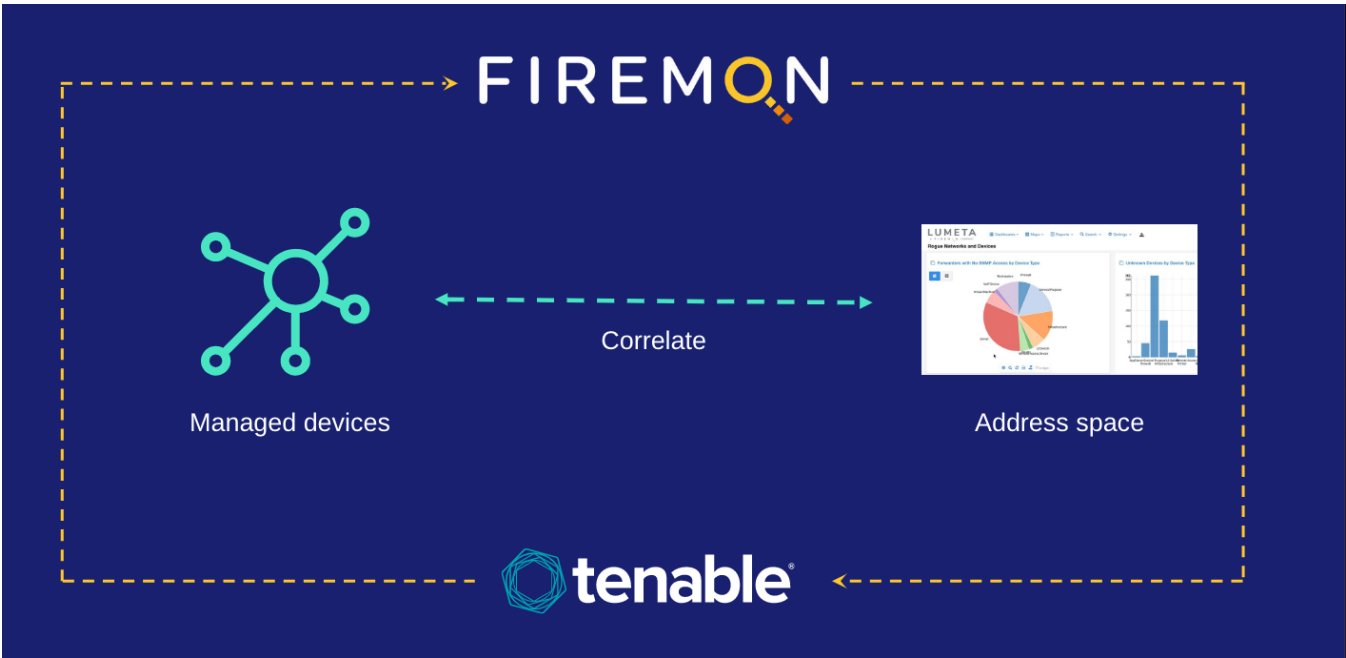


Tenable

The Tenable.sc and Tenable.io integrations tell you which hosts on your enterprise network are either undefended by Tenable or unknown to Asset Manager. By comparing Asset Manager's comprehensive index of all your network devices against that subset of network devices managed by Tenable, you can generate a list of network hosts that are *not* managed in by Tenable and then push that information to an asset group on Tenable. What's pulled from Tenable to Asset Manager is only what you request, and not an exhaustive collection of all the device details and attributes that Tenable manages. This enables Asset Manager to scan the network device attributes of value to you, and not all the rest.



How Does It Work?

1. Asset Manager queries Tenable and retrieves its inventory of devices under management. This data feed is stored on Asset Manager's database in their respective tables.
2. Asset Manager correlates this inventory against its own authoritative index of IP address space.
3. Asset Manager data is also pushed to Tenable and stored in an asset group.
4. Asset Manager highlights the commonalities and differences into views:
 - a. **Asset Manager-only IPs:** IP addresses Asset Manager knows about, but are unmanaged by Tenable
 - b. **Tenable-only IPs:** IP addresses Tenable knows about, but are unknown to Asset Manager (e.g., if Asset Manager does not have access to a network or an off-network device, but Tenable is still aware of the client agent)
 - c. **Tenable- & Asset Manager-Managed IPs:** IP addresses both Asset Manager and Tenable know about.

In reviewing the data on the Asset Manager dashboard, users can view Device Details. If the user selects Endpoint Context/Action, it will redirect to the Tenable UI where the user can take action to restart, remove, sync, or isolate an endpoint.


This information is available in Asset Manager via the [Tenable.sc Management Dashboard](#) dashboard and [Tenable.io Dashboard](#).

Configuring the Tenable Feed

Configure the Tenable feed as follows:

1. On Asset Manager's main menu, browse to **Settings > Integrations > Tenable.sc** or **Tenable.io**.
2. Enable the threat feed by toggling the slider to On.
3. Input a Polling Interval to indicate the time that should elapse between fetching the latest feed data.
4. Input the IP address of your Tenable server.
5. Input your customer Username.

Tenable.sc	Tenable.io
------------	------------



☐ Off

Polling Interval (by Hour)

Server Name

Username


Password

Purge Data

Submit

✔ Configuration Saved.

You may need to update your firewall to allow 65.246.246.60



☐ Off

Polling Interval (by Hour)

Server Name

Access Key

Secret Key

Purge Data


You may need to update you

6. Click **Submit**.
The feed of data from Tenable SecurityCenter to Asset Manager is configured. If you see the messages "Configuration saved" and "Product configured properly," then all is well.


In the Tenable SecurityCenter

To confirm that Asset Manager-discovered data has been pushed to Tenable SecurityCenter . . .

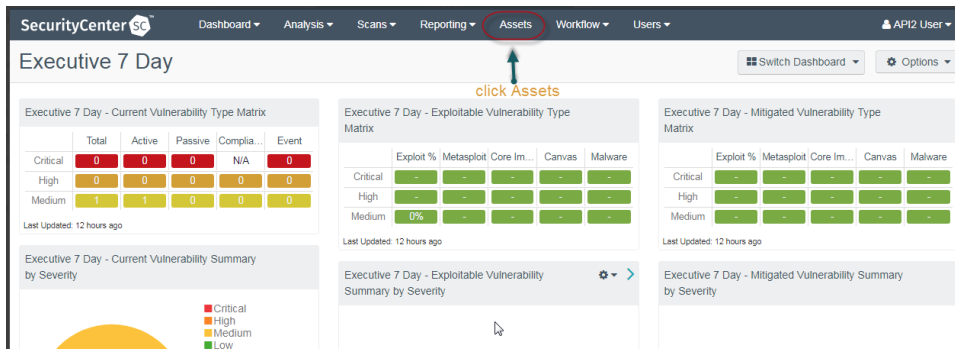
1. Log in to the Tenable server using the same credentials you used to configure the integration in Asset Manager.



Sign In



- On the SecurityCenter main menu, click **Assets**.



- This is the Asset Manager Asset List within Tenable SecurityCenter.

The screenshot shows the Asset Manager Asset List within Tenable SecurityCenter. The 'Assets' tab is highlighted. The table lists various asset groups and their details. The 'Spectre Asset List' is highlighted with a red circle and an arrow pointing to it with the text 'Click Asset group to see all spectre IP's'.

Asset Group	Owner	Access	Dynamic	Count	Last Updated	Actions
Scanned Hosts Not in DNS	Ed Young [eyoung]	Full Access	Dynamic	0	Nov 30, 2017 01:27	ⓘ ⚙
Sniffed Hosts Not in DNS	API2 User [apiuser2]	Full Access	Dynamic	0	1 week ago	ⓘ ⚙
Sniffed Hosts Not in DNS	Ed Young [eyoung]	Full Access	Dynamic	0	Nov 30, 2017 01:27	ⓘ ⚙
Solaris Hosts	API2 User [apiuser2]	Full Access	Dynamic	0	1 week ago	ⓘ ⚙
Solaris Hosts	Ed Young [eyoung]	Full Access	Dynamic	0	Nov 30, 2017 01:27	ⓘ ⚙
Spectre Asset List	API2 User [apiuser2]	Full Access	Static IP List	5	Just now	ⓘ ⚙
SSL or TLS Servers	Ed Young [eyoung]	Full Access	Dynamic	12	Nov 30, 2017 01:27	ⓘ ⚙
SSL or TLS Servers	API2 User [apiuser2]	Full Access	Dynamic	12	1 week ago	ⓘ ⚙
static test list	API2 User [apiuser2]	Full Access	Static IP List	0	1 week ago	ⓘ ⚙
static test list[1]	API2 User [apiuser2]	Full Access	Static IP List	0	6 days ago	ⓘ ⚙

- To manually edit the static list of IPs that came from Asset Manager, click the Asset Manager Asset List group.

The screenshot shows the Tenable SecurityCenter Asset Manager Asset List edit form. The 'Name' field is 'Spectre Asset List'. The 'Description' field is 'Assets known to Spectre but not known to Tenable'. The 'Tag' field is empty. The 'IP Addresses' field contains a list of IP addresses. The 'Submit' button is highlighted.

General

Name* Spectre Asset List

Description Assets known to Spectre but not known to Tenable

Tag

IP Addresses* 4.16.120.237,4.68.110.78,4.68.111.134,4.69.132.122,4.69.137.173,4.69.143.125,4.69.143.129,4.69.143.198,4.69.146.132,4.69.148.37,4.69.148.138,4.69.148.153,4.69.158.162,4.69.158.174,4.69.159.34,4.69.163.66,4.69.201.113,4.69.201.142,4.69.201.189,4.69.217.197,5.32.128.1-5.32.128.5,5.32.128.9-5.32.128.10,5.32.128.13-5.32.128.14,5.32.128.17-5.32.128.18,5.32.128.21-5.32.128.22,5.32.128.25-5.32.128.26,5.32.128.33-5.32.128.34,5.32.128.37-5.32.128.53-5.32.128.54,5.32.128.57-5.32.128.58,5.32.128.61-5.32.128.62,5.32.128.65-5.32.128.66,5.32.128.69-5.32.128.70,5.32.128.73-5.32.128.74,5.32.128.77-5.32.128.78,5.32.1

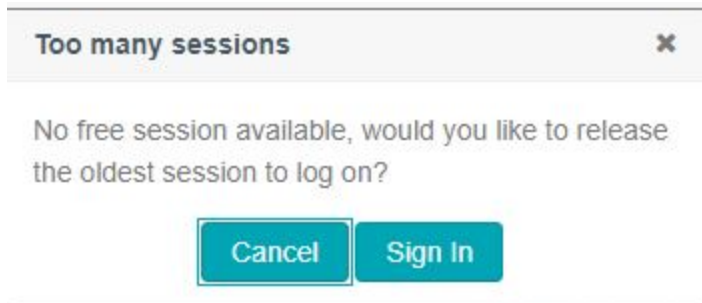
Choose File

Clear IPs

Submit Cancel

Disabling Session Management in Tenable SecurityCenter

If you see the following error when logging into Tenable, disable Session Management. Disabling Session Management Setting on your Tenable SecurityCenter is recommended.



To disable session management:

1. Log in to the Tenable SecurityCenter as a user who has system settings access.
2. Navigate to **Systems, Configuration**, and then to **Security**. The Authentication Settings will be listed.
3. Scroll down to **Allow Session Management**.
4. Clear the **Allow Session Management** option, and click **Submit**.