



Monitoring Cisco UC Voice Operating System (VOS) Applications

Cisco: UC VOS Applications PowerPack version 109

Table of Contents

Introduction	3
What are Cisco UC VOS Applications?	3
What Does the Cisco: UC VOS Applications PowerPack Monitor?	4
Installing the Cisco: UC VOS Applications PowerPack	5
Configuration and Credentials	6
Configuring Cisco UC VOS Applications for Monitoring	7
Configuring SNMP for Cisco VOS Applications	7
Creating the User Account for the Platform Administrative Web Services (PAWS) API	8
Configuring Cisco Unity Connection	9
Configuring Cisco Unified Communications Manager IM and Presence	10
Configuring Cisco Prime License Manager	11
Configuring Cisco Prime Collaboration Deployment	12
Configuring Cisco Collaboration Mediation Fulfillment	13
Configuring Hosted Collaboration Solution Intelligent Loader	13
Configuring Cisco Contact Center Express	13
Configuring Cisco Emergency Responder	13
Configuring Cisco SocialMiner	13
Enabling Network Address Translation (NAT) for Cisco UC VOS Devices	14
Creating Cisco UC VOS Application Credentials	16
Creating an SNMP Credential	16
Creating a SOAP/XML Credential (PAWS API)	17
Creating a SOAP/XML Credential (non-PAWS API)	20
Creating a Basic/Snippet Credential	23
Testing the Cisco UC VOS Credential	24
Discovery	27
Discovering VOS Application Clusters	27
Viewing VOS Devices	29

Chapter



1

Introduction

Overview

This chapter describes how to monitor Cisco Unified Communications (UC) Voice Operating System (VOS) applications in SL1.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (.
- To view a page containing all the menu options, click the Advanced menu icon (.

The following sections provide an overview of Cisco UC VOS and the *Cisco: UC VOS Applications PowerPack*:

What are Cisco UC VOS Applications?	3
What Does the Cisco: UC VOS Applications PowerPack Monitor?	4
Installing the Cisco: UC VOS Applications PowerPack	5

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 are Cisco UC VOS Applications?

The following Cisco UC applications and devices share the Cisco Voice Operating System (VOS):

- Cisco Contact Center Express (CCX)
- Cisco Unity Connection (CUC) servers
- Cisco Hosted Collaboration Mediation for Fulfillment (HCM-F)
- Cisco HCS Intelligent Loader
- Cisco IM & Presence (IM&P) servers
- Cisco Prime License Manager (PLM)
- Cisco Emergency Responder
- Cisco Prime Collaboration Deployment (PCD) servers
- Cisco SocialMiner

NOTE: In the past, Cisco labeled VOS as "Cisco Unified Communications Operating System" and "Cisco Unified Operating System."

What Does the Cisco: UC VOS Applications PowerPack Monitor?

To monitor Cisco VOS applications using SL1, you must install the *Cisco: UC VOS Applications PowerPack*. This PowerPack enables you to discover, model, and collect data about VOS applications.

The *Cisco: UC VOS Applications PowerPack* includes:

- Three example credentials you can use as templates to create SOAP/XML and/or Basic/Snippet credentials to connect to the VOS applications you want to monitor
- Dynamic Applications and Run Book Actions to discover, model, and monitor performance metrics and/or collect configuration data for VOS applications and devices.
- Device Classes for each of the VOS applications and devices SL1 monitors
- Event Policies and corresponding alerts that are triggered when VOS devices meet certain status criteria
- Run Book Action and Automation policies that do the following:
 - Align the correct device class to Cisco VOS systems based on the GUID passed in an event.
 - Align the appropriate "Cluster Status" Dynamic Applications to VOS Cluster virtual root devices.
 - Verify that component devices remain aligned to the same collector as the root device.
 - Move the physical devices discovered using the *Cisco: UC VOS Applications PowerPack* to the same collector as their component devices when merging physical and component devices.

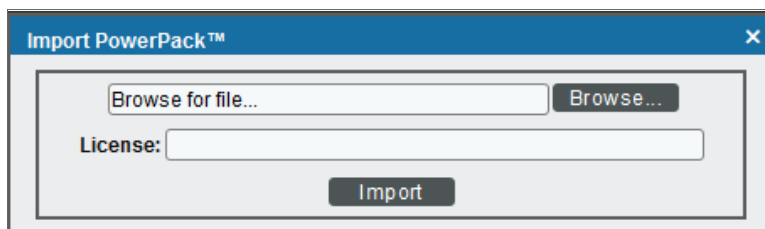
Installing the Cisco: UC VOS Applications PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *Cisco: UC VOS Applications 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 **System Administration** manual.)

To download and install a PowerPack:

1. Download the PowerPack from the [ScienceLogic Support Site](#).
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 appears, click the **[Install]** button to install the PowerPack.

NOTE: If you exit the **PowerPack Installer** modal 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. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.



Chapter

2

Configuration and Credentials

Overview

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (.
- To view a page containing all the menu options, click the Advanced menu icon (.

The following sections describe how to configure Cisco UC Voice Operating System (VOS) applications for monitoring by SL1 using the *Cisco: UC VOS Applications PowerPack*:

Configuring Cisco UC VOS Applications for Monitoring	7
<i>Configuring SNMP for Cisco VOS Applications</i>	7
<i>Creating the User Account for the Platform Administrative Web Services (PAWS) API</i>	8
<i>Configuring Cisco Unity Connection</i>	9
<i>Configuring Cisco Unified Communications Manager IM and Presence</i>	10
<i>Configuring Cisco Prime License Manager</i>	11
<i>Configuring Cisco Prime Collaboration Deployment</i>	12
<i>Configuring Cisco Collaboration Mediation Fulfillment</i>	13
<i>Configuring Hosted Collaboration Solution Intelligent Loader</i>	13
<i>Configuring Cisco Contact Center Express</i>	13
<i>Configuring Cisco Emergency Responder</i>	13
<i>Configuring Cisco SocialMiner</i>	13
Enabling Network Address Translation (NAT) for Cisco UC VOS Devices	14
Creating Cisco UC VOS Application Credentials	16

<i>Creating an SNMP Credential</i>	16
<i>Creating a SOAP/XML Credential (PAWS API)</i>	17
<i>Creating a SOAP/XML Credential (non-PAWS API)</i>	20
<i>Creating a Basic/Snippet Credential</i>	23
<i>Testing the Cisco UC VOS Credential</i>	24

Configuring Cisco UC VOS Applications for Monitoring

Before performing the other tasks in this chapter, you must create accounts for the different Cisco VOS applications that you want to monitor in SL1. The following sections describe how to configure the Cisco VOS applications.

Configuring SNMP for Cisco VOS Applications

SL1 uses SNMP to collect information about the following Cisco VOS applications:

- Cisco Contact Center Express (CCX)
- Cisco Unity Connection (CUC) servers
- Cisco Hosted Collaboration Mediation for Fulfillment (HCM-F)
- Cisco HCS Intelligent Loader
- Cisco IM & Presence (IM&P) servers (optional)
- Cisco Emergency Responder
- Cisco Prime Collaboration Deployment (PCD) servers (optional, but recommended)
- Cisco SocialMiner

To configure SNMP for Cisco VOS applications:

1. Log in as an administrative user to the command-line interface of the Cisco VOS application that you want to monitor. You can also use SSH to connect to the application.
2. Run the following command with additional parameters as needed:

```
utils snmp config
```

3. When prompted, add additional SNMP information. The following image displays additional configuration parameters, based on SNMP version (version 1 or 2, or version 3):

```
admin:utils snmp config 1/2c
      utils snmp config 1/2c community-string*
      utils snmp config 1/2c inform*
      utils snmp config 1/2c trap*

admin:utils snmp config 3
      utils snmp config 3 inform*
      utils snmp config 3 trap*
      utils snmp config 3 user*
```

4. For additional SNMP configuration commands and instructions, see the [Cisco Command Line Interface Reference Guide](#).

Creating the User Account for the Platform Administrative Web Services (PAWS) API

To get access to the Platform Administrative Web Services (PAWS) API, you can create a new user account by using the command-line interface on the console of the Cisco VOS application that you want to monitor. You can also use SSH to connect to the application.

You can then use this user account to connect to the following Cisco VOS applications:

- Cisco Contact Center Express (CCX)
- Cisco Unity Connection (CUC) servers
- Cisco Hosted Collaboration Mediation for Fulfillment (HCM-F)
- Cisco HCS Intelligent Loader
- Cisco IM & Presence (IM&P) servers
- Cisco Unified Communications Manager (CUCM)
- Cisco Prime License Manager (PLM)
- Cisco Prime Collaboration Deployment (PCD) servers
- Cisco SocialMiner

To create the PAWS API user account:

1. Log in as an administrative user to the command-line interface of the Cisco VOS application that you want to monitor.
2. To create the new account, run the following command:

```
set account name new_account_username
```


3. The interface prompts you for the privilege level and password for the new account:

```
admin:set account name em7paws

Privilege Levels are:
  Ordinary - Level 0
  Advanced - Level 1

Please enter the privilege level :0
  Please enter the password :*****
    re-enter to confirm :*****
Account successfully created
```

4. Set the privilege level to 0.
5. Type the password, then retype the password to confirm.
6. Newer versions of Cisco Unified Communications products require that new accounts created with the command-line interface must change the password at the first login. This requirement blocks the account from accessing the PAWS API until you change the password. To remove the requirement for this account, run the following command:

```
set password change-at-login disable new_account_username
```

7. To confirm that the user account works with the Cisco PAWS API, log in as an administrator to one of the following addresses:

- <https://ip-address-of-cisco-application:8443/platform-services/services/ProductService?wsdl>
- <https://ip-address-of-cisco-application:8443/platform-services/services/ClusterNodesService?wsdl>

NOTE: If you receive a message that the user does not have permission to access a page, then the Cisco VOS application requires a user account like the one you just created to access the PAWS API. You might get this message if you are using Cisco Unified Communications products older than version 9, because those products do not use the PAWS API. In this situation, use the [credential setup for non-PAWS API](#). Also, you cannot use any Dynamic Applications that use the PAWS API, but you can use the SNMP and Application APIs.

Configuring Cisco Unity Connection

You can create a user account for Cisco Unity Connection applications that gives you access to other Cisco APIs such as Administrative XML (AXL), Serviceability, and Real-Time Monitoring Service. You can configure this account using the web-based interfaces for the Cisco applications. This account does not have access to the PAWS API.

NOTE: To create a PAWS API user account for Cisco Unity Connection, see [Creating the User Account for the Platform Administrative Web Services \(PAWS\) API](#).

To create the user account for Cisco Unity Connection:

1. In a browser window, navigate to the following address:
`https://ip-address-of-cisco-application/cuadmin/home.do`
2. Navigate to the relevant **Edit Users Basics** page for your version of Cisco Unity Connection (User > Users).
3. Create a new user and complete the fields as needed.
4. Select the role of **Technician** or **System Administrator**.
5. Save the new user account.
6. To confirm that the user account works with the Cisco APIs, log into one of the following addresses:
 - `https://ip-address-of-cisco-application:8443/realservice/services/RisPort?wsdl`
 - `https://ip-address-of-cisco-application:8443/controlcenterservice/services/ControlCenterServicesPort?wsdl`
7. If you are not prompted for the username and password when testing the addresses, your previous administrative login might still be active. Close the browser and navigate to the addresses again.

Configuring Cisco Unified Communications Manager IM and Presence

You can use the same account for Cisco Unified Communication Manager (CUCM) IM and Presence that you already created for CUCM. If you are creating an account specifically for monitoring IM and Presence, you only need the Standard CCM Server Monitoring Group.

NOTE: Because SL1 does not access the Administrative XML API for IM and Presence, the Standard AXL API Access role is not required.

To create a user account for CUCM IM and Presence:

1. In a browser window, navigate to the Cisco CUCM web interface:
`https://ip-address-of-cisco-cucm/ccmadmin/showHome.do`

2. Navigate to the relevant **User Management** page for your version of Cisco CUCM (User Management > Application User):

3. Click the **[Add New]** button and complete the required information for the new user account.
4. In the Permissions Information section, select the **Standard CCM Server Monitoring** and the **Admin-3rd Party API** groups and save the user record.

NOTE: To create the Level 0 PAWS API user account for CUCM, see [Creating the User Account for the Platform Administrative Web Services \(PAWS\) API](#). The discovery process for IM and Presence queries the CUCM servers using this user account to determine the server role (IM and Presence or CUCM). As a result, the PAWS API user account needs to be enabled on the CUCM nodes during discovery for IM and Presence.

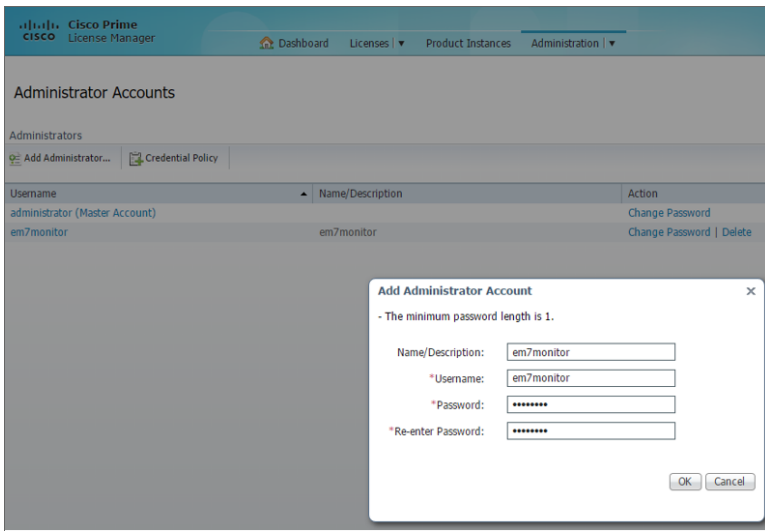
Configuring Cisco Prime License Manager

When Cisco Prime License Manager is co-resident with Cisco Unified Communications Manager, this release of the PowerPack cannot monitor Cisco Prime License Manager.

When Cisco Prime License Manager is installed as a standalone system, and is not co-resident with another Cisco product, you can only create administrative users for the application. You can use the existing administrator account or create a new account for monitoring.

To create a user account for Cisco Prime License Manager:

1. In a browser window, navigate to the following address:
`https://ip-address-of-application/elm-admin/faces/main.xhtml`
2. Navigate to the **Administrator Accounts** page for your version of Cisco Prime License Manager (Administration > Administrator Accounts):



3. Click **Add Administrator** and complete the required information.
4. After you create the user account, you can use the following address to confirm that the new account works with the APIs:

`https://ip-address-of-application/elm-admin/faces/license_usage.xhtml?`

NOTE: To create a PAWS API user account for Cisco Prime License Manager, see [Creating the User Account for the Platform Administrative Web Services \(PAWS\) API](#).

Configuring Cisco Prime Collaboration Deployment

To create the PAWS API user account for Cisco Prime Collaboration Deployment, see [Creating the User Account for the Platform Administrative Web Services \(PAWS\) API](#).

Using the PAWS API user account, use SSH to connect to the command-line interface of the application, and then run the following command to get service status:

```
utils service list
```

Configuring Cisco Collaboration Mediation Fulfillment

To create the PAWS API user account for Cisco Collaboration Mediation Fulfillment, see [Creating the User Account for the Platform Administrative Web Services \(PAWS\) API](#).

After you create the account, you can use the following address to confirm that SL1 can monitor Cisco Collaboration Mediation Fulfillment:

```
https://ip-address-of-application:8443/controlcenterservice/services/ControlCenterServicesPort?wsdl
```

Configuring Hosted Collaboration Solution Intelligent Loader

Cisco Hosted Collaboration Solution Intelligent Loader requires only a PAWS API user account. To create the PAWS API user account for Cisco Hosted Collaboration Solution Intelligent Loader, see [Creating the User Account for the Platform Administrative Web Services \(PAWS\) API](#).

After you create the account, you can use the following address to confirm that SL1 can monitor Cisco Hosted Collaboration Solution Intelligent Loader:

```
https://ip-address-of-application:8443/controlcenterservice/services/ControlCenterServicesPort?wsdl
```

Configuring Cisco Contact Center Express

Cisco Contact Center Express does not let you create additional accounts that can access the Application API. Instead of creating an Application Monitoring user account, you must use the administrative account that was assigned when the product was first installed.

To create the PAWS API user account for Cisco Contact Center Express, see [Creating the User Account for the Platform Administrative Web Services \(PAWS\) API](#).

Configuring Cisco Emergency Responder

You can only use SNMP to monitor the Cisco Emergency Responder. To set up SNMP for the Cisco Emergency Responder, see [Configuring SNMP for Cisco VOS applications](#).

Configuring Cisco SocialMiner

To set up SNMP for Cisco SocialMiner, see [Configuring SNMP for Cisco VOS applications](#).

To create the PAWS API user account for Cisco SocialMiner, see [Creating the User Account for the Platform Administrative Web Services \(PAWS\) API](#).


To use a Social Miner account, make sure that the account has Administrator credentials for API access. You can use an existing SocialMiner administrator account or create a new account for monitoring that has administrator permissions.

NOTE: Because Cisco SocialMiner is a virtual machine that does not support clusters, SL1 creates a cluster for each SocialMiner device during the discovery process. SL1 then uses that cluster to create a component level where it can use the relevant Cisco VOS dynamic applications. For more information, see [Discovering VOS Devices](#).

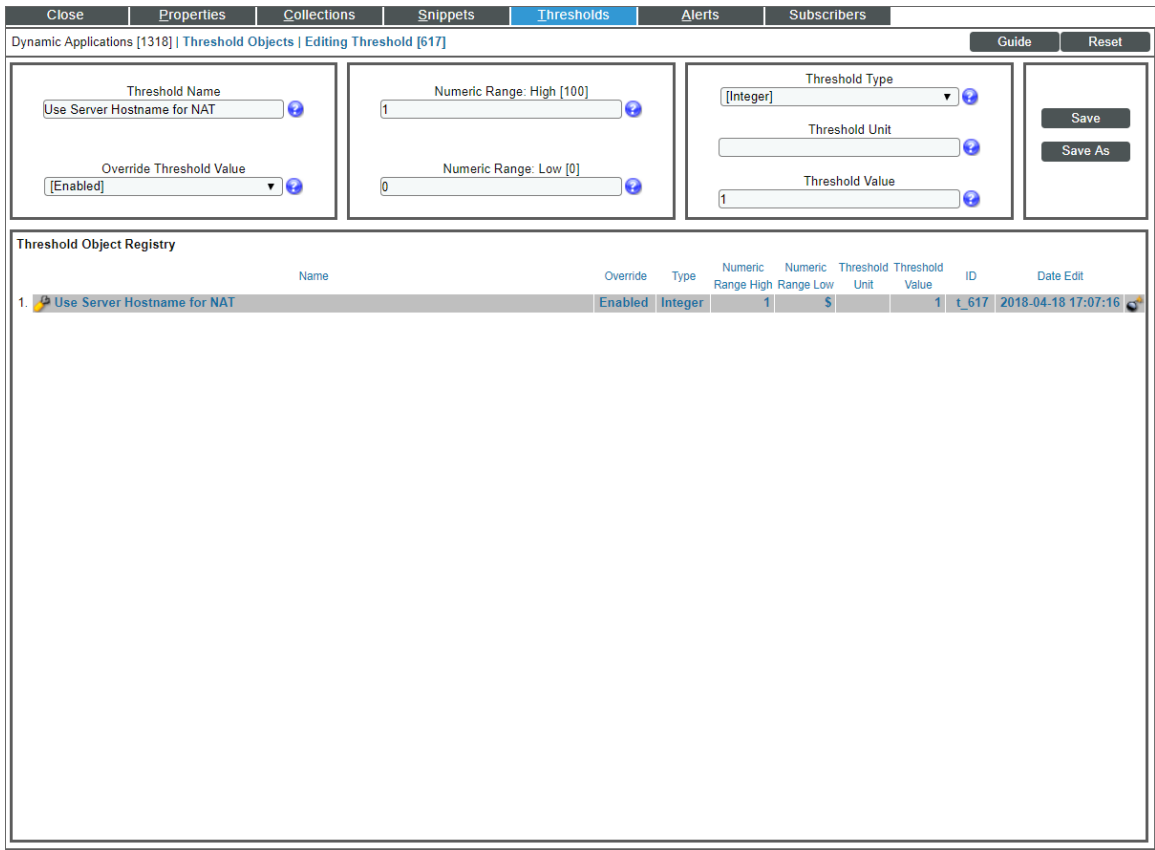
Enabling Network Address Translation (NAT) for Cisco UC VOS Devices

If you are monitoring Cisco UC VOS devices in a Network Address Translation (NAT) environment, you should enable the "Use Server Hostname for NAT" threshold object in the "Cisco: VOS Node Classification and Cluster Creation" Dynamic Application. This will cause the VOS performance monitoring Dynamic Applications to embed the target devices' component names into associated SOAP requests, rather than the devices' IP addresses.

To enable NAT support for Cisco UC VOS devices:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
2. Locate the "Cisco: VOS Node Classification and Cluster Creation" Dynamic Application and then click its wrench icon (). The **Dynamic Applications Properties Editor** page appears.
3. Click the **[Thresholds]** tab. The **Threshold Objects** page appears.

- Click the wrench icon () for the "Use Server Hostname for NAT" Threshold Object.



The screenshot shows the 'Editing Threshold' configuration page for the 'Use Server Hostname for NAT' threshold object. The page has a navigation bar with tabs for 'Close', 'Properties', 'Collections', 'Snippets', 'Thresholds', 'Alerts', and 'Subscribers'. Below the navigation bar, there are several input fields for configuring the threshold:

- Threshold Name:** 'Use Server Hostname for NAT'
- Override Threshold Value:** '[Enabled]'
- Numeric Range: High:** '100'
- Numeric Range: Low:** '0'
- Threshold Type:** '[Integer]'
- Threshold Unit:** (empty)
- Threshold Value:** '1'

There are 'Save' and 'Save As' buttons on the right side of the form. Below the form is a 'Threshold Object Registry' table with the following data:

	Name	Override	Type	Numeric Range High	Numeric Range Low	Threshold Unit	Threshold Value	ID	Date Edit
1.	Use Server Hostname for NAT	Enabled	Integer	1	0	\$	1	t_617	2018-04-18 17:07:16

- In the **Threshold Value** field, type "1". This signifies that NAT support is enabled.

NOTE: To disable NAT support, type "0" in this field. "0" and "1" are the only two values you can type in this field for the "Use Server Hostname for NAT" Threshold Object.

NOTE: This threshold is set on a per-device basis, and will affect all VOS performance Dynamic Applications aligned to a given device.

- Click **[Save]**.

Creating Cisco UC VOS Application Credentials

To configure SL1 to monitor VOS applications, you must use SL1 to create the credentials that enable SL1 to connect with the devices in those application clusters. You can create the following credential types to monitor VOS applications:

- SNMP
- SOAP/XML (PAWS API)
- SOAP/XML (non-PAWS API)
- Basic/Snippet

Creating an SNMP Credential

SL1 uses SNMP to collect information about the following devices that can be monitored using the Dynamic Applications in the *Cisco: UC VOS Applications PowerPack*:

- Cisco Contact Center Express (CCX)
- Cisco Unity Connection (CUC) servers
- Cisco Hosted Collaboration Mediation for Fulfillment (HCM-F)
- Cisco HCS Intelligent Loader
- Cisco IM & Presence (IM&P) servers (optional)
- Cisco Emergency Responder
- Cisco Prime Collaboration Deployment (PCD) servers (optional, but recommended)
- Cisco SocialMiner

To monitor these devices, you must first define one or more SNMP credentials that enable SL1 to communicate with the applications.

To configure an SNMP credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the **[Create]** button.

3. In the drop-down list that appears, select *SNMP Credential*. The **Credential Editor** page appears:

The screenshot shows a window titled "Credential Editor [22]". Inside, there's a sub-header "Edit SNMP Credential #22" with "New" and "Reset" buttons. The form is divided into three sections: "Basic Settings", "SNMP V1/V2 Settings", and "SNMP V3 Settings".

- Basic Settings:** Profile Name (text field: "SNMP Public V2"), SNMP Version (dropdown: "[SNMP V2]"), Port (text field: "161"), Timeout(ms) (text field: "1500"), Retries (text field: "1").
- SNMP V1/V2 Settings:** SNMP Community (Read-Only) (text field: "public"), SNMP Community (Read/Write) (text field).
- SNMP V3 Settings:** Security Name (text field), Security Passphrase (text field), Authentication Protocol (dropdown: "MD5"), Security Level (dropdown: "No Authentication / No Encryption"), SNMP v3 Engine ID (text field), Context Name (text field), Privacy Protocol (dropdown: "DES"), Privacy Protocol Pass Phrase (text field).

At the bottom are "Save" and "Save As" buttons.

4. In the **Profile Name** field, type a name for the credential.

TIP: If you are monitoring multiple VOS applications that have the same SNMP credential information, including community string, then you can create one common SNMP credential for those applications. Otherwise, each application should have its own unique SNMP credential. In that scenario, ScienceLogic recommends specifying the application type in the credential's **Profile Name** (e.g., "Cisco VOS SNMP - CCX").

5. In the **SNMP Version** field, select *SNMP V2*.
6. In the **SNMP Community (Read Only)** field, type the community string for the VOS application you want to monitor.
7. Supply values in the other fields on this page as needed. In most cases, you can accept the default values for the other fields.
8. Click the **[Save]** button.

Creating a SOAP/XML Credential (PAWS API)

SL1 uses SOAP API queries, Cisco Platform Administrative Web Service (PAWS) API queries, and requests to an HTML-based user interface to monitor the following Cisco VOS applications:

- Cisco Contact Center Express (CCX) (SOAP and PAWS)
- Cisco Unity Connection (CUC) servers (SOAP and PAWS)
- Cisco Hosted Collaboration Mediation for Fulfillment (HCM-F) (PAWS only)
- Cisco HCS Intelligent Loader (PAWS only)

- Cisco IM & Presence (IM&P) servers (SOAP and PAWS)
- Cisco Prime License Manager (PLM) (PAWS and HTML)
- Cisco Prime Collaboration Deployment (PCD) servers (SOAP and PAWS)
- Cisco SocialMiner (SOAP and PAWS)


As a result, several of the Dynamic Applications (including all performance Dynamic Applications) in the Cisco: UC VOS Applications PowerPack must be aligned with a SOAP/XML credential that includes the SOAP API and PAWS API login information.

If you are configuring a credential for a Cisco VOS application that does *not* use the PAWS API, see [Creating a SOAP/XML Credential \(non-PAWS API\)](#).

TIP: When possible, ScienceLogic recommends using the same login information with read access for all of the APIs required to monitor a particular application. Doing so enables you to create a single SOAP/XML credential for each application with only the "Basic Settings" configured.

The PowerPack includes an example SOAP/XML credential that you can edit for your own use.

To configure a SOAP/XML credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **Cisco VOS SOAP - Example** credential, and then click its wrench icon (). The **Edit SOAP/XML Credential** page appears.

3. Add values to the following fields:

Basic Settings

- **Profile Name.** Type a unique name for your VOS credential.

TIP: Each application should have its own unique SOAP/XML credential. ScienceLogic recommends specifying the application type in the credential's **Profile Name** (e.g., "Cisco VOS SOAP - IM&P").

- **Content Encoding.** Select *text/xml*.
- **Method.** Select POST.
- **HTTP Version.** Select HTTP/1.1.
- **URL.** Type "http://%D" .
- **HTTP Auth User.** If the SOAP API and PAWS API login information is identical, then type the common login username. Otherwise, type the SOAP API login username.
- **HTTP Auth Password.** If the SOAP API and PAWS API login information is identical, then type the common login password. Otherwise, type the SOAP API login password.
- **Timeout (seconds).** Type "10".

Proxy Settings

- **Hostname/IP.** Leave this field blank.

- **Port.** Type "0".
- **User.** Leave this field blank.

CURL Options

- **CURL Options.** Do not make any selections in this field.

SOAP Options

- **Embedded Password [%P].** If the SOAP API and PAWS API login information differ, then type the PAWS API login password. Otherwise, leave this field blank.
- **Embed Value [%1].** If the SOAP API and PAWS API login information differ, then type the PAWS API login username in this field. Otherwise, leave this field blank.
- **Embed Value [%2].** Leave this field blank.
- **Embed Value [%3].** Leave this field blank.
- **Embed Value [%4].** Leave this field blank.

HTTP Headers

- **HTTP Headers.** Do not make any selections in this field.

4. Click the [**Save As**] button.

Creating a SOAP/XML Credential (non-PAWS API)

If you do not have access to the Cisco Platform Administrative Web Service (PAWS) API, configure a SOAP/XML credential using the settings in this section.

SL1 uses SOAP API queries and requests to an HTML-based user interface to monitor the following VOS applications:

- Cisco Contact Center Express (CCX) (SOAP)
- Cisco Unity Connection (CUC) servers (SOAP)
- Cisco IM & Presence (IM&P) servers (SOAP)
- Cisco Prime License Manager (PLM) (HTML)
- Cisco Prime Collaboration Deployment (PCD) servers (SOAP)
- Cisco SocialMiner (SOAP)

As a result, several of the Dynamic Applications (including all performance Dynamic Applications) in the *Cisco: UC VOS Applications PowerPack* must be aligned with a SOAP/XML credential that includes the SOAP API login information.

TIP: When possible, ScienceLogic recommends using the same login information with read access for all of the APIs required to monitor a particular application. Doing so enables you to create a single SOAP/XML credential for each application with only the "Basic Settings" configured.

The PowerPack includes an example SOAP/XML credential that you can edit for your own use.

To configure a SOAP/XML credential for non-PAWS APIs:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **Cisco VOS SOAP - Example** credential, and then click its wrench icon (🔧). The **Edit SOAP/XML Credential** page appears.
3. Add values to the following fields:

Basic Settings

- **Profile Name.** Type a unique name for your VOS credential.

TIP: Each application should have its own unique SOAP/XML credential. ScienceLogic recommends specifying the application type in the credential's **Profile Name** (e.g., "Cisco VOS SOAP - IM&P").

- **Content Encoding.** Select *text/xml*.
- **Method.** Select POST.
- **HTTP Version.** Select HTTP/1.1.

- **URL**. Type "http://%D".
- **HTTP Auth User**. Type the SOAP API login username.
- **HTTP Auth Password**. Type the SOAP API login password.
- **Timeout (seconds)**. Type "10".

Proxy Settings

- **Hostname/IP**. Leave this field blank.
- **Port**. Type "0".
- **User**. Leave this field blank.

CURL Options

- **CURL Options**. Do not make any selections in this field.

SOAP Options

- **Embedded Password [%P]**. Leave this field blank.
- **Embed Value [%1]**. Type "SOAP" or "SNMP" as applicable. "SOAP" indicates that the PAWS service will not be queried during discovery, but SOAP will still be used for monitoring. "SNMP" indicates that neither the PAWS service nor the SOAP service will be queried during discovery. Otherwise, leave this field blank.
- **Embed Value [%2]**. If you typed "SOAP" or "SNMP" in **Embed Value [%1]**, then type the IP address or hostname list for the cluster nodes, with each address in the list separated by a comma. (The first address or hostname in the list is assumed to be primary.) Otherwise, leave this field blank.

NOTE: If you enter hostnames in this field, you must first [enable Network Address Translation \(NAT\) support for Cisco UC VOS devices](#).

NOTE: If you enter hostnames in this field that cannot be resolved to IP addresses, then you must create a Host File entry for each hostname included in the list. In a NAT environment, the Host File entry should contain an entry for the external IP addresses. For more information about Host Files, see the [System Administration](#) manual.

- **Embed Value [%3]**. If you typed "SOAP" or "SNMP" in **Embed Value [%1]**, then type the appropriate VOS application cluster type abbreviation as follows:
 - CUC
 - IM&P
 - CCX
 - PLM

- HCS Intelligent Loader
- HCM-F
- PCD
- SocialMiner

Otherwise, leave this field blank.

- **Embed Value [%4]**. Leave this field blank.

HTTP Headers

- **HTTP Headers**. Do not make any selections in this field.

4. Click the **[Save As]** button.

Creating a Basic/Snippet Credential


SL1 uses REST API queries to monitor the following VOS applications:

- Cisco Unity Connection (CUC) servers
- Cisco IM & Presence (IM&P) servers

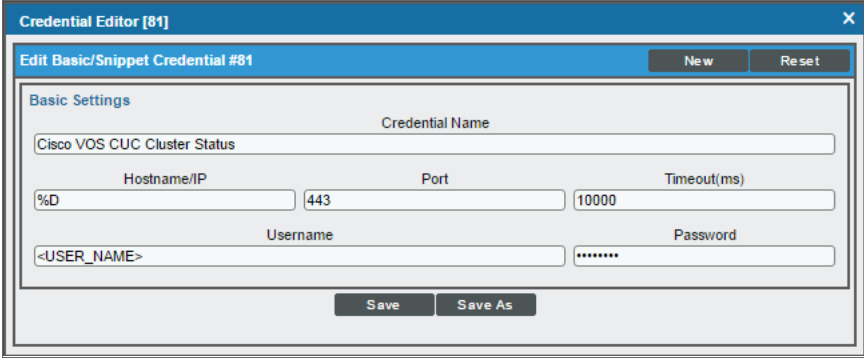
To monitor these devices, you must create one or more Basic/Snippet credentials that enable SL1 to log in to the REST API that reports the status of each VOS application's cluster. The *Cisco: UC VOS Applications PowerPack* includes two example Basic/Snippet credentials that you can edit for your own use.

NOTE: The steps below describe how to edit both example credentials, which you should do if the REST API login information is different for CUC and IM&P. However, if the REST API login information is the same for both applications, then a second Basic/Snippet credential is unnecessary.

To edit the example Basic/Snippet credentials:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **Cisco VOS CUC Cluster Status** example credential, then click its wrench icon (). The **Edit Basic/Snippet Credential** page appears.

- Update the following fields:



The screenshot shows a window titled "Credential Editor [81]" with a sub-header "Edit Basic/Snippet Credential #81". There are "New" and "Reset" buttons in the top right. The "Basic Settings" section contains the following fields:

- Credential Name:** Cisco VOS CUC Cluster Status
- Hostname/IP:** %D
- Port:** 443
- Timeout(ms):** 10000
- Username:** <USER_NAME>
- Password:** *****

At the bottom, there are "Save" and "Save As" buttons.

- **Credential Name.** Type a new name for the CUC cluster status credential.

TIP: If you are monitoring multiple VOS applications that have the same REST API login information, then you can create one common Basic/Snippet credential for those applications. Otherwise, each VOS application should have its own unique Basic/Snippet credential. In that scenario, ScienceLogic recommends specifying the application type in the credential's **Profile Name** (e.g., "Cisco VOS Basic/Snippet - CUC").

- **Hostname/IP.** Type "%D".
 - **Port.** Type "443".
 - **Timeout.** Type "10000".
 - **Username.** Type the login username for the CUC cluster status REST API.
 - **Password.** Type the password for the CUC cluster status REST API.
- Click the **[Save As]** button.
 - When the confirmation message appears, click **[OK]**.
 - To create a Basic/Snippet credential to monitor VOS IM&P, repeat steps 1-5 to edit the **Cisco VOS IM&P Cluster Status** example credential.

Testing the Cisco UC VOS Credential

SL1 includes a Credential Test for Cisco UC VOS. Credential Tests define a series of steps that SL1 can execute on demand to validate whether a credential works as expected.

The Cisco UC VOS Credential Test can be used to test a SOAP/XML credential for monitoring Cisco UC VOS using the Dynamic Applications in the *Cisco: UC VOS PowerPack*. The Cisco UC VOS Credential Test performs the following steps:

- **Test Reachability.** Performs an ICMP ping request to see if the device is reachable.
- **Test Name Resolution.** Checks to see if nslookup can resolve the IP address or hostname.
- **Test Port Availability.** Performs an NMAP request to see if the appropriate port is open.
- **Test Credential Validity.** Checks to see if the Cisco VOS credential is configured properly.
- **Test PAWS and non-PAWS Monitoring Credential.** Checks to see if a SOAP/XML credential can request a monitored resource.

To test the Cisco UC VOS credential:

1. Go to the **Credential Test Management** page (System > Customize > Credential Tests).
2. Locate the **Cisco UC VOS Credential Test** and click its lightning bolt icon (⚡). The **Credential Tester** modal page appears:

3. Supply values in the following fields:
 - **Test Type.** This field is pre-populated with the credential test you selected.
 - **Credential.** Select the credential to test. This drop-down list includes only credentials that you have access to that can be tested using the selected credential test.
 - **Hostname/IP.** Enter the IP address or hostname for the device.

NOTE: The credential being tested cannot include more than 32 characters in the **Hostname/IP** field.

- **Collector.** Select the All-In-One Appliance or Data Collector that will run the test.

4. Click the **[Run Test]** button to run the credential test. The **Test Credential** window appears:

ScienceLogic, Inc. - Google Chrome
 Not secure | 10.2.10.63/em7/index.em7?exec-credential_test_log

Test Credential | Test execution complete

Step	Description	Log Message	Status
1 Test Reachability	Check to see if the device is reachable using ICMP.	The device is reachable using ICMP. The average response time is 0.401ms	Passed
2 Test Name Resolution	Check to see if nslookup can resolve the IP and hostname.	Name resolution succeeded: Reverse returned 1 result, Forward returned 1 result	Passed
3 Test Port Availability	Check to see if the port 8443 is open on the device.	Port 8443 is open	Passed
4 Test Credential Configuration Validity	Check to see if the Cisco VOS credential is configured properly.	Cisco VOS credential configuration succeeded	Passed
5 Test PAWS API request availability	Check to see if the SOAP/XML (PAWS API) credential can be used for requesting to the device.	Cisco VOS resource PAWS request succeeded	Passed
6 Test non-PAWS API request availability	Check to see if a SOAP/XML (non-PAWS API) credential can be used for requesting to the device.	Cisco VOS resource non-PAWS request succeeded	Passed

Execute Discovery Session

The **Test Credential** window displays a log entry for each step in the credential test. The steps performed are different for each credential test. The log entry for each step includes the following information:

- **Step**. The name of the step.
- **Description**. A description of the action performed during the step.
- **Log Message**. The result of the step for this credential test.
- **Status**. Whether the result of this step indicates the credential or the network environment is configured correctly (Passed) or incorrectly (Failed).
- **Step Tip**. Mouse over the question mark icon (?) to display the tip text. The tip text recommends what to do to change the credential or the network environment if the step has a status of "Failed".



Chapter

3

Discovery

Overview

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ().
- To view a page containing all the menu options, click the Advanced menu icon (.

The following sections describe the steps required to discover Cisco UC VOS devices in SL1:

Discovering VOS Application Clusters	27
Viewing VOS Devices	29

Discovering VOS Application Clusters

To model and monitor your VOS applications, run a discovery session to discover the VOS application clusters that SL1 will use as the root devices for monitoring the applications.

Several minutes after the discovery session has completed, the Dynamic Applications in the *Cisco: UC VOS Applications* PowerPack should automatically align to the cluster root devices and then discover, model, and monitor the remaining VOS application component devices.

NOTE: Cisco Prime Collaboration Deployment (PCD) and Cisco SocialMiner do not support cluster deployment. However, to create component-level devices that can be monitored using the Dynamic Applications in the *Cisco: UC VOS Applications PowerPack*, the SL1 system creates a virtual PCD cluster device or a virtual SocialMiner cluster in addition to the PCD or SocialMiner component-level devices during discovery.

To discover the VOS application clusters that you want to monitor, perform the following steps:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. In the **Discovery Control Panel**, click the **[Create]** button.
3. The **Discovery Session Editor** page appears. In the **Discovery Session Editor** page, define values in the following fields:



The screenshot shows the 'Discovery Session Editor | Editing Session [7]' interface. It is divided into several sections:

- Identification Information:** Name: 'Cisco UK Lab soap rest', Description: (empty).
- IP and Credentials:**
 - IP Address/Hostname Discovery List:** 172.16.244.26, 172.16.244.27, 172.16.244.23, 172.16.244.24
 - SNMP Credentials:** Cisco SNMPv2 - Example, Cisco SNMPv3 - Example, EM7 Default V2, EM7 Default V3, IPSLA Example, LifeSize: Endpoint SNMP, Nexus snmp, SNMP Public V1, [SNMP Public V2]
 - Other Credentials:** QA-Silo AD, PowerShell, Lync 2010 Credentials - Example, Windows PowerShell - Example, SOAP/XML Host, Amazon Web Services Credential, Azure Credential - SOAP/XML, [Cisco UK lab SOAP]
- 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
 - 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: 5
 - Collection Server: [mg_iso_cu]
 - Organization: [System]
 - Add Devices to Device Group(s): Please create a device group first
 - Apply Device Template: [Choose a Template]

Buttons at the bottom: Save, Save As, Log All (checked).

- **IP Address/Hostname Discovery List.** Enter the IP address(es) and/or hostname(s) for all the nodes in the cluster you want to discover.


NOTE: All VOS devices on a single ScienceLogic collector must have unique host names.

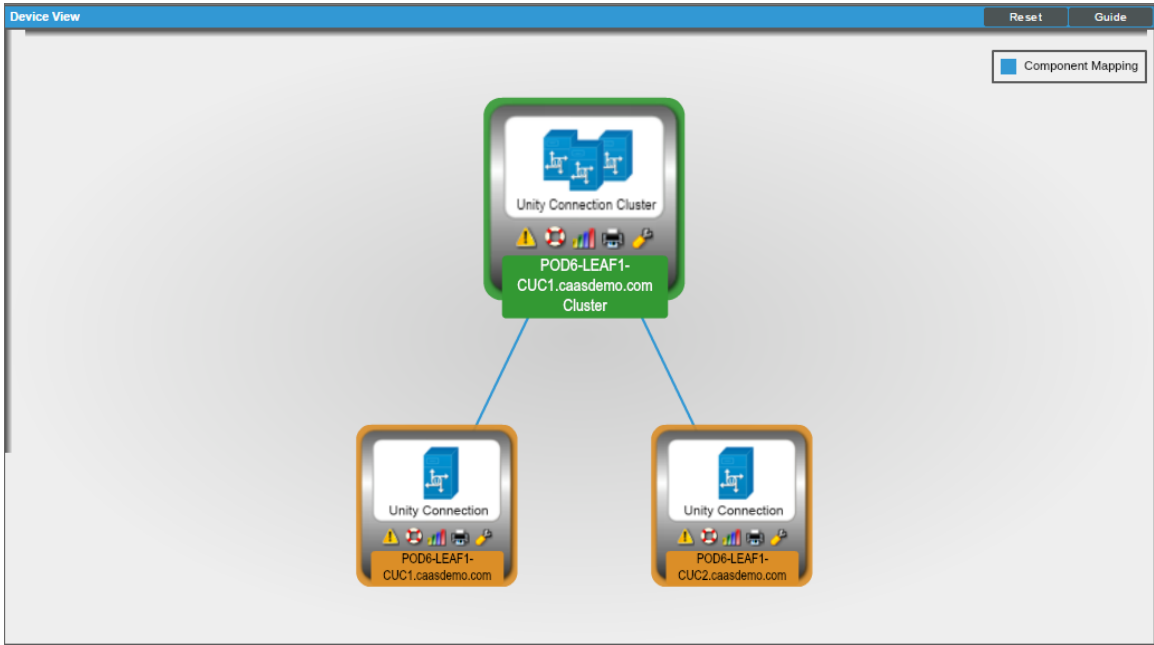
- **SNMP Credentials.** Select the SNMP credential you created for the device clusters.
 - **Other Credentials.** Select the Basic/Snippet and SOAP/XML credentials you created for the device clusters.
 - **Discover Non-SNMP.** Select this checkbox.
 - **Model Devices.** Select this checkbox.
4. Optionally, you can enter values in the other fields on this page. For more information about the other fields on this page, see the **Discovery & Credentials** manual.
 5. Click the **[Save]** button to save the discovery session and then close the **Discovery Session Editor** window.
 6. The discovery session you created appears at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon () to run the discovery session.
 7. The **Discovery Session** window appears. When the cluster root device(s) are discovered, click the device icon () to view the **Device Properties** page for each device.

Viewing VOS Devices

When SL1 discovers your VOS devices, SL1 will create component devices that represent each component in your VOS device clusters.

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

- The **Device View** 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 reloads the page with the selected device as the primary device:



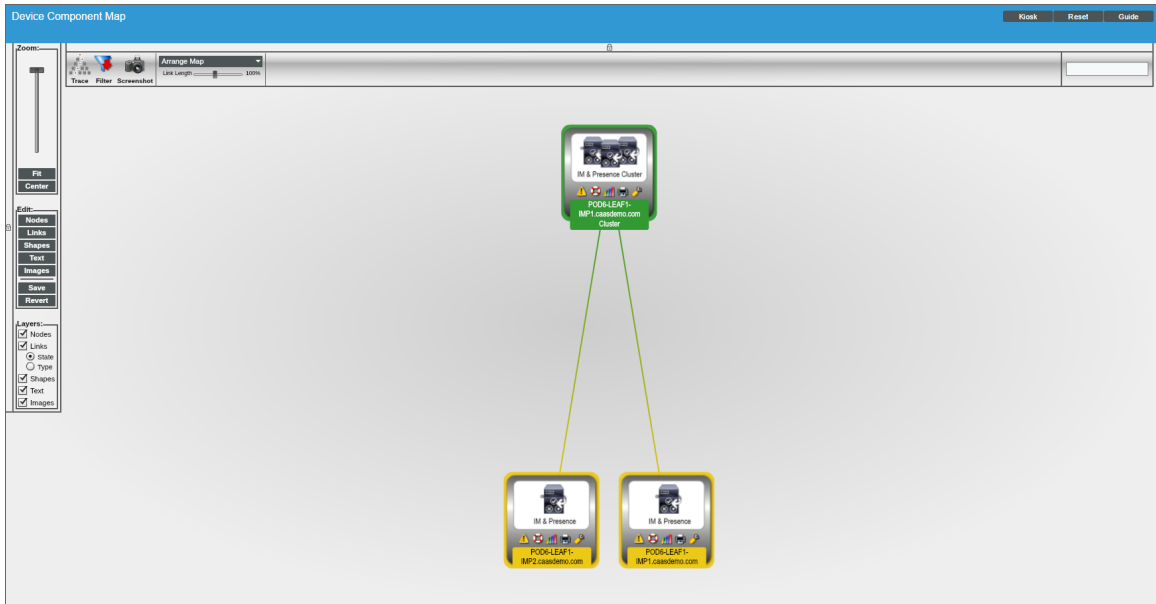
- The **Device Components** page (Registry > Devices > Device Components) displays a list of all root devices and component devices discovered by SL1, in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with your VOS device clusters, find a device cluster and click its plus icon (+):

Device Components | Devices Found [2]

	Device Name	IP Address	Device Category	Device Class Sub-class	IID	Organization	Current State	Collection Group	Collection State	
1	POD6-LEAF1-CUC1.caasdemo.com Cluster	--	Cluster	Cisco Systems Unity Connection Cluster	126	System	Healthy	CUG1	Active	
	POD6-LEAF1-CUC1.caasdemo.com	172.16.244.27	Device	Cisco Systems Unity Connection Server	124	System	Major	CUG1	Active	
	POD6-LEAF1-CUC2.caasdemo.com	172.16.244.27	Device	Cisco Systems Unity Connection Server	123	System	Major	CUG1	Active	
2	POD6-LEAF1-IMP1.caasdemo.com Cluster	--	Cluster	Cisco Systems IM and Presence Cluster	127	System	Healthy	CUG1	Active	
	POD6-LEAF1-IMP1.caasdemo.com	172.16.244.23	Device	Cisco Systems IM and Presence Server	125	System	Minor	CUG1	Active	
	POD6-LEAF1-IMP2.caasdemo.com	172.16.244.24	Device	Cisco Systems IM and Presence Server	122	System	Minor	CUG1	Active	

[Select Action] Go

- 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. The platform also updates each map with the latest status and event information. To view the map for your VOS device clusters, go to the **Component Map** page and select a map from the list in the left NavBar. To learn more about the **Component Map** page, see the **Views** manual.



© 2003 - 2021, 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



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

International: +1-703-354-1010