# Monitoring Cisco: Meeting Server

Cisco: Meeting Server PowerPack version 101

# Table of Contents

# Chapter 1

# Introduction

## Overview

This manual describes how to monitor Cisco Meeting Server devices in SL1 using the *Cisco: Meeting Server* PowerPack.

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



**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 Meeting Server?

Cisco Meeting Server is a conferencing solution that allows collaboration through secure video, audio, and web communication. Cisco Meeting Server integrates with a variety of third-party platforms across both cloud and hybrid environments.

# What Does the Cisco: Meeting Server PowerPack Monitor?

To monitor Cisco Meeting Server devices using SL1SL1, you must install the *Cisco: Meeting Server* PowerPack. This PowerPack enables you to discover, model, and collect data about Meeting Server devices.

The *Cisco: Meeting Server* PowerPack includes:

- Dynamic Applications that discover, model, and monitor performance metrics and collect configuration data for Cisco Meeting Server devices
- A Device Class for Cisco Meeting Server applications and devices SL1SL1 monitors
- Event Policies and corresponding alerts that are triggered when Meeting Server devices meet certain status criteria

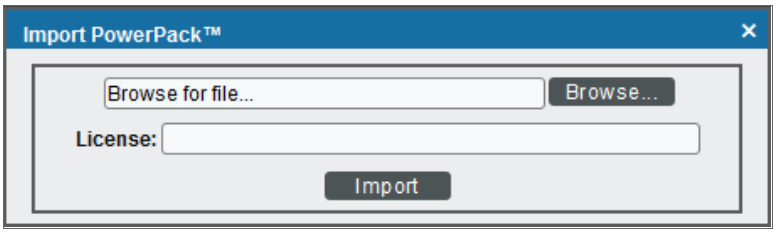
# Installing the Cisco: Meeting Server PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *Cisco: Meeting Server* 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 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 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 Discovery

## Overview

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



## Prerequisites for Monitoring Cisco Meeting Server

To monitor the Cisco Meeting Server, you must be able to access both the Cisco Meeting Server Mainboard Management Processor (MMP) and the Cisco Meeting Server API. Accessing the MMP requires an account with admin access. If you wish to create an a new user with admin access, refer to the section "MMP User Account Commands" in the Cisco Meeting Server MMP Command Line Reference document.

You access the Cisco Meeting Server MMP through SSH, while you access the Cisco Meeting Server API through HTTPS.

- If you can reach both of these through the same IP address, you can typically use a ***single Basic/Snippet credential***.

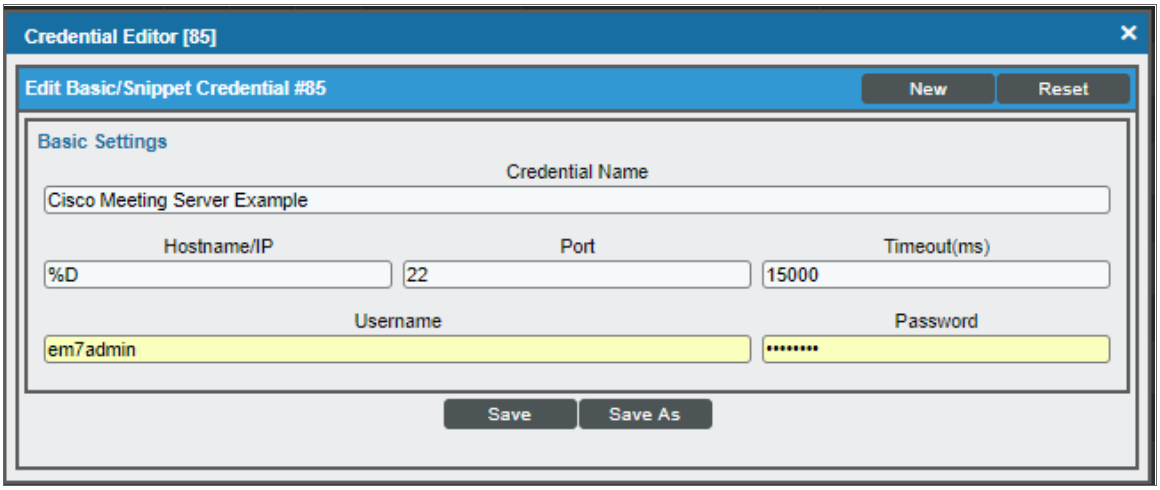
- If the two interfaces have separate IP addresses, or if the API is listening on a port other than 443, you must *create two separate credentials*. In addition, you should include an SNMP credential as part of discovery to correctly classify the device .

# Creating Credentials for Cisco Meeting Server Systems Using a Single IP Address

To monitor Cisco Meeting Server in SL1 in an environment where you can access the Cisco Meeting Server MMP and the Cisco Meeting Server API through the same IP address, you must configure a Basic/Snippet credential and a standard SNMP credential that SL1 can use to discover and communicate with Cisco Meeting Server devices.

To configure the Basic/Snippet credential for Cisco: Meeting Server:

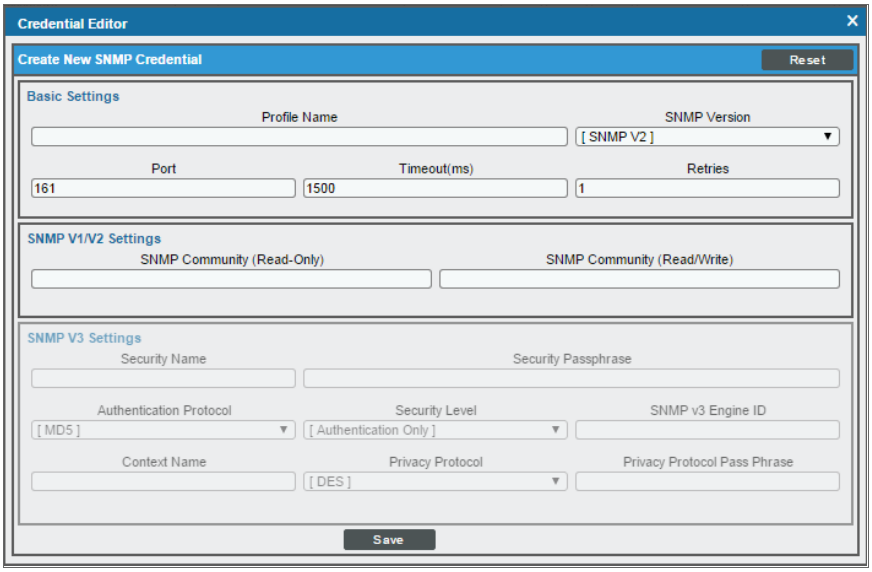
1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **Cisco Meeting Server Example** credential, and then click its wrench icon ( ). The **Edit Basic/Snippet Credential** modal page appears:




3. Supply values in the following fields:
   - ***Credential Name***. Type a new name for the credential.
   - ***Hostname/IP***. Type "%D".
   - ***Port***. Type "22".
   - ***Timeout(ms)***. Type "15000".
   - ***Username***. Type the username for the Cisco Meeting Server account with admin access.
   - ***Password***. Type the password associated with the admin account.
4. Click the **[Save As]** button.

To configure the SNMP credential for Cisco: Meeting Server:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the **[Actions]** button and select *Create SNMP Credential*. The **Credential Editor** page appears.




3. Supply values in the following fields:
   - ***Profile Name***. Name of the credential. Can be any combination of alphanumeric characters. This field is required.
   - ***SNMP Version***. SNMP version. Choices are *SNMP V1*, *SNMP V2*, and *SNMP V3*. The default value is *SNMP V2*. This field is required.
   - ***Port***. The port SL1 will use to communicate with the external device or application. The default value is *161*. This field is required.
   - ***Timeout (ms)***. Time, in milliseconds, after which SL1 will stop trying to communicate with the SNMP device. The default value is *1500*. This field is required.
   - ***Retries***. Number of times SL1 will try to authenticate and communicate with the external device. The default value is *1*. This field is required.
4. Click the **[Save]** button to save the new SNMP credential.

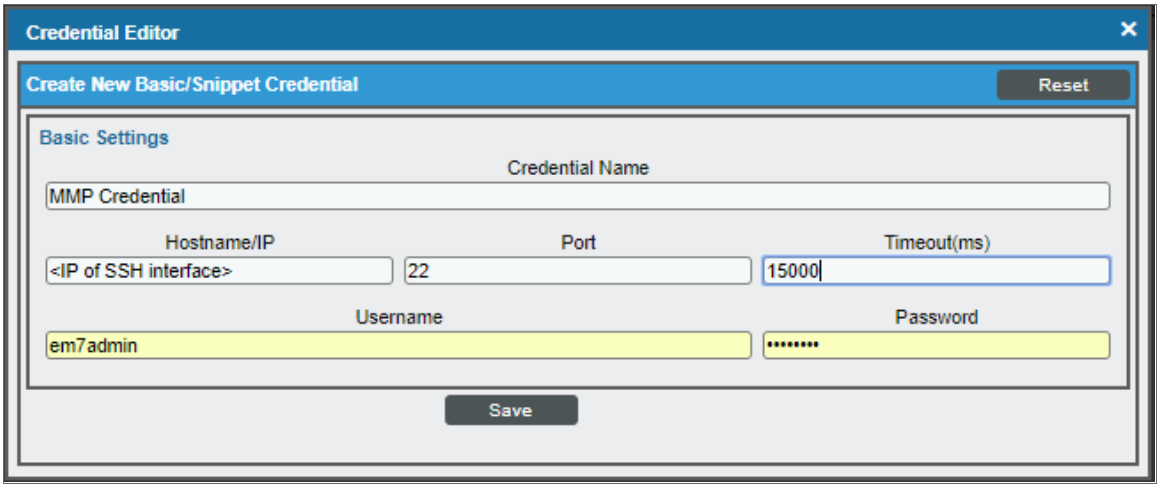
# Creating Credentials for Cisco Meeting Server Systems Using More than One IP Address

To monitor Cisco Meeting Server in SL1 in an environment where you access the Cisco Meeting Server MMP and the Cisco Meeting Server API through multiple IP addresses, you must configure a Basic/Snippet credential **for each interface** and a standard SNMP credential that SL1 can use to discover and communicate with Cisco Meeting Server devices.

You will need to manually align the associated Dynamic Applications with the corresponding Basic/Snippet credentials after discovery is complete.

To configure the Basic/Snippet credential for the system's Mainboard Management Processor (MMP)/SSH interface:

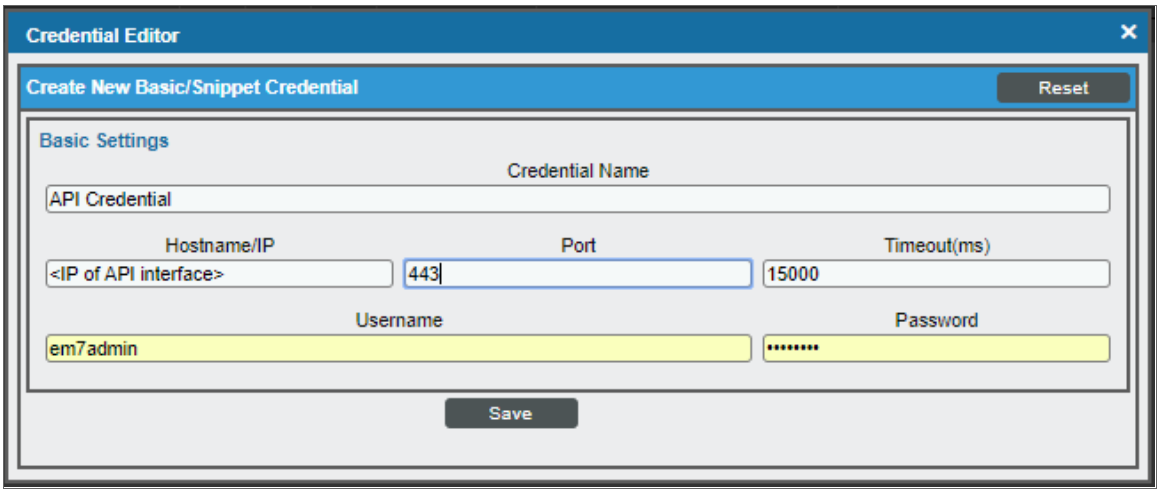
1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the **[Actions]** button and select *Create Basic/Snippet Credential*. The **Credential Editor** page appears:




3. Supply values in the following fields:
   - ***Credential Name***. Type a new name for the credential.
   - ***Hostname/IP***. Type the IP address of the SSH interface.
   - ***Port***. Type "22". This is the default value, but you can adjust it depending on your environment.
   - ***Timeout(ms)***. Type "15000". You can adjust this value depending on your environment.
   - ***Username***. Type the username for the Cisco Meeting Server account with admin access.
   - ***Password***. Type the password associated with the above account.
4. Click the **[Save As]** button.

To configure the Basic/Snippet credential for the API interface:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the **[Actions]** button and select *Create Basic/Snippet Credential*. The **Credential Editor** page appears:

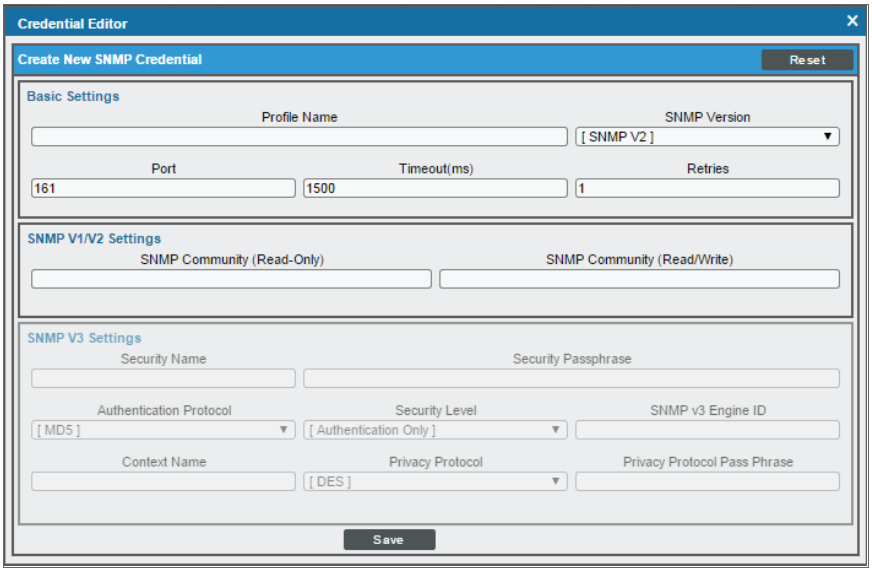



3. Supply values in the following fields:
   - ***Credential Name***. Type a new name for the credential.
   - ***Hostname/IP***. Type the IP address of the API interface.
   - ***Port***. Type "443".
   - ***Timeout(ms)***. Type "15000". This value can be adjusted depending on your environment.
   - ***Username***. Type the username for the Cisco Meeting Server account with admin access or the account with api access.
   - ***Password***. Type the password associated with the above account.
4. Click the **[Save As]** button.

To configure the SNMP credential for Cisco: Meeting Server:

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

2. Click the **[Actions]** button and select *Create SNMP Credential*. The **Credential Editor** page appears:




3. Supply values in the following fields:
   - ***Profile Name***. Name of the credential. Can be any combination of alphanumeric characters. This field is required.
   - ***SNMP Version***. SNMP version. Choices are *SNMP V1*, *SNMP V2*, and *SNMP V3*. The default value is *SNMP V2*. This field is required.
   - ***Port***. The port SL1 will use to communicate with the external device or application. The default value is *161*. This field is required.
   - ***Timeout (ms)***. Time, in milliseconds, after which SL1 will stop trying to communicate with the SNMP device. The default value is *1500*. This field is required.
   - ***Retries***. Number of times SL1 will try to authenticate and communicate with the external device. The default value is *1*. This field is required.
4. Click the **[Save]** button to save the new SNMP credential.

# Discovering Cisco Meeting Server Component Devices

The following sections describe how to discover Cisco Meeting Server devices. Discovery methods are described for devices that use a single IP address as well as those that use multiple IP addresses.

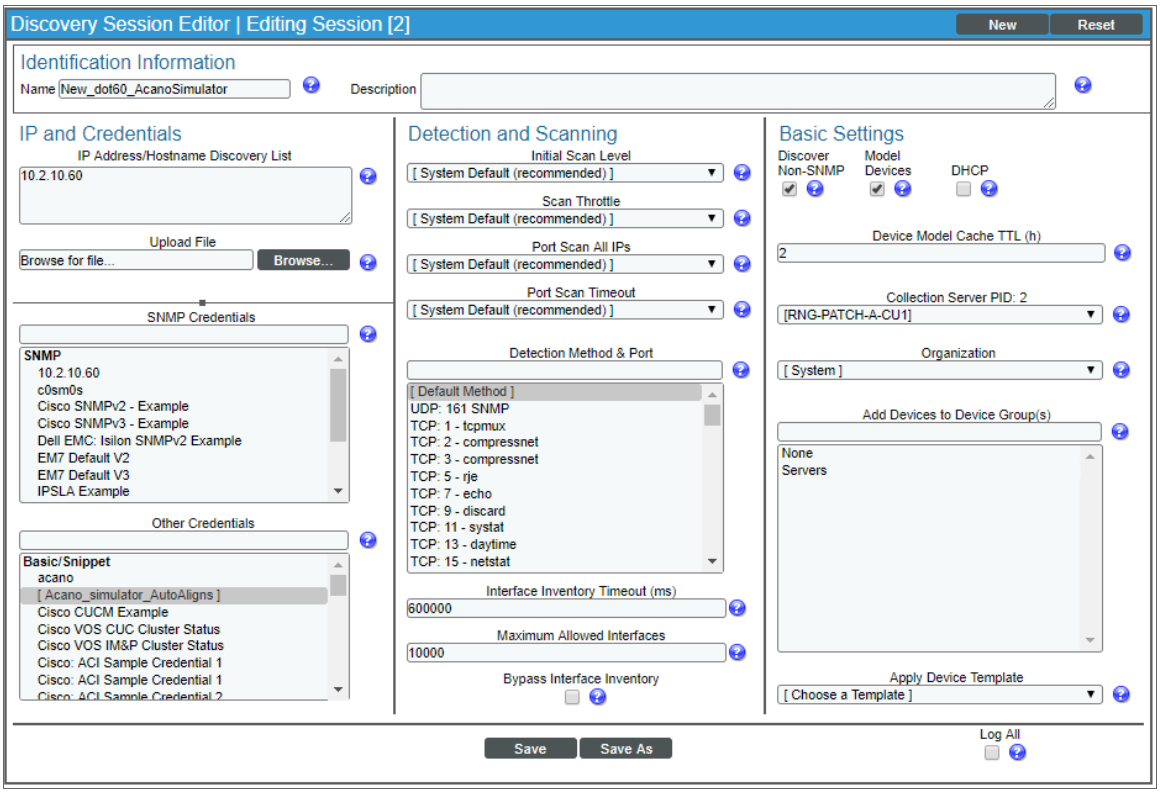
## Discovering Cisco Meeting Server Devices That Use a Single IP Address

To model and monitor your Cisco Meeting Server devices, you must run a discovery session to discover the Cisco Meeting Server component devices that SL1 will use as the root devices for monitoring the applications.

After the discovery session completes, the Dynamic Applications in the *Cisco: Meeting Server* PowerPack automatically align to the component device, and then the PowerPack discovers, models, and monitors the remaining Cisco Meeting Server devices.

To discover the devices that you want to monitor:

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




- ***IP Address/Hostname Discovery List***. Type the IP address or hostname for the set of Cisco Meeting Server devices that you want to monitor.
- ***SNMP Credentials***. Select the SNMP credential you created.
- ***Other Credentials***. Select the Basic/Snippet credential you created.
- ***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, 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. After the Cisco Meeting Server devices are discovered, click the device icon ( ) to view the **Device Properties** page for each device.

## Discovering Cisco Meeting Server Devices That Use Multiple IP Addresses

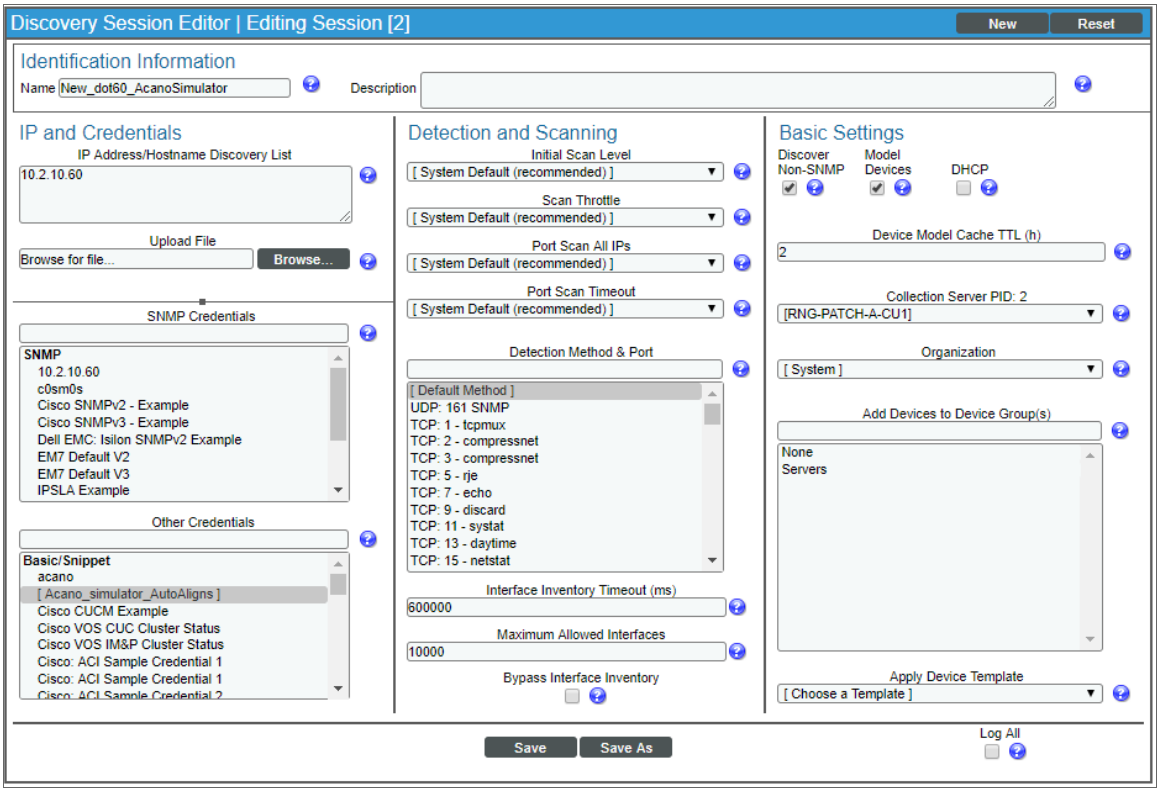
To model and monitor your Cisco Meeting Server devices, you must run a discovery session to discover the Cisco Meeting Server component devices that SL1 will use as the root devices for monitoring the applications.

In in an environment where you access the Cisco Meeting Server MMP and the Cisco Meeting Server API through multiple IP addresses, after the discovery session completes, you must manually align the Dynamic Applications associated with each Basic/Snippet credential you created.

To discover the devices that you want to monitor:

1. Go to the **Discovery Control Panel** page (System > Manage > Discovery).
2. On the **Discovery Control Panel**, click the **[Create]** button.

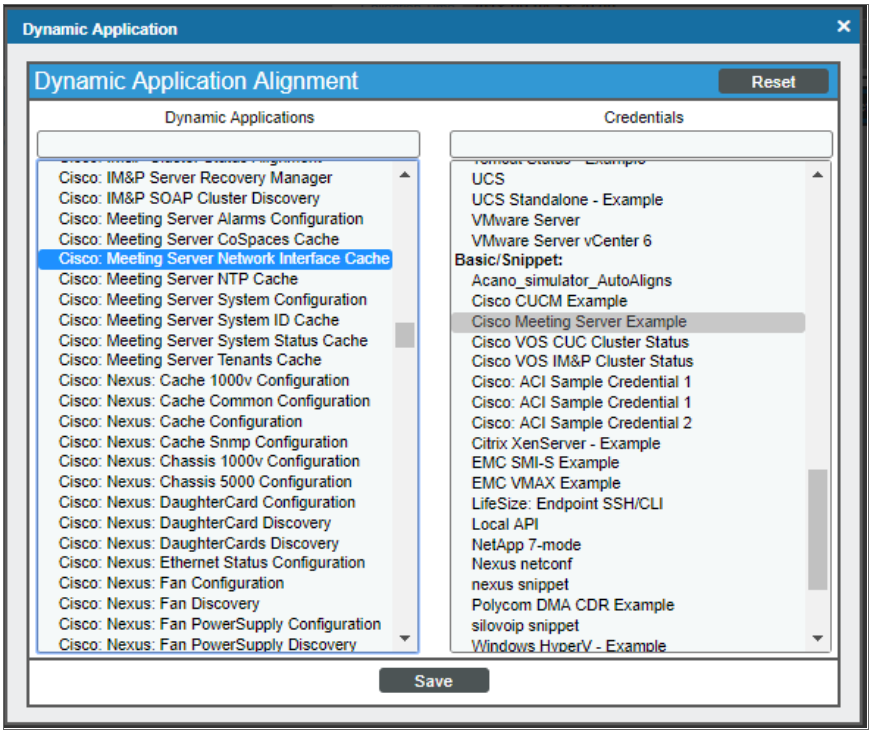
3. The **Discovery Session Editor** page appears. On the **Discovery Session Editor** page, define values in the following fields:




- ***IP Address/Hostname Discovery List***. Type the IP address or hostname for the set of Cisco Meeting Server devices that you want to monitor.
- ***SNMP Credentials***. Select the SNMP credential you created.
- ***Other Credentials***. Select the Basic/Snippet credential you created.
- ***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, 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. After the Cisco Meeting Server devices are discovered, click the device icon ( ) to view the **Device Properties** page for each device.
8. In the **Device Properties** page, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.

9. Click **[Action]** and then select *Add Dynamic Application* from the menu. The **Dynamic Application Alignment** page appears:




10. In the ***Dynamic Applications*** field, select the following Dynamic Applications:
    - Cisco: Meeting Server Network Interface Cache
    - Cisco: Meeting Server NTP Cache
    - Cisco: Meeting Server System ID Cache
11. In the ***Credentials*** field, select the Basic/Snippet credential you configured for the MMP/SSH.
12. Click **[Save]**.
13. Click **[Action]** and then select *Add Dynamic Application* from the menu. The **Dynamic Application Alignment** page appears.
14. In the ***Dynamic Applications*** field, select the following Dynamic Applications:
    - Cisco: Meeting Server Alarms Configuration
    - Cisco: Meeting Server CoSpaces Cache
    - Cisco: Meeting Server System Status Cache
    - Cisco: Meeting Server Tenants Cache
15. In the ***Credentials*** field, select the Basic/Snippet credential you configured for the API interface.
16. Click **[Save]**.

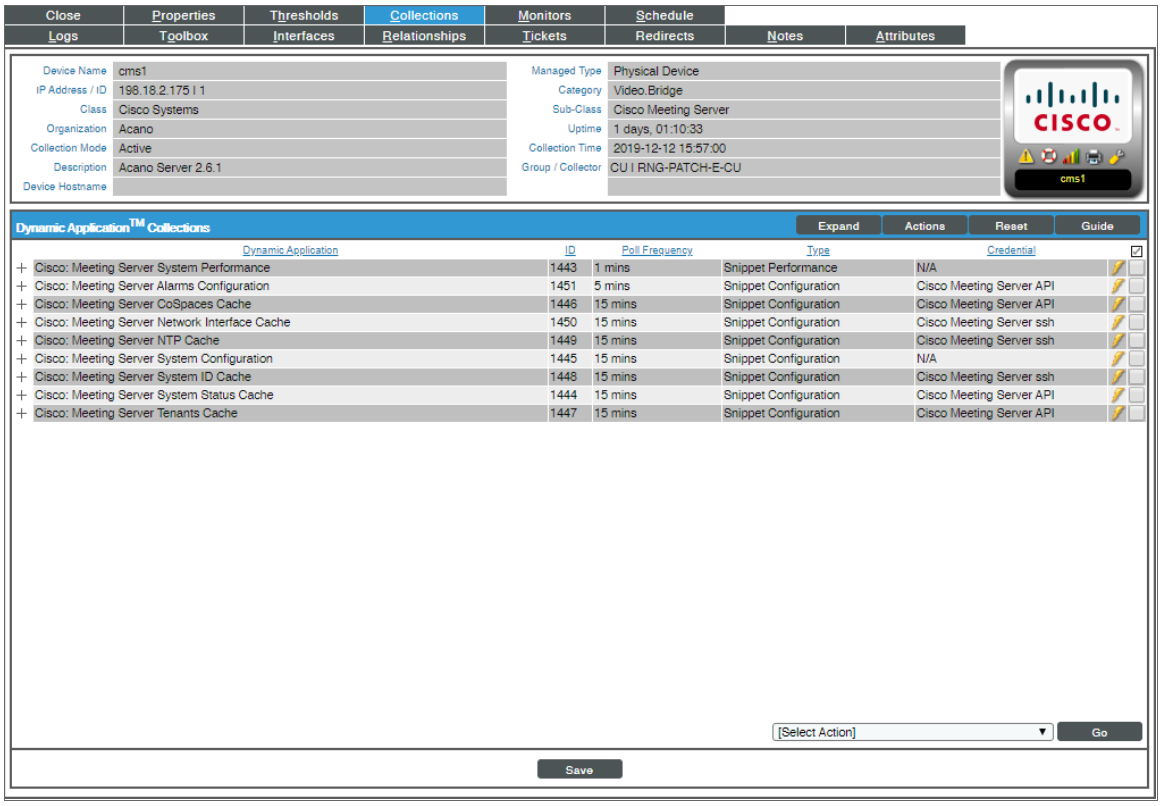
17. Click **[Action]** and then select *Add Dynamic Application* from the menu. The **Dynamic Application Alignment** page appears.
18. In the ***Dynamic Applications*** field, select the following Dynamic Applications:
    - Cisco: Meeting Server System Configuration
    - Cisco: Meeting Server System Performance
19. These applications do not require an associated credential.
20. Click **[Save]**. A few minutes after aligning the Dynamic Applications, SL1 will discover and model your Cisco Meeting Server and automatically align other Dynamic Applications to the devices in the system.

# Verifying Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery *using a single IP address*:

1. After discovery has completed, click the device icon for the Cisco Meeting Server (  ). From the **Device Properties** page for the Cisco Meeting Server, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. All applicable Dynamic Applications for the switch are automatically aligned during discovery.

> **NOTE:** It can take several minutes after the discovery session has completed for Dynamic Applications to appear in the **Dynamic Application Collections** page.



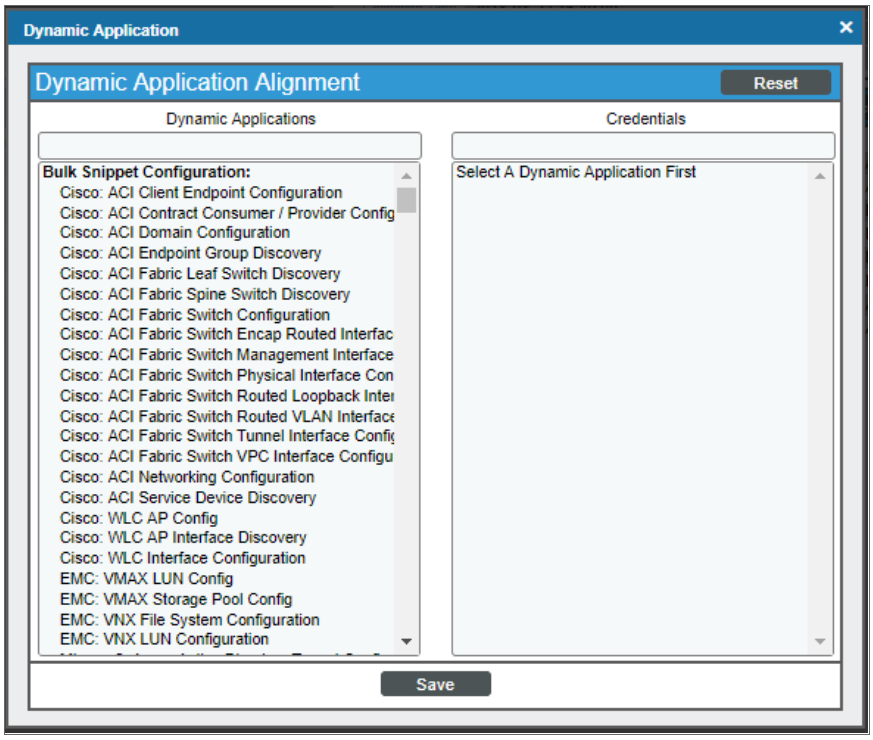

You should see the following Dynamic Applications aligned to the Cisco Meeting Server:

- Cisco: Meeting Server Network Interface Cache
- Cisco: Meeting Server NTP Cache
- Cisco: Meeting Server System ID Cache
- Cisco: Meeting Server Alarms Configuration
- Cisco: Meeting Server CoSpaces Cache
- Cisco: Meeting Server System Status Cache
- Cisco: Meeting Server Tenants Cache
- Cisco: Meeting Server System Configuration
- Cisco: Meeting Server System Performance

If the listed Dynamic Applications have not been automatically aligned during discovery, you can align them manually.

To manually align Dynamic Applications:

1. Click the **[Action]** button and then select *Add Dynamic Application*. The **Dynamic Application Alignment** page appears:




2. In the ***Dynamic Applications*** field, select the Dynamic Application you want to align.
3. In the ***Credentials*** field, select the appropriate credential.
4. Click the **[Save]** button.
5. Repeat steps 1-4 for the other unaligned Dynamic Applications.

## 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