CONFIGURATION CHANGE GUIDE

BloxOne™ Security Policy Updates for SURBL EOS

Table of Contents

Overview

This document is intended to assist with the transition associated with the end of sale of SURBL feeds in BloxOne Threat Defense. SURBL feeds will no longer be available to BloxOne Threat Defense customers because Infoblox has determined that indicators in these feeds are duplicated in other feeds or not relevant. For users currently including SURBL feeds in their policies, Infoblox recommends enabling other feeds provided in BloxOne Threat Defense. This document covers how to remove SURBL feeds from BloxOne Security Policies and replace them with feeds that offer more effective coverage.

This document covers the removal of the following feeds that are reaching EOS:

SURBL Multi: This feed is a data set of malicious domains or abused web sites.

SURBL Multi Lite: An alternate set of the SURBL Threat Feed.

SURBL Fresh: Fresh is a list of domains that have been recently added to TLD zone file delegations.

The following feeds fill similar niches:

Infoblox NOED: The NOED feed consists of newly observed and emerging domains, some of which may not be inherently suspicious. However, monitoring traffic to these domains may be advisable since there is a low likelihood of their being visited under normal circumstances which raises the possibility of their being used for potentially nefarious purposes.

Infoblox Suspicious NOED: This feed includes high-risk, newly active domains. These domains have only recently become active and share one or more characteristics with other known malicious domains to warrant concern.

Anti-Malware: This set enables protection against hostnames that contain known malicious threats that can act on or take control of your system, such as malware command and control (C&C), malware download and active phishing sites.

Malware DGA: Domain generation algorithms (DGA) appear in various families of malware used to periodically generate many domain names that can act as rendezvous points with their C&C servers.

Base Hostnames: The base hostnames set enables protection against known hostnames that are dangerous as destinations and are sources of threats such as APTs, bots, compromised host/domains, exploit kits, malicious name servers and sinkholes.

Best Practices

Infoblox recommends the following as best practices for customers currently using the SURBL feeds described in this document.

- Remove all SURBL feeds from your BloxOne Security Policies and replace them with the recommendations below prior to the EOS date.
- When replacing feeds with the recommendations below, consider policy settings, e.g., logging vs blocking, of currently used feeds and replicate them for the replacements.
- Infoblox recommends all customers use the AntiMalware, Malware DGA, and Base feeds. Ideally, you are already using these feeds in your security policies. If you are not, enable them regardless of which SURBL feeds you are replacing.

Replacement Feed Mapping

This table shows the recommended replacements for each of the SURBL feeds. For **All Customers**, Feeds listed for Threat Defense Business should be used to replace the SURBL feeds.

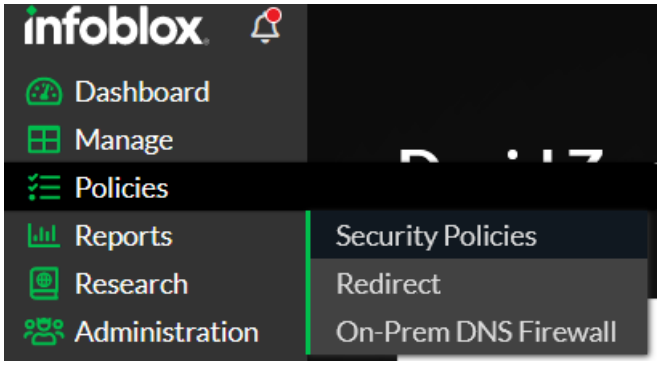
Customers with a BloxOne Threat Defense Advanced subscription should also consider enabling feeds shown for Threat Defense Advanced for even greater protection.

SURBL Feed	SURBL Fresh	SURBL Multi/SURBL Multi Lite
Threat Defense Business Feeds	Infoblox NOED	Antimalware Malware DGA Base
Threat Defense Advanced Feeds	Infoblox NOED Suspicious NOED	Antimalware Malware DGA Base Suspicious Domains Suspicious Lookalikes Suspicious NOED

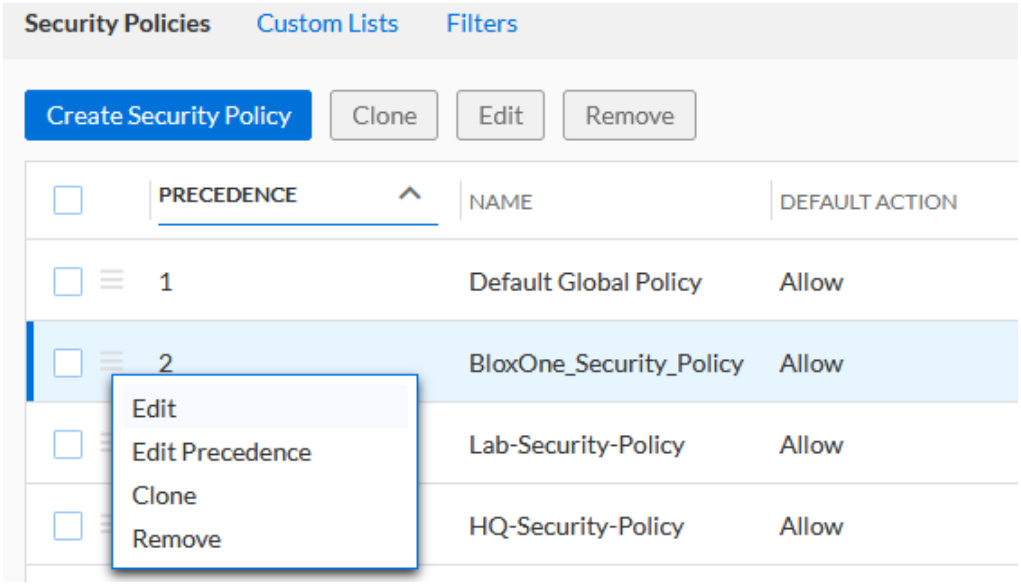
Remove SURBL feed from Security Policy

To remove SURBL feeds from an existing Security Policy, perform the following steps:

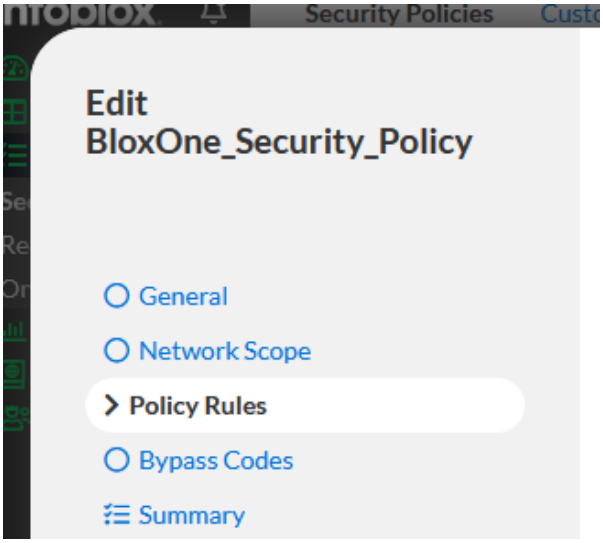
1. From the Cloud Services Portal, highlight **Policies**. Then click **Security Policies**.



2. Locate the Security Policy you wish to remove the SURBL feed from. Click the **Hamburger** icon associated with the Security policy. Then, click **Edit**.

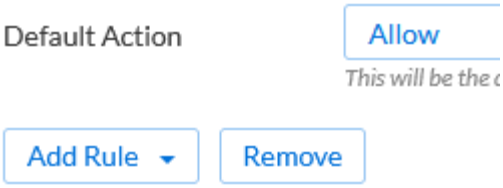


3. Click **Policy Rules** in the left navigation panel.

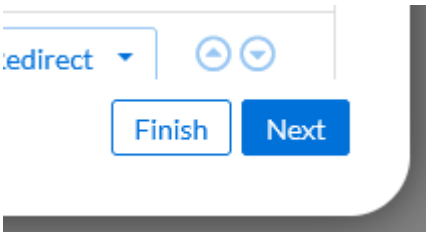


4. Click the **checkboxes** associated with the feeds **SURBL_Multi**, **SURBL_Multi_Lite**, and **SURBL_Fresh**. *Note, if the feed is not visible in the list, then it has not been added to the policy and does not need to be removed.*

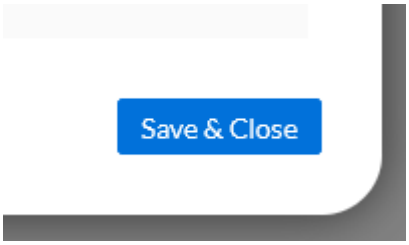
5. Click **Remove**.



6. Click **Finish**.



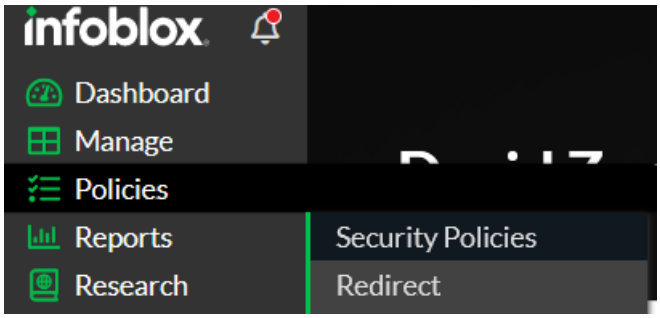
7. Click **Save & Close** to confirm the removal of the feeds from the Security Policy.



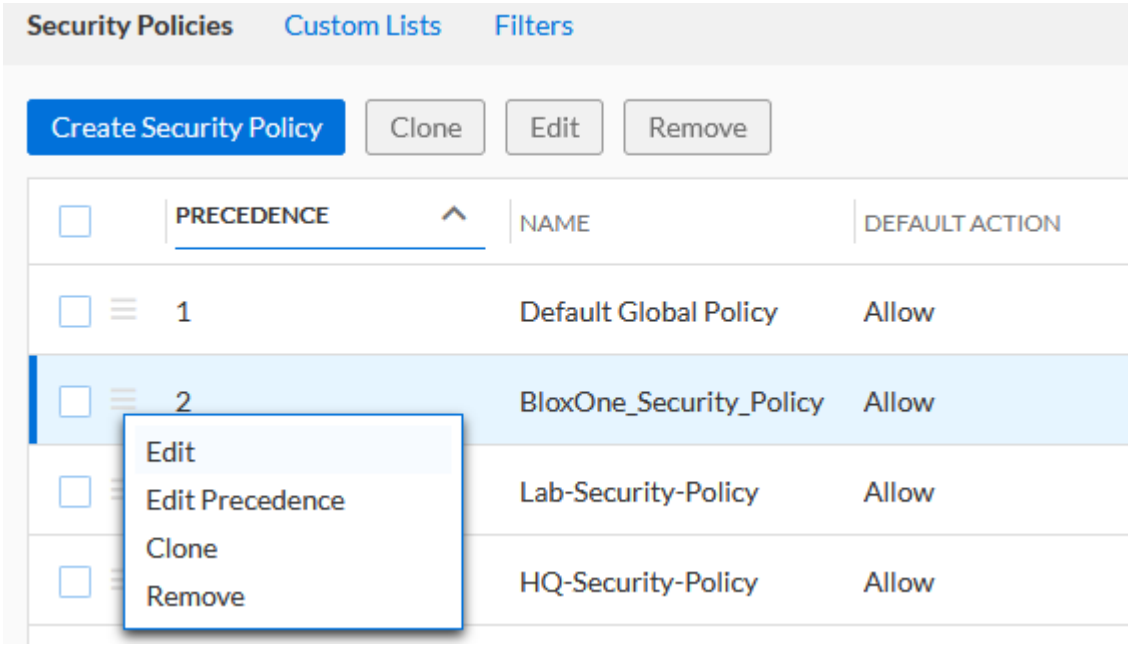
Add Feed to Security Policy

To add a Feed to an existing policy, perform the following steps:

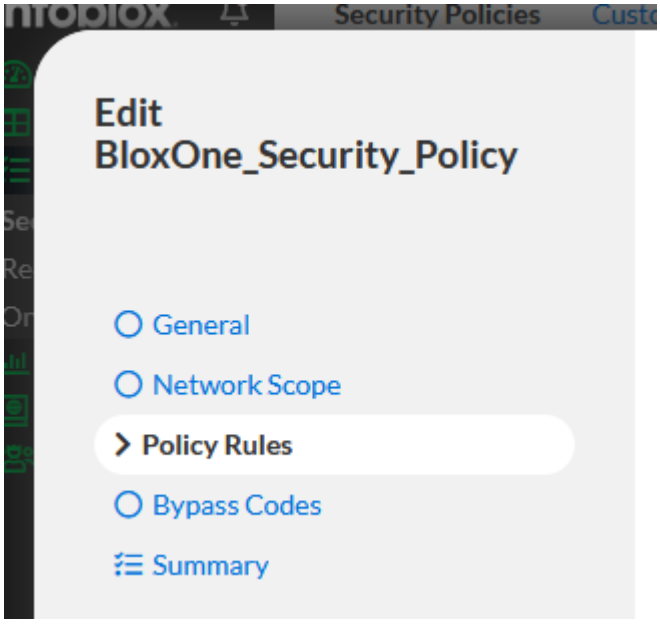
1. From the Cloud Services Portal, highlight **Policies**. Then click **Security Policies**.



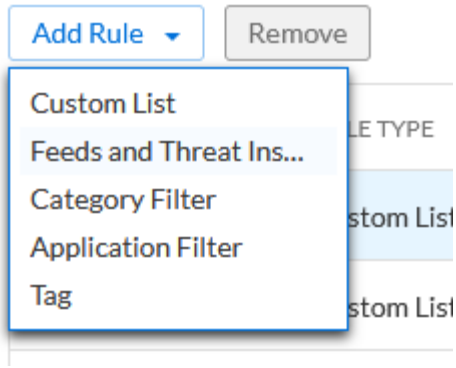
2. Locate the Security Policy you wish to add feeds to. Click the **Hamburger** icon associated with the Security policy. Then, click **Edit**.



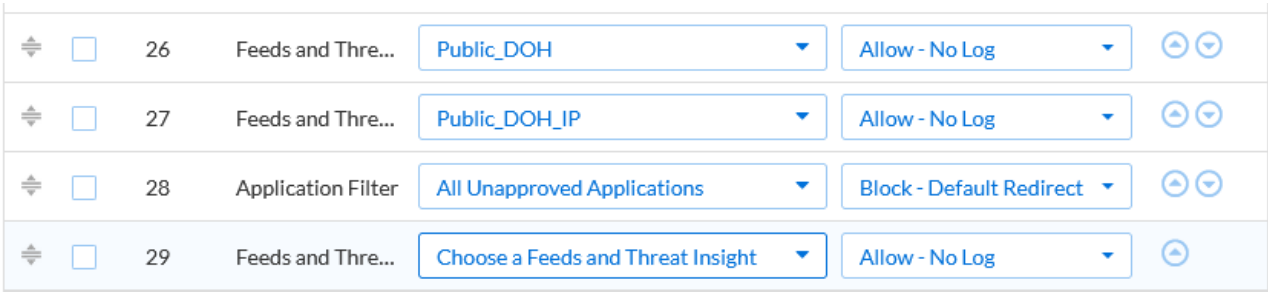
3. Click **Policy Rules** in the left navigation panel.



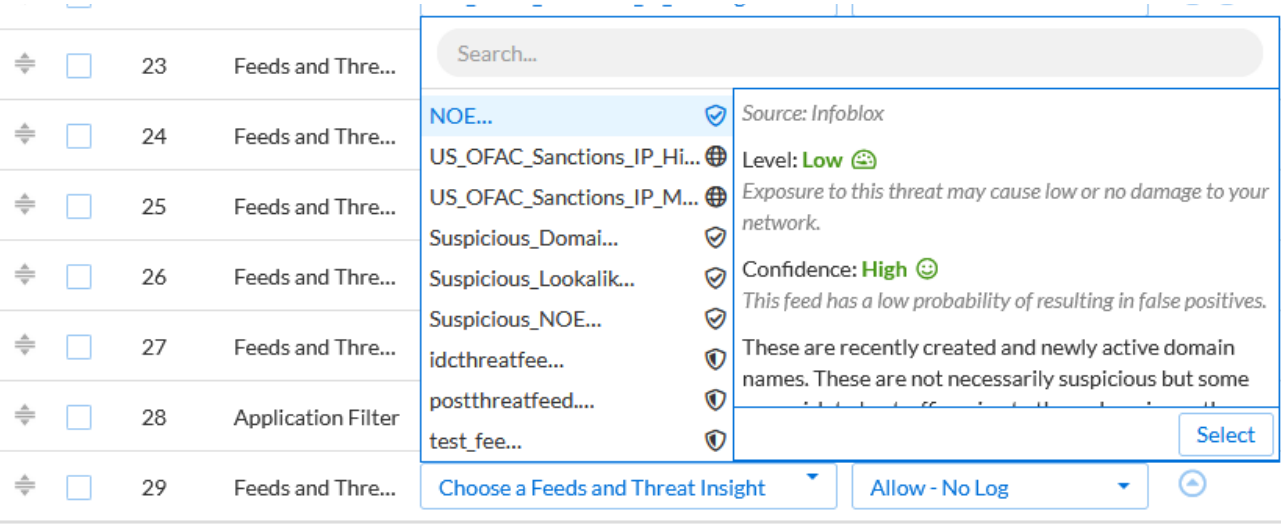
4. Click **Add Rule**. Then, click **Feeds and Threat Insight** in the list that is revealed.



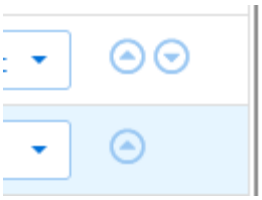
5. Locate the new entry in the Security Policy. *Note, the new Feed and Threat insight entry will be at the bottom of the Policy Rules list.*



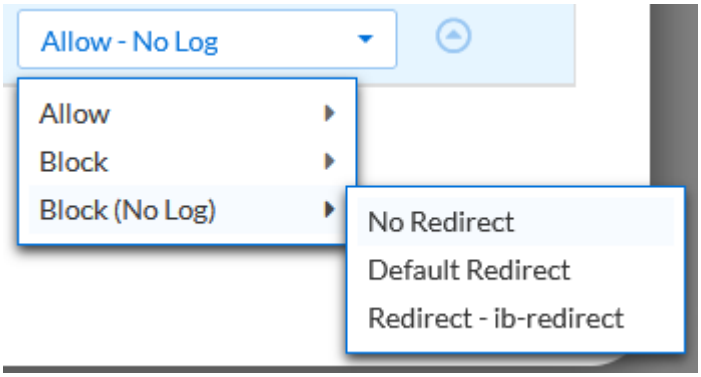
6. Click the dropdown labeled **Choose a Feeds and Threat Insight**. Select the feed that is to be added to the Security Policy. Once the new feed is selected, click **Select** to confirm the selection of the feed. *Note please refer to the Replacement Feed Mapping section for the suggested feeds. If a feed does not exist in the list it is not available for your subscription, or has already been added to this policy.*



7. Use the **Up** and **Down** arrows on the far right of the newly added Policy Rule to change the order at which the rule is checked. *Note, for the best results, it is highly suggested that any added feed from the Replacement Feed Mapping section should have the same priority as the associated SURBL feed that is being replaced.*

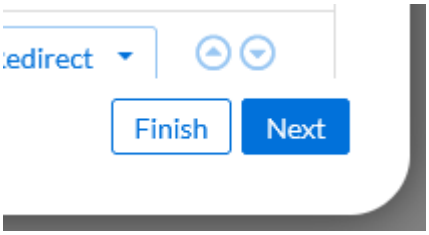


8. Change the **Action** that is associated with the newly added Policy Rule. *Note, for the best results, it is highly suggested that any added feed from the Replacement Feed Mapping section should have the same action as the associated SURBL feed that is being replaced.*

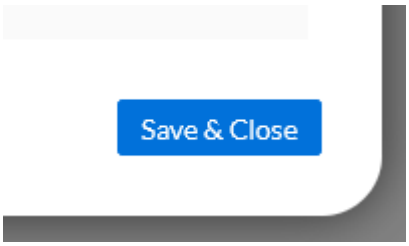


9. (Optional) If desired, add additional feeds by repeating *steps 4-8* in this section.

10. Click **Finish**.



11. Click **Save & Close** to confirm the addition of the new feed into the Security Policy.



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