FireMon Management Dashboard

Now you can share information between Asset Manager and Security Manager (SM) via API and create a group within Security Manager of Asset Manager-discovered devices it does not manage (i.e., non-managed devices in SM). Security Manager refers to devices imported from Asset Manager as "synthetic routers," and includes the data as part of the device's definition.

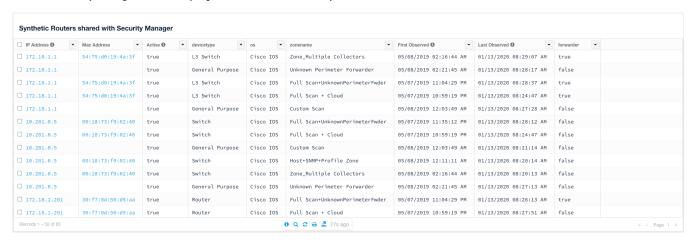
- Information on devices that profile as a unique router, switch or firewall in Asset Manager are fed to Security Manager, provided SM does not
 already know about the devices.
- Data points like device vendor, operating system, and model are conveyed, along with the description "Discovered by Asset Manager."
- Interface and routing information that Asset Manager discovers along with the device is also transmitted to Security Manager.

To amplify management capabilities, first configure the SIP Integration, and then review the FireMon Management dashboard, located on Asset Manager's Dashboards > Integrations menu.

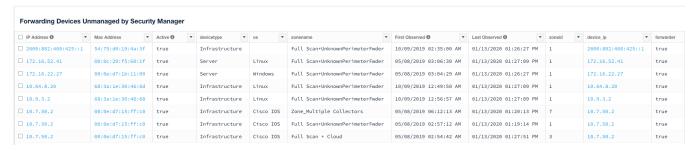
The Risk Analyzer and Security Manager dashboards are introduced here:

Security Manager

The Synthetic Routers shared with Security Manager table identifies routers, Layer 3 switches and firewalls discovered in real-time by Asset Manager and pushed to Security Manager as "synthetic routers." Only devices that are new or "unknown" to Security Manager are transmitted there automatically. In the context of Security Manager, these newly ingested devices are called "synthetic routers."



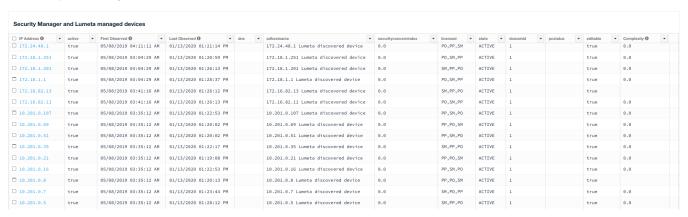
Forwarding Devices Unmanaged by Security Manager are forwarding devices Asset Manager found that do not profile as routers, switches, or firewalls. Asset Manager does not *automatically* push these findings to Security Manager. If the customer wants these findings in Security Manager, they must be added manually.



The Devices Unmanaged by Asset Manager are those devices that Asset Manager pulls from Security Manager. Ideally, this table will be empty, indicating that all devices managed by Security Manager have also been indexed by Asset Manager. The presence of records in this widget indicates a lack of visibility: Maybe a firewall is blocking discovery, maybe there's a misconfiguration, a necessary protocol is missing, or there's a poorly placed Scout component.

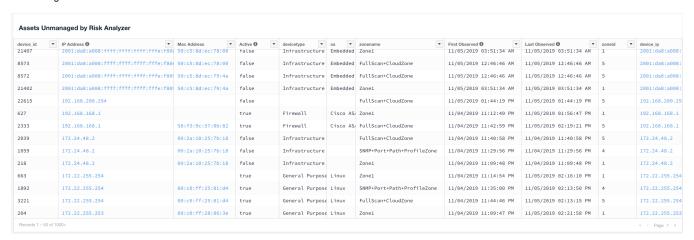


The final widget—Security Manager and Asset Manager-Managed Devices—is the full result of the Asset Manager-Security Manager integration. Devices on a network that both Security Manager and Asset Manager know about presented here, indicating that there are "no blind spots" and the customer has "full, visibility and coverage."



Risk Analyzer

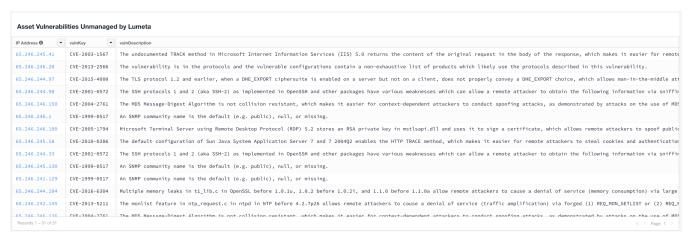
The top set of dashboard widgets shows assets Asset Manager knows about, but Risk Analyzer does not. This means that SIP is not defending the assets listed in the Assets Unmanaged by Risk Analyzer widget. Consider exporting these from Asset Manager, and importing them to Risk Analyzer to complete its coverage.



Asset Manager cannot "see" the assets listed on the Assets Unmanaged by Asset Manager widget. This indicates that your Scouts cannot "see" into the network on which they are located. Check your Scout deployment. Perhaps the device is off-network. This set presents devices Risk Analyzer knows about, yet Asset Manager does not.



This set presents asset vulnerabilities Risk Analyzer knows about, yet Asset Manager does not.



These panels will show any assets managed by both Asset Manager and Risk Analyzer.



SIP Device Details

The risk score, asset values and other device details associated with SIP-managed devices.

10.7.50.3 🖍 x										
Device Info	Devices	Assets	CVEs							
Device Profile	IP		As	set Risk Score	Asset Value	Dos Count	Interfaces		Licensed	Name
Attributes	10.7.50.3		0.0		10	0			true	gbudd5.corp.lumeta.com
Interfaces										
Connected Hosts - Layer 3										
Leak Response										
Notifications										
Alternate IPs										
Cisco pxGrid										
FireMon										
Cloud										