Monitoring Cisco: Meeting Server

Cisco: Meeting Server PowerPack version 100

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:

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 SL1the ScienceLogic platform, 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 SL1 the ScienceLogic platform monitors
- Event Policies and corresponding alerts that are triggered when Meeting Server devices meet certain status criteria

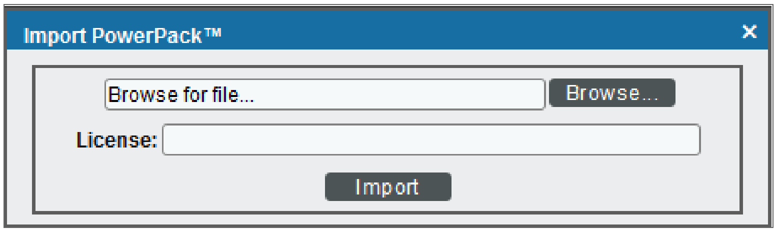
Installing the Cisco: Meeting Server PowerPack

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 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.)

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 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

Configuring Cisco: Meeting Server Monitoring

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***.

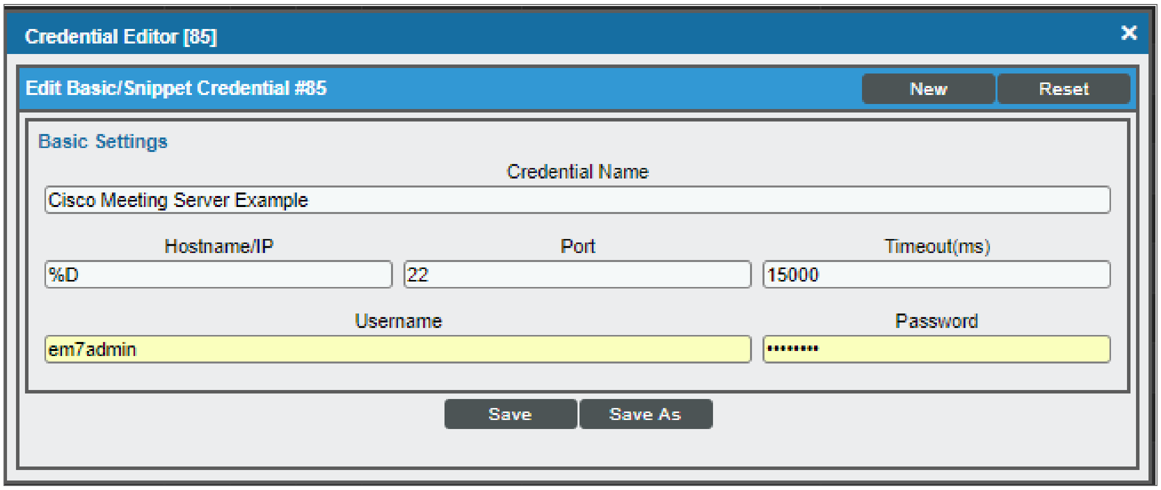
- If the two interfaces have separate IP addresses, or if the API is listening on a port other than 443, you must *create two separate credentials*. In addition, you should include an SNMP credential as part of discovery to correctly classify the device .

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:


Credential Editor [85]

Edit Basic/Snippet Credential #85

Basic Settings

Credential Name: Cisco Meeting Server Example

Hostname/IP: %D

Port: 22

Timeout(ms): 15000

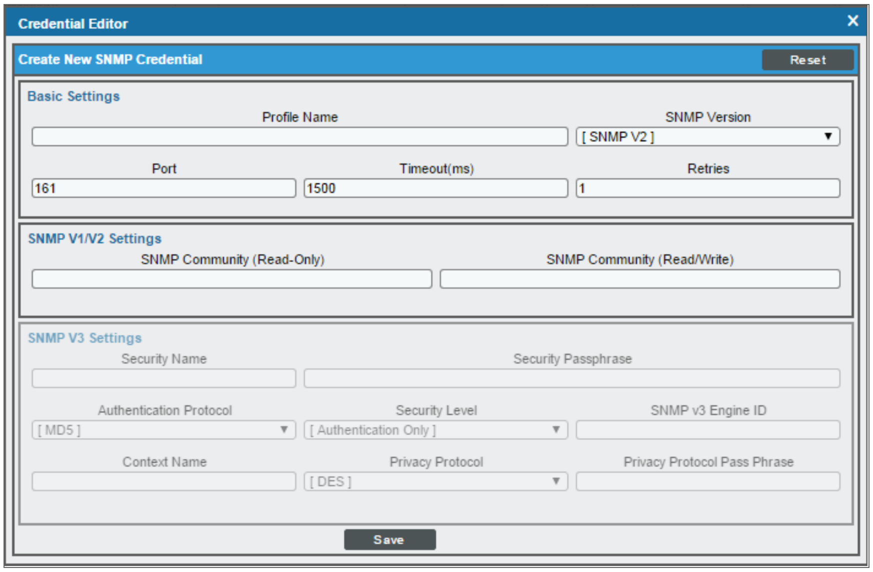
Username: em7admin

Password: ••••••••

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.



Basic Settings

Profile Name:

SNMP Version: [SNMP V2]

Port: 161

Timeout(ms): 1500

Retries: 1

SNMP V1/V2 Settings

SNMP Community (Read-Only):

SNMP Community (Read/Write):

SNMP V3 Settings

Security Name:

Security Passphrase:

Authentication Protocol: [MD5]

Security Level: [Authentication Only]

SNMP v3 Engine ID:

Context Name:

Privacy Protocol: [DES]

Privacy Protocol Pass Phrase:

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.

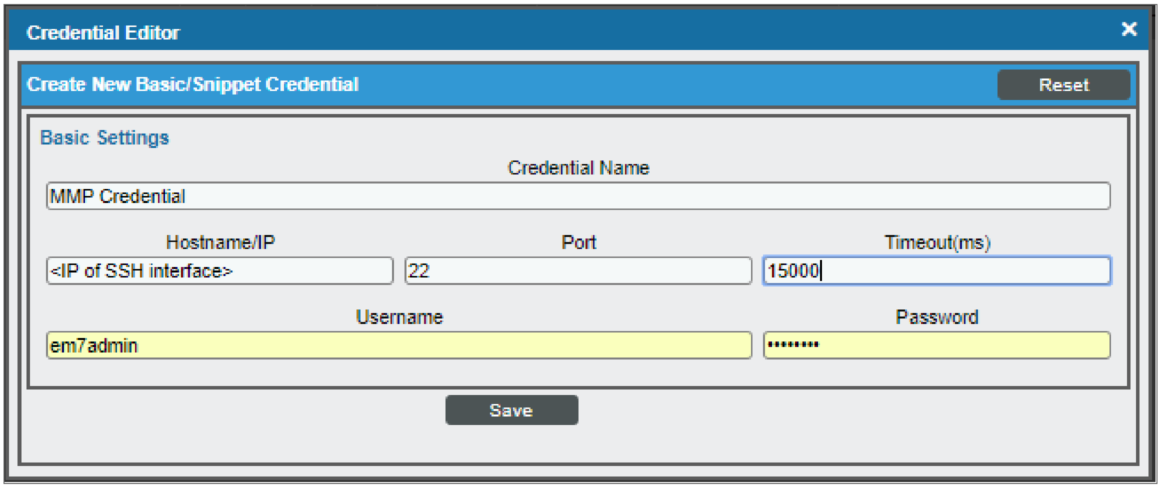
Creating Credentials for Cisco Meeting Server Systems Using More than One IP Address

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:



Credential Editor

Create New Basic/Snippet Credential

Basic Settings

Credential Name: MMP Credential

Hostname/IP: <IP of SSH interface>

Port: 22

Timeout(ms): 15000

Username: em7admin

Password: ••••••••

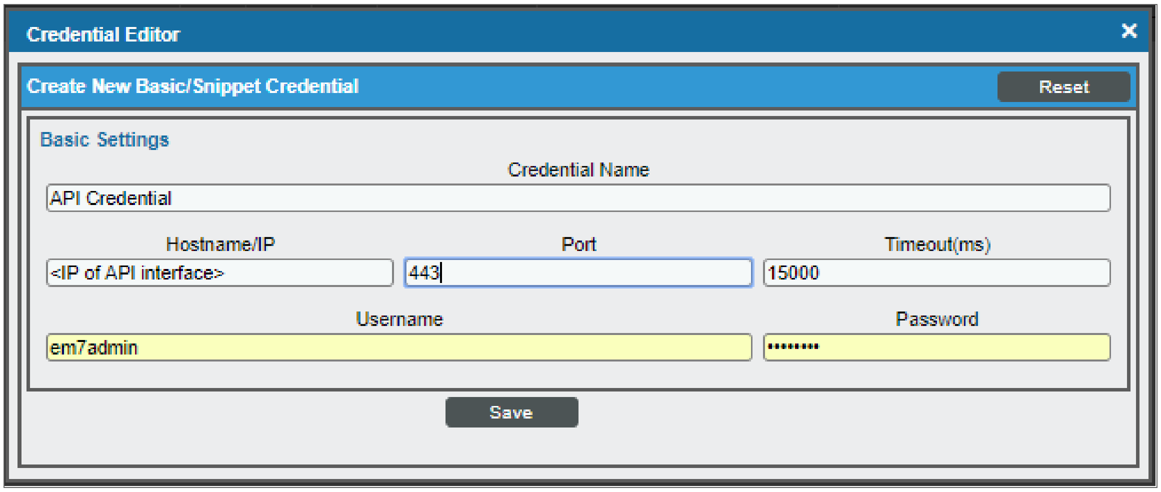
3. Supply values in the following fields:

   - ***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:



Credential Name: API Credential

Hostname/IP: <IP of API interface>

Port: 443

Timeout(ms): 15000

Username: em7admin

Password: ••••••••

3. Supply values in the following fields:

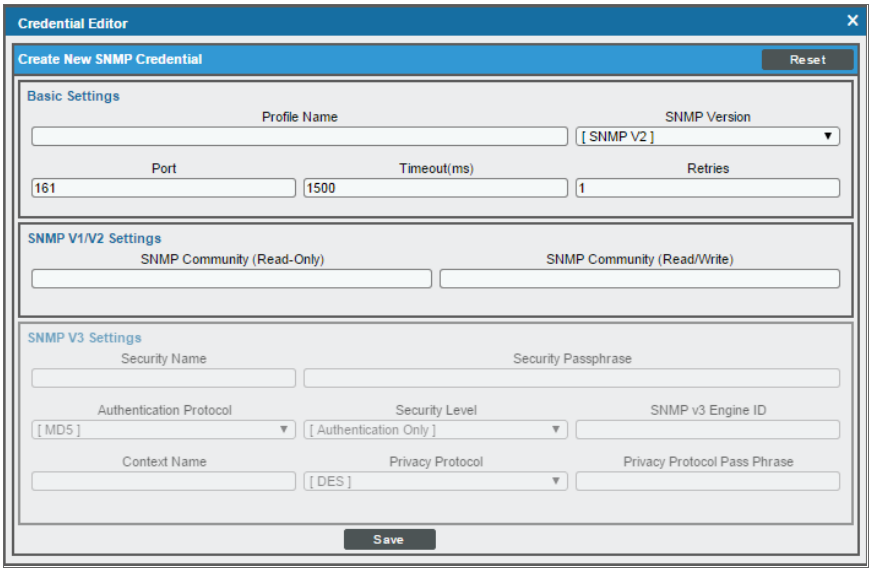
   - ***Credential Name***. Type a new name for the credential.
   - ***Hostname/IP***. Type the IP address of the API interface. If you are using a non-standard port, included the port number in the IP address. For example, 1.2.3.4:567.
   - ***Port***. Type "443". If you are using a non-standard port, include the port in the ***Hostname*** value, as specified above.
   - ***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:



SNMP Version: [SNMP V2]

Port: 161

Timeout(ms): 1500

Retries: 1

Authentication Protocol: [MD5]

Security Level: [Authentication Only]

Privacy Protocol: [DES]

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 the platform 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 the platform will stop trying to communicate with the SNMP device. The default value is *1500*. This field is required.
   - ***Retries***. Number of times the platform 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

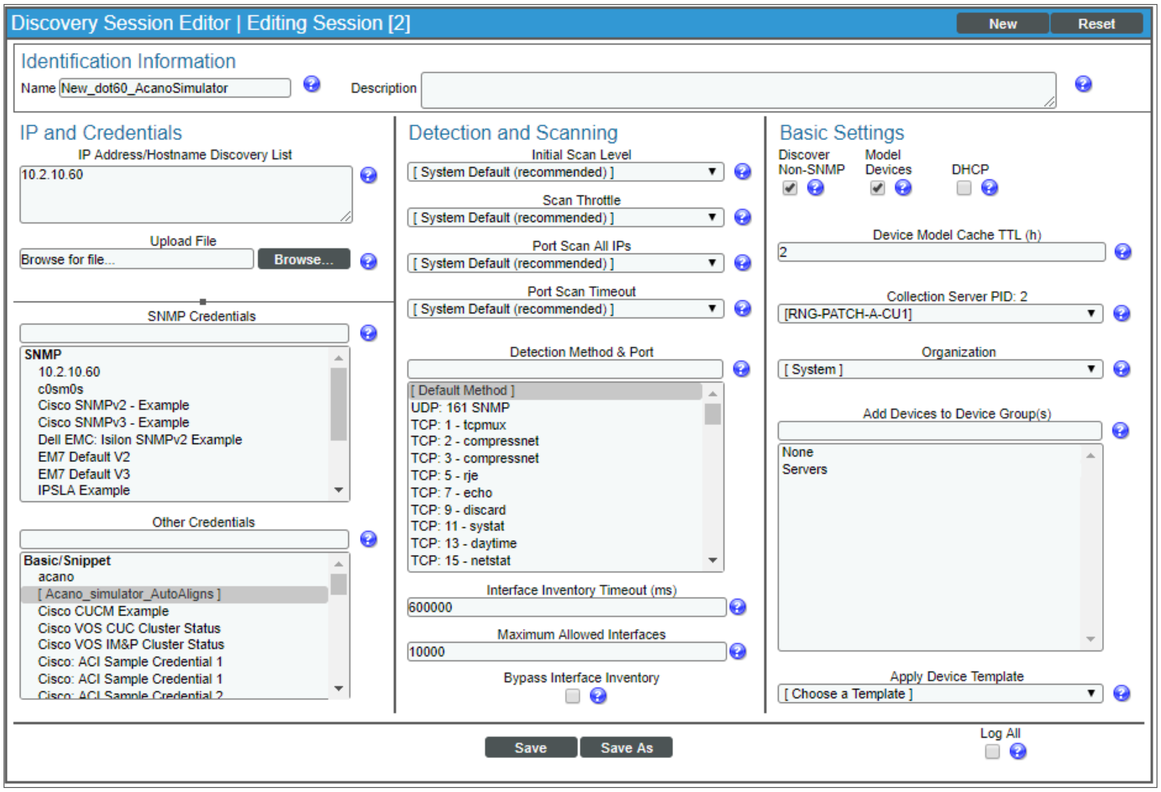
Discovering Cisco Meeting Server Devices That Use a Single IP Address

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:



Discovery Session Editor | Editing Session [2]

Identification Information

Name: New_dot60_AcanoSimulator

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.2.10.60

Upload File: Browse for file...

SNMP Credentials:

- SNMP
  - 10.2.10.60
  - c0sm0s
  - Cisco SNMPv2 - Example
  - Cisco SNMPv3 - Example
  - Dell EMC: Isilon SNMPv2 Example
  - EM7 Default V2
  - EM7 Default V3
  - IPSLA Example

Other Credentials:

- Basic/Snippet
  - acano
  - [Acano_simulator_AutoAligns]
  - Cisco CUCM Example
  - Cisco VOS CUC Cluster Status
  - Cisco VOS IM&P Cluster Status
  - Cisco: ACI Sample Credential 1
  - Cisco: ACI Sample Credential 1
  - Cisco: ACI Sample Credential 2

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: 15 - netstat

Interface Inventory Timeout (ms): 600000

Maximum Allowed Interfaces: 10000

Bypass Interface Inventory ☐

Basic Settings

Discover Non-SNMP ☑ Model Devices ☑ DHCP ☐

Device Model Cache TTL (h): 2

Collection Server PID: 2 [RNG-PATCH-A-CU1]

Organization: [System]

Add Devices to Device Group(s):

- None
- Servers

Apply Device Template: [Choose a Template]

Log All ☐

- ***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

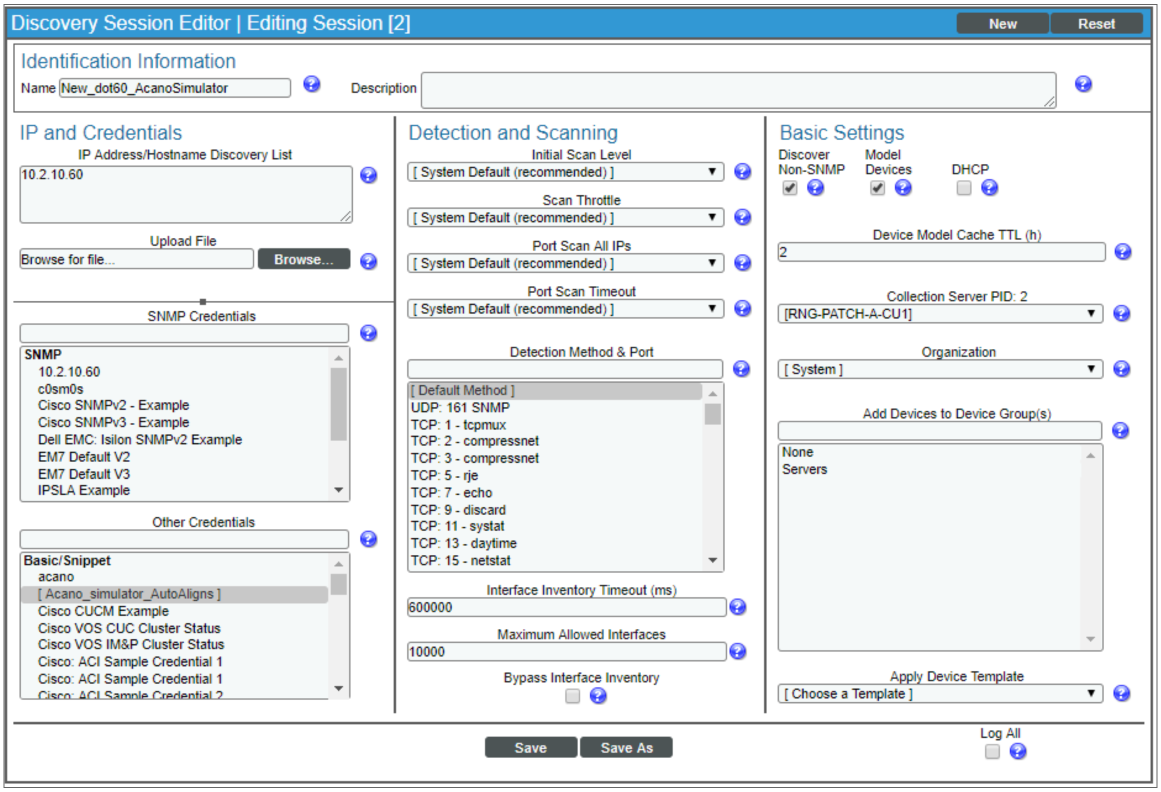
To model and monitor your Cisco Meeting Server devices, you must run a discovery session to discover the Cisco Meeting Server component devices that SL1 will use as the root devices for monitoring the applications.

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:



Discovery Session Editor | Editing Session [2]

New Reset

Identification Information

Name: New_dot60_AcanoSimulator

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.2.10.60

Upload File: Browse for file... Browse...

SNMP Credentials:

- SNMP
  - 10.2.10.60
  - c0sm0s
  - Cisco SNMPv2 - Example
  - Cisco SNMPv3 - Example
  - Dell EMC: Isilon SNMPv2 Example
  - EM7 Default V2
  - EM7 Default V3
  - IPSLA Example

Other Credentials:

- Basic/Snippet
  - acano
  - [Acano_simulator_AutoAligns]
  - Cisco CUCM Example
  - Cisco VOS CUC Cluster Status
  - Cisco VOS IM&P Cluster Status
  - Cisco: ACI Sample Credential 1
  - Cisco: ACI Sample Credential 1
  - Cisco: ACI Sample Credential 2

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: 15 - netstat

Interface Inventory Timeout (ms): 600000

Maximum Allowed Interfaces: 10000

Bypass Interface Inventory: □

Basic Settings

Discover Non-SNMP: ☑ Model Devices: ☑ DHCP: □

Device Model Cache TTL (h): 2

Collection Server PID: 2: [RNG-PATCH-A-CU1]

Organization: [System]

Add Devices to Device Group(s):

- None
- Servers

Apply Device Template: [Choose a Template]

Save Save As

Log All: □

- ***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.

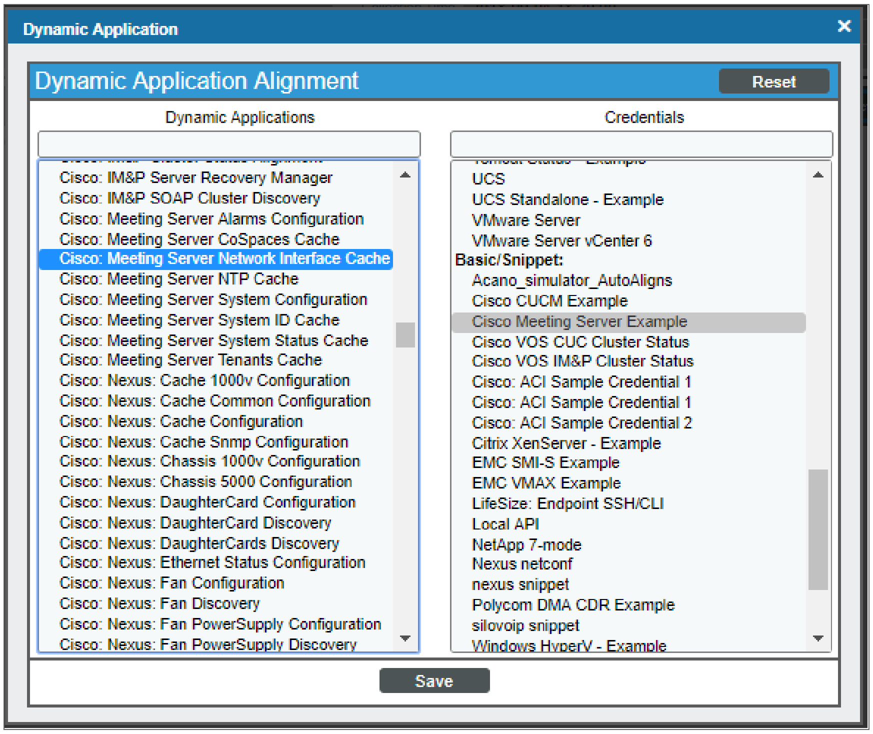
5. Click the **[Save]** button, and then close the **Discovery Session Editor** window.

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:


Dynamic Application
×
Dynamic Application Alignment
Reset
Dynamic Applications
Credentials
Cisco: IM&P Server Recovery Manager
Cisco: IM&P SOAP Cluster Discovery
Cisco: Meeting Server Alarms Configuration
Cisco: Meeting Server CoSpaces Cache
Cisco: Meeting Server Network Interface Cache
Cisco: Meeting Server NTP Cache
Cisco: Meeting Server System Configuration
Cisco: Meeting Server System ID Cache
Cisco: Meeting Server System Status Cache
Cisco: Meeting Server Tenants Cache
Cisco: Nexus: Cache 1000v Configuration
Cisco: Nexus: Cache Common Configuration
Cisco: Nexus: Cache Configuration
Cisco: Nexus: Cache Snmp Configuration
Cisco: Nexus: Chassis 1000v Configuration
Cisco: Nexus: Chassis 5000 Configuration
Cisco: Nexus: DaughterCard Configuration
Cisco: Nexus: DaughterCard Discovery
Cisco: Nexus: DaughterCards Discovery
Cisco: Nexus: Ethernet Status Configuration
Cisco: Nexus: Fan Configuration
Cisco: Nexus: Fan Discovery
Cisco: Nexus: Fan PowerSupply Configuration
Cisco: Nexus: Fan PowerSupply Discovery
UCS
UCS Standalone - Example
VMware Server
VMware Server vCenter 6
Basic/Snippet:
Acano_simulator_AutoAligns
Cisco CUCM Example
Cisco Meeting Server Example
Cisco VOS CUC Cluster Status
Cisco VOS IM&P Cluster Status
Cisco: ACI Sample Credential 1
Cisco: ACI Sample Credential 1
Cisco: ACI Sample Credential 2
Citrix XenServer - Example
EMC SMI-S Example
EMC VMAX Example
LifeSize: Endpoint SSH/CLI
Local API
NetApp 7-mode
Nexus netconf
nexus snippet
Polycom DMA CDR Example
silovoip snippet
Windows HyperV - Example
Save

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]**.

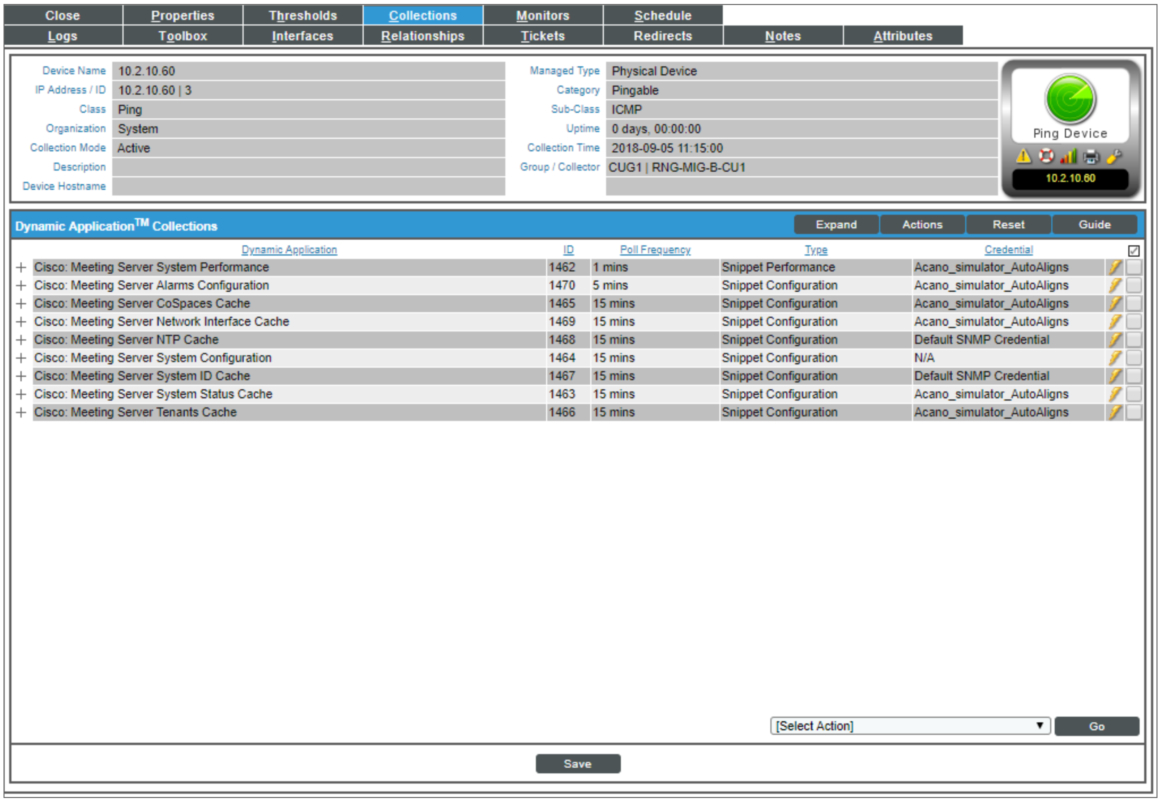
17. Click **[Action]** and then select *Add Dynamic Application* from the menu. The **Dynamic Application Alignment** page appears.
18. In the ***Dynamic Applications*** field, select the following Dynamic Applications:
    - Cisco: Meeting Server System Configuration
    - Cisco: Meeting Server System 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.



Device Name	10.2.10.60	Managed Type	Physical Device
IP Address / ID	10.2.10.60 | 3	Category	Pingable
Class	Ping	Sub-Class	ICMP
Organization	System	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2018-09-05 11:15:00
Description		Group / Collector	CUG1 | RNG-MIG-B-CU1
Device Hostname			

Dynamic Application^{TM} Collections

	Dynamic Application	ID	Poll Frequency	Type	Credential		☑
+	Cisco: Meeting Server System Performance	1462	1 mins	Snippet Performance	Acano_simulator_AutoAligns		□
+	Cisco: Meeting Server Alarms Configuration	1470	5 mins	Snippet Configuration	Acano_simulator_AutoAligns		□
+	Cisco: Meeting Server CoSpaces Cache	1465	15 mins	Snippet Configuration	Acano_simulator_AutoAligns		□
+	Cisco: Meeting Server Network Interface Cache	1469	15 mins	Snippet Configuration	Acano_simulator_AutoAligns		□
+	Cisco: Meeting Server NTP Cache	1468	15 mins	Snippet Configuration	Default SNMP Credential		□
+	Cisco: Meeting Server System Configuration	1464	15 mins	Snippet Configuration	N/A		□
+	Cisco: Meeting Server System ID Cache	1467	15 mins	Snippet Configuration	Default SNMP Credential		□
+	Cisco: Meeting Server System Status Cache	1463	15 mins	Snippet Configuration	Acano_simulator_AutoAligns		□
+	Cisco: Meeting Server Tenants Cache	1466	15 mins	Snippet Configuration	Acano_simulator_AutoAligns		□

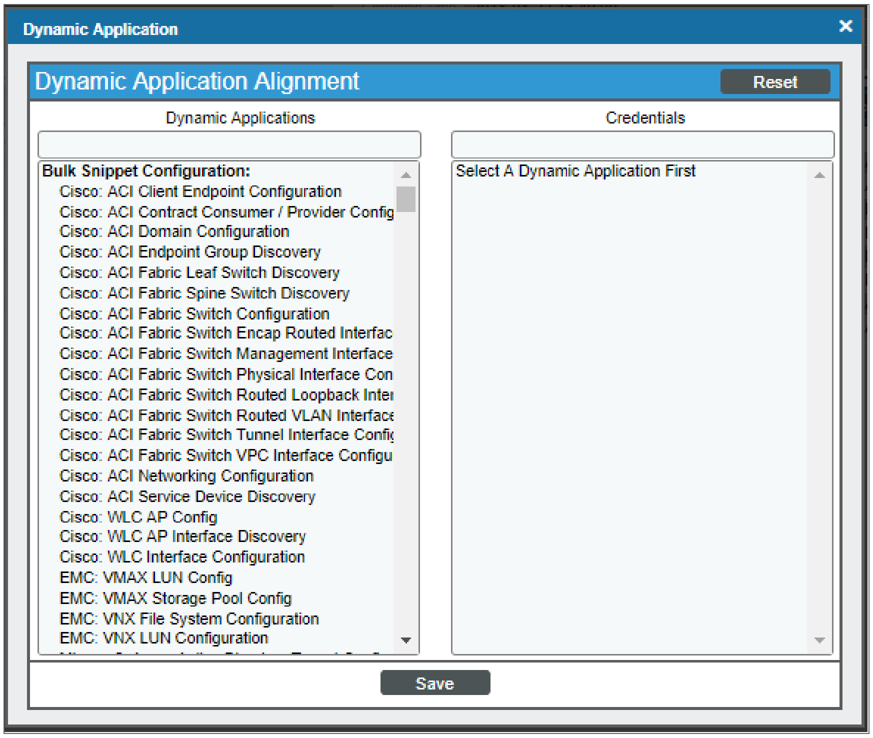
You should see the following Dynamic Applications aligned to the Cisco Meeting Server:

- 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:


Dynamic Application
×
Dynamic Application Alignment
Reset
Dynamic Applications
Credentials
Bulk Snippet Configuration:
Cisco: ACI Client Endpoint Configuration
Cisco: ACI Contract Consumer / Provider Config
Cisco: ACI Domain Configuration
Cisco: ACI Endpoint Group Discovery
Cisco: ACI Fabric Leaf Switch Discovery
Cisco: ACI Fabric Spine Switch Discovery
Cisco: ACI Fabric Switch Configuration
Cisco: ACI Fabric Switch Encap Routed Interfac
Cisco: ACI Fabric Switch Management Interface
Cisco: ACI Fabric Switch Physical Interface Con
Cisco: ACI Fabric Switch Routed Loopback Inter
Cisco: ACI Fabric Switch Routed VLAN Interface
Cisco: ACI Fabric Switch Tunnel Interface Confi
Cisco: ACI Fabric Switch VPC Interface Configu
Cisco: ACI Networking Configuration
Cisco: ACI Service Device Discovery
Cisco: WLC AP Config
Cisco: WLC AP Interface Discovery
Cisco: WLC Interface Configuration
EMC: VMAX LUN Config
EMC: VMAX Storage Pool Config
EMC: VNX File System Configuration
EMC: VNX LUN Configuration
Select A Dynamic Application First
Save

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

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