

Deployment Guide

# Accessing BloxOne™ Threat Defense Using BloxOne Endpoint

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Introduction</b>	<b>2</b>
<b>Prerequisites</b>	<b>2</b>
<b>Known Limitations</b>	<b>3</b>
<b>Best Practices</b>	<b>3</b>
<b>Workflow</b>	<b>3</b>
<b>BloxOne Endpoint Configuration</b>	<b>4</b>
Part 1: Installation Package	4
Part 2: Endpoint Installation	5
Installation On Linux	6
Installation on Windows	6
Installation on Mac	6
Work From Home Installations	6
Endpoint Status	6
Troubleshooting the Endpoint Status	7
Part 3: Endpoint Management	7
Part 4: Internal Domain Lists	9
Part 5: Policy Management	11
<b>Additional Information</b>	<b>16</b>

# Introduction

BloxOne™ Endpoint is a lightweight mobile agent that can be used to access BloxOne Threat Defense Cloud service to secure roaming end users in varying environments such as home offices, branch offices, public spaces, and more.

BloxOne Threat Defense protects users, devices, and systems no matter where they are, extending enterprise-level security to remote locations, and work from home environments. It leverages the power of your core network services to provide a foundational layer of security for on-prem, cloud and hybrid networks, streamlining and automating threat response.

This deployment guide is intended to guide administrators through deploying the BloxOne Endpoint agent, and how to apply security policies via the Infoblox™ Cloud Services Portal, the user interface for BloxOne Threat Defense.

## Prerequisites

The following is a list of prerequisites required to use BloxOne Endpoint with BloxOne Threat Defense.

1. Administrative access to the Infoblox Cloud Services Portal (<https://csp.infoblox.com>).
  - *Note: If you have never used the Infoblox Cloud Services Portal before and have recently acquired a BloxOne Threat Defense license, check the email that was given during account creation. An email with information on how to initialize the account will be sent from Infoblox.*
2. BloxOne Threat Defense License (One of the following):
  - BloxOne Threat Defense - Business Cloud
  - BloxOne Threat Defense - Advanced license
3. A supported client Operating System
  - *Note: for a full list of supported operating systems please refer to the Infoblox documentation: [Downloading Endpoint - BloxOne Threat Defense - Infoblox Documentation Portal](#)*
4. Client Access to the BloxOne Cloud
  - Ensure any client devices that you will be installing BloxOne Endpoint has access to the following URLs, IPs, and Ports with the Protocols shown:
    - URL:
      - <https://csp.infoblox.com> (Protocol: TCP, Port: 443)
    - IP Addresses:
      - 52.119.40.100 (Protocol: TCP/UDP, Port: 53, 443)
      - 103.80.5.100 (Protocol: TCP/UDP, Port: 53, 443)
6. Client devices must be able to ICMP ping IP addresses 52.119.40.100, and 103.80.5.100.
7. Client devices must not be utilizing any program that is listening on port 53 (DNS).

8. Client devices running Mac OS X must have Internet Sharing turned off.
9. For automatic updates, client devices must have HTTPS access to s3.amazonaws.com for automatic upgrades.Heading Level 1
10. Client devices using a VPN should utilize a Split Tunnel for all Network Protocols (IPv4, or IPv4/IPv6 for dual stack configurations).

## Known Limitations

BloxOne Endpoint does not currently support IPv6-only environments. IPv4 and Dual-stack (IPv4 and IPv6) configurations are supported. This guide does not cover Mobile deployments, for more information regarding Mobile deployments view the [Infoblox documentation portal](#), or this [deployment guide](#).

## Best Practices

It is recommended to not disable or delete any active devices that currently have BloxOne Endpoint installed via the Cloud Services Portal. If the device is removed from the CSP, the client device will not be protected, and the device will not show up on the CSP's Endpoints page. To correct this issue, you may need to contact Infoblox Technical Support to restore the associated database.

When installing BloxOne Endpoint from an install package, ensure the install package was downloaded from the correct Organization in the Cloud Services Portal. The install package contains a Customer ID that defines what organization the endpoint will be assigned to.

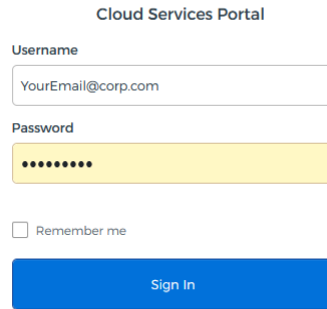
## Workflow

1. Ensure all prerequisites listed on page 2 and 3 have been fulfilled.
2. Log into the Infoblox Cloud Services Portal and acquire the Endpoint install package from the correct Organization.
3. Distribute and install the BloxOne Installation package.
4. Apply security policies to endpoints.
5. Add Internal Domains if needed.

# BloxOne Endpoint Configuration

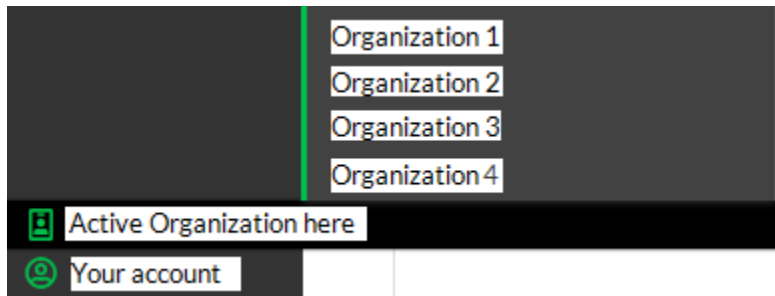
## Part 1: Installation Package

1. Log into the CSP (<https://csp.infoblox.com>) using your credentials.

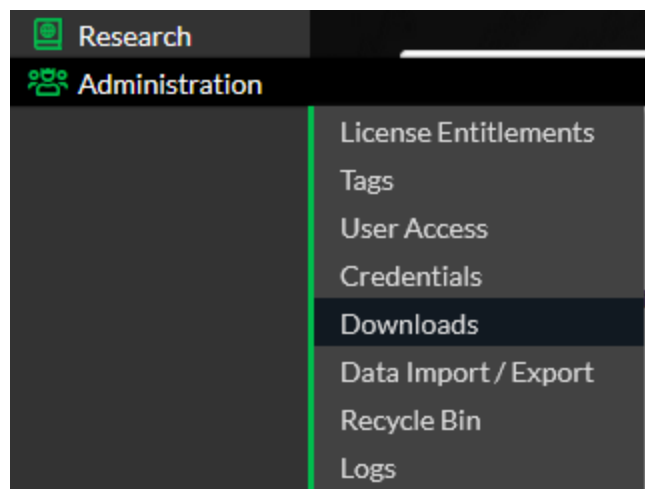


The screenshot shows the 'Cloud Services Portal' login interface. It includes a 'Username' field with the placeholder 'YourEmail@corp.com', a 'Password' field with masked characters, a 'Remember me' checkbox, and a blue 'Sign In' button.

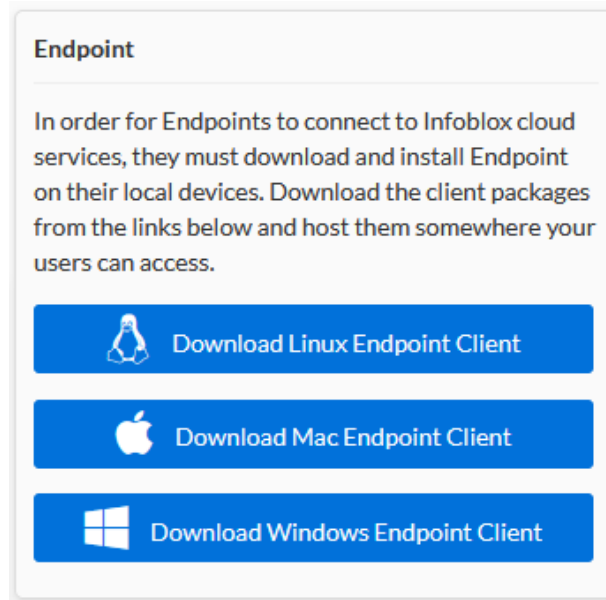
2. Verify you are in the correct **Organization** (Only if you have multiple organizations). If you have access to multiple Organizations, you can view and change your active Organization on the bottom left of the CSP. To change your active Organization, highlight your current Organization, and click the correct Organization in the menu that is revealed.



3. Highlight **Administration** in the left side-panel. Then, click on **Downloads** in the menu that is revealed.



4. **Download** the correct installation package for the clients you intend to deploy BloxOne Endpoint to.
  - For **Linux** clients, click **Download Linux Endpoint Client**.
  - For **Mac OS X** clients, click **Download Mac Endpoint Client**.
  - For **Windows** clients, click **Download Windows Endpoint Client**.



The install package contains a zip file containing 4 files in case of Windows and Mac OS, and 6 files in case of Linux:

- **Installation file**
- **systray\_icon.txt**: This file contains the value of visibility of the systray icon of the endpoint application.
- **endpoint\_group.txt**: The value of this text file corresponds to the respective endpoint group in the cloud services portal.
- **customer\_id.txt**: This file contains the customer ID, corresponding to the organization.
- **installer.sh (Linux)**: This file contains the shell script to run for installing the endpoint.
- **uninstaller.sh (Linux)**: file to run for uninstalling the endpoint.

## Part 2: Endpoint Installation

BloxOne Endpoint can be deployed via many methods, any software installation automation program that allows for the transferring of the entire folder with the installation package can be used. Listed below is how to manually deploy the software. If automation is desired, ensure BloxOne Endpoint has its own folder, the correct Customer ID, and all files that were contained in the .zip are present when it is distributed. Once installed, BloxOne Endpoint will automatically update when updates are available. For further guidance on additional installation methods view the documentation listed here: <https://docs.infoblox.com/space/BloxOneThreatDefense/35374340/Installing+Endpoint>.

## Installation On Linux

1. To download the Linux BloxOne Endpoint zip file navigate to the downloads page (**Administration > Downloads**). Click **Download Linux Endpoint Client**.
2. Unzip the downloaded file and run the **installer.sh** file.
3. Install BloxOne Endpoint using the command `sudo sh installer.sh`.
4. After the successful Installation we can see the BloxOne Endpoint icon. All the related files will be extracted in `/usr/local/b1e`.

## Installation on Windows

1. To download the Linux BloxOne Endpoint zip file navigate to the downloads page (**Administration > Downloads**). Click **Download Windows Endpoint Client**.
2. Unzip the downloaded file and run the **.msi** file.
3. After the successful Installation we can see the BloxOne Endpoint icon in the system tray.



## Installation on Mac

1. To download the Linux BloxOne Endpoint zip file navigate to the downloads page (**Administration > Downloads**). Click **Download Mac Endpoint Client**.
2. Unzip the downloaded file and run the **.pkg** file.
3. After the successful Installation we can see the BloxOne Endpoint icon in the system tray.

## Work From Home Installations

In cases where employees are in a Work-From-Home environment, users can install BloxOne Endpoint on their devices manually. The administrator may distribute BloxOne Endpoint via Google Drive or another cloud based storage platform to all the work from home users. Ensure the .zip file stays intact, and the users follow the instructions above.

## Endpoint Status

To ensure BloxOne Endpoint is correctly configured, view the endpoint status that is listed on the Infoblox Cloud icon. Listed below are the types of statuses, and what they mean:

1. **Protected** (Encrypted DNS, DNS Queries are sent to BloxOne DNS Server):



2. **Protected** (DNS Queries are sent to an On-Prem DFP, DNS Queries are sent to the corporate network when the device is connected to the corporate network):



3. **Bypassed** (DNS Queries are being sent to the default DNS resolvers, the device is not currently protected by Infoblox)



4. **Unprotected** (The Application is not currently running, or could not be reached by Infoblox. The device is not currently protected by Infoblox)



## Troubleshooting the Endpoint Status

If the device is showing **Bypassed** or **Unprotected**, verify the following:

### **Bypassed:**

1. Verify that the device has internet connectivity.
2. Verify that the device is not being blocked by a Captive portal.

### **Unprotected:**

1. Verify that the service can be contacted.
  - Verify that the Ports, IPs and URLs specified in the Prerequisites on Page 2 are reachable by the device.
  - Verify that the device has Internet connectivity.
2. No Organization identifier has been specified.
  - Verify that the Customer ID that was included in the installation package was present during the BloxOne Endpoint Installation.
3. DNS Proxy Module is experiencing a malfunction.
  - Ensure the Proxy module is properly configured.
4. Problem with User Account.
  - Contact Infoblox Support for assistance.

For more information, you may access logs via the client experiencing issues.

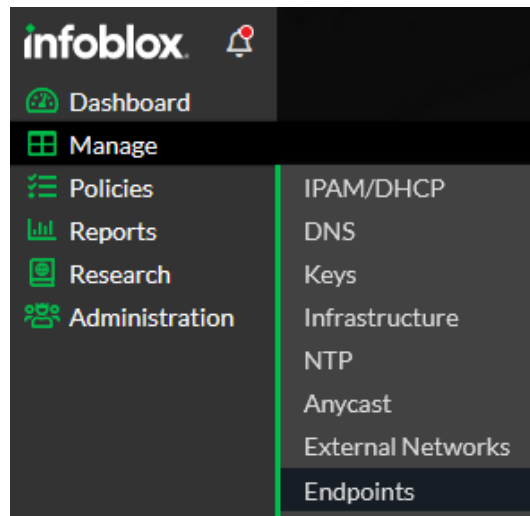
1. Click on the BloxOne Endpoint application on the client and click **Troubleshoot**.
2. In the window that is revealed click **Download Logs**. Logs will be downloaded in a .zip format.

## Part 3: Endpoint Management

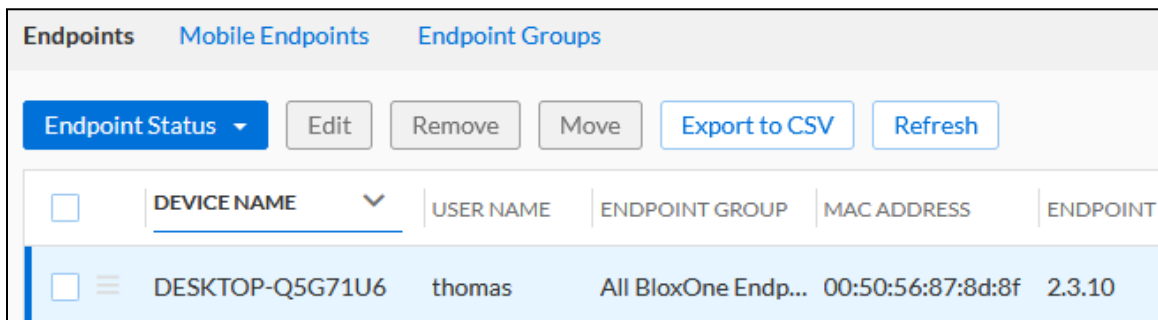
1. Log into the **CSP** (<https://csp.infoblox.com>) using your credentials.



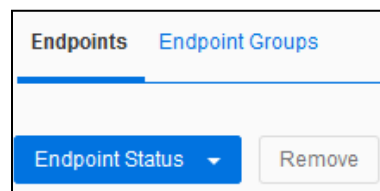
- In the left side-panel highlight **Manage**, then click **Endpoints**.



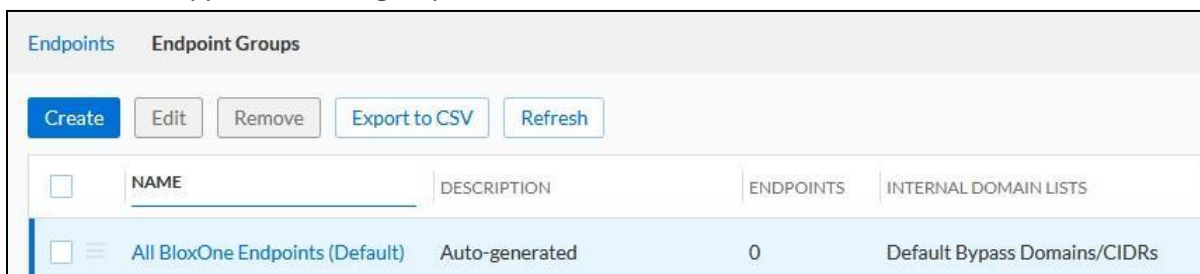
- Here you have a list of all **Endpoints** that are assigned to this Organization, along with additional information regarding the Endpoint.



- Click on the **Endpoint Groups** tab located at the top of the CSP window.

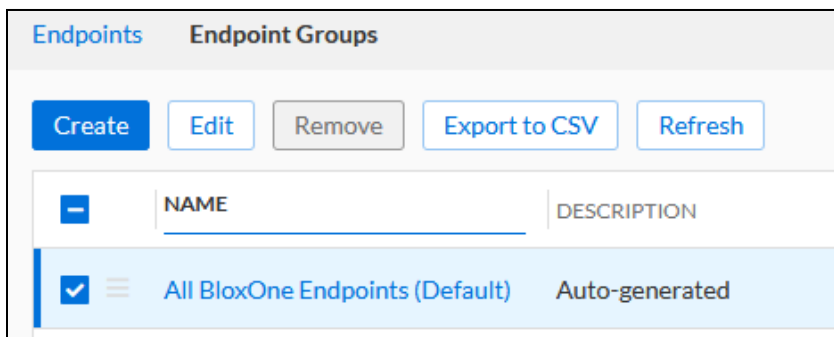


- Here you can define what Endpoints belong to which Endpoint Group, and what policies are applied to these groups.



- Click the Checkbox associated with an Endpoint group. Then, click **Edit** located above the

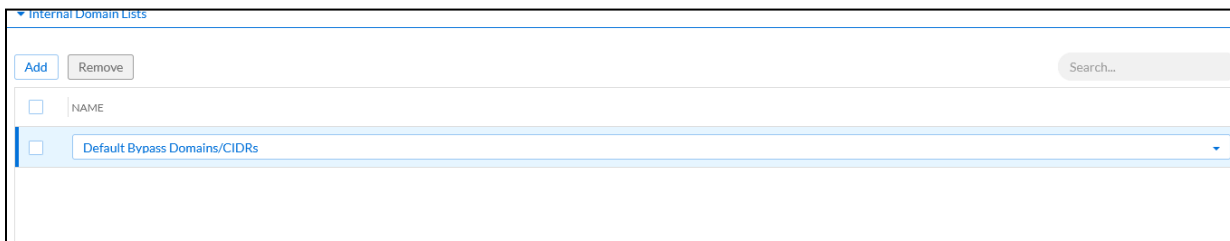
Name column.



- Here you can see the settings of an Endpoint Group. Expand **Internal Domains** list.



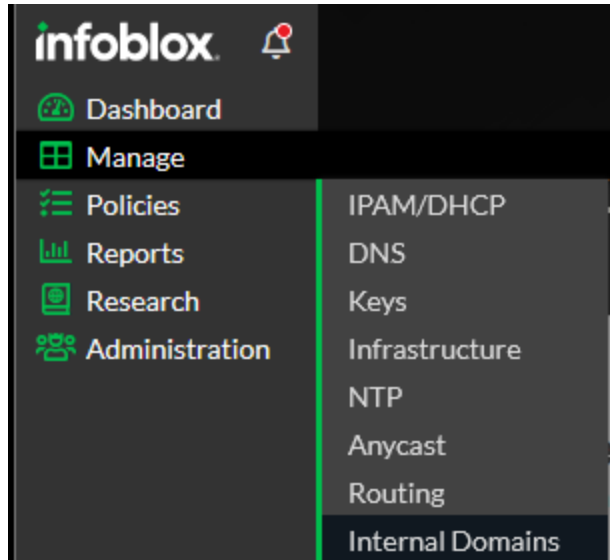
- Here you can assign one or more Internal Domain lists to the Endpoint Group.



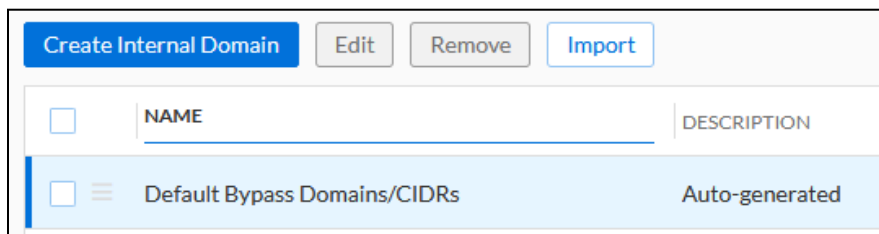
## Part 4: Internal Domain Lists

Internal Domain Lists allow for the uninterrupted access of internal domains that are served by a local DNS server. Queries destined for an IP, Subnet, or Domain contained in an Internal Domains list bypass the BloxOne Threat Defense Cloud. This portion of the Quick Start Guide will showcase how to add an IP, Subnet, or Domain to an Internal Domain list.

1. In the left navigation bar, highlight **Manage**. Then, click **Internal Domains**.



2. To create a new Internal Domain list click the **Create Internal Domain** button located above the Internal Domains list.



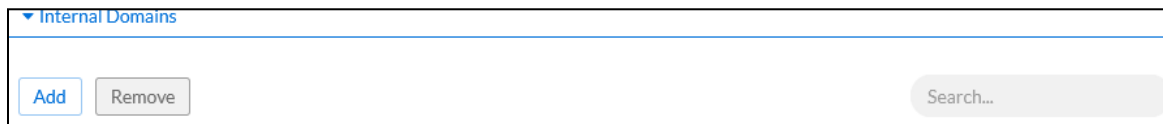
3. Give the Internal Domain a **Name**, and if desired a **Description**.

Create Internal Domains List [Collapse All Sections](#) [Sections](#) ▾

Name

Description

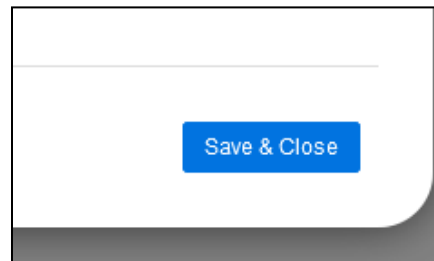
4. To add a Domain, IP, or Subnet, click **Add**.



5. Input a Domain, IP, or Subnet in the text field that is revealed. *Note: Internal Domain lists support wildcards (\*), IPv4 and IPv6 addresses, as well as IPv4 and IPv6 networks in CIDR notation.*

<input type="button" value="Add"/> <input type="button" value="Remove"/> <span style="float: right;">Search...</span>	
<input type="checkbox"/>	DOMAIN/IP ADDRESS/SUBNET
<input type="checkbox"/>	example.com
<input type="checkbox"/>	*.example.com
<input type="checkbox"/>	2001:db8:a0b:12f0::1/64

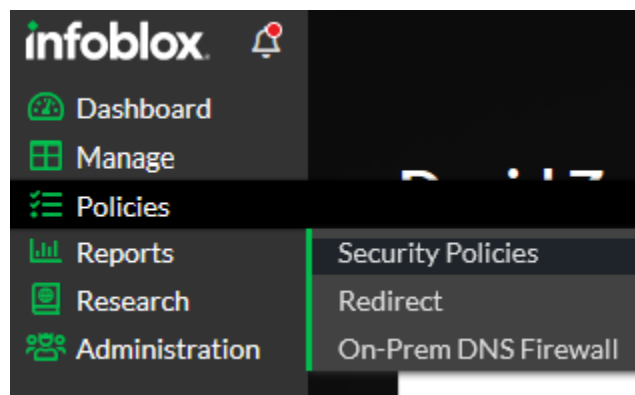
- Once you are done configuring the Internal Domains List, click **Save & Close**.



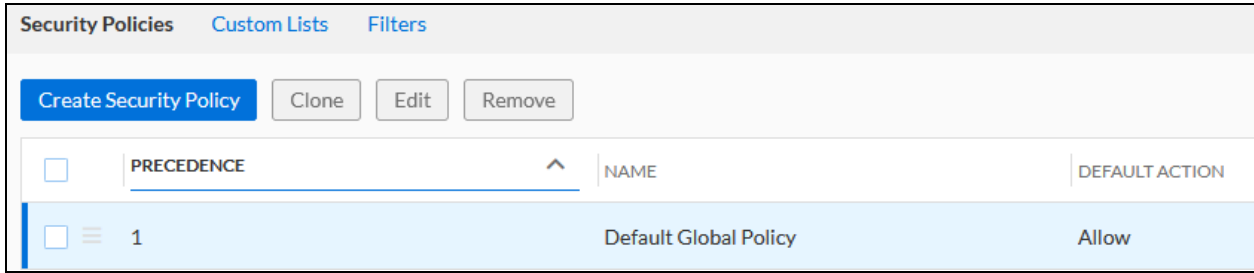
## Part 5: Policy Management

Policies determine what content is blocked or allowed on Endpoints that are assigned to the policy. This section is meant to be a brief tour with information regarding each section in a Security Policy. As with any changes to your production environment it is suggested to fully test any changes in a lab environment before deploying them into production.

- Highlight **Policies** in the left side-panel of the CSP. Then, click on **Security Policies**.



- Here you can see any active **Security Policies** on this Organization. *Note: It is suggested to use the **Default Global Policy** that all endpoints are assigned to by default. This reduces the administrative workload and ensures all new clients are protected.*

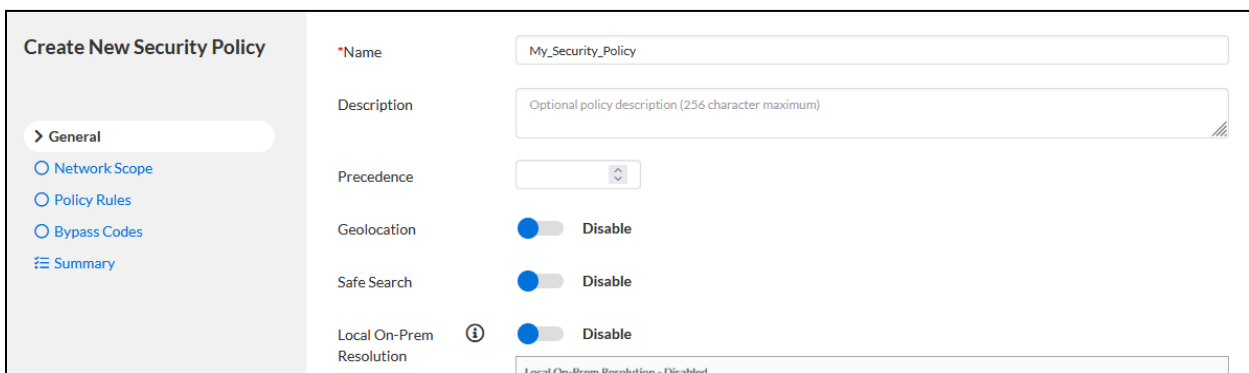


2. To Create a new Security Policy, click **Create Security Policy**.

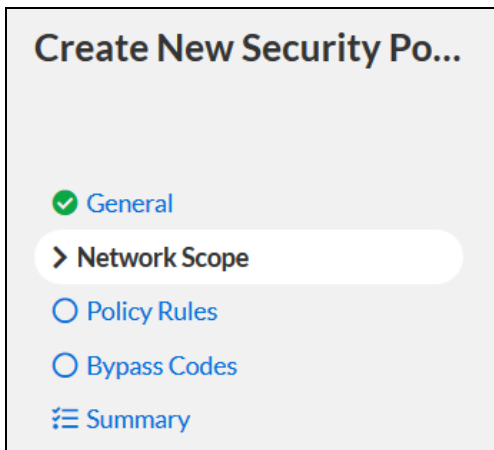


3. Revealed is the **Create New Security Policy** panel. Configure the following settings:

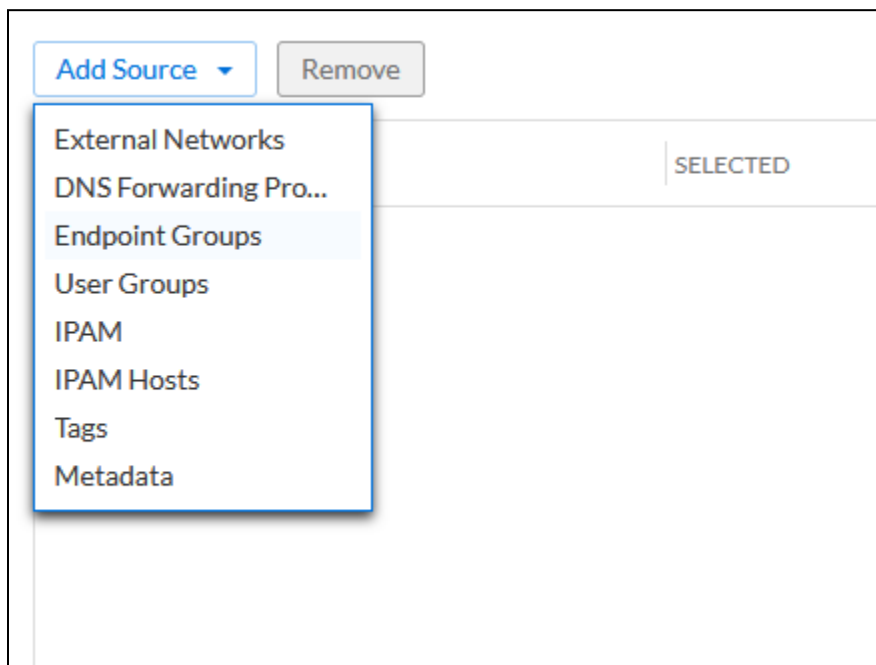
- **Name:** Give the Security Policy a **Name**.
- **Description (Optional):** If desired, input a **Description**.
- **Tags (Optional):** Input **Tags** for the Security policy. *Note: Tags act as metadata that is attached to objects in BloxOne.*
- **Precedence:** Set the **Precedence** of the security policy. *Note that the lower the precedence, the higher the priority of the policy for any assigned network asset. This only applies if an asset is assigned to multiple policies.*
- **Geolocation:** Click the **Geolocation** toggle switch to enable Geolocation. *Note, Enabling Geolocation allows passing the client's subnet to a third party DNS server. This setting is disabled by default*
- **Safe Search:** Click the **Safe Search** toggle switch to enable Safe Search. *Note, Enabling Safe Search forces search engines to exclude inappropriate results. This setting is disabled by default. For a list of supported search engines, please view the [Infoblox Documentation portal](#).*
- **Local On-Prem Resolution:** Click the **Local On-Prem Resolution** toggle switch to enable Local On-Prem Resolution. *Note, enabling Local On-Prem Resolution allows for local DNS servers to be used. This setting is disabled by default. For more information regarding Local On-Prem Resolution, please view the [Infoblox Documentation portal](#).*



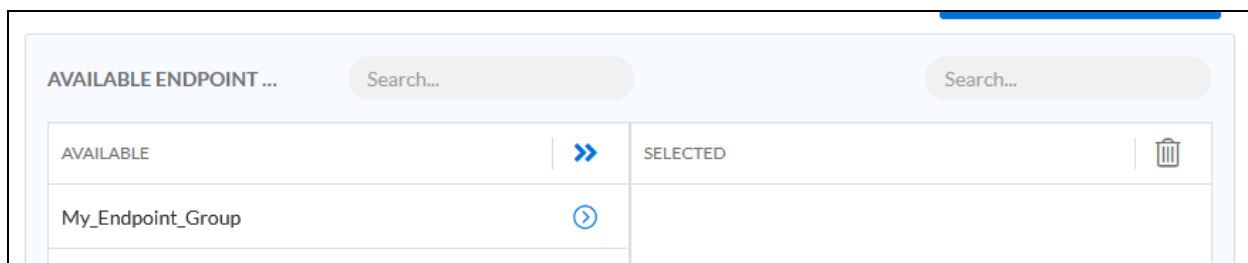
4. Click **Network Scope** to apply specific parameters to the policy.



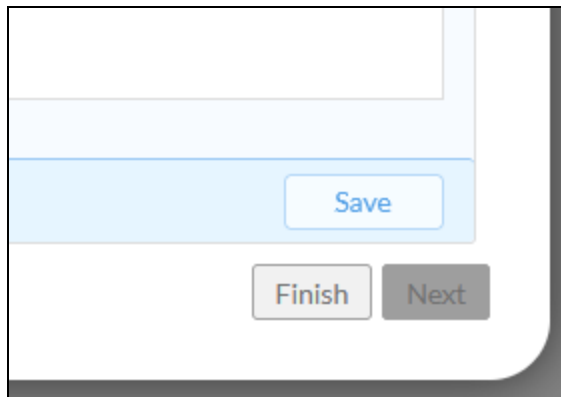
5. Click **Add Source**, then click **Endpoint Groups**. *Note, you select multiple sources for any given Security Policy, this guide will only cover the addition of Endpoint Groups.*



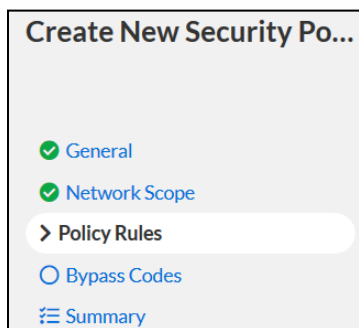
- Select an **Endpoint Group**. Then, click the **right arrow** to move the selected endpoint group to the *Selected* table.



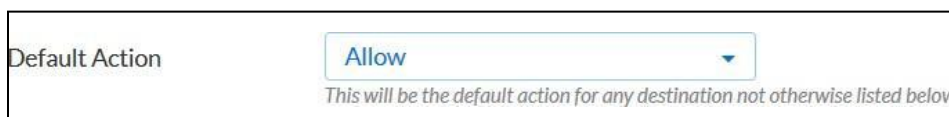
- Click **Save** to confirm the selection of the Endpoint Group.



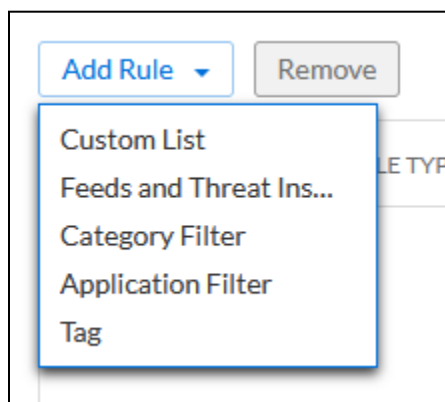
6. Click **Policy Rules** to define rules to apply to this Security Policy.



7. On the Policies Rules page **Default Action** determines what action to perform to traffic that this Security Policy applies to.



8. Click **Add Rule** to specify a rule to add to the Security Policy.



- By clicking **Custom List** you can define which custom lists apply to this policy. Custom lists contain **Addresses** or **Domains** that can be allowed (with or without logging) or blocked (with or without redirecting). *Note: Custom Lists can be created and configured in the Customs Lists tab.*

<input type="checkbox"/>	ORDER	RULE TYPE	NAME	ACTION
<input type="checkbox"/>	1	Custom List	My_Custom_List	Block - No Redirect

- By clicking **Feeds and Threat Insight** you can define which threat feeds to apply to this policy. By clicking on the dropdown you may select from various threat categories, and determine how they are handled when detected. Detected Threats can be allowed (with or without logging) or blocked (with or without redirecting).

Feeds and Threat Insight	Threat Insight - Data Exfiltra...	Block - Default Redirect
--------------------------	-----------------------------------	--------------------------

- By clicking **Category Filters** you can define if a category filter applies to this Security Policy. Category Features can be configured to block or allow content based on category. *Note: Category Features can be created and configured in the Category Features tab.*

Category Filter	Drugs	Block - No Redirect
-----------------	-------	---------------------

- By clicking **Application Filter** you can define how discovered applications are handled by this Security Policy. *For more information regarding Applications and Application Discovery please view the [Infoblox Documentation portal](#).*

Application Filter	All Approved Applications	Allow - No Log
--------------------	---------------------------	----------------

- By clicking **Tag** you can define which tagged BloxOne objects are covered by this Security Policy. *Note, If you select Tag you must provide the Name of a tag, the value of the tag, and the scope of the rule.*

Tag	demo	infoblox	Category Filter	Block - Default Redirect
-----	------	----------	-----------------	--------------------------

- By clicking the **up** and **down** arrows on the right of each entry you can change the order of the rules that are checked by BloxOne.

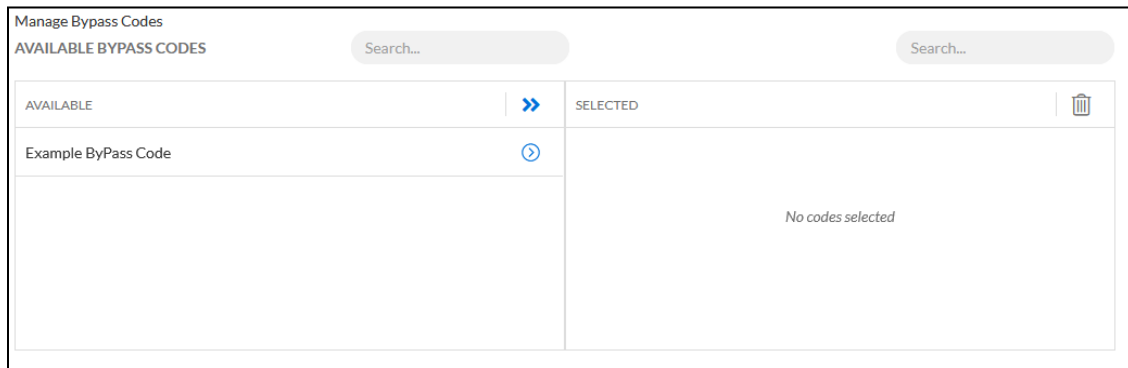
Log	⬆️
Redirect	⬆️ ⬆️
Log	⬆️ ⬆️
Log	⬆️

- Click **Bypass Codes** in the left navigation panel.

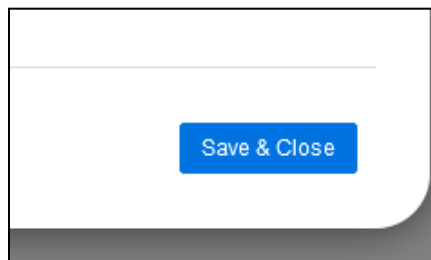




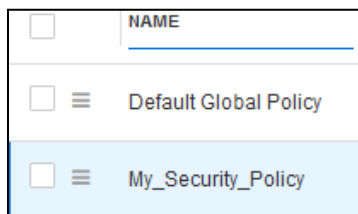
To select a ByPass code, click the **right arrow** in the Available table. *Note, once configured Bypass Codes can allow blocked content to be accessed if requested by a user, this process requires an administrator's approval.*



10. Once you are done configuring the policy, click **Save & Close**.



This **Security Policy** can now be modified, and/or applied to any Endpoint Group that you define.



## Additional Information

For more extensive information in regards to BloxOne Threat Defense, please access the BloxOne Threat Defense Deployment guide:

<https://docs.infoblox.com/space/BloxOneThreatDefense/9928706/BloxOne+Threat+Defense>

For general questions, information, and blogs, please visit our Community website at:

<https://community.infoblox.com>



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](http://www.infoblox.com)