

# 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>.

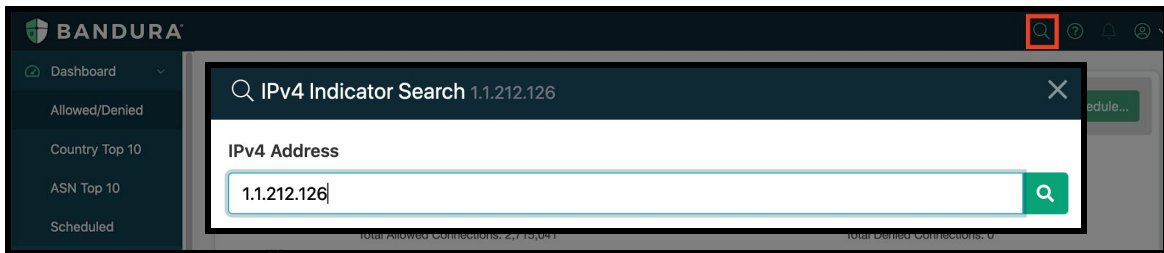
## RELEASE NOTES

**Release:** GMC Build 33 on 22 December 2020

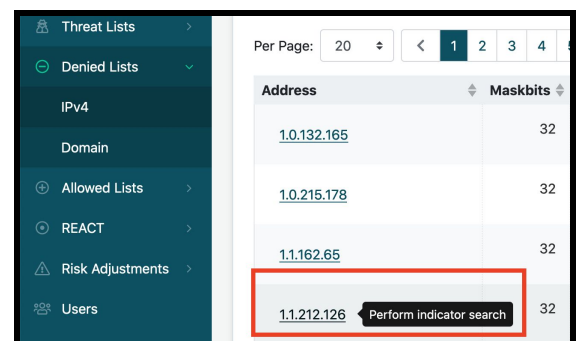
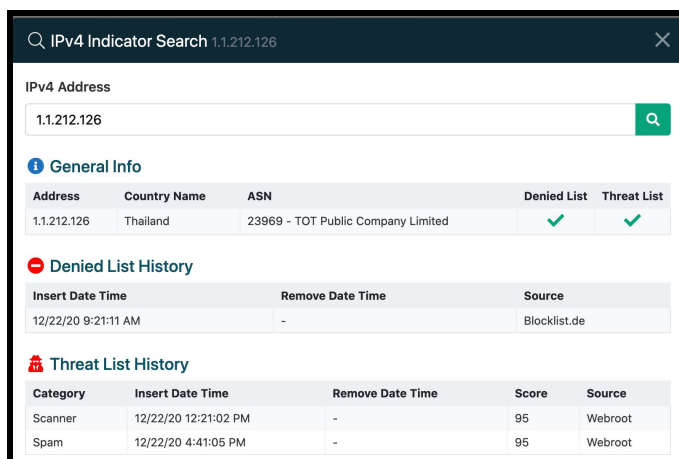
### New Features & Enhancements

#### Indicator of Compromise (IOC) Search:

Users now have the ability to search any IP Address and see if it is a malicious actor! To perform a search, simply select the spyglass icon in the top right corner of the screen, enter an IP address, and select the search icon in the modal.



The results that display will provide general information on the IP address and will indicate if the IP is included in any of our Bandura Threat or Denied feeds. Within a Bandura provided feed, users can also perform the search by selecting the hyperlinked IP address.

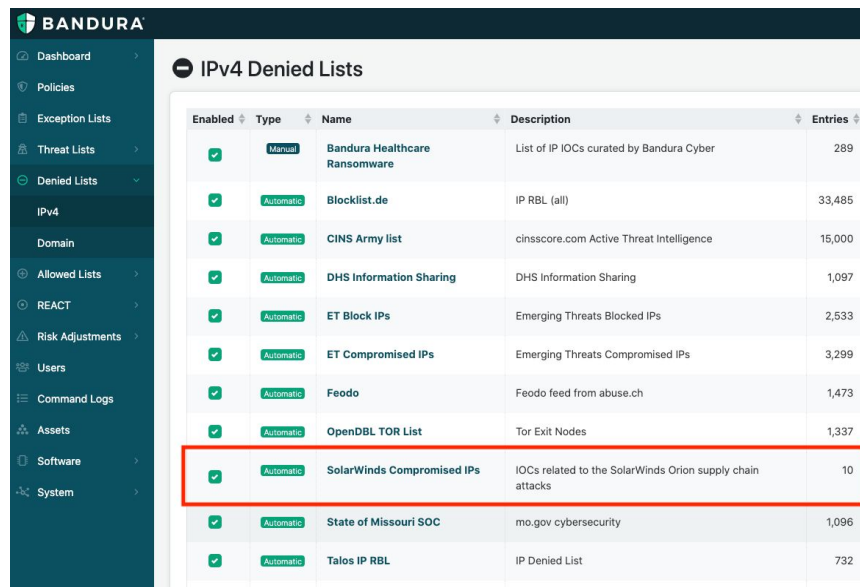


## SolarWinds Compromised IP and Domain Denied Lists:

We have added a new source to each of these lists, which are available now to all customers and can be found in the IPv4 and Domain Denied List pages. When the lists were released on December 15, they included integration with the FireEye published indicators of compromise. We have now added integration with the recently published US-CERT Stix file.

Like all of our threat intelligence data, these lists will be automatically updated with the most current threat indicators as they are released.

**Please note: These lists will not be enabled by default.** You can enable them on your Denied Lists by checking the Enabled checkbox as seen below. **Bandura STRONGLY recommends enabling these lists ASAP.**



Enabled	Type	Name	Description	Entries
<input checked="" type="checkbox"/>	Manual	Bandura Healthcare Ransomware	List of IP IOCs curated by Bandura Cyber	289
<input checked="" type="checkbox"/>	Automatic	Blocklist.de	IP RBL (all)	33,485
<input checked="" type="checkbox"/>	Automatic	CINS Army list	cinsscore.com Active Threat Intelligence	15,000
<input checked="" type="checkbox"/>	Automatic	DHS Information Sharing	DHS Information Sharing	1,097
<input checked="" type="checkbox"/>	Automatic	ET Block IPs	Emerging Threats Blocked IPs	2,533
<input checked="" type="checkbox"/>	Automatic	ET Compromised IPs	Emerging Threats Compromised IPs	3,299
<input checked="" type="checkbox"/>	Automatic	Feodo	Feodo feed from abuse.ch	1,473
<input checked="" type="checkbox"/>	Automatic	OpenDBL TOR List	Tor Exit Nodes	1,337
<input checked="" type="checkbox"/>	Automatic	SolarWinds Compromised IPs	IOCs related to the SolarWinds Orion supply chain attacks	10
<input checked="" type="checkbox"/>	Automatic	State of Missouri SOC	mo.gov cybersecurity	1,096
<input checked="" type="checkbox"/>	Automatic	Talos IP RBL	IP Denied List	732

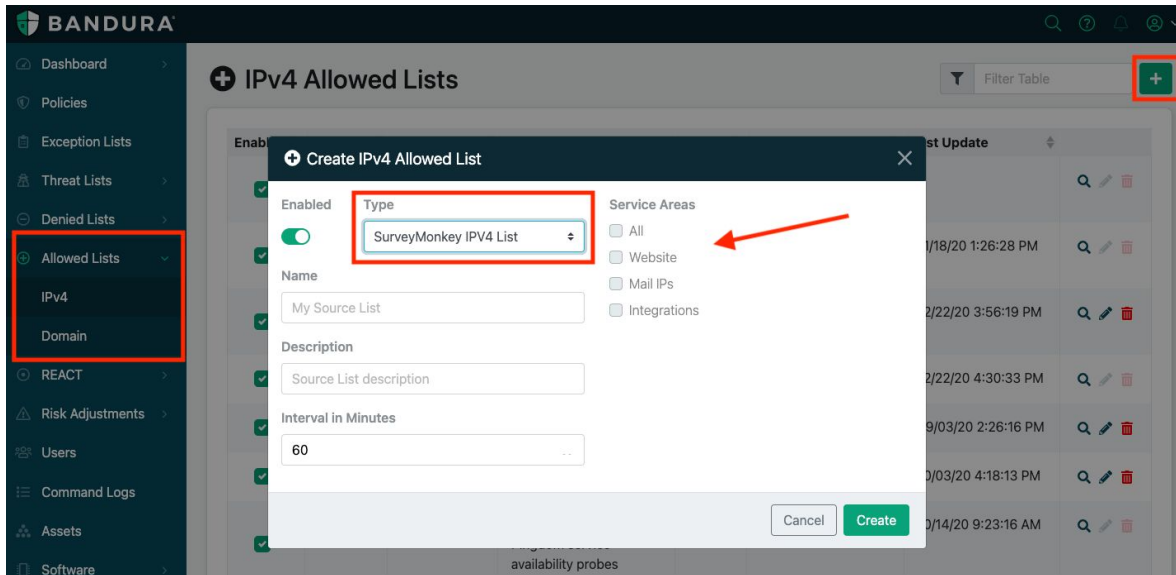
For more information about the SolarWinds attack, check out our [blog post](#) detailing the denied lists publication.

If you have any questions about these lists, feel free to reach out to our customer support team at [customersupport@banduracyber.com](mailto:customersupport@banduracyber.com).

## SurveyMonkey IPv4 and Domain Allowed Lists:

Customers utilizing SurveyMonkey services can now ensure traffic is not blocked by your ThreatBlockr by using the new SurveyMonkey plugins to create IPv4 and Domain Allowed Lists.

These plugins are easy to set up and configure and are available via the Create button in the top-right corner of the Allowed List - both IPv4 and Domain - screens.



Customers can choose to allow all service areas - Website, Mail IPs, and Integrations for IPv4 and Site Domains and Mail Sender Domains for Domain.