LINKSHADOW®
Combat the Dark

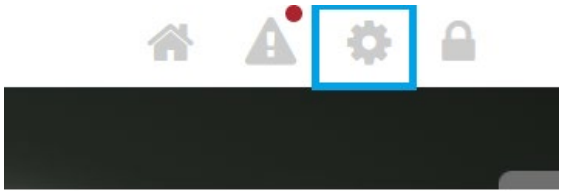
LinkShadow

and Cisco ISE Integration Guide

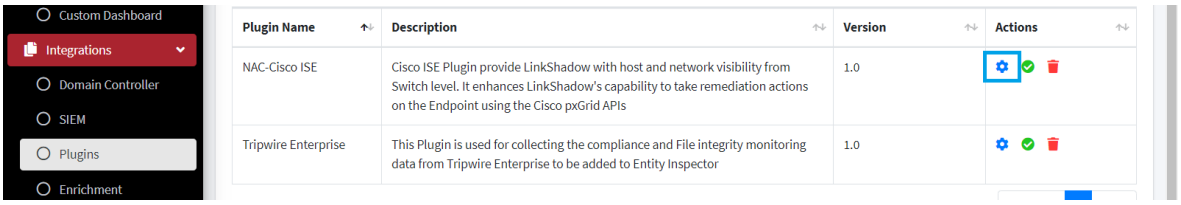
www.linkshadow.com

To integrate Cisco ISE with LinkShadow follow the following steps:

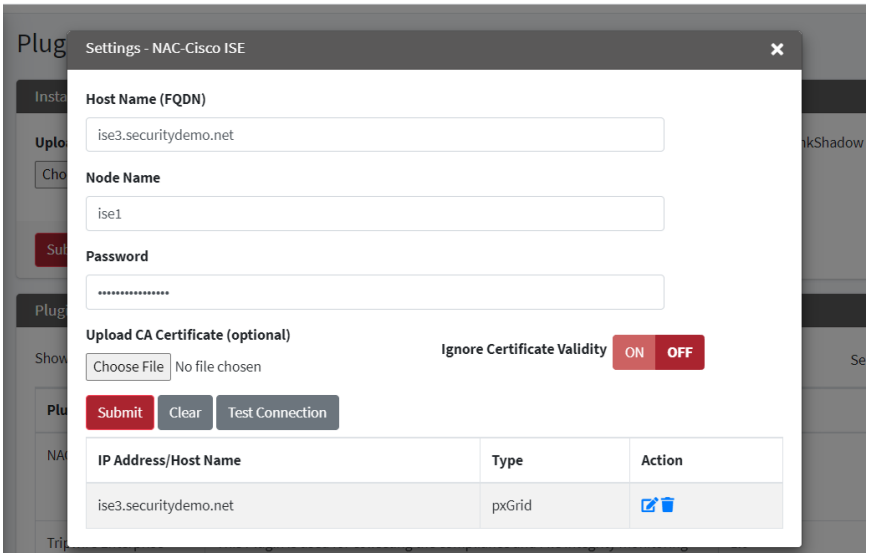
1- Go to Settings by Clicking on the gear icon on the top right corner



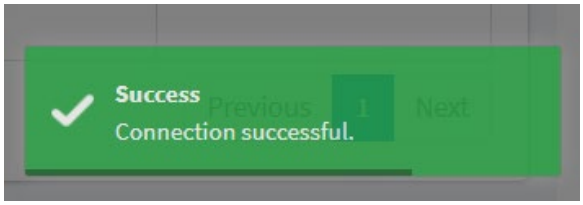
2- **In the settings page, on the left section, click on Integrations -> Plugins**.
Search for the NAC-Cisco ISE plugin and click on the blue gear icon to open the settings for the plugin. A screenshot is shown below.



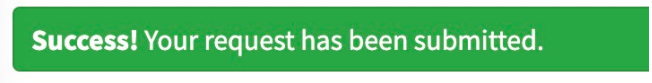
3- Enter the required information into the fields mentioned below:



- Host Name (FQDN): This should be the Fully Qualified Domain Name of the ISE node running the pxGrid service.
- Node Name: This is your client node name (username)
- Password: This is the password that you generated for pxGrid authentication
- To find out how to generate the password, please refer to the official documentation from Cisco here: https://d1nmyq4gcgsfi5.cloudfront.net/fileMedia/ea02ce59-2668-441a-601d-0c6ca59d8bf4/CiscopxGrid20_je.pdf
- Upload the CA certificate if needed
- Choose whether you want to ignore the certificate's validity or not
- Click on the 'Test Connection' button to check whether LinkShadow can successfully authenticate against ISE. You will see a message at the bottom right corner of the screen telling you whether it was successful or not. A successful message is shown in the screenshot.



4- Submit



Once the information is saved successfully, you can continue with adding additional pxGrid nodes into LinkShadow. If a pxGrid node is unreachable, LinkShadow will automatically try the next available node till it either succeeds or runs out of nodes to connect to. At that point it will display an error message at the bottom right of the screen.

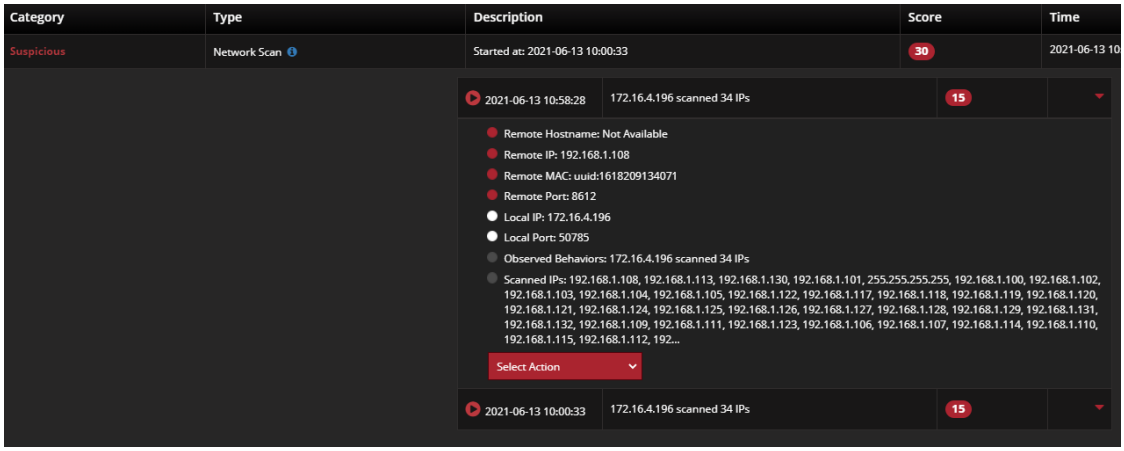
To Check the Response through Cisco ISE:

1- Go to ThreatShadow:

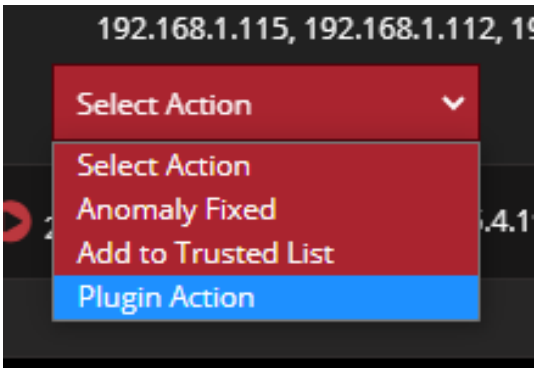
2- Select an Anomaly, eg: Network Scanning, and click on the device name to bring up the Entity Inspector page:

Host	Last Seen	Score
SWILSON	2021/06/13 11:07:01	30
172.16.5.26	2021/06/13 11:05:51	30
Re-XI	2021/06/13 11:05:22	30
172.16.4.203	2021/06/13 11:03:26	30
BBANNER	2021/06/13 11:02:15	30
CDANVERS	2021/06/13 11:02:03	30
172.16.5.37	2021/06/13 11:01:01	30
172.16.4.106	2021/06/13 10:58:36	30
android-1155acb3885c9a4d	2021/06/13 10:58:28	30
172.16.4.71	2021/06/13 10:58:20	30
172.16.4.160	2021/06/13 10:54:23	30

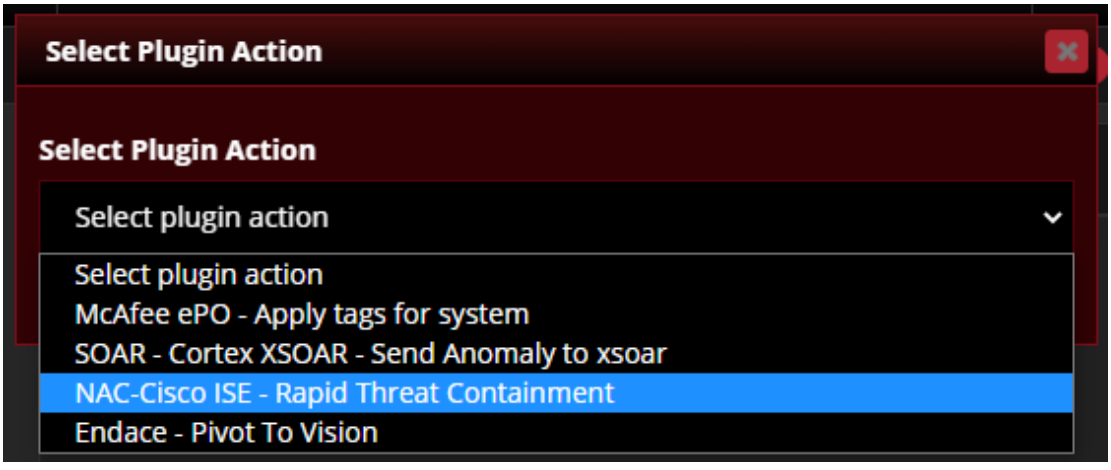
3- Scroll to the bottom to get to the anomalies section and expand the anomaly in question:



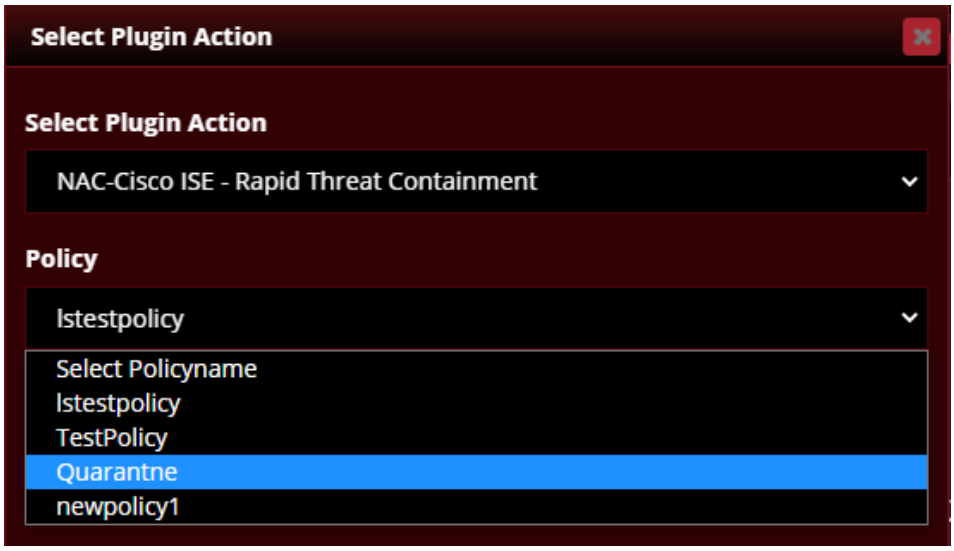
4- Click on the Select Action dropdown, and click on 'Plugin Action'



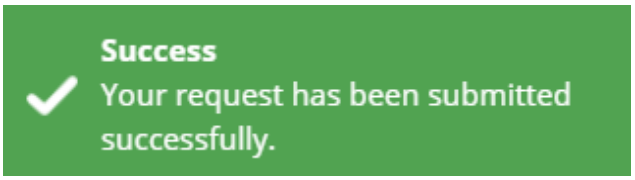
5- Click on the 'Select Plugin Action' dropdown and click on NAC-Cisco ISE – Rapid Threat Containment



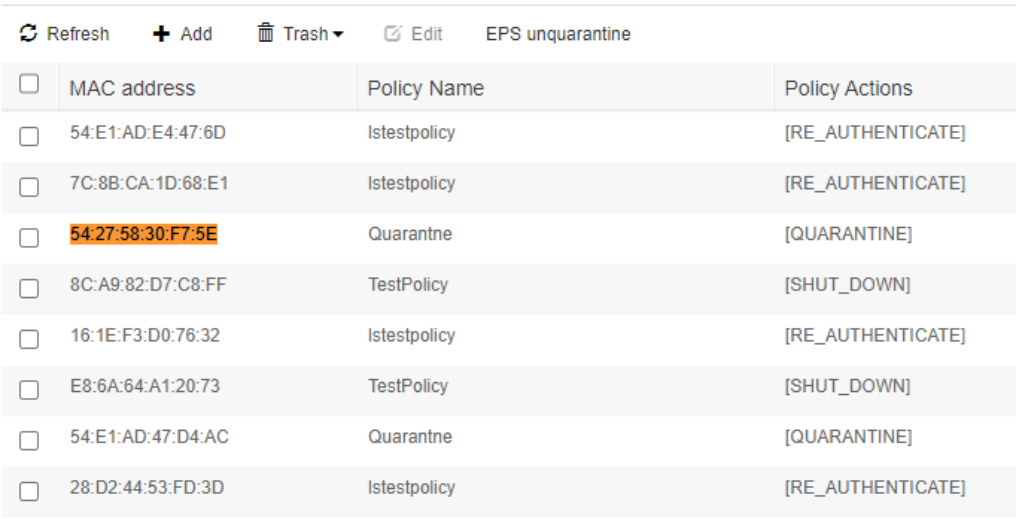
6- **You will be presented with a list of all policies available on ISE.** Choose one of these policies and click 'Submit' to apply the ISE policy to the device. In the screenshot below we selected the 'Quarantne' policy.



7- **If successfully applied, you will be shown the following message in LinkShadow**



8- **To verify that the policy has been applied, go back to ISE**. You should see the device added to the 'Quarantne' Policy in the ISE web console as shown below.



MAC address	Policy Name	Policy Actions
54:E1:AD:E4:47:6D	lstestpolicy	[RE_AUTHENTICATE]
7C:8B:CA:1D:68:E1	lstestpolicy	[RE_AUTHENTICATE]
54:27:58:30:F7:5E	Quarantne	[QUARANTINE]
8C:A9:82:D7:C8:FF	TestPolicy	[SHUT_DOWN]
16:1E:F3:D0:76:32	lstestpolicy	[RE_AUTHENTICATE]
E8:6A:64:A1:20:73	TestPolicy	[SHUT_DOWN]
54:E1:AD:47:D4:AC	Quarantne	[QUARANTINE]
28:D2:44:53:FD:3D	lstestpolicy	[RE_AUTHENTICATE]

LINKSHADOW
Combat the Dark

THANK YOU

linkshadow.com

Suite 444,320 East Clayton Street, Athens, Georgia 30601, USA | T: +1 877 267 7313