Monitoring Cisco Cloud Services Platform 2100

Beta Version

Cisco: CSP-2100 PowerPack version 104

Table of Contents

Overview 3
- Introduction 3
- Prerequisites 3
- What Does the Cisco: CSP-2100 PowerPack Monitor? 4
- Installing the Cisco: CSP-2100 PowerPack 4

Discovering Cisco Cloud Services Platform Devices 6
- Overview 6
- Creating SNMP Credentials for CSP-2100 Clusters 6
- Creating a Basic/Snippet Credential for CSP-2100 Clusters 8
- Discovering CSP-2100 Clusters 9
- Viewing CSP-2100 Component Devices 11
- Relationships Between Component Devices 13

Cisco Cloud Services Platform Device Dashboards 14
- Overview 14
- Device Dashboards 14
  - Cisco: CSP 2100 Cluster 15
  - Cisco: CSP 2100 Node 16
  - Cisco: CSP 2100 Service 17

Chapter 1

Overview

Introduction

This manual describes how to use the *Cisco: CSP-2100* PowerPack to monitor Cisco Cloud Services Platform (CSP) 2100 clusters in the ScienceLogic platform.

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

Prerequisites

Before performing the tasks in this manual, you must have the following information about the CSP-2100 clusters that you want to monitor:

- Username and password of a user with REST API read access and a role of operator-group or admin-group
- SNMP community string with read privileges and the port set to 161

NOTE: For more information about these requirements, see http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/config_guide/b_Cisco_CSP_2100_Config_Guide.html.

Additionally, you must establish a Net-SNMP public community string with the port set to 1610. To do so:

1. Log in to the command line of the CSP-2100 device as an administrative user.
2. Run the following commands:

```
netsnmp agent port 1610
netsnmp community public
```

What Does the Cisco: CSP-2100 PowerPack Monitor?

To monitor CSP-2100 devices using the ScienceLogic platform, you must install the *Cisco: CSP-2100* PowerPack. This PowerPack enables you to discover, model, and collect data about CSP-2100 clusters, nodes, and services.

The *Cisco: CSP-2100* PowerPack includes:

- Three example credentials (two SNMP credentials and a Basic/Snippet credential) you can use to create the credentials that enable you to collect data from CSP-2100 devices
- Dynamic Applications to discover and monitor the CSP-2100 component devices
- Device Classes for each type of CSP-2100 component device the ScienceLogic platform monitors
- Event Policies and corresponding alerts that are triggered when CSP-2100 component devices meet certain status criteria
- Run Book Actions and Policies that align the correct device class to CSP-2100 component devices based on GUID and that merge CSP-2100 component devices with the appropriate physical components
- Device dashboards for each type of discovered CSP-2100 component device

Installing the Cisco: CSP-2100 PowerPack

Before completing the steps in this manual, you must import and install version 104 of the *Cisco: CSP-2100* PowerPack.

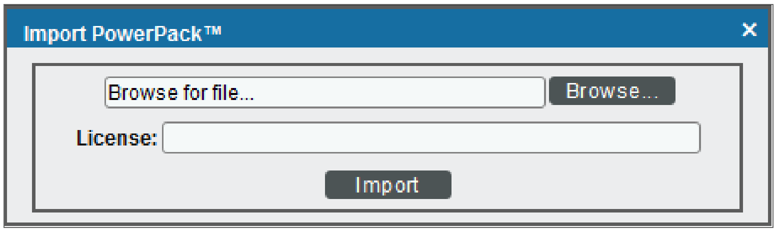
NOTE: To install version 104 of the *Cisco: CSP-2100* PowerPack, your ScienceLogic system must be upgraded to the 8.1.0 or later release.

To download and install a PowerPack:

TIP: By default, installing a new version of a PowerPack overwrites all content in that PowerPack that has already been installed on the target system. You can use the ***Enable Selective PowerPack Field Protection*** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. (For more information, see the ***System Administration*** manual.)

1. Download the PowerPack from the ScienceLogic Customer Portal.

2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*.
4. The **Import PowerPack** dialog box appears:



5. Click the **[Browse]** button and navigate to the PowerPack file.
6. When the **PowerPack Installer** modal page appears, click the **[Install]** button to install the PowerPack.

NOTE: If you exit the **PowerPack Installer** modal page without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPack Manager** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal page. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Chapter 2

Discovering Cisco Cloud Services Platform Devices

Overview

The following sections describe how to configure the ScienceLogic platform to discover and monitor Cisco Cloud Services Platform (CSP) 2100 clusters:

- *Creating SNMP Credentials for CSP-2100 Clusters*
- *Creating a Basic/Snippet Credential for CSP-2100 Clusters*
- *Discovering CSP-2100 Clusters*
- *Viewing CSP-2100 Component Devices*

Creating SNMP Credentials for CSP-2100 Clusters

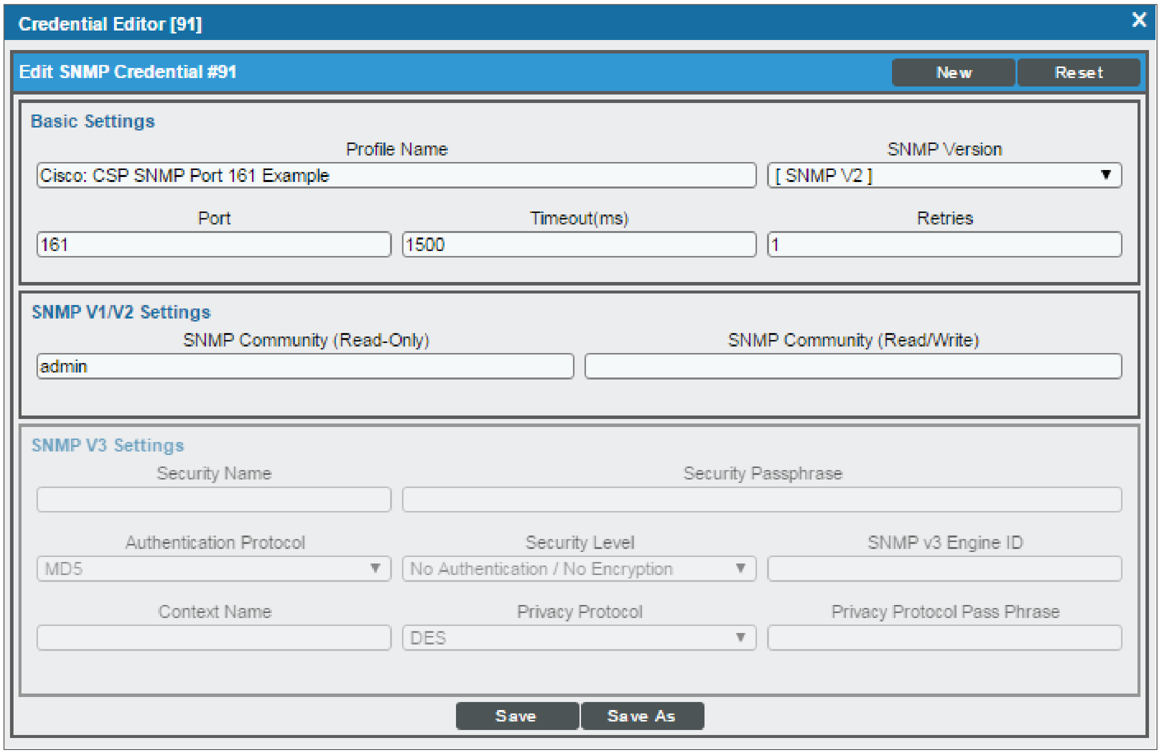
Before you can discover and monitor CSP-2100 clusters in the ScienceLogic platform, you must first create two SNMP credentials (one for port 161 and another for port 1610) in the platform. These credentials, along with a *Basic/Snippet credential that you must also create*, enable the platform to collect data from the clusters. Two example SNMP credentials that you can edit for your own use are included in the *Cisco: CSP-2100* PowerPack.

> NOTE: For more information about the configuration required for the two SNMP credentials, see the *Prerequisites* section.

To configure the port 161 SNMP credential for CSP-2100:

1. Go to the **Credential Management** page (System > Manage > Credentials).

2. Locate the **Cisco: CSP SNMP Port 161 Example** credential, then click its wrench icon (🔧). The **Edit SNMP Credential** modal page appears.
3. Make entries in the following fields:



Basic Settings

Profile Name: Cisco: CSP SNMP Port 161 Example

SNMP Version: [SNMP V2]

Port: 161

Timeout(ms): 1500

Retries: 1

SNMP V1/V2 Settings

SNMP Community (Read-Only): admin

SNMP Community (Read/Write):

SNMP V3 Settings

Security Name:

Security Passphrase:

Authentication Protocol: MD5

Security Level: No Authentication / No Encryption

SNMP v3 Engine ID:

Context Name:

Privacy Protocol: DES

Privacy Protocol Pass Phrase:

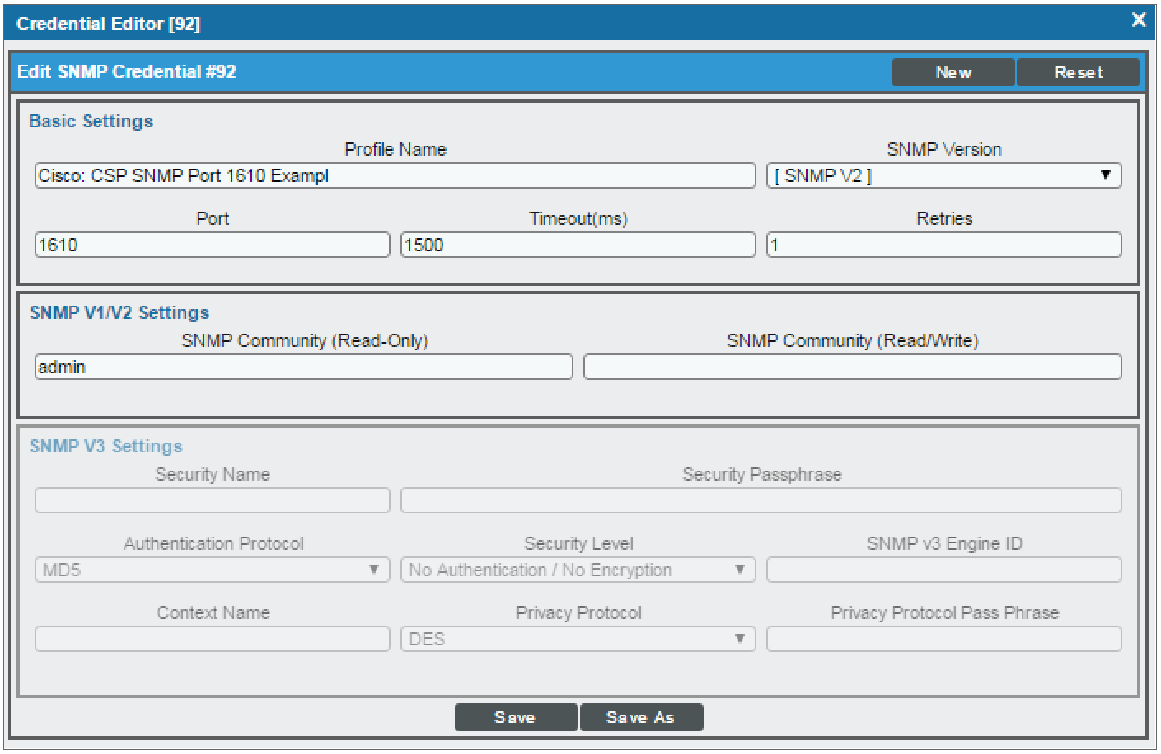
- ***Profile Name***. Enter a new name for the credential.
- ***SNMP Community (Read Only)***. Enter the port 161 community string for the CSP-2100 cluster.

4. Use the default values for the other fields on this page.
5. Click the **[Save As]** button.
6. When the confirmation message appears, click **[OK]**.

To configure the port 1610 SNMP credential for CSP-2100:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **Cisco: CSP SNMP Port 1610 Example** credential, then click its wrench icon (🔧). The **Edit SNMP Credential** modal page appears.

3. Make entries in the following fields:



Edit SNMP Credential #92

Basic Settings

Profile Name: Cisco: CSP SNMP Port 1610 Exampl

SNMP Version: [SNMP V2] ▼

Port: 1610

Timeout(ms): 1500

Retries: 1

SNMP V1/V2 Settings

SNMP Community (Read-Only): admin

SNMP Community (Read/Write):

SNMP V3 Settings

Security Name:

Security Passphrase:

Authentication Protocol: MD5 ▼

Security Level: No Authentication / No Encryption ▼

SNMP v3 Engine ID:

Context Name:

Privacy Protocol: DES ▼

Privacy Protocol Pass Phrase:

- ***Profile Name***. Enter a new name for the credential.
- ***SNMP Community (Read Only)***. Enter the port 1610 community string for the CSP-2100 cluster.

4. Use the default values for the other fields on this page.
5. Click the **[Save As]** button.
6. When the confirmation message appears, click **[OK]**.

Creating a Basic/Snippet Credential for CSP-2100 Clusters

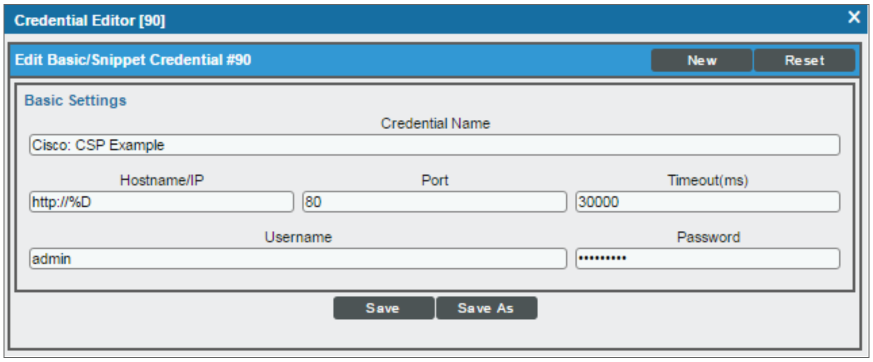
Some Dynamic Applications in the *Cisco: CSP-2100* PowerPack collect data from CSP-2100 clusters using REST API. These Dynamic Applications require a Basic/Snippet credential to enable the ScienceLogic platform to communicate with the cluster. An example Basic/Snippet credential that you can edit for your own use is included in the *Cisco: CSP-2100* PowerPack.

NOTE: For more information about the configuration required for the Basic/Snippet credential, see the *Prerequisites* section.

To create a Basic/Snippet credential to monitor CSP-2100:

1. Go to the **Credential Management** page (System > Manage > Credentials).

2. Locate the **Cisco: CCE Sample Credential**, then click its wrench icon (🔧). The **Edit Basic/Snippet Credential** modal page appears.
3. Enter values in the following fields:



Credential Editor [90]

Edit Basic/Snippet Credential #90

Basic Settings

Credential Name: Cisco: CSP Example

Hostname/IP: http://%D

Port: 80

Timeout(ms): 30000

Username: admin

Password: •••••••••

- ***Credential Name***. Enter a new name for the credential.
- ***Username***. Enter the username for a user with REST API read access to the CSP-2100 cluster and a role of operator-group or admin-group.
- ***Password***. Enter the password for the REST API user.

4. Use the default values for the other fields on this page.
5. Click the **[Save As]** button.
6. When the confirmation message appears, click **[OK]**.

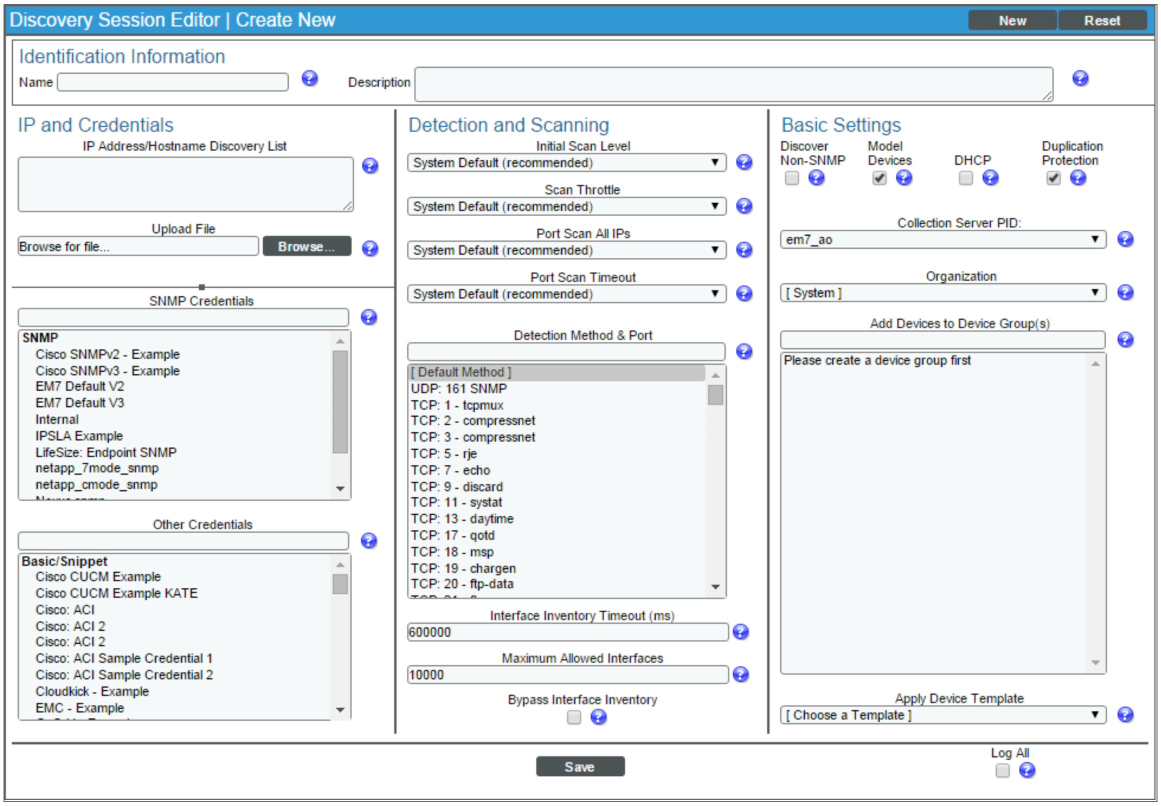
Discovering CSP-2100 Clusters

When you discover your CSP-2100 cluster with the ScienceLogic platform, the platform auto-aligns a series of Dynamic Applications to discover, configure, and monitor the CSP-2100 cluster and all of its associated component devices.

To discover your CSP-2100 cluster, perform the following steps:

1. Go to the **Discovery Control Panel** page (System > Manage > Discovery).

2. Click the **[Create]** button. The **Discovery Session Editor** page appears:



Discovery Session Editor | Create New

New Reset

Identification Information

Name

Description

IP and Credentials

IP Address/Hostname Discovery List

Upload File

Browse for file... Browse...

SNMP Credentials

SNMP
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
EM7 Default V2
EM7 Default V3
Internal
IPSLA Example
LifeSize: Endpoint SNMP
netapp_7mode_snmp
netapp_cmode_snmp

Other Credentials

Basic/Snippet
Cisco CUCM Example
Cisco CUCM Example KATE
Cisco: ACI
Cisco: ACI 2
Cisco: ACI 2
Cisco: ACI Sample Credential 1
Cisco: ACI Sample Credential 2
Cloudkick - Example
EMC - Example

Detection and Scanning

Initial Scan Level: System Default (recommended)

Scan Throttle: System Default (recommended)

Port Scan All IPs: System Default (recommended)

Port Scan Timeout: System Default (recommended)

Detection Method & Port

[Default Method]
UDP: 161 SNMP
TCP: 1 - tcpmux
TCP: 2 - compressnet
TCP: 3 - compressnet
TCP: 5 - rje
TCP: 7 - echo
TCP: 9 - discard
TCP: 11 - systat
TCP: 13 - daytime
TCP: 17 - qotd
TCP: 18 - msp
TCP: 19 - chargen
TCP: 20 - ftp-data

Interface Inventory Timeout (ms): 600000

Maximum Allowed Interfaces: 10000

Bypass Interface Inventory ☐

Basic Settings

Discover Non-SNMP ☐ Model Devices ☑ DHCP ☐ Duplication Protection ☑

Collection Server PID: em7_ao

Organization: [System]

Add Devices to Device Group(s)

Please create a device group first

Apply Device Template: [Choose a Template]

Save

Log All ☐

3. Supply values in the following fields:

   - ***IP Address/Hostname Discovery List***. Enter the IP addresses of the CSP-2100 nodes you want to discover.
   - ***SNMP Credentials***. Select the SNMP credentials you created.
   - ***Other Credentials***. Select the Basic/Snippet credentials you created.
   - ***Discover Non-SNMP***. Select this checkbox.

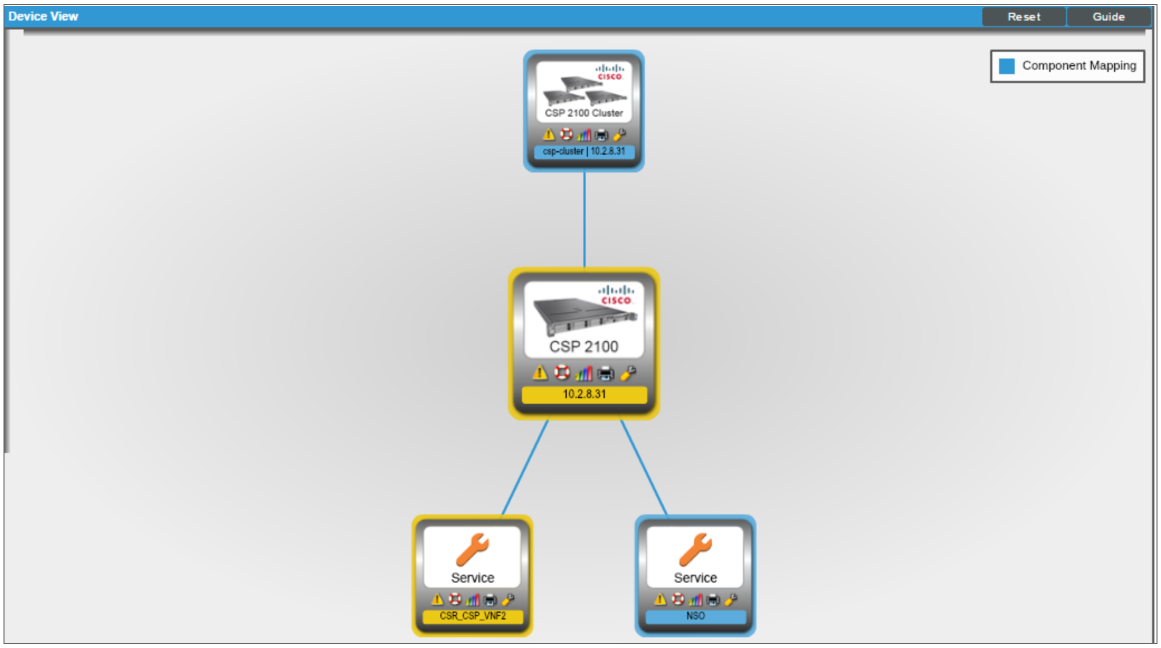
4. Optionally, supply values in the other fields in this page. For a description of the fields in this page, see the ***Discovery & Credentials*** manual.
5. Click the **[Save]** button.
6. The **Discovery Control Panel** page will refresh. Click the lightning bolt icon (⚡) for the discovery session you created.
7. In the pop-up window that appears, click the **[OK]** button. The **Discovery Session** page displays the progress of the discovery session.

Viewing CSP-2100 Component Devices

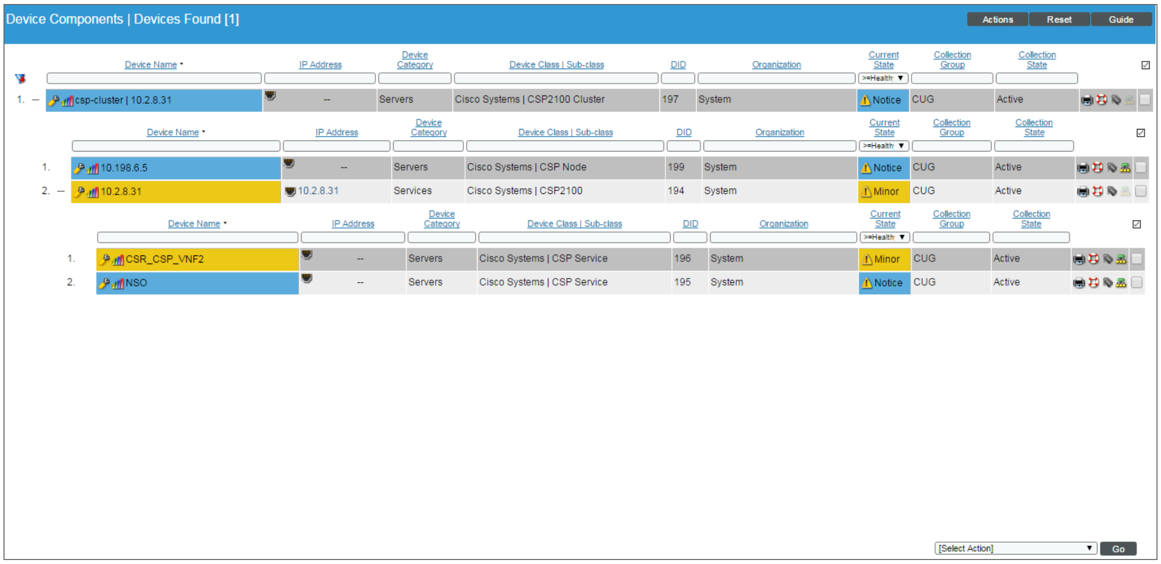
When the ScienceLogic platform discovers your CSP-2100 cluster, the platform creates component devices that represent each component in the cluster.

In addition to the **Device Manager** page, you can view all associated component devices in the following places in the user interface:

- The **Device View** modal page (click the bar-graph icon [📊] for a device, then click the **Topology** tab) displays a map of the selected device and all of the devices with which it has parent-child relationships. Double-clicking any of the devices listed reloads the page to make the selected device the primary device:



- The **Device Components** page (Registry > Devices > Device Components) displays a list of all root devices and component devices discovered by the ScienceLogic platform, in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with your CSP-2100 cluster, find the root device and click its plus icon (**+**):



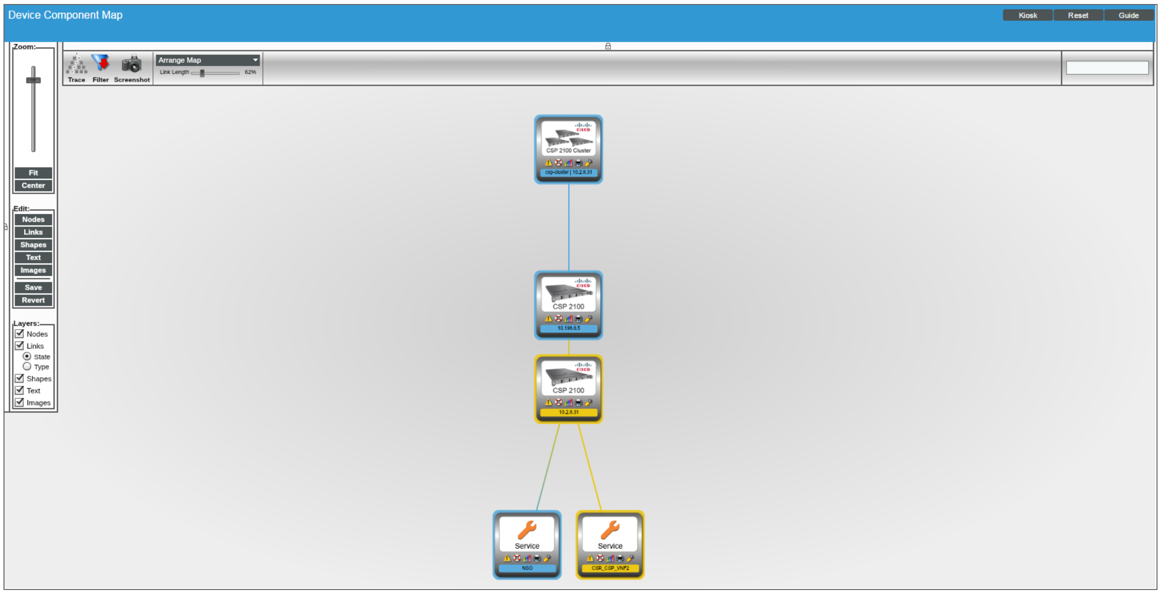
Device Components | Devices Found [1]

	Device Name	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State	Collection Group	Collection State
1. –	csp-cluster | 10.2.8.31	--	Servers	Cisco Systems | CSP2100 Cluster	197	System	Notice	CUG	Active

	Device Name	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State	Collection Group	Collection State
1.	10.198.6.5	--	Servers	Cisco Systems | CSP Node	199	System	Notice	CUG	Active
2. –	10.2.8.31	10.2.8.31	Services	Cisco Systems | CSP2100	194	System	Minor	CUG	Active

	Device Name	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State	Collection Group	Collection State
1.	CSR_CSP_VNF2	--	Servers	Cisco Systems | CSP Service	196	System	Minor	CUG	Active
2.	NSO	--	Servers	Cisco Systems | CSP Service	195	System	Notice	CUG	Active

- The **Component Map** page (Views > Device Maps > Components) allows you to view devices by root node and view the relationships between root nodes, parent components, and child components in a map. This makes it easy to visualize and manage root nodes and their components. The ScienceLogic platform automatically updates the **Component Map** as new component devices are discovered. The platform also updates each map with the latest status and event information. To view the map for your CSP-2100 cluster, go to the **Component Map** page and select the map from the list in the left NavBar. To learn more about the **Component Map** page, see the ***Views*** manual.



Device Component Map

Relationships Between Component Devices

In addition to parent/child relationships between component devices, the ScienceLogic platform also creates relationships between CSP-2100 nodes and Cisco UCS Standalone servers.

Chapter

3

Cisco Cloud Services Platform Device Dashboards

Overview

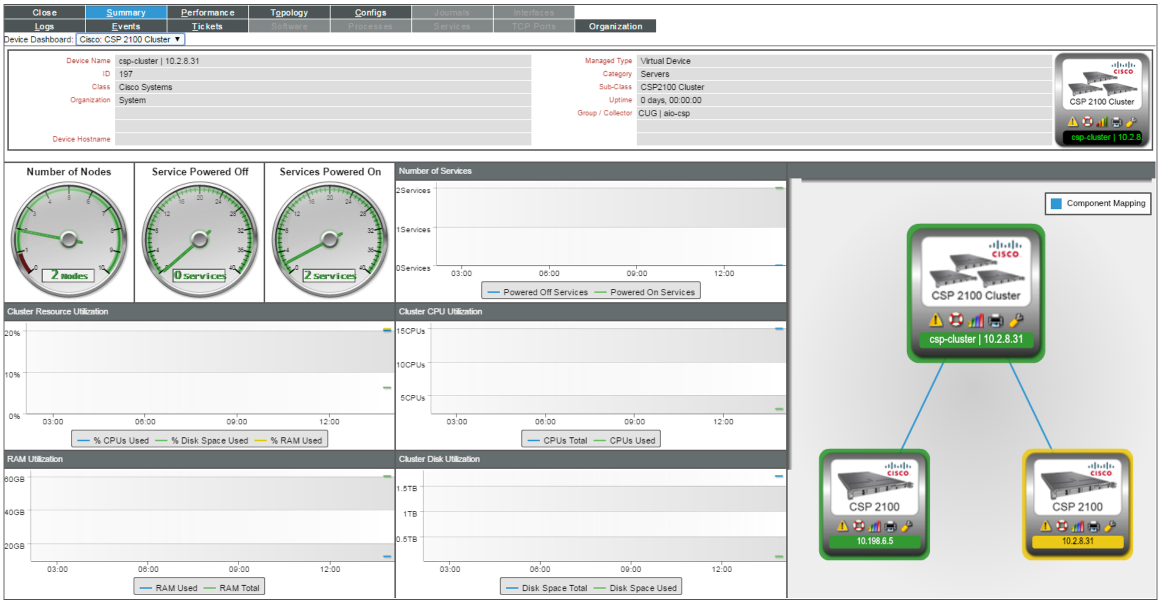
This chapter describes the device dashboards that are included in the *Cisco: CSP-2100* PowerPack.

Device Dashboards

The *Cisco: CSP-2100* PowerPack includes device dashboards that provide summary information for Cisco Cloud Services Platform (CSP) 2100 component devices. The following device dashboards in the *Cisco: CSP-2100* PowerPack are set as the default device dashboard for the equivalent device class:

- *Cisco: CSP 2100 Cluster*
- *Cisco: CSP 2100 Node*
- *Cisco: CSP 2100 Service*

Cisco: CSP 2100 Cluster



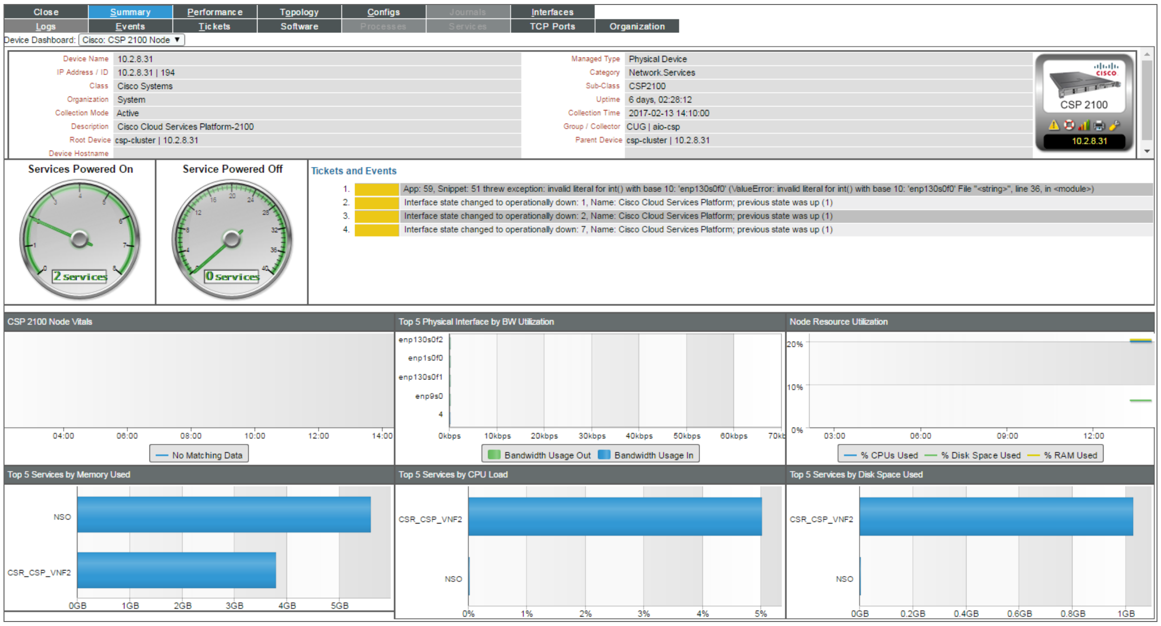
Device Dashboard: Cisco: CSP 2100 Cluster

Device Name	csp-cluster | 10.2.8.31	Managed Type	Virtual Device
ID	197	Category	Servers
Class	Cisco Systems	Sub-Class	CSP2100 Cluster
Organization	System	Uptime	0 days, 00:00:00
		Group / Collector	CUG | aio-csp
Device Hostname			

The Cisco: CSP 2100 Cluster device dashboard displays the following information:

- Gauges that indicate:
  - The number of nodes in the cluster
  - The number of services in the cluster that are currently powered off
  - The number of services in the cluster that are currently powered on
- The number of services over a specified period of time
- Cluster resource utilization over a specified period of time
- Cluster CPU utilization over a specified period of time
- RAM utilization over a specified period of time
- Cluster disk utilization over a specified period of time
- A topology map displaying the component device and its parent-child relationships

Cisco: CSP 2100 Node



Device Dashboard: Cisco: CSP 2100 Node

Device Name	10.2.8.31	Managed Type	Physical Device
IP Address / ID	10.2.8.31 | 194	Category	Network.Services
Class	Cisco Systems	Sub-Class	CSP2100
Organization	System	Uptime	6 days, 02:28:12
Collection Mode	Active	Collection Time	2017-02-13 14:10:00
Description	Cisco Cloud Services Platform-2100	Group / Collector	CUG | aio-csp
Root Device	csp-cluster | 10.2.8.31	Parent Device	csp-cluster | 10.2.8.31
Device Hostname			

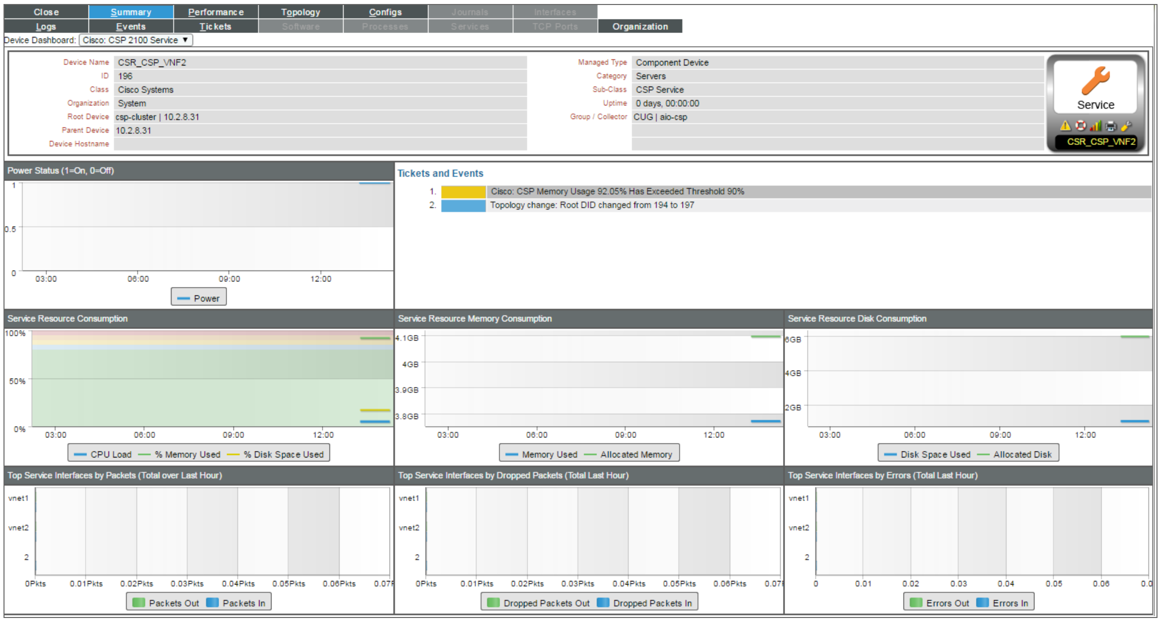
Tickets and Events

1. App: 59, Snippet: 51 threw exception: invalid literal for int() with base 10: 'enp130s0f0' (ValueError: invalid literal for int() with base 10: 'enp130s0f0' File "<string>", line 36, in <module>)
2. Interface state changed to operationally down: 1, Name: Cisco Cloud Services Platform; previous state was up (1)
3. Interface state changed to operationally down: 2, Name: Cisco Cloud Services Platform; previous state was up (1)
4. Interface state changed to operationally down: 7, Name: Cisco Cloud Services Platform; previous state was up (1)

The Cisco: CSP 2100 Node device dashboard displays the following information:

- Gauges that indicate:
  - The number of services in the node that are currently powered on
  - The number of services in the node that are currently powered off
- A list of tickets and events relating to the node
- Node vitals over a specified period of time
- The top 5 physical interfaces in the node based on bandwidth utilization
- Node resource utilization over a specified period of time
- The top 5 services in the node based on memory utilization
- The top 5 services in the node based on CPU load
- The top 5 services in the node based on disk space utilization

Cisco: CSP 2100 Service



Device Dashboard: Cisco: CSP 2100 Service ▼

Device Name	CSR_CSP_VNF2	Managed Type	Component Device
ID	196	Category	Servers
Class	Cisco Systems	Sub-Class	CSP Service
Organization	System	Uptime	0 days, 00:00:00
Root Device	csp-cluster | 10.2.8.31	Group / Collector	CUG | aio-csp
Parent Device	10.2.8.31		
Device Hostname			

Tickets and Events

1. Cisco: CSP Memory Usage 92.05% Has Exceeded Threshold 90%
2. Topology change: Root DID changed from 194 to 197

The Cisco: CSP 2100 Service device dashboard displays the following information:

- The service's power status (i.e., on or off) over a specified period of time
- A list of tickets and events relating to the service
- Service resource consumption over a specified period of time
- Service resource memory consumption over a specified period of time
- Service resource disk consumption over a specified period of time
- The top service interfaces based on packets in and out over the previous hour
- The top service interfaces based on dropped packets in and out over the previous hour
- The top service interfaces based on errors in and out over the previous hour

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com

ScienceLogic

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010