

Trellix ePO Management Dashboard

This Trellix-ePO integration combines the reach of Asset Manager's network discovery with Trellix's ePolicy Orchestrator (Trellix ePO) to improve your organization's security posture.

The Trellix ePO integration provides Trellix ePO customers with a way to ensure that the ePO agent is installed comprehensively on all network devices in a particular segment (or multiple segments) as intended. The integration reconciles Trellix findings with Asset Manager findings and insodoing, uncovers:

1. Assets lacking the Trellix ePO agent
2. Assets to which visibility is blocked
3. Assets with comprehensive management

To manage e-policy in Asset Manager, first [configure the Trellix feed](#), then review the ePO Management dashboard, located on Asset Manager's main Dashboards menu.

To manage e-policy in Trellix ePO server, [configure the Trellix feed](#), then install the Asset Manager extension to your ePO server.

The dashboard provides a variety of useful information:

IPs Unmanaged by Trellix - IPs Asset Manager found on your network that Trellix doesn't know about and doesn't have under management. Together, these unknowns represent a policy-management gap and vulnerability that could be exploited. This information is presented visually, in a bar chart that shows the volume of unmanaged, and also in a table with details on each unmanaged IP address (i.e., IP and MAC address, responsiveness and when the first and last response was received, and the Zone in which the device is located).

IPs Unmanaged by Asset Manager - These are those IPs managed by Trellix that Asset Manager did not find on the network. Typically there will not be any devices managed by Trellix that have not been indexed by Asset Manager. In the event these widgets show results, check your your Asset Manager discovery configuration, which is not providing the level of visibility you require. Contact us for help in identifying the prospective source of the problem.

Trellix- and Asset Manager-Managed IPs - When this subset becomes the whole (i.e., when all devices are managed by both resources, your organization's e-policy is well in hand.

Following is the ePO Management dashboard and a description of the data fields returned. All analytics from the Trellix feed go here. None affect Map filters, Reports or Search.

- **IP Address** - Device identifier
- **MAC Address** - Device identifier
- **Active** - device responded to Asset Manager probe
- **First Observed** - Device came on the network
- **Last Observed** - Device left the network after this point
- **Zone** - Number corresponding to the zone to which the device belongs

IPs Unmanaged by ePO

IP Address	Mac Address	Active	devicetype	os	zonename	First Observed	Last Observed
<input type="checkbox"/> fe80::32f7:dff:fe50:d5aa		true	Infrastructure	(Cisco)	Lumeta-333	05/21/2019 04:02:55 PM	05/18/2020 08:00:31 PM
<input type="checkbox"/> fe80::200:caff:fe11:2233		true			Lumeta-333	03/08/2020 02:54:53 PM	05/18/2020 08:00:31 PM
<input type="checkbox"/> 2601:44:1:b9c0:e9b3:feca:a161:75dc		true			Lumeta-333	03/08/2020 04:09:14 PM	05/18/2020 08:00:31 PM
<input type="checkbox"/> 2600:802:460:652::2		true			Lumeta-333	09/03/2019 11:33:07 AM	05/18/2020 08:00:31 PM
<input type="checkbox"/> 2600:802:460:652::1		true			Lumeta-333	10/14/2019 12:51:08 PM	05/18/2020 08:00:31 PM
<input type="checkbox"/> 2600:802:460:632:d03c:f4c5:a72c:7152		true			Lumeta-333	02/12/2020 06:52:58 PM	05/18/2020 08:00:31 PM
<input type="checkbox"/> 2600:802:460:624::1		true			Lumeta-333	11/19/2019 06:13:40 AM	05/18/2020 08:00:31 PM
<input type="checkbox"/> 2600:802:460:622::1		true			Lumeta-333	04/07/2020 11:21:29 PM	05/18/2020 08:00:31 PM
<input type="checkbox"/> 2600:802:460:425:250:56ff:feb9:cdce		true			Lumeta-333	02/04/2020 09:42:19 PM	05/18/2020 08:00:31 PM
<input type="checkbox"/> 2600:802:460:425:250:56ff:feb5:88a8		true			Lumeta-333	11/22/2019 03:13:56 PM	05/18/2020 08:00:31 PM

ePO and Lumeta Managed IPs

IP Address	active	First Observed	Last Observed	dns
<input type="checkbox"/> 172.16.52.5	true	05/21/2019 04:04:56 PM	05/18/2020 08:00:31 PM	
<input type="checkbox"/> 172.16.52.2	true	05/21/2019 04:04:56 PM	05/18/2020 08:00:31 PM	
<input type="checkbox"/> 172.16.42.19	true	05/21/2019 04:04:56 PM	05/18/2020 08:00:31 PM	LUMETA
<input type="checkbox"/> 172.16.42.16	true	05/21/2019 04:04:56 PM	05/18/2020 08:00:31 PM	lumeta
<input type="checkbox"/> 172.16.22.5	true	05/21/2019 04:04:56 PM	05/18/2020 08:00:31 PM	

IPs Unmanaged by Lumeta

IP Address	DNS Name
<input type="checkbox"/> 172.16.22.44	(none)
<input type="checkbox"/> 65.246.245.52	(none)
<input type="checkbox"/> 65.246.245.23	corp.lumeta.com
<input type="checkbox"/> 65.246.245.122	
<input type="checkbox"/> 172.16.52.10	
<input type="checkbox"/> 10.9.4.3	WORKGROUP
<input type="checkbox"/> 65.246.245.102	

The data in any dashboard widget can be exported by clicking the Export icon (i.e., the away-pointing arrow). After identifying Asset Manager-discovered IPs that you'd like to bring into Trellix, you can either export the data from the source widget and then import it to Trellix. Or, you can install the Asset Manager extension on your Trellix ePO server.

Submit a comment at the bottom of this page if you have a question or need additional information about the ePO Management dashboard.