Bandura Cyber GMC Release Notes

This document provides release notes for the Bandura Cyber Global Management Center (GMC).

The complete GMC User Manual can be retrieved from the Bandura Cyber Support Center, located here: https://helpdesk.banduracyber.com/hc/en-us.

RELEASE NOTES

Release: GMC Build 24 on 20 November 2020

New Features

ThreatSTOP threat intelligence integration with plugins to create:

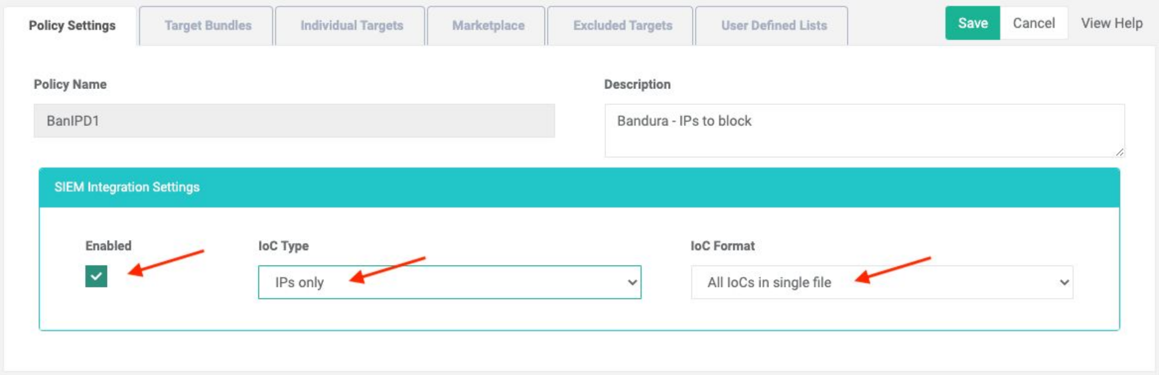
- IPv4 Denied List
- Domain Denied List
- IPv4 Allowed List
- Domain Allowed List

ThreatSTOP is a cloud-based automated threat intelligence platform that converts threat intelligence data into enforcement policies. ThreatSTOP leverages the company's comprehensive and authoritative database of IP addresses, domains and the network infrastructure used in cyberattacks to develop best-in-class threat intelligence.

The ThreatSTOP-Bandura integration enables mutual customers to easily integrate threat intelligence and enforcement policies from the ThreatSTOP platform into the Bandura platform. The ThreatSTOP plugin enables the simple and automated creation of IP and domain-based block lists based on ThreatSTOP threat intel and enforcement policies. The integration enables mutual customers to leverage the Bandura platform to use to detect and block IP and domain-based threats using threat intelligence at a scale that far exceeds the capabilities of existing network security controls.

To leverage the Bandura platform to use to detect and block IP and domain-based threats, customers can create and enable IPv4 or Domain Denied or Allowed Lists based on policies created with ThreatSTOP.

When creating a policy with ThreatSTOP, customers should ensure the policy is enabled under "SEIM Integration Settings". Customers will also want to ensure "All IoCs in single file" is chosen as the IoC format and note the IoC Type selected (IPs only, Domains only, or All IoCs).



Policy Name: BanIPD1

Description: Bandura - IPs to block

SIEM Integration Settings

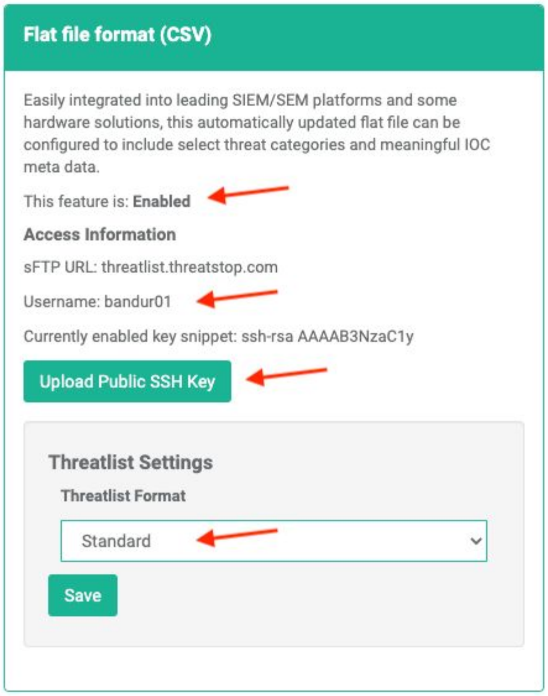
Enabled: ☑

IoC Type: IPs only

IoC Format: All IoCs in single file

After creating the policy with ThreatSTOP, customers will need to navigate to the “SEIM Integration” page on ThreatSTOP. In the “Flat file format (CSV)” block, ensure the feature states that it is enabled. Make sure to note the Username shown (which should be the same as the customer’s ThreatSTOP Org ID). Under “Threatlist Settings”, Standard should be selected as the Threatlist Format.

Finally, customers will need to create an SSH Key (using either RSA or OpenSSH). The Public SSH Key must be uploaded in the “Flat file format (CSV)” block. The Private SSH Key will be entered later when setting up a Denied or Allowed list in Bandura.



Flat file format (CSV)

Easily integrated into leading SIEM/SEM platforms and some hardware solutions, this automatically updated flat file can be configured to include select threat categories and meaningful IOC meta data.

This feature is: **Enabled**

Access Information

sFTP URL: threatlist.threatstop.com

Username: bandur01

Currently enabled key snippet: ssh-rsa AAAAB3NzaC1y

Threatlist Settings

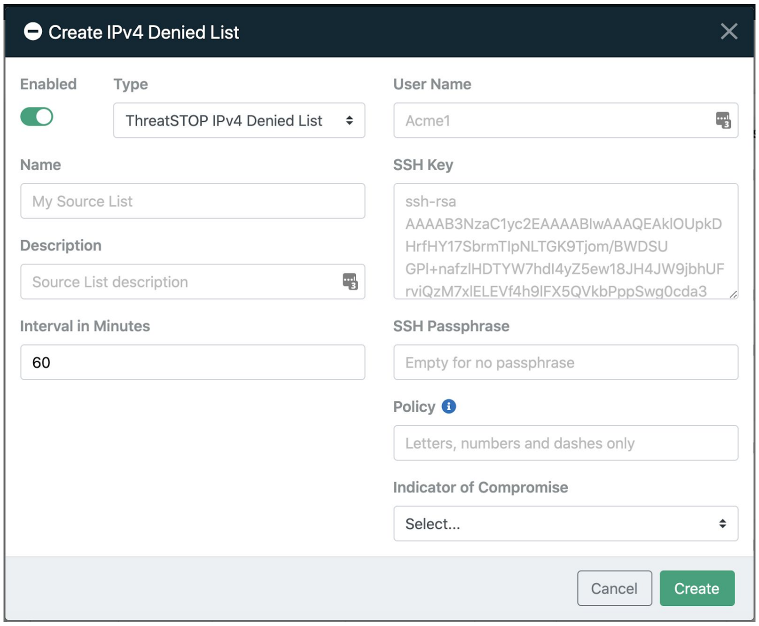
Threatlist Format: Standard

After a policy has been created and configurations are set with ThreatSTOP, customers can then create their Denied or Allowed lists in Bandura. In order to create a list, customers will need the following information:

- User Name - As mentioned above, this is found in the “Flat file format (CSV)” block on the “SEIM Integration” page on ThreatSTOP.
- SSH Key - This is the Private SSH Key that pairs with the Public SSH Key uploaded with ThreatSTOP.
- SSH Passphrase - If the SSH Key created is encrypted (highly recommended), a password to accompany the SSH Private Key is required.
- Policy - The exact name of the Policy to be used in the creation of the list.
- Indicator of Compromise - The IoC Type as established for the Policy in ThreatSTOP.

To create a list, log into the Bandura console and select either Denied or Allowed from the left menu, then choose either IPv4 or Domain. Click the green plus icon + in the top right corner. In the Create Denied or Allowed List modal that opens, Choose “ThreatSTOP [IPv4 or Domain] Denied List” as the Type. Give this list a name (required) and add a description if desired (optional). The recommended Interval in Minutes is 60, this represents how often Bandura will check for updates to the ThreatSTOP policy list.

To complete the setup of the list, customers will need to reference the fields mentioned above. Please note that each of these fields is case sensitive and must match to the values in ThreatSTOP exactly. For the SSH Key field, customers will need to enter the Private SSH Key exactly as was created, including any leading and trailing lines (such as “-----BEGIN OPENSSH PRIVATE KEY-----”, “-----END RSA PRIVATE KEY-----”, etc.).



Create IPv4 Denied List

Enabled

Type: ThreatSTOP IPv4 Denied List

Name: My Source List

Description: Source List description

Interval in Minutes: 60

User Name: Acme1

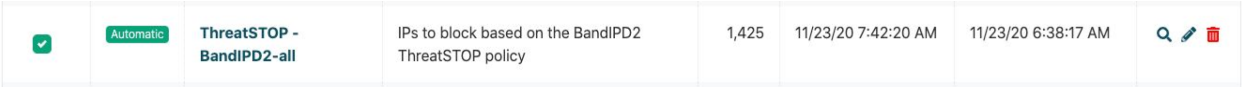
SSH Key: ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAklOUpkD HrfHY17SbrmTIpNLTGK9Tjom/BWDSU GPl+nafzlHDTYW7hdI4yZ5ew18JH4JW9jbhUF rviQzM7xlELEVf4h9lFX5QVkbPppSwg0cda3

SSH Passphrase: Empty for no passphrase

Policy: Letters, numbers and dashes only

Indicator of Compromise: Select...

After filling out the left side of the modal, customers should click on “Create” to add the new list. The newly created entry will be seen on the list. Please note that it may take 10-15 minutes to begin pulling the indicators from ThreatSTOP. Also, for newly created ThreatSTOP policies, the file pulled from ThreatSTOP can take up to 2 hours to be created and become available for Bandura to pull.



☑	Automatic	ThreatSTOP - BandIPD2-all	IPs to block based on the BandIPD2 ThreatSTOP policy	1,425	11/23/20 7:42:20 AM	11/23/20 6:38:17 AM	🔍 ✎ 🗑

If customers have any questions or need assistance in setting up ThreatSTOP Denied or Allowed Lists, please contact the Bandura Support team at **support@banduracyber.com** or by calling **+1-855-765-4925**.