Deployment guide

BloxOne™ Threat Defense DNS Forwarding Proxy

Table of Contents

Overview

Infoblox BloxOne™ Threat Defense Cloud (B1TD Cloud) is a SaaS offering designed to provide protection to devices on and off-premises, including roaming, remote, and branch offices. It provides visibility into infected and compromised devices, prevents DNS-based data exfiltration, and automatically stops device communications with command-and-control servers (C&Cs) and botnets, in addition to providing recursive DNS services in the cloud. It's possible to access the services by deploying the DNS forwarding proxy.

The DNS Forwarding Proxy (DFP), which can be run on a BloxOne Host, is a DNS forwarder that forwards DNS queries to B1TD Cloud or to a local DNS server. DFP continually monitors connectivity to B1TD Cloud. If a BloxOne Host cannot reach BloxOne Threat Defense Cloud Anycast DNS server for any reason, it will send requests to a local DNS server which protects clients via security RPZ (DNS Firewall) feeds. For DFP running on NIOS having the DNS Forwarding Proxy fallback to a local DNS server, instead of the default DNS resolution path can be used in situations where DFP can't reach BloxOne Threat Defense Cloud from its network.

Prerequisites

Licensing

One of the following:

- BloxOne Threat Defense Advanced
- BloxOne Threat Defense Business – Cloud

BloxOne Host

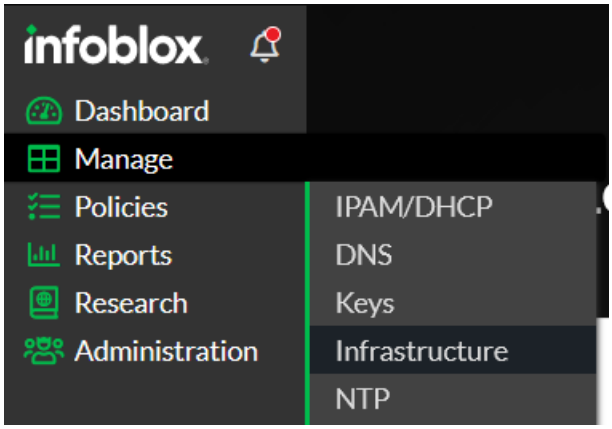
A configured BloxOne Host with the following configuration and connectivity is required before proceeding with this Deployment guide:

- **Minimum System Requirements:** The minimum system requirements for VM's are listed on the Infoblox Documentation portal.
- **Connectivity:** To ensure connectivity with BloxOne ensure that the BloxOne host is not being blocked from reaching any of the Destinations listed in the Infoblox Documentation portal for sections *DNS Forwarding Proxy* and *BloxOne DNS*. The listed ports also must not be used by any applications on the host.

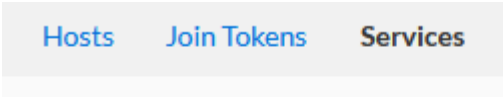
Create the DFP Service

To create the DFP service, perform the following steps:

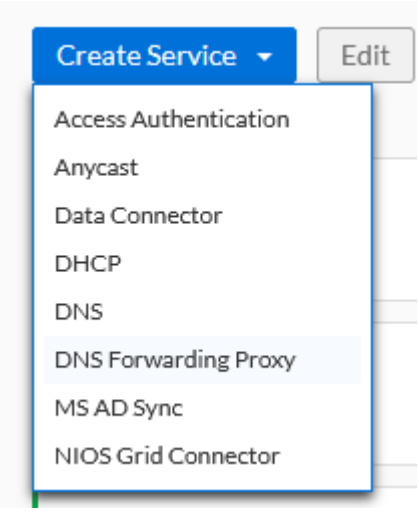
1. From the Cloud Services Portal, click **Manage** → **Infrastructure**.



2. Click the **Services** tab.

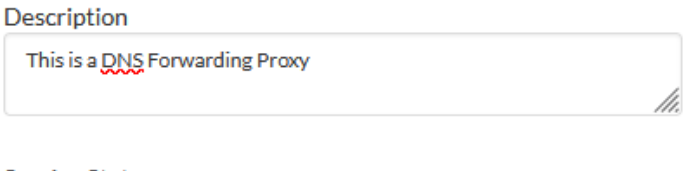


3. Click **Create Service**. Then, click **DNS Forwarding Proxy** from the list that is revealed.

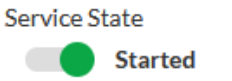


4. In the Create DNS Forwarding Proxy (DFP) panel complete the following:
   - Give the DFP a **Name**.

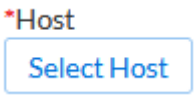
- (Optional) Input a **Description** for the DFP.



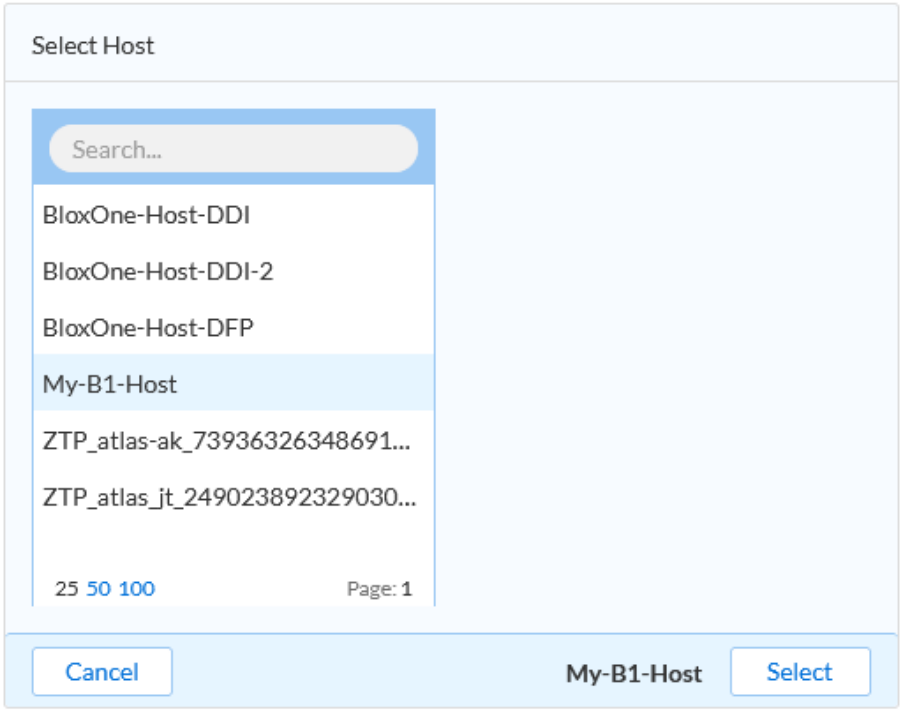
- Ensure the Toggle switch is **Enabled**. If desired, you may also disable the service via this toggle switch.



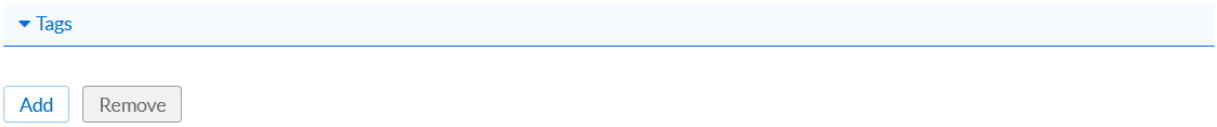
- Select a Host. Click the **Select Host** button.



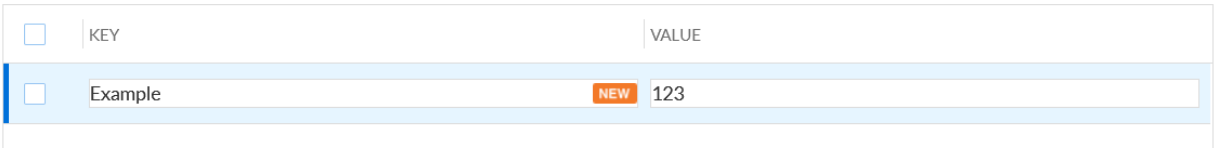
- Locate and click on the **BloxOne Host** that will run the DFP service. Click **Select** to confirm the selection.



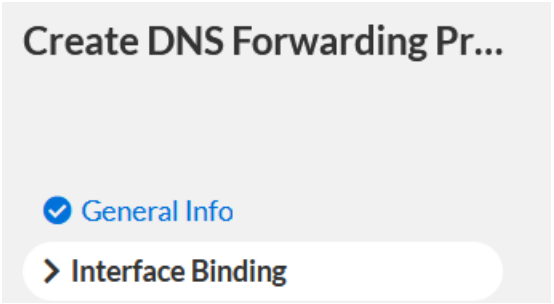
- (Optional) Expand the Tags section and input one or many Tags. *Note: Tags are a type of metadata that is attached to this service.*
    - Click **Add** to add a Tag.



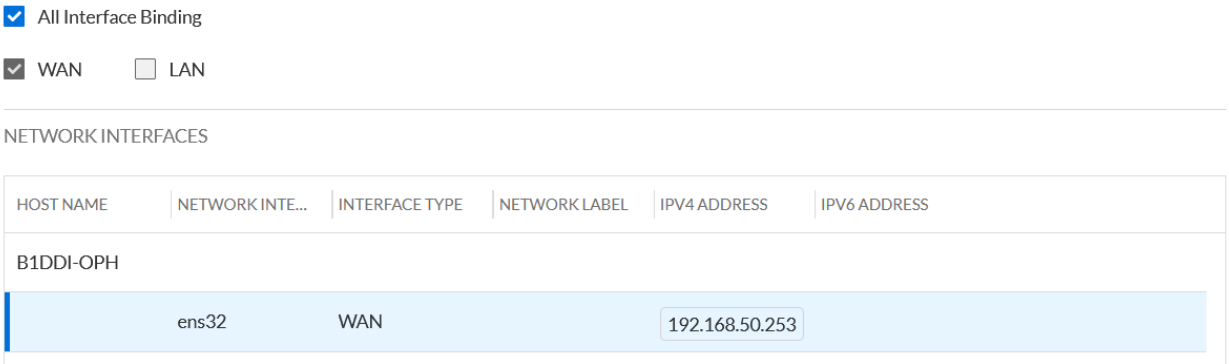
    - For each Tag Input a **Key** and **Value**.



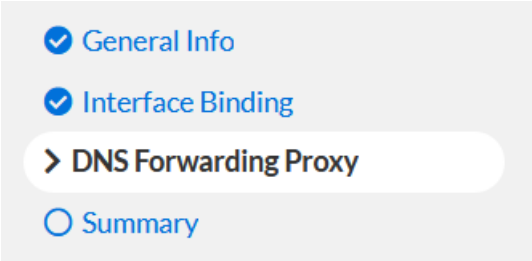
- (Optional) Click **Interface Binding** in the left navigation panel:



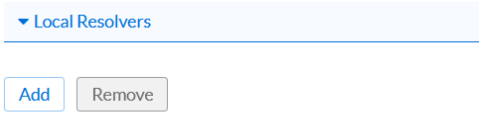
    - **Interface Bindings**: If desired you may select the interface the DFP service runs on. *Note the DFP service can be bound to WAN, LAN, a custom interface label, or all interfaces. This setting is set to All Interface Binding by default.*



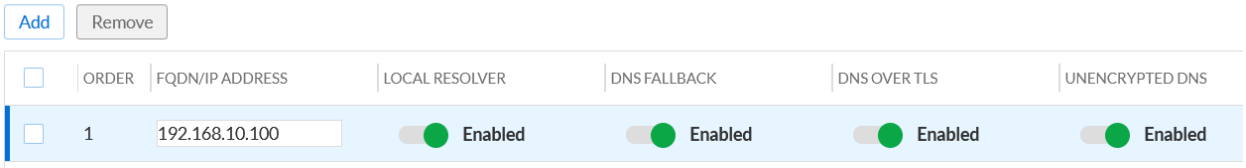
- Click **DNS Forwarding Proxy** in the left navigation panel. *Note the following settings on the DNS Forwarding Proxy page are optional and are not required to be configured for the DFP service to work.*



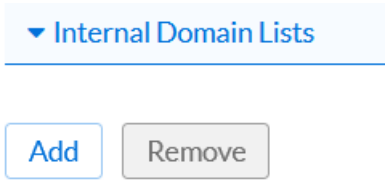
- Expand Local Resolvers. *Note In some networks it may be necessary for BloxOne to communicate with a local DNS server for the resolution of internal domains. To do this, a Local Resolver must be configured.*
    - To add a Local Resolver, click **Add**:



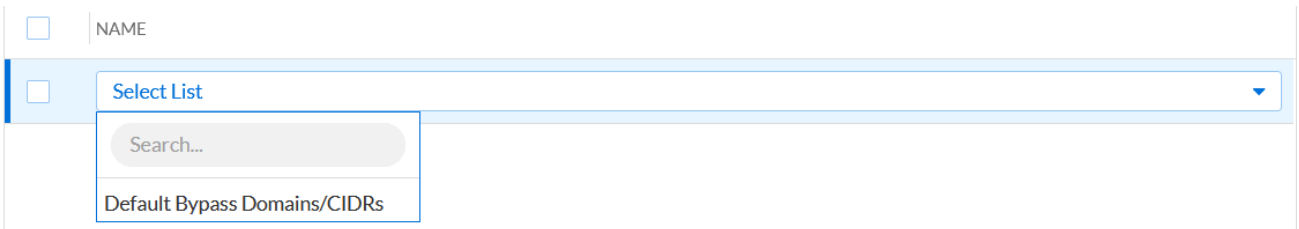
- For the new Local Resolver, configure the following settings:
    - **IP Address**: This is the IP address of the local DNS resolver. The IP address should be accessible to the BloxOne Host that the DFP service is attached to.
    - **Local Resolver**: A local resolver is a local server that stores a central database of DNS nameservers and manages DNS requests for all the clients on your network. This setting is Disabled by default.
    - **DNS Fallback**: DNS Fallback is a backup endpoint and is used when the primary server is unavailable. This setting is Disabled by default.
    - **DNS Over TLS:** Enable this setting to allow connectivity to the Local Resolver via DNS over TLS or DoT. This setting is Disabled by default.
    - **Unencrypted DNS:** Enable this setting to allow unencrypted DNS traffic to this Local Resolver. This setting is Disabled by default.



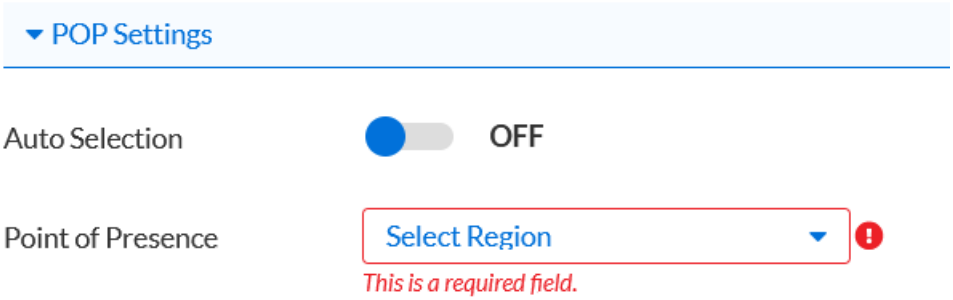
- Expand Internal Domain Lists
    - Click **Add** to add a new Internal Domains list. *Note: when a DNS query is made to a domain contained within an Internal Domain List, this query is sent directly to the local DNS server specified. Warning: Do not add Infoblox.com to an internal domain list, this will break some of BloxOne's functionality.*



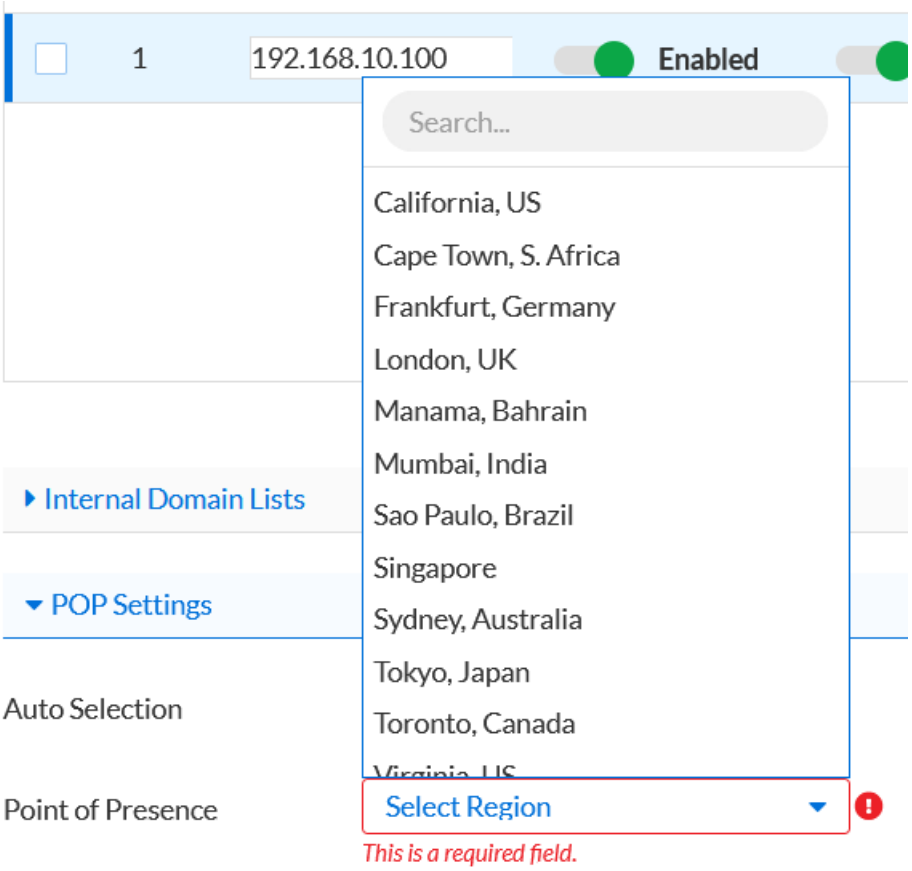
    - Use the dropdown to select an **Internal Domain List**. *By default, there is only one Internal Domain List, for more information on how to configure Internal Domain Lists please view the [Infoblox Documentation Portal]*



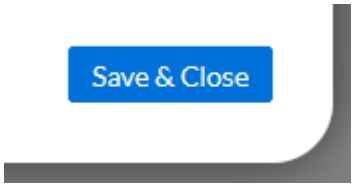
- Expand POP Settings
    - To choose a custom POP use the toggle switch to set Auto-Selection to **Off**. *By default, the service will choose the closest BloxOne POP. This occurs when the Toggle switch for Auto-Selection is set to On.*



    - To select a custom *Point of Presence*, use the **dropdown** and select a location.



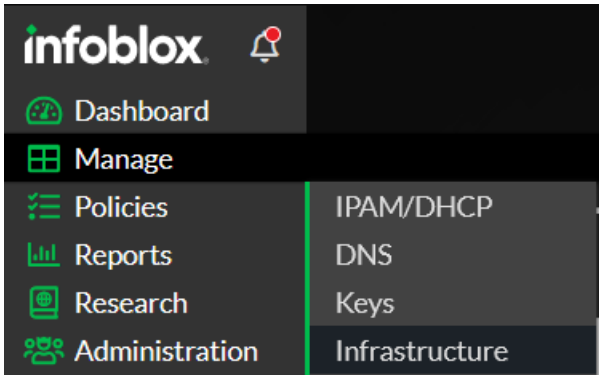
5. Click **Save & Close** to confirm the creation of the DFP Service.



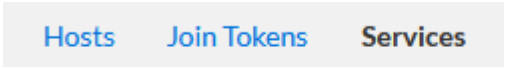
Editing the DFP Service post deployment

To make changes to the DFP service post deployment perform the following steps:

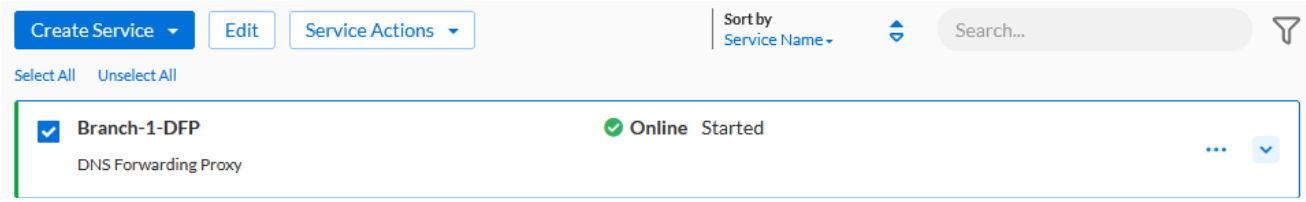
1. From the Cloud Services Portal, click **Manage** → **Infrastructure**.



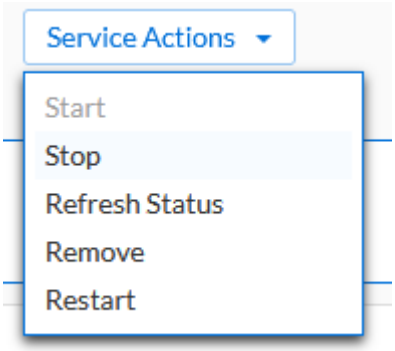
2. Click the **Services** tab.



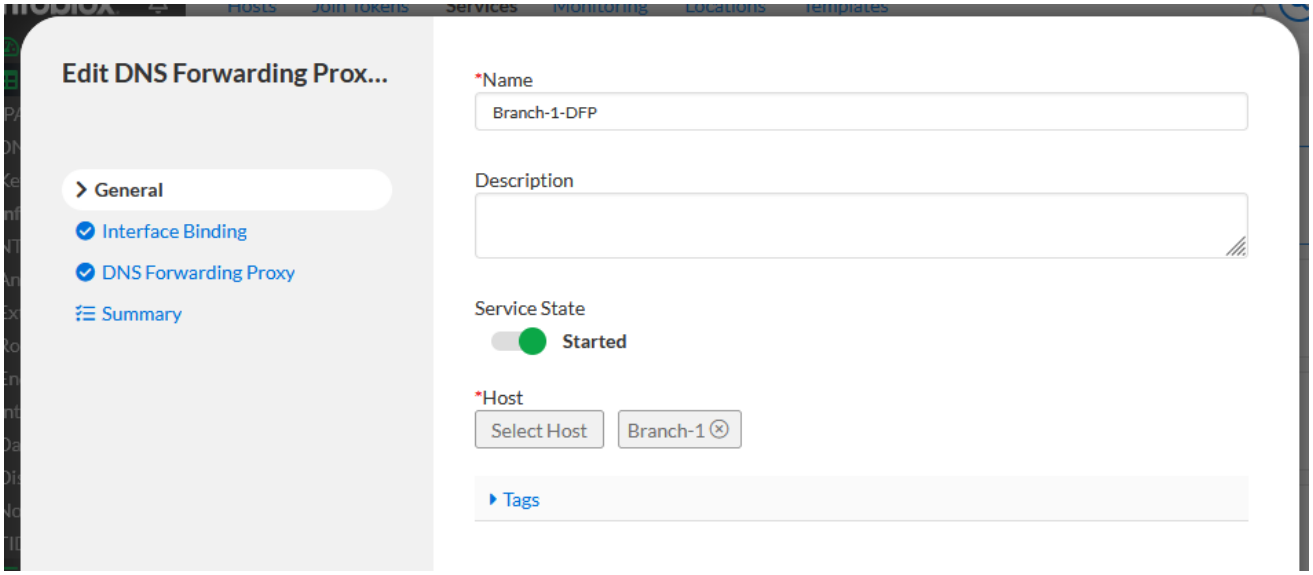
3. Locate the DFP service that you would like to edit in the list of services. Then, click the **checkbox** associated with the DFP.



4. At the top of the Services page click the **Service Actions** button.
    - In the Service Actions dropdown, you can **Start** the Service, **Stop** the Service, **Refresh** it's status, **Remove** the service, or **Restart** the Service.



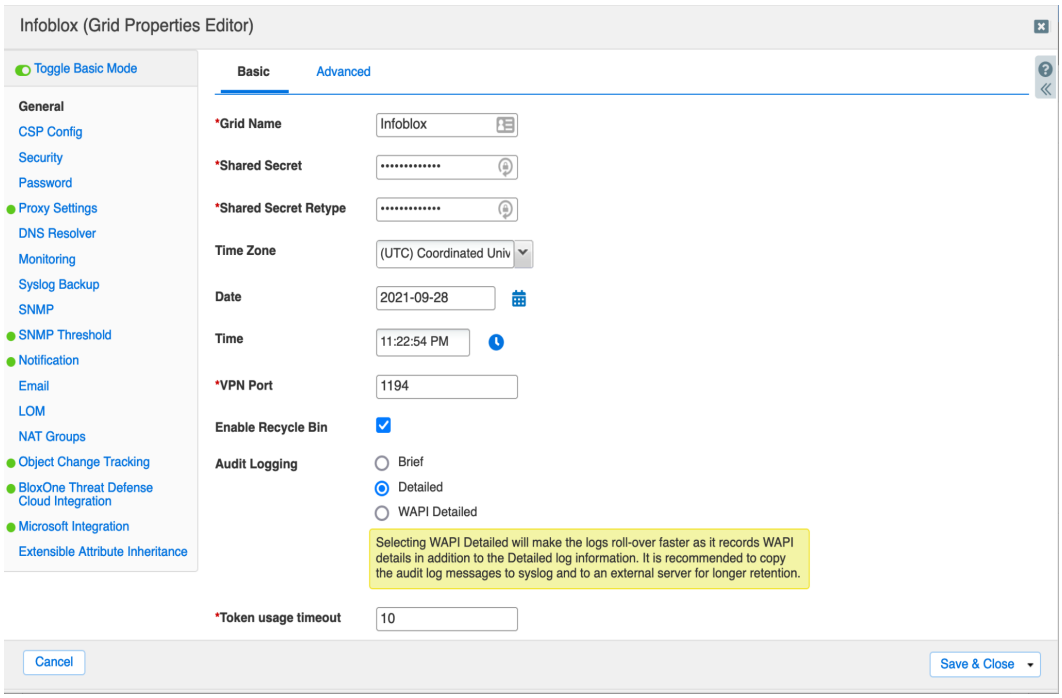
5. At the top of the Services page click the **Edit** button.
    - In the Edit DNS Forwarding Proxy panel you can edit all settings associated with the DFP. *Note for more information regarding each setting, view pages 3-8 of this guide.*



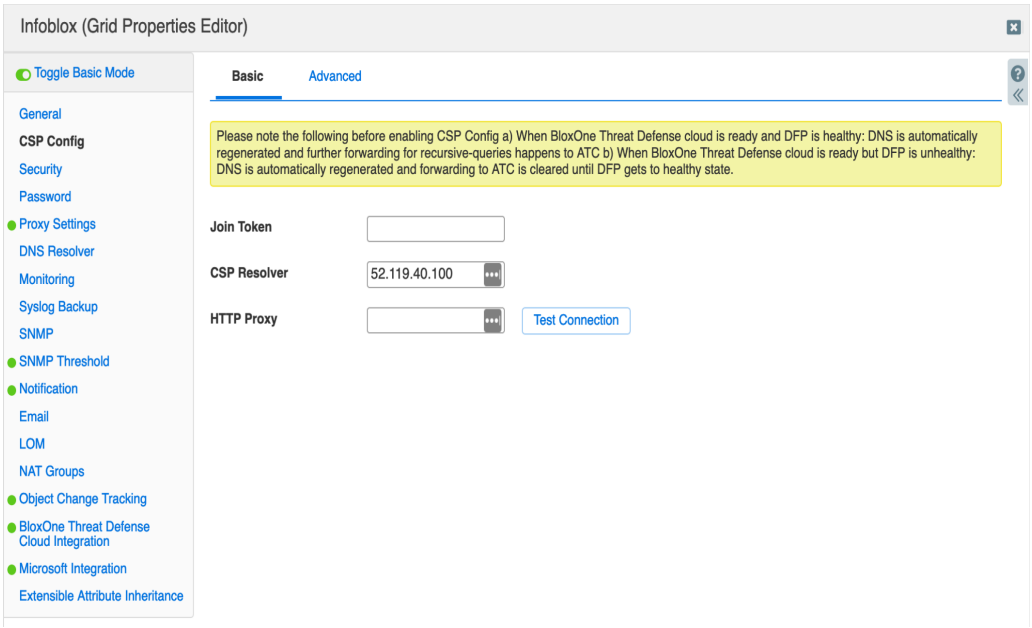
DFP on NIOS appliances with NIOS 8.5 and above

To enable DNS Forwarding Proxy on NIOS appliances running 8.5 or above perform the following steps:

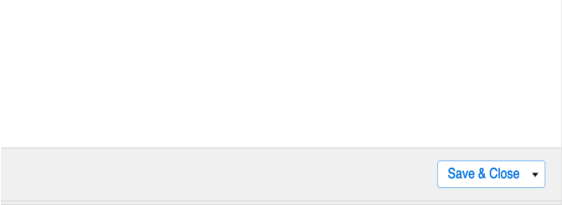
1. Navigate to **Grid** → **Grid Manager** → **Edit (In the toolbar)** → **Grid Properties**.



2. Click **CSP Config** located in the side panel of the Grid Properties Editor.



3. Enter a **Join Token** acquired from the Infoblox CSP in the *Join Token* field. *Note, for more information on acquiring a Join token, please refer to the [Infoblox Documentation Portal](#).*
4. (Optional) input a **HTTP Proxy** if needed.
5. Click **Save & Close**.



Additional Resources

- Deployment Guide: Configuring BloxOne DDI Post Deployment
- Infoblox BloxOne DDI Documentation
- Azure CLI 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