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

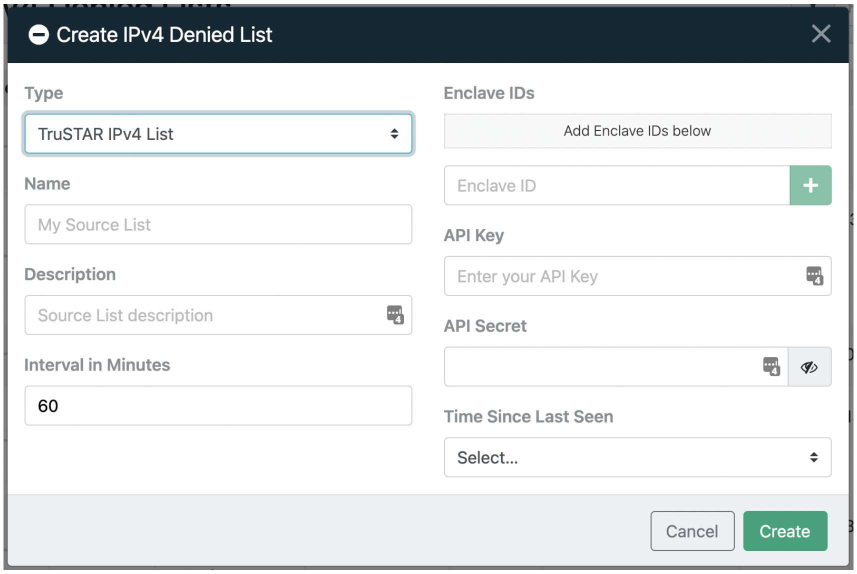
Release: GMC Build 48 on March 26, 2021

New Features:

TruSTAR Threat Intelligence integration:

Customers with access to threat intelligence through the TruSTAR Intelligence Management Platform are now able to leverage our new IPv4 and Domain Denied List plugins to block traffic using indicators pulled from TruSTAR enclaves.

To integrate your TruSTAR threat intelligence in GMC select Denied List from the navigation and choose IPv4 or Domain. In the top right corner click the green "+" icon. In the Create modal, select "TruSTAR" from the "Type" dropdown.



Create IPv4 Denied List

Type: TruSTAR IPv4 List

Interval in Minutes: 60

Time Since Last Seen: Select...

Give your list a name and, if you'd like, a description. We recommend checking for updates every 60 minutes, however you may choose to adjust the interval if you wish.

Enter your Enclave Id as found in your TruSTAR User Profile Settings under "View Enclave

Subscriptions”. You may also obtain the Enclave Id from the Enclave member organization, if applicable. Click the green “+” icon to add the Enclave Id. You may enter one or more Enclave Ids to pull indicators from.

Next, enter your TruSTAR API Key and your API Secret as found in your TruSTAR API Settings. You may also obtain the API Key and API Secret from the Enclave member organization, if applicable.

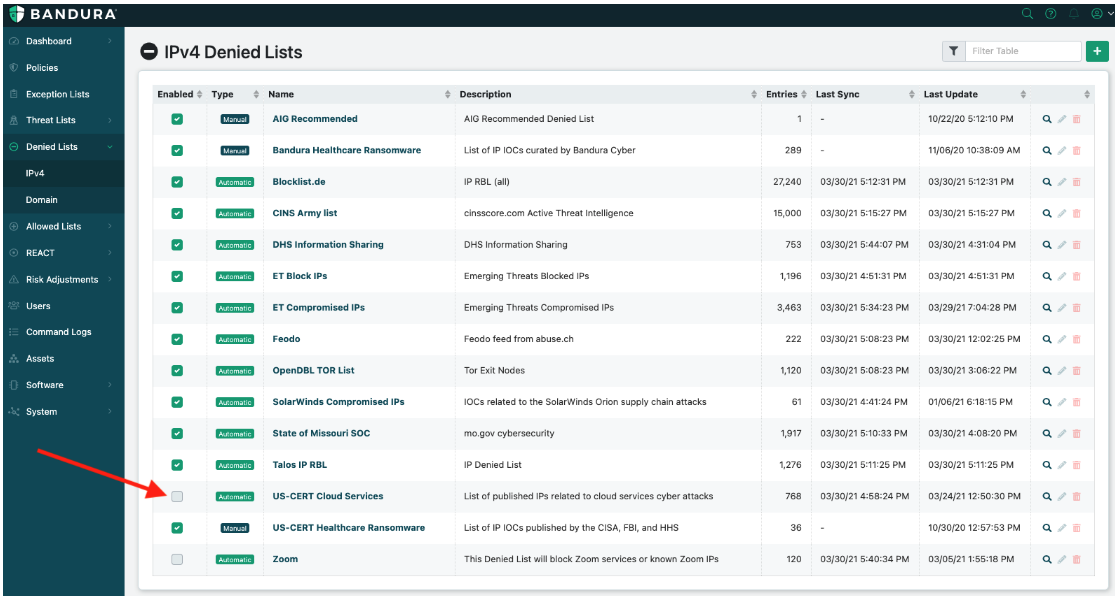
Finally, select the Time Since Last Seen value to determine the age of the indicators you wish to pull and click on "Create" to add the feed to your list. Please allow anywhere from 15-30 minutes for the indicators to populate.

To learn more about TruSTAR, please visit their website at trustar.co. If customers have any questions or need assistance in setting up TruSTAR Denied Lists using the plugin, please contact the Bandura Support team at **support@banduracyber.com** or by calling **+1-855-765-4925**.

US-CERT Cloud Services cyber attack protection:

The United States Computer Emergency Readiness Team (US-CERT), an organization within the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency, recently issued an alert regarding threat actors attempting to exploit poor cyber hygiene and phishing tactics through attacks against organizations’ cloud services.

As part of the alert, US-CERT included reference to a STIX file containing indicators of compromise. Bandura has created an automated IPv4 Denied list that allows customers to block traffic based on the IOCs provided. To enable the list in GMC, select Denied List from the navigation and choose IPv4. You will find the list, entitled “US-CERT Cloud Services”, on the page and ready to be enabled. Simply click on the “Enabled” check box in the left column and you will now be protected.



IPv4 Denied Lists

Enabled	Type	Name	Description	Entries	Last Sync	Last Update
☑	Manual	AIG Recommended	AIG Recommended Denied List	1	-	10/22/20 5:12:10 PM
☑	Manual	Bandura Healthcare Ransomware	List of IP IOCs curated by Bandura Cyber	289	-	11/06/20 10:38:09 AM
☑	Automatic	Blocklist.de	IP RBL (all)	27,240	03/30/21 5:12:31 PM	03/30/21 5:12:31 PM
☑	Automatic	CINS Army list	cinsscore.com Active Threat Intelligence	15,000	03/30/21 5:15:27 PM	03/30/21 5:15:27 PM
☑	Automatic	DHS Information Sharing	DHS Information Sharing	753	03/30/21 5:44:07 PM	03/30/21 4:31:04 PM
☑	Automatic	ET Block IPs	Emerging Threats Blocked IPs	1,196	03/30/21 4:51:31 PM	03/30/21 4:51:31 PM
☑	Automatic	ET Compromised IPs	Emerging Threats Compromised IPs	3,463	03/30/21 5:34:23 PM	03/29/21 7:04:28 PM
☑	Automatic	Feodo	Feodo feed from abuse.ch	222	03/30/21 5:08:23 PM	03/30/21 12:02:25 PM
☑	Automatic	OpenDBL TOR List	Tor Exit Nodes	1,120	03/30/21 5:08:23 PM	03/30/21 3:06:22 PM
☑	Automatic	SolarWinds Compromised IPs	IOCs related to the SolarWinds Orion supply chain attacks	61	03/30/21 4:41:24 PM	01/06/21 6:18:15 PM
☑	Automatic	State of Missouri SOC	mo.gov cybersecurity	1,917	03/30/21 5:10:33 PM	03/30/21 4:08:20 PM
☑	Automatic	Talos IP RBL	IP Denied List	1,276	03/30/21 5:11:25 PM	03/30/21 5:11:25 PM
□	Automatic	US-CERT Cloud Services	List of published IPs related to cloud services cyber attacks	768	03/30/21 4:58:24 PM	03/24/21 12:50:30 PM
☑	Manual	US-CERT Healthcare Ransomware	List of IP IOCs published by the CISA, FBI, and HHS	36	-	10/30/20 12:57:53 PM
□	Automatic	Zoom	This Denied List will block Zoom services or known Zoom IPs	120	03/30/21 5:40:34 PM	03/05/21 1:55:18 PM

To learn more about using Denied Lists to protect your network, please contact the Bandura Support team at **support@banduracyber.com** or by calling **+1-855-765-4925**.