Monitoring

The **Monitoring** options available to you vary depending on your role.

Agent Monitoring

The page displays the count of all monitored agents in a cluster based on the currently selected root scope.

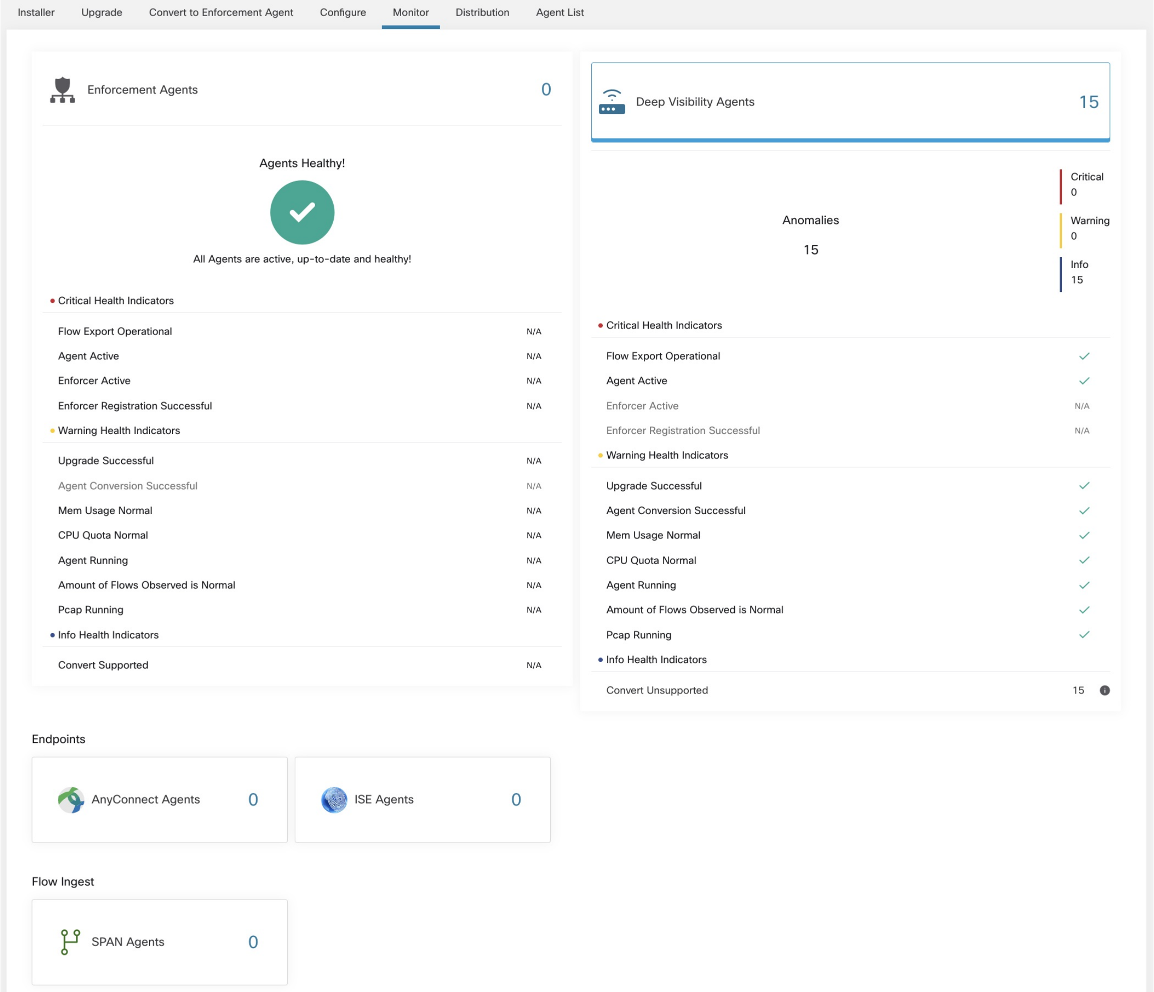
Note Total Inventory count is the summation of all inventory observed on the network after applying collection rules.

Agent Monitoring Type

To monitor agents, click **Manage** > **Agents** in the left navigation bar, then click the **Monitor** tab.

This page is only available for users that have **Site Admin** and **Customer Support** roles. **Scope owners** can see Inventory, Deep Visibility Agents, and Enforcement Agents.

Figure 1: Total Number of Installed Agents



Enforcement Agents 0

Agents Healthy!

All Agents are active, up-to-date and healthy!

● Critical Health Indicators	
Flow Export Operational	N/A
Agent Active	N/A
Enforcer Active	N/A
Enforcer Registration Successful	N/A
● Warning Health Indicators	
Upgrade Successful	N/A
Agent Conversion Successful	N/A
Mem Usage Normal	N/A
CPU Quota Normal	N/A
Agent Running	N/A
Amount of Flows Observed is Normal	N/A
Pcap Running	N/A
● Info Health Indicators	
Convert Supported	N/A

Deep Visibility Agents 15

Anomalies 15

Critical 0
Warning 0
Info 15

● Critical Health Indicators	
Flow Export Operational	✓
Agent Active	✓
Enforcer Active	N/A
Enforcer Registration Successful	N/A
● Warning Health Indicators	
Upgrade Successful	✓
Agent Conversion Successful	✓
Mem Usage Normal	✓
CPU Quota Normal	✓
Agent Running	✓
Amount of Flows Observed is Normal	✓
Pcap Running	✓
● Info Health Indicators	
Convert Unsupported	15

Endpoints

AnyConnect Agents 0

ISE Agents 0

Flow Ingest

SPAN Agents 0

The following table shows the differences between each agent type.

Agent Type	Description
Deep Visibility	Provides highest fidelity in terms of time series flow data, processes running on a host. Most Linux and Windows platforms are supported. See sw_agents_deployment-label
Enforcement	Provides all capabilities available in Deep Visibility Agents. In addition, Enforcement agents are capable of setting firewall rules on the installed host.

AnyConnect	Provides time series flow data on endpoints running AnyConnect Secure Mobility Agent with Network Visibility Module (NVM) without requiring any Cisco Secure Workload agent installation. IPFIX records generated by NVM are sent to Secure Workload AnyConnect Proxy connector. Windows, Mac, and certain smartphone platforms are supported.
ISE	Provides metadata about endpoints registered with Cisco ISE. Through ISE pxGrid, ISE connector collects the metadata, registers the ISE endpoints on Secure Workload as ISE agents pushes labels based on the attributes fetched from ISE appliance and LDAP attributes for the users logged in to the endpoints.
The following table provides a brief summary of various appliance agents provided by Cisco Secure Workload.	
Appliance Agents	Description
SPAN	Provides the flow analysis without requiring any per-host agent installation. It runs in the Secure Workload ERSPAN VM appliance. It consumes ERSPAN packets sourced by any Cisco switch.

Note Appliance agents such as NetFlow, NetScaler, F5, AWS, and AnyConnect Proxy are now supported as connectors. For more information on connectors, see What are Connectors.

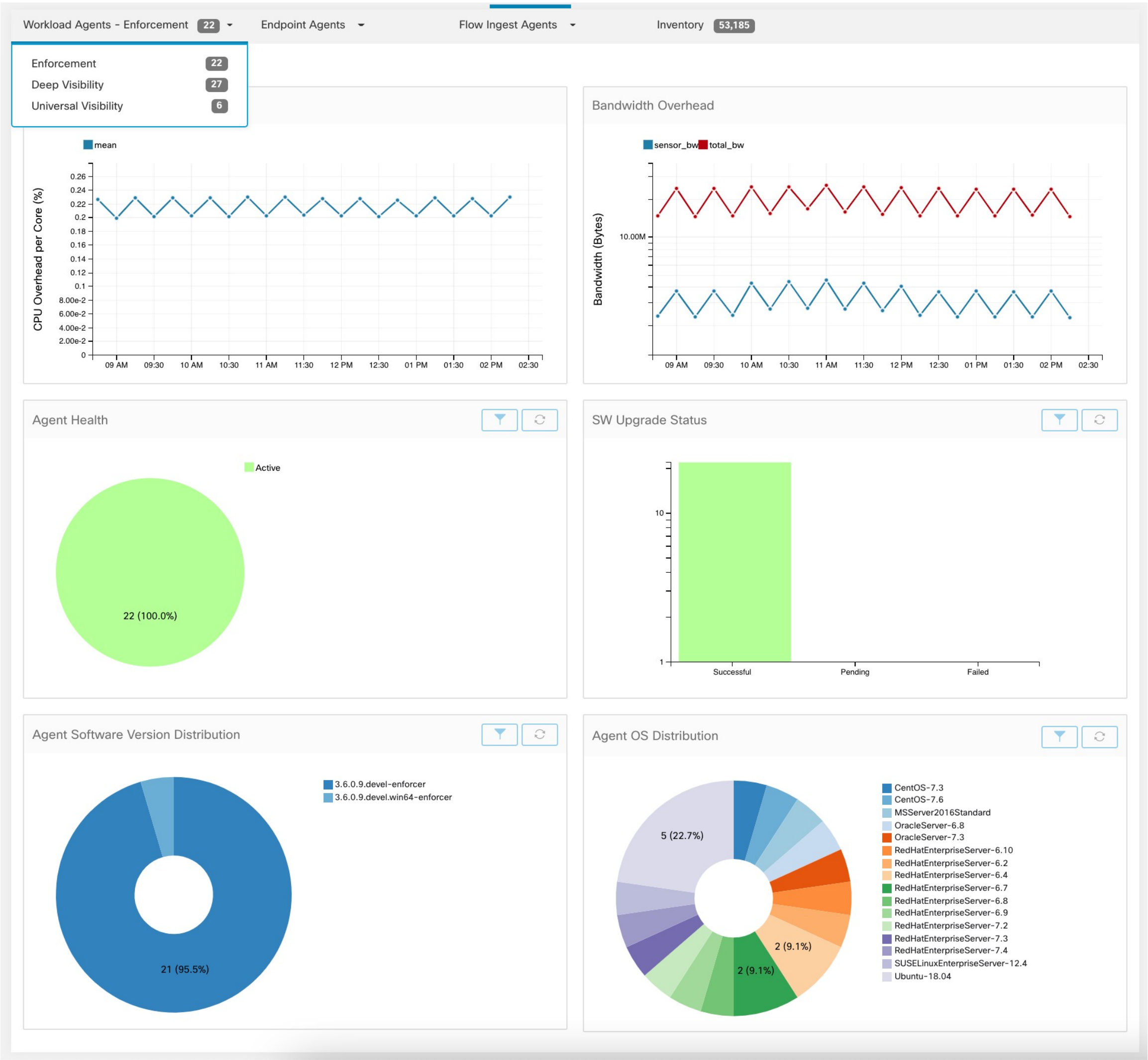
Any non-zero agent type button allows further drill-down into the distribution of each agent type.

Agent Status and Statistics

To view the charts described in this topic, choose **Manage** > **Agents**, then click the **Distribution** tab.

The following charts are available for both Deep Visibility and Enforcement Agent types.

Figure 2: Agents Distribution



For each agent type, this page provides an overview and the health of registered agents including overall CPU overhead, bandwidth overhead, missed packets, OS/version distribution and agent upgrade status.

CPU Overhead Chart

The CPU Overhead chart provides an aggregated view of CPU overhead per core from all agents. Per-agent CPU Overhead is provided as part of the Workload Profile. This chart is only available for Deep Visibility and Enforcement Agent Types.

Bandwidth Overhead Chart

The Bandwidth Overhead chart provides aggregated stats of total bandwidth and bandwidth used by agents. Per-agent bandwidth overhead is provided as part of the Workload Profile. This chart is only available for Deep Visibility and Enforcement Agent Types.

Agent Health Chart

The Agent Health chart provides the number of active/inactive agents. Active agents are the one schecking in with config server for upgrade on regular intervals. The checking interval is 30 minutes. If we see that an agent has missed more than two check-in periods from a agent, it would be declared as inactive agent.

Software Agent Updates to Latest Revision Chart

Every time an agent checks in with the config server, the agent would also provide its current RPM version. If an agent is configured to a specific version and is not able to update after 2 check-in periods, the agent would be declared as not able to upgrade to the latest version.

Agent Packet Missed Chart

In rare occasions when the traffic volume traversing a host is greater than the rate at which the agent is able to inspect, some packets are skipped from being analyzed. The number of missed packets and the corresponding agent name are displayed in this chart.

Agent Software Version/OS Distribution Charts

These charts show the agent version distribution and parent OS platform of all agents registered with the Secure Workload cluster.

Enforcement Status

To view enforcement status, click **Defend** > **Enforcement Status** in the navigation bar at the left side of the window.

This page is available for site admin/customer support users and scope owners to get an overview of the current status of all the enforcement agents, including the cloud connectors that are enforcing a policy.

If any of the charts shows red or orange, see the applicable topic:

Table 1: Enforcement Status Charts

Chart	Result	Take Action
Agent Enforcement Enabled	**Not Enabled**	Make sure enforcement is enabled in the agent configuration. See Create an Agent Configuration Profile.
Agent Policy Config	**Stale Policies**	This situation is generally temporary and typically doesn’t require any action. It occurs because a Secure Workload deployment based on labels updates inventory and policies dynamically. However, if this situation persists for any individual workloads, contact Cisco TAC.
Agent Concrete Policies	**Skipped**	This indicates that policies weren’t pushed to some agents.

Tip

- To view status for individual scopes or for the entire tenant, use the **Filter by Scope** option at the top-left side of the page.
- If the charts indicate a problem, identify which workloads have the problem by clicking the relevant part of a chart.

  The table displays the affected workloads.

  Alternatively, to see filtering options, click the (i) button in the **Filter** box below the charts.
- To view a wealth of additional details, click the IP address link in the filtered list of workloads to display the Workload Profile page.

The following table describes the fields shown in the enforcement status table.

Field	Description
Host Name	Host name of the workload.
Address	IP addresses of all the interfaces on the workload.
Enforcement Enabled	Indicates whether enforcement is enabled or not on the agent.
Concrete Policies in Sync	This indicates whether the desired version of concrete policies are currently enforced on the agent.
Concrete Policies	If this value shows **Skipped** for any host, this means the limit on policies is reached for the agent on that host. (See Limits Related to Policies.)
Policy Count	The number of concrete policies on the agent.
Status	The status of the latest policy config enforcement. If the status is **CONFIG_SUCCESS**, it indicates that current version is enforced without any issue.

Enforcement Status for Cloud Connectors

If you have set up AWS or Azure cloud connectors:

All interfaces enforcement status are displayed on the enforcement status page. If the policies are applied successfully, the policies are in sync else the corresponding error messages are displayed.

Policy count in the enforcement status page is Secure Workload accounting but not AWS or Azure rule accounting.

(AWS only) The hostname field on this page is derived from public DNS. If the public DNS is not enabled on the given VPC, the hostname field is empty.

Pausing Policy Updates

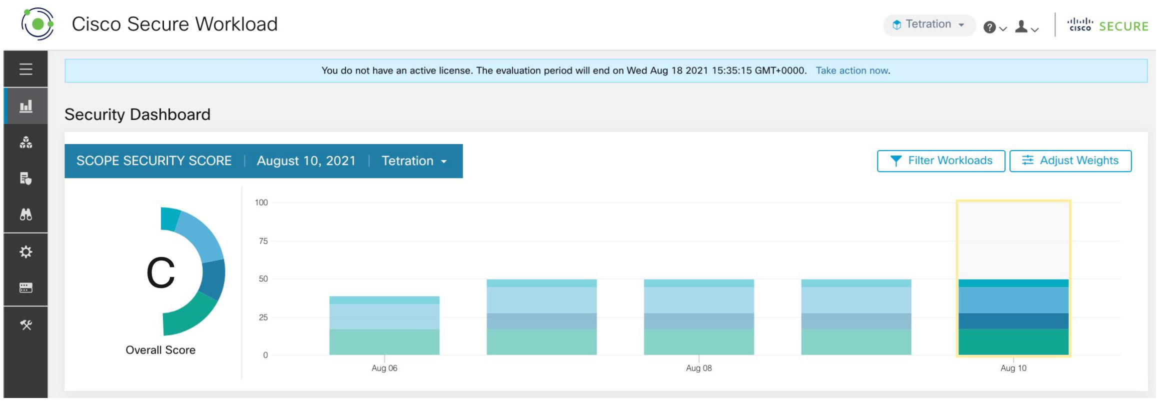
See Pause Policy Updates.

Licenses

To view the status of your Secure Workload licenses, click **Manage** > **Licenses** in the navigation bar at the left side of the window.

This page is available for the site admin to get an overview of the current licensing status and license usages. In this release and forward, it is required to register the cluster for on-premises deployment. When you upgrade to or deploy a new cluster with this release, software automatically enters a 90 days evaluation mode. A banner is displayed and shows the evaluation expiration date.

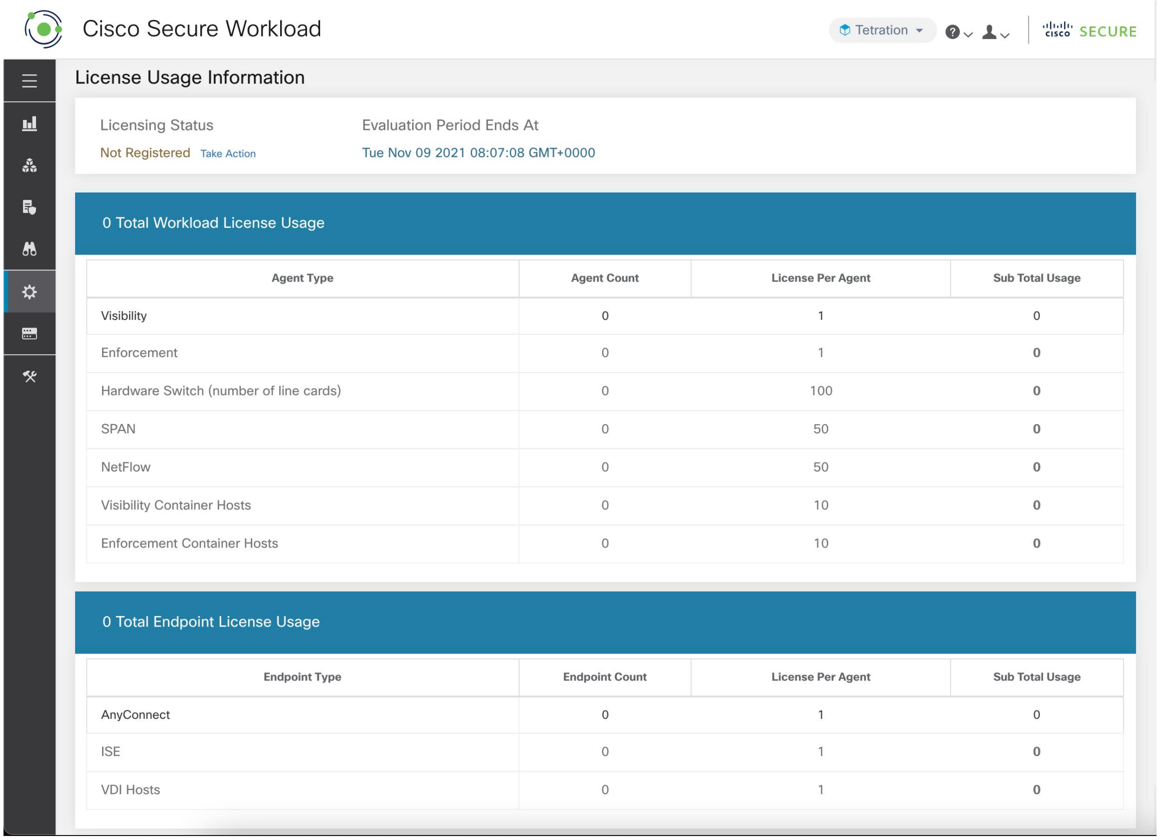
Figure 3: License banner



You do not have an active license. The evaluation period will end on Wed Aug 18 2021 15:35:15 GMT+0000. Take action now.

Note If the registration isn't completed successfully within the 90 days period, the banner message changes to out-of-compliance. No feature or functionality is blocked due to non-registration.

Figure 4: In monitoring - licenses page, detailed license information is displayed



License Usage Information

Licensing Status

Not Registered Take Action

Evaluation Period Ends At

Tue Nov 09 2021 08:07:08 GMT+0000

0 Total Workload License Usage

Agent Type	Agent Count	License Per Agent	Sub Total Usage
Visibility	0	1	0
Enforcement	0	1	0
Hardware Switch (number of line cards)	0	100	0
SPAN	0	50	0
NetFlow	0	50	0
Visibility Container Hosts	0	10	0
Enforcement Container Hosts	0	10	0

0 Total Endpoint License Usage

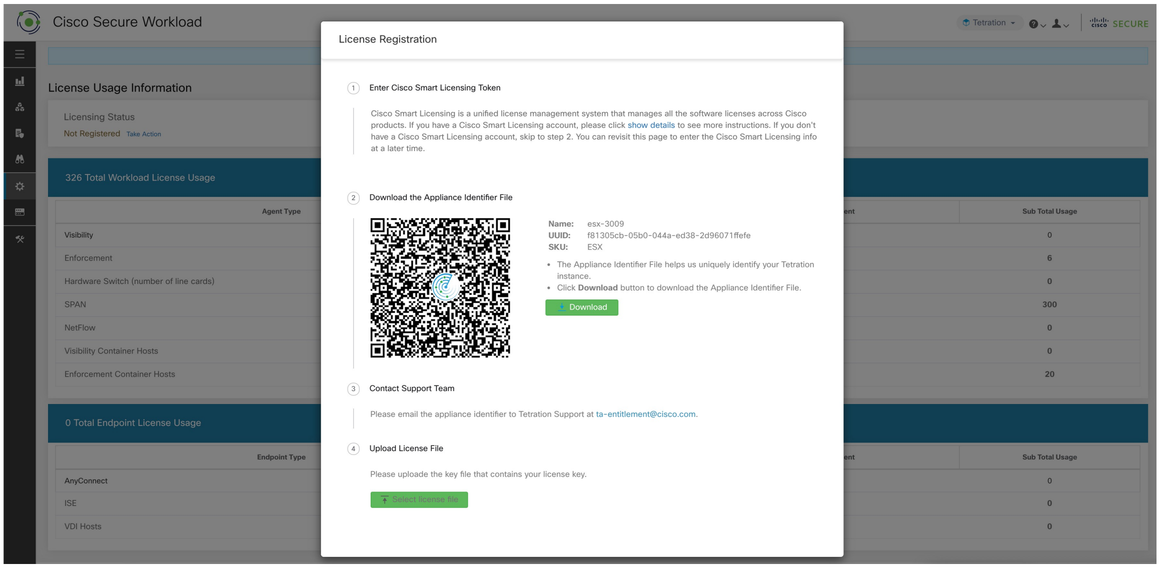
Endpoint Type	Endpoint Count	License Per Agent	Sub Total Usage
AnyConnect	0	1	0
ISE	0	1	0
VDI Hosts	0	1	0

License Registration

This section explains how to obtain a license.

Click **Take Action** in the license banner or in the **Manage** > **Licenses** page to request a license. You will see instructions on how to download a cluster identify file and how to acquire a license.

Figure 5: License registration modal - Download cluster identify file



License Usage Information

Licensing Status
Not Registered Take Action

326 Total Workload License Usage

Agent Type	…ent	Sub Total Usage
Visibility		0
Enforcement		6
Hardware Switch (number of line cards)		0
SPAN		300
NetFlow		0
Visibility Container Hosts		0
Enforcement Container Hosts		20

0 Total Endpoint License Usage

Endpoint Type	…ent	Sub Total Usage
AnyConnect		0
ISE		0
VDI Hosts		0

License Registration

1. Enter Cisco Smart Licensing Token

   Cisco Smart Licensing is a unified license management system that manages all the software licenses across Cisco products. If you have a Cisco Smart Licensing account, please click show details to see more instructions. If you don't have a Cisco Smart Licensing account, skip to step 2. You can revisit this page to enter the Cisco Smart Licensing info at a later time.

2. Download the Appliance Identifier File

   Name: esx-3009
   UUID: f81305cb-05b0-044a-ed38-2d96071ffefe
   SKU: ESX

   - The Appliance Identifier File helps us uniquely identify your Tetration instance.
   - Click **Download** button to download the Appliance Identifier File.

   Download

3. Contact Support Team

   Please email the appliance identifier to Tetration Support at ta-entitlement@cisco.com.

4. Upload License File

   Please uploade the key file that contains your license key.

   Select license file

Step 1 To complete **License Registration Modal**, it requires a registration token generated through CSSM Smart software licensing portal. The steps to generate the token through CSSM is provided in the license modal itself. Once you have the registration token, copy and paste the token into the text box in the licensing modal and click **Submit**.

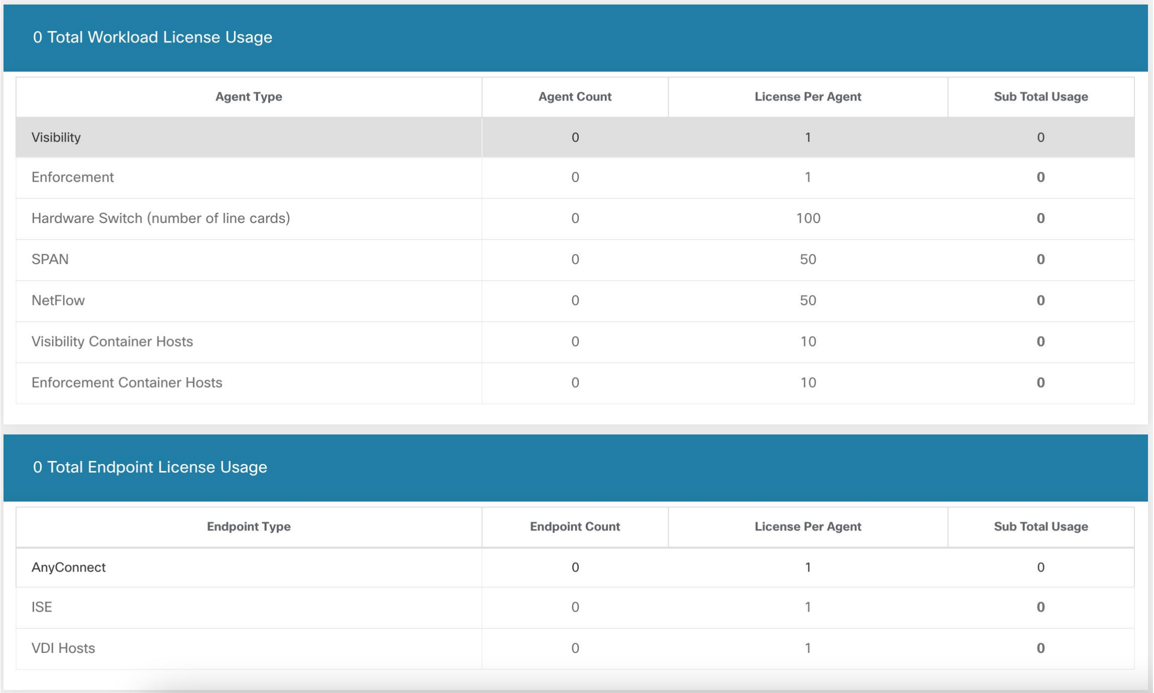
Step 2 Next, click **Download** to download the cluster identify file to local storage. File name format for the identify file is: **reg_id_<cluster_name>_<cluster_uuid>.gz**. The identity file doesn't contain any IP address information, specific workload details or PII information. This identity file needs to be sent to ta-entitlement@cisco.com. A response that contains the **license key file** is sent to the same email address from which the identity file was received.

Step 3 This **license key file** must be uploaded through the licensing modal. Step 4 of the licensing modal should be used to upload the response file.

Check License Usage

This section explains how to check the detailed license usage. In the left navigation menu, click **Manage** > **Licenses**.

Figure 6: License Table and Detailed Usage



0 Total Workload License Usage

Agent Type	Agent Count	License Per Agent	Sub Total Usage
Visibility	0	1	0
Enforcement	0	1	0
Hardware Switch (number of line cards)	0	100	0
SPAN	0	50	0
NetFlow	0	50	0
Visibility Container Hosts	0	10	0
Enforcement Container Hosts	0	10	0

0 Total Endpoint License Usage

Endpoint Type	Endpoint Count	License Per Agent	Sub Total Usage
AnyConnect	0	1	0
ISE	0	1	0
VDI Hosts	0	1	0

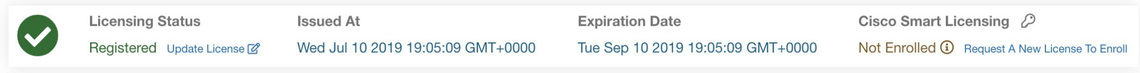
Note After the registration, if the license usage exceeds the entitlement (workload or endpoint), a noncompliant warning banner would be displayed in the UI. Exceeding the license usage doesn't block any feature or functionality including installing additional sensors. If the usage falls below the entitlement, then the compliance warning banner goes away. If additional licenses are purchased, you can reach out to ta-entitlement@cisco.com along with the identity information (download it again from the license modal) and request an updated license key file.

More on Cisco Smart Licensing

Cisco Smart Licensing is a unified license management system that manages all the software licenses across Cisco products. If you have a Cisco Smart Licensing account, you can associate the Cisco Smart Licensing Token with a Secure Workload license. If you don't have a Cisco Smart Licensing account, you can acquire/update a license without Cisco Smart Licensing.

Step 1 If you already have a valid Secure Workload license, click **Request A New License To Enroll** to acquire a new license with Cisco Smart Licensing Token.

Figure 7: Acquire a new license to associate Cisco Smart Licensing Token with a Secure Workload license



Licensing Status	Issued At	Expiration Date	Cisco Smart Licensing
Registered Update License	Wed Jul 10 2019 19:05:09 GMT+0000	Tue Sep 10 2019 19:05:09 GMT+0000	Not Enrolled ⓘ Request A New License To Enroll

Step 2 If you don’t have a valid Secure Workload license, click **Take Action** to acquire a new license as described in the previous sections.