

Cisco pxGrid

The Cisco pxGrid integration for Lumeta 3.3 and later, enables you to exchange context with Cisco products to retrieve endpoint, identity group, security group, and session data from a Cisco ISE server. The session data (only) is correlated by IP across Cisco and Lumeta, providing additional session data on the Lumeta side. Endpoint, identity group, and security group data is the same from both Cisco and Lumeta, only the GUI is different.

Prerequisites

To make use of this integration, your network must be running the Cisco pxGrid agent and be monitored by Lumeta. You'll also need the following:

1. Login credentials to your organization's Cisco ISE server
2. Filename and password of the keystore certificate to Cisco ISE server
3. Filename and password truststore certificate to Cisco ISE server

Ask your Cisco pxGrid server admin for this information if you do not have it already.

Configuring the Cisco pxGrid Integration

To enable the Cisco pxGrid integration from Lumeta's GUI:

1. Browse to **Settings > Integrations**.
2. Click **Other Solutions > Cisco**.
3. Establish that Lumeta is certified to receive Cisco pxGrid notifications by completing the form and clicking **Submit**:
 - a. **Server Name** - IP of Cisco pxGrid server
 - b. **Username** - User account associated with the Cisco pxGrid server
 - c. **Password** - User's password to the server
 - d. **Version** - Version of Cisco pxGrid which is populated by default
 - e. **Keystore File** - Cisco server cert
 - f. **Keystore Password** - Cisco server password
 - g. **Truststore File** - Cisco server cert
 - h. **Truststore Password** - Cisco server password

Cisco Unified Communications

Off

Server Name
65.246.246.78

Username
admin

keyStore.jks
Type: other, Size: 3.5 kB

Keystore Password
.....

trustStore.jks
Type: other, Size: 4.1 kB

Truststore Password
.....

Submit

The message "configuration saved" will display.

Enable the Cisco pxGrid Integration

When you're ready to receive Cisco ISE data, power on the integration.

- Return to **Settings > Integrations > Other Solutions > Cisco**.



- Toggle the slider to "On."

Validate the Feed

Confirm that data from Cisco ISE is available.

- Browse to **Settings > Tables**.
- Search on **Cisco**.

Tables

▲ Name	Table type
cisco_ise_endpointprofile	Managed primary
cisco_ise_identity_group	Managed primary
cisco_ise_securitygroup	Managed primary
cisco_ise_session	Managed primary

The "session" data as well as other tables of data from Cisco display.

View Results

Cisco pxGrid data is available in tables, dashboard widgets, and device details as follows:

- Click **Settings > Tables > Search on Cisco > View** to open the table and view session fields.

```
SELECT * FROM "cisco_ise_session"
```

	adhostdnsdomain	adhostnetbiosname	aduserdnsdomain	adusernetbiosname	auditsessionId	callingstationid	endpointprofile
1	null	null	null	null	1001	11:11:11:11:11:11	Unknown
2	null	null	null	null	1001	11:11:11:11:11:11	Unknown

epsstatus	ip	nasip	port	posture	posturetimestamp	radiusavpairs	securitygroup
null	10.9.0.117	10.9.0.117		null		Acct-Session-Id=123	null
null	10.9.0.117	10.9.0.117		null		Acct-Session-Id=123	null

sessionlastupdate	sessionstate	username
Fri Oct 07 12:10:11 EDT 2016	DISCONNECTED	LumetaUser
Fri Oct 07 12:10:19 EDT 2016	STARTED	LumetaUser

•

- Click **Dashboards > Cisco pxGrid >** to populate Session, Identify Group, Security Group, and Endpoint table data.

The screenshot displays four data tables from the Cisco pxGrid dashboard:

- Cisco ISE Session:** A table with columns: authsessionid, callignationalid, endpointprofile, genericattributename, genericattributvalue. It lists 12 records of session data.
- Cisco ISE Identity Group:** A table with columns: group, user. It shows 4 records for groups like Employee and User Identity Groups.
- Cisco ISE Security Group:** A table with columns: changestype, desc, name, securitygroupid, sig. It lists 9 records of security group changes.
- Cisco ISE Endpoint:** A table with columns: changestype, deviceprofileid, ipname, name. It lists 7 records of endpoint additions and modifications.

pxGrid Device Details

Right-click any linked IP address and select **Click Device Details > Cisco Pxgrid IP** view session data for pxGrid IP. A subset of Cisco pxGrid data is also available in **Search > Device details** with the following column heads. More information and an example will be added here; pxGrid Device Details cannot be displayed in our test environment at this time.

1. IP address
2. Nasip
3. Port
4. Session state
5. Username
6. Last updated
7. RADIUS av pairs

Lumeta 3.3.3 and later	Before Lumeta 3.3.3														
	<p>Device Details</p> <p>10.9.0.117 IPsonar Mapping <input type="text" value="Search"/></p> <p>10.9.0.117</p> <p>Device Info Device Profile Attributes Interfaces Connected Hosts - Layer 3 Open TCP Ports Closed TCP Ports Leak Response Notifications Alternate IPs PxGrid IP Sessions</p> <table border="1"> <thead> <tr> <th>IP Address</th> <th>Nasip</th> <th>Port</th> <th>Session state</th> <th>User Name</th> <th>Last Updated</th> <th>Rad</th> </tr> </thead> <tbody> <tr> <td>10.9.0.117</td> <td>10.9.0.117</td> <td></td> <td>STARTED</td> <td>LumetaUser</td> <td>Thu Oct 06 16:06:10 EDT 2016</td> <td>Act</td> </tr> </tbody> </table>	IP Address	Nasip	Port	Session state	User Name	Last Updated	Rad	10.9.0.117	10.9.0.117		STARTED	LumetaUser	Thu Oct 06 16:06:10 EDT 2016	Act
IP Address	Nasip	Port	Session state	User Name	Last Updated	Rad									
10.9.0.117	10.9.0.117		STARTED	LumetaUser	Thu Oct 06 16:06:10 EDT 2016	Act									

Device Info
Device Profile
Attributes
Interfaces
Connected Hosts - Layer 3
Leak Response
Notifications
Alternate IPs
WMI Services
Cisco pxGrid
Firemon
Cloud