Quick Start Guide

Accessing BloxOne™ Threat Defense using BloxOne Endpoint

Table of Contents

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. Client Operating System (One of the following):
    - Windows:
        - Windows 10
        - Windows 8
        - Windows 7
    - Apple OS X:
        - 10.15.x (Catalina)
        - 10.14.x (Mojave)
        - 10.13.x (High Sierra)
        - 10.12.x (Sierra)
        - 10.11.6 (Sierra)
        - 10.10.x (Yosemite)

4. Client Access to the Active Trust Cloud DNS Server

   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)

5. Client devices must not be utilizing any program that is listening on port 53 (DNS).
6. Client devices running Mac OS X must have Internet Sharing turned off.
7. 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.

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.

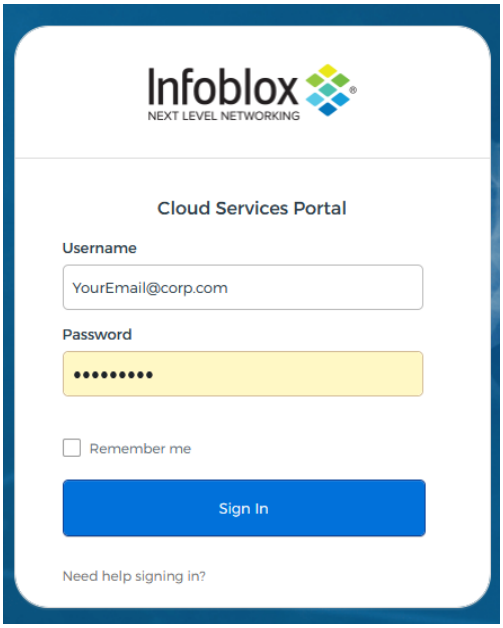
Workflow

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.

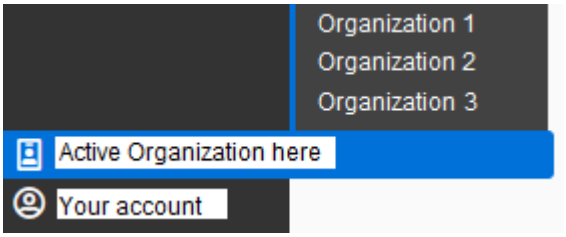
BloxOne Endpoint Configuration

Part 1: Installation Package

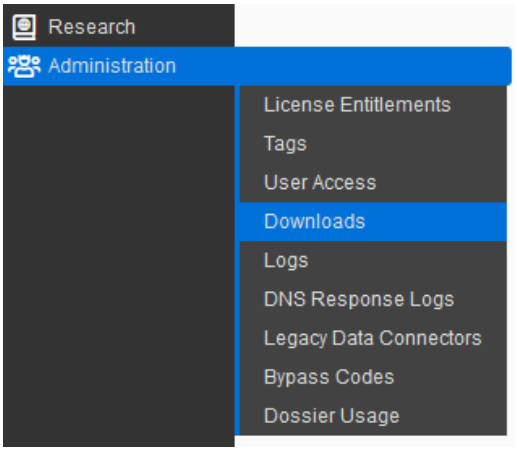
1. Log into the **CSP** (https://csp.infoblox.com) using your credentials.



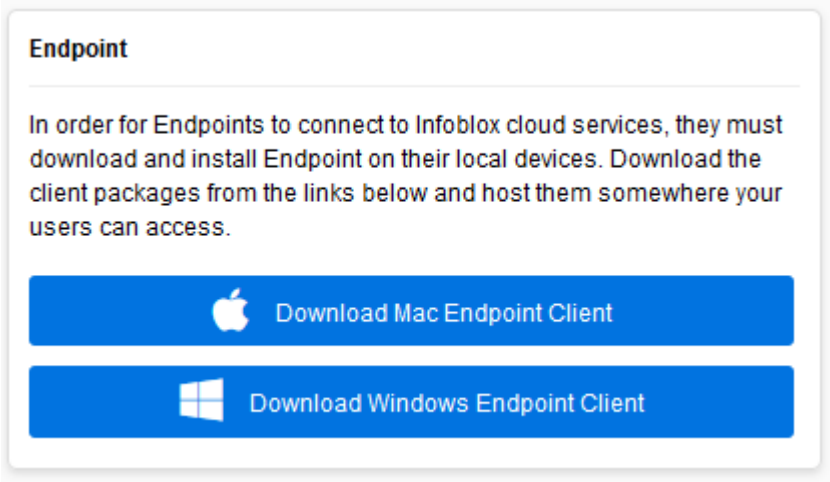
2. Verify you are in the correct **Organization** (Only if you have multiple organizations). If you have access to multiple Organizations, you can view and change your active Organization on the bottom left of the CSP. To change your active Organization, highlight your current Organization, and click 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. Acquire the correct installation package for the clients you intend to deploy BloxOne Endpoint to.
    - For **Mac OS X** clients, click **Download Mac Endpoint Client**.
    - For **Windows** clients, click **Download Windows Endpoint Client**.



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 it's 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/display/BloxOneThreatDefense/Installing+Endpoint.

Standalone Deployment - Manual

1. Create a new folder on the client that BloxOne Endpoint will be installed to. Ensure that this folder is exclusively for Endpoint files.
2. Acquire the installation .zip file that was downloaded in Part 1 of this guide.
3. Extract the .zip file into the folder created that was in Step 1.
4. Navigate to the folder that contains the extracted files from the .zip file.
5. Run the installation file that is contained in the folder. The installation file will be named ActiveTrustEndpoint<VersionNumberHere>.
6. Follow the Prompts in the BloxOne Endpoint Setup window.
7. Once installed, verify that BloxOne Endpoint has successfully been installed indicated by an Infoblox Cloud icon.
    - For **Windows**, the status icon will be visible in the system tray on the bottom right of the Windows desktop.
    - For **Mac OS X**, that status icon will be shown in the menu bar at the top of the Mac desktop.

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:

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

9. **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):

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

11. **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.

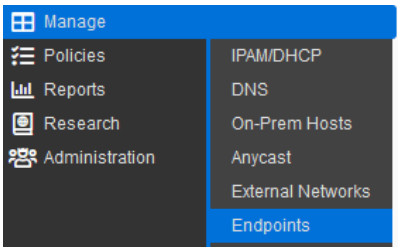
- Contact Infoblox Support for assistance.

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

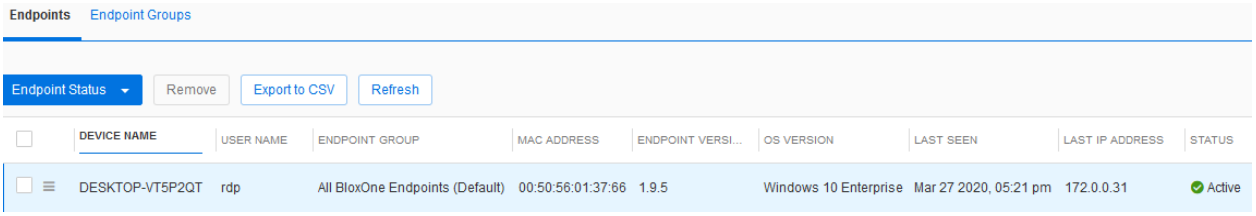
1. Click on the BloxOne Endpoint application on the client and click **Troubleshoot**.
2. In the window that is revealed click **Download Logs**. Logs will be downloaded in a .zip format.

Part 3: Endpoint Management

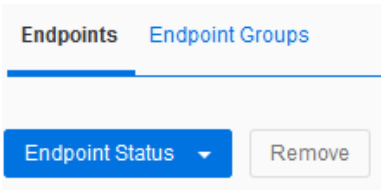
1. Log into the **CSP** (https://csp.infoblox.com) using your credentials.
2. In the left side-panel highlight **Manage**, then click **Endpoints**.



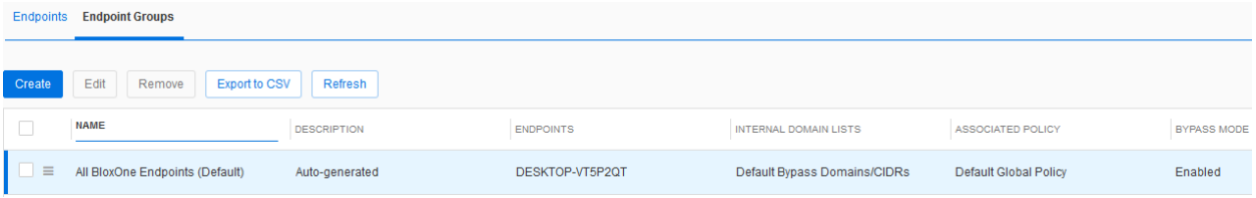
3. Here you have a list of all **Endpoints** that are assigned to this Organization, along with verbose information regarding the Endpoint.



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



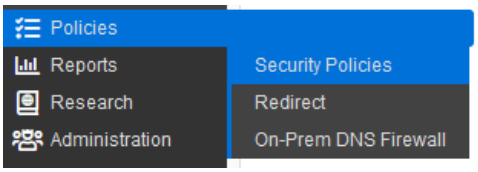
- Here you can define what Endpoints belong to which Endpoint Group, and what policies are applied to these groups.



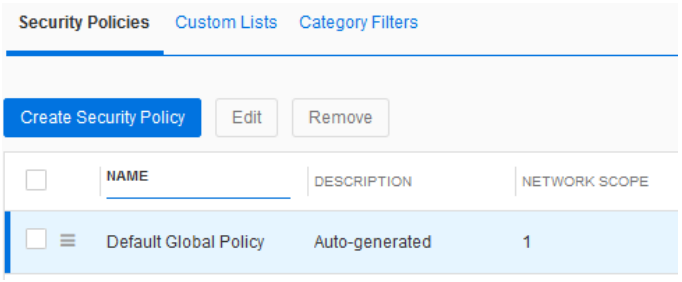
Part 4: Policy Management

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.

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

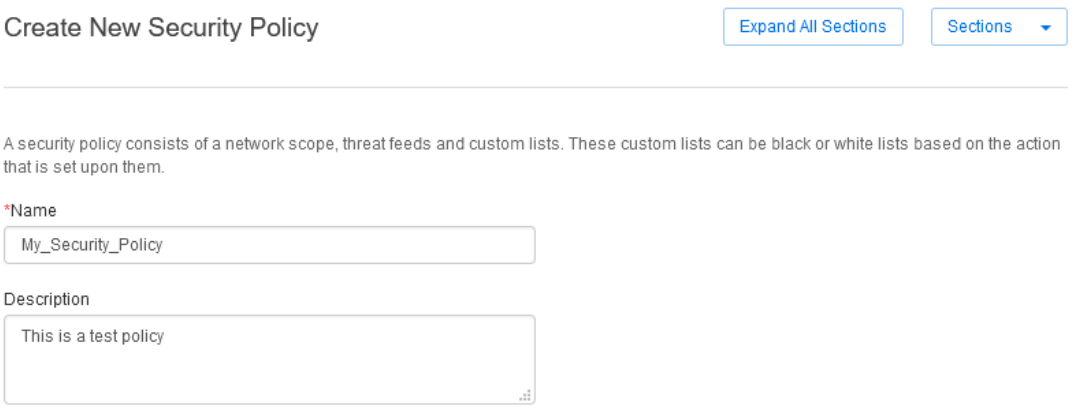


   - Here you can see any active **Security Policies** on this Organization. *Note: It is suggested to use the **Default Global Policy** that all endpoints are assigned to by default. This reduces the administrative workload and ensures all new clients are protected.*

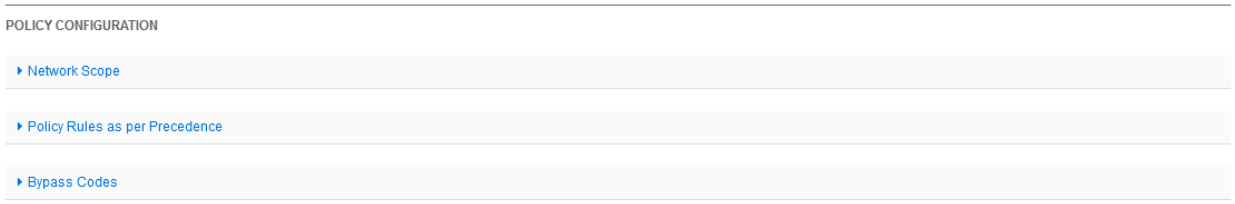


2. To Create a new Security Policy, click **Create Security Policy**.

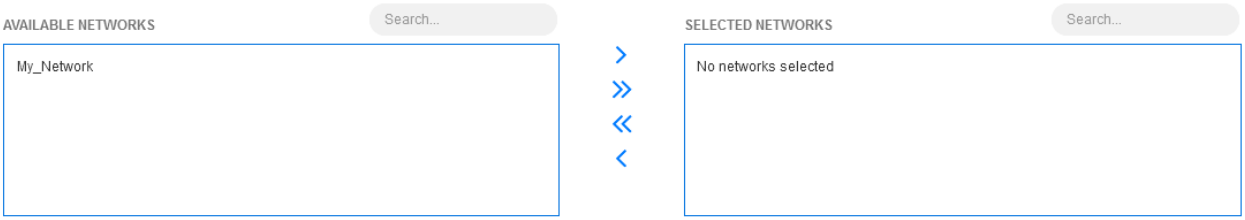
3. Revealed is a panel titled **Create New Security Policy**. Give the Security Policy a **Name**, and if desired a **Description**.



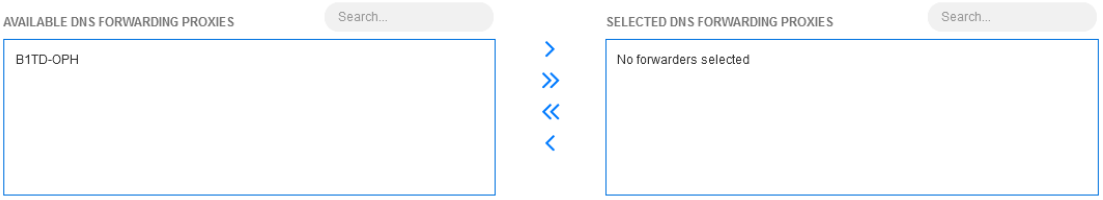
4. Expand **Network Scope** to apply specific parameters to the policy.



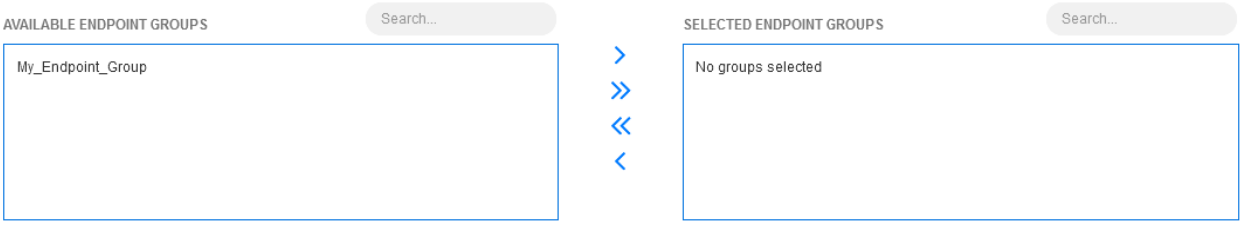
- **Available Networks** defines which networks this policy applies to.



- **Available DNS Forwarding Proxies** defines which DNS Forwarding Proxies this policy applies to.

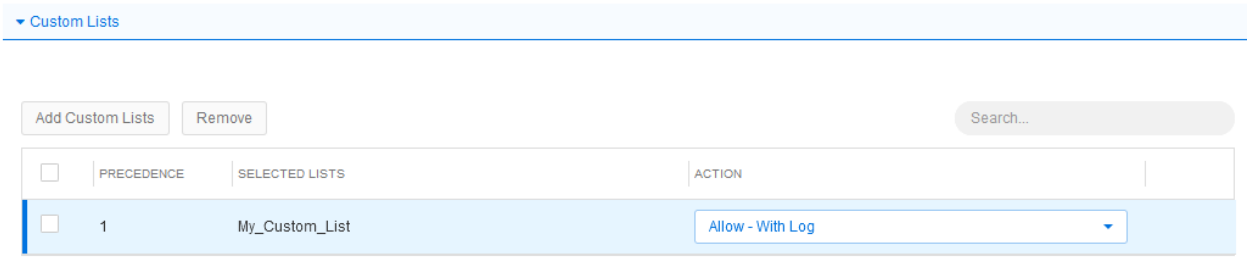


- **Available Endpoint Groups** defines which Endpoints this policy applies to.

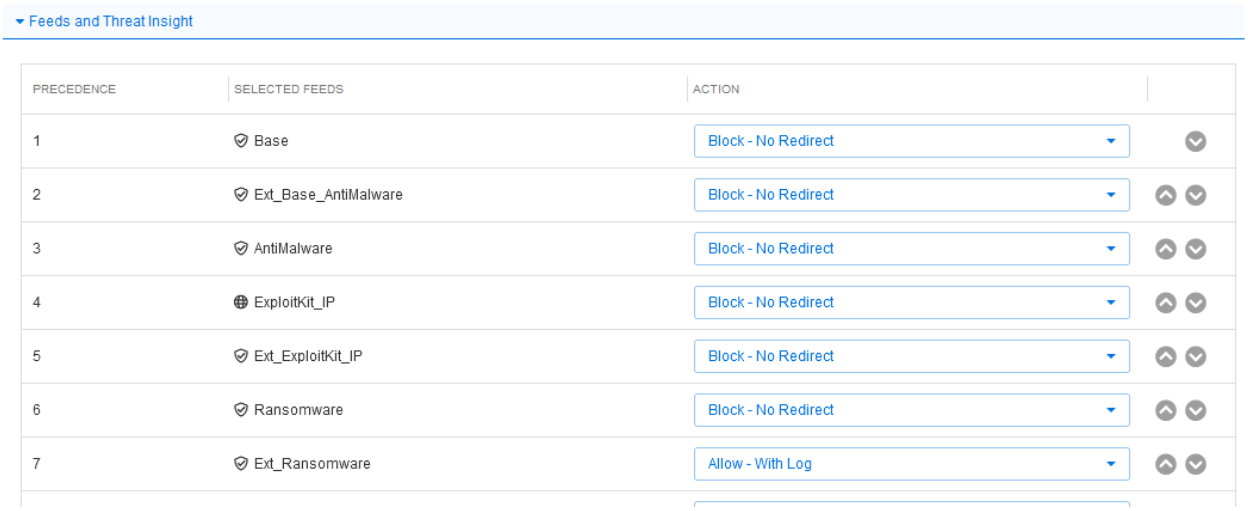


5. Expand **Policy Rules as per Precedence**.

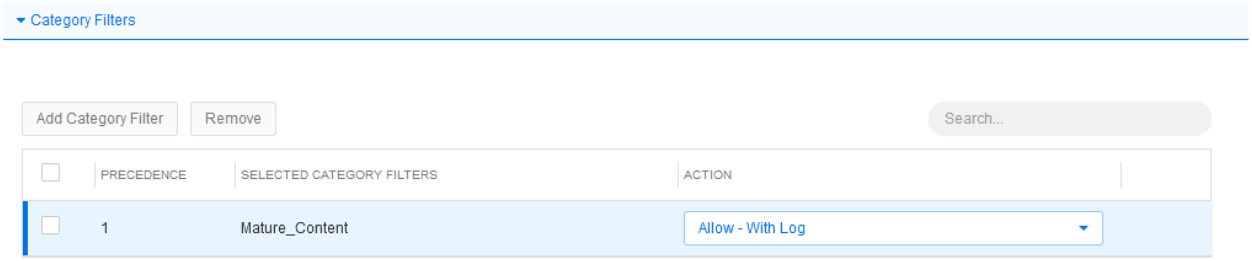
- Expand **Custom Lists** define which custom lists apply to this policy. Custom lists contain **Addresses** or **Domains** that can be allowed (with or without logging) or blocked (with or without redirecting). *Note: Custom Lists can be created and configured in the Customs Lists tab.*



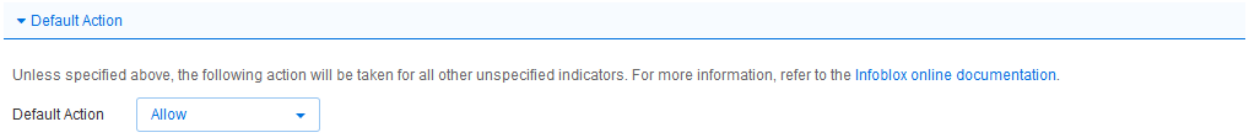
- Expand **Feeds and Threat Insight**. Shown are various threat categories, and how they are handled when detected. Detected Threats can be allowed (with or without logging) or blocked (with or without redirecting).



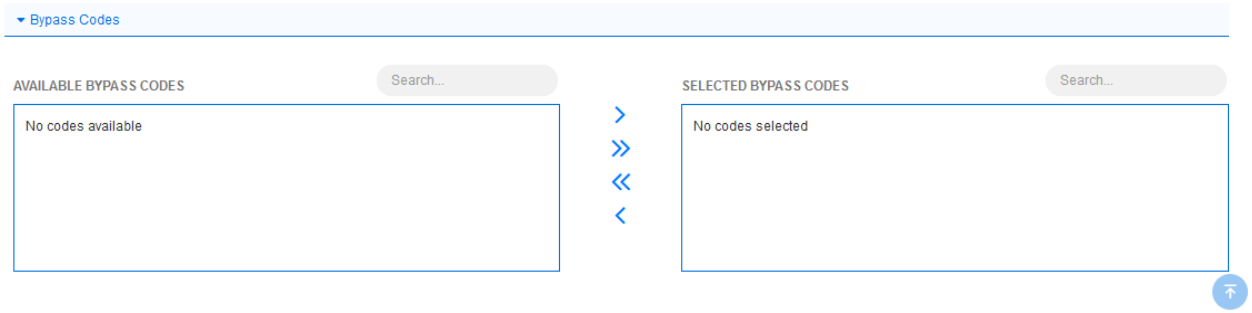
- Expand **Category Filters**. Category Features can be configured to block or allow content based on category. *Note: Category Features can be created and configured in the Category Features tab.*



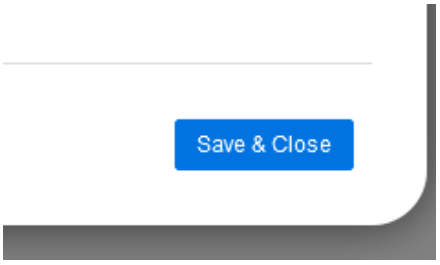
- Expand **Default Action**. Default action determines what action is performed with no other rule has been triggered.



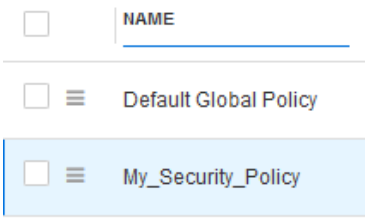
6. Expand **Bypass Codes**. Once configured Bypass Codes can allow blocked content to be accessed if requested by a user, this process requires an administrator's approval.



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



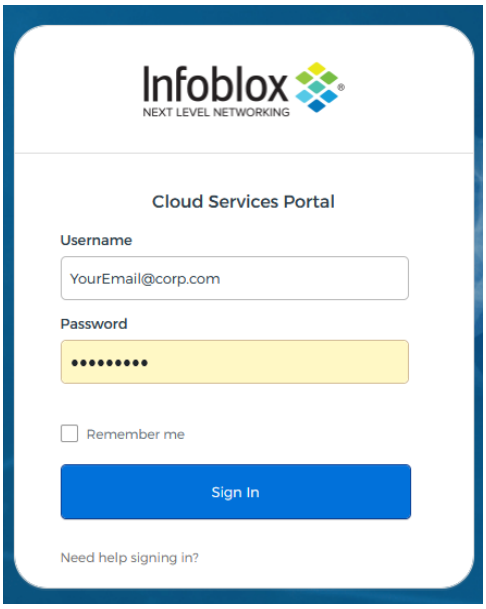
   - This **Security Policy** can now be modified, and/or applied to any Endpoint Group that you define.



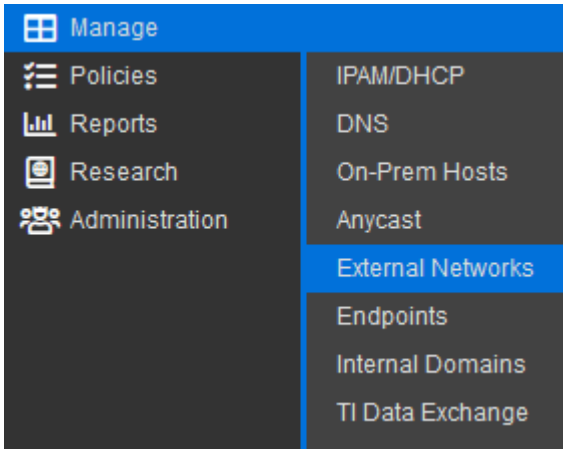
Protecting Home Networks

Optionally, administrators may opt to protect their employee's entire home network using BloxOne Threat Defense. This section covers how an administrator would apply BloxOne Threat Defense, and security policies to an employee's home network. *Note: this section requires the public routable IP of the employees home router.*

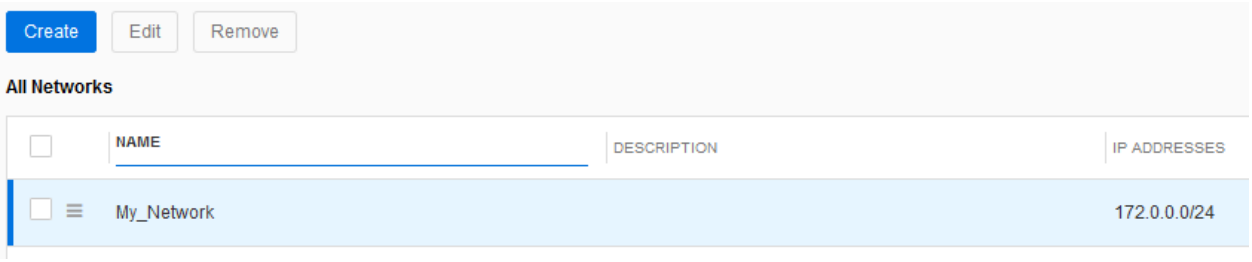
1. Notify your employee that this option is available. If they opt to use this functionality, guide the employee to a public website such as https://whatsmyip.com/, so they can acquire their public routable IPv4 Address. Once the user has the address, have them send it to you.
2. Log into the **CSP** (https://csp.infoblox.com) using your credentials.



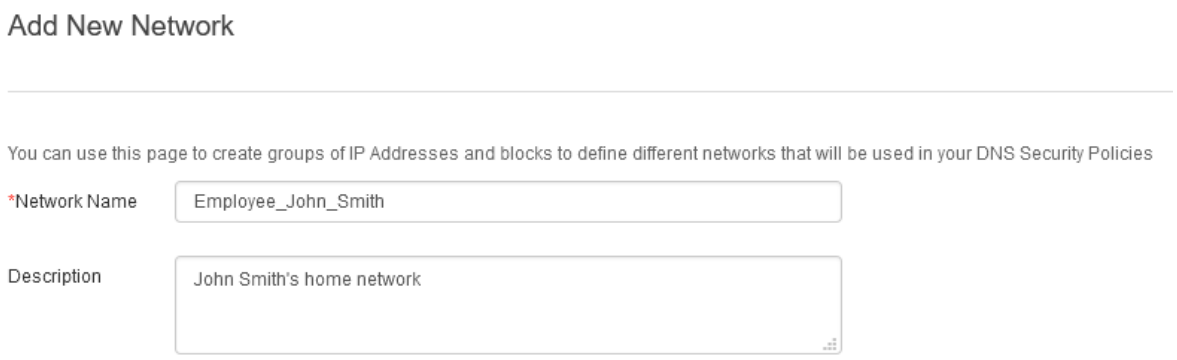
3. Navigate to **External Networks** in the left side-panel. Highlight **Manage**, then click **External Networks**.



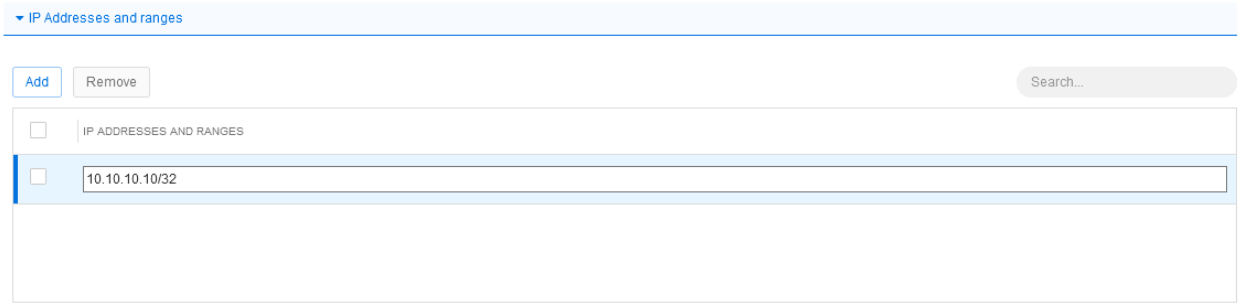
4. Listed are all external networks currently protected by BloxOne Threat Defense. Click **Create** to add the employees home network.



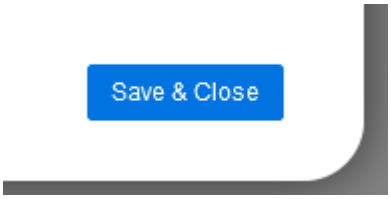
5. Revealed is an **Add New Network** window. Give the new network a **Name**, and if desired a **Description**.



6. Expand the **IP Addresses and Ranges** section. Input the user's public routable IPv4 address in CIDR format, use /32 to specify the range of only one IPv4 address.



7. Click **Save & Close** to finalize the creation of the **Network**.

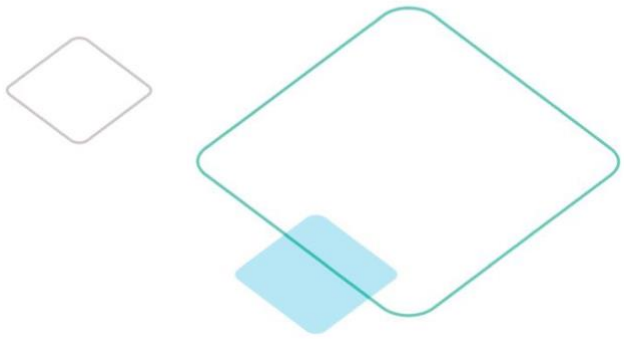


8. By default, this Network will be added to the Security Policy named **Default Global Policy**. You may add this Network to a different policy by navigating to Security policies and adding the network to the Security policy of your choosing. Security policies were covered on **pages 7-10** in this document.
9. Once the Network has been added to the Organization in the CSP, the employee must point their router's DNS to the BloxOne Threat Defense DNS located at IPv4 Address **52.119.40.100**. Have the employee consult their router's user manual to modify their router's DNS configuration.

Additional Information

For more extensive information in regards to BloxOne Threat Defense, please access the BloxOne Threat Defense Deployment guide:
https://docs.infoblox.com/display/BloxOneThreatDefense/BloxOne+Threat+Defense

For general questions, information, and blogs, please visit our Community website at:
https://community.infoblox.com



Infoblox enables next level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com