Monitoring Cisco: Intersight

Cisco: Intersight PowerPack version 101

Table of Contents

Chapter 3

Introduction

Overview

This manual describes how to monitor Cisco Intersight devices in SL1 using the Dynamic Applications in the *Cisco: Intersight* PowerPack.

The following sections provide an overview of Cisco Intersight and the *Cisco: Intersight* PowerPack:

This chapter covers the following topics:

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.

What is Cisco Intersight?

Cisco Intersight is a cloud operations platform allowing for advanced infrastructure, workload optimization, and Kubernetes services. Cisco Intersight infrastructure services include the deployment, monitoring, management, and support of physical and virtual infrastructure.

What Does the Cisco: Intersight PowerPack Monitor?

To monitor Cisco Intersight using SL1, you must install the *Cisco: Intersight* PowerPack. This PowerPack enables you to discover, model, and collect data about Cisco:Intersight devices.

The *Cisco: Intersight* PowerPack includes:

- Dynamic Applications that enable SL1 to discover, model, and monitor Cisco Intersight devices
- Event Policies that are triggered when Cisco Intersight devices meet certain status criteria
- Device Classes for each type of Cisco Intersight device monitored

Installing the Cisco: Intersight PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *Cisco: Intersight* PowerPack.

TIP: By default, installing a new version of a PowerPack overwrites all content from a previous version of 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 section on ***Global Settings***.

To download and install the PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page (Product Downloads > PowerPacks & SyncPacks) at the ScienceLogic Support Site.
2. In SL1, go to the **PowerPacks** page (System > Manage > PowerPacks).
3. Click the **[Actions]** button and choose *Import PowerPack*. The **Import PowerPack** dialog box appears.
4. Click **[Browse]** and navigate to the PowerPack file from step 1.
5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal displays a list of the PowerPack contents.
6. Click **[Install]**. The PowerPack is added to the **PowerPacks** page.

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

Chapter 4

Configuration and Discovery

Overview

The following sections describe how to configure and discover Cisco Intersight devices for monitoring by SL1 using the *Cisco: Intersight* PowerPack:

This chapter covers the following topics:

Prerequisites for Monitoring Cisco Intersight

To configure the SL1 system to monitor Cisco Intersight devices using the *Cisco: Intersight* PowerPack, you must first have the following information about Cisco Intersight:

- The username and password for your Cisco Intersight account.
- A Cisco Intersight REST API key ID and Secret Key. See the Introduction to the Cisco Intersight REST API section of the Cisco Intersight documentation to view how to generate the REST API key ID and Secret Key.

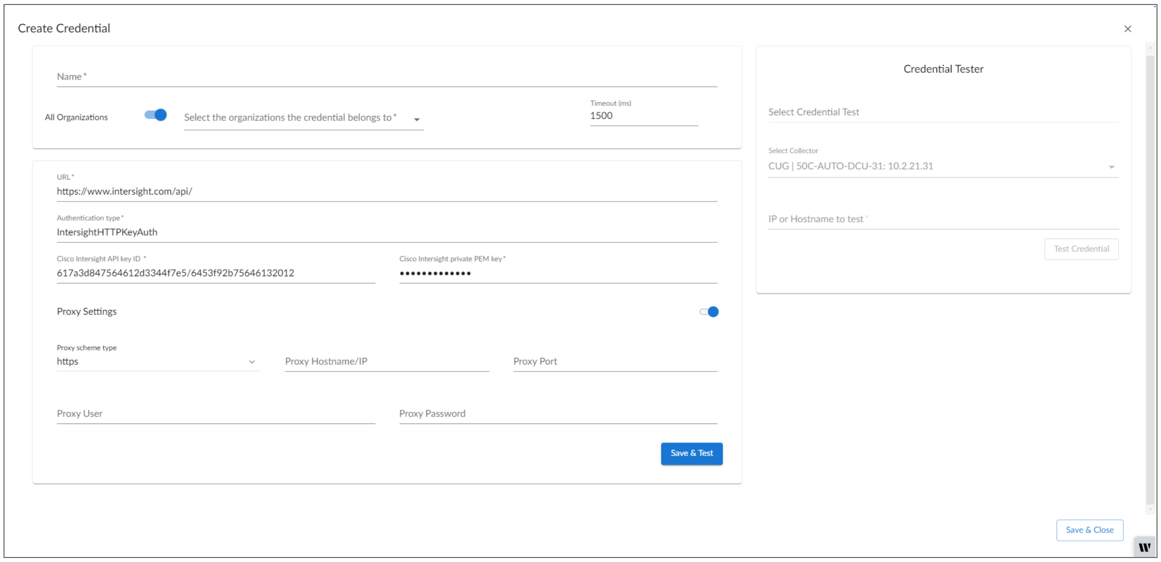
NOTE: ScienceLogic recommends that you use API key schema version 2 to reconnect to the Intersight API. However, the API key schema version 2 will be deprecated in future versions.

Creating a "Universal" Type Credential for Cisco Intersight

To configure SL1 to monitor Cisco Intersight devices, you must create a "universal" type credential. This credential allows the Dynamic Applications in the *Cisco: Intersight* PowerPack to communicate with Cisco Intersight.

To define a "universal" type credential to access Cisco Intersight:

1. Go to the **Credentials** page (Manage > Credentials).
2. Click **[Create New]** and select *Create Cisco Intersight Credential*. The **Create Credential** modal page appears.


Create Credential

Timeout (ms): 1500

URL*: https://www.intersight.com/api/

Authentication type*: IntersightHTTPKeyAuth

Cisco Intersight API key ID *: 617a3d847564612d3344f7e5/6453f92b75646132012

Cisco Intersight private PEM key*: •••••••••••••

Proxy scheme type: https

Select Collector: CUG | 50C-AUTO-DCU-31: 10.2.21.31

3. Supply values in the following fields:
   - ***Name***. Type a name for your credential.
   - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the from the ***What organization manages this service?*** drop-down field to align the credential with those specific organizations.
   - ***Timeout (ms)***. Keep the default value of 1500.
   - ***URL***. Keep the default URL (https://www.intersight.com/api/).
   - ***Authentication type***. Keep the default value (IntersightHTTPKeyAuth).
   - ***Cisco Intersight API Key ID***.Type your Cisco Intersight API key ID.
   - ***Cisco Intersight private PEM key***. Type your Cisco Intersight secret key.

   <u>Proxy Settings</u>

   Toggle on this field if you are using a proxy server to communicate with your Cisco Intersight account, enter the values in the fields listed below:

- ***Proxy scheme type***. Select *http* or *https* from the drop-down field.
- ***Proxy Hostname/IP***. Enter the hostname or the IP address associated with your device.
- ***Proxy Port***. Enter the port number for the proxy server.
- ***Proxy User***. Enter the username for the proxy server.
- ***Proxy Password***. Enter the password for the proxy server.

> **NOTE:** There is not currently a credential test available for the Cisco: Intersight PowerPack.

4. Click **[Save & Close]**.

Cisco Intersight Guided Discovery

You can use the Guided Discovery Framework process in SL1to guide you through a variety of existing discovery types in addition to traditional SNMP discovery. This process, which is also called "guided discovery", lets you choose a discovery type based on the type of devices you want to monitor. The Guided Discovery workflow includes a button for Cisco Intersight.

To run a Guided Discovery:

1. On the **Devices** page (🖥) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears.
2. Select the **[Cisco]** button. Additional information about the requirements for device discovery appears in the **General Information** pane to the right.
3. Click **[Select]**. The **Credential Selection** page appears.

> **NOTE:** During the guided discovery process, you cannot click **[Next]** until the required fields are filled on the page, nor can you skip to future steps. However, you can revisit previous steps that you have already completed.

4. On the **Credential Selection** page of the guided discovery process, select the Cisco Intersight "universal" type credential that you configured, and then click **[Next]**. The **Root Device Details** page appears.
5. Complete the following fields:
   - ***Root Device Name***. Type the name of the root device for the Cisco Intersight root device you want to monitor.
   - ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered device.
   - ***Collector Group Name***. Select an existing collector group to communicate with the discovered device. This field is required.
6. Click **[Next]**. SL1 creates the Cisco Intersight root device with the appropriate Device Class assigned to it and aligns the relevant Dynamic Applications. The **Final Summary** page appears.
7. Click **[Close]**.

TIP: This PowerPack uses the snippet framework in order to function. Not all values returned in an API call in a Dynamic Application may have a collection object. For more information about how collections can be modified, added, or deleted using the snippet framework, see the ***Snippet Framework*** documentation.

NOTE: The results of a guided discovery do not display on the **Discovery Sessions** page (Devices > Discovery Sessions).

Viewing Cisco Intersight Component Devices

In addition to the **Devices** page, you can view the Cisco Intersight system and all associated component devices in the following places in the user interface:

- The **Device Investigator** Map page (click **Map** in the **Device Investigator** page) displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the listed devices reloads the page to make the selected device the primary device

- The **Device Components** page (Devices > Device Components) displays a list of all root devices and component devices discovered by SL1 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 a Kubernetes cluster, find the cluster device and click its plus icon (**+**).

- The **Component Map** page (Classic Maps > 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. SL1 automatically updates the **Component Map** as new component devices are discovered. SL1 also updates each map with the latest status and event information. To view the map for a Kubernetes cluster, go to Classic Maps > Device Maps > Components, and select the map from the list in the left NavBar. To learn more about the **Component Map** page, see the ***Views*** manual.

Configuring Alerts to Receive Alarms from Cisco Intersight

The Cisco: Intersight PowerPack includes the "Cisco: Intersight Alarms Configuration" Dynamic Application that monitors Cisco Intersight alarms and associates the alarms with the appropriate component devices, if applicable. The Cisco Intersight API reports alarms regardless of whether or not they are acknowledged. You can choose to change your alert formulas in SL1 to ignore acknowledged alerts if you do not want to see them. To learn more about filtering alerts, see the ***Dynamic Application Development*** manual.

NOTE: If you expect that you will go 24 hours without collecting an alarm, ScienceLogic recommends toggling on the Disable Object Maintenance option on the Dynamic Application to avoid it being auto-disabled due to no collected data.

Troubleshooting Known Issues for Cisco Intersight

The following sections describe some issues you might encounter when monitoring Cisco Intersight.

Error when Running Dynamic Applications in Debug Mode

An error message similar to the one below displays when executing any Cisco: Intersight " Dynamic Application in debug mode.

```
WARNING:snippet_framework.internal.silo.low_code_
steps.rest.authenticators:Error parsing time to next request from
Credential. Setting to 5.
```

```
2023-10-30 18:32:43,752 - [a:896,d:27,c:9500,s:low_code] Successfully
parsed the Snippet Argument
```

```
INFO:snippet_framework.step.generic_step_area:[a:896,d:27,c:9500,s:low_
code] Successfully parsed the Snippet Argument
```

```
2023-10-30 18:32:43,752 - Error parsing time to next request from
Credential. Setting to 5.
```

Current Limitations of the Cisco: Intersight PowerPack

The "Cisco: Intersight"" PowerPack is currently limited due to the way that Cisco Intersight returns data from the API.

- The Cisco Intersight API returns the last collected data when a device is disconnected and does not provide any indication that the device is disconnected. If a device is disconnected in Cisco Intersight, SL1 may continue to show the last collected data from Cisco Intersight.
- Cisco Intersight does not publish rate limiting. Due to this, SL1 cannot provide scale numbers.

Support for RSA Private Keys for the PEM Key

The "Cisco: Intersight" PowerPack only supports the RSA Private Keys for the Cisco: Intersight private PEM key in the universal credential required for authentication.

If you are unable to connect to the Intersight API after renewing your API key, you may receive one of the following errors after a debug run:

Error Line	Message
126	Exception: Traceback (most recent call last):
127	File "/opt/em7/envs/uenv-273658009003493483O/lib/python3.6/site-packages/silo/cisco_intersight/auth.py", line 184, in __init__
128	backend=default_backend(),
129	File "/opt/em7/lib/python3/cryptography/hazmat/primitives/serialization/base.py", line 22, in load_pem_private_key
130	return ossl.load_pem_private_key(data, password)
131	File "/opt/em7/lib/python3/cryptography/hazmat/backends/openssl/backend.py", line 906, in load_pem_private_key
132	password,
133	File "/opt/em7/lib/python3/cryptography/hazmat/backends/openssl/backend.py", line 1170, in _load_key
134	self._handle_key_loading_error()
135	File "/opt/em7/lib/python3/cryptography/hazmat/backends/openssl/backend.py", line 1234, in _handle_key_loading_error
136	errors_with_text,
137	ValueError: ('Could not deserialize key data. The data may be in an incorrect format, it may be encrypted with an unsupported algorithm, or it may be an unsupported key type (e.g. EC curves with explicit parameters).', [_OpenSSLErrorWithText(code=503841036, lib=60, reason=524556, reason_text=b'error:1E08010C:DECODER routines::unsupported')])

or these errors:

Error Line	Message
151	File "/opt/em7/envs/uenv-273658009003493483O/lib/python3.6/site-packages/silo/cisco_intersight/auth.py", line 216, in __call__
152	signing_headers, r.method, path, self.api_key_id, self.secret_key
153	File "/opt/em7/envs/uenv-273658009003493483O/lib/python3.6/site-packages/silo/cisco_intersight/auth.py", line 75, in _get_auth_header
154	b64_signed_auth_digest = _get_rsasig_b64(secret_key, string_to_sign.encode())
155	File "/opt/em7/envs/uenv-273658009003493483O/lib/python3.6/site-packages/silo/cisco_intersight/auth.py", line 70, in _get_rsasig_b64
156	return b64encode(key.sign(string_to_sign, padding.PKCS1v15(), hashes.SHA256()))

Error Line	Message
157	TypeError: sign() takes 3 positional arguments but 4 were given
158	2024-08-28 14:22:43,429 - [a:3770,d:174677,c:31266,s:http] A blocking error occurred for the collection and can no longer continue.
159	Executor: <bound method HTTPRequest.call of <silo.low_code_steps.rest.network_request.HTTPRequest object at 0x7f61e1ebd390>>

To resolve this issue and reconnect to the API, the PEM key must be a private RSA key in the following format:

```
-----BEGIN RSA PRIVATE KEY-----

MIIEowIBAAKCAQEA7rrAbwAMLKvbPQ2RrDhpuNyxATfAYjVBn7m2JdSvHZVikFBY

....

GP5oSIV+K1VtD3uMUCNgb4x/M7tk3VnB9BXL3BFvDG0j3dL5x7hTMSDBSHJWAGnW

-----END RSA PRIVATE KEY-----
```

NOTE: The current version of this PowerPack supports API key schema version 2 to communicate to the Intersight API. However, the API key schema version 2 will be deprecated in future versions.

© 2003 - 2025, ScienceLogic, Inc.

All rights reserved.

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. For more information, see https://sciencelogic.com/company/legal.

ScienceLogic

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

International: +1-703-354-1010