



Recorded Future Plugin Installation Instructions

Creating an Automated IP or Domain Denied List

1. In Bandura Cyber Global Management Center (GMC), click Denied Lists on the left menu. Select IPv4 to create an automated IP denied list or select Domains to create an automated domain denied list. The process is the same for both. After selecting IPv4 or Domains, click the green plus sign in the upper right corner of the screen.

Enabled	Type	Name	Description	#	Last Update	
<input checked="" type="checkbox"/>	Automatic	Blocklist.de	IP RBL (all)	28,744	08/17/20 9:36:07 AM	
<input checked="" type="checkbox"/>	Automatic	CINS Army list	cinsscore.com Active Threat Intelligence	15,000	08/17/20 10:07:15 AM	
<input checked="" type="checkbox"/>	Automatic	DHS Information Sharing	DHS Information Sharing	149,756	08/17/20 3:31:03 PM	

2. On the Create IPv4 or Domain Denied List screen, from the Type dropdown menu a Name and Description for your blacklist, select the Interval you wish to pull indicators from Recorded Future, and select **Recorded Future** from the Plugin Name dropdown list. The Configuration screen will appear automatically.

Create IPv4 Denied List

Enabled:

Type: Manual

Name: My Source List

Description: Source List desc

Plugins: Recorded Future

- Abuse IPv4 Lists
- AlienVault OTX IPv4
- Basic IPv4 address list
- E-ISAC IPv4 Lists
- Exception List to IPv4 deny list
- FS-ISAC IPv4 Lists
- H-ISAC IPv4 Lists
- IP2Proxy
- IntSights
- MS-ISAC IPv4
- Recorded Future**
- Recorded Future Security Control
- STIX/TAXII IPv4 address list
- ThreatConnect IPv4 List



3. Configuring the Recorded Future Plugin is easy. Enter your API Key from Recorded Future. Name your Denied List and give it a Description. Select the Interval you would like to pull indicators and the Risk Score (1-100). Click Create. In a matter of minutes, your Recorded Future Denied List should begin to populate.

The screenshot shows the 'IPv4 Denied Lists' management interface. A modal window titled 'Create IPv4 Denied List' is open, allowing the user to configure a new list. The background shows a table of existing lists with columns for 'Enabled', 'Type', 'Name', and 'Description'. The modal window contains the following fields:

- Enabled:** A toggle switch is turned on.
- Type:** A dropdown menu is set to 'Recorded Future'.
- API Key:** A text input field containing 'YOUR_API_KEY'.
- Name:** A text input field containing 'Recorded Future IP Denied List'.
- Risk Level:** A slider control set to 90.
- Description:** A text input field containing 'Malicious IPs from Recorded Future'.
- Interval in Minutes:** A text input field containing '60'.

At the bottom of the modal, there are 'Cancel' and 'Create' buttons.



BANDURA®

Creating an Automated Blacklist based on Security Control Feeds

1. In Bandura Cyber Global Management Center (GMC), click Denied Lists on the left menu. Select IPv4 to create an automated IP denied list or select Domains to create an automated domain denied list. The process is the same for both. After selecting IPv4 or Domains, click the green plus sign in the upper right corner of the screen.

Enabled	Type	Name	Description	#	Last Update	
<input checked="" type="checkbox"/>	Automatic	Blocklist.de	IP RBL (all)	28,744	08/17/20 9:36:07 AM	
<input checked="" type="checkbox"/>	Automatic	CINS Army list	cinsscore.com Active Threat Intelligence	15,000	08/17/20 10:07:15 AM	
<input checked="" type="checkbox"/>	Automatic	DHS Information Sharing	DHS Information Sharing	149,756	08/17/20 3:31:03 PM	

2. On the Create IPv4 or Domain Denied List screen, from the Type dropdown menu a Name and Description for your blacklist, select the Interval you wish to pull indicators from Recorded Future, and select **Recorded Future Security Control** from the Plugin Name dropdown list. The Configuration screen will appear automatically.

IPv4 Denied Lists

Enabled	Type	Name	Description
<input checked="" type="checkbox"/>	Automatic	Blocklist.de	
<input checked="" type="checkbox"/>	Automatic	CINS Army list	
<input checked="" type="checkbox"/>	Automatic	DHS Information Sharing	
<input checked="" type="checkbox"/>	Automatic	ET Block IPs	
<input checked="" type="checkbox"/>	Automatic	ET Compromised IPs	
<input checked="" type="checkbox"/>	Automatic	Feodo	
<input checked="" type="checkbox"/>	Automatic	OpenDBL TOR List	
<input checked="" type="checkbox"/>	Automatic	State of Missouri SOC	mo.gov
<input checked="" type="checkbox"/>	Automatic	TW Cool Deny List	

Create IPv4 Denied List

Enabled:

Type: **Manual**

Name: My Source List

Description: Source List desc

Plugins

- Abuse IPv4 Lists
- AlienVault OTX IPv4
- Basic IPv4 address list
- E-ISAC IPv4 Lists
- Exception List to IPv4 deny list
- FS-ISAC IPv4 Lists
- H-ISAC IPv4 Lists
- IP2Proxy
- IntSights
- MS-ISAC IPv4
- Recorded Future
- Recorded Future Security Control**
- STIX/TAXII IPv4 address list
- ThreatConnect IPv4 List



BANDURA®

3. Configuring the Recorded Future Plugin is easy. Enter your API Key from Recorded Future. Name your Denied List and give it a Description. Select the Interval you would like to pull indicators and select which Security Control Feeds you want to pull. Click Create. In a matter of minutes, your Recorded Future Denied List should begin to populate.

The screenshot displays the 'IPv4 Denied Lists' management interface. A modal window titled 'Create IPv4 Denied List' is open, allowing for the configuration of a new denied list. The background shows a table of existing lists with columns for 'Enabled', 'Type', 'Name', and 'Description'. The modal form includes the following fields and options:

- Enabled:** A toggle switch is turned on.
- Type:** A dropdown menu is set to 'Recorded Future Security Contrc'.
- API Key:** A text input field containing 'YOUR_API KEY'.
- Name:** A text input field containing 'Recorded Future IP SCF'.
- Description:** A text input field containing 'Denied List based on Recorded Future'.
- Interval in Minutes:** A text input field containing '60'.
- Security Control Feeds:** A list of checkboxes with the following items checked: 'Active RAT C2 Infrastructure IPs', 'Command and Control IPs (Prevent)', 'Dynamic DNS Hosts IPs', 'Fast Flux Hosts IPs', and 'Tor IPs'. 'Command and Control IPs (Detect)' is unchecked.

At the bottom right of the modal, there are 'Cancel' and 'Create' buttons.