DEPLOYMENT GUIDE

BloxOne Threat Defense Integration in ZScaler Environment

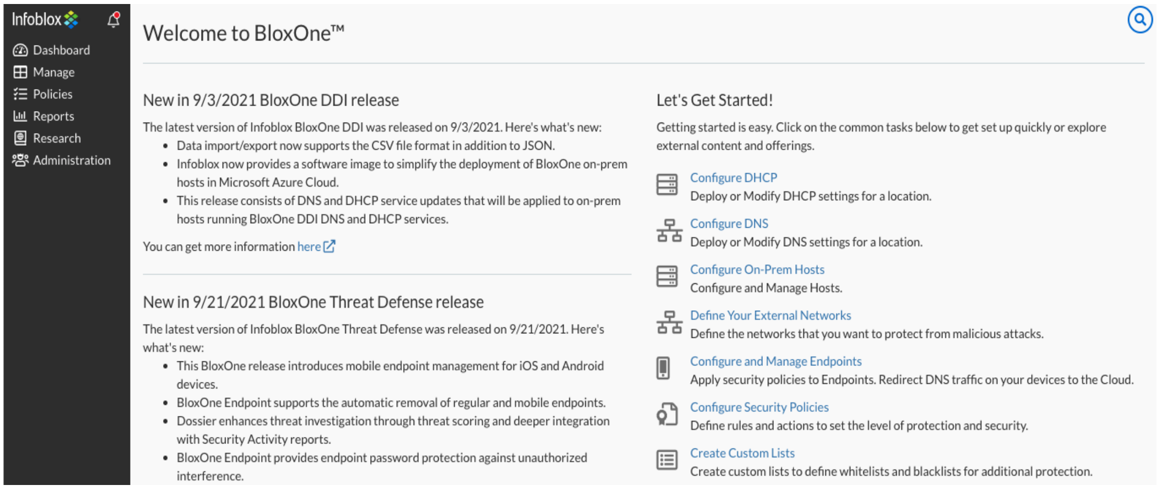
Table of Contents

Introduction

In a Zscaler Internet Access environment, PAC files are used a lot regardless if the workstation is on-premises or remote. Proxy Auto-Configuration (PAC) file is a JavaScript function that determines whether web browser requests (HTTP, HTTPS, and FTP) go directly to the destination or are forwarded to a web proxy server. With Zscaler Internet Access, you can use the BloxOne Threat Defense client to send DNS queries to the BloxOne cloud for resolution. The BloxOne Threat Defense will check the query to determine if you are trying to resolve a malicious site or not. This all occurs before traffic is sent through the Zscaler proxy/cloud by the PAC file. This deployment guide shows you how to install the BloxOne Threat Defense Client and shows the PAC file segment that allows the BloxOne Threat Defense Client to be used.

Instructions for installing BloxOne Threat Defense Client

1. Log into https://csp.infoblox.com .



Welcome to BloxOne™

New in 9/3/2021 BloxOne DDI release

The latest version of Infoblox BloxOne DDI was released on 9/3/2021. Here's what's new:

- Data import/export now supports the CSV file format in addition to JSON.
- Infoblox now provides a software image to simplify the deployment of BloxOne on-prem hosts in Microsoft Azure Cloud.
- This release consists of DNS and DHCP service updates that will be applied to on-prem hosts running BloxOne DDI DNS and DHCP services.

You can get more information here

New in 9/21/2021 BloxOne Threat Defense release

The latest version of Infoblox BloxOne Threat Defense was released on 9/21/2021. Here's what's new:

- This BloxOne release introduces mobile endpoint management for iOS and Android devices.
- BloxOne Endpoint supports the automatic removal of regular and mobile endpoints.
- Dossier enhances threat investigation through threat scoring and deeper integration with Security Activity reports.
- BloxOne Endpoint provides endpoint password protection against unauthorized interference.

Let's Get Started!

Getting started is easy. Click on the common tasks below to get set up quickly or explore external content and offerings.

Configure DHCP
Deploy or Modify DHCP settings for a location.

Configure DNS
Deploy or Modify DNS settings for a location.

Configure On-Prem Hosts
Configure and Manage Hosts.

Define Your External Networks
Define the networks that you want to protect from malicious attacks.

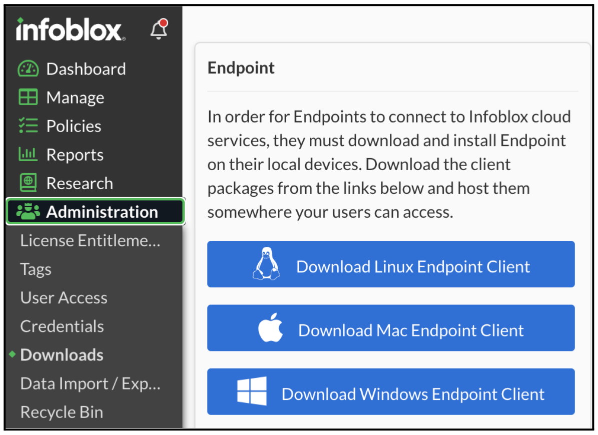
Configure and Manage Endpoints
Apply security policies to Endpoints. Redirect DNS traffic on your devices to the Cloud.

Configure Security Policies
Define rules and actions to set the level of protection and security.

Create Custom Lists
Create custom lists to define whitelists and blacklists for additional protection.

2. Navigate to **Administration** → **Downloads**.

3. In the Endpoint section, click on the appropriate button to download the compressed file for the endpoint client.



Endpoint

In order for Endpoints to connect to Infoblox cloud services, they must download and install Endpoint on their local devices. Download the client packages from the links below and host them somewhere your users can access.

4. Extract the **ZIP** file to the folder that you created earlier, and then properly extract the **ZIP** file.

   NOTE: Ensure that you extract all the files from the ZIP archive before starting the installation process. Otherwise, the installation might fail if there is any missing file. Go to the folder that contains all the extracted files and click the *ActiveTrustEndpoint.pkg* file if you are an Apple Mac user, or click the *ActiveTrustEndpoint.msi* file if you are a Microsoft Windows user.
5. The BloxOne Endpoint Setup Wizard appears when you run the installer program. Click **Next**.
6. **Enter** the destination folder in which you want to save the BloxOne Endpoint application. Click **Next**.
7. Click **Install** in the wizard to install BloxOne Endpoint.
8. Click **Finish** when the installation completes.
    - After the endpoint software is installed, the successful status will show up as one of the following:

Protected

    - Endpoint is running properly, and your device is fully protected against malicious attacks by Infoblox Endpoint.

This icon is displayed for the following states:

- DNS queries are encrypted and are being sent to the BloxOne DNS Server.
- DNS queries are being sent to the BloxOne DNS Server.

Protected

If your device is connected to the corporate network, it is protected against malicious attacks by the corporate network.

This icon is displayed for the following states:

- When the endpoint is connected to the corporate network, the DNS queries are being sent to the corporate DNS servers.
- If you have configured an on-prem DNS forwarding proxy, the DNS queries are being sent to the proxy

The data flow will occur as follows when using your browser to access a URL:

1. User types in a URL and hits the return key.

2. The PAC file script will execute.

3. The first statement in the script file will make a DNS query for the URL.

4. The BloxOne Threat Defense client takes that DNS query and forwards it to the BloxOne Cloud for resolution.

5. The results of the resolution are sent back.

6. If the IP address is not local or a BloxOne walled garden, then the HTTP or HTTPS request to the IP address will be sent to the Zscaler proxy.

Below is a PAC file segment that allows for the integration of the BloxOne Threat Defense client.

```
function FindProxyForURL(url, host)

// At this point BloxOne TD client is involved with the DNS query going to the BloxOne TD cloud in the next two statements

if (isResolvable(host))

          myHostIpAddress = dnsResolve(host); // called only once (to reduce DNS load)

          if (isPlainHostName(host) ||

          shExpMatch(host, "*.local") ||

    isInNet(myHostIpAddress, "10.0.0.0", "255.0.0.0") ||

    isInNet(myHostIpAddress, "172.16.0.0",  "255.240.0.0") ||

          isInNet(myHostIpAddress, "192.168.0.0",  "255.255.0.0") ||

    isInNet(myHostIpAddress, "127.0.0.0", "255.255.255.0") ||

// Or whatever is the Custom ActiveTrust Cloud blocking page IP or subnet

    isInNet(myHostIpAddress, "52.52.52.52", "255.255.255.255"))

return "DIRECT";

          else

// send to internet proxy

          return myInternetProxy;
```

```
else

//send to internet proxy

return myInternetProxy;
```

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