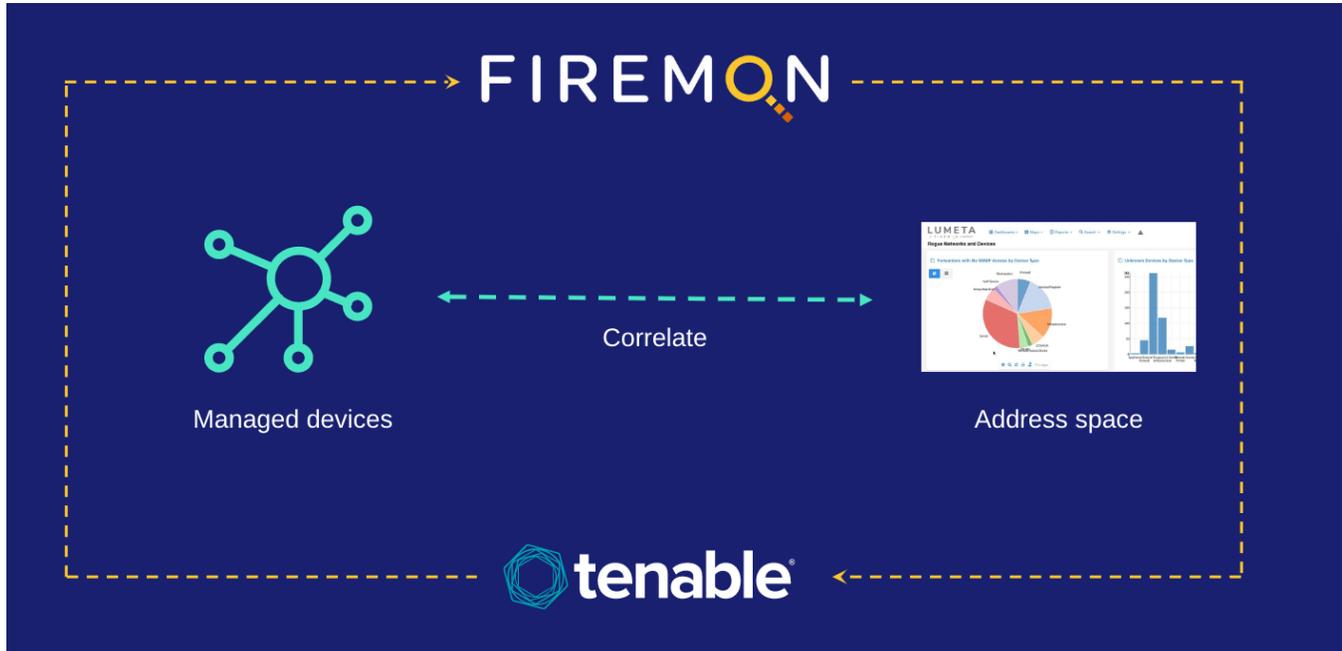


Tenable

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

✔ 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

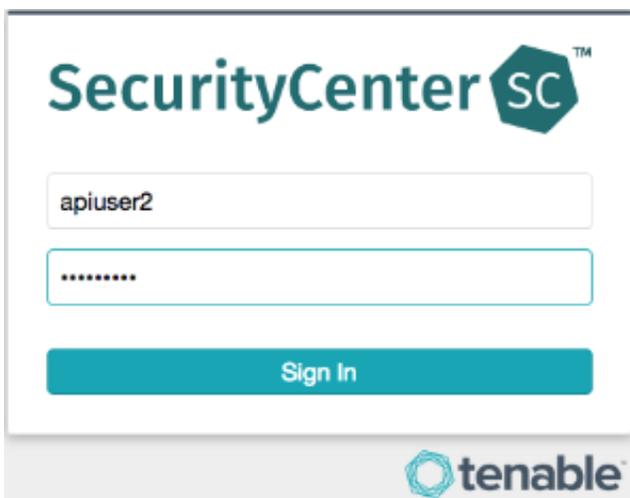
You may need to update you

- 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 . . .

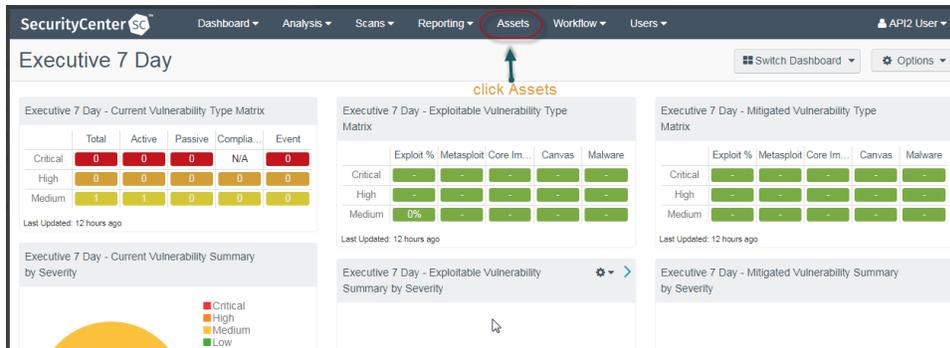
- Log in to the Tenable server using the same credentials you used to configure the integration in Asset Manager.



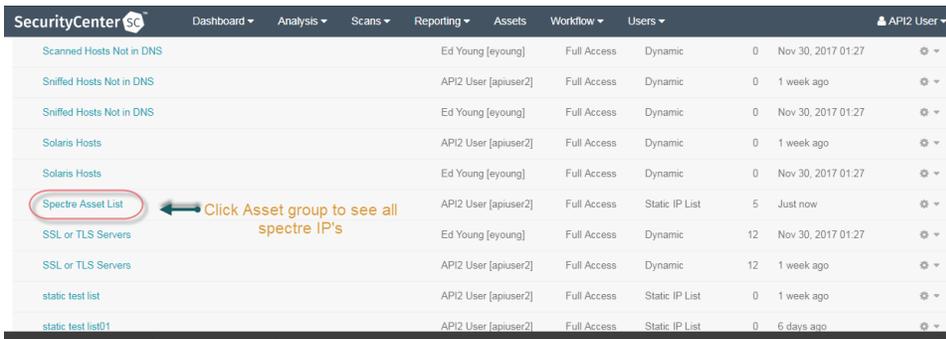
SecurityCenter SC™



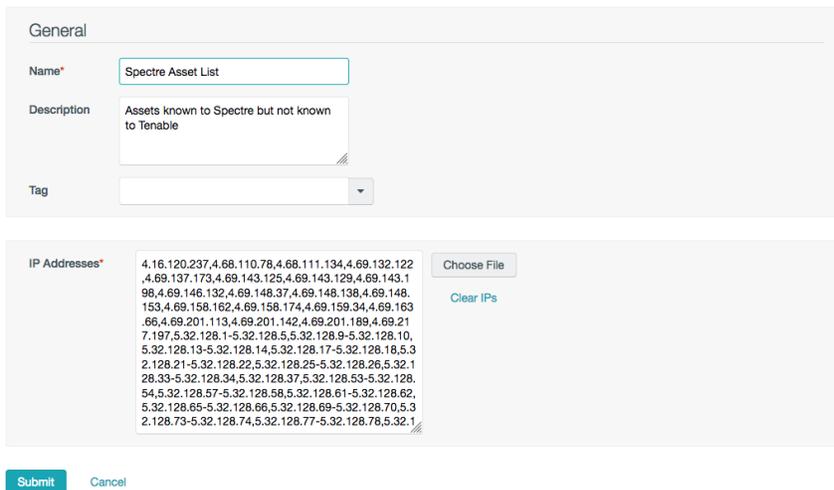
2. On the SecurityCenter main menu, click **Assets**.



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

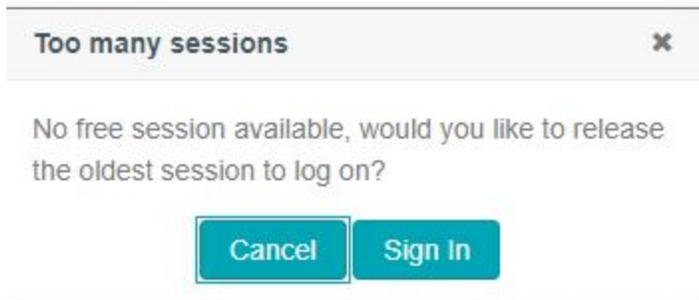


4. To manually edit the static list of IPs that came from Asset Manager, click the Asset Manager Asset List group.



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**.