, click **API** in the list that is revealed.

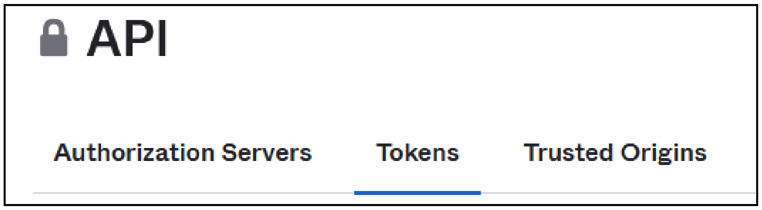


4. On the API page's Authorization Servers tab Copy the Issuer URL and remove the text https:// and /oauth2/default from the URL. Copy and Paste this URL to a text file so it can be used later.

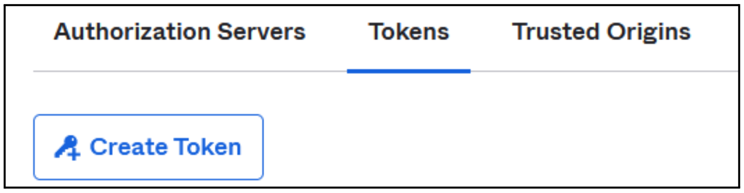


Name	Audience	Issuer URI
default	api://default	https://dev-7[redacted]3.okta.com/oauth2/default

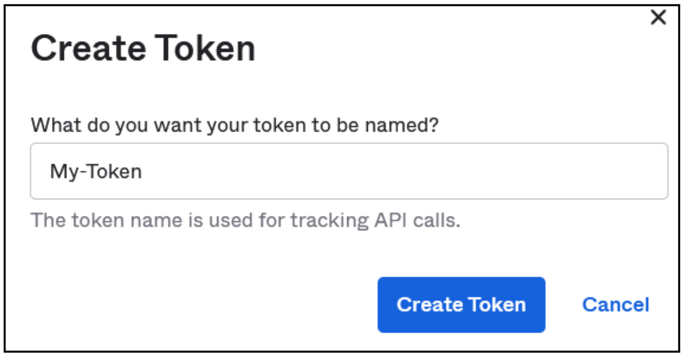
5. On the API page, navigate to the Tokens tab.



6. On the Tokens tab of the API page, click the **Create Token** button.



7. Give the Token a name, then click **Create Token**.

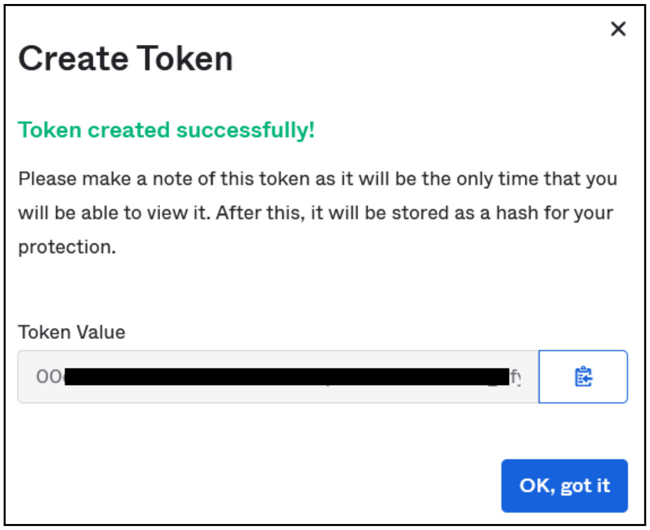


What do you want your token to be named?

My-Token

The token name is used for tracking API calls.

8. Copy and paste the Token to a text file for use later. Then, click **OK, got it** to continue.



Create Token

Token created successfully!

Please make a note of this token as it will be the only time that you will be able to view it. After this, it will be stored as a hash for your protection.

Token Value

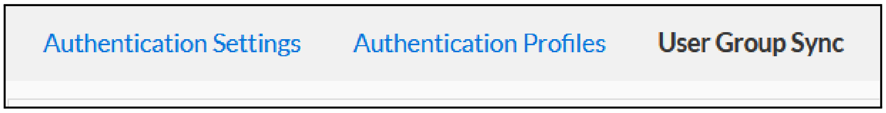
00[redacted]

Sync Groups to BloxOne from the Okta Application

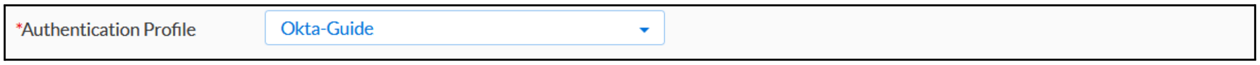
To sync groups that were assigned to the Okta application, perform the following steps:

1. Navigate to the Infoblox CSP's Access Authentication page that was accessed earlier in this guide. Note, please keep the Okta admin page open in another tab or browser.

2. On the Access Authentication page, click the **User Group Sync** tab.

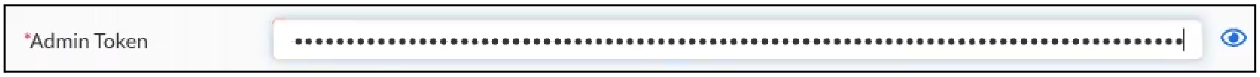


3. On the User Group Sync, select the Authentication Profile that was created earlier in this guide.



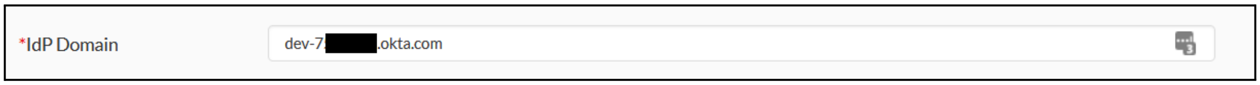
*Authentication Profile: Okta-Guide

4. In the Admin Token text field, paste the Okta token that was acquired in step 8 of the previous section.



*Admin Token: ••

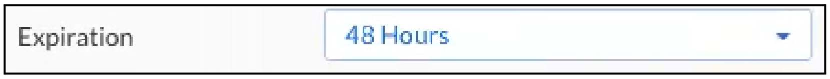
5. Input the IdP Domain that was acquired in step 4 of the previous section.



*IdP Domain: dev-7[redacted].okta.com

6. (Optional) If desired, select a new Expiration for the sync. This setting designates the period of time the CSP holds the user group data. Note: If the IdP defined in your authentication profile has a user group renamed or deleted, you must resynchronize the user groups to get the latest information.

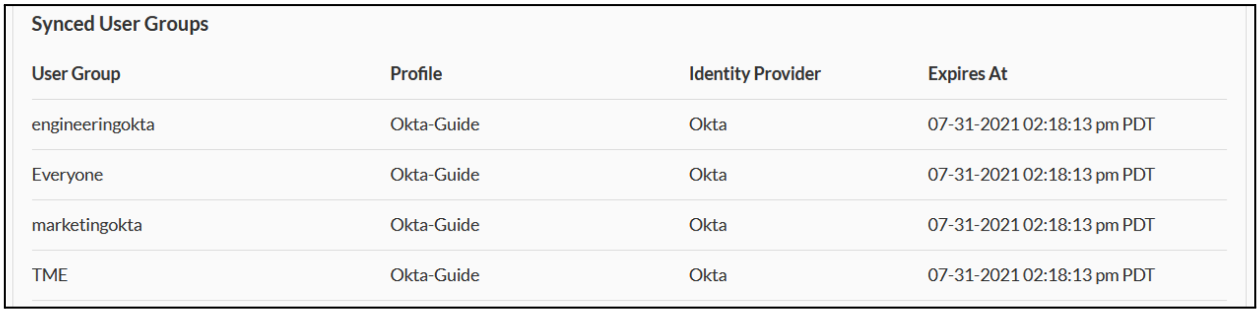
For more details on this setting please see the Synchronizing User Groups doc on the Infoblox Documentation portal.



Expiration: 48 Hours

7. Click **Sync** to sync groups between Okta and BloxOne.

8. After a few moments you will see groups from Okta populate in the Synced User Groups panel.



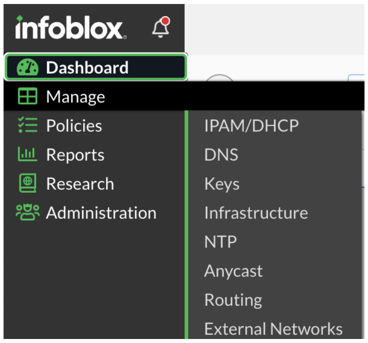
Synced User Groups

User Group	Profile	Identity Provider	Expires At
engineeringokta	Okta-Guide	Okta	07-31-2021 02:18:13 pm PDT
Everyone	Okta-Guide	Okta	07-31-2021 02:18:13 pm PDT
marketingokta	Okta-Guide	Okta	07-31-2021 02:18:13 pm PDT
TME	Okta-Guide	Okta	07-31-2021 02:18:13 pm PDT

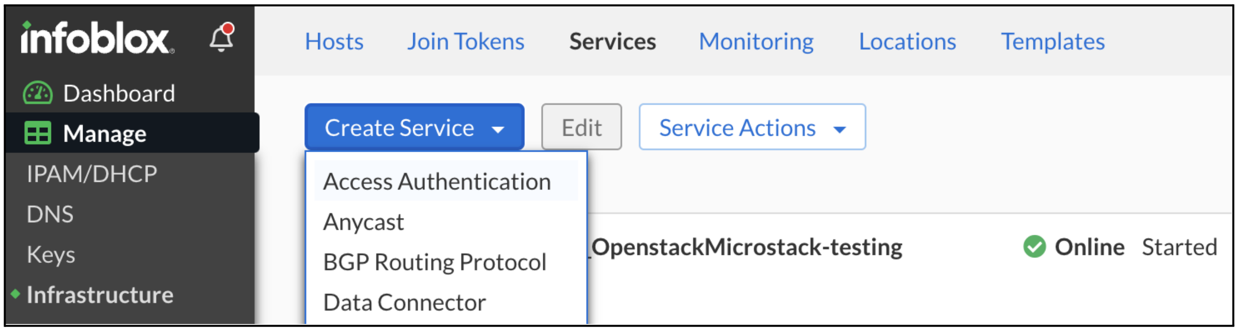
Enable the Access Authentication Service on a Host

To enable the Access Authentication service on an Host, perform the following steps:

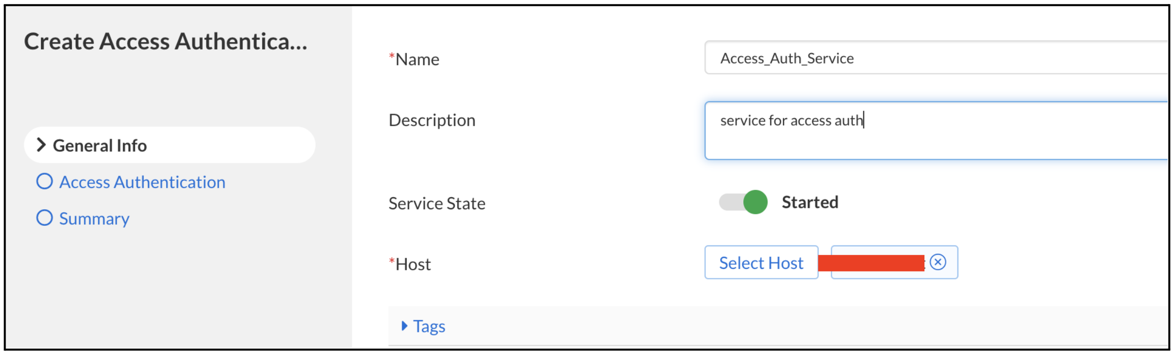
7. On the Infoblox CSP access the Infrastructure page. Highlight **Manage**, then click **Infrastructure**.



8. Navigate to **Services** tab, click **Create Service** and select **Access Authentication**.



9. Under General Info, enter the **Name**, **Description** and select a **Host** on which this service will be associated with. Click **Next**.



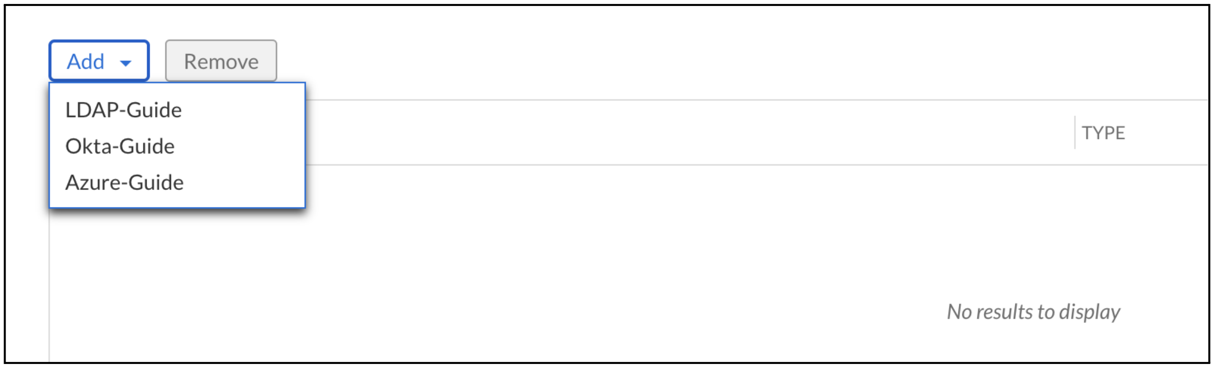
*Name: Access_Auth_Service

Description: service for access auth

Service State: Started

*Host: [redacted]

10. Under Access Authentication, click **Add** then click the configured Okta Access Authentication IdP in the list that is revealed.



No results to display

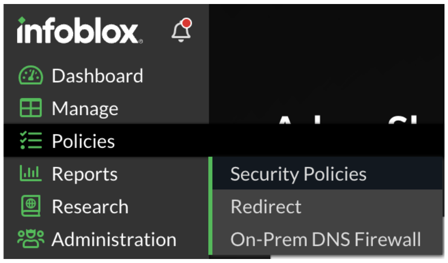
11. Click **Finish**

12. Click **Save & Close** to confirm the changes to the Access Authentication service.

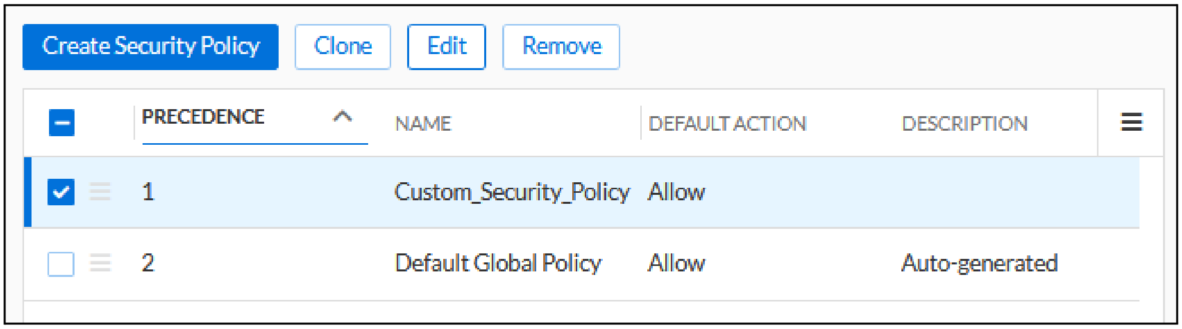
Add User Groups to Security Policy

Once User Groups are synced between Okta, you can apply security policies to a User Group. Perform the following steps to apply a security policy to a User Group.

1. On the Infoblox CSP access the Security Policies page. Highlight **Policies**, then click **Security Policies**.

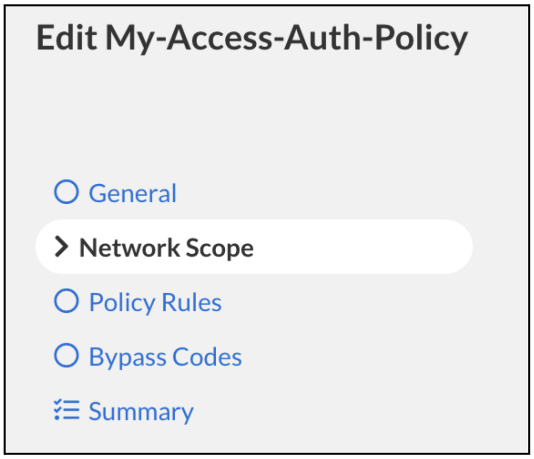


2. Click the **checkbox** associated with an existing Security Policy that you would like to assign an Okta user group to. Then, click Edit. *Note: Create a new Security policy if desired.*

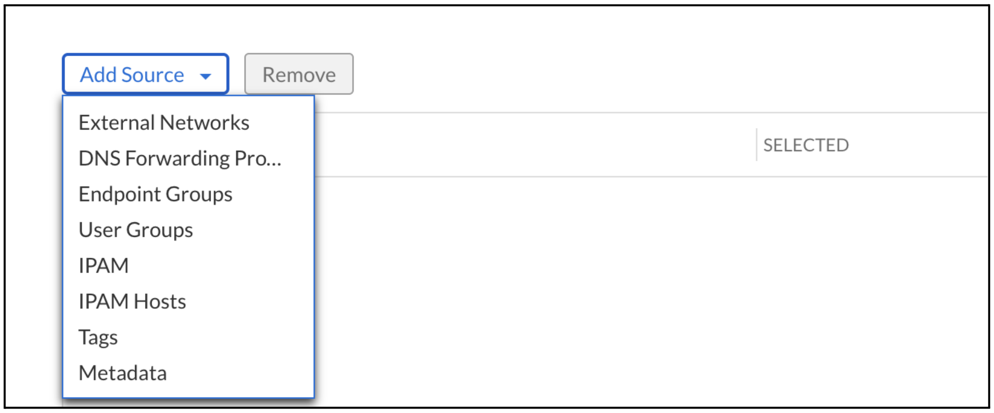


☐	PRECEDENCE	NAME	DEFAULT ACTION	DESCRIPTION
☑	1	Custom_Security_Policy	Allow	
☐	2	Default Global Policy	Allow	Auto-generated

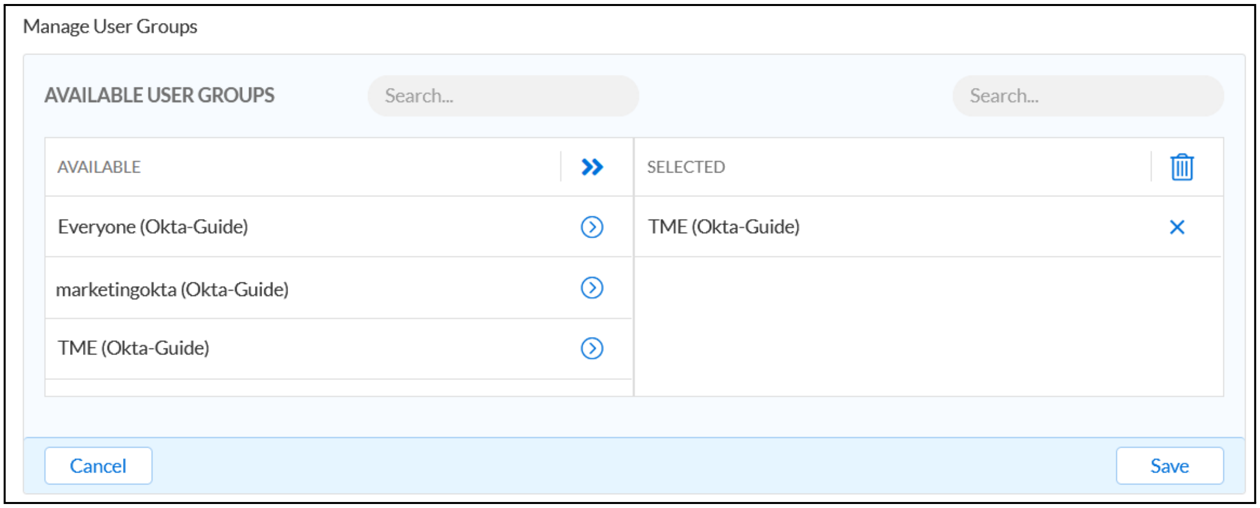
3. In the Edit Security Policy panel, click **Network Scope** located in the left navigation panel.


Edit My-Access-Auth-Policy

4. On the Network Scope panel, click the **Add Source** button. Then, click **User Groups** in the list that is revealed.



5. Select any desired User Groups to add to the Security Policy.



Manage User Groups

AVAILABLE USER GROUPS

AVAILABLE	SELECTED
Everyone (Okta-Guide)	TME (Okta-Guide)
marketingokta (Okta-Guide)	
TME (Okta-Guide)	

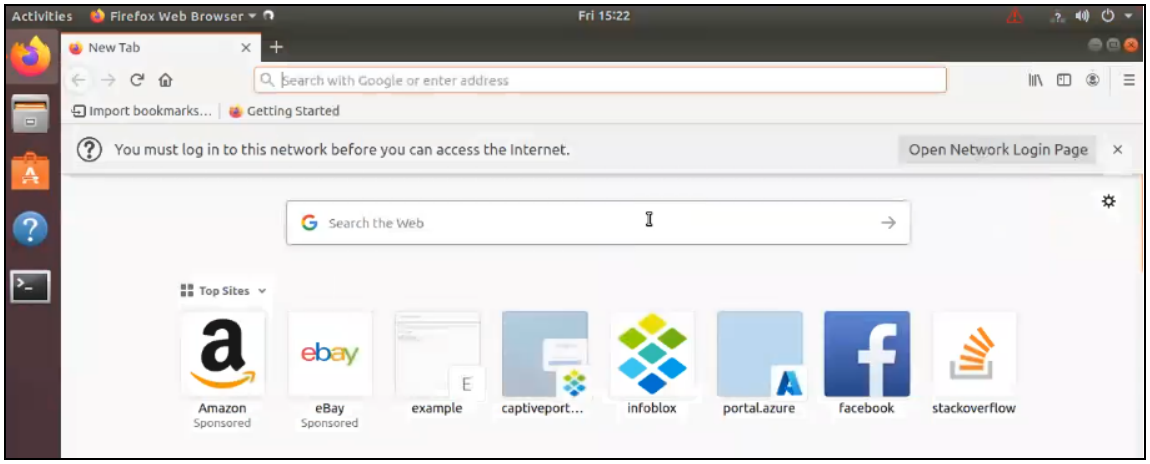
6. Click **Save** to confirm the addition of the User Groups

7. Click **Finish** to confirm the changes to the Security Policy.

Test the Access Authentication with Okta Configuration

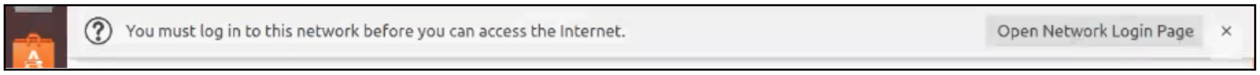
To test the configuration perform the following steps:

1. Access a device that is utilizing the previously configured BloxOne Host as its primary DNS. Open a Web browser on the client.



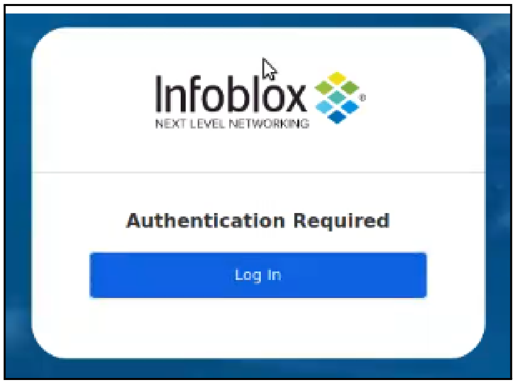
You must log in to this network before you can access the Internet.

- The web browser on the client will prompt the user to log in via IdP. Shown is Firefox's prompt.

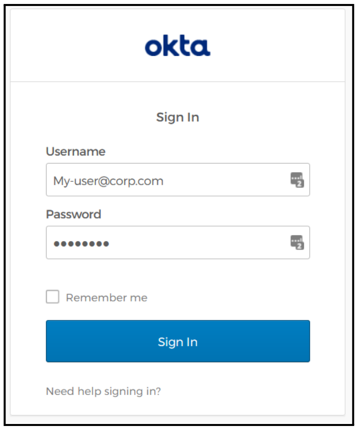


You must log in to this network before you can access the Internet.

2. By clicking the prompt the user will be redirected to a page requesting the user Log In. Click Log In to log in.



3. The user will be redirected to login via an Okta portal. Log in using the credentials of a user that has been synced between the BloxOne platform and Okta.

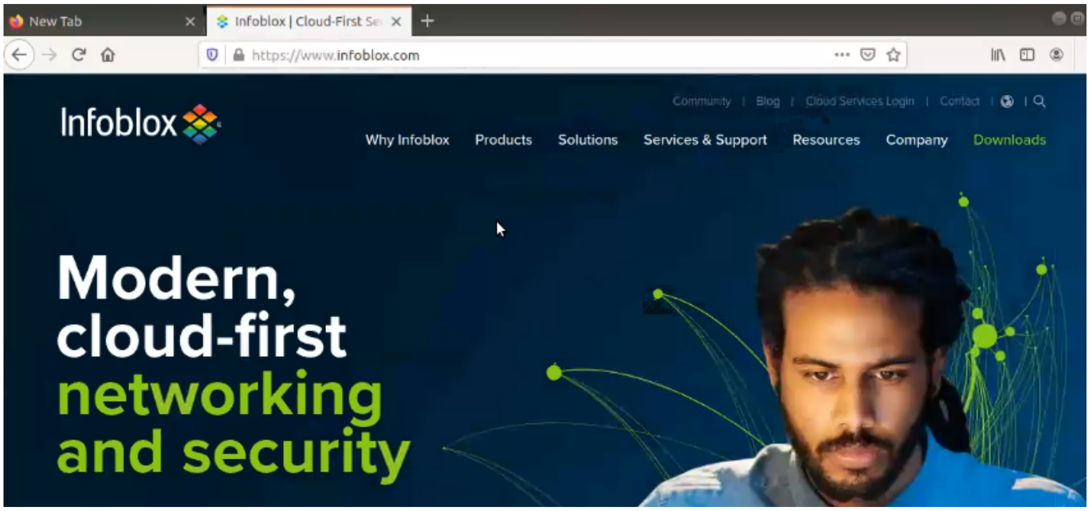


Username: My-user@corp.com

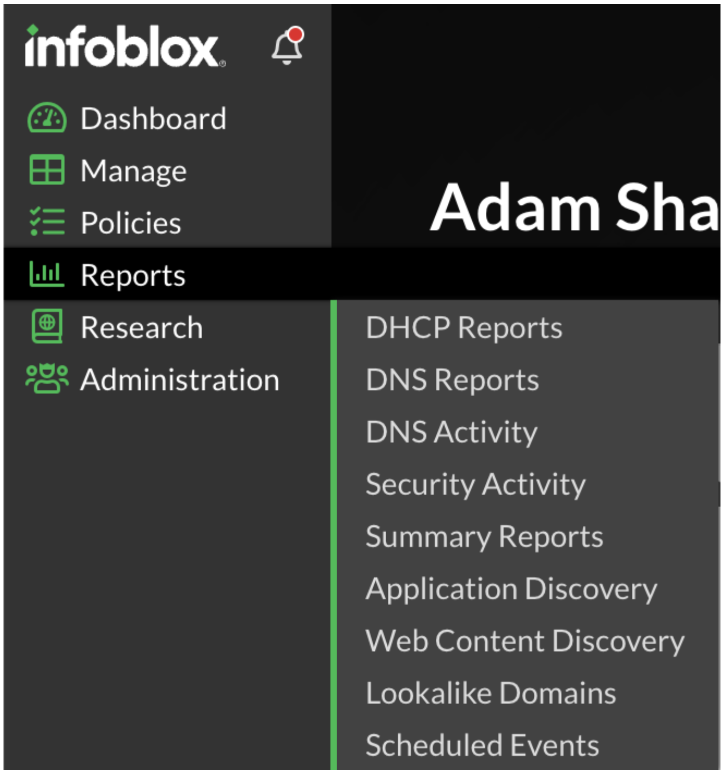
Password: ••••••••

□ Remember me

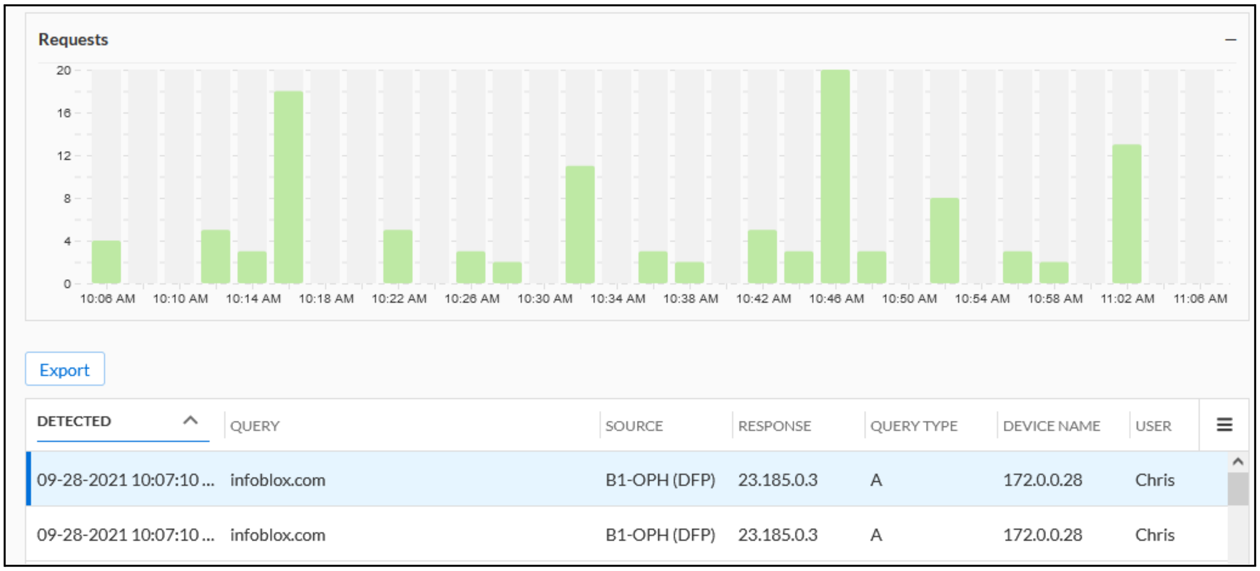
- After a successful login, the user will be able to access the Internet.


New Tab
Infoblox | Cloud-First Se
https://www.infoblox.com
Community | Blog | Cloud Services Login | Contact
Infoblox
Why Infoblox
Products
Solutions
Services & Support
Resources
Company
Downloads
Modern, cloud-first networking and security

4. To view the user's activity in the Infoblox CSP access BloxOne's Reporting.



- Shown are the DNS Activity reports. Observe the User Chris representing the user Chris that was synced with BloxOne from the Azure Active Directory. *Note that the User field is visible in the DNS Activity, Security Activity, and the Security reports pages.*



DETECTED	QUERY	SOURCE	RESPONSE	QUERY TYPE	DEVICE NAME	USER
09-28-2021 10:07:10 ...	infoblox.com	B1-OPH (DFP)	23.185.0.3	A	172.0.0.28	Chris
09-28-2021 10:07:10 ...	infoblox.com	B1-OPH (DFP)	23.185.0.3	A	172.0.0.28	Chris

Additional Resources

For more information regarding Infoblox or Qualys, access these websites:

1. Infoblox Documentation Website: Infoblox Documentation Portal

2. Infoblox Website: Infoblox

3. Infoblox Community Website: Infoblox Community

4. Azure Documentation Website: Azure Documentation

5. Okta Documentation Website: Okta Documentation

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com