Credentials and Discovery for Monitored Devices

ScienceLogic version 10.2.0

Table of Contents

Chapter 1

Introduction

Overview

This manual describes the configuration steps, credentials, and discovery processes required for monitoring third-party products in SL1 using the latest versions of the following PowerPacks:

- Alibaba Cloud: Aliyun
- Apcon
- Amazon Web Services
- AMQP: RabbitMQ
- Aruba Central
- Cisco: ACI
- Cisco: ACI Multi-Site Manager
- Cisco: AppDynamics
- Cisco: CloudCenter
- Cisco: Contact Center Enterprise
- Cisco: Cloud Services Platform
- Cisco: CUCM Unified Communications Manager
- Cisco: ESA
- Cisco: Hyperflex
- Cisco: Meeting Server
- Cisco: Meraki [API]
- Cisco: Tetration
- Cisco: UC Ancillary

- Cisco: UC VOS Applications
- Cisco: UCS
- Cisco: UCS Director
- Cisco: UCS Standalone Rack Server
- Cisco: Unity Express
- Cisco: Viptela
- Cisco: Wireless
- Citrix: Xen
- CouchBase
- Dell EMC: Isilon
- Dell EMC: Unity
- Dell EMC: VMAX and PowerMax Unisphere API
- Dell EMC: XtremIO
- Docker
- Dynatrace
- ELK: AWS CloudTrail
- ELK: Azure Activity Log
- EMC: VMAX
- EMC: VNX
- F5 BIG-IP
- F5: BIG-IP DNS
- Google Cloud Platform *BETA*
- Hitachi Data Systems: VSP
- IBM: DataPower
- IBM: Db2
- IBM: MQ
- IBM: SVC
- IBM: Tivoli Storage Manager
- IBM: WebSphere Application Server
- JMX Base Pack *BETA*
- Kubernetes
- LayerX Appliance Monitoring
- Linux Base Pack
- Microsoft: Azure
- Microsoft: Office 365

- Microsoft: SQL Server Enhanced
- MySQL
- NetApp Base Pack
- New Relic: APM
- NGINX: Open Source and Plus
- Nimble Storage (2.3)
- Nutanix: Base Pack
- OpenStack
- Oracle: Database
- Palo Alto
- Pure Storage
- Silver Peak
- SMI-S: Array
- SoftLayer: Cloud
- VMware: NSX
- VMware: vSphere Base Pack

Additional Reading

For more information about each of the PowerPacks listed in the previous section, see the appropriate PowerPack-specific manual.

For more information about a PowerPack that is not listed in the previous section, see one of the following manuals:

- Monitoring SNMP-Enabled Devices
- Monitoring Switches, Routers, and Firewalls with SNMP
- Monitoring Video Devices
- Monitoring Windows Systems with PowerShell
- Monitoring Windows Systems with WMI

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.

Chapter 2

Alibaba Cloud: Aliyun

Overview

The following sections describe how to configure and discover Alibaba Aliyun services and component devices for monitoring by SL1 using the *Alibaba Cloud: Aliyun* PowerPack:

> NOTE: For more information about the *Alibaba Cloud: Aliyun* PowerPack, see the ***Monitoring Alibaba Cloud*** manual.

Prerequisites

To configure the SL1 system to monitor Aliyun using the *Alibaba Cloud: Aliyun* PowerPack, you must have the account access key ID and password for the Aliyun service you want to monitor.

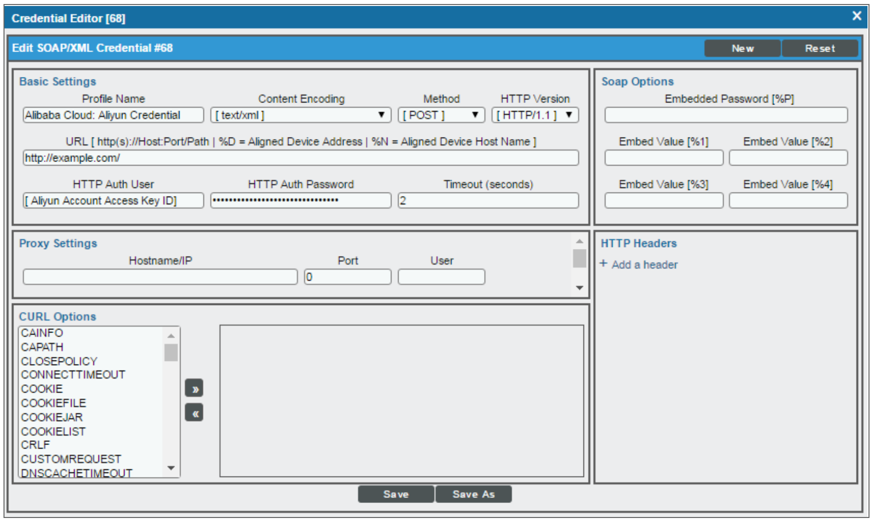
> NOTE: To properly discover and model your Aliyun service in SL1, the account must have at least Read-Only access to the Aliyun service you want to monitor.

Creating a SOAP/XML Credential for Aliyun

To configure SL1 to monitor Aliyun, you must first create a SOAP/XML credential. This credential allows SL1 (specifically, the Dynamic Applications in the *Alibaba Cloud: Aliyun* PowerPack) to connect with the Aliyun service. An example SOAP/XML credential that you can edit for your own use is included in the PowerPack.

To configure a SOAP/XML credential to access Aliyun:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the sample credential included in the *Alibaba Cloud: Aliyun* PowerPack, called **Alibaba Cloud: Aliyun Credential**, then click its wrench icon (🔧).
3. Enter values in the following fields:



Profile Name: Alibaba Cloud: Aliyun Credential
Content Encoding: [text/xml]
Method: [POST]
HTTP Version: [HTTP/1.1]
URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: http://example.com/
HTTP Auth User: [Aliyun Account Access Key ID]
HTTP Auth Password: ••••••••••••••••••••••••••••••••
Timeout (seconds): 2
Embedded Password [%P]:
Embed Value [%1]:
Embed Value [%2]:
Embed Value [%3]:
Embed Value [%4]:
Hostname/IP:
Port: 0
User:

   - ***Profile Name***. Enter a new name for the Aliyun credential.
   - ***Content Encoding***. Select *text/xml*.
   - ***Method***. Select POST.
   - ***HTTP Version***. Select HTTP/1.1.
   - ***URL***. Keep the default value.

> **NOTE:** The Aliyun service does not require a specific URL to access the service, but SL1 does require a URL value when creating SOAP/XML credentials. Therefore, the ***URL*** field must have an entry but the value itself does not matter.

   - ***HTTP Auth User***. Enter the account access key ID for the Aliyun service.
   - ***HTTP Auth Password***. Enter the account access key password for the Aliyun service.

4. Click **[Save As]**.
5. In the confirmation message, click **[OK]**.

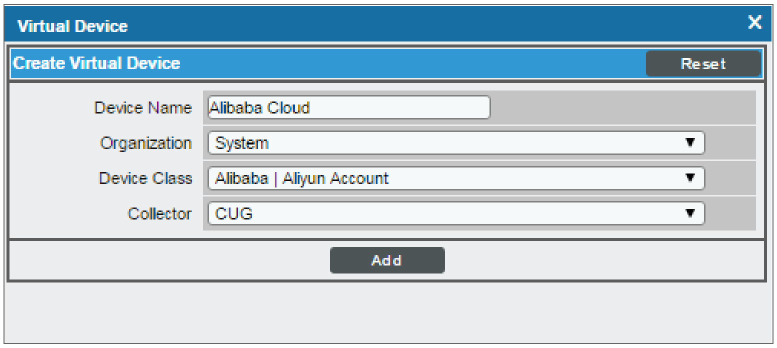
Creating an Aliyun Virtual Device

Because the Aliyun service does not have a static IP address, you cannot discover an Aliyun device using discovery. Instead, you must create a ***virtual device*** that represents the Aliyun service. A virtual device is a user-defined container that represents a device or service that cannot be discovered by SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications.

> **TIP:** If you have multiple Aliyun subscriptions you want to monitor, you should create a separate credential and virtual root device for each.

To create a virtual device that represents your Aliyun service:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Click **[Actions]** and select *Create Virtual Device* from the menu. The **Virtual Device** modal page appears.
3. Enter values in the following fields:



Device Name: Alibaba Cloud
Organization: System
Device Class: Alibaba | Aliyun Account
Collector: CUG

- ***Device Name***. Enter a name for the device. For example, you could enter "Alibaba Cloud" in this field.
- ***Organization***. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.
- ***Device Class***. Select *Alibaba | Aliyun Account*.
- ***Collector***. Select the collector group that will monitor the device.

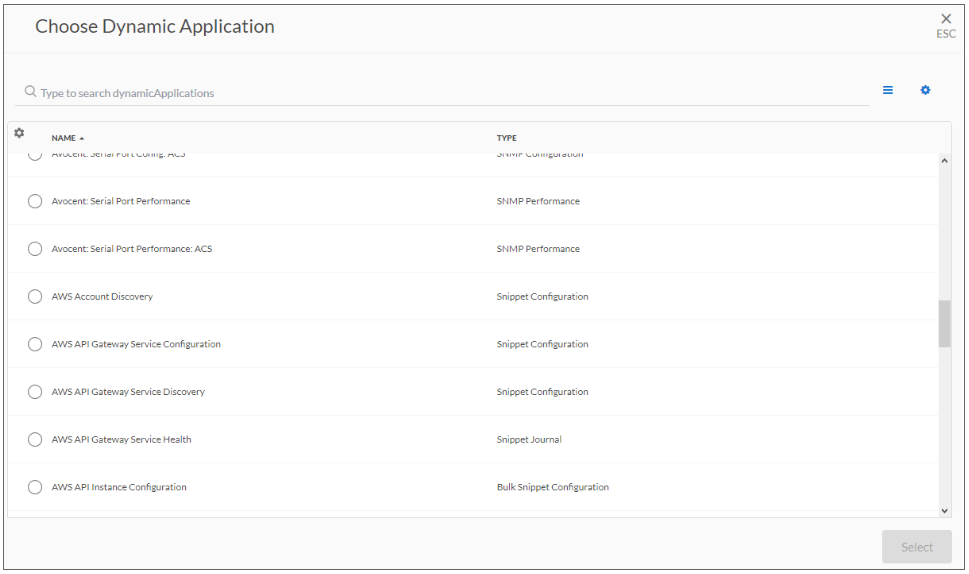
4. Click **[Add]** to create the virtual device.

Discovering Aliyun Component Devices

To discover all of the components of your Aliyun service, you must manually align the "Aliyun Account Configuration" and "Aliyun Region Discovery" Dynamic Applications with the Aliyun virtual device.

To discover your Aliyun service, perform the following steps:

1. Go to the **Devices** page and click on the Aliyun virtual device to open the **Device Investigator**.
2. Click the **[Collections]** tab.
3. Click **[Edit]** and then click **[Align Dynamic App]**. The **Align Dynamic Application** window appears.
4. Click *Choose Dynamic Application*. The **Choose Dynamic Application** window appears:



Choose Dynamic Application

Type to search dynamicApplications

	NAME ▲	TYPE
○	Avocent: Serial Port Config: ACS	SNMP Configuration
○	Avocent: Serial Port Performance	SNMP Performance
○	Avocent: Serial Port Performance: ACS	SNMP Performance
○	AWS Account Discovery	Snippet Configuration
○	AWS API Gateway Service Configuration	Snippet Configuration
○	AWS API Gateway Service Discovery	Snippet Configuration
○	AWS API Gateway Service Health	Snippet Journal
○	AWS API Instance Configuration	Bulk Snippet Configuration

3. Select the "Aliyun Account Configuration" Dynamic Application and click **[Select]**. The name of the selected Dynamic Application appears in the **Align Dynamic Application** window.
4. If a default credential is listed below the Dynamic Application and it is the *credential you created for your Aliyun service*, skip ahead to step 7. Otherwise, uncheck the box next to the credential name.
5. Click *Choose Credential*. The **Choose Credential** window appears.
6. Select the *credential you created for your Aliyun service* for the Dynamic Application and click the **[Select]** button. The name of the selected credential appears in the **Align Dynamic Application** window.
7. Click the **[Align Dynamic App]** button. When the Dynamic Application is successfully aligned, it is added to the **Collections** tab, and a confirmation message appears at the bottom of the tab.
8. Repeat these steps to align the "Aliyun Region Discovery" Dynamic Application with the Aliyun virtual device.

When you align the "Aliyun Account Configuration" Dynamic Application with the Aliyun virtual device, the Dynamic Application creates a component device representing the Aliyun account.

When you align the "Aliyun Region Discovery" Dynamic Application to the account component device, the Dynamic Application determines the regions used by the Aliyun account and creates a component device for each region.

Under each region, SL1 then discovers the following component device categories:

- Availability Zones
    - CloudDisk services
        - CloudDisk instances
    - Elastic Compute Service (ECS) services
        - ECS instances

TIP: To *unalign* a Dynamic Application from a device, click the **[Actions]** button (⋯) for that Dynamic Application and select *Unalign Dynamic App*. However, be advised that when you unalign a Dynamic Application, you also delete the data it has collected.

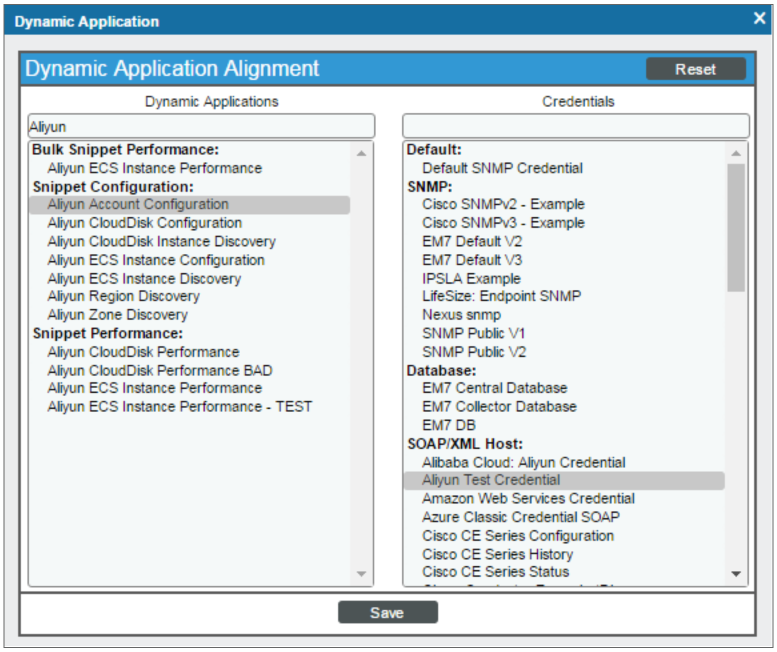
Discovering Aliyun Component Devices in the SL1 Classic User Interface

To discover all of the components of your Aliyun service, you must manually align the "Aliyun Account Configuration" and "Aliyun Region Discovery" Dynamic Applications with the Aliyun virtual device.

To discover your Aliyun service, perform the following steps:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Click the wrench icon (🔧) for your Aliyun virtual device.
3. In the **Device Administration** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
4. Click **[Actions]** and select *Add Dynamic Application* from the menu.

5. In the **Dynamic Application Alignment** modal page:



Dynamic Application

Dynamic Application Alignment

Reset

Dynamic Applications

Aliyun

Bulk Snippet Performance:
- Aliyun ECS Instance Performance

Snippet Configuration:
- Aliyun Account Configuration
- Aliyun CloudDisk Configuration
- Aliyun CloudDisk Instance Discovery
- Aliyun ECS Instance Configuration
- Aliyun ECS Instance Discovery
- Aliyun Region Discovery
- Aliyun Zone Discovery

Snippet Performance:
- Aliyun CloudDisk Performance
- Aliyun CloudDisk Performance BAD
- Aliyun ECS Instance Performance
- Aliyun ECS Instance Performance - TEST

Credentials

Default:
- Default SNMP Credential

SNMP:
- 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

Database:
- EM7 Central Database
- EM7 Collector Database
- EM7 DB

SOAP/XML Host:
- Alibaba Cloud: Aliyun Credential
- Aliyun Test Credential
- Amazon Web Services Credential
- Azure Classic Credential SOAP
- Cisco CE Series Configuration
- Cisco CE Series History
- Cisco CE Series Status

Save

- In the ***Dynamic Applications*** field, select the "Aliyun Account Configuration" Dynamic Application.
- In the ***Credentials*** field, select the ***credential you created for your Aliyun service***.

6. Click **[Save]** to align the Dynamic Application with the Aliyun virtual device.
7. Repeat steps 4-6 to align the "Aliyun Region Discovery" Dynamic Application with the Aliyun virtual device.

When you align the "Aliyun Account Configuration" Dynamic Application with the Aliyun virtual device, the Dynamic Application creates a component device representing the Aliyun account.

When you align the "Aliyun Region Discovery" Dynamic Application to the account component device, the Dynamic Application determines the regions used by the Aliyun account and creates a component device for each region.

Under each region, SL1 then discovers the following component device categories:

- Availability Zones
  - CloudDisk services
    - CloudDisk instances
  - Elastic Compute Service (ECS) services
    - ECS instances

Chapter 3

Apcon

Overview

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

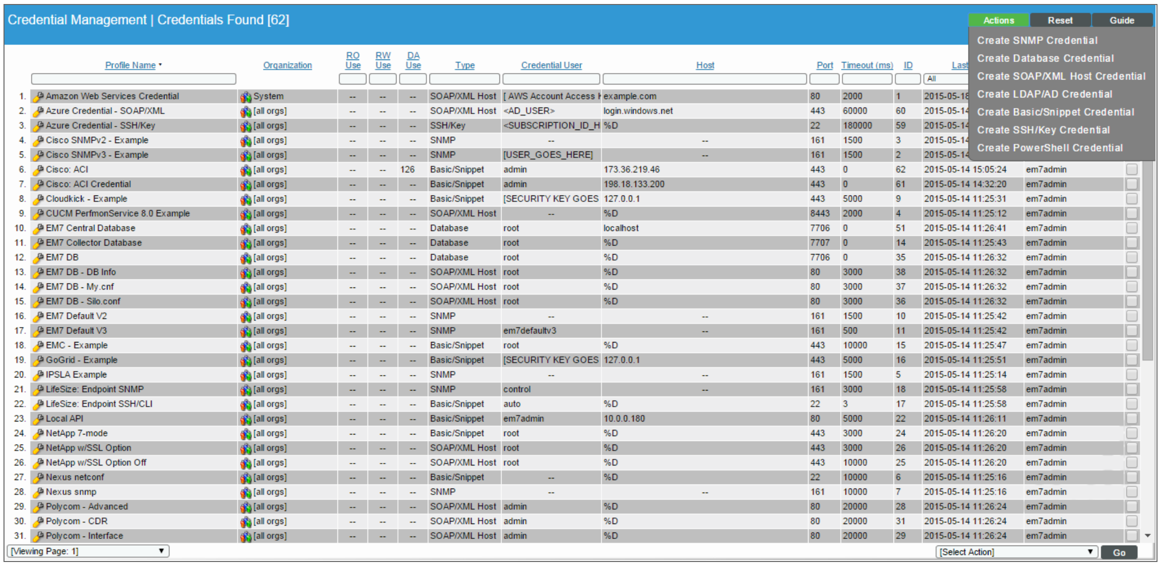
NOTE: For more information about the *Apcon*PowerPack, see the ***Monitoring APCON*** manual.

Creating an SNMP Credential for APCON

To monitor APCON devices with SL1, you must first create an SNMP credential. This credential enables the Dynamic Applications in the *Apcon* PowerPack to collect data from your APCON devices.

To create an SNMP credential:

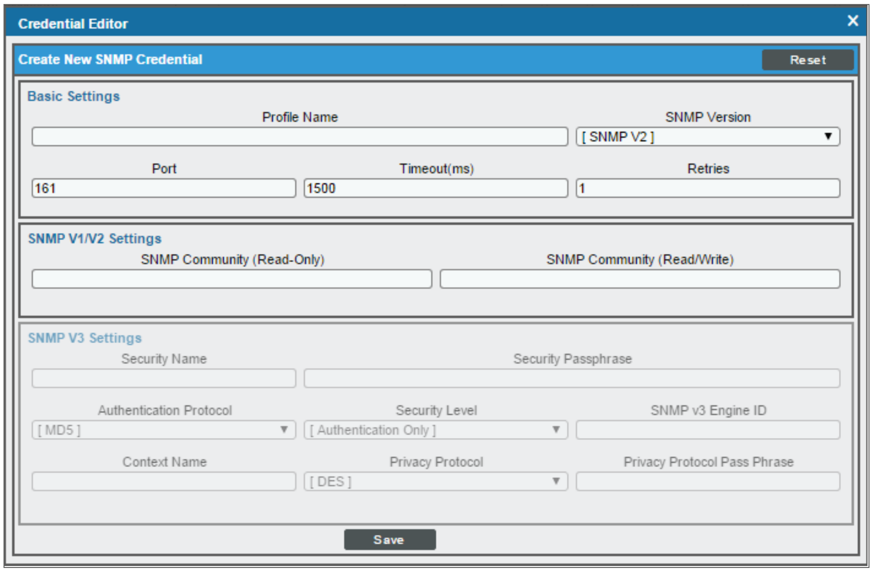
1. Go to the **Credential Management** page (System > Manage > Credentials).


Actions
Reset
Guide
Create SNMP Credential
Create Database Credential
Create SOAP/XML Host Credential
Create LDAP/AD Credential
Create Basic/Snippet Credential
Create SSH/Key Credential
Create PowerShell Credential
[Viewing Page: 1]
[Select Action]
Go

Credential Management | Credentials Found [62]

	Profile Name	Organization	RO Use	RW Use	DA Use	Type	Credential User	Host	Port	Timeout (ms)	ID	Last		
												All		
1.	Amazon Web Services Credential	System	--	--	--	SOAP/XML Host	[AWS Account Access K	example.com	80	2000	1	2015-05-18		
2.	Azure Credential - SOAP/XML	[all orgs]	--	--	--	SOAP/XML Host	<AD_USER>	login.windows.net	443	60000	60	2015-05-14		
3.	Azure Credential - SSH/Key	[all orgs]	--	--	--	SSH/Key	<SUBSCRIPTION_ID_H	%D	22	180000	59	2015-05-14		
4.	Cisco SNMPv2 - Example	[all orgs]	--	--	--	SNMP	--	--	161	1500	3	2015-05-14		
5.	Cisco SNMPv3 - Example	[all orgs]	--	--	--	SNMP	[USER_GOES_HERE]	--	161	1500	2	2015-05-14		
6.	Cisco: ACI	[all orgs]	--	--	126	Basic/Snippet	admin	173.36.219.46	443	0	62	2015-05-14 15:05:24	em7admin	□
7.	Cisco: ACI Credential	[all orgs]	--	--	--	Basic/Snippet	admin	198.18.133.200	443	0	61	2015-05-14 14:32:20	em7admin	□
8.	Cloudkick - Example	[all orgs]	--	--	--	Basic/Snippet	[SECURITY KEY GOES	127.0.0.1	443	5000	9	2015-05-14 11:25:31	em7admin	□
9.	CUCM PerfmonService 8.0 Example	[all orgs]	--	--	--	SOAP/XML Host	--	%D	8443	2000	4	2015-05-14 11:25:12	em7admin	□
10.	EM7 Central Database	[all orgs]	--	--	--	Database	root	localhost	7706	0	51	2015-05-14 11:26:41	em7admin	□
11.	EM7 Collector Database	[all orgs]	--	--	--	Database	root	%D	7707	0	14	2015-05-14 11:25:43	em7admin	□
12.	EM7 DB	[all orgs]	--	--	--	Database	root	%D	7706	0	35	2015-05-14 11:26:32	em7admin	□
13.	EM7 DB - DB Info	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	38	2015-05-14 11:26:32	em7admin	□
14.	EM7 DB - My.cnf	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	37	2015-05-14 11:26:32	em7admin	□
15.	EM7 DB - Silo.conf	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	36	2015-05-14 11:26:32	em7admin	□
16.	EM7 Default V2	[all orgs]	--	--	--	SNMP	--	--	161	1500	10	2015-05-14 11:25:42	em7admin	□
17.	EM7 Default V3	[all orgs]	--	--	--	SNMP	em7defaultv3	--	161	500	11	2015-05-14 11:25:42	em7admin	□
18.	EMC - Example	[all orgs]	--	--	--	Basic/Snippet	root	%D	443	10000	15	2015-05-14 11:25:47	em7admin	□
19.	GoGrid - Example	[all orgs]	--	--	--	Basic/Snippet	[SECURITY KEY GOES	127.0.0.1	443	5000	16	2015-05-14 11:25:51	em7admin	□
20.	IPSLA Example	[all orgs]	--	--	--	SNMP	--	--	161	1500	5	2015-05-14 11:25:14	em7admin	□
21.	LifeSize: Endpoint SNMP	[all orgs]	--	--	--	SNMP	control	--	161	3000	18	2015-05-14 11:25:58	em7admin	□
22.	LifeSize: Endpoint SSH/CLI	[all orgs]	--	--	--	Basic/Snippet	auto	%D	22	3	17	2015-05-14 11:25:58	em7admin	□
23.	Local API	[all orgs]	--	--	--	Basic/Snippet	em7admin	10.0.0.180	80	5000	22	2015-05-14 11:26:11	em7admin	□
24.	NetApp 7-mode	[all orgs]	--	--	--	Basic/Snippet	root	%D	443	3000	24	2015-05-14 11:26:20	em7admin	□
25.	NetApp w/SSL Option	[all orgs]	--	--	--	SOAP/XML Host	root	%D	443	3000	26	2015-05-14 11:26:20	em7admin	□
26.	NetApp w/SSL Option Off	[all orgs]	--	--	--	SOAP/XML Host	root	%D	443	10000	25	2015-05-14 11:26:20	em7admin	□
27.	Nexus netconf	[all orgs]	--	--	--	Basic/Snippet	--	%D	22	10000	6	2015-05-14 11:25:16	em7admin	□
28.	Nexus snmp	[all orgs]	--	--	--	SNMP	--	--	161	10000	7	2015-05-14 11:25:16	em7admin	□
29.	Polycom - Advanced	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	28	2015-05-14 11:26:24	em7admin	□
30.	Polycom - CDR	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	31	2015-05-14 11:26:24	em7admin	□
31.	Polycom - Interface	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	29	2015-05-14 11:26:24	em7admin	□

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



Credential Editor

Create New SNMP Credential

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. Leave it set at the default value of *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.

SNMP V2 Settings

These fields appear if you selected *SNMP V2* in the ***SNMP Version*** field.

- ***SNMP Community (Read Only)***. The SNMP community string (password) required for read-only access of SNMP data on the remote device or application. For SNMP V2 credentials, you must supply a community string, either in this field or in the ***SNMP Community (Read/Write)*** field.
- ***SNMP Community (Read/Write)***. The SNMP community string (password) required for read and write access of SNMP data on the remote device or application. For and SNMP V2 credentials, you must supply a community string, either in this field or in the ***SNMP Community (Read Only)*** field.

4. Click the **[Save]** button to save the new SNMP credential.

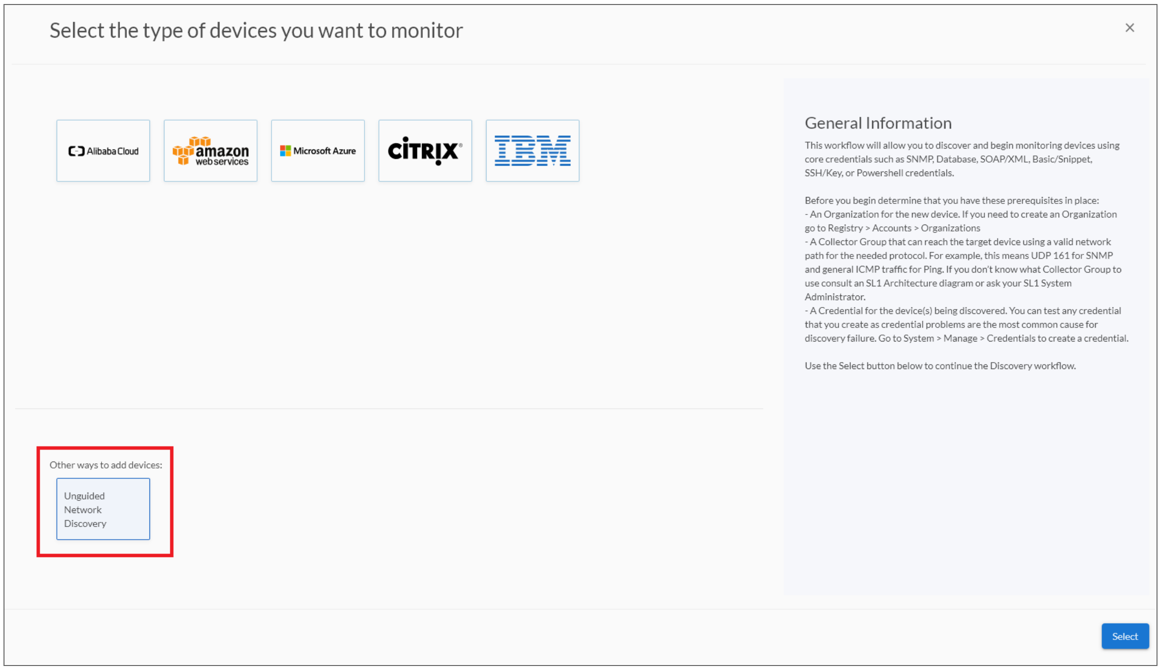
Discovering APCON Devices

To model and monitor your APCON device, you must run a discovery session to discover the Apcon device.

Several minutes after the discovery session has completed, the Dynamic Applications in the *Apcon* PowerPack should automatically align to the device.

To discover the APCON device that you want to monitor, perform the following steps:

1. On the **Devices** page (🖥) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears:



Select the type of devices you want to monitor

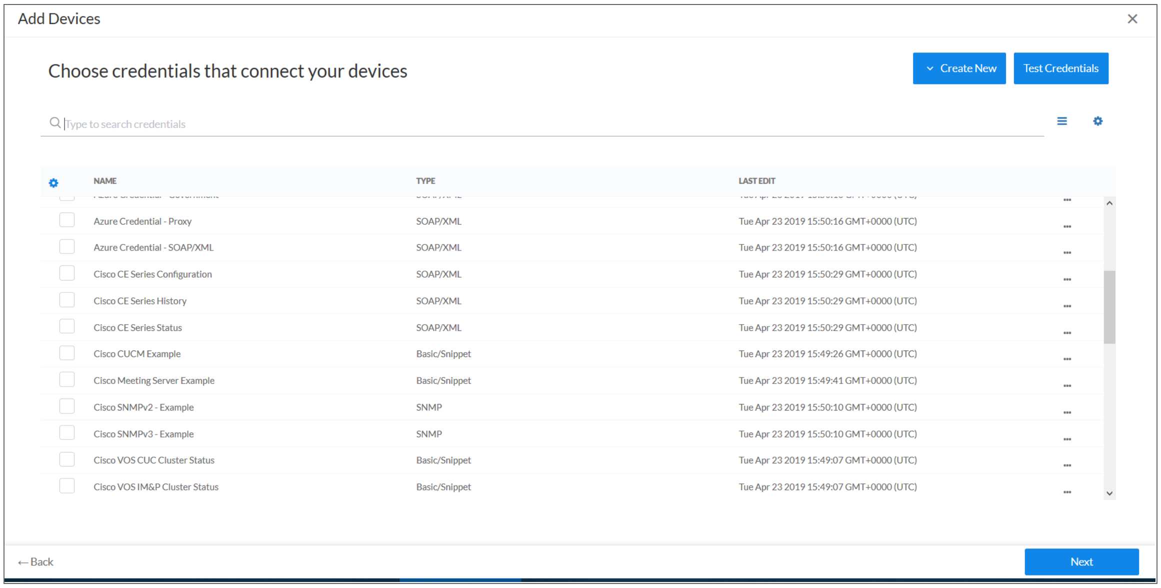
General Information

This workflow will allow you to discover and begin monitoring devices using core credentials such as SNMP, Database, SOAP/XML, Basic/Snippet, SSH/Key, or Powershell credentials.

Before you begin determine that you have these prerequisites in place:
- An Organization for the new device. If you need to create an Organization go to Registry > Accounts > Organizations
- A Collector Group that can reach the target device using a valid network path for the needed protocol. For example, this means UDP 161 for SNMP and general ICMP traffic for Ping. If you don't know what Collector Group to use consult an SL1 Architecture diagram or ask your SL1 System Administrator.
- A Credential for the device(s) being discovered. You can test any credential that you create as credential problems are the most common cause for discovery failure. Go to System > Manage > Credentials to create a credential.

Use the Select button below to continue the Discovery workflow.

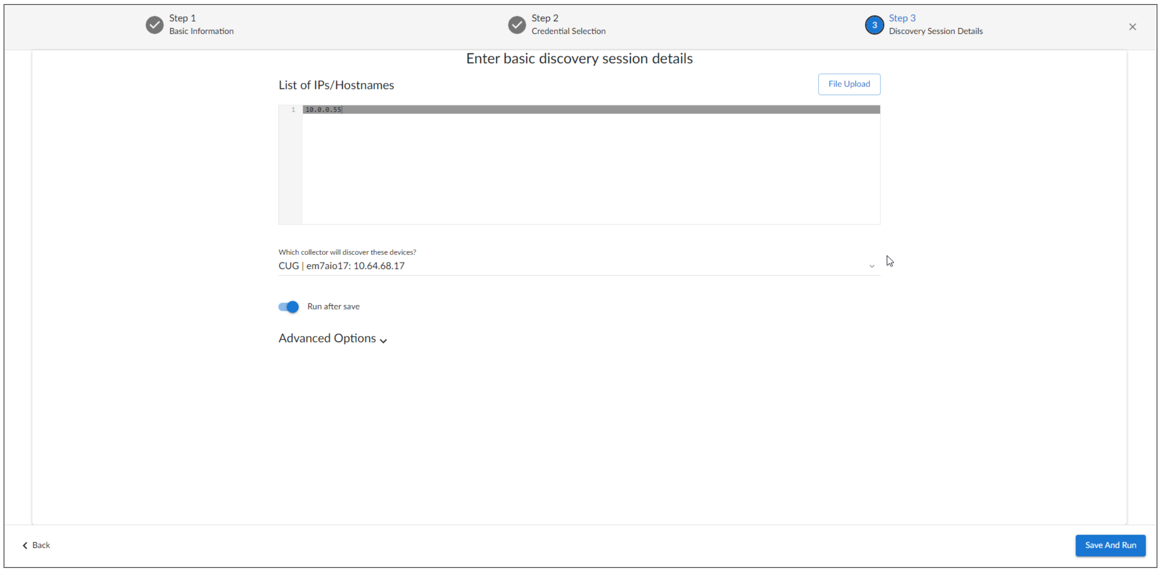
2. Click the **[Unguided Network Discovery]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.
3. Click **[Select]**. The **Add Devices** page appears.
4. Complete the following fields:
   - ***Name***. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.
   - ***Description***. Optional. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **[Discovery Sessions]** tab.
   - ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered devices
5. Click **[Next]**. The **Credentials** page of the **Add Devices** wizard appears:



Choose credentials that connect your devices

	NAME	TYPE	LAST EDIT
□	Azure Credential - Proxy	SOAP/XML	Tue Apr 23 2019 15:50:16 GMT+0000 (UTC)
□	Azure Credential - SOAP/XML	SOAP/XML	Tue Apr 23 2019 15:50:16 GMT+0000 (UTC)
□	Cisco CE Series Configuration	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)
□	Cisco CE Series History	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)
□	Cisco CE Series Status	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)
□	Cisco CUCM Example	Basic/Snippet	Tue Apr 23 2019 15:49:26 GMT+0000 (UTC)
□	Cisco Meeting Server Example	Basic/Snippet	Tue Apr 23 2019 15:49:41 GMT+0000 (UTC)
□	Cisco SNMPv2 - Example	SNMP	Tue Apr 23 2019 15:50:10 GMT+0000 (UTC)
□	Cisco SNMPv3 - Example	SNMP	Tue Apr 23 2019 15:50:10 GMT+0000 (UTC)
□	Cisco VOS CUC Cluster Status	Basic/Snippet	Tue Apr 23 2019 15:49:07 GMT+0000 (UTC)
□	Cisco VOS IM&P Cluster Status	Basic/Snippet	Tue Apr 23 2019 15:49:07 GMT+0000 (UTC)

6. On the **Credentials** page, locate and select the *SNMP credential* you created for the APCON device.
7. Click **[Next]**. The **Discovery Session Details** page of the **Add Devices** wizard appears:



Enter basic discovery session details

List of IPs/Hostnames

```
10.0.0.55
```

Which collector will discover these devices?
CUG | em7aio17: 10.64.68.17

Run after save

8. Complete the following fields:
   - ***List of IPs/Hostnames***. Enter the IP address or fully qualified domain name of the APCON device you want to discover.
   - ***Which collector will monitor these devices?***. Required. Select an existing collector to monitor the discovered devices.
   - ***Run after save***. Select this option to run this discovery session as soon as you save the session.

   In the **Advanced options** section, click the down arrow icon (⌄) to complete the following fields:

- ◦ *Model Devices*. Enable this setting.

9. Click **[Save and Run]** if you enabled the Run after save setting, or **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.
10. If you selected the **Run after save** option on this page, the discovery session runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page includes a link to the **Device Investigator** page for the discovered device.

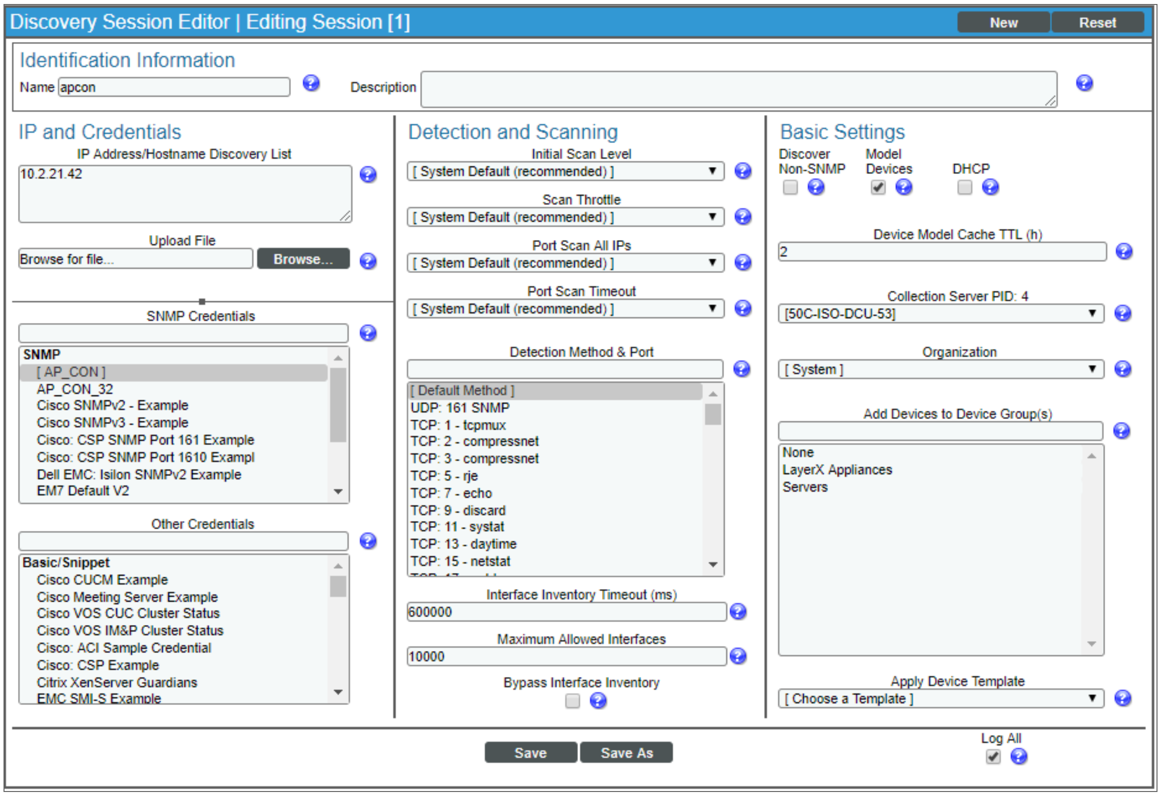
Discovering APCON Devices in the SL1 Classic User Interface

To model and monitor your APCON device, you must run a discovery session to discover the Apcon device.

Several minutes after the discovery session has completed, the Dynamic Applications in the *Apcon* PowerPack should automatically align to the device.

To discover the APCON device 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. The **Discovery Session Editor** page appears.



Name: apcon

Description:

IP Address/Hostname Discovery List: 10.2.21.42

Initial Scan Level: [System Default (recommended)]

Scan Throttle: [System Default (recommended)]

Port Scan All IPs: [System Default (recommended)]

Port Scan Timeout: [System Default (recommended)]

Interface Inventory Timeout (ms): 600000

Maximum Allowed Interfaces: 10000

Bypass Interface Inventory: ☐

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

Device Model Cache TTL (h): 2

Collection Server PID: 4: [50C-ISO-DCU-53]

Organization: [System]

Apply Device Template: [Choose a Template]

Log All: ☑

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

- *Name*. Enter a name for the discovery session. This name is displayed in the list of discovery sessions in the **Discovery Control Panel** page.

- ***IP Address/Hostname Discovery List***. Enter the IP address or fully qualified domain name of the Apcon device you want to discover.
- ***SNMP Credentials***. Select the SNMP credential you created for the Apcon device.
- ***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.

Verifying Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. After the discovery session has completed, find the APCON device in the **Devices** page and click on it.
2. From the **Device Investigator** page for the APCON device, click the **[Collections]** tab.
3. All applicable Dynamic Applications for the device are automatically aligned during discovery. You should see the following Dynamic Applications aligned to the APCON device:
    - Apcon: Interface Performance
    - Apcon: SFP/XFP Module Performance
    - Apcon: Configuration

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

If the listed Dynamic Applications have not been automatically aligned during discovery, you can align them manually. To do so, perform the following steps:

1. From the **[Collections]** tab, click **[Edit]** and then click **[Align Dynamic App]**. The **Align Dynamic Application** window appears.
2. Click *Choose Dynamic Application*. The **Choose Dynamic Application** window appears.
3. Select the "Apcon: Interface Performance" Dynamic Application and click **[Select]**. The name of the selected Dynamic Application appears in the **Align Dynamic Application** window.
4. If a default credential is listed below the Dynamic Application and it is the ***credential you created for your APCON device***, skip ahead to step 7. Otherwise, uncheck the box next to the credential name.
5. Click *Choose Credential*. The **Choose Credential** window appears.

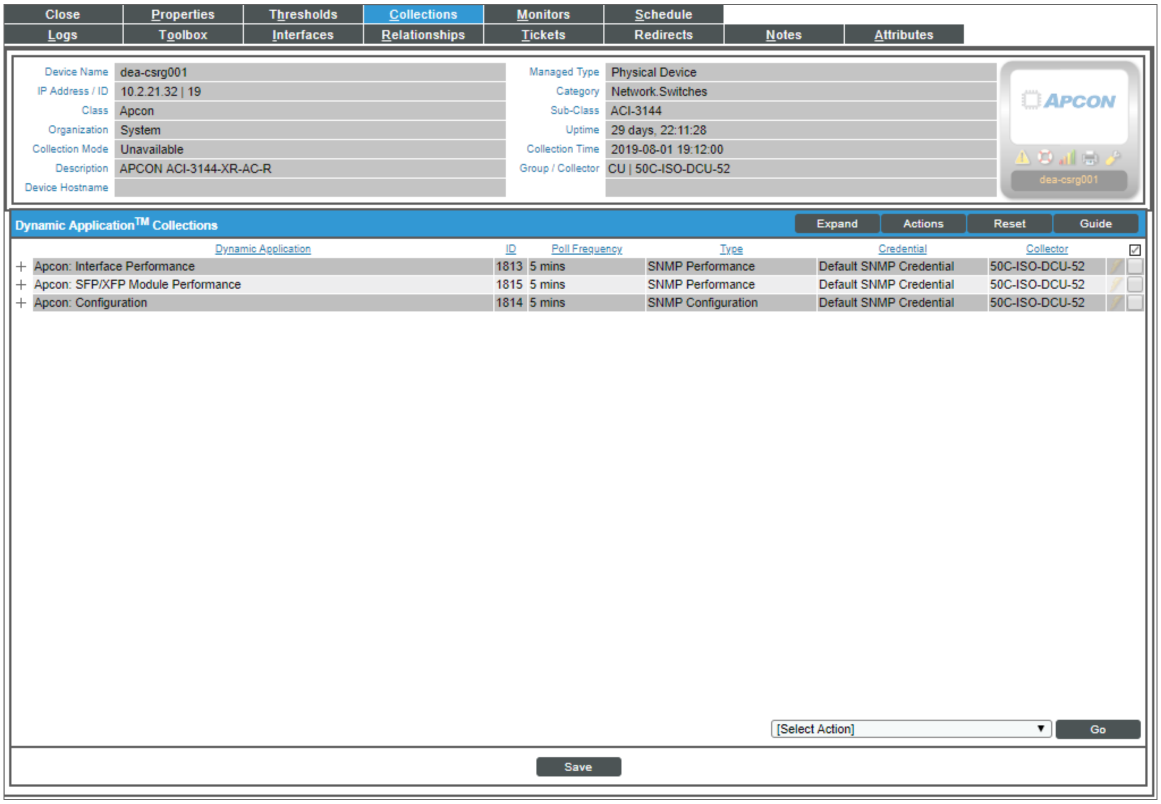
6. Select the *credential you created for your APCON device* for the Dynamic Application and click the **[Select]** button. The name of the selected credential appears in the **Align Dynamic Application** window.
7. Click the **[Align Dynamic App]** button. When the Dynamic Application is successfully aligned, it is added to the **Collections** tab, and a confirmation message appears at the bottom of the tab.
8. Repeat these steps to align the "Apcon: SFP/XFP Module Performance" and "Apcon: Configuration" Dynamic Applications with the APCON device.

Verifying Discovery and Dynamic Application Alignment in the SL1 Classic User Interface

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

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

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



Device Name: dea-csrg001
IP Address / ID: 10.2.21.32 | 19
Class: Apcon
Organization: System
Collection Mode: Unavailable
Description: APCON ACI-3144-XR-AC-R
Device Hostname:

Managed Type: Physical Device
Category: Network.Switches
Sub-Class: ACI-3144
Uptime: 29 days, 22:11:28
Collection Time: 2019-08-01 19:12:00
Group / Collector: CU | 50C-ISO-DCU-52

Dynamic Application^{TM} Collections

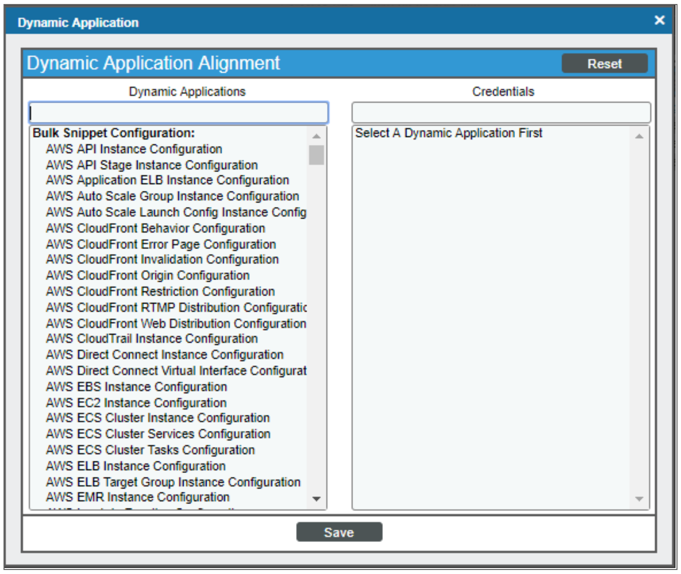
	Dynamic Application	ID	Poll Frequency	Type	Credential	Collector	☑
+	Apcon: Interface Performance	1813	5 mins	SNMP Performance	Default SNMP Credential	50C-ISO-DCU-52	□
+	Apcon: SFP/XFP Module Performance	1815	5 mins	SNMP Performance	Default SNMP Credential	50C-ISO-DCU-52	□
+	Apcon: Configuration	1814	5 mins	SNMP Configuration	Default SNMP Credential	50C-ISO-DCU-52	□

You should see the following Dynamic Applications aligned to the APCON device:

- Apcon: Interface Performance
- Apcon: SFP/XFP Module Performance
- Apcon: Configuration

If the listed Dynamic Applications have not been automatically aligned during discovery, you can align them manually. To do so, perform the following steps:

1. From the **Dynamic Application Collections** page, 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:
AWS API Instance Configuration
AWS API Stage Instance Configuration
AWS Application ELB Instance Configuration
AWS Auto Scale Group Instance Configuration
AWS Auto Scale Launch Config Instance Config
AWS CloudFront Behavior Configuration
AWS CloudFront Error Page Configuration
AWS CloudFront Invalidation Configuration
AWS CloudFront Origin Configuration
AWS CloudFront Restriction Configuration
AWS CloudFront RTMP Distribution Configuratic
AWS CloudFront Web Distribution Configuration
AWS CloudTrail Instance Configuration
AWS Direct Connect Instance Configuration
AWS Direct Connect Virtual Interface Configurat
AWS EBS Instance Configuration
AWS EC2 Instance Configuration
AWS ECS Cluster Instance Configuration
AWS ECS Cluster Services Configuration
AWS ECS Cluster Tasks Configuration
AWS ELB Instance Configuration
AWS ELB Target Group Instance Configuration
AWS EMR Instance 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.

Chapter

4

Amazon Web Services

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 (•••).

For more information about discovering and monitoring your AWS Infrastructure, watch the video at https://www.youtube.com/watch?v=ZPqNciWv0Tk.

The following sections describe several options available for using the *Amazon Web Services* PowerPack to monitor your AWS accounts.

NOTE: For more information about the *Amazon Web Services* PowerPack, see the ***Monitoring Amazon Web Services*** manual.

Configuring AWS to Report Billing Metrics

To use the "AWS: Billing Performance Percent" Dynamic Application, your AWS account must meet the following requirements:

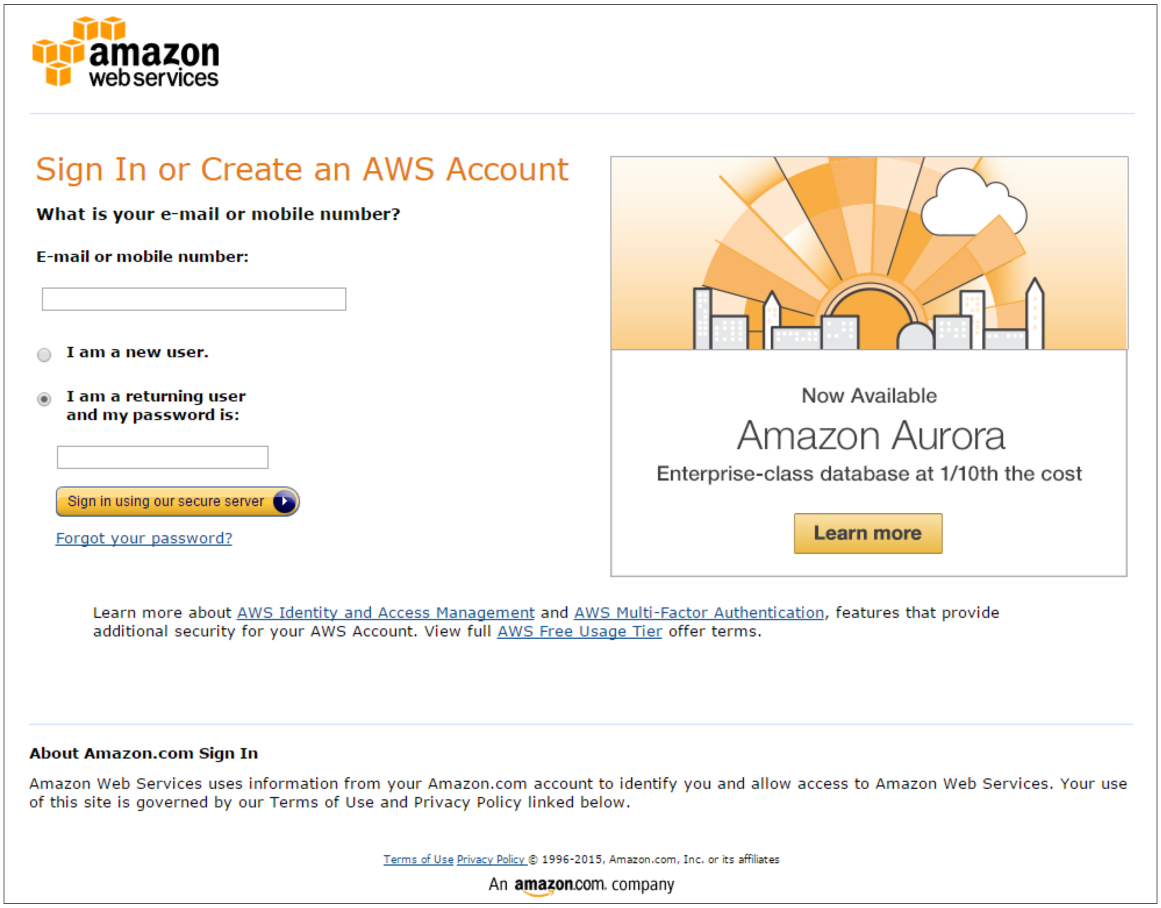
- The user account you supplied in the AWS credential must have permission to view the us-east-1 zone.
- Your AWS account must be configured to export billing metrics to the CloudWatch service.

If your AWS account is not configured to export billing metrics to the CloudWatch service, the "AWS: Billing Performance Percent" Dynamic Application will generate the following event:

```
No billing metrics can be retrieved. Your AWS account is not configured to export
billing metrics into CloudWatch.
```

To configure your AWS account to export billing metrics to the CloudWatch service, perform the following steps:

1. Open a browser session and go to aws.amazon.com.
2. Click **[My Account]** and then select *Billing & Cost Management*. If you are not currently logged in to the AWS site, you will be prompted to log in:



Sign In or Create an AWS Account

What is your e-mail or mobile number?

E-mail or mobile number:

○ **I am a new user.**

● **I am a returning user and my password is:**

Learn more about AWS Identity and Access Management and AWS Multi-Factor Authentication, features that provide additional security for your AWS Account. View full AWS Free Usage Tier offer terms.

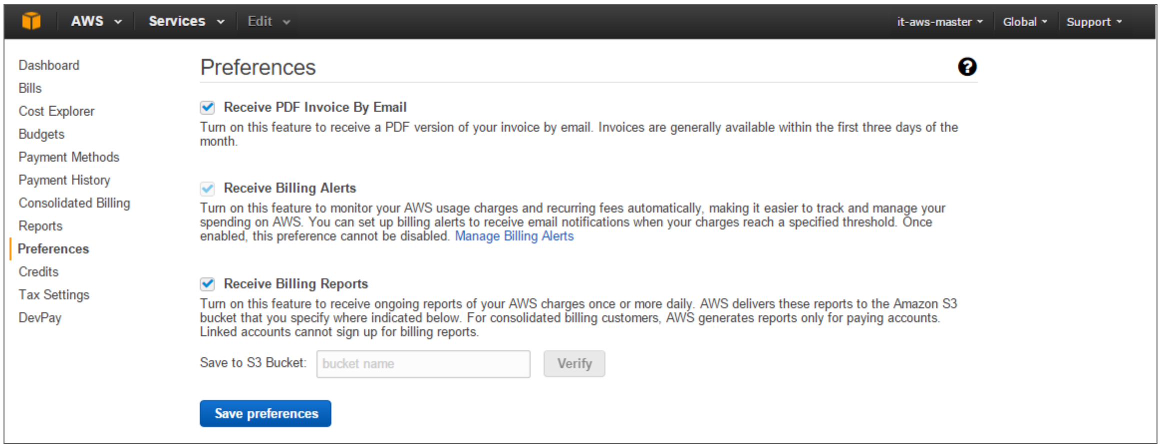
About Amazon.com Sign In

Amazon Web Services uses information from your Amazon.com account to identify you and allow access to Amazon Web Services. Your use of this site is governed by our Terms of Use and Privacy Policy linked below.

Terms of Use Privacy Policy © 1996-2015, Amazon.com, Inc. or its affiliates

An amazon.com company

3. After logging in, the **Billing & Cost Management Dashboard** page appears. In the left navigation bar, click **[Preferences]**. The **Preferences** page appears:



Preferences

☑ **Receive PDF Invoice By Email**

Turn on this feature to receive a PDF version of your invoice by email. Invoices are generally available within the first three days of the month.

☑ **Receive Billing Alerts**

Turn on this feature to monitor your AWS usage charges and recurring fees automatically, making it easier to track and manage your spending on AWS. You can set up billing alerts to receive email notifications when your charges reach a specified threshold. Once enabled, this preference cannot be disabled. Manage Billing Alerts

☑ **Receive Billing Reports**

Turn on this feature to receive ongoing reports of your AWS charges once or more daily. AWS delivers these reports to the Amazon S3 bucket that you specify where indicated below. For consolidated billing customers, AWS generates reports only for paying accounts. Linked accounts cannot sign up for billing reports.

Save to S3 Bucket: bucket name [Verify]

[Save preferences]

4. Select the ***Receive Billing Alerts*** checkbox.

CAUTION: If you enable this option, this option cannot be disabled.

5. Click the **[Save Preferences]** button.

Filtering EC2 Instances By Tag

To discover EC2 instances and filter them by tag, you can use the "AWS Credential - Tag Filter" sample credential to enter EC2 tag keys and values.

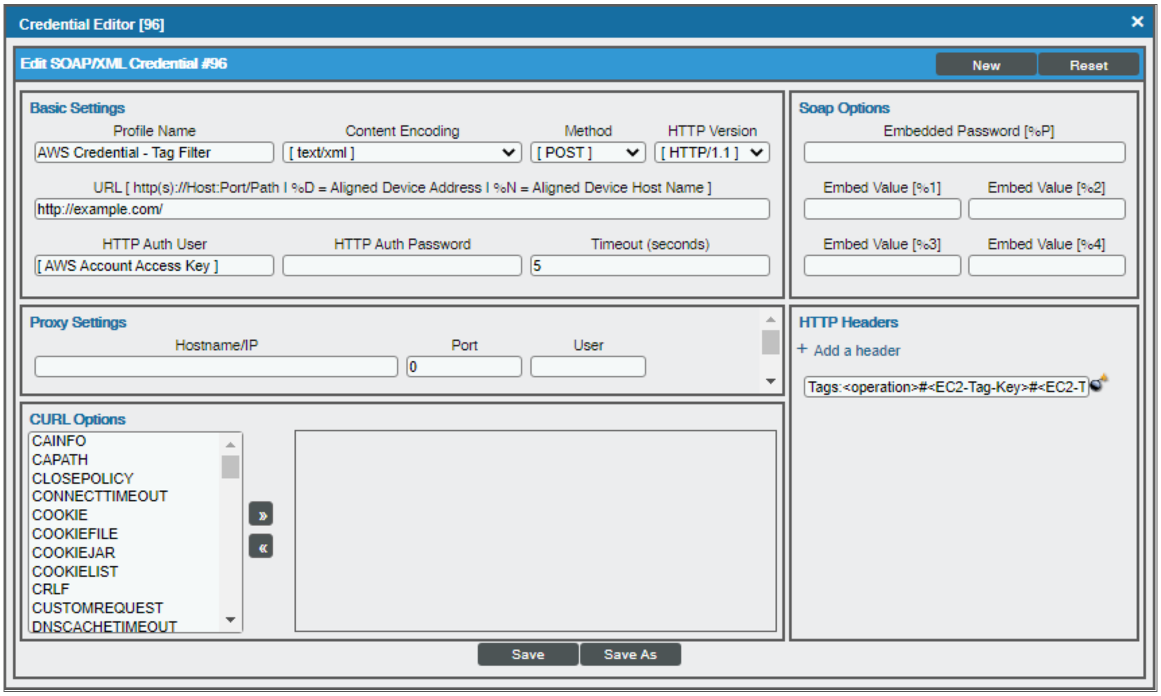
NOTE: Filtering EC2 instance by tag will apply to **all** accounts discovered.

NOTE: Any EC2 instances that have already been discovered, but do not match the tag filter, will be set to "Unavailable."

To define an AWS credential to discover EC2 instances and filter them by tag:

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

2. Locate the **AWS Credential - Tag Filter** sample credential and click its wrench icon (🔧). The **Credential Editor** modal page appears:



Credential Editor [96]

Edit SOAP/XML Credential #96

Basic Settings

Profile Name: AWS Credential - Tag Filter

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: http://example.com/

HTTP Auth User: [AWS Account Access Key]

HTTP Auth Password:

Timeout (seconds): 5

Proxy Settings

Hostname/IP:

Port: 0

User:

CURL Options

CAINFO
CAPATH
CLOSEPOLICY
CONNECTTIMEOUT
COOKIE
COOKIEFILE
COOKIEJAR
COOKIELIST
CRLF
CUSTOMREQUEST
DNSCACHETIMEOUT

HTTP Headers

Tags:<operation>#<EC2-Tag-Key>#<EC2-T

3. Enter values in the following fields:

Basic Settings

- ***Profile Name***. Type a new name for your AWS credential.
- ***HTTP Auth User***. Type your AWS access key ID.
- ***HTTP Auth Password***. Type your AWS secret access key.

HTTP Headers

- Edit the HTTP header provided:
  - *Tags:<operation>#<EC2-Tag-Key>#<EC2-Tag-Value>*. Type the tag, followed by its operation, tag key, or tag value. For example, if you want to filter by Tag Name, you would type the following:

```
Tags:equals#Name#Example
```

Valid operations include:

- equals
- notEquals
- contains
- notContains

You can chain together multiple filters separating them by a comma. For example:

```
Tags:equals#Name#Example,contains#Owner#Someone
```

4. Click the **[Save As]** button, and then click **[OK]**.

Automatic SL1 Organization Creation

This feature is only applicable to the two discovery methods that use the Assume Role and automatically discover multiple accounts.

When multiple accounts are discovered, this feature places each account in its own SL1 organization. This feature requires an optional header in the SOAP/XML credential you will create. When this header is present, it will place each account into a new SL1 organization. When this header is not present, each account will be placed in the SL1 organization selected in the discovery session. The name of the organization can be controlled depending on what is provided in the header as follows:

- ***OrganizationCreation:NAME:ID***. Autocreates an SL1 organization for accounts using AssumeRole. You can enter one of the following options:
  - ***OrganizationCreation:NAME***. The name of the organization will contain the name of the user.
  - ***OrganizationCreation:ID***. The name of the organization will contain the ID of the user.
  - ***OrganizationCreation:ID:NAME***. The name of the organization will contain both the ID and name of the user, in that order.
  - ***OrganizationCreation:NAME:ID***. The name of the organization will contain both the name and ID of the user, in that order.

Monitoring Consolidated Billing Accounts

Consolidated billing is an option provided by Amazon that allows multiple AWS accounts to be billed under a single account. For more information about consolidated billing, see http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html.

If a consolidated billing account is monitored by SL1, the billing metrics associated with that account include only the consolidated amounts, per service. If you use consolidated billing and want to collect billing metrics per-account, you must discover each account separately. To monitor only the billing metrics for an AWS account, you can create credentials that include only billing permissions.

ScienceLogic Events and AWS Alarms

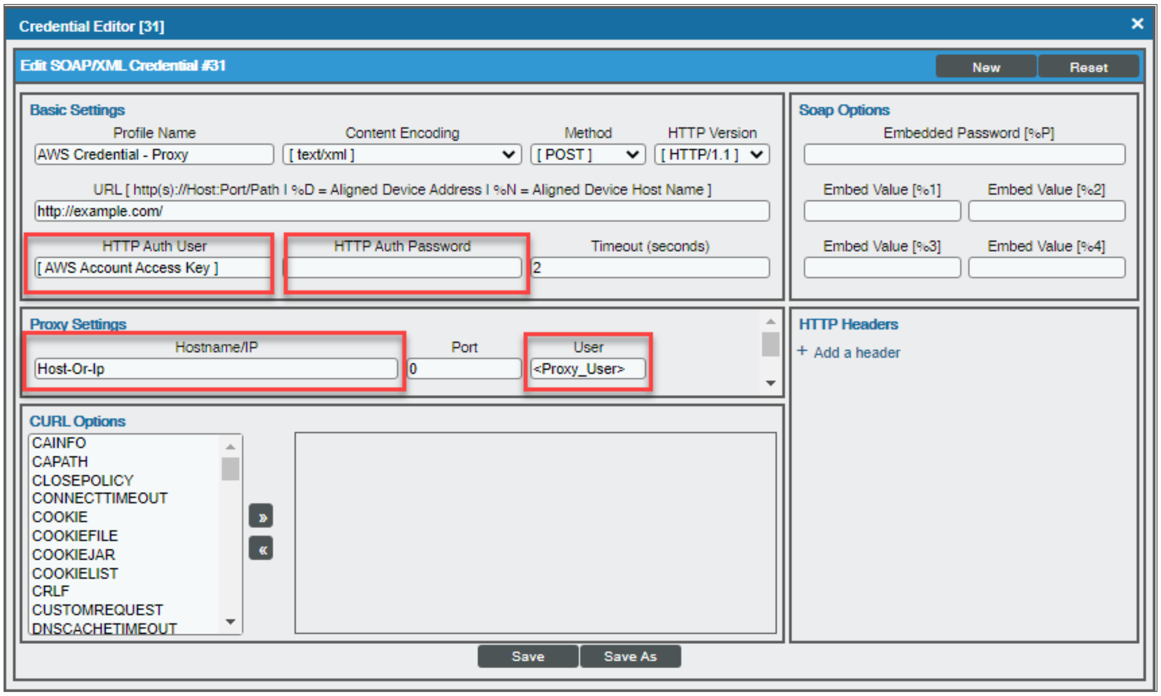
In addition to SL1 collecting metrics for AWS instances, you can configure CloudWatch to send alarm information to SL1 via API. SL1 can then generate an event for each alarm.

For instructions on how configure CloudWatch and SL1 to generate events based on CloudWatch alarms, see the ***Configuring Inbound CloudWatch Alarms*** section.

Using a Proxy Server

You can use a proxy server with the *Manual Discovery* and the *Automated Discovery Using AssumeRole with a Single IAM Key from the AWS Master Account* discovery methods.

To use a proxy server in both cases, you must fill in the proxy settings in the SOAP/XML credential.



Credential Editor [31]

Edit SOAP/XML Credential #31

Basic Settings

Profile Name: AWS Credential - Proxy
Content Encoding: [text/xml]
Method: [POST]
HTTP Version: [HTTP/1.1]
URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: http://example.com/
HTTP Auth User: [AWS Account Access Key]
HTTP Auth Password:
Timeout (seconds): 2

Soap Options

Embedded Password [%P]:
Embed Value [%1]:
Embed Value [%2]:
Embed Value [%3]:
Embed Value [%4]:

Proxy Settings

Hostname/IP: Host-Or-Ip
Port: 0
User: <Proxy_User>

HTTP Headers

CURL Options

For the *Automated Discovery Using AssumeRole with a Single IAM Key from the AWS Master Account* discovery method, if the proxy does not support ping passthrough you will also need to follow the steps in the ***Automated Discovery Using AssumeRole with a Single IAM Key from the AWS Master Account*** section without ping support.

Configuring "AWS: Lambda Service Discovery"

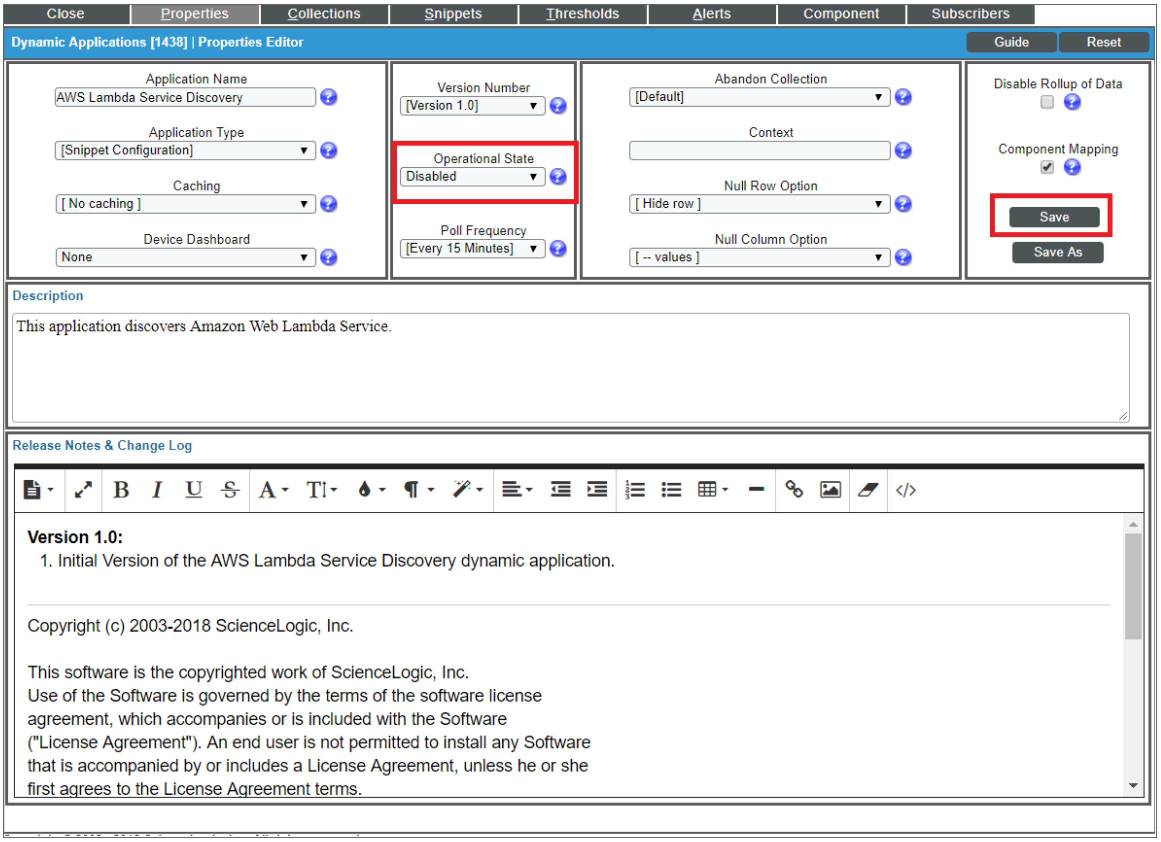
By default, the "AWS: Lambda Service Discovery" Dynamic Application is configured to discover only regular Lambda functions, not replica functions. If you want to discover both regular and replica Lambda functions, then you must configure the "AWS: Lambda Service Discovery" Dynamic Application to do so ***prior*** to discovering your Lambda service.

To configure the "AWS: Lambda Service Discovery" Dynamic Application to discover both regular and replica Lambda functions:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).

2. Locate the "AWS: Lambda Service Discovery" Dynamic Application and click its wrench icon (🔧). The **Dynamic Applications Properties Editor** page appears.

3. In the ***Operational State*** field, select *Disabled*, and then click **[Save]**. This disables the Dynamic Application from collecting data.



Dynamic Applications [1438] | Properties Editor

Application Name: AWS Lambda Service Discovery
Application Type: [Snippet Configuration]
Caching: [No caching]
Device Dashboard: None
Version Number: [Version 1.0]
Operational State: Disabled
Poll Frequency: [Every 15 Minutes]
Abandon Collection: [Default]
Context:
Null Row Option: [Hide row]
Null Column Option: [-- values]
Disable Rollup of Data: ☐
Component Mapping: ☑

Description

This application discovers Amazon Web Lambda Service.

Release Notes & Change Log

Version 1.0:

1. Initial Version of the AWS Lambda Service Discovery dynamic application.

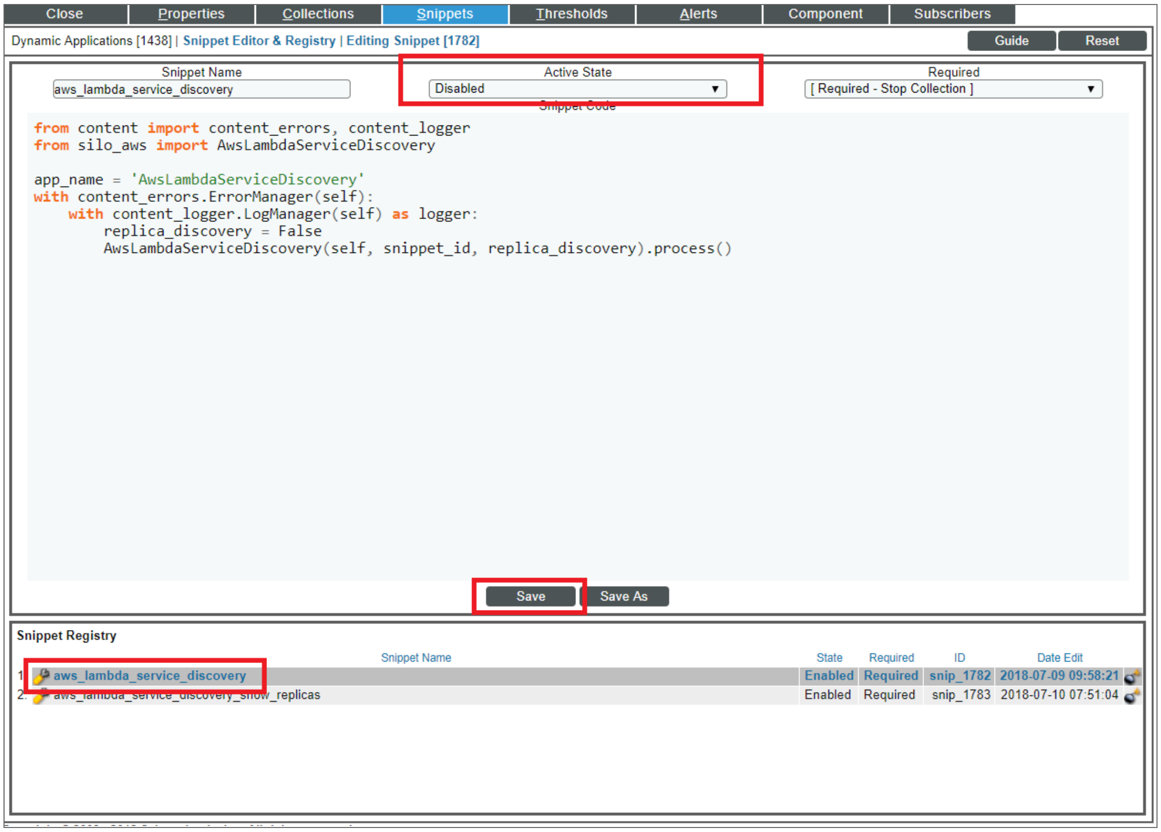
Copyright (c) 2003-2018 ScienceLogic, Inc.

This software is the copyrighted work of ScienceLogic, Inc.
Use of the Software is governed by the terms of the software license
agreement, which accompanies or is included with the Software
("License Agreement"). An end user is not permitted to install any Software
that is accompanied by or includes a License Agreement, unless he or she
first agrees to the License Agreement terms.

4. Click the **[Snippets]** tab. The **Dynamic Applications Snippet Editor & Registry** page appears.

5. In the **Snippet Registry** pane, click the wrench icon (🔧) for the "aws_lambda_service_discovery" snippet.

6. In the ***Active State*** field, select *Disabled*, and then click **[Save]**. This disables the "aws_lambda_service_discovery" snippet.



Dynamic Applications [1438] | Snippet Editor & Registry | Editing Snippet [1782]

Snippet Name	Active State	Required
aws_lambda_service_discovery	Disabled	[Required - Stop Collection]

Snippet Code

```
from content import content_errors, content_logger
from silo_aws import AwsLambdaServiceDiscovery

app_name = 'AwsLambdaServiceDiscovery'
with content_errors.ErrorManager(self):
    with content_logger.LogManager(self) as logger:
        replica_discovery = False
        AwsLambdaServiceDiscovery(self, snippet_id, replica_discovery).process()
```

Snippet Registry

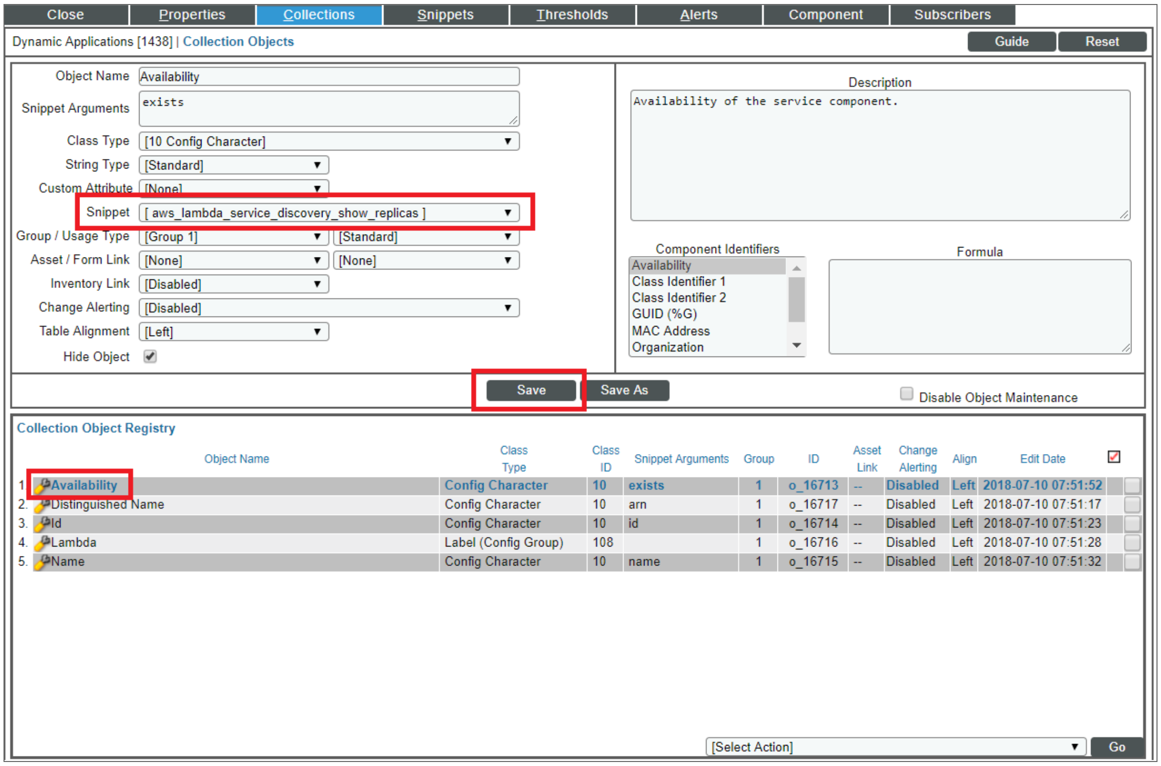
	Snippet Name	State	Required	ID	Date Edit
1.	aws_lambda_service_discovery	Enabled	Required	snip_1782	2018-07-09 09:58:21
2.	aws_lambda_service_discovery_show_replicas	Enabled	Required	snip_1783	2018-07-10 07:51:04

7. In the **Snippet Registry** pane, click the wrench icon (🔧) for the "aws_lambda_service_discovery_show_replicas" snippet.

8. In the ***Active State*** field, select *Enabled*, and then click **[Save]**. This enables the "aws_lambda_service_discovery_show_replicas" snippet.

9. Click the **[Collections]** tab. The **Dynamic Applications | Collections Objects** page appears.

10. Click the wrench icon ( ) for the first Collection Object listed in the **Collection Object Registry** pane, select *aws_lambda_service_discovery_show_replicas* in the ***Snippet*** field for that Collection Object, and then click **[Save]**.



Dynamic Applications [1438] | Collection Objects

Object Name	Availability
Snippet Arguments	exists
Class Type	[10 Config Character]
String Type	[Standard]
Custom Attribute	[None]
Snippet	[aws_lambda_service_discovery_show_replicas]
Group / Usage Type	[Group 1] [Standard]
Asset / Form Link	[None] [None]
Inventory Link	[Disabled]
Change Alerting	[Disabled]
Table Alignment	[Left]
Hide Object	☑

Description

```
Availability of the service component.
```

Component Identifiers

Availability
Class Identifier 1
Class Identifier 2
GUID (%G)
MAC Address
Organization

Formula

□ Disable Object Maintenance

Collection Object Registry

	Object Name	Class Type	Class ID	Snippet Arguments	Group	ID	Asset Link	Change Alerting	Align	Edit Date	☑
1.	Availability	Config Character	10	exists	1	o_16713	--	Disabled	Left	2018-07-10 07:51:52	□
2.	Distinguished Name	Config Character	10	arn	1	o_16717	--	Disabled	Left	2018-07-10 07:51:17	□
3.	Id	Config Character	10	id	1	o_16714	--	Disabled	Left	2018-07-10 07:51:23	□
4.	Lambda	Label (Config Group)	108		1	o_16716	--	Disabled	Left	2018-07-10 07:51:28	□
5.	Name	Config Character	10	name	1	o_16715	--	Disabled	Left	2018-07-10 07:51:32	□

[Select Action]

11. Repeat step 10 for all of the remaining Collection Objects listed in the **Collection Object Registry** pane.

12. Click the **[Properties]** tab.

13. In the ***Operational State*** field, select *Enabled*, and then click **[Save]**. This re-enables data collection for the Dynamic Application.

NOTE: If you configure the "AWS: Lambda Service Discovery" Dynamic Application to discover both regular and replica Lambda functions, then when you run discovery, the Dynamic Applications in the *Amazon Web Services* PowerPack will create ***parent/child relationships*** between replica Lambda functions and their corresponding master Lambda functions. In this scenario, the ***Device View and other device component maps*** will display the relationship in this order: Lambda Function Service > Lambda Replica Function > Master Lambda Function. The replica appears as the parent to the master Lambda function because the replica could be in the same or a different region than the master Lambda function.

Configuring "AWS: Lambda Function Qualified Discovery"

By default, the "AWS: Lambda Function Qualified Discovery" Dynamic Application is configured to discover and model all Lambda alias components. An ***alias*** is a qualifier inside an AWS Lambda function that enables the user to control which versions of the Lambda function are executable—for instance, a production version and a test version.

When the "AWS: Lambda Function Qualified Discovery" Dynamic Application is configured to discover alias components, SL1 collects data only for the Lambda function versions specified in the alias.

Depending on your needs, you can optionally configure the Dynamic Application to instead do one of the following:

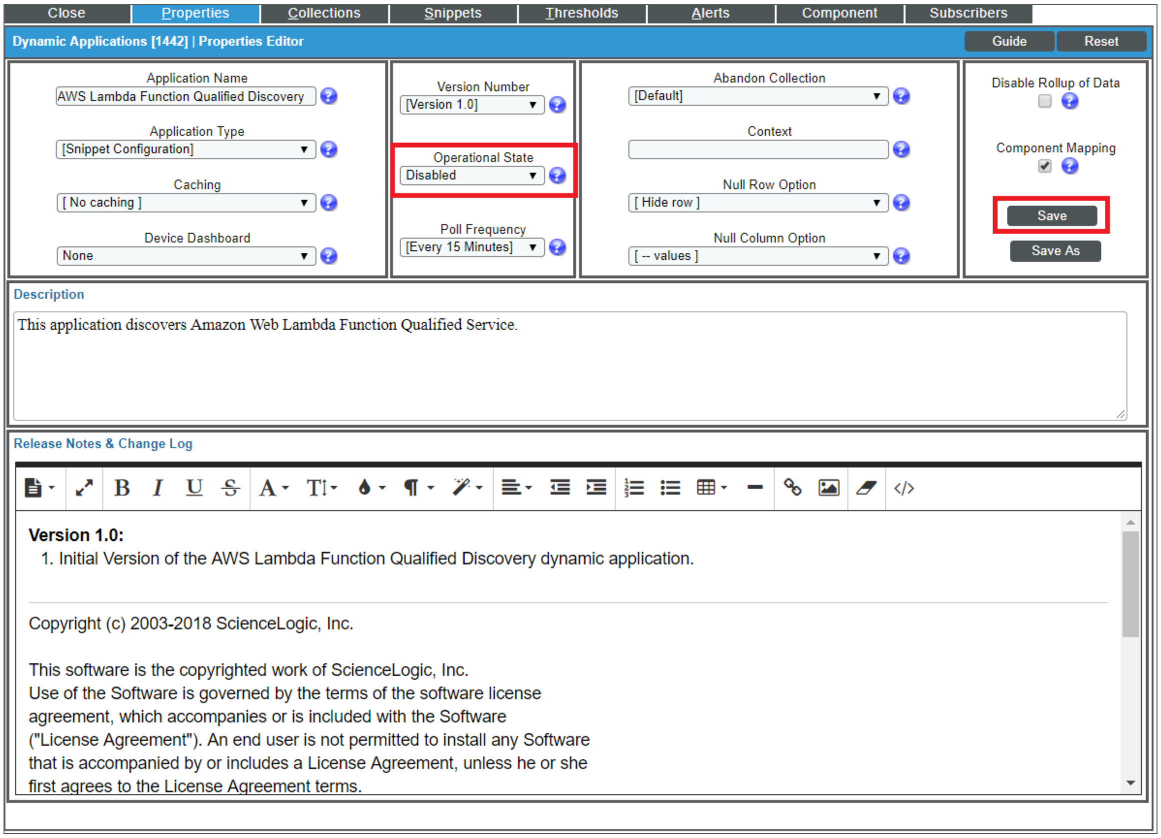
- Discover and model all Lambda version components. If you select this configuration, SL1 collects data for all existing versions of the Lambda function.
- Discover and model only Lambda version components with AWS configurations filtered by a trigger. If you select this configuration, SL1 collects data only for versions of the Lambda function that have triggers or are specified in an alias.

> **NOTE:** If you have ***configured the "AWS: Lambda Service Discovery" Dynamic Application*** to discover both regular and replica Lambda functions and you want SL1 to ***create dynamic component map relationships*** between replica Lambda functions and their parent Lambda function versions, you must follow these instructions to configure the "AWS: Lambda Function Qualified Discovery" Dynamic Application to discover and model all Lambda version components.

To configure the "AWS: Lambda Function Qualified Discovery" Dynamic Application:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
2. Locate the "AWS: Lambda Function Qualified Discovery" Dynamic Application and click its wrench icon (🔧). The **Dynamic Applications Properties Editor** page appears.

3. In the ***Operational State*** field, select *Disabled*, and then click **[Save]**. This disables the Dynamic Application from collecting data.



Dynamic Applications [1442] | Properties Editor

Application Name: AWS Lambda Function Qualified Discovery

Application Type: [Snippet Configuration]

Caching: [No caching]

Device Dashboard: None

Version Number: [Version 1.0]

Operational State: Disabled

Poll Frequency: [Every 15 Minutes]

Abandon Collection: [Default]

Context:

Null Row Option: [Hide row]

Null Column Option: [-- values]

Disable Rollup of Data: □

Component Mapping: ☑

Description

This application discovers Amazon Web Lambda Function Qualified Service.

Release Notes & Change Log

Version 1.0:

1. Initial Version of the AWS Lambda Function Qualified Discovery dynamic application.

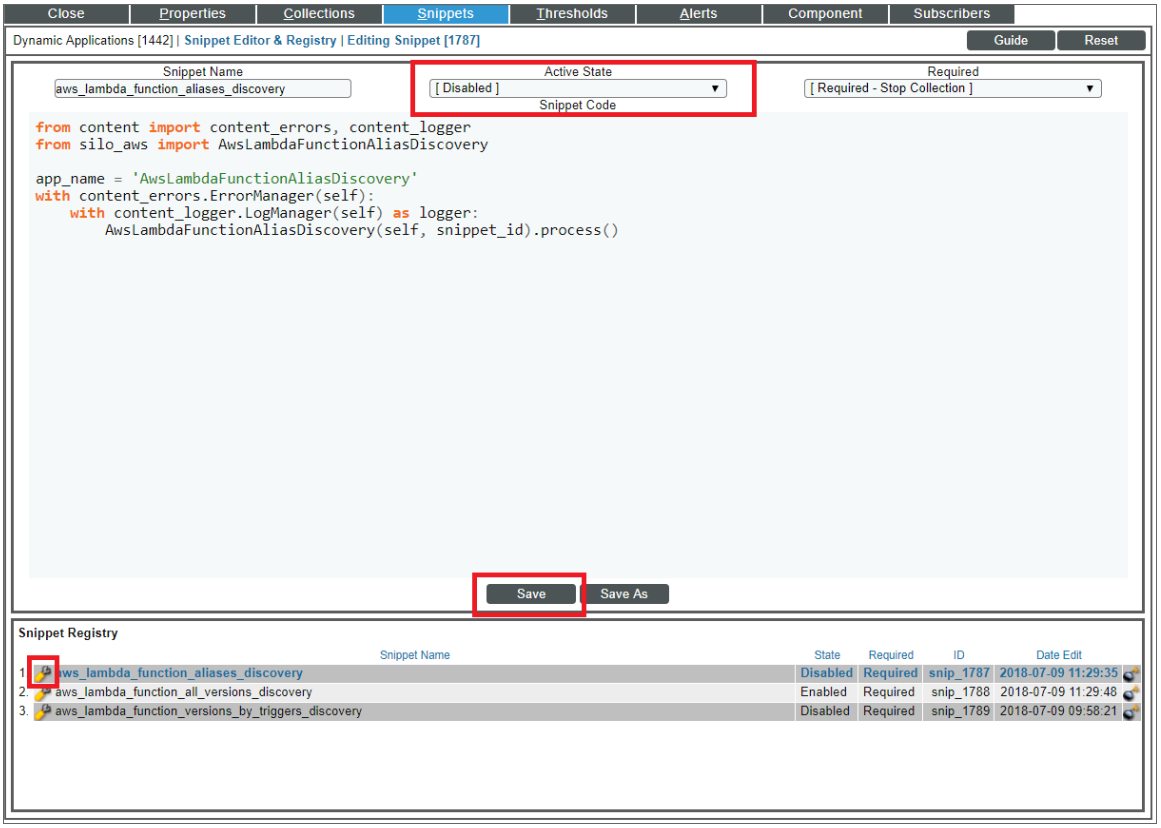
Copyright (c) 2003-2018 ScienceLogic, Inc.

This software is the copyrighted work of ScienceLogic, Inc.
Use of the Software is governed by the terms of the software license agreement, which accompanies or is included with the Software ("License Agreement"). An end user is not permitted to install any Software that is accompanied by or includes a License Agreement, unless he or she first agrees to the License Agreement terms.

4. Click the **[Snippets]** tab. The **Dynamic Applications Snippet Editor & Registry** page appears. The **Snippet Registry** pane includes the following snippets:

   - *aws_lambda_function_aliases_discovery*. When this snippet is enabled, the Dynamic Application discovers all Lambda alias components.
   - *aws_lambda_function_all_versions_discovery*. When this snippet is enabled, the Dynamic Application discovers all Lambda version components.
   - *aws_lambda_function_versions_by_triggers_discovery*. When this snippet is enabled, the Dynamic Application discovers Lambda version components with AWS configurations containing a trigger or those with an alias.

5. One at a time, click the wrench icon (🔧) for each of the snippets, select *Enabled* or *Disabled* in the ***Active State*** field, and then click **[Save]** to enable the appropriate snippet and disable the others.



Dynamic Applications [1442] | Snippet Editor & Registry | Editing Snippet [1787]

Snippet Name: aws_lambda_function_aliases_discovery

Active State: [Disabled]

Required: [Required - Stop Collection]

Snippet Code

```
from content import content_errors, content_logger
from silo_aws import AwsLambdaFunctionAliasDiscovery

app_name = 'AwsLambdaFunctionAliasDiscovery'
with content_errors.ErrorManager(self):
    with content_logger.LogManager(self) as logger:
        AwsLambdaFunctionAliasDiscovery(self, snippet_id).process()
```

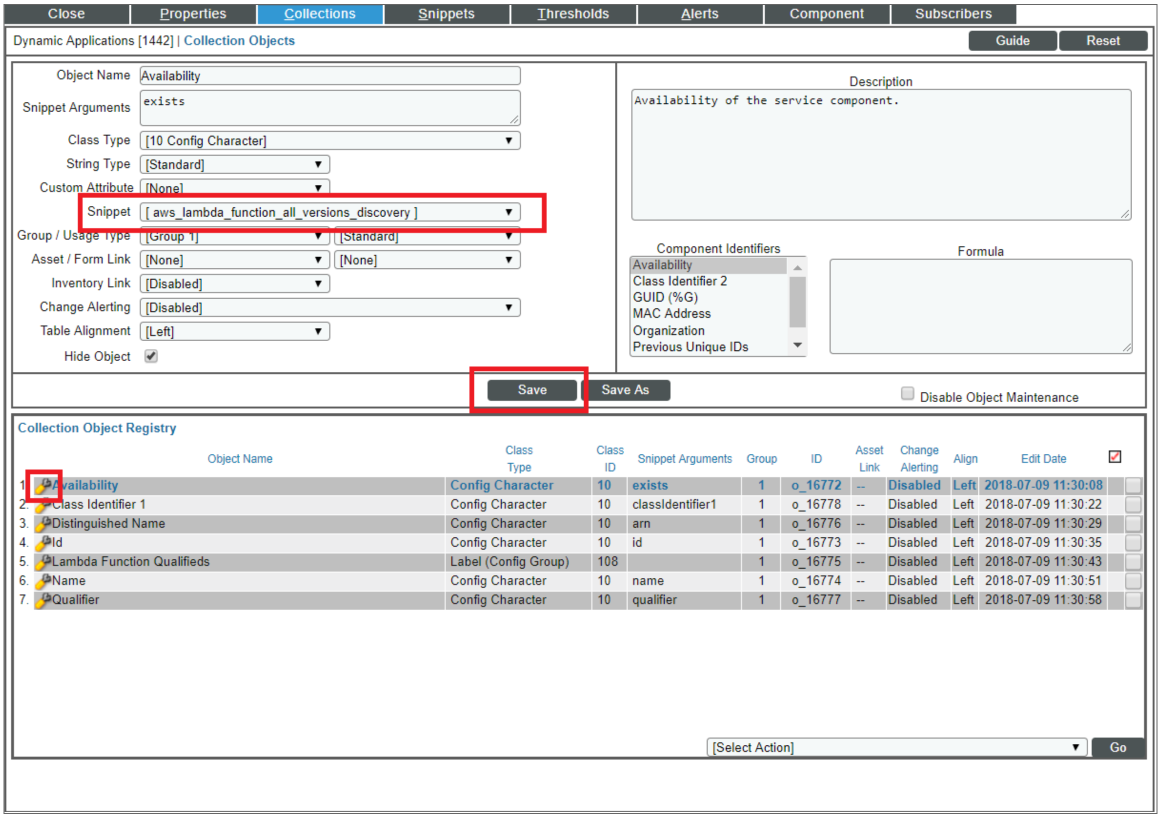
Snippet Registry

	Snippet Name	State	Required	ID	Date Edit
1.	aws_lambda_function_aliases_discovery	Disabled	Required	snip_1787	2018-07-09 11:29:35
2.	aws_lambda_function_all_versions_discovery	Enabled	Required	snip_1788	2018-07-09 11:29:48
3.	aws_lambda_function_versions_by_triggers_discovery	Disabled	Required	snip_1789	2018-07-09 09:58:21

NOTE: You can enable only one of these snippets at a time.

6. Click the **[Collections]** tab. The **Dynamic Applications | Collections Objects** page appears.

7. Click the wrench icon (🔧) for the first Collection Object listed in the **Collection Object Registry** pane, select the snippet you enabled in step 5 in the ***Snippet*** field for that Collection Object, and then click **[Save]**.



Dynamic Applications [1442] | Collection Objects

Object Name	Availability	
Snippet Arguments	exists	
Class Type	[10 Config Character]	
String Type	[Standard]	
Custom Attribute	[None]	
Snippet	[aws_lambda_function_all_versions_discovery]	
Group / Usage Type	[Group 1]	[Standard]
Asset / Form Link	[None]	[None]
Inventory Link	[Disabled]	
Change Alerting	[Disabled]	
Table Alignment	[Left]	
Hide Object	☑	

Description

Availability of the service component.

Component Identifiers

Availability
Class Identifier 2
GUID (%G)
MAC Address
Organization
Previous Unique IDs

Formula

☐ Disable Object Maintenance

Collection Object Registry

	Object Name	Class Type	Class ID	Snippet Arguments	Group	ID	Asset Link	Change Alerting	Align	Edit Date	☑
1.	Availability	Config Character	10	exists	1	o_16772	--	Disabled	Left	2018-07-09 11:30:08	☐
2.	Class Identifier 1	Config Character	10	classIdentifier1	1	o_16778	--	Disabled	Left	2018-07-09 11:30:22	☐
3.	Distinguished Name	Config Character	10	arn	1	o_16776	--	Disabled	Left	2018-07-09 11:30:29	☐
4.	Id	Config Character	10	id	1	o_16773	--	Disabled	Left	2018-07-09 11:30:35	☐
5.	Lambda Function Qualifieds	Label (Config Group)	108		1	o_16775	--	Disabled	Left	2018-07-09 11:30:43	☐
6.	Name	Config Character	10	name	1	o_16774	--	Disabled	Left	2018-07-09 11:30:51	☐
7.	Qualifier	Config Character	10	qualifier	1	o_16777	--	Disabled	Left	2018-07-09 11:30:58	☐

8. Repeat step 7 for all of the remaining Collection Objects listed in the **Collection Object Registry** pane.

9. Click the **[Properties]** tab.

10. In the ***Operational State*** field, select *Enabled*, and then click **[Save]**. This re-enables data collection for the Dynamic Application. The next time discovery is run, new component devices might be discovered and some previously discovered components might become unavailable, depending on how you configured the Dynamic Application.

NOTE: If you configure the "AWS: Lambda Function Qualified Discovery" Dynamic Application to discover Lambda alias or version components and your AWS service includes an API Gateway that triggers a Lambda Function, then the Dynamic Applications in the *Amazon Web Services* PowerPack will create *a device relationship* between that Lambda Function and its corresponding Lambda alias or version component device.

Configuring AWS Integration with Docker

If you have discovered EC2-backed ECS clusters using the *Amazon Web Services* PowerPack, you can optionally use the *Docker* PowerPack to collect container information in addition to what the AWS API provides for the ECS service.

NOTE: This integration does not work with Fargate-backed ECS clusters.

To configure this integration, cURL version 7.40 or later must be installed on the ECS AMI image. For example, the 2018.03 ECS AMI image is compatible is compatible because it includes cURL 7.43.1.

Additionally, you must install the most recent version of the *Docker* PowerPack on your SL1 System and run a discovery session using an SSH credential that will work on the EC2 host(s). This discovery session will discover the EC2 instances that comprise the ECS cluster and align the Docker host Dynamic Applications with those EC2 instances. Optionally, you can merge the EC2 host with the Docker host if you so choose.

NOTE: For more information about the *Docker* PowerPack, including instructions about creating the SSH credential and running discovery, see the ***Monitoring Docker*** manual.

NOTE: ScienceLogic does not recommend enabling and securing the Docker HTTP API when aligning EC2 instances with Docker hosts. Doing so requires you to complete manual steps on each EC2 host. Furthermore, if you use this method and then merge the EC2 host with the Docker host, data collection will fail for all containers that are children of the merged host.

Configuring AWS Integration with Kubernetes

If you are using the AWS EKS service you can optionally use the *Kubernetes* PowerPack to provide visibility into your Kubernetes worker nodes and their associated workloads.

To use the *Kubernetes* PowerPack with the *Amazon Web Services* PowerPack, you must have the following versions of these PowerPacks installed:

- *Amazon Web Services* version 118 or later
- *Kubernetes* version 104 or later

If you are using AWS EKS but do ***not*** want to use this feature, then it is recommended to disable the "AWS EKS Cluster Virtual Discovery" Dynamic Application. To do this:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Dynamic Applications).
2. Search for "AWS EKS" in the ***Dynamic Application Name*** column.
3. Click on the wrench icon (🔧) for the "AWS EKS Cluster Virtual Device Discovery" Dynamic Application and

set the ***Operational State*** dropdown to *Disabled*.

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

Using the *Kubernetes* PowerPack is completely automated on SL1. If the proper credentials have been assigned on AWS and the AWS EKS Cluster, then SL1 will automatically discover the Kubernetes worker nodes and the associated workloads. The following additional components will be automatically created:

1. A new DCM tree root device to represent the Kubernetes cluster. This will be a virtual device of the type "Kubernetes Cluster".
2. A child component of the cluster will be created for each worker node in the cluster. This will be a component device of the type "Kubernetes Node".
3. A child component of the cluster will be created that represents the Namespaces. This will be a component device of the type "Kubernetes Namespace Folder".
4. A child component of the Namespace Folder will be created for each Namespace discovered. This will be a component device of the type "Kubernetes Namespace".
5. A child component of the Namespace will be created for each controller discovered as follows:
   - Kubernetes Daemon Set
   - Kubernetes Deployment

     NOTE: At most only a single component is created to represent a controller. If a deployment and replica set exists, SL1 models only the deployment and replica set info as provided by the deployment component.

   - Kubernetes Job
   - Kubernetes Cronjob
   - Kubernetes Replication Controller
   - Kubernetes Replication Set
   - Kubernetes Stateful Set
6. A child component of the cluster will be created for each ingress defined. This will be a component device of the type "Kubernetes: Ingress".

For SL1 to automatically discovery the EKS cluster, you must perform the following steps:

NOTE: When logging into the Kubernetes cluster, ensure that the AWS credentials that `kubectl` is using are already authorized for your cluster. The IAM user that created the cluster has these permissions by default.

1. *Enable the Prometheus Metrics Server*. AWS EKS does not have the metrics server enabled by default. This is highly recommended as it will provide CPU and memory utilization metrics for both the worker nodes as well as the pods.

NOTE: SL1 automatically aggregates the CPU and memory utilization for pods and presents data at the controller level.

2. *Define the cluster role* needed by SL1 so that it can access the necessary APIs. This is done on the EKS Cluster.
3. *Define the ClusterRoleBinding*. This is done on the EKS Cluster.
4. *Map the IAM user or role to the RBAC role and groups* using the aws-auth ConfigMap. This is done on the EKS Cluster.

Enabling the Prometheus Metrics Server

The Prometheus Metrics Server is required to provide CPU and memory utilization for pods and for nodes. The metrics server can be easily installed on Kubernetes clusters with the following:

```
kubectl apply -f https://github.com/kubernetes-sigs/metrics-
server/releases/latest/download/components.yaml
```

To verify that the server is running, execute the command:

```
kubectl get deployment metrics-server -n kube-system
```

The following output will show that the metrics server is running:

```
NAME            READY  UP-TO-DATE  AVAILABLE  AGE
 metrics-server   1/1    1           14h
```

Define the Cluster Role

The cluster role defines the minimum permissions that SL1 needs to monitor the Kubernetes cluster. ClusterRole is used as it provides access to all namespaces. Since SL1 is directly monitoring the Kubernetes cluster via the Kuberneties API, this role's permissions need to be defined on the cluster itself.

To define the cluster role in Kubernetes:

1. Log in to the EKS cluster with the same user or role that created the cluster.
2. Create a new file called `SL1_cluster_role.yaml` and cut and paste the following text into that file:

```
adpiVersion: rbac.authorization.k8s.io/v1
 kind: ClusterRole
 metadata:
   name: eks-readonly-clusterrole
rules:
- apiGroups:
  - ""
  resources:
  - nodes
  - namespaces
  - pods
  - replicationscontrollers
  - events    {
  - persistentvolumes
  - persistentvolumeclaims
  - componentstatuses
  - services
  verbs:
  - get
  - list
  - watch
-apiGroups:
  - apps
  resources:
  - deployments
  - daemonsets
  - statefulsets
  - replicasets
  verbs:
  - get
  - list
  - watch
- apiGroups:
  - batch
  resources:
  - jobs
  - cronjobs
  verbs:
  - get
  - list
  - watch
- apiGroups:
  - metrics.k8s.io
  resources:
  - nodes
  - pods
  verbs:
  - get
  - list
  - watch
- apiGroups:
  - networking.k8s.io
  resources:
  - ingresses
  verbs:
  - get
  - list
  - watch
- apiGroups:
  - autoscaling
  resources:
  - horizontalpodautoscalers
  verbs:
  - get
  - list
  - watch
```

The above file defines the minimum read-only permissions needed for SL1 to monitor Kubernetes.

3. Once the file is defined, execute the following command to apply the file:

   ```
   kubect1 apply -f cluster_role.yaml
   ```

Define the ClusterRoleBinding

Once the role is defined, it must be bound to users, groups, or services. This is done by defining a ClusterRoleBinding:

1. Log in to the EKS cluster with the same user or role that created the cluster.
2. Create a new file called `SL1_ClusterRoleBinding.yaml` and cut and paste the following text into that file:

```
apiVersion: rbac.authorization.k8s.io/v1
 kind: ClusterRoleBinding
 metadata:
  name: eks-cluster-role-binding
subjects:
 - kind: User
   name: Sciencelogic-Monitor
   apiGroup: rbac.authorization.k8s.io
roleref:
 kind: ClusterRole
 name: eks-readonly-clusterrole
 apiGroup: rbac.authorization.k8s.io
```

3. Once the file is created, apply the ClusterRoleBinding by executing the following command:

   ```
   kubectl apply -f SL1_ClusterRoleBinding.yaml
   ```

NOTE: Under subjects, "name: Sciencelogic-Monitor" defines the Kubernetes user and it must match the username field in the config map shown below.

NOTE: Under roleRef, "name: eks-readonly-clusterrole" must match the name defined in the cluster role.

Map the IAM User or Role to the Kubernetes RBAC Role

After defining the ClusterRoleBinding, you must map the AWS credentials that SL1 is using to the username created above in the `SL1_ClusterRoleBinding.yaml` file. To do this, perform the following steps:

1. Enter the `kubectl edit -n kube-system configmap/aws-auth` command. This will bring up the `configmap`. How the `configmap` is updated depends on what type of IAM was used to discover SL1.

NOTE: If the `configmap/aws-auth` does not exist, follow the procedures defined in https://docs.aws.amazon.com/eks/latest/userguide/add-user-role.html

Example 1

If SL1 has discovered your AWS organization using assume role, add the following text to the `mapRoles:` section in the `configmap`:

```
- groups:
   - eks-cluster-role-binding
   rolearn:arn:aws:iam::<Account number that hosts the Kubernetes cluster-
>:role/Sciencelogic-Monitor
   username: Sciencelogic-Monitor
```

NOTE: If `mapRoles` does not exist, then you can add the `mapRoles` section to the `configmap`.

The text should appear in the `configmap` as the highlighted text below:

```
# Please edit the object below. Lines beginning with a '#' will be ignored,
 # and an emty file will abort the edit. If an error occurs while saving, this fiel
will be
 # reopened with the relevant failures
 #
apiVersion: v1
data:
 mapRoles: |
  - groups:
    - system:bootstrappers
    - system:nodes
    rolearn: arn:aws-us-gov:iam::<account number>:role/eksctl-eks-cluster-test-
friday-nod-NodeInstanceRole-6VCMS669U9NA
    username: system:node:{{EC2PrivateDNSName}}
   - groups:
     - eks-cluster-role-binding
     rolearn: arn:aws:iam::<account number>:role/Sciencelogic-Monitor
     username: Sciencelogic-Monitor
kind: ConfigMap
metadata:
 creationTimestamp: "2021-07-30T20:43:55Z"
 name: aws-auth
 namespace: kube-system
 resourceVersion: "173718"
 selfLink: /api/v1/namespaces/kube-system/configmaps/aws-auth
 uid: d1bcdafd-fc40-44e6-96d4-9a079b407d06
```

Example 2

If SL1 has been discovered with a single IAM key for the account, add the following text to the `mapUsers:` section of the `configmap`:

```
- groups:
   - eks-cluster-role-binding
   userarn:arn:aws:iam::<Account number that hosts the Kubernetes
```

```
cluster>:user/<Name of the user associated with the IAM key
   username: Sciencelogic-Monitor
```

The text should appear in the `configmap` as the highlighted text below:

```
# Please edit the object below. Lines beginning with a '#' will be ignored,
 # and an emty file will abort the edit. If an error occurs while saving, this fiel
will be
 # reopened with the relevant failures
 #
apiVersion: v1
data:
 mapRoles: |
  - groups:
    - system:bootstrappers
    - system:nodes
    rolearn: arn:aws-us-gov:iam::<account number>:role/eksctl-eks-cluster-test-
friday-nod-NodeInstanceRole-6VCMS669U9NA
    username: system:node:{{EC2PrivateDNSName}}
 mapUsers: |
  - groups:
    - eks-cluster-role-binding
    userarn: arn:aws:iam::<account number>:user/<username>
    username: Sciencelogic-Monitor
kind: ConfigMap
metadata:
 creationTimestamp: "2021-07-30T20:43:55Z"
 name: aws-auth
 namespace: kube-system
 resourceVersion: "173718"
 selfLink: /api/v1/namespaces/kube-system/configmaps/aws-auth
 uid: d1bcdafd-fc40-44e6-96d4-9a079b407d06
```

NOTE: In `userarn: arn:aws:iam::<account number>:user/<username>`, the username is the userarn that SL1 is using to monitor the Kubernetes cluster.

NOTE: Under `mapUsers`, the `username:` is the name used in the ClusterRoleBinding.

Amazon API Throttling Events

By default, SL1 will use the Collector Group aligned with the root AWS virtual device to retrieve data from AWS devices and services.

If SL1 must collect data from a large set of AWS devices and services, SL1 might generate Notify events with a message ending in the text "Retry #1-10 Sleeping: ... seconds". SL1 generates these events when the Amazon API throttles collection in response to a large number of requests to the API. Even though SL1 is generating Notify "Retry" events, SL1 is still collecting data from AWS. This issue commonly occurs when a specific Amazon data center edge is close to capacity.

If SL1 generates the Minor event "Collection missed on <device> on 5 minute poll", this indicates that SL1 was unable to retrieve that specific datum from the Amazon cloud during the most recent five-minute polling cycle. If you frequently see the "Collection missed" event across your cloud, you must contact Amazon support to whitelist the IP address of your Data Collector. This will prevent further throttling from occurring.

Support for AWS China Regions

Currently, the only method of discovery for AWS China Regions is the ***Manual Discovery*** method. In this case, the ***Embed Value %1*** field in the ***SOAP/XML credential*** must contain the specific Chinese region to be monitored.

Support for AWS GovCloud Regions

AWS GovCloud Regions can be discovered using all discovery methods as defined below:

- For an individual account using the ***Manual Discovery*** method, type the name of the AWS GovCloud region in the ***Embed Value %1*** field in the ***SOAP/XML credential***.
- For those using one of the discovery methods with AssumeRole, enter one of the following URLs in the ***URL*** field of the ***SOAP/XML credential*** to specify the specific government region:
    - https://organizations.us-gov-west-1.amazonaws.com
    - https://organizations.us-gov-east-1.amazonaws.com

NOTE: All examples shown are for commercial AWS accounts. When AWS Gov is being monitored, the JSON data that refers to ARN will need to be modified from "aws" to "aws-us-gov". For example: `Resource": "arn:aws:iam::<account number>:role/Sciencelogic-Monitor` would need to be `Resource": "arn:aws:iam-us-gov::<account number>:role/Sciencelogic-Monitor`

Minimum Permissions Needed to Monitor Your AWS Accounts

The following table displays the minimum permissions required for Dynamic Applications in the *Amazon Web Services* PowerPack to collect data.

Service	Actions	
API Gateway	Read	GET
CloudFront	List	ListDistributions ListInvalidations ListStreamingDistributions
	Read	GetDistribution GetStreamingDistribution
CloudTrail	List	DescribeTrails
	Read	GetTrailStatus
CloudWatch	List	ListMetrics
	Read	DescribeAlarmHistory DescribeAlarms GetMetricData GetMetricStatistics
Direct Connect	Read	DescribeConnections DescribeTags DescribeVirtualInterfaces
DynamoDB	List	ListTables
	Read	DescribeTable
EC2	List	DescribeAvailabilityZones DescribeImages DescribeInstances DescribeNatGateways DescribeRegions DescribeRouteTables DescribeSecurityGroups DescribeSubnets DescribeSnapshots DescribeTransitGatewayRouteTables DescribeTransitGateways DescribeTransitGatewayAttachments DescribeVolumes DescribeVpcPeeringConnections DescribeVpcs DescribeVpnGateways
	Read	DescribeVpnConnections
EC2 Auto Scaling	List	DescribeAutoScalingGroups DescribeAutoScalingInstances DescribeLaunchConfigurations
EFS	List	DescribeFileSystems
Elastic Beanstalk	List	DescribeEnvironments
	Read	DescribeConfigurationSettings DescribeEnvironmentResources
Elastic Container	List	ListClusters

Service	Actions	
Services (ECS)		ListContainerInstances ListServices ListTasks
	Read	DescribeClusters DescribeContainerInstances DescribeServices DescribeTaskDefinition DescribeTasks
ElasticCache	List	DescribeCacheClusters
Elastic Kubernetes Service (EKS)	List	ListClusters
	Read	DescribeClusters
ELB	List	DescribeLoadBalancers
	Read	DescribeTags
ELB v2	Read	DescribeListeners DescribeLoadBalancers DescribeTags DescribeTargetGroups DescribeTargetHealth
EMR	List	ListClusters
	Read	ListInstances
Glacier	List	ListTagsForVault ListVaults
	Read	GetVaultNotifications
IAM	Read	GetUser GetAccountAuthorizationDetails
IoT	List	ListThings ListTagsForResource
	Read	DescribeThing
Key Management Service (KMS)	List	ListKeys ListAliases
	Read	DescribeKey ListResourceTags
Lambda	List	ListFunctions ListAliases ListEventSourceMappings
	Read	ListTags
Lightsail	List	GetBundles GetRegions
	Read	GetInstanceMetricData GetInstances
OpsWorks	List	DescribeInstances

Service	Actions	
		DescribeStacks
RDS	List	DescribeDBClusters DescribeDBInstances DescribeDBSubnetGroups
	Read	ListTagsForResource
Redshift	List	DescribeClusters
	Read	DescribeLoggingStatus
Route 53	List	GetHostedZone ListHealthChecks ListHostedZones ListResourceRecordSets
S3	List	ListAllMyBuckets ListBucket
	Read	GetBucketLocation GetBucketLogging GetBucketTagging GetBucketWebsite GetObject (Restrict access to specific resources of Elastic Beanstalk. For instance, Bucket name: elasticbeanstalk-*, Any Object name.)
Shield	List	ListAttacks ListProtections
	Read	DescribeEmergencyContactSettings GetSubscriptionState
Simple Email Service (SES)	List	ListIdentities
Simple Notification Service (SES)	List	ListTopics ListSubscriptions
SQS	List	ListQueues
	Read	GetQueueAttributes
Storage Gateway	List	ListGateways ListVolumes
STS	Read	GetCallerIdentity
WAF	List	ListWebACLs
	Read	GetRateBasedRule GetRule GetRuleGroup GetWebACL
WAF Regional	List	ListResourcesForWebACL ListWebACLs
	Read	GetRateBasedRule

Service	Actions	
		GetRule GetRuleGroup GetWebACL

To create the Minimum Permission policy:

1. Go to the AWS console and select **IAM > Policies > Create Policy**. Select **JSON** and cut and paste the following JSON document:

```
{
   "Statement": [
       {
               "Action": [
                       "apigateway:GET",
                       "autoscaling:DescribeAutoScalingGroups",
                       "autoscaling:DescribeAutoScalingInstances",
                       "autoscaling:DescribeLaunchConfigurations",
                       "cloudfront:GetDistribution",
                       "cloudfront:ListDistributions",
                       "cloudfront:ListInvalidations",
                       "cloudfront:ListStreamingDistributions",
                       "cloudtrail:DescribeTrails",
                       "cloudtrail:GetTrailStatus",
                       "cloudwatch:DescribeAlarmHistory",
                       "cloudwatch:DescribeAlarms",
                       "cloudwatch:GetMetricData",
                       "cloudwatch:GetMetricStatistics",
                       "cloudwatch:ListMetrics",
                       "config:GetDiscoveredResourceCounts",
                       "directconnect:DescribeConnections",
                       "directconnect:DescribeTags",
                       "directconnect:DescribeVirtualInterfaces",
                       "dynamodb:DescribeTable",
                       "dynamodb:ListTables",
                       "ec2:DescribeAvailabilityZones",
                       "ec2:DescribeImages",
                       "ec2:DescribeInstances",
                       "ec2:DescribeNatGateways",
                       "ec2:DescribeRegions",
                       "ec2:DescribeRouteTables",
                       "ec2:DescribeSecurityGroups",
                       "ec2:DescribeSnapshots",
                       "ec2:DescribeSubnets",
                       "ec2:DescribeTransitGatewayAttachments",
                       "ec2:DescribeTransitGatewayRouteTables",
                       "ec2:DescribeTransitGateways",
                       "ec2:DescribeVolumes",
                       "ec2:DescribeVpcPeeringConnections",
                       "ec2:DescribeVpcs",
                       "ec2:DescribeVpnConnections",
                       "ec2:DescribeVpnGateways",
                       "ecs:DescribeClusters",
                       "ecs:DescribeContainerInstances",
                       "ecs:DescribeServices",
                       "ecs:DescribeTaskDefinition",
                       "ecs:DescribeTasks",
                       "ecs:ListClusters",
                       "ecs:ListContainerInstances",
                       "ecs:ListServices",
                       "ecs:ListTasks",
                       "eks:DescribeCluster",
                       "eks:ListClusters",
                       "elasticache:DescribeCacheClusters",
                       "elasticbeanstalk:DescribeConfigurationSettings",
                       "elasticbeanstalk:DescribeEnvironmentResources",
                       "elasticbeanstalk:DescribeEnvironments",
                       "elasticfilesystem:DescribeFileSystems",
                       "elasticloadbalancing:DescribeListeners",
                       "elasticloadbalancing:DescribeLoadBalancers",
                       "elasticloadbalancing:DescribeTags",
                       "elasticloadbalancing:DescribeTargetGroups",
                       "elasticloadbalancing:DescribeTargetHealth",
                       "elasticmapreduce:ListClusters",
                       "elasticmapreduce:ListInstances",
                       "glacier:GetVaultNotifications",
                       "glacier:ListTagsForVault",
                       "glacier:ListVaults",
                       "iam:GetAccountAuthorizationDetails",
                       "iam:GetUser",
                       "iot:DescribeThing",
                       "iot:ListTagsForResource",
                       "iot:ListThings",
                       "kms:DescribeKey",
                       "kms:ListAliases",
                       "kms:ListKeys",
                       "kms:ListResourceTags",
                       "lambda:GetAccountSettings",
                       "lambda:ListAliases",
                       "lambda:ListEventSourceMappings",
                       "lambda:ListFunctions",
                       "lambda:ListTags",
                       "lightsail:GetBundles",
                       "lightsail:GetInstanceMetricData",
                       "lightsail:GetInstances",
                       "lightsail:GetRegions",
                       "opsworks:DescribeInstances",
                       "opsworks:DescribeStacks",
                       "rds:DescribeDBClusters",
                       "rds:DescribeDBInstances",
                       "rds:DescribeDBSubnetGroups",
                       "rds:ListTagsForResource",
                       "redshift:DescribeClusters",
                       "redshift:DescribeLoggingStatus",
                       "route53:GetHostedZone",
                       "route53:ListHealthChecks",
                       "route53:ListHostedZones",
                       "route53:ListResourceRecordSets",
                       "s3:GetBucketLocation",
                       "s3:GetBucketLogging",
                       "s3:GetBucketTagging",
                       "s3:GetBucketWebsite",
                       "s3:GetObject",
                       "s3:ListAllMyBuckets",
                       "s3:ListBucket",
                       "ses:ListIdentities",
                       "shield:DescribeEmergencyContactSettings",
                       "shield:GetSubscriptionState",
                       "shield:ListAttacks",
                       "shield:ListProtections",
                       "sns:ListSubscriptions",
                       "sns:ListTopics",
                       "sqs:GetQueueAttributes",
                       "sqs:ListQueues",
                       "ssm:GetParameters",
                       "storagegateway:ListGateways",
                       "storagegateway:ListVolumes",
                       "sts:GetCallerIdentity",
                       "tag:Get*",
                       "waf-regional:GetRateBasedRule",
                       "waf-regional:GetRule",
                       "waf-regional:GetRuleGroup",
                       "waf-regional:GetWebACL",
                       "waf-regional:ListResourcesForWebACL",
                       "waf-regional:ListWebACLs",
                       "waf:GetRateBasedRule",
                       "waf:GetRule",
                       "waf:GetRuleGroup",
                       "waf:GetWebACL",
                       "waf:ListWebACLs"
               ],
               "Effect": "Allow",
               "Resource": "*",
               "Sid": "VisualEditor0"
          }
   ],
   "Version": "2012-10-17"
}
```

2. Click **[Next: Tags]**. If applicable, enter your Tags.
3. Click **[Next: Review]**. Name the policy "SL1MinimumPermissions" and click **[Create Policy]**.

This policy needs to be available in each account that is to be monitored and will be referenced in the following sections.

Testing the AWS Credential

> **NOTE:** The Credential Test is for use with the *Manual Discovery* method only.

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

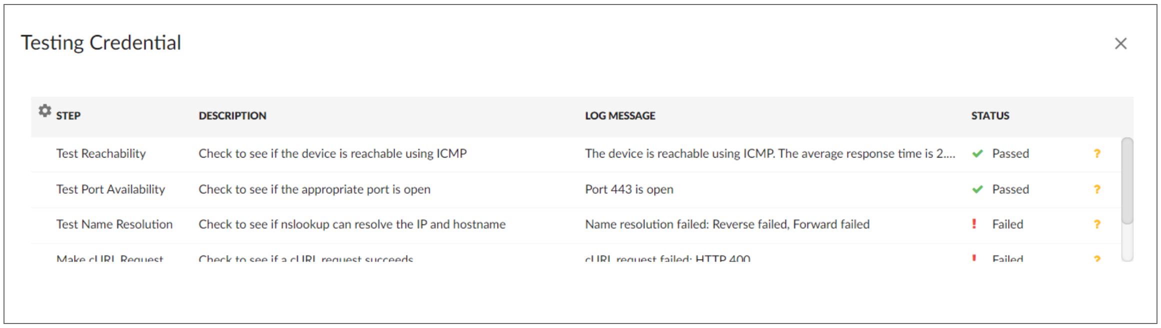
The AWS Credential Test can be used to test a SOAP/XML credential for monitoring AWS using the Dynamic Applications in the *Amazon Web Services* PowerPack. The AWS Credential Test performs the following steps:

- ***Test Reachability***. Performs an ICMP ping request to the URL for the EC2 service in the region specified in the credential. If a region is not specified in the credential, the us-east-1 region is used.
- ***Test Port Availability***. Performs an NMAP request to TCP port 443 on the URL for the EC2 service in the region specified in the credential. If a region is not specified in the credential, the us-east-1 region is used.
- ***Test Name Resolution***. Performs an nslookup request on the URL for the EC2 service in the region specified in the credential. If a region is not specified in the credential, the us-east-1 region is used.
- ***Make connection to AWS account***. Attempts to connect to the AWS service using the account specified in the credential.
- ***Scan AWS services***. Verifies that the account specified in the credential has access to the services.

> NOTE: The AWS Credential Test does not support the testing of credentials that connect to AWS through a proxy server.

To test the AWS credential:

1. Go to the **Credentials** page (Manage > Credentials).
2. Locate the credential you wish to test, select the **Actions** button (⋯) next to it and click *Test*.
3. The **Credential Test Form** modal page appears. Fill out the following fields on this page:
    - ***Credential***. This field is read-only and displays the name of the credential you selected.
    - ***Select Credential Test***. Select **AWS Credential Test**.
    - ***Collector***. Select the All-In-One Appliance or Data Collector that will run the test.
    - ***IP or Hostname to Test***. Enter a valid IP address.
4. Click the **[Run Test]** button to run the credential test. The **Testing Credential** window appears:



Testing Credential

STEP	DESCRIPTION	LOG MESSAGE	STATUS	
Test Reachability	Check to see if the device is reachable using ICMP	The device is reachable using ICMP. The average response time is 2....	✓ Passed	?
Test Port Availability	Check to see if the appropriate port is open	Port 443 is open	✓ Passed	?
Test Name Resolution	Check to see if nslookup can resolve the IP and hostname	Name resolution failed: Reverse failed, Forward failed	! Failed	?
Make cURL Request	Check to see if a cURL request succeeds	cURL request failed: HTTP 400	! Failed	?

The **Testing 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 execution of the credential test.
- ***Status***. Whether the result of this step indicates the credential and/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 and/or the network environment if the step has a status of "Failed".

Testing the AWS Credential in the SL1 Classic User Interface

NOTE: The Credential Test is for use with the *Manual Discovery* method only.

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

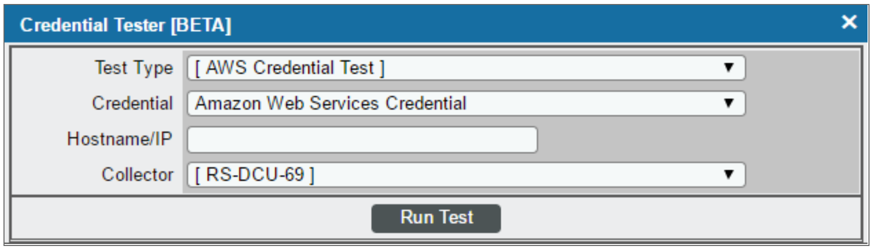
The AWS Credential Test can be used to test a SOAP/XML credential for monitoring AWS using the Dynamic Applications in the *Amazon Web Services* PowerPack. The AWS Credential Test performs the following steps:

- ***Test Reachability***. Performs an ICMP ping request to the URL for the EC2 service in the region specified in the credential. If a region is not specified in the credential, the us-east-1 region is used.
- ***Test Port Availability***. Performs an NMAP request to TCP port 443 on the URL for the EC2 service in the region specified in the credential. If a region is not specified in the credential, the us-east-1 region is used.
- ***Test Name Resolution***. Performs an nslookup request on the URL for the EC2 service in the region specified in the credential. If a region is not specified in the credential, the us-east-1 region is used.
- ***Make connection to AWS account***. Attempts to connect to the AWS service using the account specified in the credential.
- ***Scan AWS services***. Verifies that the account specified in the credential has access to the services.

NOTE: The AWS Credential Test does not support the testing of credentials that connect to AWS through a proxy server.

To test the AWS credential:

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



Credential Tester [BETA]

Test Type: [AWS Credential Test]

Credential: Amazon Web Services Credential

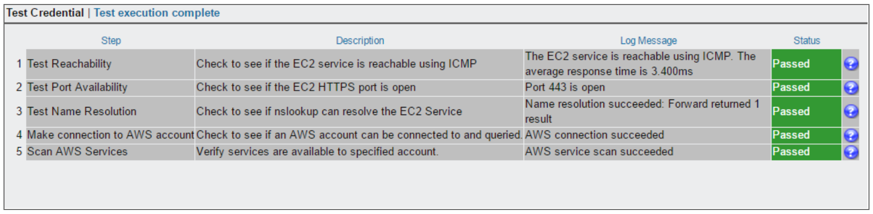
Hostname/IP:

Collector: [RS-DCU-69]

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***. Leave this field blank.
- ***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:



Test Credential | Test execution complete

	Step	Description	Log Message	Status	
1	Test Reachability	Check to see if the EC2 service is reachable using ICMP	The EC2 service is reachable using ICMP. The average response time is 3.400ms	Passed	?
2	Test Port Availability	Check to see if the EC2 HTTPS port is open	Port 443 is open	Passed	?
3	Test Name Resolution	Check to see if nslookup can resolve the EC2 Service	Name resolution succeeded: Forward returned 1 result	Passed	?
4	Make connection to AWS account	Check to see if an AWS account can be connected to and queried.	AWS connection succeeded	Passed	?
5	Scan AWS Services	Verify services are available to specified account.	AWS service scan succeeded	Passed	?

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".

Discovering Amazon Web Services

SL1 currently supports the following methods to discover your AWS accounts:

- *Manual Discovery*. Requires the creation of a virtual device, manual alignment of Dynamic Applications, and an IAM key. This process needs to be repeated for each AWS account.
- *Automated Discovery using Assume Role with single IAM key from Master Account*. Provides an automated mechanism to discover all your AWS accounts within an organization using a single IAM key. This is the recommended method of discovery when your Data Collector is not an EC2 instance.
- *Automated Discovery when the Data Collector runs as an EC2 instance*. Provides a fully automated mechanism to discover all your AWS accounts when your Data Collectors are running as EC2 instances. SL1 does not need any AWS credentials in this case. This is the recommended approach when your Data Collectors are EC2 instances.
- *AWS Guided Discovery*. Uses a guided workflow in SL1. This method is recommended when you want to use a separate IAM key for each AWS account. The guided workflow provides a more user-friendly version of the manual process.

Before determining your method of discovery, it is recommended to define the minimum permissions policy in AWS. This policy defines the minimum permissions needed to monitor all AWS services and is needed regardless of which of the above methods is used.

Manual Discovery

Manual discovery is used to discover a single AWS account at a time and requires an IAM key for the account.

NOTE: Using one of the Assume Role methods of discovery is recommended.

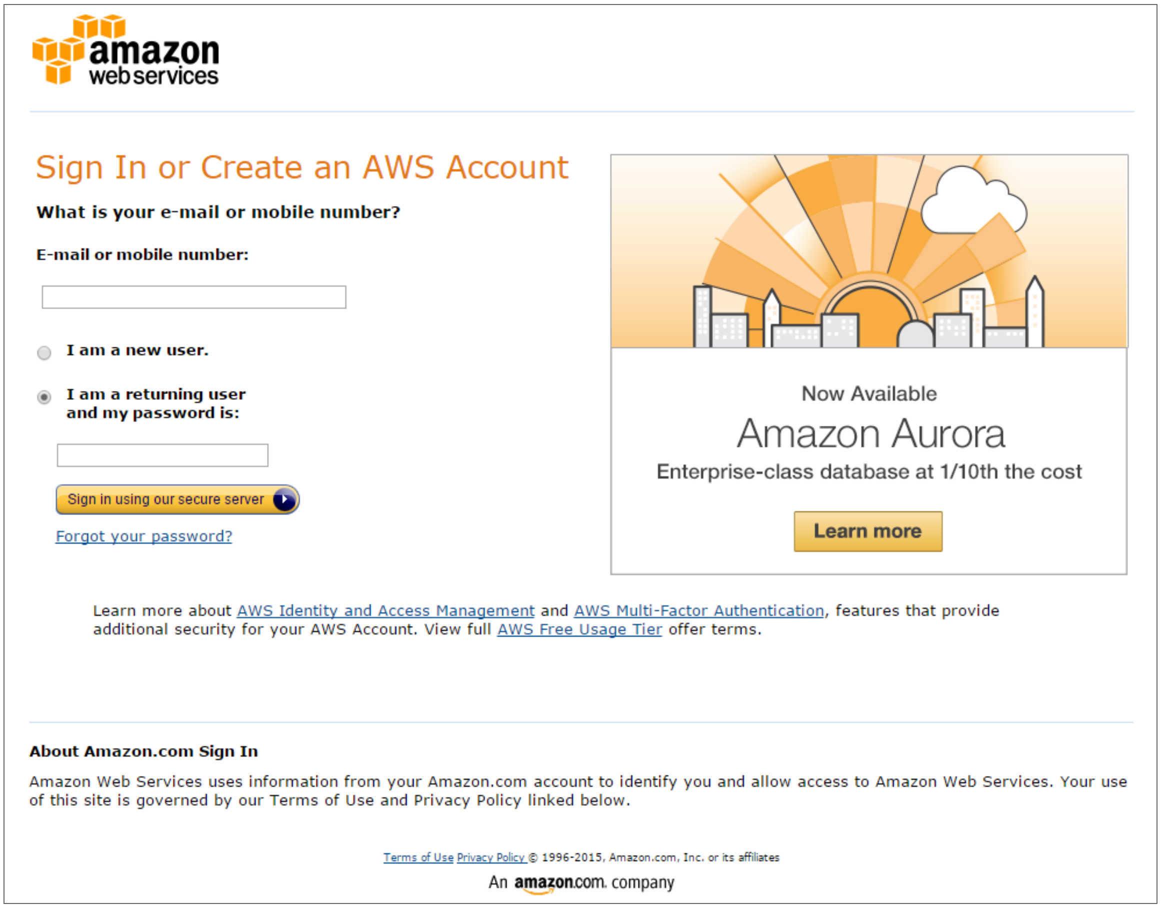
The process consists of the following steps:

1. *Configure a user in the AWS Account*
2. *Configure the SL1 Credential*
3. *Create a Virtual Device*
4. *Align the Discovery Dynamic Application*

Configuring a User in AWS

To create a read-only user account in AWS, perform the following steps:

1. Open a browser session and go to aws.amazon.com.
2. Click **[My Account]** and then select *AWS Management Console*. If you are not currently logged in to the AWS site, you will be prompted to log in:



Sign In or Create an AWS Account

What is your e-mail or mobile number?

E-mail or mobile number:

○ **I am a new user.**

● **I am a returning user and my password is:**

Sign in using our secure server

Forgot your password?

Now Available

Amazon Aurora

Enterprise-class database at 1/10th the cost

Learn more

Learn more about AWS Identity and Access Management and AWS Multi-Factor Authentication, features that provide additional security for your AWS Account. View full AWS Free Usage Tier offer terms.

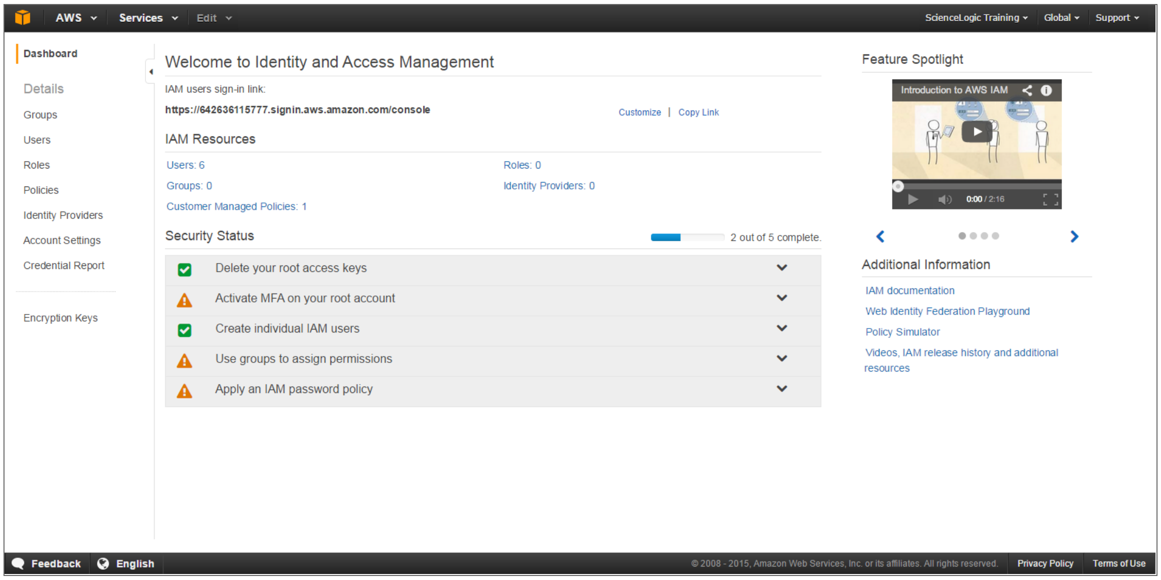
About Amazon.com Sign In

Amazon Web Services uses information from your Amazon.com account to identify you and allow access to Amazon Web Services. Your use of this site is governed by our Terms of Use and Privacy Policy linked below.

Terms of Use Privacy Policy © 1996-2015, Amazon.com, Inc. or its affiliates

An amazon.com. company

3. In the **AWS Management Console**, under the **Security & Identity** heading, click **[Identity & Access Management]**.
4. After logging in, the **Identity & Access Management Dashboard** page appears:



Welcome to Identity and Access Management

IAM users sign-in link:
https://642636115777.signin.aws.amazon.com/console

IAM Resources

Users: 6
Roles: 0
Groups: 0
Identity Providers: 0
Customer Managed Policies: 1

Security Status — 2 out of 5 complete.

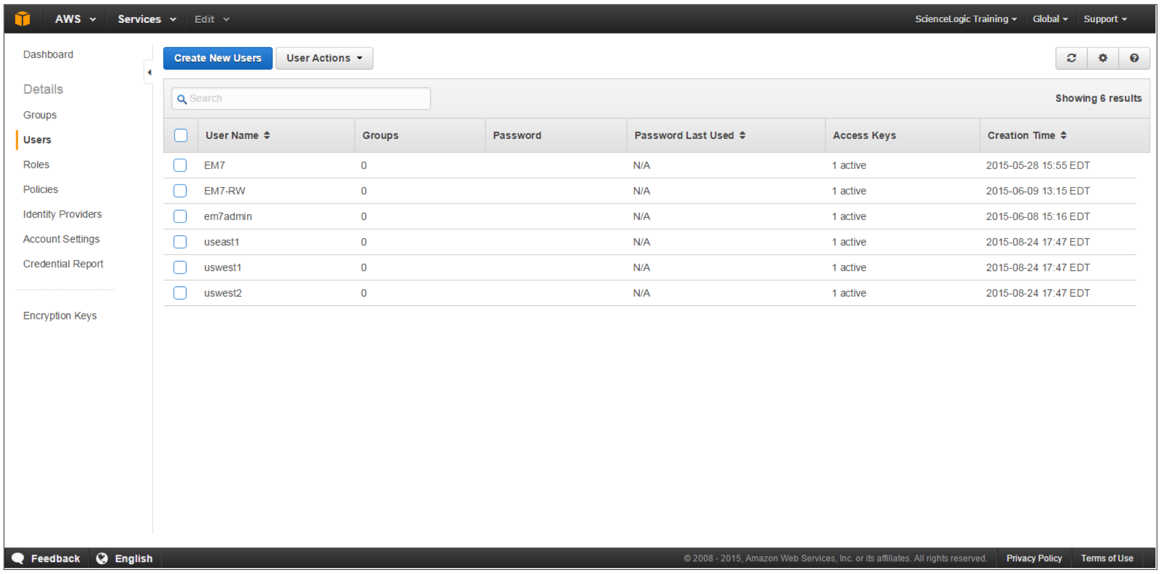
- ✓ Delete your root access keys
- ⚠ Activate MFA on your root account
- ✓ Create individual IAM users
- ⚠ Use groups to assign permissions
- ⚠ Apply an IAM password policy

Additional Information

- IAM documentation
- Web Identity Federation Playground
- Policy Simulator
- Videos, IAM release history and additional resources

© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.

5. To create a user account for SL1, click **[Users]** on the Dashboard menu.



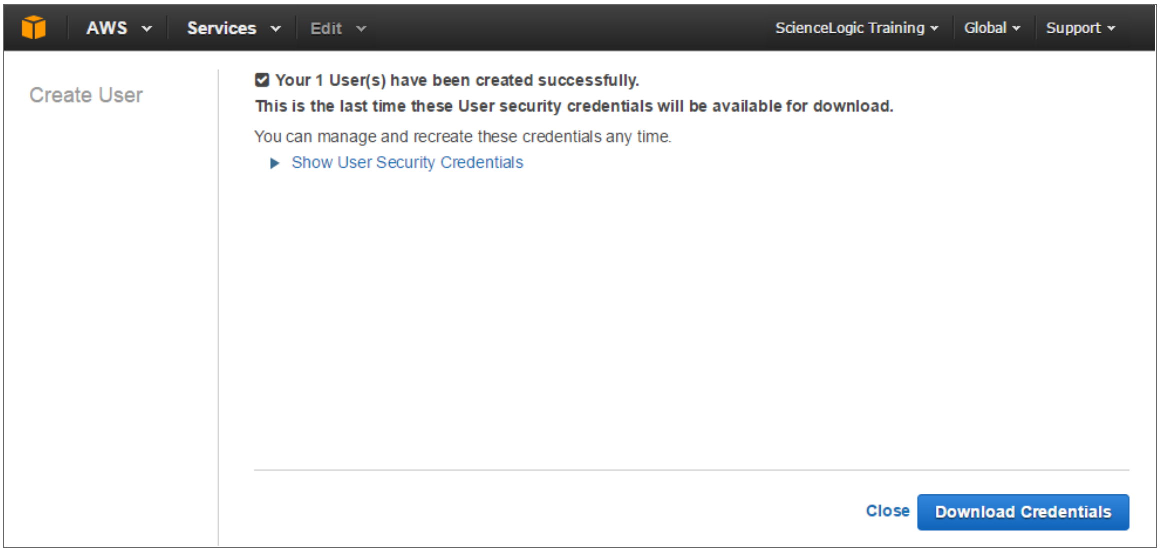
Showing 6 results

□	User Name	Groups	Password	Password Last Used	Access Keys	Creation Time
□	EM7	0		N/A	1 active	2015-05-28 15:55 EDT
□	EM7-RW	0		N/A	1 active	2015-06-09 13:15 EDT
□	em7admin	0		N/A	1 active	2015-06-08 15:16 EDT
□	useast1	0		N/A	1 active	2015-08-24 17:47 EDT
□	uswest1	0		N/A	1 active	2015-08-24 17:47 EDT
□	uswest2	0		N/A	1 active	2015-08-24 17:47 EDT

© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.

6. Click the **[Create New Users]** button.
7. Enter a username for the new user, e.g. "SL1", and make sure the ***Generate an access key for each user*** checkbox is selected.

8. Click the **[Create]** button to generate your user account. The **Create User** page appears:



☑ **Your 1 User(s) have been created successfully.**

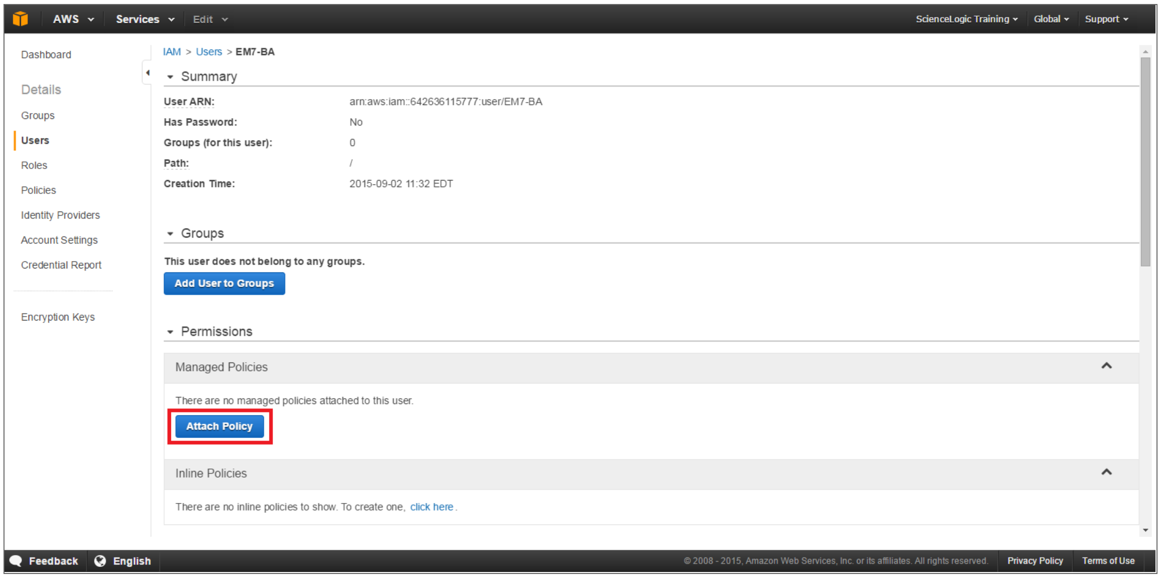
This is the last time these User security credentials will be available for download.

You can manage and recreate these credentials any time.

▶ Show User Security Credentials

9. Click the **[Download Credentials]** button to save your Access Key ID and Secret Key as a CSV (comma-separated value) text file, and then click **[Close]**.

10. After creating a user, you must assign it a set of permissions policies. Click the username of the user account you created. The user's account information appears:



User ARN: arn:aws:iam::642636115777:user/EM7-BA
Has Password: No
Groups (for this user): 0
Path: /
Creation Time: 2015-09-02 11:32 EDT

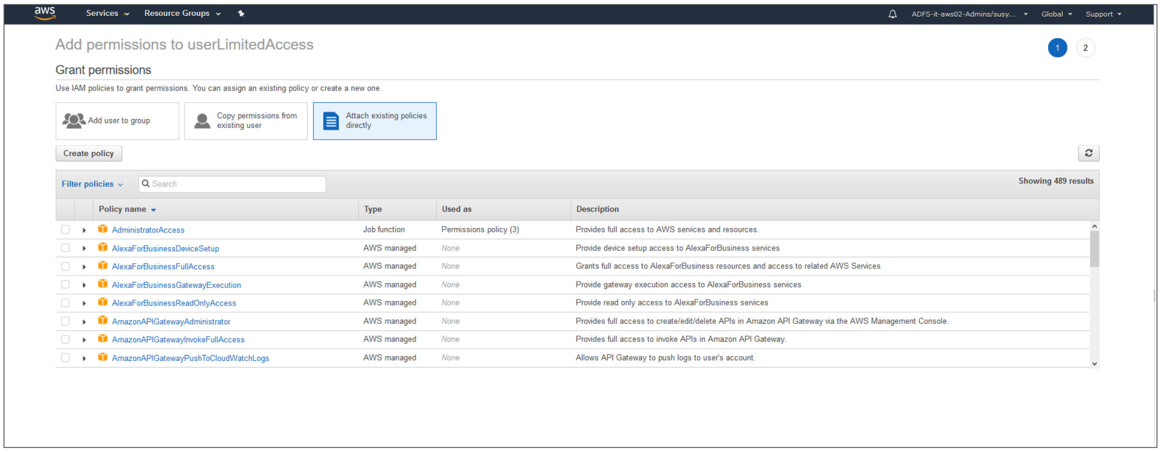
This user does not belong to any groups.

There are no managed policies attached to this user.

There are no inline policies to show. To create one, click here.

Feedback
English
© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

11. Under the **Permissions** heading, click the **[Attach existing policies directly]** button. The **Add permissions** page appears:


aws
Services
Resource Groups
ADFS-it-aws02-Admins/susy....
Global
Support
1
2
Add user to group
Copy permissions from existing user
Attach existing policies directly
Create policy
Filter policies
Search

Add permissions to userLimitedAccess

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Showing 489 results

	Policy name	Type	Used as	Description
☐	AdministratorAccess	Job function	Permissions policy (3)	Provides full access to AWS services and resources.
☐	AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaForBusiness services
☐	AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness resources and access to related AWS Services
☐	AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to AlexaForBusiness services
☐	AlexaForBusinessReadOnlyAccess	AWS managed	None	Provide read only access to AlexaForBusiness services
☐	AmazonAPIGatewayAdministrator	AWS managed	None	Provides full access to create/edit/delete APIs in Amazon API Gateway via the AWS Management Console.
☐	AmazonAPIGatewayInvokeFullAccess	AWS managed	None	Provides full access to invoke APIs in Amazon API Gateway.
☐	AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	None	Allows API Gateway to push logs to user's account.

12. Select the checkbox for your policy based on the definition of the minimum required permissions described in the ***Minimum Permissions for Dynamic Applications*** section.

13. Click the **[Attach Policy]** button.

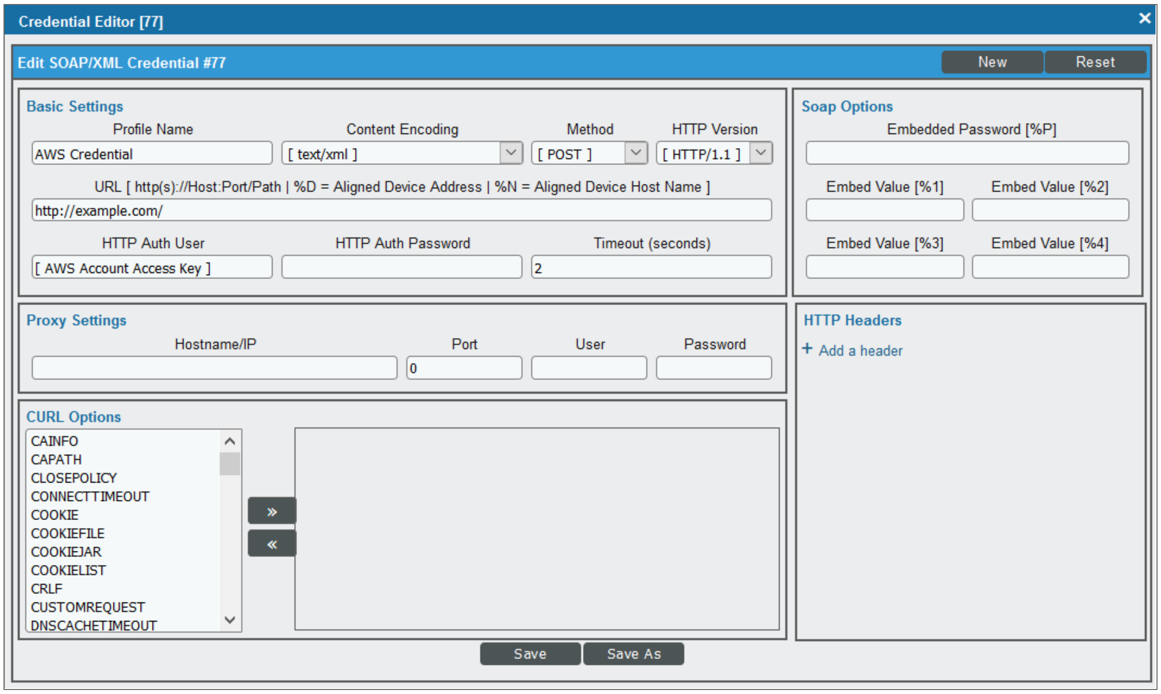
Creating the SOAP/XML Credential for AWS

To discover AWS using the manual discovery method, you must first define an AWS credential in SL1.

To define an AWS credential:

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

2. Locate the **AWS Manual Discovery** sample credential and click its wrench icon (). The **Credential Editor** modal page appears:



Credential Editor [77]

Edit SOAP/XML Credential #77

Basic Settings

Profile Name	Content Encoding	Method	HTTP Version
AWS Credential	[text/xml]	[POST]	[HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: http://example.com/

HTTP Auth User	HTTP Auth Password	Timeout (seconds)
[AWS Account Access Key]		2

Proxy Settings

Hostname/IP	Port	User	Password
	0		

CURL Options

CAINFO
CAPATH
CLOSEPOLICY
CONNECTTIMEOUT
COOKIE
COOKIEFILE
COOKIEJAR
COOKIELIST
CRLF
CUSTOMREQUEST
DNSCACHETIMEOUT

Soap Options

Embedded Password [%P]

Embed Value [%1] Embed Value [%2]

Embed Value [%3] Embed Value [%4]

HTTP Headers

3. Enter values in the following fields:

Basic Settings

- ***Profile Name***. Type a new name for your AWS credential.
- ***URL***. Enter a valid URL. This field is not used for this discovery method but must be populated with a valid URL for discovery to complete.
- ***HTTP Auth User***. Type your ***Access Key ID***.
- ***HTTP Auth Password***. Type your ***Secret Access Key***. The characters appear as asterisks to protect your password privacy.

Proxy Settings

NOTE: The ***Proxy Settings*** fields are required only if you are discovering AWS services through a proxy server. Otherwise, leave these fields blank.

- ***Hostname/IP***. Type the host name or IP address of the proxy server.
- ***Port***. Type the port on the proxy server to which you will connect.
- ***User***. Type the username used to access the proxy server.
- ***Password***. Type the password used to access the proxy server.

CAUTION: If you are creating a credential from the **AWS Credential - Proxy** example and the proxy server does not require a username and password, then the ***User*** and ***Password*** fields must both be blank. In that scenario, if you leave the "<Proxy_User>" text in the ***User*** field, SL1 cannot properly discover your AWS services.

SOAP Options

- ***Embed Value [%1]***. Do one of the following:
  - To monitor a GovCloud account, type "us-gov-west-1" or "us-gov-east-1".
  - To monitor the Beijing region, type "cn-north-1".
  - To monitor the Ningxia region, type "cn-northwest-1".

  Otherwise, leave this field blank.

NOTE: If you are monitoring both the Beijing and Ningxia regions, you must create a unique credential for each region.

- ***Embed Value [%2]***:
  - If you are using the AWS Config service and want to discover only regions that have that service enabled, type "[AUTO]" in this field. After discovery, only regions that have AWS Config enabled will be displayed in the dynamic component map tree. Global resources will also be discovered.
  - If you are using not using the AWS Config service, type "[FILTER]" in this field so it will discover only regions that are reporting CloudWatch metrics. This will reduce the number of regions being monitored and the load on the Data Collector.

CAUTION: If you are performing discovery using [AUTO] or [FILTER] in the ***Embed Value [%2]*** field, the status of regions that don't meet these requirements will change to *Unavailable* and vanish if enabled.

NOTE: If you are performing discovery based on the AWS Config service and do not have any regions with the AWS Config service enabled, the *Amazon Web Services* PowerPack will discover all regions that have resources.

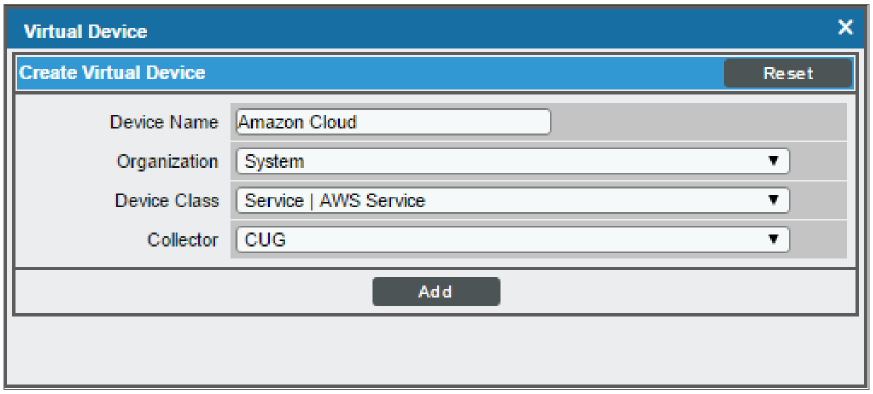
4. Click the **[Save As]** button, and then click **[OK]**.

Creating an AWS Virtual Device for Discovery in the SL1 Classic User Interface

Because the Amazon Web Service does not have a specific IP address, you cannot discover an AWS device using discovery. Instead, you must create a ***virtual device*** that represents the Amazon Web Service. A virtual device is a user-defined container that represents a device or service that cannot be discovered by SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications.

To create a virtual device that represents your Amazon service:

1. Go to the **Device Manager** page (Devices > Device Manager or Registry > Devices > Device Manager in the SL1 classic user interface).
2. Click the **[Actions]** button, then select *Create Virtual Device*. The **Virtual Device** modal page appears:



Device Name: Amazon Cloud
Organization: System
Device Class: Service | AWS Service
Collector: CUG

3. Enter values in the following fields:

   - ***Device Name***. Enter a name for the device. For example, you could enter "Amazon Cloud" in this field.
   - ***Organization***. Select the organization for this device. The organization the device is associated with limits the users that will be able to view and edit the device.
   - ***Device Class***. Select *Service | AWS Service*.
   - ***Collector***. Select the collector group that will monitor the device.

4. Click the **[Add]** button to create the virtual device.

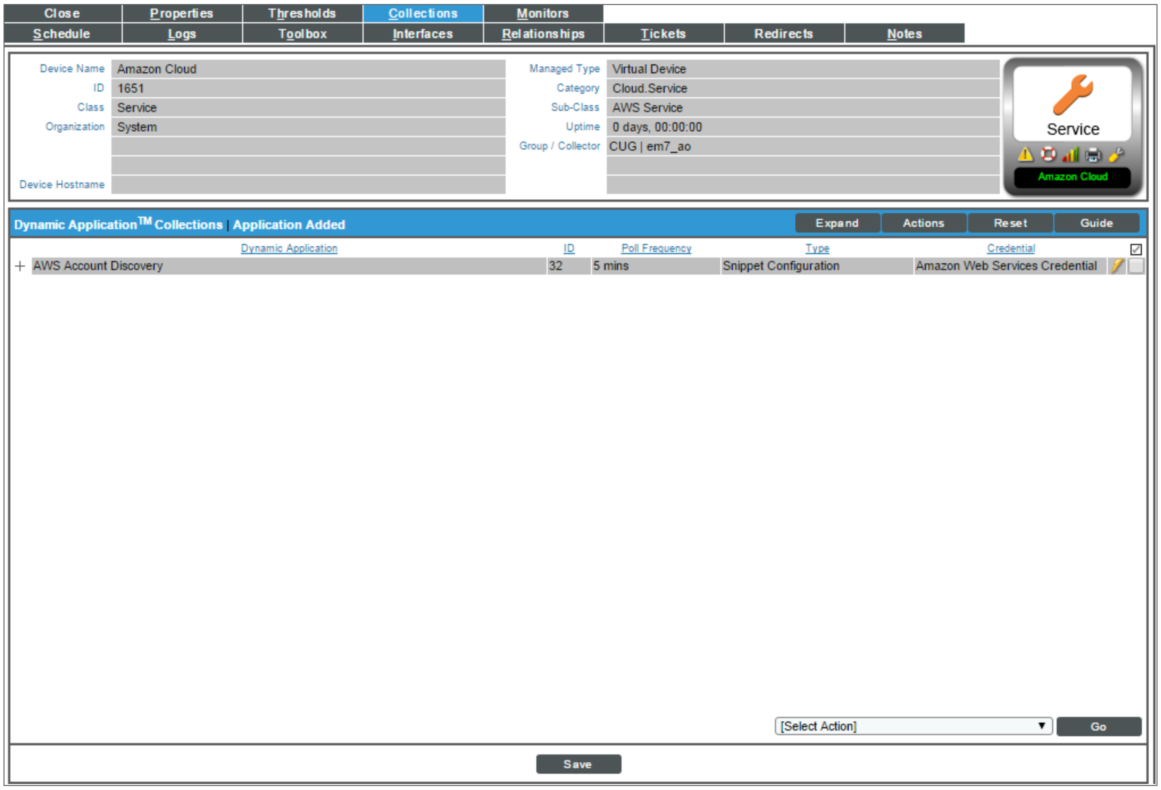
Aligning the Discovery Dynamic Application in the SL1 Classic User Interface

To discover your AWS account, you must manually align the "AWS: Account Discovery" Dynamic Application with the AWS virtual device. After you do so, the other Dynamic Applications in the *Amazon Web Services* PowerPack will automatically align to discover and monitor all of the components in your AWS account.

TIP: If your AWS account includes API Gateways or Lambda services to be monitored and you want SL1 to put those component devices in a "vanished" state if the platform cannot retrieve data about them for a specified period of time, ScienceLogic recommends setting the ***Component Vanish Timeout Mins.*** field to at least 120 minutes. For more information, see the chapter on "Vanishing and Purging Devices" in the ***Device Management*** manual.

To align the "AWS: Account Discovery" Dynamic Application to your virtual device:

1. Go to the **Device Manager** page (Devices > Device Manager or Registry > Devices > Device Manager in the SL1 classic user interface).
2. Click the wrench icon (🔧) for your virtual device.
3. In the **Device Administration** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears:
4. Click the **[Actions]** button, and then select *Add Dynamic Application* from the menu.
5. In the **Dynamic Application Alignment** modal page, select *AWS: Account Discovery* in the ***Dynamic Applications*** field.
6. In the ***Credentials*** field, select the *credential you created for your AWS service*.
7. Click the **[Save]** button to align the Dynamic Application.



Device Name: Amazon Cloud
ID: 1651
Class: Service
Organization: System
Device Hostname:

Managed Type: Virtual Device
Category: Cloud.Service
Sub-Class: AWS Service
Uptime: 0 days, 00:00:00
Group / Collector: CUG | em7_ao

Dynamic Application^{TM} Collections | Application Added

Dynamic Application	ID	Poll Frequency	Type	Credential	☑
+ AWS Account Discovery	32	5 mins	Snippet Configuration	Amazon Web Services Credential	□

Automated Discovery Using AssumeRole with a Single IAM Key from the AWS Master Account

Automated discovery using AssumeRole with an IAM key is the recommended approach to monitor your AWS accounts when your Data Collectors are ***not*** acting as EC2 instances. In this method of discovery, your organization will be discovered first and then the accounts within the organization will be created automatically.

This method of discovery has the following benefits:

- Only a single IAM key needs to be managed on SL1, instead of an IAM key for every AWS account.
- The IAM key is only used to get the information about the organization, and all the actual monitoring is done via temporary tokens, which is the recommended approach by AWS.

This method can also be used in the following scenarios:

- When a proxy server is between the Data Collector and the AWS cloud
- When Ping is not available
- In the Government cloud

NOTE: All examples shown are for commercial AWS accounts. When AWS Gov is being monitored, the JSON data that refers to ARN will need to be modified from "aws" to "aws-us-gov". For example: `Resource": "arn:aws:iam::<account number>:role/Sciencelogic-Monitor` would need to be `Resource": "arn:aws:iam-us-gov::<account number>:role/Sciencelogic-Monitor`

To use this method of discovery, perform the following steps:

1. *Configure a user in the master billing account*
2. *Create a role in each account*
3. *Configuring the SL1 credential*
4. *Create and run the discovery session*

NOTE: If Ping is blocked, then you must follow the steps in the *Manually Create the Organization and Align the Dynamic Applications* section.

Configure a User in the Master Billing Account

The first step in this discovery method is to create a policy that defines the permissions needed by SL1. To do this, copy the policy below into an editor:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "organizations:ListAccounts",
            "organizations:DescribeOrganization",
            "organizations:DescribeAccount"
         ],
         "Resource": "*"
      },
      {
         "Sid": "VisualEditor1",
         "Effect": "Allow",
         "Action": "sts:AssumeRole",
         "Resource": "arn:aws:iam::<account number>:role/Sciencelogic-Monitor"
      }
   ]
}
```

For each account that needs to be monitored, duplicate the `"Resource": "arn:aws:iam::<Account Number>:role/Sciencelogic-Monitor"` line and set the `<Account Number>` to the correct account number.

After editing the policy, perform the following steps in the AWS console:

1. Go to **IAM > Policies > Create Policy**. Select the **JSON** tab and copy the edited JSON text into the AWS console.
2. Click **Next: Tags** and then click **Next: Review**.
3. Type a name for the policy (for example, "SL1MasterBillingPermissions") and then select **[Create Policy]**.
4. To create a user in the master billing account, go to **IAM > Users > Add User**.
5. Type the user's name and select the option for **Programmatic Access**. Click **[Next: Permissions]**.
6. Select ***Attach existing policies directly*** and select the checkbox for the policy you created.
7. Select **Next: Tags > Next: Review > Create User**.

NOTE: The Access Key and Secret Key need to be saved as these will be needed when configuring the SL1 credential.

Create a Role in Each Account

In every AWS account that is to be monitored, a role with the ***same name*** needs to be created. The default name is "ScienceLogic-Monitor". To create the role, perform the following steps for each account that is to be monitored:

1. In the AWS console, go to **IAM > Roles** and select **Create Role**.
2. Select **Another AWS Account** and enter the account ID of the Master Billing Account. Select **Next: Permissions**.

3. Select the policy that was created in the *Minimum Permissions Needed to Monitor Your AWS Accounts* section.
4. Select **Next: Tags** and then **Next: Review**.
5. Enter "ScienceLogic-Monitor" in the ***Role name*** field and then select **[Create role]**.
6. Repeat these steps for each AWS account that you want to monitor.

Next you will need to edit the trust relationship of the role to restrict the principle to the user you created. To do this:

1. In the AWS console, go to **IAM > Roles** and select the "ScienceLogic-Monitor" role.
2. Select the **Trust Relationships** tab and click **[Edit trust relationship]**.
3. Edit the JSON to look like the following:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": [
            "AWS": "arn:aws:iam::<Master Billing Account>:user/<Master Billing
Account User>"
      },

      {
         "Action": "sts:AssumeRole",
         "Condition": {}
      }
   ]
}
```

NOTE: The ARN above is the ARN of the user that was created in the previous steps.

4. Once you have updated the policy, click **[Update Trust Policy]**.

Configure the SL1 Credential

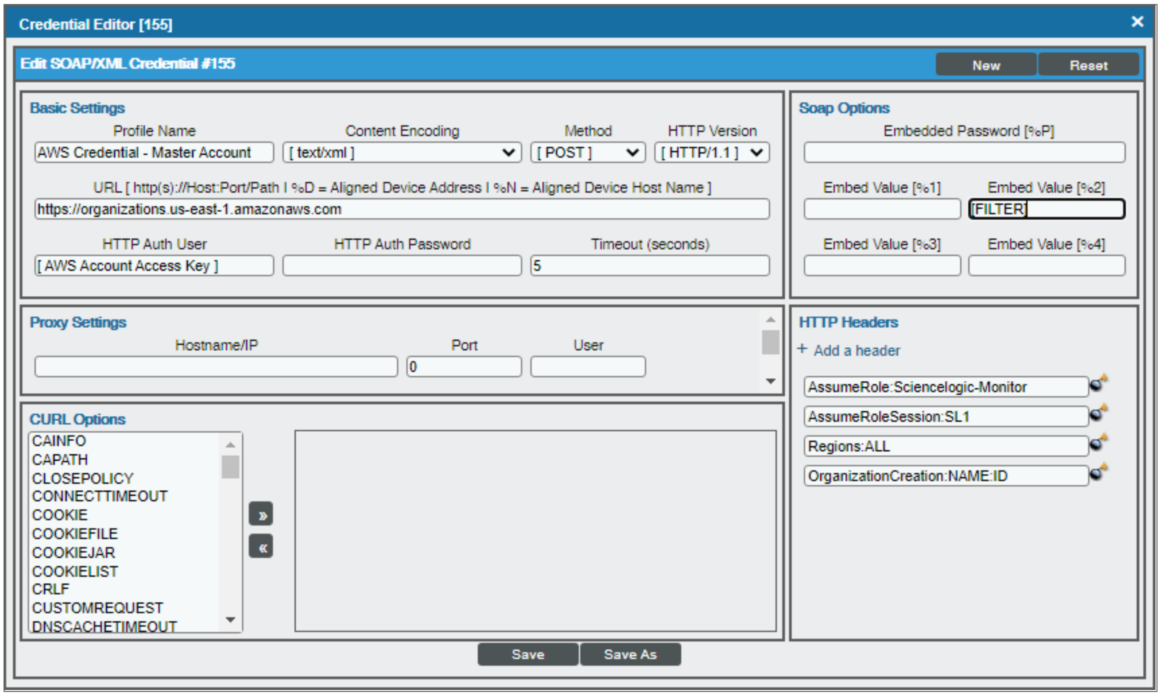
You can use your master organization account to automatically discover all AWS accounts, instead of having to enter a key for each account. This process will also create a separate DCM tree for each account.

NOTE: Discovery of China accounts does not support alignment using AssumeRole. For those accounts customers must continue to use manual alignment of Dynamic Applications.

To define the credential:

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

2. Locate the **AWS Credential - Master Account** sample credential that you need and click its wrench icon ( ). The **Credential Editor** modal page appears:



Profile Name: AWS Credential - Master Account
Content Encoding: [text/xml]
Method: [POST]
HTTP Version: [HTTP/1.1]
URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://organizations.us-east-1.amazonaws.com
HTTP Auth User: [AWS Account Access Key]
HTTP Auth Password:
Timeout (seconds): 5

Embedded Password [%P]:
Embed Value [%1]:
Embed Value [%2]: [FILTER]
Embed Value [%3]:
Embed Value [%4]:

Hostname/IP:
Port: 0
User:

AssumeRole:Sciencelogic-Monitor
AssumeRoleSession:SL1
Regions:ALL
OrganizationCreation:NAME:ID

CAINFO
CAPATH
CLOSEPOLICY
CONNECTTIMEOUT
COOKIE
COOKIEFILE
COOKIEJAR
COOKIELIST
CRLF
CUSTOMREQUEST
DNSCACHETIMEOUT

3. Enter values in the following fields:

Basic Settings

- ***Profile Name***. Type a new name for your AWS credential.
- ***URL***. Type `https://organizations.us-east-1.amazonaws.com` in the field. If your administrator has configured a different region, you can change it or use the default region. To discover Gov accounts using AssumeRole, type `https://organizations.us-gov-west-1.amazonaws.com`
- ***HTTP Auth User***. Type the AWS access key ID of the user you created in the master account.
- ***HTTP Auth Password***. Type the AWS secret access key of the user created in the master account.

SOAP Options

- *Embed Value [%2]*:
  - If you are using the AWS Config service and want to discover only regions that have that service enabled, type "[AUTO]" in this field. After discovery, only regions that have AWS Config enabled will be displayed in the dynamic component map tree. Global resources will also be discovered.
  - If you are using not using the AWS Config service, type "[FILTER]" in this field so it will discover only regions that are reporting CloudWatch metrics. This will reduce the number of regions being monitored and the load on the Data Collector.

HTTP Headers

- Click ***+ Add a header*** to add a header field. You can enter the following options:
  - *AssumeRole*. Type the AWS Role you created in each account. The default name is "ScienceLogic-Monitor".
  - *AssumeRoleSession*. Optional. The default value is "AssumeRoleSession:SL1".
  - *Regions*. The regions entered in this field will be discovered. For example, entering "Regions:ap-southeast-2, us-east-2" will discover two regions. If left blank, all regions will be discovered. The default value is "Regions:ALL".
  - *OrganizationCreation:NAME:ID*. Autocreates an SL1 organization for accounts using AssumeRole. You can enter one of the following options:
    - **OrganizationCreation:NAME**. The name of the organization will contain the name of the user.
    - **OrganizationCreation:ID**. The name of the organization will contain the ID of the user.
    - **OrganizationCreation:ID:NAME**. The name of the organization will contain both the ID and name of the user, in that order.
    - **OrganizationCreation:NAME:ID**. The name of the organization will contain both the name and ID of the user, in that order.

NOTE: The existing organization will be changed by this setting only if it is the default (System) organization. If this header is not included, then **all** the discovered accounts will be placed into the organization selected in the discovery session.

4. Click the **[Save As]** button, and then click **[OK]**.

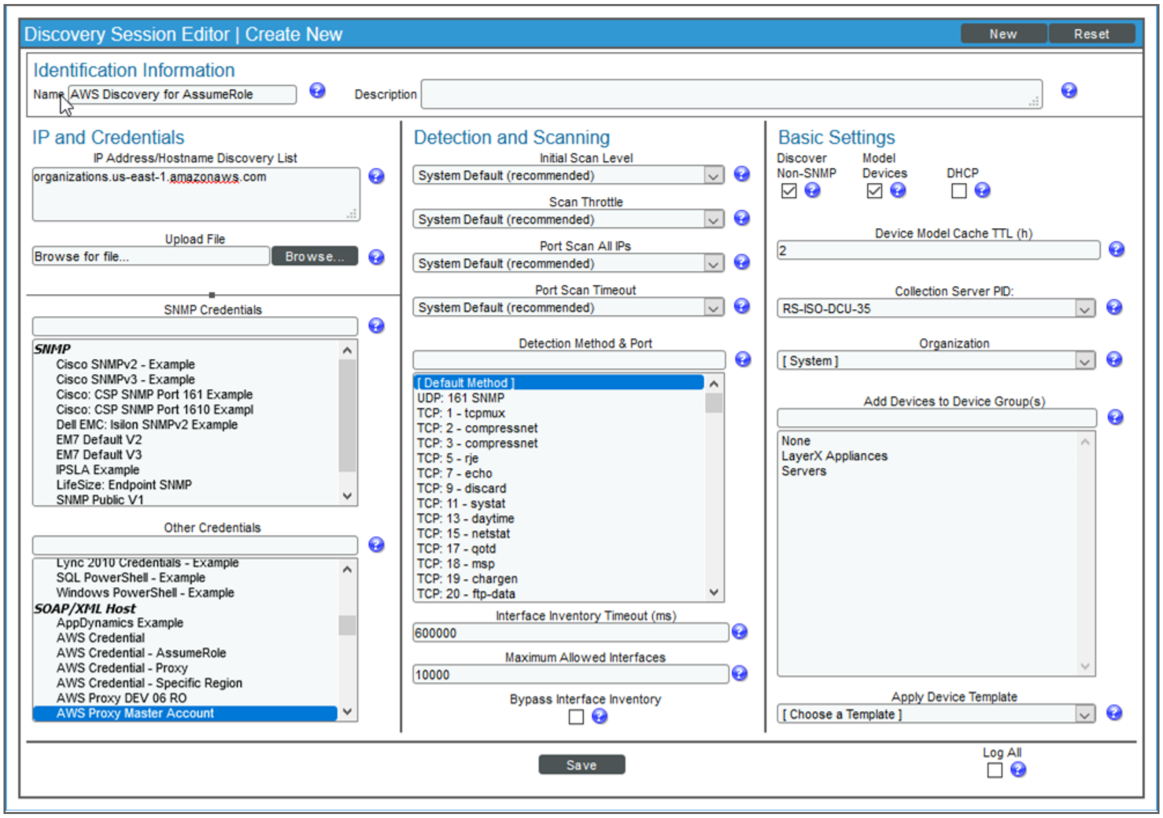
NOTE: If the "AWS: Account Creation" Dynamic Application is reporting that it is unable to use your AssumeRole, double-check your trust relationships on your configured roles.

Create and Run the Discovery Session

To discover AWS Accounts in an AWS Organization using AssumeRole, perform the following steps:

NOTE: If Ping is not supported between the Data Collector and AWS, you can skip this section and go to the *Manually Create the Organization and Align Dynamic Applications* section.

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. Click the **[Create]** button. The **Discovery Session Editor** page appears:



Discovery Session Editor | Create New

Identification Information

Name: AWS Discovery for AssumeRole

Description:

IP and Credentials

IP Address/Hostname Discovery List: organizations.us-east-1.amazonaws.com

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

SNMP Credentials

SNMP
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Cisco: CSP SNMP Port 161 Example
Cisco: CSP SNMP Port 1610 Exampl
Dell EMC: Isilon SNMPv2 Example
EM7 Default V2
EM7 Default V3
IPSLA Example
LifeSize: Endpoint SNMP
SNMP Public V1

Other Credentials

Lync 2010 Credentials - Example
SQL PowerShell - Example
Windows PowerShell - Example
SOAP/XML Host
AppDynamics Example
AWS Credential
AWS Credential - AssumeRole
AWS Credential - Proxy
AWS Credential - Specific Region
AWS Proxy DEV 06 RO
AWS Proxy Master Account

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
TCP: 17 - qotd
TCP: 18 - msp
TCP: 19 - chargen
TCP: 20 - ftp-data

Interface Inventory Timeout (ms): 600000

Maximum Allowed Interfaces: 10000

Bypass Interface Inventory: □

Basic Settings

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

Device Model Cache TTL (h): 2

Collection Server PID: RS-ISO-DCU-35

Organization: [System]

Add Devices to Device Group(s)

None
LayerX Appliances
Servers

Apply Device Template: [Choose a Template]

Log All: □

3. Supply values in the following fields:

- ***IP Address Discovery List***. Type the URL of your AWS master billing account.
- ***Other Credentials***. Select the credential you created.
- ***Discover Non-SNMP***. Select this checkbox.
- ***Model Devices***. Select this checkbox.

4. Optionally, supply values in the other fields in this page. For a description of the fields in this page, see the ***Discovery & Credentials*** manual.
5. Click the **[Save]** button.

6. The **Discovery Control Panel** page will refresh. Click the lightning bolt icon (⚡) for the discovery session you just created.
7. In the pop-up window that appears, click the **[OK]** button. The page displays the progress of the discovery session.

> **NOTE**: If you discontinue monitoring on any devices that are using the Assume Role authentication method, ScienceLogic recommends the best practice of first disabling the devices, deleting the devices from the DCM tree, and then cleaning up any AWS permissions in IAM. This will avoid any unnecessary alerts.

Manually Creating the Organization and Aligning Dynamic Applications

> **NOTE:** The following steps are needed only if ping is **not** supported between the Data Collector and AWS.

To create a virtual device to create the organization:

1. Go to the **Device Manager** page (Devices > Device Manager or Registry > Devices > Device Manager in the SL1 classic user interface).
2. Click the **[Actions]** button, then select *Create Virtual Device*. The **Virtual Device** modal page appears:
3. Enter values in the following fields:
   - ***Device Name***. Enter a name for the device. For example, you could enter "Amazon Organization" in this field.
   - ***Organization***. Select the organization for this device. The organization the device is associated with limits the users that will be able to view and edit the device.
   - ***Device Class***. Select *AWS | Organization*.
   - ***Collector***. Select the collector group that will monitor the device.
4. Click the **[Add]** button to create the virtual device.

Next, you must manually align the "AWS: Account Creation" Dynamic Application with the AWS virtual device. After you do so, the other Dynamic Applications in the *Amazon Web Services* PowerPack will automatically align to discover and monitor all of the components in your AWS account.

To align the "AWS: Account Creation" Dynamic Application to your virtual device:

1. Go to the **Device Manager** page (Devices > Device Manager or Registry > Devices > Device Manager in the SL1 classic user interface).
2. Click the wrench icon (🔧) for your virtual device.
3. In the **Device Administration** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears:

4. Click the **[Actions]** button, and then select *Add Dynamic Application* from the menu.
5. In the **Dynamic Application Alignment** modal page, select *AWS: Account Creation* in the ***Dynamic Applications*** field.
6. In the ***Credentials*** field, select the credential you created for your AWS service.
7. Click the **[Save]** button to align the Dynamic Application.

Automated Discovery when the Data Collector Runs as an EC2 Instance

This method of discovery is recommended for monitoring your AWS accounts within an organization when your Data Collectors are EC2 instances. In this case, a standard SL1 discovery process is created, and this mechanism will first discover your organization and then create all the accounts within the organization.

This method of discovery has the following benefits:

- No AWS credentials are needed in SL1

NOTE: All examples shown are for commercial AWS accounts. When AWS Gov is being monitored, the JSON data that refers to ARN will need to be modified from "aws" to "aws-us-gov". For example: `Resource": "arn:aws:iam::<account number>:role/Sciencelogic-Monitor` would need to be `Resource": "arn:aws:iam-us-gov::<account number>:role/Sciencelogic-Monitor`

To use this method of discovery, perform the following steps:

1. *Create an AWS role in the master billing account*
2. *Create an AWS role in account that the collector is in*
3. *Create an AWS role in each account that is to be monitored*
4. *Create an SL1 credential*
5. *Create and run the discovery session*

Create a Role in the Master Billing Account

The role you will create in the master billing account is assumed from the account that the EC2 instance is in. This role will enable SL1 to temporarily log in to the master billing account and discover other accounts.

Before creating the role, you must first create a policy that defines the permissions needed by SL1. To do this, copy and the policy from below into an editor:

```
{ "Version": "2012-10-17",
   "Statement":
      {"Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "organizations:ListAccounts",
            "organizations:DescribeOrganization",
            "organizations:DescribeAccount"
          ]
          "Resource": "*"
      },
}
```

Next, perform the following steps:

1. Log in to the Master Billing Account via the AWS console and select **IAM > Policies > Create Policy**.
2. Select the **JSON** tab and paste the JSON text you edited above into the AWS console.
3. Click **Next: Tags** and then click **Next: Review**.
4. Type a name for the policy (for example, "SL1MasterBillingPermissions") in the ***Name*** field and then click **Create Policy**.

To create the role:

1. Go to **IAM > Roles > Create Role**.
2. Under ***Select type of trusted entity***, select **Another AWS account**.
3. Type the account number of the account that contains the EC2 instance running on the collector in the ***Account ID*** field, and then click **Next: Permissions**.
4. Select the checkbox for the policy you created above.
5. Click **Next: Tags** and then click **Next: Review**.
6. Type the role name from the example above (SL1MasterAccountRole) in the ***Role name*** field, then click **Create role**.

The trust policy is set up by the console automatically as follows:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
          "AWS": "arn:aws:iam::581618222958:root"
         },
         "Action": "sts:AssumeRole",
         "Condition":{}

        }
      ]
    }
```

7. In the console, edit the trust relationship and replace `:root` with `:role/ec2-collector`.

NOTE: "ec2-collector" is the name of the role that will be created in the account that the EC2 collector is in. This policy allows only the "ec2-colletor" role to assume this role in the master billing account. If you use another name for the role, then this trust relationship must use that name instead of "ec2-collector".

Create an AWS Role in the Account your Data Collector is In

The role you create in the account your Data Collector is in will be assigned to the EC2 instances that house those Data Collectors. This role enables the SL1 Data Collector to assume a role in the master billing account, which is then used to discover the organization and retrieve the accounts associated with that organization. Once the accounts have been discovered, this role allows SL1 to assume the monitor role in each of the accounts.

First you will need to create a policy in the accounts that the Data Collectors are in. To create this policy, first cut and paste the following JSON text into an editor:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": "sts:AssumeRole",
         "Resource": [
                    "arn:aws:iam::<master billing account ID>:role/SL1MasterAccountRole",
                    "arn:aws:iam::<monitored account 1>:role/ScienceLogic-Monitor",
                    "arn:aws:iam::<monitored account 2>:role/ScienceLogic-Monitor",
                    "arn:aws:iam::<monitored account 3>:role/ScienceLogic-Monitor"
         ]
      }
   ]
}
```

Replace the **"master billing account"** with your master billing account number.

For each account to be monitored, ensure that there is a line under Resource that matches the account ID. The example above shows three accounts to be monitored.

NOTE: If the master billing account is to be monitored, it will also need a line in the Resource list.

If you did not use the example "SL1MasterAccountRole" name, replace it with the name of your role.

Next, perform the following steps:

1. Log in to the AWS console and select **IAM > Policies > Create Policy**.
2. Select the **JSON** tab and copy the JSON text you edited above into the AWS console.
3. Click **Next: Tags** and then click **Next: Review**.

4. Type a name for the policy (for example, "EC2CollectorPolicy") in the ***Name*** field and then click **Create Policy**.

To create the role:

> **NOTE**: If you already have a role assigned to the Data Collector that houses the EC2 instance, then you can add the policy you just created to that existing role. Otherwise, follow the steps below to create the role.

1. Go to **IAM > Roles > Create Role**.
2. Under ***Select type of trusted entity***, select **AWS service**.
3. Under ***Choose a use case***, select **EC2**.
4. Click **Next: Permissions** and select the policy you created above.
5. Click **Next: Tags** and then click **Next: Review**.
6. Type the name from our example (ec2-collector) in the ***Role name*** field, then click **Create role**.

Next, you need to assign this instance profile to the EC2 instances that are Data Collectors. To do this:

1. Go to the AWS console and click **EC2 > Instances**.
2. Select the checkbox for each instance that is a Data Collector.
3. Click **Actions > Security > Modify IAM Role**.
4. In the drop-down field, select the role that you just created and then click **[Save]**.

Create a Role in Each Account

In every account that is to be monitored, a role with the ***same name*** needs to be created. The default name is ScienceLogic-Monitor. The following steps must be performed for each account that is to be monitored:

1. In the AWS console for the account and go to **IAM > Roles > Create Role**.
2. Under ***Select type of trusted entity***, select **Another AWS account**.
3. Type the account number that houses the EC2 collectors in the ***Account ID*** field, and then click **Next: Permissions**.
4. Select the checkbox for the policy you created in the *Minimum Permissions Needed to Monitor Your AWS Accounts* section (called "SL1MinimumPermissions").
5. Click **Next: Tags** and then click **Next: Review**.
6. Type ScienceLogic-Monitor in the ***Role name*** field, then click **Create role**.
7. Click on the role that was just created and select the **Trust Relationships** tab.
8. Click the **[Edit trust relationship]** button.

9. In the **Policy Document** editor, change the Principle from `"AWS": "arn:aws:iam::<ec2 collector account>:root` to `"AWS": "arn:aws:iam::<collector account>:role/ec2-collector"` (where `ec2-collector` is the name of the role created on the account housing the EC2 collector). Then click the **[Update Trust Policy]** button.

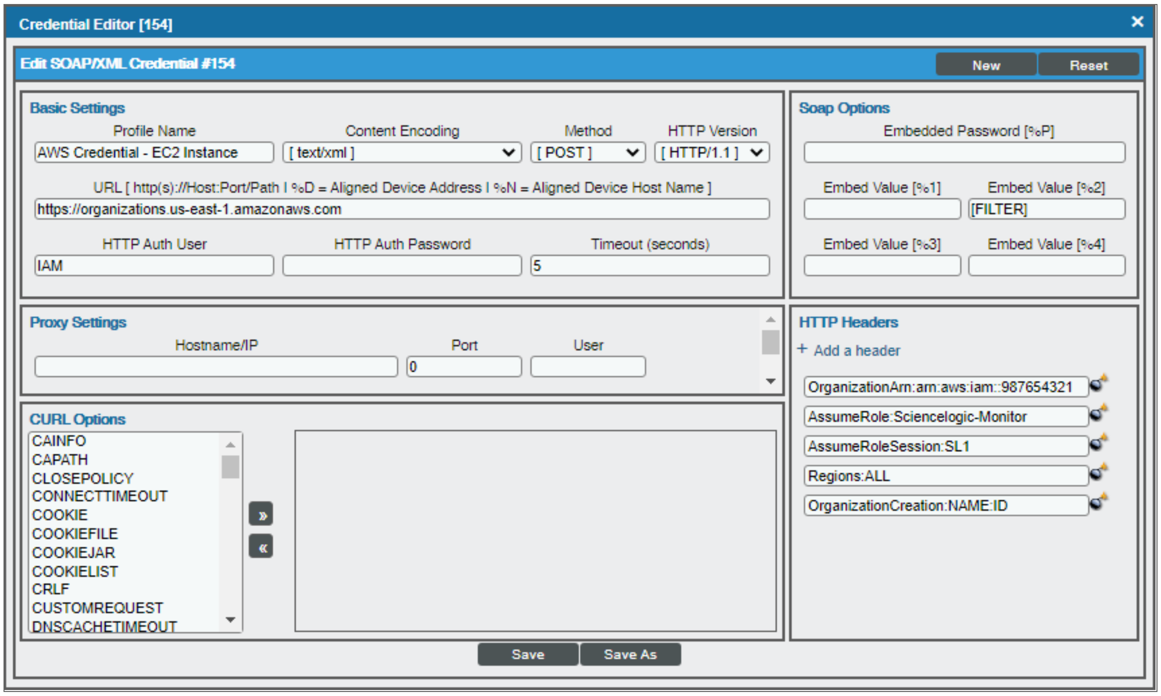
10. Repeat these steps for each account that is to be monitored.

Configuring the Credential to Discover AWS on an EC2 Collector

To define an AWS credential to discover AWS on an EC2 collector:

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

2. Locate the **AWS Credential - EC2 Instance** sample credential that you need and click its wrench icon (🔧). The **Credential Editor** modal page appears:



Basic Settings

Profile Name: AWS Credential - EC2 Instance

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://organizations.us-east-1.amazonaws.com

HTTP Auth User: IAM

HTTP Auth Password:

Timeout (seconds): 5

Soap Options

Embedded Password [%P]:

Embed Value [%1]:

Embed Value [%2]: [FILTER]

Embed Value [%3]:

Embed Value [%4]:

Proxy Settings

Hostname/IP:

Port: 0

User:

HTTP Headers

+ Add a header

OrganizationArn:arn:aws:iam::987654321

AssumeRole:Sciencelogic-Monitor

AssumeRoleSession:SL1

Regions:ALL

OrganizationCreation:NAME:ID

CURL Options

CAINFO
CAPATH
CLOSEPOLICY
CONNECTTIMEOUT
COOKIE
COOKIEFILE
COOKIEJAR
COOKIELIST
CRLF
CUSTOMREQUEST
DNSCACHETIMEOUT

3. Enter values in the following fields:

Basic Settings

- ***Profile Name***. Type a new name for your AWS credential.
- ***URL***. Type `https://organizations.us-east-1.amazonaws.com` in the field. If your administrator has configured a different region, you can change it or use the default region. **To discover Gov accounts** using AssumeRole, type `https://organizations.us-gov-west-1.amazonaws.com`.
- ***HTTP Auth User***. Leave the default value "IAM" in the field.

SOAP Options

- ***Embed Value [%2]***:
  - If you are using the AWS Config service and want to discover only regions that have that service enabled, type "[AUTO]" in this field. After discovery, only regions that have AWS Config enabled will be displayed in the dynamic component map tree. Global resources will also be discovered.
  - If you are using not using the AWS Config service, type "[FILTER]" in this field so it will discover only regions that are reporting CloudWatch metrics. This will reduce the number of regions being monitored and the load on the Data Collector.

HTTP Headers

- Click ***+ Add a header*** to add a header field. You can enter the following options:
  - *OrganizationArn*. Defines the ARN for the AssumeRole. This is the ARN of the role created in the master billing account. In the ***example above*** it was called "SL1MasterAccountRole". For example, `OrganizationArn:arn:aws:iam::<Master Billing Account>:role/SL1MasterAccountRole`
  - *AssumeRole*. Type the AWS Role you created in each account. The default name is "ScienceLogic-Monitor".
  - *AssumeRoleSession*. Optional. The default value is "AssumeRoleSession:SL1".
  - *OrganizationCreation:NAME:ID*. Autocreates an SL1 organization for accounts using AssumeRole. You can enter one of the following options:
    - **OrganizationCreation:NAME**. The name of the organization will contain the name of the user.
    - **OrganizationCreation:ID**. The name of the organization will contain the ID of the user.
    - **OrganizationCreation:ID:NAME**. The name of the organization will contain both the ID and name of the user, in that order.
    - **OrganizationCreation:NAME:ID**. The name of the organization will contain both the name and ID of the user, in that order.

NOTE: The existing organization will be changed by this setting only if it is the default (System) organization.

4. Click the **[Save As]** button, then click **[OK]**.

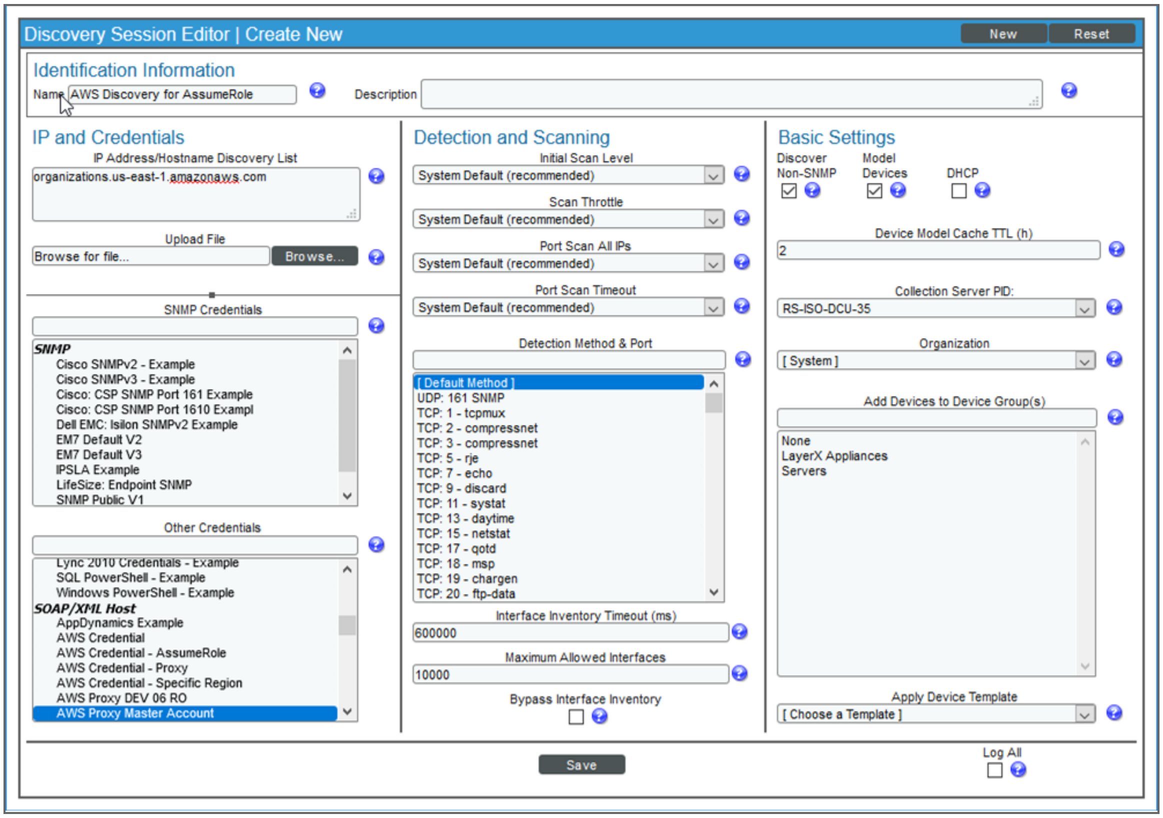
Create and Run the Discovery Session

To discover AWS Accounts in an AWS Organization using AssumeRole, perform the following steps:

NOTE: If you are upgrading the PowerPack and had previously discovered accounts within an organization separately and now want to use a different discovery method, you must first disable the "AWS: Account Discovery" Dynamic Application in each account that is being upgraded.

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

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



Discovery Session Editor | Create New

Identification Information

Name: AWS Discovery for AssumeRole

Description:

IP and Credentials

IP Address/Hostname Discovery List: organizations.us-east-1.amazonaws.com

Upload File: Browse for file...

Other Credentials: AWS Proxy Master Account

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]

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: RS-ISO-DCU-35

Organization: [System]

Apply Device Template: [Choose a Template]

Log All: □

3. Supply values in the following fields:

   - ***IP Address Discovery List***. Type the URL of your AWS master billing account.
   - ***Other Credentials***. Select the credential you created.
   - ***Discover Non-SNMP***. Select this checkbox.
   - ***Model Devices***. Select this checkbox.

4. Optionally, supply values in the other fields in this page. For a description of the fields in this page, see the ***Discovery & Credentials*** manual.

5. Click the **[Save]** button.

6. The **Discovery Control Panel** page will refresh. Click the lightning bolt icon ( ) for the discovery session you just created.

7. In the pop-up window that appears, click the **[OK]** button. The page displays the progress of the discovery session.

NOTE: If you discontinue monitoring on any devices that are using the Assume Role authentication method, ScienceLogic recommends the best practice of first disabling the devices, deleting the devices from the DCM tree, and then cleaning up any AWS permissions in IAM. This will avoid any unnecessary alerts.

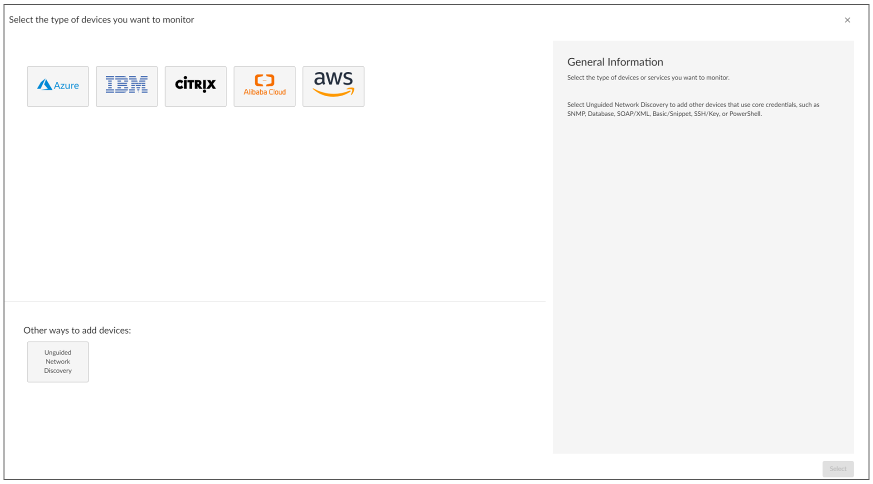
AWS Guided Discovery

You can use the Universal Discovery Framework process in SL1 that guides you through a variety of existing discovery types in addition to traditional SNMP discovery. This process, which is also called "guided discovery", lets you pick a discovery type based on the type of devices you want to monitor. The Universal Discovery workflow includes a button for Amazon Web Services.

NOTE: If you want to discover one of the third-party products that are available as an option when using the Universal Discovery workflow, you must have the corresponding PowerPack installed on your SL1 system to ensure that the appropriate Dynamic Applications, Device Classes, and other elements can be utilized for discovery. For example, if you want to discover an Amazon Web Services account, you must have the *Amazon Web Services* PowerPack installed.

To run a guided or Universal Discovery:

1. On the **Devices** page (🖥) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears.

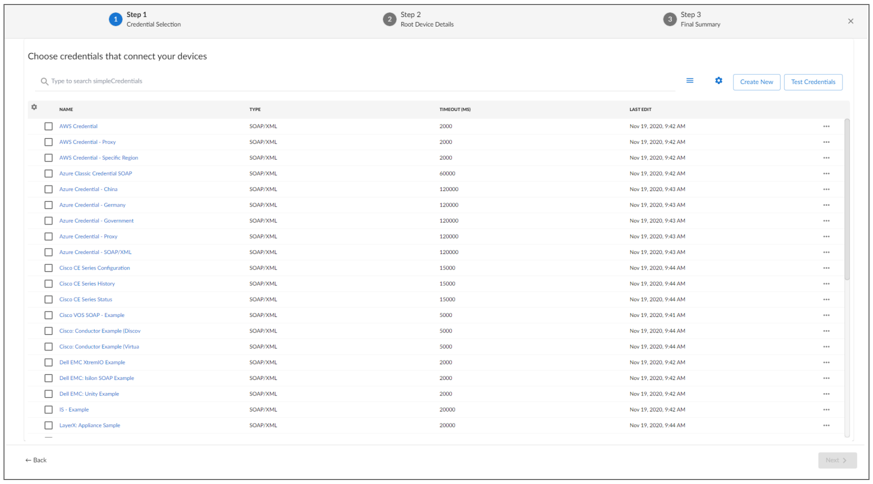

Select the type of devices you want to monitor
×
Azure
IBM
CITRIX
Alibaba Cloud
aws
Other ways to add devices:
Unguided Network Discovery
Select

General Information

Select the type of devices or services you want to monitor.

Select Unguided Network Discovery to add other devices that use core credentials, such as SNMP, Database, SOAP/XML, Basic/Snippet, SSH/Key, or PowerShell.

2. Select the **Amazon Web Services** button. Additional information about the requirements for device discovery appears in the **General Information** pane to the right.
3. Click **[Select]**. The **Credential Selection** page appears.

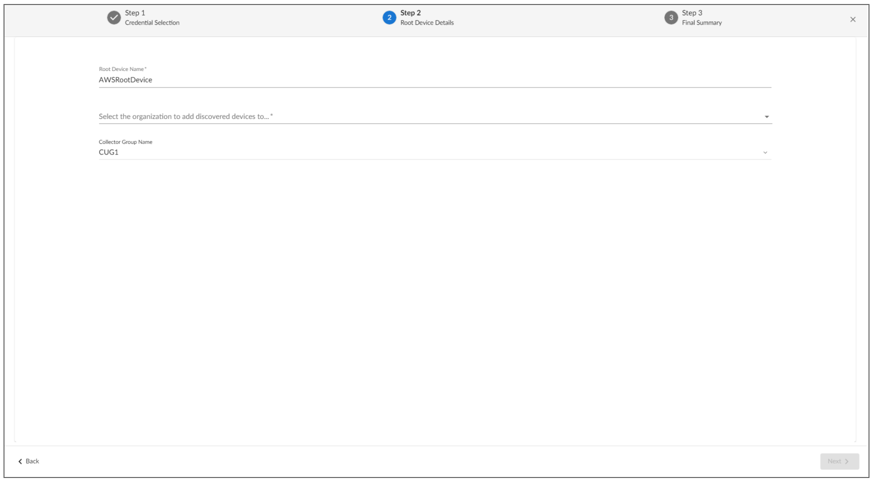


Choose credentials that connect your devices

	NAME	TYPE	TIMEOUT (MS)	LAST EDIT	
□	AWS Credential	SOAP/XML	2000	Nov 19, 2020, 9:42 AM	•••
□	AWS Credential - Proxy	SOAP/XML	2000	Nov 19, 2020, 9:42 AM	•••
□	AWS Credential - Specific Region	SOAP/XML	2000	Nov 19, 2020, 9:42 AM	•••
□	Azure Classic Credential SOAP	SOAP/XML	60000	Nov 19, 2020, 9:42 AM	•••
□	Azure Credential - China	SOAP/XML	120000	Nov 19, 2020, 9:43 AM	•••
□	Azure Credential - Germany	SOAP/XML	120000	Nov 19, 2020, 9:43 AM	•••
□	Azure Credential - Government	SOAP/XML	120000	Nov 19, 2020, 9:43 AM	•••
□	Azure Credential - Proxy	SOAP/XML	120000	Nov 19, 2020, 9:43 AM	•••
□	Azure Credential - SOAP/XML	SOAP/XML	120000	Nov 19, 2020, 9:43 AM	•••
□	Cisco CE Series Configuration	SOAP/XML	15000	Nov 19, 2020, 9:44 AM	•••
□	Cisco CE Series History	SOAP/XML	15000	Nov 19, 2020, 9:44 AM	•••
□	Cisco CE Series Status	SOAP/XML	15000	Nov 19, 2020, 9:44 AM	•••
□	Cisco VOS SOAP - Example	SOAP/XML	5000	Nov 19, 2020, 9:41 AM	•••
□	Cisco: Conductor Example (Discov	SOAP/XML	5000	Nov 19, 2020, 9:44 AM	•••
□	Cisco: Conductor Example (Virtua	SOAP/XML	5000	Nov 19, 2020, 9:44 AM	•••
□	Dell EMC XtremIO Example	SOAP/XML	2000	Nov 19, 2020, 9:42 AM	•••
□	Dell EMC: Isilon SOAP Example	SOAP/XML	2000	Nov 19, 2020, 9:42 AM	•••
□	Dell EMC: Unity Example	SOAP/XML	2000	Nov 19, 2020, 9:42 AM	•••
□	IS - Example	SOAP/XML	20000	Nov 19, 2020, 9:42 AM	•••
□	LayerX: Appliance Sample	SOAP/XML	20000	Nov 19, 2020, 9:44 AM	•••

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

4. On the **Credential Selection** page of the guided discovery process, select the AWS credential that you configured, and then click **[Next]**. The **Root Device Details** page appears.



Root Device Name*
AWSRootDevice

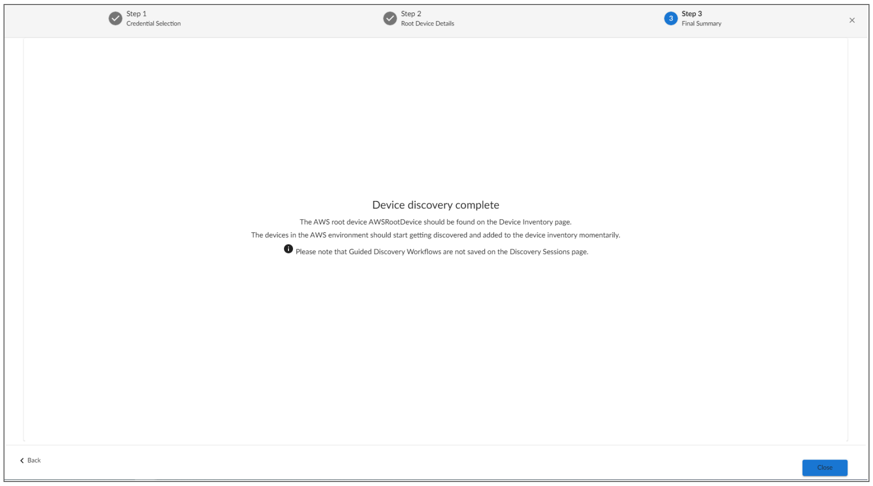
Select the organization to add discovered devices to...*

Collector Group Name
CUG1

5. Complete the following fields:

   - ***Root Device Name***. Type the name of the root device for the Amazon Web Services root device you want to monitor.
   - ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered device.
   - ***Collector Group Name***. Select an existing collector group to communicate with the discovered device. This field is required.

6. Click **[Next]**. SL1 creates the AWS root device with the appropriate Device Class assigned to it and aligns the relevant Dynamic Applications. The **Final Summary** page appears.



Device discovery complete

The AWS root device AWSRootDevice should be found on the Device Inventory page.

The devices in the AWS environment should start getting discovered and added to the device inventory momentarily.

Please note that Guided Discovery Workflows are not saved on the Discovery Sessions page.

8. Click **[Close]**.

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

Chapter 5

AMQP: RabbitMQ

Overview

The following sections describe how to configure and discover a RabbitMQ system for monitoring by SL1 using the *AMQP: RabbitMQ* PowerPack:

NOTE: For more information about the *AMQP: RabbitMQ* PowerPack, see the ***Monitoring Monitoring RabbitMQ Systems*** manual.

Prerequisites for Monitoring RabbitMQ

To configure SL1 to monitor a RabbitMQ system using the *AMQP: RabbitMQ* PowerPack, you must first have the following information:

- The IP address of the server running the RabbitMQ system
- The username and password for a RabbitMQ user that has read permission to the RabbitMQ API. For information about configuring users in RabbitMQ, see https://www.rabbitmq.com/management.html.

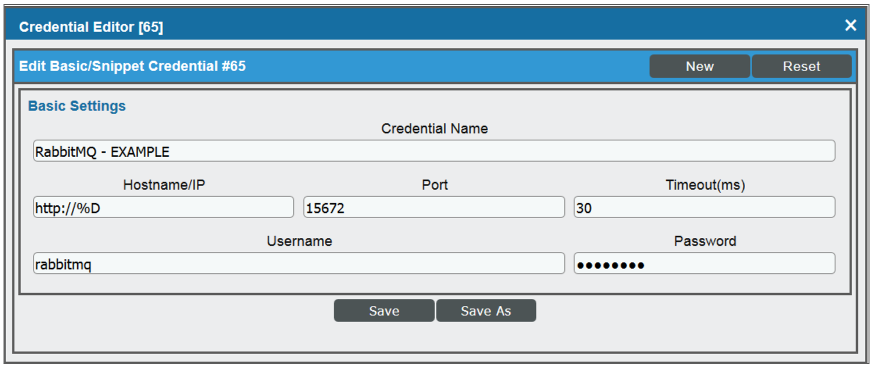
Creating a Credential for RabbitMQ

To configure SL1 to monitor a RabbitMQ system, you must first create a Basic/Snippet credential. This credential allows the Dynamic Applications in the *AMQP: RabbitMQ* PowerPack to communicate with your RabbitMQ system.

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

To configure a Basic/Snippet credential to access a RabbitMQ system:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **RabbitMQ - EXAMPLE** credential, then click its wrench icon (🔧). The **Edit Basic/Snippet Credential** modal page appears.
3. Enter values in the following fields:



Credential Editor [65]

Edit Basic/Snippet Credential #65

Basic Settings

Credential Name: RabbitMQ - EXAMPLE

Hostname/IP: http://%D

Port: 15672

Timeout(ms): 30

Username: rabbitmq

Password: ••••••••

- ***Profile Name***. Enter a name for the RabbitMQ credential.
- ***Hostname/IP***. Use the provided "http://%D".

NOTE: The IP address in the ***Hostname/IP*** field must be preceded by "http://".

- ***Username***. Enter the username for a RabbitMQ user that has read permission to the RabbitMQ API.
- ***Password***. Enter the password for the user you entered in the ***Username*** field.

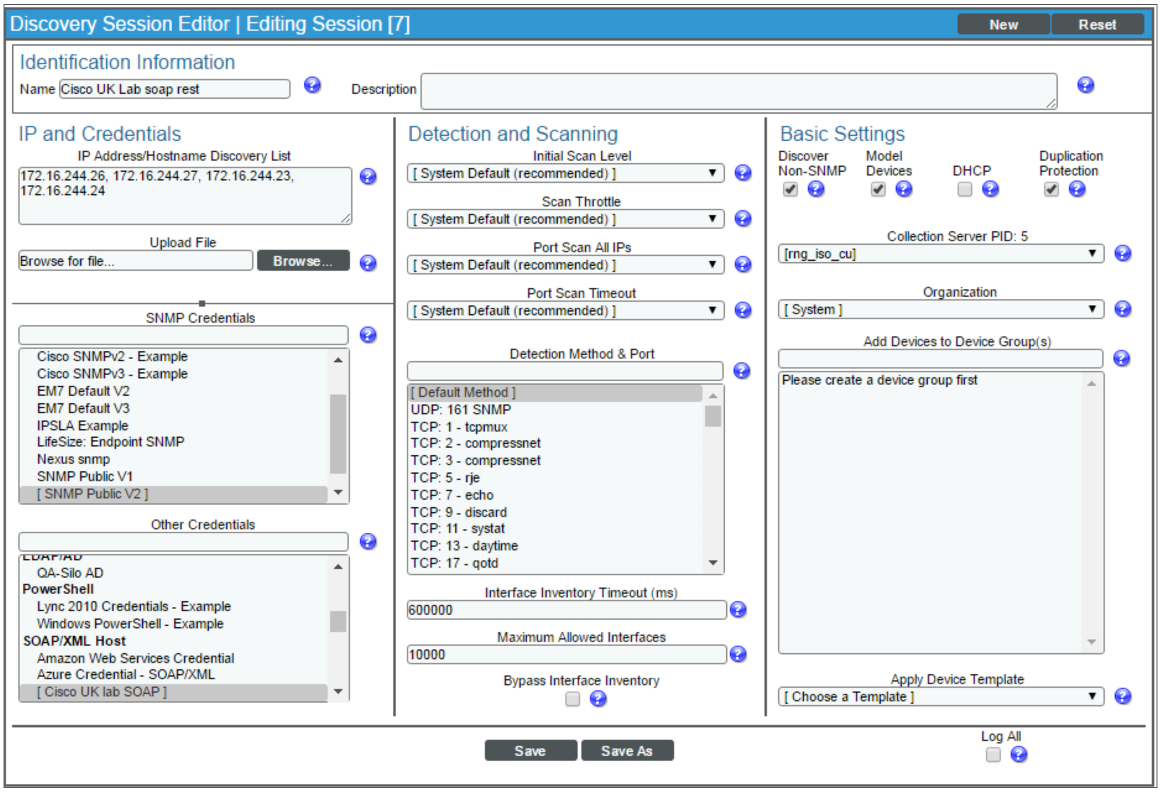
4. Leave all other fields set to the default values. Click the **[Save As]** button.

Discovering RabbitMQ Devices

To monitor your RabbitMQ system, you must run a discovery session to discover the server on which RabbitMQ is installed.

To discover the server on which RabbitMQ is installed, 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:



Discovery Session Editor | Editing Session [7]

Identification Information

Name: Cisco UK Lab soap rest

Description:

IP and Credentials

IP Address/Hostname Discovery List: 172.16.244.26, 172.16.244.27, 172.16.244.23, 172.16.244.24

Upload File: Browse for file...

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:
- LDAP/AD
  - 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: [rng_iso_cu]

Organization: [System]

Add Devices to Device Group(s): Please create a device group first

Apply Device Template: [Choose a Template]

Log All: □

- ***IP Address/Hostname Discovery List***. Enter the IP address for the server on which RabbitMQ is installed.
- ***SNMP Credentials***. Optionally, select the SNMP credential for the Linux or Windows server you are discovering.
- ***Other Credentials***. Select the Basic/Snippet credential you created for the RabbitMQ API.
- ***Discover Non-SNMP***. 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.

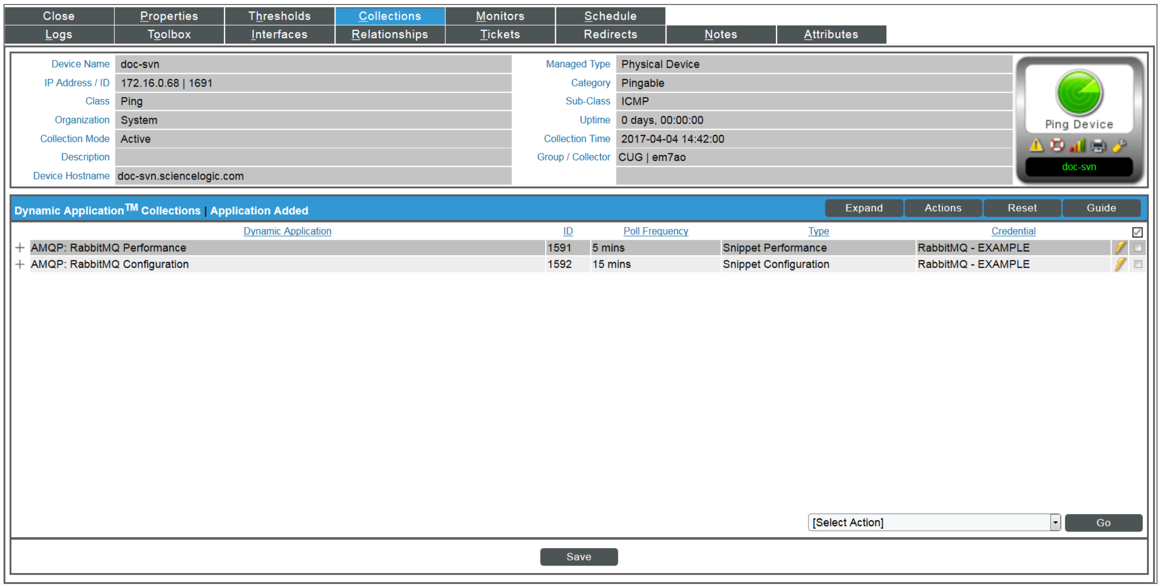
5. Click the **[Save]** button to save the discovery session and then close the **Discovery Session Editor** window.
6. The discovery session you created appears at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon (⚡) to run the discovery session.
7. The **Discovery Session** window appears. When the device is discovered, click the device icon (🖨) to view the **Device Properties** page for the device.

Verifying Discovery and Dynamic Application Alignment

To verify that SL1 automatically aligned the correct Dynamic Applications during discovery:

1. From the **Device Properties** page for the server on which RabbitMQ is installed, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. All applicable Dynamic Applications for RabbitMQ 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	doc-svn	Managed Type	Physical Device
IP Address / ID	172.16.0.68 | 1691	Category	Pingable
Class	Ping	Sub-Class	ICMP
Organization	System	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2017-04-04 14:42:00
Description		Group / Collector	CUG | em7ao
Device Hostname	doc-svn.sciencelogic.com		

doc-svn

Dynamic Application^{TM} Collections | Application Added

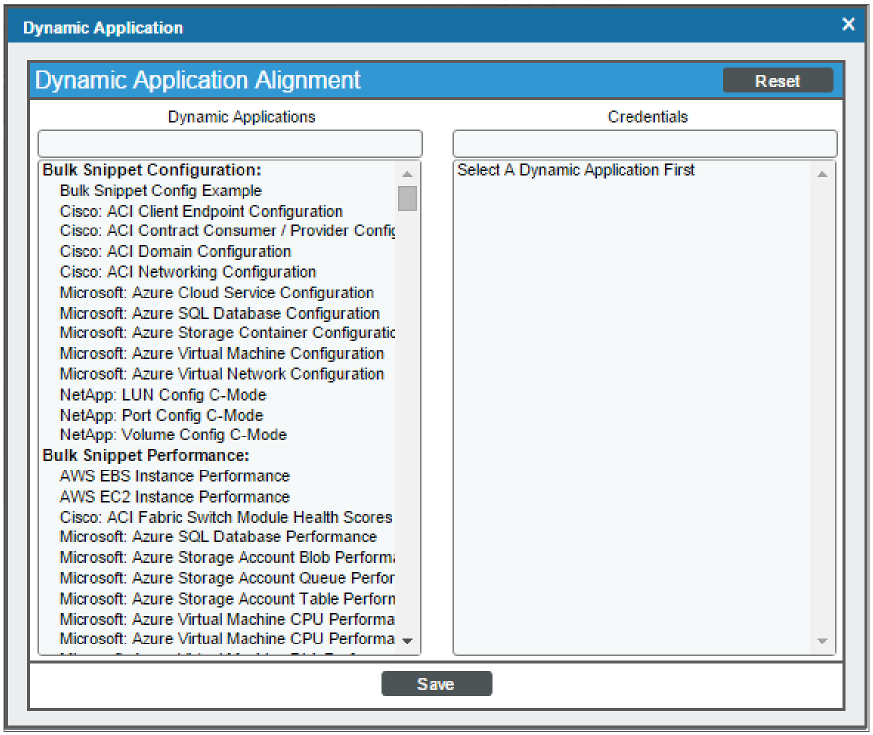
Dynamic Application	ID	Poll Frequency	Type	Credential	☑
+ AMQP: RabbitMQ Performance	1591	5 mins	Snippet Performance	RabbitMQ - EXAMPLE	□
+ AMQP: RabbitMQ Configuration	1592	15 mins	Snippet Configuration	RabbitMQ - EXAMPLE	□

The following Dynamic Applications should be aligned to the device:

- AMQP: RabbitMQ Configuration
- AMQP: RabbitMQ Performance

If the listed Dynamic Applications have not been automatically aligned during discovery, you can align them manually. To do so, perform the following steps:

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



Bulk Snippet Configuration:
Bulk Snippet Config Example
Cisco: ACI Client Endpoint Configuration
Cisco: ACI Contract Consumer / Provider Config
Cisco: ACI Domain Configuration
Cisco: ACI Networking Configuration
Microsoft: Azure Cloud Service Configuration
Microsoft: Azure SQL Database Configuration
Microsoft: Azure Storage Container Configuratic
Microsoft: Azure Virtual Machine Configuration
Microsoft: Azure Virtual Network Configuration
NetApp: LUN Config C-Mode
NetApp: Port Config C-Mode
NetApp: Volume Config C-Mode
Bulk Snippet Performance:
AWS EBS Instance Performance
AWS EC2 Instance Performance
Cisco: ACI Fabric Switch Module Health Scores
Microsoft: Azure SQL Database Performance
Microsoft: Azure Storage Account Blob Performa
Microsoft: Azure Storage Account Queue Perfor
Microsoft: Azure Storage Account Table Perforn
Microsoft: Azure Virtual Machine CPU Performa
Microsoft: Azure Virtual Machine CPU Performa

Select A Dynamic Application First

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

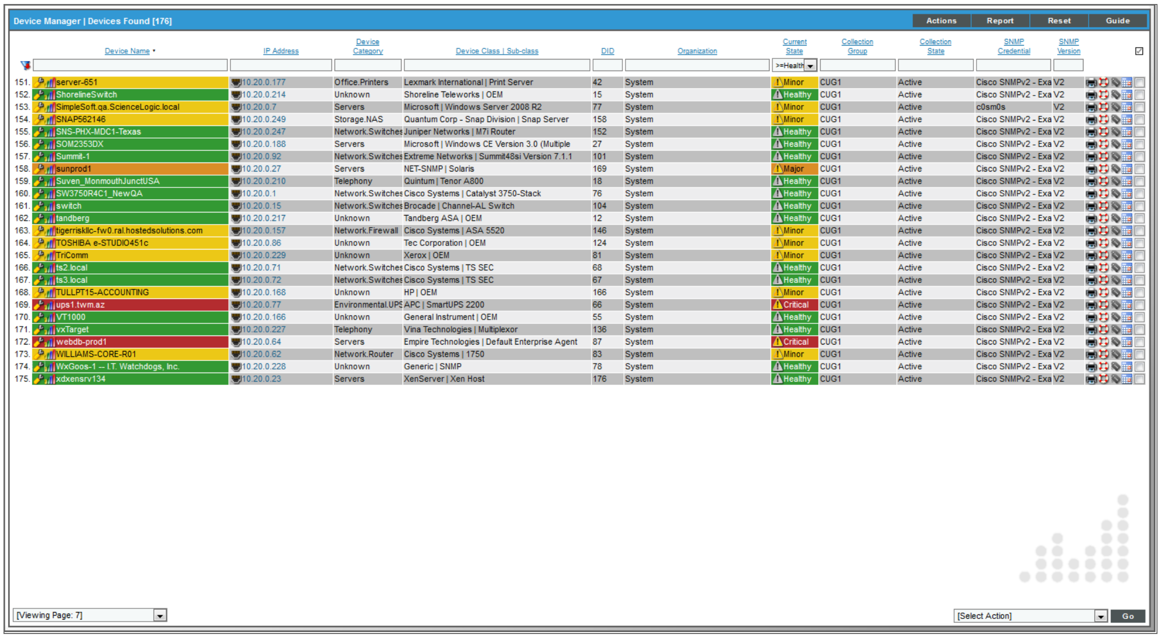
Aligning the RabbitMQ Device Class

By default, SL1 discovers the server running the RabbitMQ system as a Linux, Windows, or Pingable device. Optionally, you can align the AMQP | RabbitMQ device class to the device.

To align the device class:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).

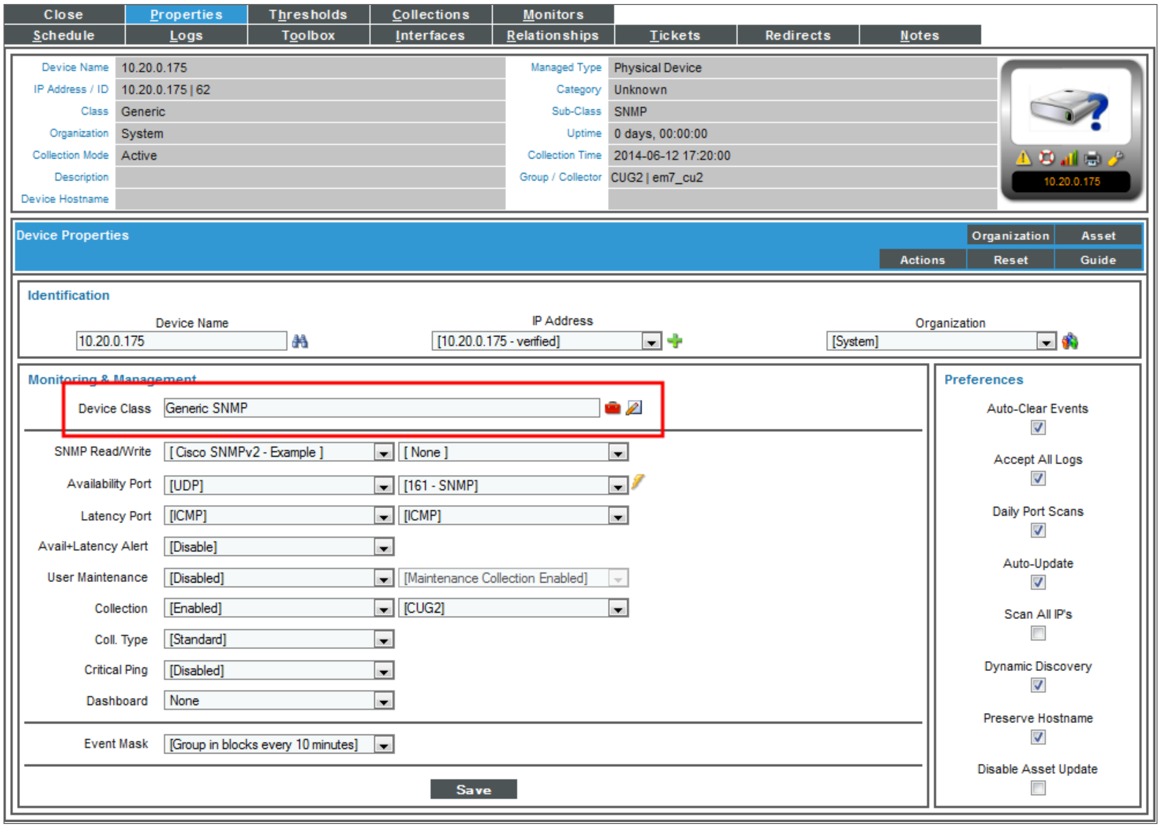
2. Find the device you want to edit. Click its wrench icon (🔧).



Device Manager | Devices Found [176]

	Device Name •	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State	Collection Group	Collection State	SNMP Credential	SNMP Version	☑
							>=Health					
151.	server-651	10.20.0.177	Office.Printers	Lexmark International | Print Server	42	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
152.	ShorelineSwitch	10.20.0.214	Unknown	Shoreline Teleworks | OEM	15	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
153.	SimpleSoft.qa.ScienceLogic.local	10.20.0.7	Servers	Microsoft | Windows Server 2008 R2	77	System	Minor	CUG1	Active	c0sm0s	V2	☐
154.	SNAP562146	10.20.0.249	Storage.NAS	Quantum Corp - Snap Division | Snap Server	158	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
155.	SNS-PHX-MDC1-Texas	10.20.0.247	Network.Switches	Juniper Networks | M7i Router	152	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
156.	SOM2353DX	10.20.0.188	Servers	Microsoft | Windows CE Version 3.0 (Multiple	27	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
157.	Summit-1	10.20.0.92	Network.Switches	Extreme Networks | Summit48si Version 7.1.1	101	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
158.	sunprod1	10.20.0.27	Servers	NET-SNMP | Solaris	169	System	Major	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
159.	Suven_MonmouthJunctUSA	10.20.0.210	Telephony	Quintum | Tenor A800	18	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
160.	SW3750R4C1_NewQA	10.20.0.1	Network.Switches	Cisco Systems | Catalyst 3750-Stack	76	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
161.	switch	10.20.0.15	Network.Switches	Brocade | Channel-AL Switch	104	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
162.	tandberg	10.20.0.217	Unknown	Tandberg ASA | OEM	12	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
163.	tigerriskllc-fw0.ral.hostedsolutions.com	10.20.0.157	Network.Firewall	Cisco Systems | ASA 5520	146	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
164.	TOSHIBA e-STUDIO451c	10.20.0.86	Unknown	Tec Corporation | OEM	124	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
165.	TriComm	10.20.0.229	Unknown	Xerox | OEM	81	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
166.	ts2.local	10.20.0.71	Network.Switches	Cisco Systems | TS SEC	68	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
167.	ts3.local	10.20.0.72	Network.Switches	Cisco Systems | TS SEC	67	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
168.	TULLPT15-ACCOUNTING	10.20.0.168	Unknown	HP | OEM	166	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
169.	ups1.twm.az	10.20.0.77	Environmental.UPS	APC | SmartUPS 2200	66	System	Critical	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
170.	VT1000	10.20.0.166	Unknown	General Instrument | OEM	55	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
171.	vxTarget	10.20.0.227	Telephony	Vina Technologies | Multiplexor	136	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
172.	webdb-prod1	10.20.0.64	Servers	Empire Technologies | Default Enterprise Agent	87	System	Critical	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
173.	WILLIAMS-CORE-R01	10.20.0.62	Network.Router	Cisco Systems | 1750	83	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
174.	WxGoos-1 -- I.T. Watchdogs, Inc.	10.20.0.228	Unknown	Generic | SNMP	78	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐
175.	xdxensrv134	10.20.0.23	Servers	XenServer | Xen Host	176	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa	V2	☐

3. In the **Device Properties** page, find the *Device Class* field. Click the toolbox icon (🧰).



Device Name	10.20.0.175	Managed Type	Physical Device
IP Address / ID	10.20.0.175 | 62	Category	Unknown
Class	Generic	Sub-Class	SNMP
Organization	System	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2014-06-12 17:20:00
Description		Group / Collector	CUG2 | em7_cu2
Device Hostname			

Identification

Device Name: 10.20.0.175
IP Address: [10.20.0.175 - verified]
Organization: [System]

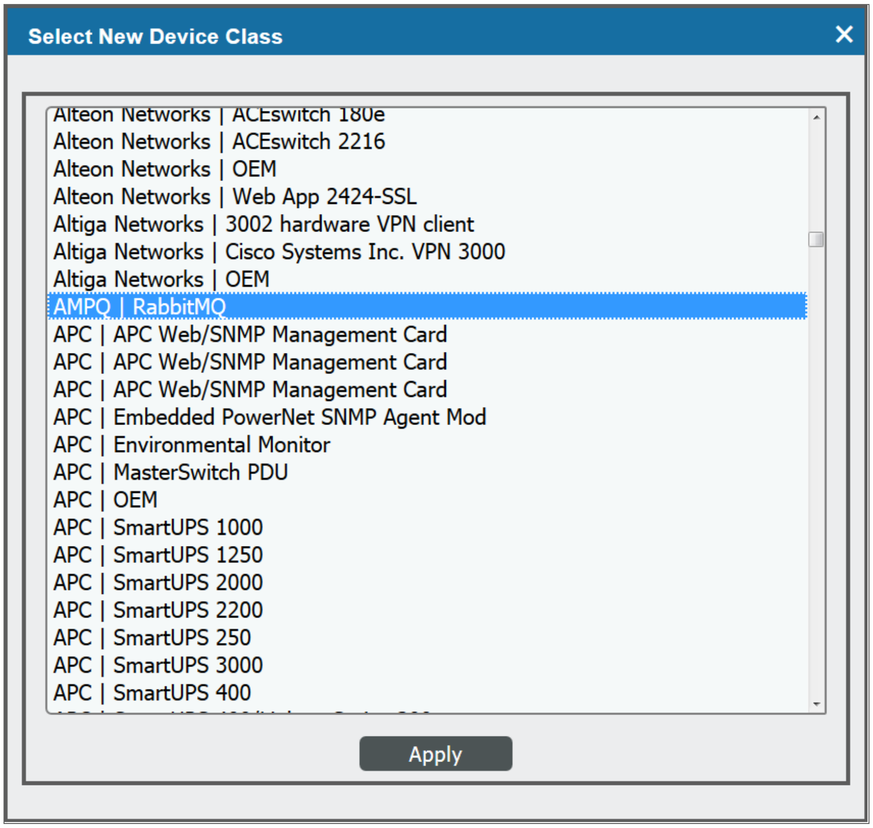
Monitoring & Management

Device Class: Generic SNMP
SNMP Read/Write: [Cisco SNMPv2 - Example] [None]
Availability Port: [UDP] [161 - SNMP]
Latency Port: [ICMP] [ICMP]
Avail+Latency Alert: [Disable]
User Maintenance: [Disabled] [Maintenance Collection Enabled]
Collection: [Enabled] [CUG2]
Coll. Type: [Standard]
Critical Ping: [Disabled]
Dashboard: None
Event Mask: [Group in blocks every 10 minutes]

Preferences

Auto-Clear Events ☑
Accept All Logs ☑
Daily Port Scans ☑
Auto-Update ☑
Scan All IP's ☐
Dynamic Discovery ☑
Preserve Hostname ☑
Disable Asset Update ☐

4. In the **Select New Device Class** modal page, select the AMQP | RabbitMQ device class.


Select New Device Class
Alteon Networks | ACEswitch 180e
Alteon Networks | ACEswitch 2216
Alteon Networks | OEM
Alteon Networks | Web App 2424-SSL
Altiga Networks | 3002 hardware VPN client
Altiga Networks | Cisco Systems Inc. VPN 3000
Altiga Networks | OEM
AMPQ | RabbitMQ
APC | APC Web/SNMP Management Card
APC | APC Web/SNMP Management Card
APC | APC Web/SNMP Management Card
APC | Embedded PowerNet SNMP Agent Mod
APC | Environmental Monitor
APC | MasterSwitch PDU
APC | OEM
APC | SmartUPS 1000
APC | SmartUPS 1250
APC | SmartUPS 2000
APC | SmartUPS 2200
APC | SmartUPS 250
APC | SmartUPS 3000
APC | SmartUPS 400
Apply

5. Click the **[Apply]** button.
6. In the **Device Properties** page, deselect the ***Auto-Update*** checkbox.
7. Click the **[Save]** button.

Chapter

6

Aruba Central

Overview

The following sections describe how to configure and discover Aruba Central virtual controllers for monitoring by SL1 using the *Aruba Central* PowerPack:

NOTE: For more information about the *Aruba Central* PowerPack, see the ***Monitoring Aruba Central*** manual.

Prerequisites for Monitoring Aruba Central

Before you can monitor Aruba Central virtual controllers and their component devices using the *Aruba Central* PowerPack, you must first have the following information:

- Aruba Central username and password
- Aruba Central customer ID

- Aruba Central client ID
- Aruba Central client secret key

You can request these items by registering with Aruba Technical Support.

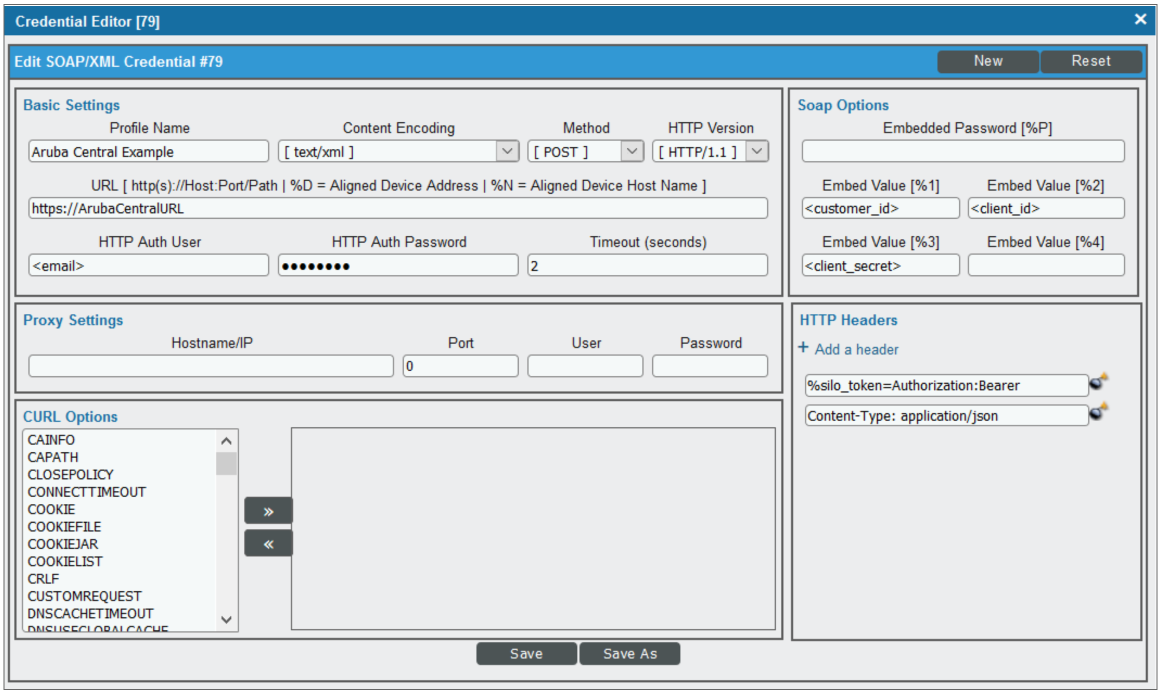
Configuring Aruba Central Credentials

To configure SL1 to monitor Aruba Central devices, you must first create a SOAP/XML credential. This credential allows the Dynamic Applications in the *Aruba Central* PowerPack to use your Aruba Central user account to retrieve information from the Aruba Central virtual controller and component devices.

The PowerPack includes an example SOAP/XML credential (**Aruba Central Example**) that you can edit for your own use.

To configure a SOAP/XML credential to access Aruba Central:

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



Basic Settings

Profile Name: Aruba Central Example

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://ArubaCentralURL

HTTP Auth User: <email>

HTTP Auth Password: ••••••••

Timeout (seconds): 2

Soap Options

Embedded Password [%P]:

Embed Value [%1]: <customer_id>

Embed Value [%2]: <client_id>

Embed Value [%3]: <client_secret>

Embed Value [%4]:

Proxy Settings

Hostname/IP:

Port: 0

User:

Password:

HTTP Headers

+ Add a header

%silo_token=Authorization:Bearer

Content-Type: application/json

CURL Options

3. Complete the following fields:

Basic Settings

- ***Profile Name***. Type a new name for the Aruba Central credential.
- ***URL***. Type your Aruba Central URL.

- ***HTTP Auth User***. Type your Aruba Central username email address.
- ***HTTP Auth Password***. Type your Aruba Central password.

SOAP Options

- ***Embed Value [%1]***. Type your Aruba Central customer ID.
- ***Embed Value [%2]***. Type your Aruba Central client ID.
- ***Embed Value [%3]***. Type your Aruba Central client secret key.

HTTP Headers

- Keep the default values that appear in this section.

4. For the remaining fields, use the default values.
5. Click the **[Save As]** button.

Discovering Aruba Central Devices

To discover and monitor your Aruba Central virtual controller, you must do the following:

- Create a virtual device representing the virtual controller
- Configure the Aruba Central device template that is included in the *Aruba Central* PowerPack
- Align the device template to the Aruba Central virtual device

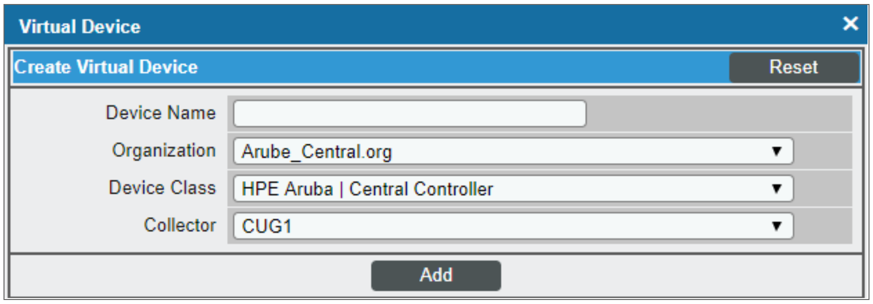
Each of these steps is documented in the following sections.

Creating an Aruba Central Virtual Device

Because the Aruba Central virtual controller does not have a static IP address, you cannot discover an Aruba Central device by running a discovery session. Instead, you must create a ***virtual device*** that represents the Aruba Central virtual controller. A virtual device is a user-defined container that represents a device or service that cannot be discovered by SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications.

To create a virtual device that represents your Aruba Central virtual controller:

1. Go to the **Device Manager** page (Devices > Device Manager, or Registry > Devices > Device Manager in the SL1 classic user interface).
2. Click the **[Actions]** button and select *Create Virtual Device* from the menu. The **Virtual Device** modal page appears:



Device Name
Organization: Arube_Central.org
Device Class: HPE Aruba | Central Controller
Collector: CUG1

3. Complete the following fields:
   - ***Device Name***. Type a name for the device.
   - ***Organization***. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.
   - ***Device Class***. Select *HPE Aruba | Central Controller*.
   - ***Collector***. Select the collector group that will monitor the device.
4. Click **[Add]** to create the virtual device.

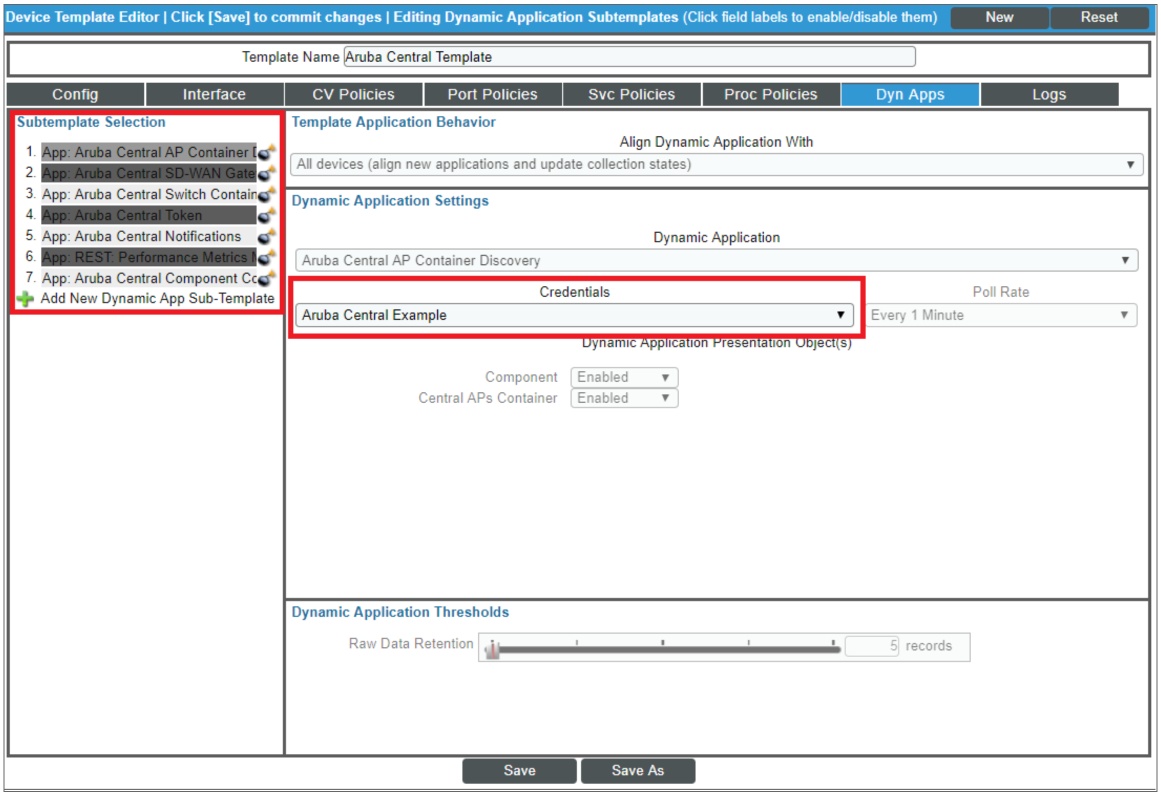
Configuring the Aruba Central Device Template

A ***device template*** allows you to save a device configuration and apply it to multiple devices. The *Aruba Central* PowerPack includes the "Aruba Central Template," which enables SL1 to align all of the necessary Dynamic Applications to the virtual controller root component device.

Before you can use the "Aruba Central Template", you must configure the template so that each Dynamic Application in the template aligns with the ***credential you created earlier***.

To configure the Aruba Central device template:

1. Go to the **Configuration Templates** page (Devices > Templates, or Registry > Devices > Templates in the SL1 classic user interface).
2. Locate the "Aruba Central Template" and click its wrench icon (🔧). The **Device Template Editor** modal page appears.
3. Click the **[Dyn Apps]** tab. The **Editing Dynamic Application Subtemplates** page appears:


Device Template Editor | Click [Save] to commit changes | Editing Dynamic Application Subtemplates (Click field labels to enable/disable them)
New
Reset
Config
Interface
CV Policies
Port Policies
Svc Policies
Proc Policies
Dyn Apps
Logs
Save
Save As

Template Name: Aruba Central Template

Subtemplate Selection

1. App: Aruba Central AP Container I
2. App: Aruba Central SD-WAN Gate
3. App: Aruba Central Switch Contain
4. App: Aruba Central Token
5. App: Aruba Central Notifications
6. App: REST: Performance Metrics I
7. App: Aruba Central Component Co

Add New Dynamic App Sub-Template

Template Application Behavior

Align Dynamic Application With: All devices (align new applications and update collection states)

Dynamic Application Settings

Dynamic Application: Aruba Central AP Container Discovery

Credentials: Aruba Central Example

Poll Rate: Every 1 Minute

Dynamic Application Presentation Object(s)

Component: Enabled

Central APs Container: Enabled

Dynamic Application Thresholds

Raw Data Retention: 5 records

4. In the ***Credentials*** drop-down list, select the credential that you created for Aruba Central.
5. Click the next Dynamic Application listed in the **Subtemplate Selection** section on the left side of the page and then select the credential you created in the ***Credentials*** field.
6. Repeat step 5 until you have selected your Aruba Central credential in the ***Credentials*** field for all of the Dynamic Applications listed in the **Subtemplate Selection** section.
7. Click **[Save]**.

> **NOTE:** To maintain a "clean" version of the template, type a new name in the ***Template Name*** field and then click **[Save As]** instead of **[Save]**.

Aligning the Device Template to Your Aruba Central Virtual Device

After you have configured the Aruba Central device template so that each Dynamic Application in the template aligns with your Aruba Central credential, you can use that template to align the Dynamic Applications to the virtual device that you created to act as the root device for your Aruba Central virtual controller. When you do so, SL1 discovers and models all of the components in your Aruba Central virtual controller.

To align the Aruba Central device template to the Aruba Central virtual device:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).

2. On the **Device Manager** page, select the checkbox for the Aruba Central virtual device.
3. In the ***Select Action*** field, in the lower right corner of the page, select the option *MODIFY by Template* and then click the **[Go]** button. The **Device Template Editor** page appears.
4. In the ***Template*** drop-down list, select your Aruba Central device template.
5. Click the **[Apply]** button, and then click **[Confirm]** to align the Dynamic Applications to the root component device.

Chapter

7

Cisco: ACI

Overview

The following sections describe how to configure and discover Cisco Application Centric Infrastructure (ACI) component devices for monitoring by SL1 using the *Cisco: ACI* PowerPack:

NOTE: For more information about the *Cisco: ACI* PowerPack, see the ***Monitoring Cisco ACI*** manual.

Prerequisites for Monitoring Cisco ACI

To configure the SL1 system to monitor a Cisco ACI system using the *Cisco: ACI* PowerPack, you must first:

- Know the credentials (username and password) for a user account that has access to the API for the Cisco ACI system. The user account must have read-all access.
- Ensure that the APIC in your ACI system supports TLS 1.1 or TLS 1.2. SL1 does not support TLS 1.0.

NOTE: If the credentials for your account have been changed, the PowerPack will not recognize the new credentials. To recognize new credentials, you can either delete or disable the previous administrator account, or delete any cache entries with "1C88582E76AADD40EB8C5E6A6F71B64A_ACI_{host}_{cred_id}_TOKENS".

Recommended System Values

ScienceLogic recommends that you set the following values on your Cisco ACI system:

- ***ACI HTTPS Throttle***. 5 requests per second.
- ***Web Session Timeout***. 600 seconds or greater.
- ***Web Session Idle Timeout***. 600 seconds (default).

Configuring a Credential for the Cisco ACI System

To use the Dynamic Applications in the *Cisco: ACI* PowerPack, you must first define an ACI credential in SL1. This credential allows SL1 to collect data from your ACI system.

NOTE: You will need to create a separate credential for each APIC that you want to discover.

The *Cisco: ACI* PowerPack includes the following example credentials that you can use as templates when creating your own credentials for discovering your ACI system:

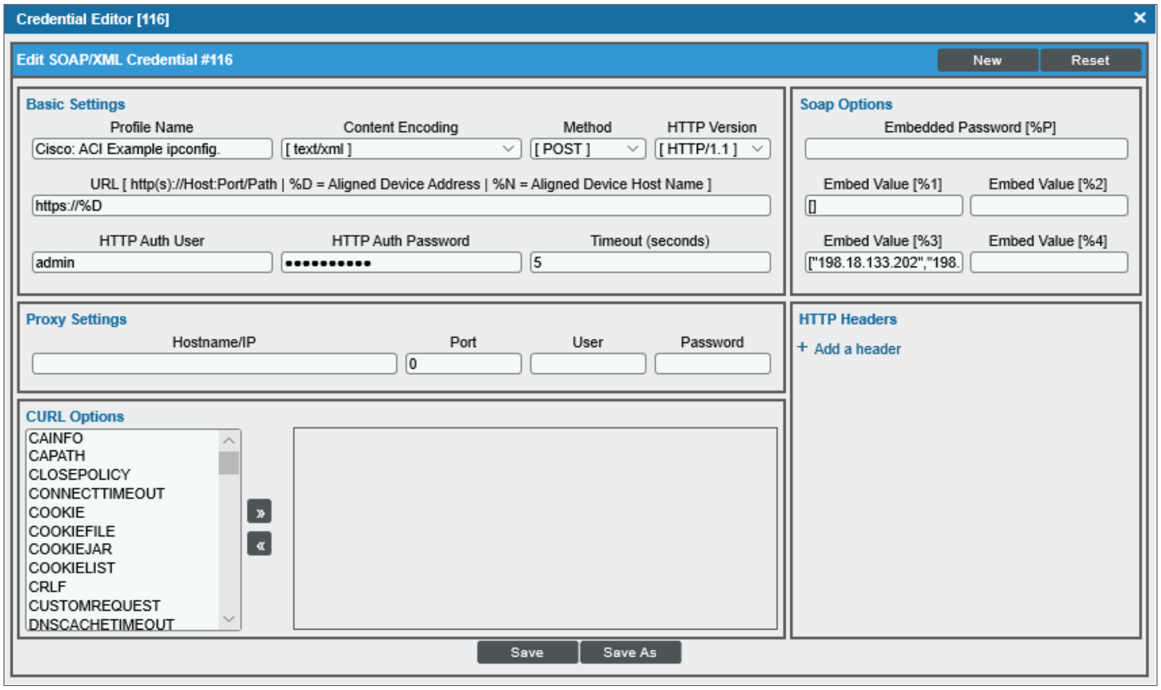
- ***Cisco: ACI Example Priority***. Use this SOAP/XML credential if you want to specify particular APICs from which SL1 should ***not*** collect data and to establish the precedence order of the APICs in the event that the first one fails.
- ***Cisco: ACI Sample Credential***. Use this Basic/Snippet credential if you want to discover an ACI system without specifying APICs that should not be monitored or the APIC precedence order.

The following sections describe how to configure these credentials.

Creating a SOAP/XML Credential for Cisco ACI

To configure a SOAP/XML credential for Cisco ACI, perform the following steps:

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



Credential Editor [116]

Edit SOAP/XML Credential #116

Basic Settings

Profile Name: Cisco: ACI Example ipconfig.

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://%D

HTTP Auth User: admin

HTTP Auth Password: ●●●●●●●●●●

Timeout (seconds): 5

Soap Options

Embedded Password [%P]:

Embed Value [%1]: []

Embed Value [%2]:

Embed Value [%3]: ["198.18.133.202","198.

Embed Value [%4]:

Proxy Settings

Hostname/IP:

Port: 0

User:

Password:

HTTP Headers

CURL Options

3. Enter values in the following fields:

Basic Settings

- ***Profile Name***. Type a new name for the credential.
- ***URL***. Type "%D". You can type the IP address of the cluster where the APIC resides, but this is not recommended.
- ***HTTP Auth User***. Type the username for a user account that has read-all access to the APIC API.
- ***HTTP Auth Password***. Type the password for the username you entered in the ***HTTP Auth User*** field.
- ***Timeout***. It is recommended that you set this value to 5 seconds or lower.

NOTE: If the credentials for your account have been changed, the PowerPack will not recognize the new credentials. To recognize new credentials, you can either delete or disable the previous administrator account, or delete any cache entries with "1C88582E76AADD40EB8C5E6A6F71B64A_ACI_{host}_{cred_id}_TOKENS".

SOAP Options

- ***Embed Value [%1]***. If you want to specify one or more APICs from which SL1 should ***not*** collect data, type the IP addresses of those APICs.
- ***Embed Value [%3]***. If you want to specify the APIC precedence order, type the IP addresses of the APICs in your desired precedence order. When you do so, if the primary APIC being monitored becomes unavailable, SL1 will use this order to determine the next APIC it should monitor instead.

> NOTE: When entering IP addresses in the ***Embed Value [%1]*** or ***Embed Value [%3]*** fields, each IP address should be surrounded by quotation marks and include a comma and space between IP addresses. Additionally, the list of IP addresses should be surrounded by brackets. For example: ["198.18.133.200", "198.18.133.201", "198.18.133.202"]

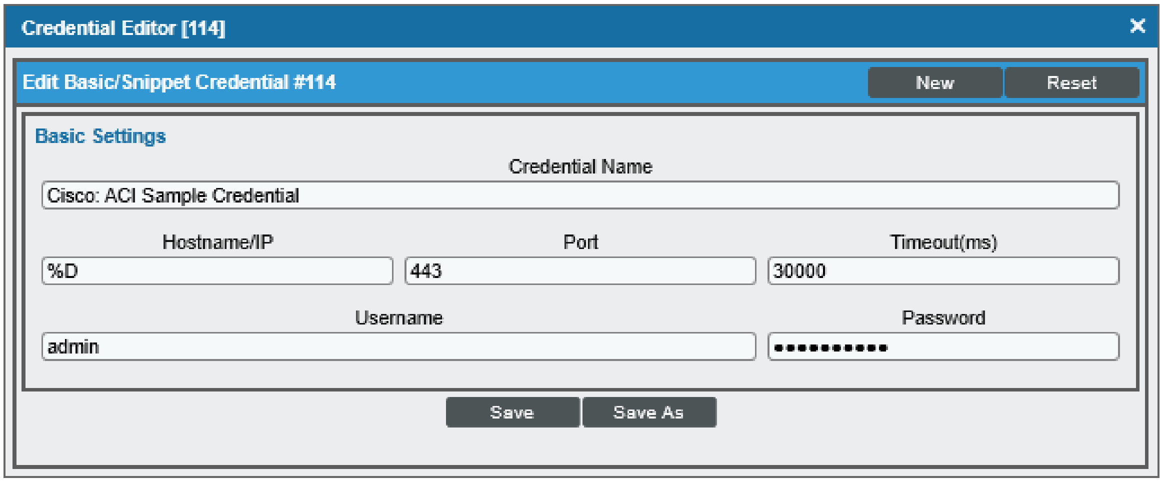
> NOTE: When creating the *discovery session*, the **first** entry in the ***Embed Value [%3]*** field must be entered in the ***IP Address Discovery List*** field in the **Discovery Session Editor**.

4. Click **[Save As]**.
5. In the confirmation message, click **[OK]**.

Creating a Basic/Snippet Credential for Cisco ACI

To configure a Basic/Snippet credential for Cisco ACI, perform the following steps:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the wrench icon (🔧) for *Cisco: ACI Sample Credential*. The **Credential Editor** page appears:



Credential Editor [114]

Edit Basic/Snippet Credential #114

Basic Settings

Credential Name: Cisco: ACI Sample Credential

Hostname/IP: %D

Port: 443

Timeout(ms): 30000

Username: admin

Password: ●●●●●●●●●●●

3. Supply values in the following fields:

- ***Credential Name***. Type a new name for the credential.
- ***Hostname/IP***. Type "%D". You can enter the IP address of the cluster where the APIC resides, but this is not recommended.
- ***Username***. Type the username for a user account that has read-all access to the APIC API.
- ***Password***. Type the password for the username you entered in the ***Username*** field.

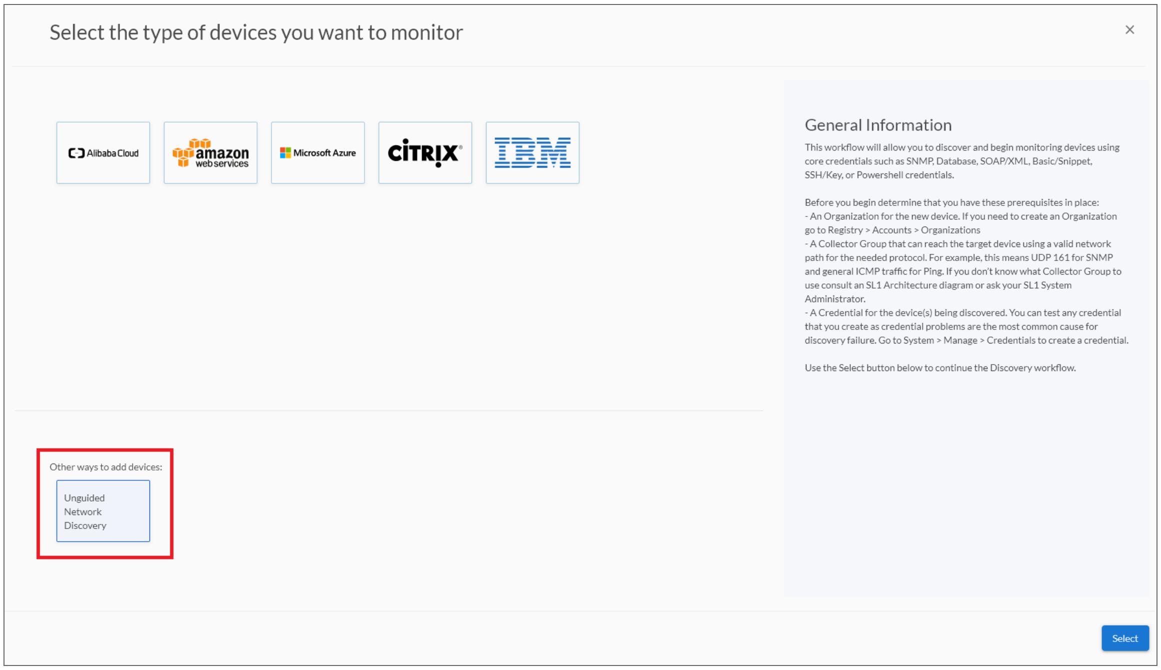
NOTE: If the credentials for your account have been changed, the PowerPack will not recognize the new credentials. To recognize new credentials, you can either delete or disable the previous administrator account, or delete any cache entries with "1C88582E76AADD40EB8C5E6A6F71B64A_ACI_{host}_{cred_id}_TOKENS".

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

Discovering a Cisco ACI System

To discover a Cisco ACI system, perform the following steps:

1. On the **Devices** page (🖥) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears:



Select the type of devices you want to monitor

General Information

This workflow will allow you to discover and begin monitoring devices using core credentials such as SNMP, Database, SOAP/XML, Basic/Snippet, SSH/Key, or Powershell credentials.

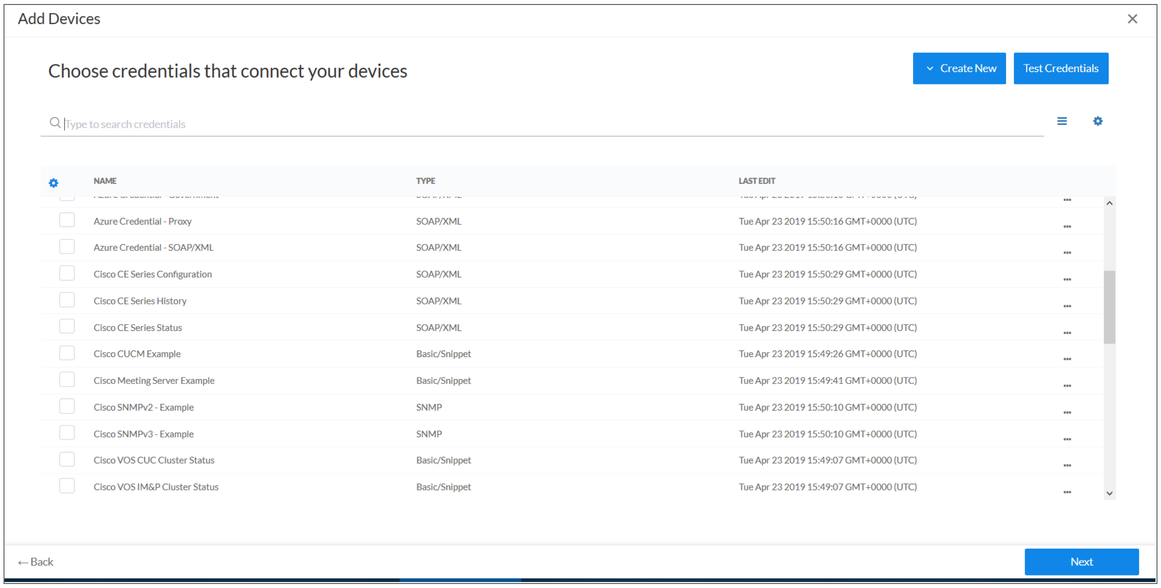
Before you begin determine that you have these prerequisites in place:
- An Organization for the new device. If you need to create an Organization go to Registry > Accounts > Organizations
- A Collector Group that can reach the target device using a valid network path for the needed protocol. For example, this means UDP 161 for SNMP and general ICMP traffic for Ping. If you don't know what Collector Group to use consult an SL1 Architecture diagram or ask your SL1 System Administrator.
- A Credential for the device(s) being discovered. You can test any credential that you create as credential problems are the most common cause for discovery failure. Go to System > Manage > Credentials to create a credential.

Use the Select button below to continue the Discovery workflow.

2. Click the **[Unguided Network Discovery]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.
3. Click **[Select]**. The **Add Devices** page appears.
4. Complete the following fields:

- ***Name***. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.
- ***Description***. Optional. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **[Discovery Sessions]** tab.
- ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered devices

5. Click **[Next]**. The **Credentials** page of the **Add Devices** wizard appears:

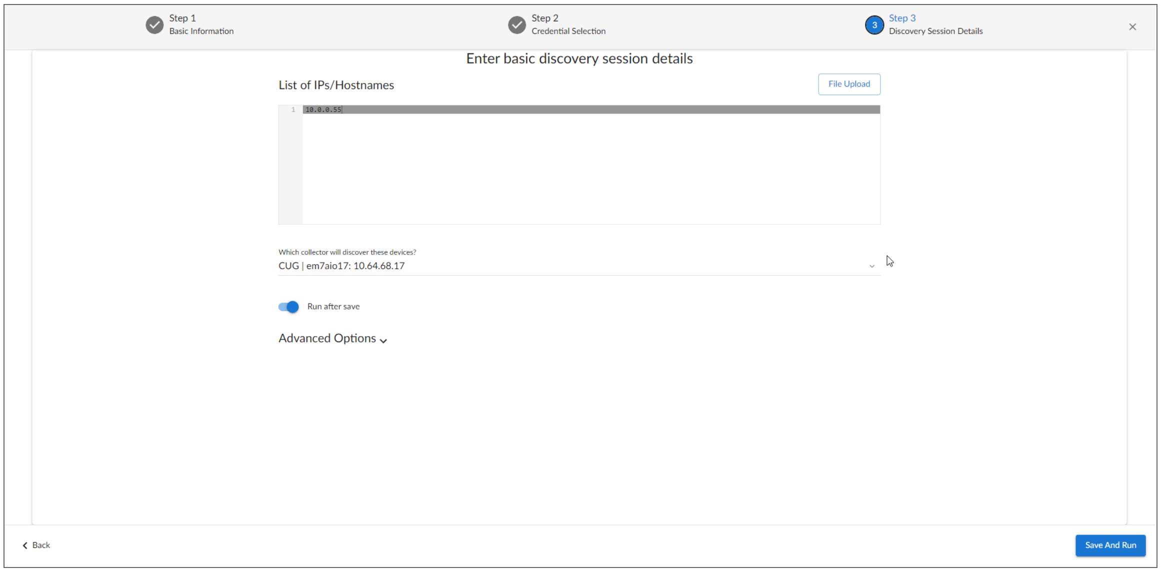


Choose credentials that connect your devices

Type to search credentials

	NAME	TYPE	LAST EDIT	
□	Azure Credential - Proxy	SOAP/XML	Tue Apr 23 2019 15:50:16 GMT+0000 (UTC)	...
□	Azure Credential - SOAP/XML	SOAP/XML	Tue Apr 23 2019 15:50:16 GMT+0000 (UTC)	...
□	Cisco CE Series Configuration	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)	...
□	Cisco CE Series History	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)	...
□	Cisco CE Series Status	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)	...
□	Cisco CUCM Example	Basic/Snippet	Tue Apr 23 2019 15:49:26 GMT+0000 (UTC)	...
□	Cisco Meeting Server Example	Basic/Snippet	Tue Apr 23 2019 15:49:41 GMT+0000 (UTC)	...
□	Cisco SNMPv2 - Example	SNMP	Tue Apr 23 2019 15:50:10 GMT+0000 (UTC)	...
□	Cisco SNMPv3 - Example	SNMP	Tue Apr 23 2019 15:50:10 GMT+0000 (UTC)	...
□	Cisco VOS CUC Cluster Status	Basic/Snippet	Tue Apr 23 2019 15:49:07 GMT+0000 (UTC)	...
□	Cisco VOS IM&P Cluster Status	Basic/Snippet	Tue Apr 23 2019 15:49:07 GMT+0000 (UTC)	...

6. On the **Credentials** page, locate and select the *credential* you created for the Cisco ACI system.
7. Click **[Next]**. The **Discovery Session Details** page of the **Add Devices** wizard appears:



Enter basic discovery session details

List of IPs/Hostnames

```
10.0.0.55
```

Which collector will discover these devices?
CUG | em7aio17: 10.64.68.17

● Run after save

8. Complete the following fields:

- ***List of IPs/Hostnames***. Type the IP address of the **first** controller listed in the ***Embed Value [%3]*** field of the ***SOAP/XML credential***.
- ***Which collector will monitor these devices?***. Required. Select an existing collector to monitor the discovered devices.
- ***Run after save***. Select this option to run this discovery session as soon as you save the session.

  In the **Advanced options** section, click the down arrow icon (⌄) to complete the following fields:

  - ***Discover Non-SNMP***. Enable this setting.

9. Click **[Save and Run]** if you enabled the Run after save setting, or **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.
10. If you selected the **Run after save** option on this page, the discovery session runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page includes a link to the **Device Investigator** page for the discovered device.

NOTE: In version 109 and later, the tenant's IP address will match the APIC used for the API calls. If failover occurs, the ACI root IP stays the same, but the tenants will get new IP addresses.

NOTE: If failover occurs during discovery of an ACI system using a ***SOAP/XML credential***, it will fail over to the next IP address in the ***Embed Value [%3]*** field.

NOTE: If failover occurs during discovery of an ACI system using a ***Basic Snippet credential***, the APIC with the subsequent controller ID will be used.

NOTE: If your discovery session causes an HTTP 403 error, edit the ***Basic Snippet credential*** so that the ***Hostname/IP*** field contains ***only a single IP address*** and then re-try discovery.

The initial discovery of a Cisco ACI system will align most Dynamic Applications; however, you will need to manually align the "Cisco: ACI IC UpTime" Dynamic Application for the internal collections data to be displayed on the **Device Properties** page (Registry > Devices > wrench icon).

To manually align the "Cisco: ACI IC UpTime" Dynamic Application:

1. After the discovery session has completed, find the Cisco ACI device in the **Devices** page and click on it.
2. From the **Device Investigator** page for the Cisco ACI device, click the **[Collections]** tab.
3. Click **[Edit]** and then click **[Align Dynamic App]**. The **Align Dynamic Application** window appears.
4. Click *Choose Dynamic Application*. The **Choose Dynamic Application** window appears.
5. Select the "Cisco: ACI IC UpTime" Dynamic Application and click **[Select]**. The name of the selected Dynamic Application appears in the **Align Dynamic Application** window.

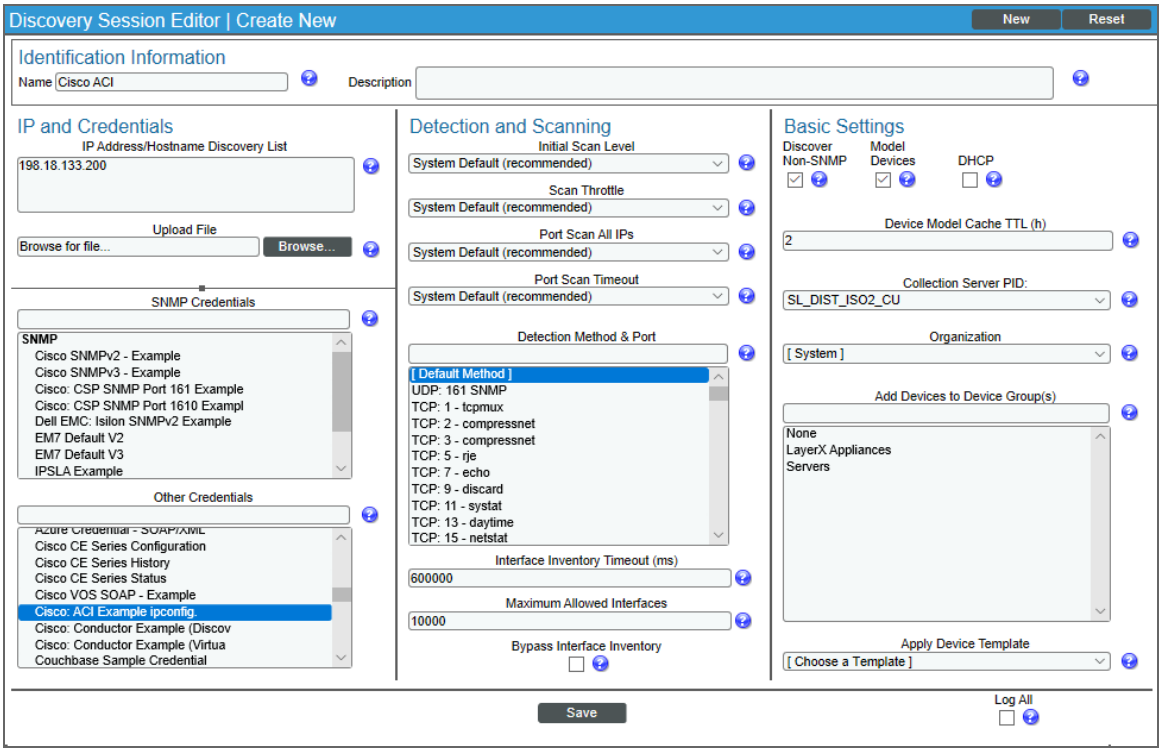
6. If a default credential is listed below the Dynamic Application and it is the *credential you created*, skip ahead to step 9. Otherwise, uncheck the box next to the credential name.
7. Click *Choose Credential*. The **Choose Credential** window appears.
8. Select the *credential you created for your Cisco ACI device* for the Dynamic Application and click the **[Select]** button. The name of the selected credential appears in the **Align Dynamic Application** window.
9. Click the **[Align Dynamic App]** button. When the Dynamic Application is successfully aligned, it is added to the **Collections** tab, and a confirmation message appears at the bottom of the tab.

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

Discovering a Cisco ACI System in the SL1 Classic User Interface

To discover a Cisco ACI system, perform the following steps:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. Click the **[Create]** button. The **Discovery Session Editor** page appears:



Discovery Session Editor | Create New

Identification Information

Name: Cisco ACI

Description:

IP and Credentials

IP Address/Hostname Discovery List: 198.18.133.200

Upload File: Browse for file...

SNMP Credentials:
SNMP
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Cisco: CSP SNMP Port 161 Example
Cisco: CSP SNMP Port 1610 Exampl
Dell EMC: Isilon SNMPv2 Example
EM7 Default V2
EM7 Default V3
IPSLA Example

Other Credentials:
Azure Credential - SOAP/XML
Cisco CE Series Configuration
Cisco CE Series History
Cisco CE Series Status
Cisco VOS SOAP - Example
Cisco: ACI Example ipconfig.
Cisco: Conductor Example (Discov
Cisco: Conductor Example (Virtua
Couchbase Sample Credential

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: SL_DIST_ISO2_CU

Organization: [System]

Add Devices to Device Group(s):
None
LayerX Appliances
Servers

Apply Device Template: [Choose a Template]

Log All: □

3. Supply values in the following fields:

   - ***IP Address Discovery List***. Type the IP address of the **first** controller listed in the ***Embed Value [%3]*** field of the SOAP/XML credential.
   - ***Other Credentials***. Select the credential you created for the Cisco ACI system.
   - ***Discover Non-SNMP***. Select this checkbox.

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

NOTE: In version 109 and later, the tenant's IP address will match the APIC used for the API calls. If failover occurs, the ACI root IP stays the same, but the tenants will get new IP addresses.

NOTE: If failover occurs during discovery of an ACI system using a SOAP/XML credential, it will fail over to the next IP address in the ***Embed Value [%3]*** field.

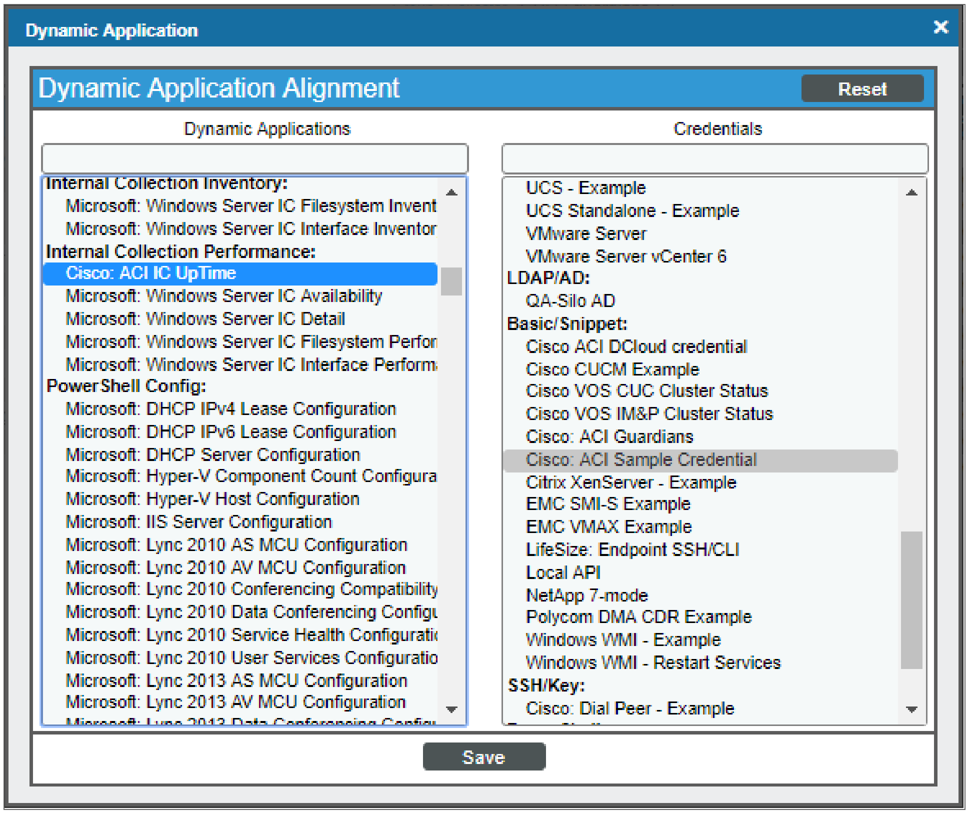
NOTE: If failover occurs during discovery of an ACI system using a Basic Snippet credential, the APIC with the subsequent controller ID will be used.

NOTE: If your discovery session causes an HTTP 403 error, edit the credential so that the ***Hostname/IP*** field contains ***only a single IP address*** and then re-try discovery.

The initial discovery of a Cisco ACI system will align most Dynamic Applications; however, you will need to manually align the "Cisco: ACI IC UpTime" Dynamic Application for the internal collections data to be displayed on the **Device Properties** page (Registry > Devices > wrench icon).

To manually align the "Cisco: ACI IC UpTime" Dynamic Application:

1. From the **Device Properties** page for the Cisco ACI system, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. In the **Dynamic Application Collections** page, click the **[Action]** button and then select *Add Dynamic Application* from the menu. The **Dynamic Application Alignment** page appears.
3. In the ***Dynamic Applications*** field, select *Cisco: ACI IC UpTime*.



Dynamic Application

Dynamic Application Alignment

Reset

Dynamic Applications

Internal Collection Inventory:
Microsoft: Windows Server IC Filesystem Invent
Microsoft: Windows Server IC Interface Inventor
Internal Collection Performance:
Cisco: ACI IC UpTime
Microsoft: Windows Server IC Availability
Microsoft: Windows Server IC Detail
Microsoft: Windows Server IC Filesystem Perfor
Microsoft: Windows Server IC Interface Perform
PowerShell Config:
Microsoft: DHCP IPv4 Lease Configuration
Microsoft: DHCP IPv6 Lease Configuration
Microsoft: DHCP Server Configuration
Microsoft: Hyper-V Component Count Configura
Microsoft: Hyper-V Host Configuration
Microsoft: IIS Server Configuration
Microsoft: Lync 2010 AS MCU Configuration
Microsoft: Lync 2010 AV MCU Configuration
Microsoft: Lync 2010 Conferencing Compatibility
Microsoft: Lync 2010 Data Conferencing Configu
Microsoft: Lync 2010 Service Health Configuratio
Microsoft: Lync 2010 User Services Configuratio
Microsoft: Lync 2013 AS MCU Configuration
Microsoft: Lync 2013 AV MCU Configuration

Credentials

UCS - Example
UCS Standalone - Example
VMware Server
VMware Server vCenter 6
LDAP/AD:
QA-Silo AD
Basic/Snippet:
Cisco ACI DCloud credential
Cisco CUCM Example
Cisco VOS CUC Cluster Status
Cisco VOS IM&P Cluster Status
Cisco: ACI Guardians
Cisco: ACI Sample Credential
Citrix XenServer - Example
EMC SMI-S Example
EMC VMAX Example
LifeSize: Endpoint SSH/CLI
Local API
NetApp 7-mode
Polycom DMA CDR Example
Windows WMI - Example
Windows WMI - Restart Services
SSH/Key:
Cisco: Dial Peer - Example

Save

4. In the ***Credentials*** field, select the credential you created for the Cisco ACI system.

5. Click the **[Save]** button.

6. After aligning the Dynamic Application, click the **[Reset]** button and then click the plus icon (+) for the Dynamic Application. If collection for the Dynamic Application was successful, the graph icons (📊) for the Dynamic Application are enabled.

Performing a Manual Failover

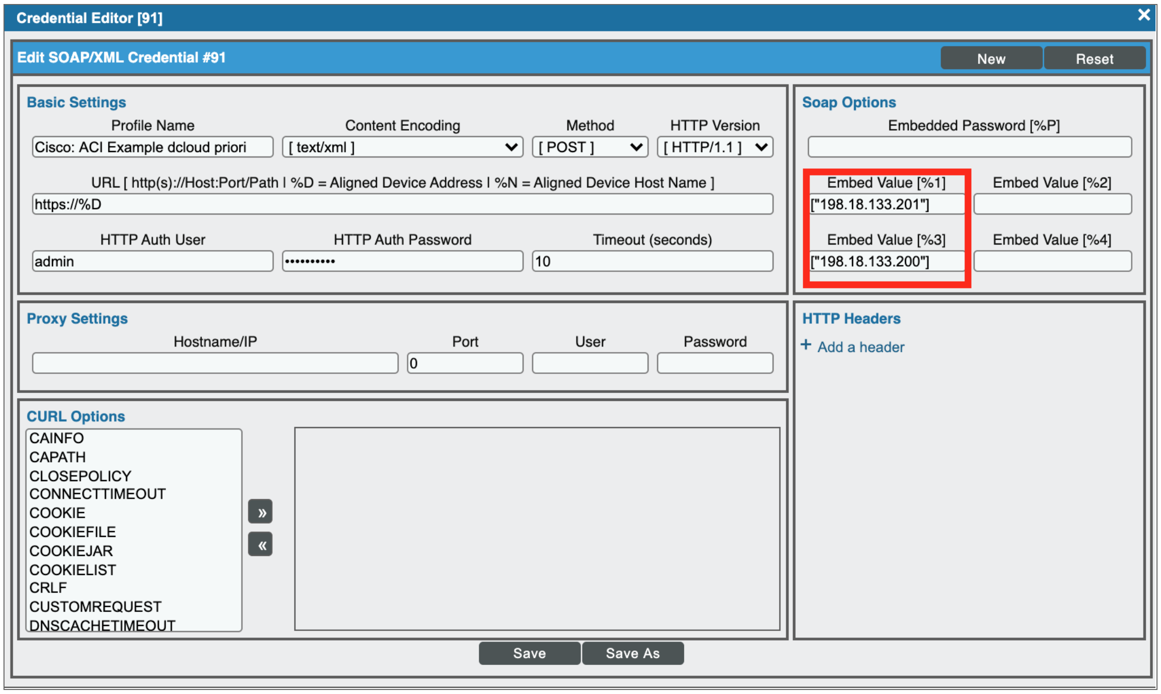
If you want to change the APIC being used by the PowerPack, you can perform a manual failover by editing your SOAP/XML credential. To do this:

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

2. Locate the SOAP/XML credential you created and then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears:

3. There are two ways to failover manually:

   - Type the IP address of the APIC that you no longer want to use in the Embed Value ***Embed Value [%1]*** field.



Profile Name: Cisco: ACI Example dcloud priori

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://%D

HTTP Auth User: admin

HTTP Auth Password: ••••••••••

Timeout (seconds): 10

Embedded Password [%P]:

Embed Value [%1]: ["198.18.133.201"]

Embed Value [%2]:

Embed Value [%3]: ["198.18.133.200"]

Embed Value [%4]:

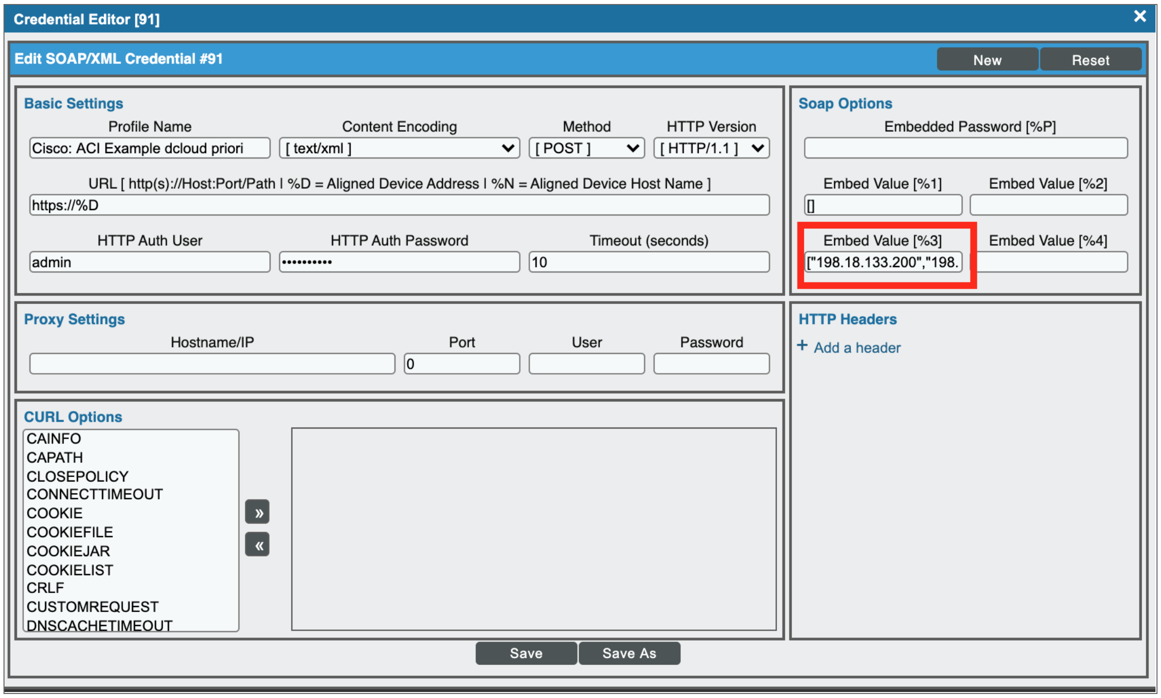
Hostname/IP:

Port: 0

User:

Password:

- Edit the ***Embed Value [3%]*** field to change the order of the APIC IP addresses, making the first IP address in the list the APIC that you want to failover to.



Profile Name: Cisco: ACI Example dcloud priori

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://%D

HTTP Auth User: admin

HTTP Auth Password: ••••••••••

Timeout (seconds): 10

Embedded Password [%P]:

Embed Value [%1]: []

Embed Value [%2]:

Embed Value [%3]: ["198.18.133.200","198.

Embed Value [%4]:

Hostname/IP:

Port: 0

User:

Password:

4. Click **[Save]**. The next time the "Cisco: ACI APIC Communications Manager" Dynamic Application runs, the PowerPack will use the new APIC IP address specified.

When SL1 performs collection for the ACI cluster, SL1 will create component devices for the components associated with the ACI system and align other Dynamic Applications to those component devices. Some of the Dynamic Applications aligned to the component devices will also be used to create additional component devices.

NOTE: If you delete a Tenant in a monitored device, that component device will still appear in SL1 but the Dynamic Applications aligned to it will stop collecting data, and a message indicating "Failed Availability" will appear in the device log of its child component devices.

You can view all the devices, virtual devices, and component devices in the Cisco ACI system in the following places in the user interface:

- The **Device Investigator** Map page (click **Map** in the **Device Investigator** page) displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the listed devices reloads the page to make the selected device the primary device.
- The **Device Components** page (Devices > Device Components) displays a list of all root devices and component devices discovered by SL1. The **Device Components** page displays all root devices and component devices in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with a Cisco ACI system, find the Cisco ACI root device and click its plus icon (+).
- The **Component Map** page (Classic Maps > Device Maps > Components) allows you to view devices by root node and view the relationships between root nodes, parent components, and child components in a map. This makes it easy to visualize and manage root nodes and their components. SL1 automatically updates the **Component Map** as new component devices are discovered. The platform also updates each map with the latest status and event information. To view the map for a Cisco ACI device, go to the **Component Map** page and select the map from the list in the left NavBar. To learn more about the **Component Map** page, see the ***Views*** manual.

Chapter

8

Cisco: ACI Multi-Site Manager

Overview

The following sections describe how to configure and discover Cisco ACI Multi-Site Manager for monitoring by SL1 using the *Cisco: ACI Multi-Site Manager* PowerPack:

> NOTE: For more information about the *Cisco: ACI Multi-Site Manager* PowerPack, see the ***Monitoring Cisco ACI Multi-Site Manager*** manual.

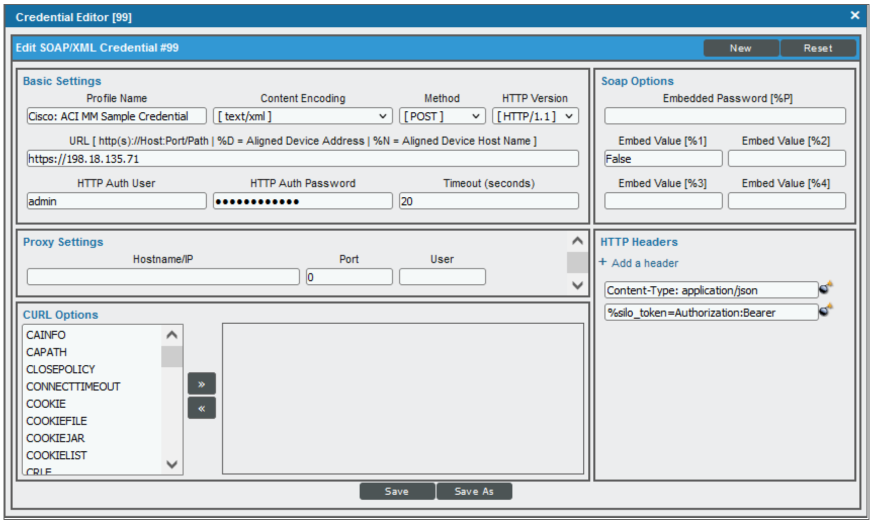
Creating a Credential for Cisco ACI Multi-Site Manager

To configure SL1 to monitor Cisco ACI Multi-Site architecture, you must first create a SOAP/XML credential. This credential allows the Dynamic Applications in the *Cisco: ACI Multi-Site Manager*PowerPack) to communicate with your Cisco ACI Multi-Site account.

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: ACI MM Sample Credential** credential, then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears.
3. Enter values in the following fields:



Credential Editor [99]

Edit SOAP/XML Credential #99

Basic Settings

Profile Name: Cisco: ACI MM Sample Credential

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://198.18.135.71

HTTP Auth User: admin

HTTP Auth Password: ●●●●●●●●●●●●●

Timeout (seconds): 20

Soap Options

Embedded Password [%P]:

Embed Value [%1]: False

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

Proxy Settings

Hostname/IP:

Port: 0

User:

HTTP Headers

Content-Type: application/json

%silo_token=Authorization:Bearer

Basic Settings

- ***HTTP Auth User***. Enter the username for the Cisco ACI Multi-Site web interface
- ***HTTP Auth Password***. Enter the password for the Cisco ACI Multi-Site web interface
- ***URL***. Specify the IP of the Cisco ACI Multi-Site web interface

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

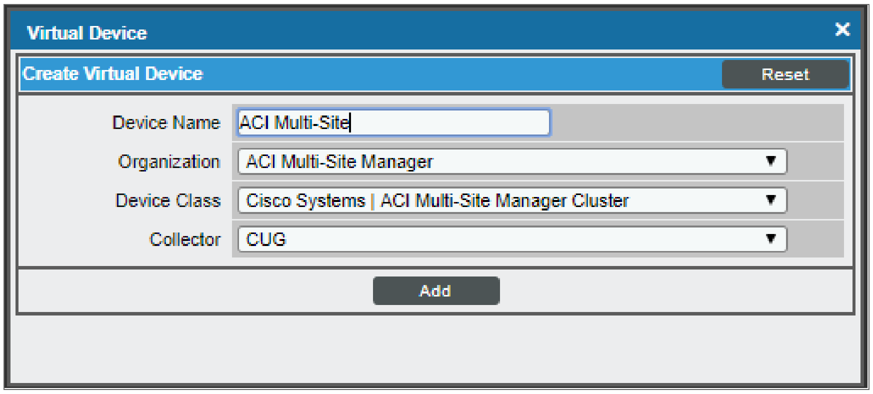
Creating a Cisco ACI Multi-Site Manager Virtual Device and Discovering Cisco ACI Multi-Site

To discover a Cisco ACI Multi-Site architecture, you must create a ***virtual device*** that represents the root device. A virtual device is a user-defined container that represents a device or service that cannot be discovered by SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications.

> TIP: If you have multiple Cisco ACI Multi-Site architecture you want to monitor, you should create a separate virtual device for each root device. You can also create different organizations for each architecture.

To create a virtual device that represents your Cisco ACI Multi-Site architecture:

1. Go to the **Device Manager** page (Devices > Device Manager, or Registry > Devices > Device Manager in the SL1 classic user interface).
2. Click the **[Actions]** button and select *Create Virtual Device* from the menu. The **Create Virtual Device** modal page appears.
3. Enter values in the following fields:



Device Name: ACI Multi-Site

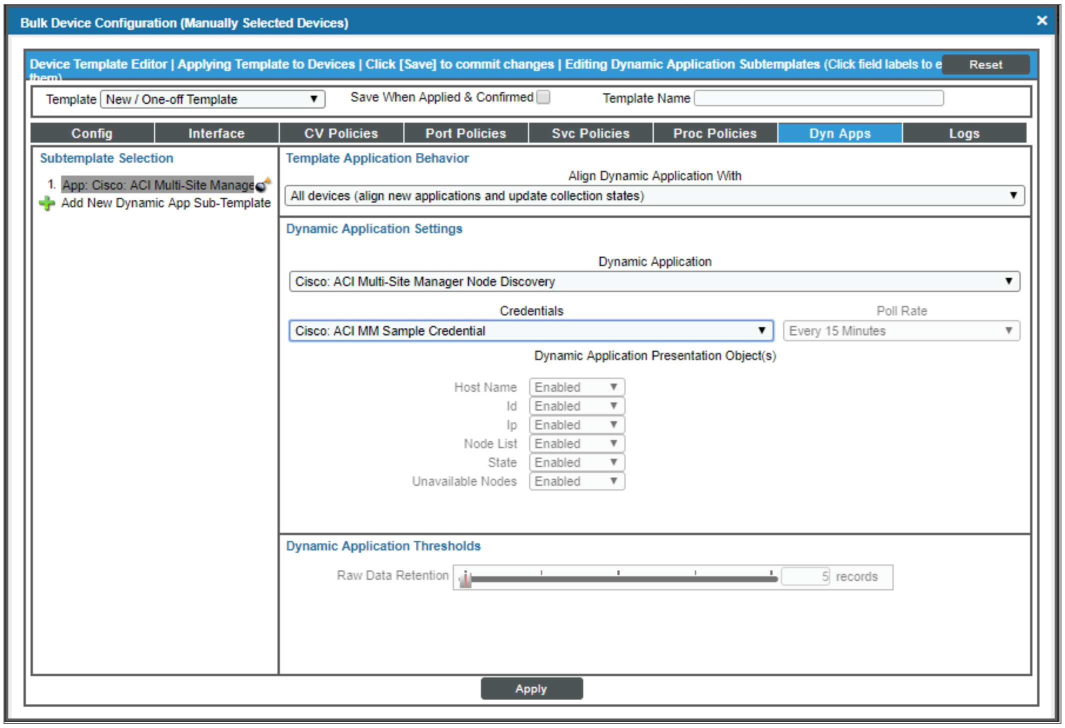
Organization: ACI Multi-Site Manager

Device Class: Cisco Systems | ACI Multi-Site Manager Cluster

Collector: CUG

- ***Device Name***. Enter a name for the device. For example, you could enter "ACI Multi-Site" in this field.
- ***Organization***. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.
- ***Device Class***. Select *Cisco Systems | ACI Multi-Site Manager Cluster*.
- ***Collector***. Select *CUG*.

4. Click the **[Add]** button to create the virtual device.
5. Once you have created the device, go to the **Device Manager** page ((Devices > Device Manager, or Registry > Devices > Device Manager in the SL1 classic user interface) and select the virtual device you created.
6. In the ***Select Action*** menu, select *MODIFY By Template* and click **[Go]**.
7. In the **Device Template Editor** window, select the **[Dyn Apps]** tab.
8. Click the plus sign in the **Subtemplate Selection** pane.
9. In the **Dynamic Application Settings** pane, select the "Cisco: ACI Multi-Site Manager Node Discovery" Dynamic Application.
10. In the ***Credentials*** drop-down, select the "Cisco: ACI MM Sample Credential". Click **[Apply]**.



Bulk Device Configuration (Manually Selected Devices)

Device Template Editor | Applying Template to Devices | Click [Save] to commit changes | Editing Dynamic Application Subtemplates (Click field labels to e them)

Template: New / One-off Template | Save When Applied & Confirmed □ | Template Name:

Subtemplate Selection
1. App: Cisco: ACI Multi-Site Manage
Add New Dynamic App Sub-Template

Template Application Behavior
Align Dynamic Application With: All devices (align new applications and update collection states)

Dynamic Application Settings
Dynamic Application: Cisco: ACI Multi-Site Manager Node Discovery
Credentials: Cisco: ACI MM Sample Credential
Poll Rate: Every 15 Minutes

Dynamic Application Presentation Object(s)
Host Name: Enabled
Id: Enabled
Ip: Enabled
Node List: Enabled
State: Enabled
Unavailable Nodes: Enabled

Dynamic Application Thresholds
Raw Data Retention: 5 records

Once you have completed modifying the device template, discovery will run and the Dynamic Applications will be aligned.

Verifying Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. After creating the virtual device and aligning the credential to the template, go to the **Devices** page and click on the ACI Multi-Site virtual device. From the **Device Investigator** page, click the **[Collections]** tab.
2. All applicable Dynamic Applications for the switch are automatically aligned during discovery and will appear in the **[Collections]** tab.

You should see the following Dynamic Applications aligned to the ACI Multi-Site virtual device:

- Cisco: ACI Multi-Site Manager Component Counts
- Cisco: ACI Multi-Site Manager Node Discovery
- Cisco: ACI Multi-Site Manager Site Discovery
- Cisco: ACI Multi-Site Manager Tenant Discovery
- Cisco: ACI Multi-Site Manager Token

The following Dynamic Applications will automatically align to their corresponding device components:

- Cisco: ACI Multi-Site Manager Node Configuration
- Cisco: ACI Multi-Site Manager Site Config

- Cisco: ACI Multi-Site Manager Site Performance
- Cisco: ACI Multi-Site Manager Tenant Config

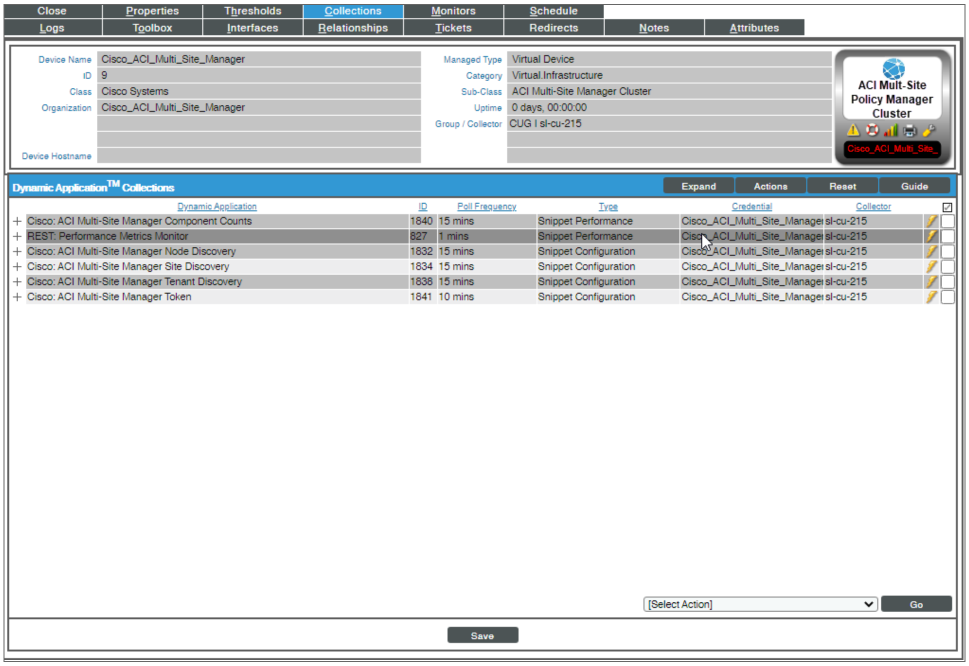
Verifying Discovery and Dynamic Application Alignment in the SL1 Classic User Interface

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. After creating the virtual device and aligning the credential to the template, go to the **Device Manager** page and click the wrench icon (🔧)for the ACI Multi-Site virtual device. From the **Device Properties** page, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. All applicable Dynamic Applications for the switch are automatically aligned during discovery.

You should see the following Dynamic Applications aligned to the ACI Multi-Site virtual device:

- Cisco: ACI Multi-Site Manager Component Counts
- Cisco: ACI Multi-Site Manager Node Discovery
- Cisco: ACI Multi-Site Manager Site Discovery
- Cisco: ACI Multi-Site Manager Tenant Discovery
- Cisco: ACI Multi-Site Manager Token



Device Name	Cisco_ACI_Multi_Site_Manager	Managed Type	Virtual Device
ID	9	Category	Virtual.Infrastructure
Class	Cisco Systems	Sub-Class	ACI Multi-Site Manager Cluster
Organization	Cisco_ACI_Multi_Site_Manager	Uptime	0 days, 00:00:00
		Group / Collector	CUG I sl-cu-215
Device Hostname			

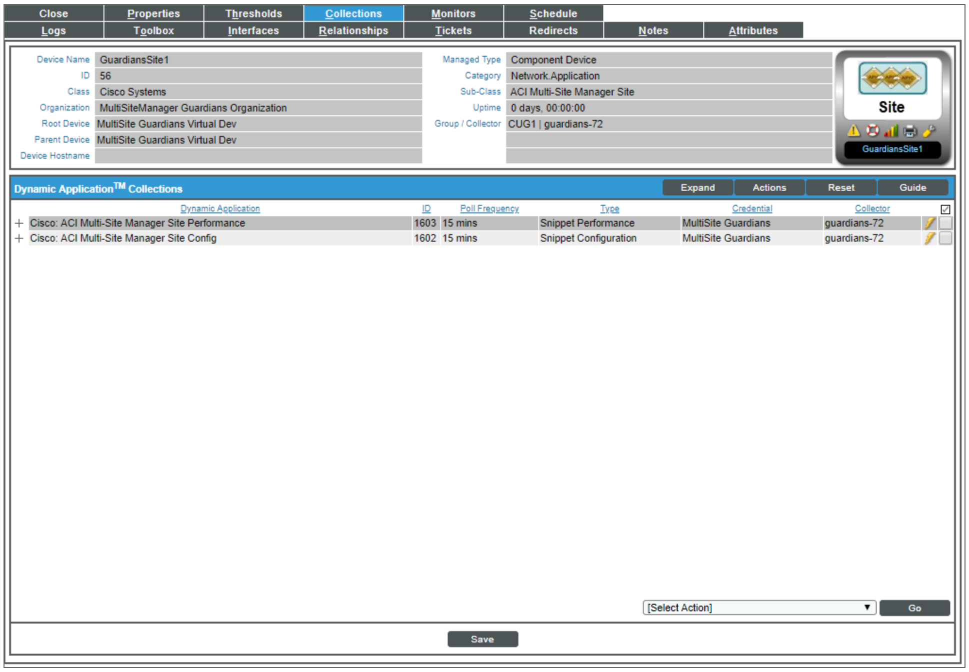
Dynamic Application™ Collections

	Dynamic Application	ID	Poll Frequency	Type	Credential	Collector		☑
+	Cisco: ACI Multi-Site Manager Component Counts	1840	15 mins	Snippet Performance	Cisco_ACI_Multi_Site_Manager	sl-cu-215	🔧	□
+	REST: Performance Metrics Monitor	827	1 mins	Snippet Performance	Cisco_ACI_Multi_Site_Manager	sl-cu-215	🔧	□
+	Cisco: ACI Multi-Site Manager Node Discovery	1832	15 mins	Snippet Configuration	Cisco_ACI_Multi_Site_Manager	sl-cu-215	🔧	□
+	Cisco: ACI Multi-Site Manager Site Discovery	1834	15 mins	Snippet Configuration	Cisco_ACI_Multi_Site_Manager	sl-cu-215	🔧	□
+	Cisco: ACI Multi-Site Manager Tenant Discovery	1838	15 mins	Snippet Configuration	Cisco_ACI_Multi_Site_Manager	sl-cu-215	🔧	□
+	Cisco: ACI Multi-Site Manager Token	1841	10 mins	Snippet Configuration	Cisco_ACI_Multi_Site_Manager	sl-cu-215	🔧	□

The following Dynamic Applications will automatically align to their correspondent device components:

- Cisco: ACI Multi-Site Manager Node Configuration
- Cisco: ACI Multi-Site Manager Site Config

- Cisco: ACI Multi-Site Manager Site Performance
- Cisco: ACI Multi-Site Manager Tenant Config



Device Name	GuardiansSite1	Managed Type	Component Device
ID	56	Category	Network.Application
Class	Cisco Systems	Sub-Class	ACI Multi-Site Manager Site
Organization	MultiSiteManager Guardians Organization	Uptime	0 days, 00:00:00
Root Device	MultiSite Guardians Virtual Dev	Group / Collector	CUG1 | guardians-72
Parent Device	MultiSite Guardians Virtual Dev		
Device Hostname			

Dynamic Application^{TM} Collections

Dynamic Application	ID	Poll Frequency	Type	Credential	Collector	☑
+ Cisco: ACI Multi-Site Manager Site Performance	1603	15 mins	Snippet Performance	MultiSite Guardians	guardians-72	□
+ Cisco: ACI Multi-Site Manager Site Config	1602	15 mins	Snippet Configuration	MultiSite Guardians	guardians-72	□

Chapter 9

Cisco: AppDynamics

Overview

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

NOTE: For more information about the *Cisco: AppDynamics* PowerPack, see the ***Monitoring Cisco AppDynamics*** manual.

Prerequisites for Monitoring Cisco AppDynamics

Before you can monitor Cisco AppDynamics applications using the *Cisco: AppDynamics* PowerPack, you must first create a user account that is assigned the "Applications and Dashboard Viewer" role in the AppDynamics account portal. This user account must also have sufficient permissions to obtain metrics information from the AppDynamics REST API.

For more information about creating the AppDynamics user account, see https://docs.appdynamics.com/display/PRO44/Roles+and+Permissions.

Creating a SOAP/XML Credential for Cisco AppDynamics

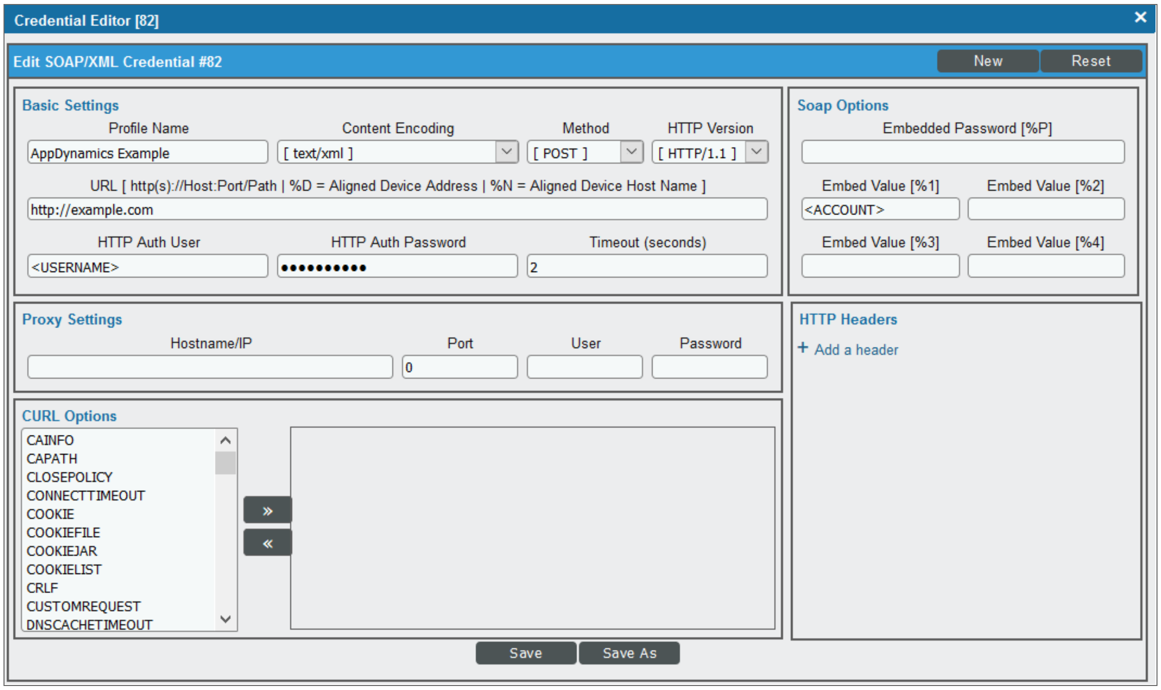
To use the Dynamic Applications in the *Cisco: AppDynamics* PowerPack, you must first define a SOAP/XML credential in SL1. This credential allows SL1 to communicate with the AppDynamics applications.

The *Cisco: AppDynamics* PowerPack includes a sample credential you can use as a template for creating SOAP/XML credentials for AppDynamics.

To configure a SOAP/XML credential for AppDynamics:

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

2. Locate the **AppDynamics Example** credential and then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears:



Credential Editor [82]

Edit SOAP/XML Credential #82

Basic Settings

Profile Name: AppDynamics Example

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: http://example.com

HTTP Auth User: <USERNAME>

HTTP Auth Password: ••••••••••

Timeout (seconds): 2

Soap Options

Embedded Password [%P]:

Embed Value [%1]: <ACCOUNT>

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

Proxy Settings

Hostname/IP:

Port: 0

User:

Password:

HTTP Headers

3. Enter values in the following fields:

   Basic Settings

   - ***Profile Name***. Type a new name for the credential.
   - ***URL***. Type the URL for the AppDynamics account controller.
   - ***HTTP Auth User***. Type the username of an AppDynamics user account that is assigned the "Applications and Dashboard Viewer" role in the AppDynamics portal.
   - ***HTTP Auth Password***. Type the AppDynamics user account password.

   Proxy Settings

   - ***Hostname/IP***. If you are connecting to AppDynamics via a proxy server, type the server's hostname or IP address. Otherwise, leave this field blank.
   - ***Port***. If you are connecting to AppDynamics via a proxy server, type the port number you opened when setting up the proxy server. Otherwise, leave this field blank.
   - ***User***. If you are connecting to AppDynamics via a proxy server, type the server's administrator username. Otherwise, leave this field blank.
   - ***Password***. If you are connecting to AppDynamics via a proxy server, type the server's administrator password. Otherwise, leave this field blank.

   SOAP Options

   - ***Embed Value [%1]***. Type your AppDynamics account name.
4. Click **[Save As]**.
5. In the confirmation message, click **[OK]**.

NOTE: You must rename the sample **AppDynamics Example** credential and click **[Save As]** to save it. If you do not rename the sample credential, then your credential will be overwritten the next time you upgrade the *Cisco: AppDynamics* PowerPack.

Configuring an AppDynamics Device Template

A ***device template*** allows you to save a device configuration and apply it to multiple devices. The *Cisco: AppDynamics* PowerPack includes the "Cisco: AppDynamics Application Template." You must configure this device template to use the AppDynamics SOAP/XML credentials that you created.

If you configure this device template correctly, then when you align the "Cisco: AppDynamics Application Discovery" Dynamic Application to the AppDynamics account controller virtual device, SL1 will use the device template to automatically align the AppDynamics Dynamic Applications to each of the AppDynamics applications it discovers in your account.

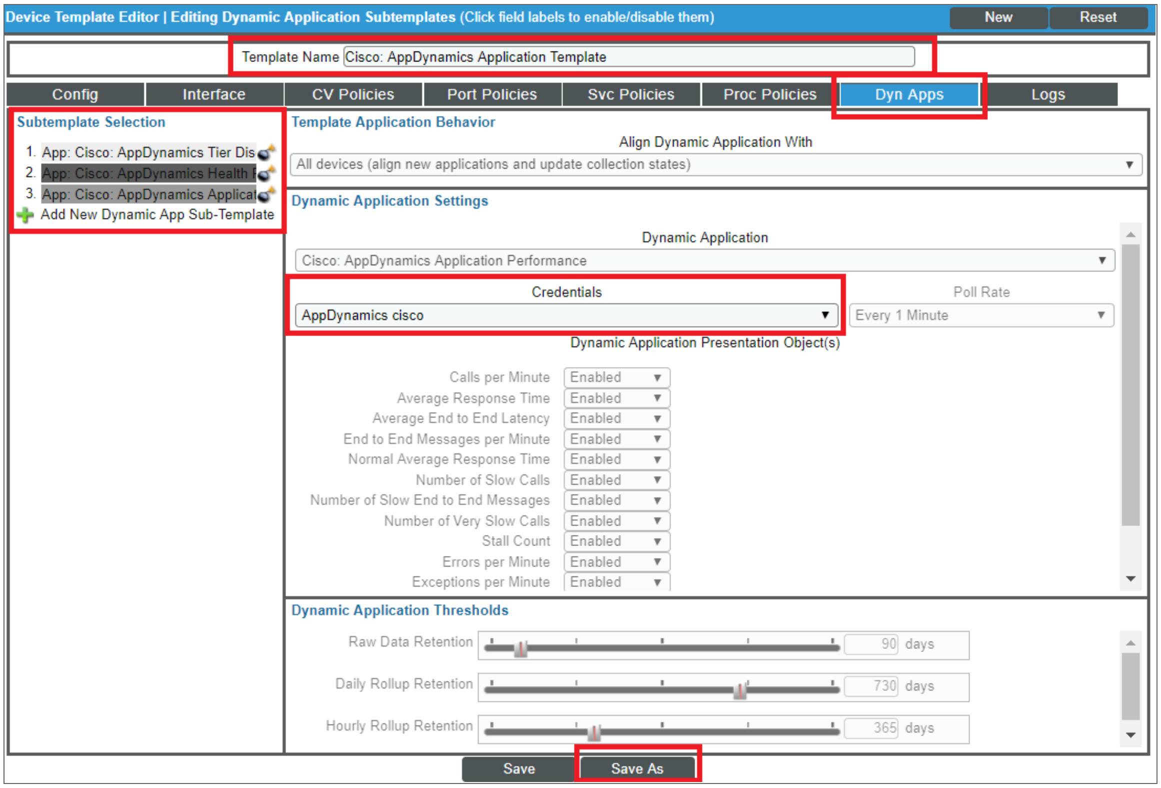
To configure the AppDynamics device template:

1. Go to the **Configuration Templates** page (Devices > Templates, or Registry > Devices > Templates in the SL1 classic user interface).

2. Locate the "Cisco: AppDynamics Application Template" and click its wrench icon (🔧). The **Device Template Editor** page appears.

3. Click the **[Dyn Apps]** tab. The **Editing Dynamic Application Subtemplates** page appears.

4. Complete the following fields:



Device Template Editor | Editing Dynamic Application Subtemplates (Click field labels to enable/disable them)

Template Name: Cisco: AppDynamics Application Template

Subtemplate Selection

1. App: Cisco: AppDynamics Tier Dis
2. App: Cisco: AppDynamics Health I
3. App: Cisco: AppDynamics Applicat

Template Application Behavior

Align Dynamic Application With: All devices (align new applications and update collection states)

Dynamic Application Settings

Dynamic Application: Cisco: AppDynamics Application Performance

Credentials: AppDynamics cisco

Poll Rate: Every 1 Minute

Dynamic Application Presentation Object(s)

Calls per Minute: Enabled
Average Response Time: Enabled
Average End to End Latency: Enabled
End to End Messages per Minute: Enabled
Normal Average Response Time: Enabled
Number of Slow Calls: Enabled
Number of Slow End to End Messages: Enabled
Number of Very Slow Calls: Enabled
Stall Count: Enabled
Errors per Minute: Enabled
Exceptions per Minute: Enabled

Dynamic Application Thresholds

Raw Data Retention: 90 days
Daily Rollup Retention: 730 days
Hourly Rollup Retention: 365 days

- **Template Name**. Type a new name for the device template.
- **Credentials**. Select the SOAP/XML credential that you created for AppDynamics.

5. Click the next Dynamic Application listed in the **Subtemplate Selection** section on the left side of the page and then select the AppDynamics SOAP/XML credential in the ***Credentials*** field.

6. Repeat step 5 until the you have selected the AppDynamics SOAP/XML credential in the ***Credentials*** field for all of the Dynamic Applications listed in the **Subtemplate Selection** section.

7. Click **[Save As]**.

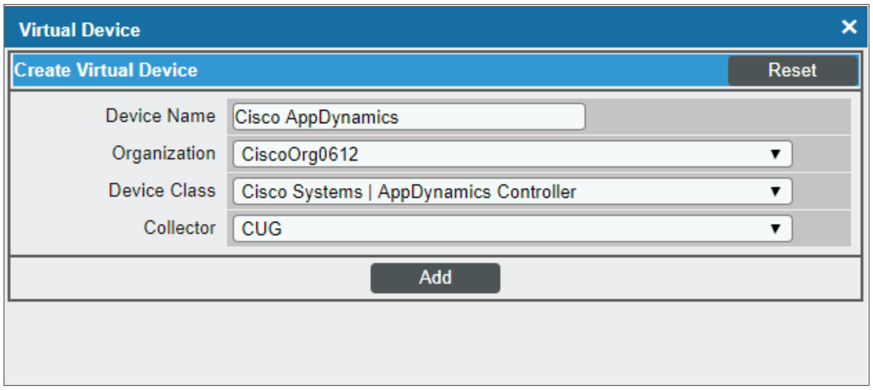
> NOTE: You must rename the sample **Cisco: AppDynamics Application Template** and click **[Save As]** to save it. If you do not rename the device template, then your device template will be overwritten the next time you upgrade the *Cisco: AppDynamics* PowerPack.

Creating an AppDynamics Virtual Device

Because the AppDynamics account controller does not have a static IP address, you cannot discover it using a typical discovery session. Instead, you must create a ***virtual device*** that represents the account controller. A virtual device is a user-defined container that represents a device or service that cannot be discovered by SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications.

To create a virtual device that represents your AppDynamics account controller:

1. Go to the **Device Manager** page (Devices > Device Manager, or Registry > Devices > Device Manager in the SL1 classic user interface).
2. Click the **[Actions]** button and select *Create Virtual Device* from the menu. The **Create Virtual Device** modal page appears.
3. Enter values in the following fields:



Device Name: Cisco AppDynamics
Organization: CiscoOrg0612
Device Class: Cisco Systems | AppDynamics Controller
Collector: CUG

- ***Device Name***. Type a name for the device.
- ***Organization***. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.
- ***Device Class***. Select *Cisco Systems | AppDynamics Controller*.
- ***Collector***. Select the collector group that will monitor the device.

4. Click **[Add]** to create the virtual device.

Aligning the AppDynamics Dynamic Applications

The Dynamic Applications in the *Cisco: AppDynamics* PowerPack are divided into the following types:

- ***Count***. This Dynamic Application polls AppDynamics to determine the number of component devices monitored by SL1.

- ***Discovery***. These Dynamic Applications poll AppDynamics for new applications or changes to existing applications.
- ***Configuration***. These Dynamic Applications retrieve configuration information about each application and component device and retrieve any changes to that configuration information.
- ***Performance***. These Dynamic Applications poll AppDynamics for performance metrics.

Counting AppDynamics Component Devices

If you want to determine the number of AppDynamics component devices that will be monitored prior to running discovery (for instance, to estimate license usage), you can manually align the "Cisco: AppDynamics Component Count" Dynamic Application with the AppDynamics application controller virtual device.

To manually align the "Cisco: AppDynamics Component Count" Dynamic Application:

1. Go to the **Devices** page.
2. Locate the AppDynamics controller virtual device and click on it.
3. In the **Device Investigator** page, click the **[Collections]** tab.
4. Click **[Edit]** and then click the**[Align Dynamic App]** button. The **Align Dynamic Application** window appears.
5. Click *Choose Dynamic Application*. The **Choose Dynamic Application** window appears.
6. Select the "Cisco: AppDynamics Component Count" Dynamic Application and click **[Select]**. The name of the selected Dynamic Application appears in the **Align Dynamic Application** window.
7. If a default credential is listed below the Dynamic Application and it is the ***credential you created for your AppDynamics device***, skip ahead to step 10. Otherwise, uncheck the box next to the credential name.
8. Click *Choose Credential*. The **Choose Credential** window appears.
9. Select the ***credential you created for your AppDynamics device*** for the Dynamic Application and click the **[Select]** button. The name of the selected credential appears in the **Align Dynamic Application** window.
10. Click the **[Align Dynamic App]** button. When the Dynamic Application is successfully aligned, it is added to the **Collections** tab, and a confirmation message appears at the bottom of the tab.

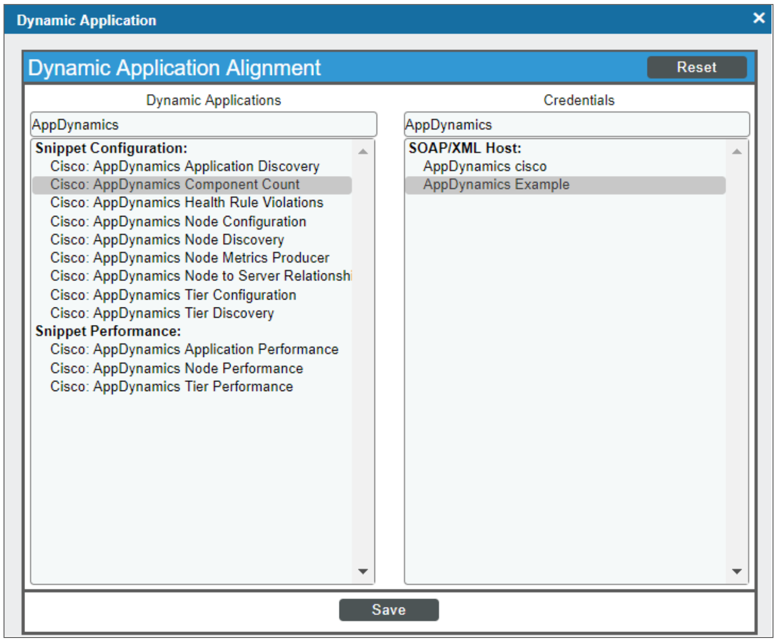
NOTE: If your AppDynamics account has a large number of applications, tiers, or nodes, ScienceLogic recommends discovering your account on a Collector Group with a sufficient number of Data Collectors. For guidelines about the number of Data Collectors you might need, see the ***ScienceLogic Architecture*** manual.

Counting AppDynamics Component Devices in the SL1 Classic User Interface

If you want to determine the number of AppDynamics component devices that will be monitored prior to running discovery (for instance, to estimate license usage), you can manually align the "Cisco: AppDynamics Component Count" Dynamic Application with the AppDynamics application controller virtual device.

To manually align the "Cisco: AppDynamics Component Count" Dynamic Application:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Locate the AppDynamics controller virtual device and then click its wrench icon (🔧).
3. In the ***Device Administration*** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
4. Click the **[Actions]** button and select *Add Dynamic Application* from the menu.
5. In the **Dynamic Application Alignment** modal:



Dynamic Applications: AppDynamics

Snippet Configuration:
Cisco: AppDynamics Application Discovery
Cisco: AppDynamics Component Count
Cisco: AppDynamics Health Rule Violations
Cisco: AppDynamics Node Configuration
Cisco: AppDynamics Node Discovery
Cisco: AppDynamics Node Metrics Producer
Cisco: AppDynamics Node to Server Relationshi
Cisco: AppDynamics Tier Configuration
Cisco: AppDynamics Tier Discovery
Snippet Performance:
Cisco: AppDynamics Application Performance
Cisco: AppDynamics Node Performance
Cisco: AppDynamics Tier Performance

Credentials: AppDynamics

SOAP/XML Host:
AppDynamics cisco
AppDynamics Example

- In the ***Dynamic Applications*** field, select *Cisco: AppDynamics Component Count*.
- In the ***Credentials*** field, select the credential you created for AppDynamics.

6. Click **[Save]** to align the Dynamic Application with the AppDynamics account controller virtual device.

NOTE: If your AppDynamics account has a large number of applications, tiers, or nodes, ScienceLogic recommends discovering your account on a Collector Group with a sufficient number of Data Collectors. For guidelines about the number of Data Collectors you might need, see the ***ScienceLogic Architecture*** manual.

Discovering AppDynamics Applications and Component Devices

To discover all of the applications and components of your AppDynamics account, you must manually align the "Cisco: AppDynamics Application Discovery" Dynamic Application with the AppDynamics account controller virtual device.

To manually align the "Cisco: AppDynamics Application Discovery" Dynamic Application:

1. Go to the **Devices** page, locate the AppDynamics controller virtual device, and click on it.
2. In the **Device Investigator**, click the **[Collections]** tab.
3. Click **[Edit]** and then click the **[Align Dynamic App]** button.
4. In the **Align Dynamic Application** window, click *Choose Dynamic Application*. The **Choose Dynamic Application** window appears.
5. Select the "Cisco: AppDynamics Application Discovery" Dynamic Application and click **[Select]**. The name of the selected Dynamic Application appears in the **Align Dynamic Application** window.
6. If a default credential is listed below the Dynamic Application in the **Align Dynamic Application** window and it is the ***credential you created for your AppDynamics device***, skip ahead to step 9. Otherwise, uncheck the box next to the credential name.
7. Click *Choose Credential*. The **Choose Credential** window appears.
8. Select the ***credential you created for your AppDynamics device*** for the Dynamic Application and click the **[Select]** button. The name of the selected credential appears in the **Align Dynamic Application** window.
9. Click the **[Align Dynamic App]** button. When the Dynamic Application is successfully aligned, it is added to the **Collections** tab, and a confirmation message appears at the bottom of the tab.

When you align the "Cisco: AppDynamics Application Discovery" Dynamic Application with the AppDynamics controller virtual device, and if you have ***configured the AppDynamics device template correctly***, then the following happens:

- Events are triggered indicating that AppDynamics application virtual devices are being created for each application discovered in the AppDynamics account.
- Those events trigger Run Book Actions that apply the AppDynamics device template to each of the application virtual devices
- The device template aligns additional Dynamic Applications to each of the application virtual devices, which results in the creation of child component devices representing the tiers and nodes under those applications.

CAUTION: After you align the "Cisco: AppDynamics Application Discovery" Dynamic Application to the AppDynamics account controller virtual device, it is important to let the Dynamic Application run at its predetermined polling interval; you ***should not*** run the Dynamic Application manually. Running the Dynamic Application manually will result in the application virtual devices not being created. If this happens, you must delete the account controller virtual device and repeat the process again.

CAUTION: If the application virtual devices are not discovered when you align the "Cisco: AppDynamics Application Discovery" Dynamic Application to the AppDynamics account controller virtual device or if the application virtual devices are discovered but the Dynamic Applications aligned to those application virtual devices are using the incorrect credentials because *the "Cisco: AppDynamics Application Template" Device Template was not modified* to use your correct AppDynamics credentials, then you must delete all devices including the account controller virtual device and repeat the process again.

NOTE: SL1 is unable to discover applications with names that include special characters.

NOTE: If a tier or node name includes special characters, SL1 replaces the special characters with empty spaces in the device name. This does not affect data collection, but it does prevent a relationship from being created between a physical server and a component node if the node's machine name contains special characters.

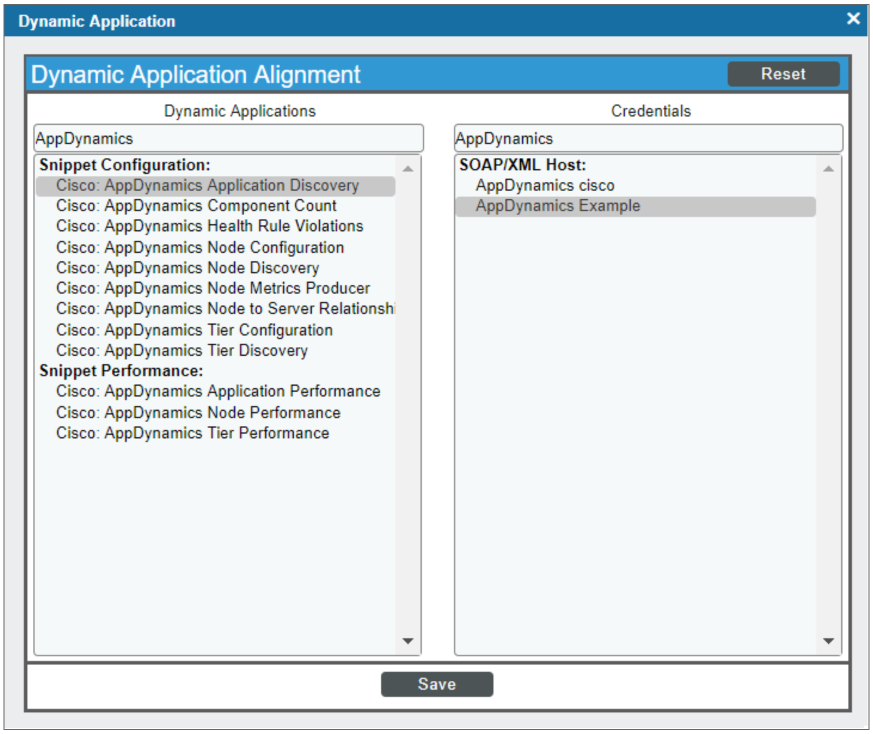
Discovering AppDynamics Applications and Component Devices in the SL1 Classic User Interface

To discover all of the applications and components of your AppDynamics account, you must manually align the "Cisco: AppDynamics Application Discovery" Dynamic Application with the AppDynamics account controller virtual device.

To manually align the "Cisco: AppDynamics Application Discovery" Dynamic Application:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Locate the AppDynamics controller virtual device and then click its wrench icon (🔧).
3. In the ***Device Administration*** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
4. Click the **[Actions]** button and select *Add Dynamic Application* from the menu.

5. In the **Dynamic Application Alignment** modal:



Dynamic Application

Dynamic Application Alignment

Dynamic Applications: AppDynamics

Snippet Configuration:
- Cisco: AppDynamics Application Discovery
- Cisco: AppDynamics Component Count
- Cisco: AppDynamics Health Rule Violations
- Cisco: AppDynamics Node Configuration
- Cisco: AppDynamics Node Discovery
- Cisco: AppDynamics Node Metrics Producer
- Cisco: AppDynamics Node to Server Relationshi
- Cisco: AppDynamics Tier Configuration
- Cisco: AppDynamics Tier Discovery

Snippet Performance:
- Cisco: AppDynamics Application Performance
- Cisco: AppDynamics Node Performance
- Cisco: AppDynamics Tier Performance

Credentials: AppDynamics

SOAP/XML Host:
- AppDynamics cisco
- AppDynamics Example

- In the ***Dynamic Applications*** field, select *Cisco: AppDynamics Application Discovery*.
- In the ***Credentials*** field, select the credential you created for AppDynamics.

6. Click **[Save]** to align the Dynamic Application with the AppDynamics account controller virtual device.

When you align the "Cisco: AppDynamics Application Discovery" Dynamic Application with the AppDynamics controller virtual device, if you have ***configured the AppDynamics device template correctly***, then the following happens:

- Events are triggered indicating that AppDynamics application virtual devices are being created for each application discovered in the AppDynamics account.
- Those events trigger Run Book Actions that apply the AppDynamics device template to each of the application virtual devices
- The device template aligns additional Dynamic Applications to each of the application virtual devices, which results in the creation of child component devices representing the tiers and nodes under those applications.

CAUTION: After you align the "Cisco: AppDynamics Application Discovery" Dynamic Application to the AppDynamics account controller virtual device, it is important to let the Dynamic Application run at its predetermined polling interval; you ***should not*** run the Dynamic Application manually by clicking its lightning bolt icon (⚡). Clicking the lightning bolt icon (⚡) for the "Cisco: AppDynamics Application Discovery" Dynamic Application will result in the application virtual devices not being created. If this happens, you must delete the account controller virtual device and repeat the process again.

CAUTION: If the application virtual devices are not discovered when you align the "Cisco: AppDynamics Application Discovery" Dynamic Application to the AppDynamics account controller virtual device or if the application virtual devices are discovered but the Dynamic Applications aligned to those application virtual devices are using the incorrect credentials because *the "Cisco: AppDynamics Application Template" Device Template was not modified* to use your correct AppDynamics credentials, then you must delete all devices including the account controller virtual device and repeat the process again.

NOTE: SL1 is unable to discover applications with names that include special characters.

NOTE: If a tier or node name includes special characters, SL1 replaces the special characters with empty spaces in the device name. This does not affect data collection, but it does prevent a relationship from being created between a physical server and a component node if the node's machine name contains special characters.

Discovering Multiple AppDynamics Accounts

To discover multiple AppDynamics accounts, you must:

1. *Create a separate credential for each account*, using a unique ***Profile Name*** for each credential.
2. *Create a separate device template for each account*, using a unique ***Template Name*** and aligning the appropriate credential to the Dynamic Applications in each device template.
3. *Create a separate AppDynamics account controller virtual device for each account*.
4. *Discover each account's applications and components*.

Creating Device Relationships Between Nodes and Servers

If you want to create a device relationship between AppDynamics nodes and the physical servers where they reside, you must manually align the "Cisco: AppDynamics Node to Server Relationship" Dynamic Application to the physical server device. The "Cisco: AppDynamics Node to Server Relationship" Dynamic Application can create relationships between a single server and one or more nodes.

To manually align the "Cisco: AppDynamics Node to Server Relationship" Dynamic Application:

1. Go to the **Devices** page, locate the AppDynamics physical server device, and click on it. In the **Device Investigator**, click the **[Collections]** tab.
2. Click **[Edit]** and then click the **[Align Dynamic App]** button.
4. In the **Align Dynamic Application** window, click *Choose Dynamic Application*. The **Choose Dynamic Application** window appears.
5. Select the "Cisco: AppDynamics Node to Server Relationship" Dynamic Application and click **[Select]**. The name of the selected Dynamic Application appears in the **Align Dynamic Application** window.
6. If a default credential is listed below the Dynamic Application in the **Align Dynamic Application** window and it is the ***credential you created for your AppDynamics device***, skip ahead to step 9. Otherwise, uncheck the box next to the credential name.
7. Click *Choose Credential*. The **Choose Credential** window appears.
8. Select the ***credential you created for your AppDynamics device*** for the Dynamic Application and click the **[Select]** button. The name of the selected credential appears in the **Align Dynamic Application** window.
9. Click the **[Align Dynamic App]** button. When the Dynamic Application is successfully aligned, it is added to the **Collections** tab, and a confirmation message appears at the bottom of the tab.
10. To view the relationship, go to the **Device Investigator** Map page (click the **[Map]** tab) or the **Component Map** page (Classic Maps > Device Maps > Components) for the node device.

NOTE: You must ensure that the server hostname matches the node machine name that is collected by the "Cisco: AppDynamics Node Configuration" Dynamic Application. If the physical server device name is an IP address or otherwise differs from the machine name collected by the "Cisco: AppDynamics Node Configuration" Dynamic Application, you can go to the server's **Device Investigator** page, click **[Edit]**, and edit the ***Device Name*** to match the node machine name.

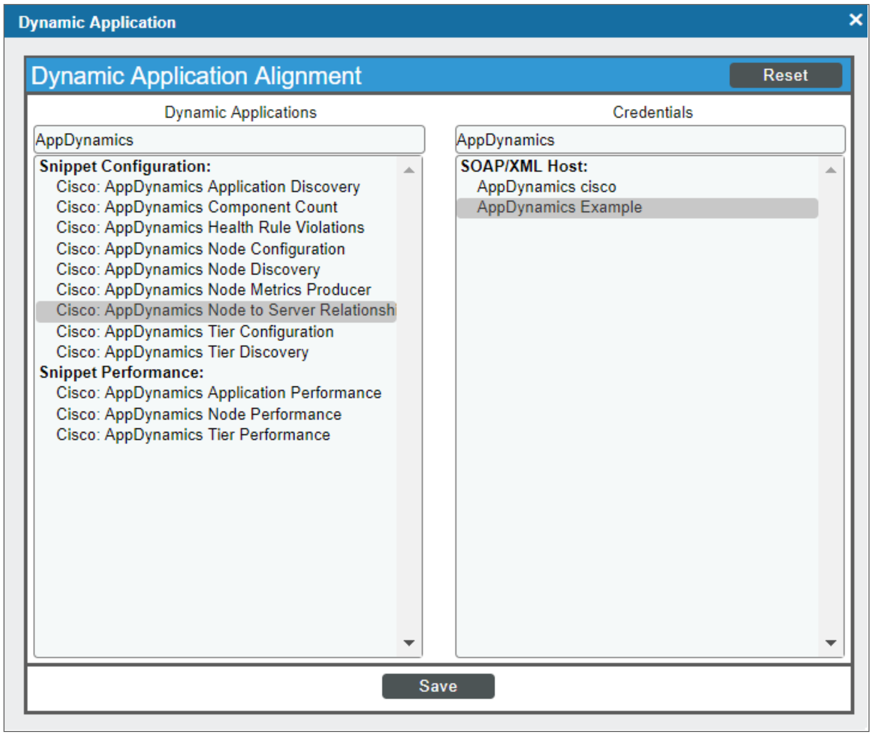
Creating Device Relationships Between Nodes and Servers in the SL1 Classic User Interface

If you want to create a device relationship between AppDynamics nodes and the physical servers where they reside, you must manually align the "Cisco: AppDynamics Node to Server Relationship" Dynamic Application to the physical server device. The "Cisco: AppDynamics Node to Server Relationship" Dynamic Application can create relationships between a single server and one or more nodes.

To create device relationships between nodes and servers:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Locate the AppDynamics physical server device and then click its wrench icon (🔧).
3. In the ***Device Administration*** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
4. Click the **[Actions]** button and select *Add Dynamic Application* from the menu.

5. In the **Dynamic Application Alignment** modal:



AppDynamics

Snippet Configuration:
- Cisco: AppDynamics Application Discovery
- Cisco: AppDynamics Component Count
- Cisco: AppDynamics Health Rule Violations
- Cisco: AppDynamics Node Configuration
- Cisco: AppDynamics Node Discovery
- Cisco: AppDynamics Node Metrics Producer
- Cisco: AppDynamics Node to Server Relationsh
- Cisco: AppDynamics Tier Configuration
- Cisco: AppDynamics Tier Discovery

Snippet Performance:
- Cisco: AppDynamics Application Performance
- Cisco: AppDynamics Node Performance
- Cisco: AppDynamics Tier Performance

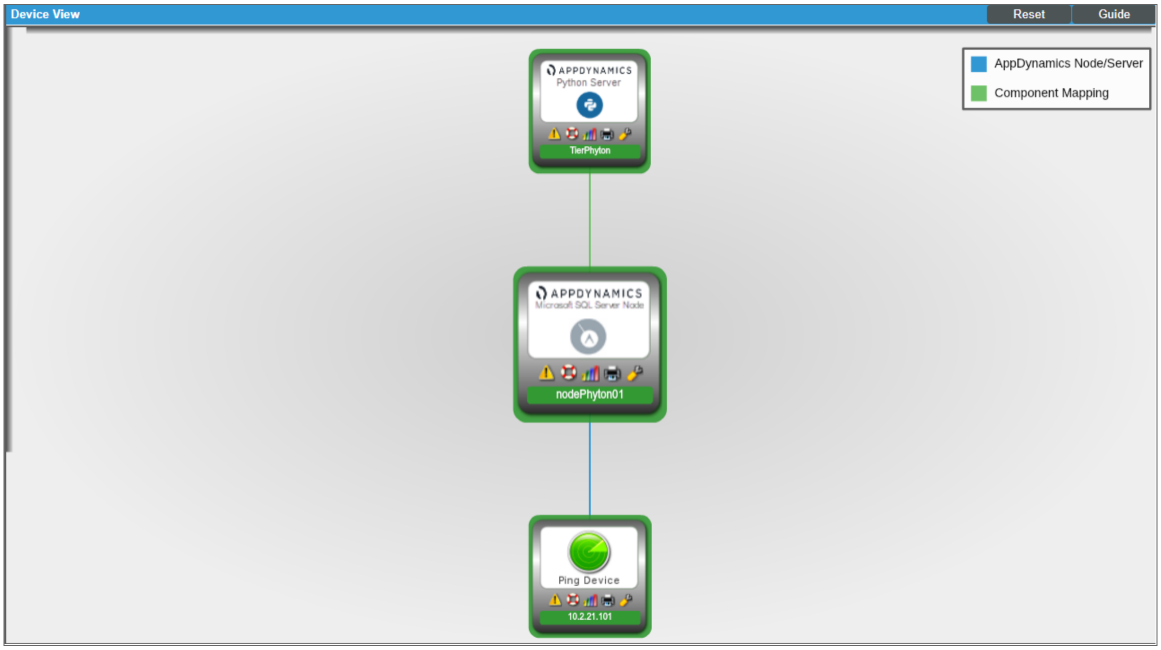
AppDynamics

SOAP/XML Host:
- AppDynamics cisco
- AppDynamics Example

- In the ***Dynamic Applications*** field, select *Cisco: AppDynamics Node to Server Relationship*.
- In the ***Credentials*** field, select the credential you created for AppDynamics.

6. Click **[Save]** to align the Dynamic Application with the AppDynamics physical server device.

7. To view the relationship, go to the **Device View** modal page (click the bar-graph icon [📊] for a device, then click the **Topology** tab) or the **Device Component Map** page (Classic Maps > Device Maps > Components) for the node device.



NOTE: You must ensure that the server hostname matches the node machine name that is collected by the "Cisco: AppDynamics Node Configuration" Dynamic Application. If the physical server device name is an IP address or otherwise differs from the machine name collected by the "Cisco: AppDynamics Node Configuration" Dynamic Application, you can go to the server's **Device Properties** page (Registry > Devices > wrench icon) and edit the ***Device Name*** to match the node machine name.

Chapter 10

Cisco: CloudCenter

Overview

The following sections describe how to configure and discover a Cloud Center Manager for monitoring by SL1 using the *Cisco: CloudCenter* PowerPack:

NOTE: For more information about the *Cisco: CloudCenter* PowerPack, see the ***Monitoring Cisco CloudCenter*** manual.

Configuration and Discovery for Standard Cisco CloudCenter Deployments

The *Cisco: CloudCenter* PowerPack enables you to discover and collect configuration and performance data about standard or high-availability (HA) CloudCenter deployments and their components. The following sections describe the configuration and discovery steps for monitoring standard (non-HA) CloudCenter deployments.

For information about HA deployments, see the section on ***Configuration and Discovery for High-Availability Cisco CloudCenter Deployments***.

Prerequisites for Monitoring Standard CloudCenter Deployments

To configure the SL1 system to monitor standard (non-HA) Cisco CloudCenter deployments using the *Cisco: CloudCenter* PowerPack, you must first have the following information about the CloudCenter Manager that you want to monitor:

- The IP address of the CloudCenter Manager system
- The username and API key for a Cisco CloudCenter Manager user that has root tenant administration privileges. This account must be an API user, not a GUI user. For information about configuring API users in Cisco CloudCenter Manager, see http://docs.cloudcenter.cisco.com/display/40API/API+Management+Key.

Creating a Basic/Snippet Credential for Standard Deployments

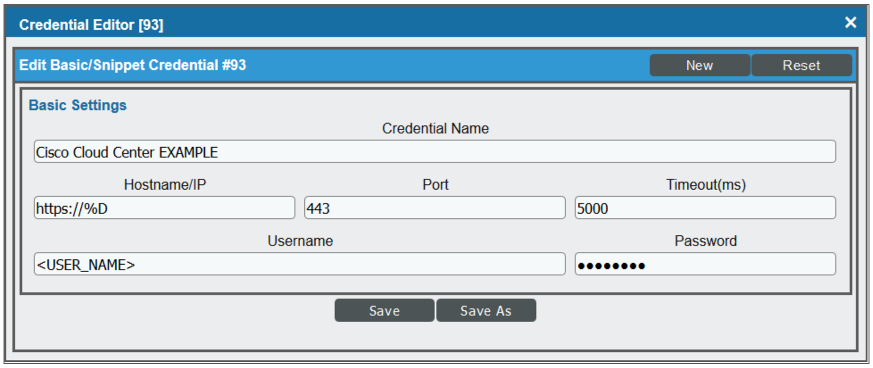
To configure SL1 to monitor a standard (non-HA) CloudCenter Manager deployment, you must first create a Basic/Snippet credential. This credential allows the Dynamic Applications in the *Cisco: CloudCenter* PowerPack to communicate with your CloudCenter Manager.

The PowerPack includes an example Basic/Snippet credential (**Cisco CloudCenter EXAMPLE**) that you can edit for your own use.

To configure a Basic/Snippet credential to access a CloudCenter Manager:

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

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



Credential Editor [93]

Edit Basic/Snippet Credential #93

Basic Settings

Credential Name: Cisco Cloud Center EXAMPLE

Hostname/IP: https://%D

Port: 443

Timeout(ms): 5000

Username: <USER_NAME>

Password: ●●●●●●●●

   - ***Profile Name***. Type a name for the CloudCenter Manager credential.
   - ***Username***. Type the username for a CloudCenter Manager user that has root tenant administration privileges. This account must be an API user, not a GUI user.
   - ***Password***. Type the API key for the user you entered in the ***Username*** field.

4. Leave all other fields set to the default values. Click the **[Save As]** button.

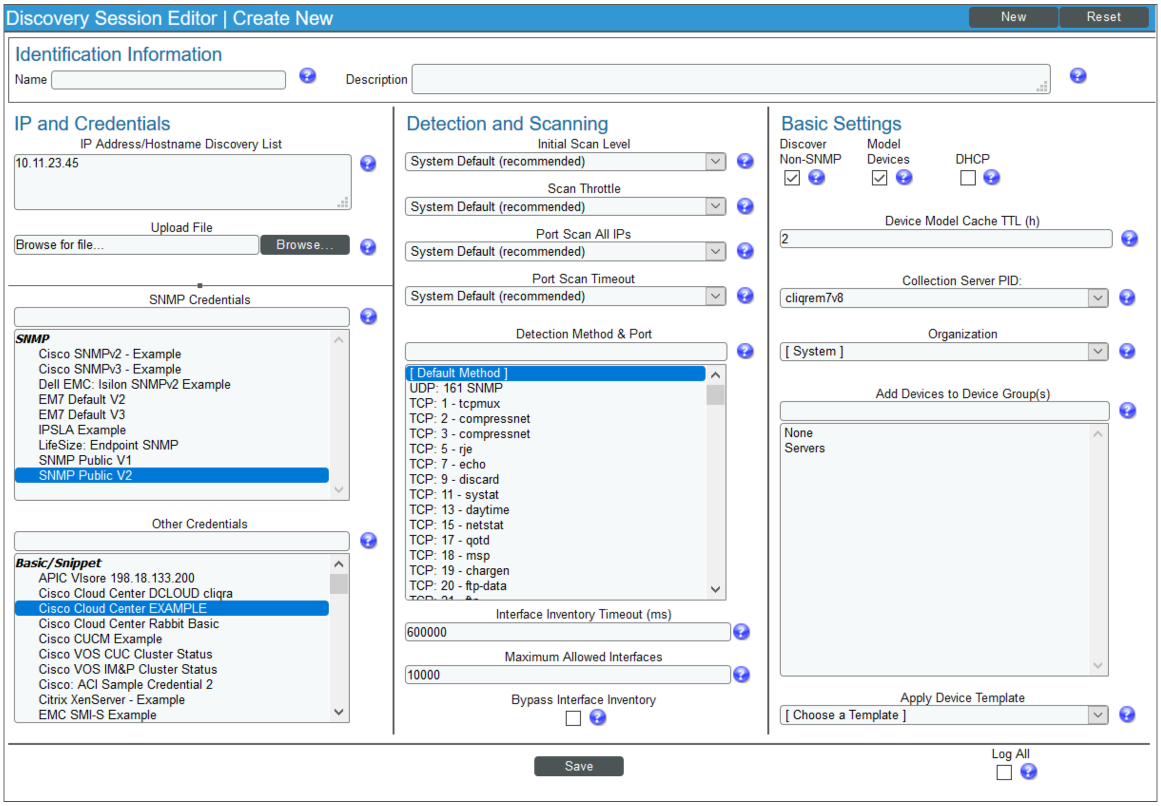
Discovering the CloudCenter Manager Root Tenant for Standard Deployments

Discovering the CloudCenter Manager Root Tenant for Standard Deployments in the SL1 Classic User Interface

To discover CloudCenter Manager, 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:



Discovery Session Editor | Create New

Identification Information

Name:

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.11.23.45

Upload File: Browse for file...

SNMP Credentials: SNMP Public V2

Other Credentials: Cisco Cloud Center EXAMPLE

Detection and Scanning

Initial Scan Level: System Default (recommended)

Scan Throttle: System Default (recommended)

Port Scan All IPs: System Default (recommended)

Port Scan Timeout: System Default (recommended)

Detection Method & Port: [Default Method]

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: cliqrem7v8

Organization: [System]

Add Devices to Device Group(s):

Apply Device Template: [Choose a Template]

Log All: □

- ***IP Address/Hostname Discovery List***. Enter the IP address for the CloudCenter Manager.
- ***SNMP Credentials***. Optionally, select the SNMP credential for the CloudCenter Manager you are discovering.
- ***Other Credentials***. Select the Basic/Snippet credential you created for the CloudCenter Manager root tenant.
- ***Discover Non-SNMP***. 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.

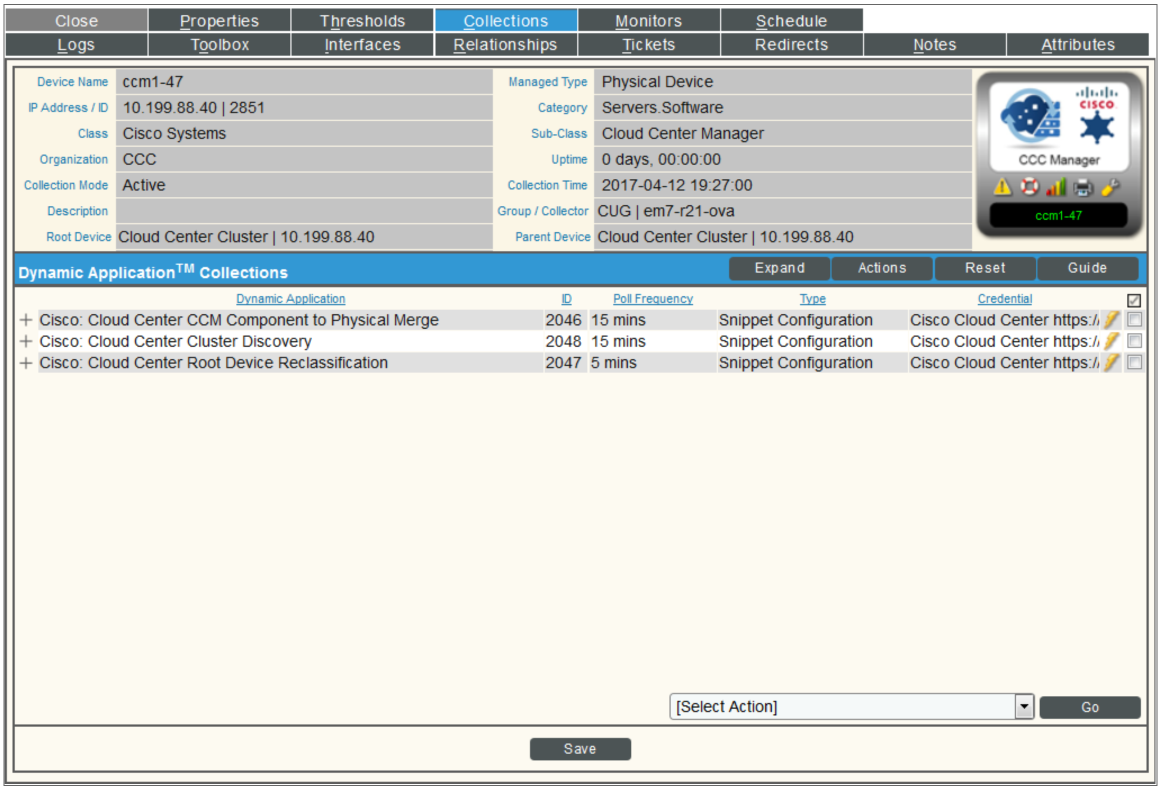
7. The **Discovery Session** window appears. When the device is discovered, click the device icon ( ) to view the **Device Properties** page for the device.

Verifying Discovery and Dynamic Application Alignment

To verify that SL1 automatically aligned the correct Dynamic Applications during discovery:

1. From the **Device Properties** page for the CloudCenter Manager device, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. All applicable Dynamic Applications for CloudCenter Manager 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	ccm1-47	Managed Type	Physical Device
IP Address / ID	10.199.88.40 | 2851	Category	Servers.Software
Class	Cisco Systems	Sub-Class	Cloud Center Manager
Organization	CCC	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2017-04-12 19:27:00
Description		Group / Collector	CUG | em7-r21-ova
Root Device	Cloud Center Cluster | 10.199.88.40	Parent Device	Cloud Center Cluster | 10.199.88.40

Dynamic Application™ Collections

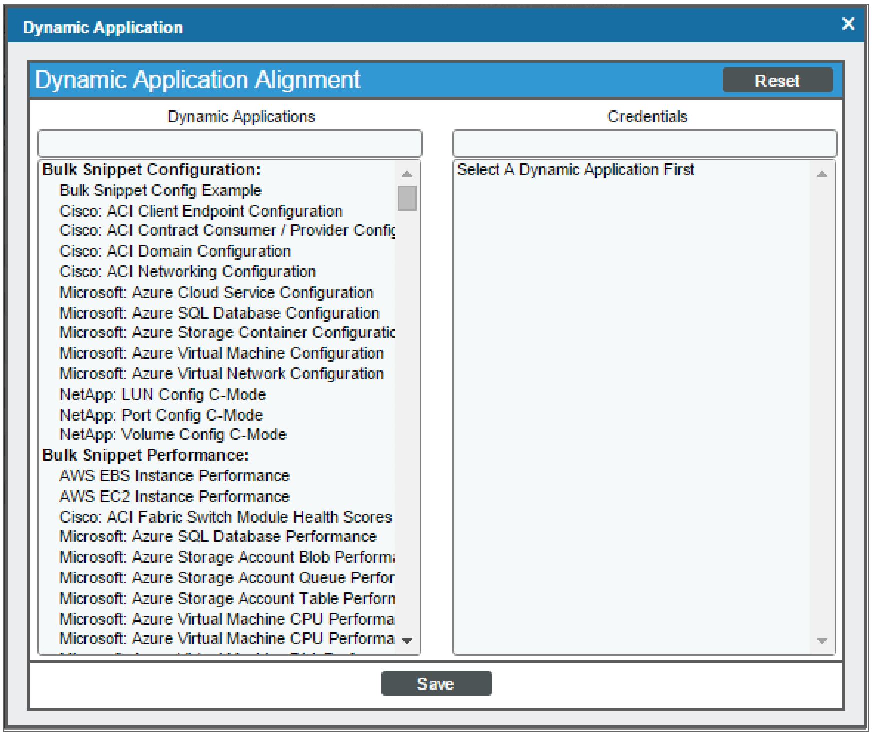
Dynamic Application	ID	Poll Frequency	Type	Credential	☑
+ Cisco: Cloud Center CCM Component to Physical Merge	2046	15 mins	Snippet Configuration	Cisco Cloud Center https:/	□
+ Cisco: Cloud Center Cluster Discovery	2048	15 mins	Snippet Configuration	Cisco Cloud Center https:/	□
+ Cisco: Cloud Center Root Device Reclassification	2047	5 mins	Snippet Configuration	Cisco Cloud Center https:/	□

The following Dynamic Applications should be aligned to the device:

- Cisco: CloudCenter CCM Component to Physical Merge
- Cisco: CloudCenter Cluster Discovery
- Cisco: CloudCenter Root Device Reclassification

If the listed Dynamic Applications have not been automatically aligned during discovery, you can align them manually. To do so, perform the following steps:

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



Bulk Snippet Configuration:
Bulk Snippet Config Example
Cisco: ACI Client Endpoint Configuration
Cisco: ACI Contract Consumer / Provider Config
Cisco: ACI Domain Configuration
Cisco: ACI Networking Configuration
Microsoft: Azure Cloud Service Configuration
Microsoft: Azure SQL Database Configuration
Microsoft: Azure Storage Container Configuratic
Microsoft: Azure Virtual Machine Configuration
Microsoft: Azure Virtual Network Configuration
NetApp: LUN Config C-Mode
NetApp: Port Config C-Mode
NetApp: Volume Config C-Mode
Bulk Snippet Performance:
AWS EBS Instance Performance
AWS EC2 Instance Performance
Cisco: ACI Fabric Switch Module Health Scores
Microsoft: Azure SQL Database Performance
Microsoft: Azure Storage Account Blob Performa
Microsoft: Azure Storage Account Queue Perfor
Microsoft: Azure Storage Account Table Perforn
Microsoft: Azure Virtual Machine CPU Performa
Microsoft: Azure Virtual Machine CPU Performa

Select A Dynamic Application First

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

Discovering Multiple Tenants for Standard Deployments

The *Cisco: CloudCenter* PowerPack can be used to monitor a CloudCenter Manager that includes multiple tenants. To discover multiple tenants, you must follow the steps in the following sections for each tenant in order (in other words, parents must be discovered before their children):

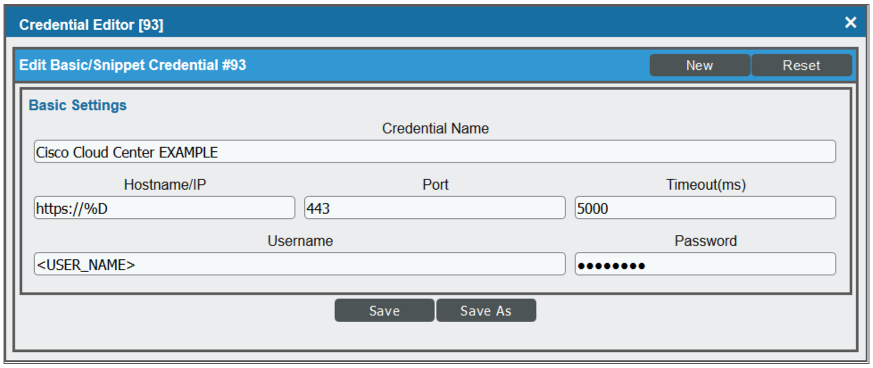
- *Creating a Credential for a CloudCenter Manager Tenant*
- *Discovering an additional CloudCenter Manager Tenant*

For each tenant, you must use the administrator account for that tenant when you create the credential.

Creating a Credential for a CloudCenter Manager Tenant

To configure a Basic/Snippet credential to access an additional CloudCenter Manager tenant:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the credential you used to discover the root tenant, then click its wrench icon (🔧). The **Edit Basic/Snippet Credential** modal page appears.
3. Enter values in the following fields:



Edit Basic/Snippet Credential #93

Basic Settings

Credential Name		
Cisco Cloud Center EXAMPLE		
Hostname/IP	Port	Timeout(ms)
https://%D	443	5000
Username		Password
<USER_NAME>		••••••••

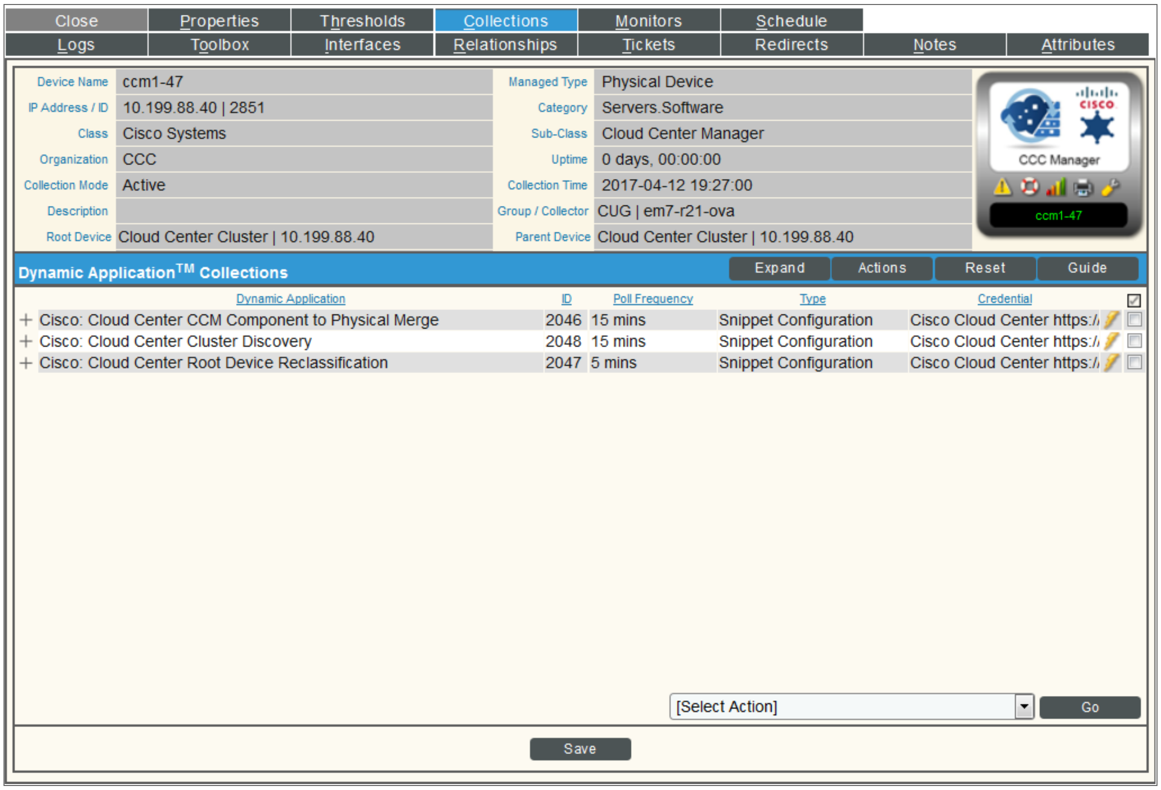
- ***Profile Name***. Enter a new name for the CloudCenter Manager tenant credential.
- ***Username***. Enter the username for a CloudCenter Manager user that is an administrator for the tenant you want to discover. This account must be an API user, not a GUI user.
- ***Password***. Enter the API key for the user you entered in the ***Username*** field.

4. Leave all other fields set to the default values. Click the **[Save As]** button.

Discovering an Additional CloudCenter Manager Tenant

To discover an additional tenant:

1. From the **Device Properties** page for the CloudCenter Suite root device, click the name of the CloudCenter Cluster device that appears in the ***Root Device*** field.
2. Click the **[Collections]** tab. The **Dynamic Application Collections** page appears.



Device Name	ccm1-47	Managed Type	Physical Device
IP Address / ID	10.199.88.40 | 2851	Category	Servers.Software
Class	Cisco Systems	Sub-Class	Cloud Center Manager
Organization	CCC	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2017-04-12 19:27:00
Description		Group / Collector	CUG | em7-r21-ova
Root Device	Cloud Center Cluster | 10.199.88.40	Parent Device	Cloud Center Cluster | 10.199.88.40

Dynamic Application^{TM} Collections

Dynamic Application	ID	Poll Frequency	Type	Credential	☑
+ Cisco: Cloud Center CCM Component to Physical Merge	2046	15 mins	Snippet Configuration	Cisco Cloud Center https:/	□
+ Cisco: Cloud Center Cluster Discovery	2048	15 mins	Snippet Configuration	Cisco Cloud Center https:/	□
+ Cisco: Cloud Center Root Device Reclassification	2047	5 mins	Snippet Configuration	Cisco Cloud Center https:/	□

[Select Action]

3. Select the checkbox for the "Cisco: CloudCenter Tenant Discovery" Dynamic Application.
4. In the ***Select Action*** drop-down list, select the credential you created for the tenant.
5. Click **[Go]**.

Configuration and Discovery for High-Availability Cisco CloudCenter Deployments

The *Cisco: CloudCenter* PowerPack enables you to discover and collect configuration and performance data about standard or high-availability (HA) CloudCenter deployments and their components. The following sections describe the configuration and discovery steps for monitoring HA CloudCenter deployments.

For information about standard (non-HA) deployments, see the section on ***Configuration and Discovery for Standard Cisco CloudCenter Deployments***.

Prerequisites for Monitoring High-Availability CloudCenter Deployments

To configure the SL1 system to monitor HA Cisco CloudCenter deployments using the *Cisco: CloudCenter* PowerPack, you must first have the following information about the CloudCenter components that you want to monitor:

- The IP address or hostname for each of the following components:
  - RabbitMQ
  - RabbitMQ Load Balancer
  - Cisco CloudCenter Manager
  - Cisco CloudCenter Manager Load Balancer
  - CloudCenter PostgreSQL database
  - CloudCenter Orchestrator
  - CloudCenter Orchestrator Load Balancer
  - CloudCenter Health Monitor
  - CloudCenter ELK components
- The username and API key for a Cisco CloudCenter Manager user that has root tenant administration privileges. This account must be an API user, not a GUI user. For information about configuring API users in Cisco CloudCenter Manager, see http://docs.cloudcenter.cisco.com/display/40API/API+Management+Key.
- The username and password for a RabbitMQ user that has read permission to the RabbitMQ API. For information about configuring users in RabbitMQ, see https://www.rabbitmq.com/management.html.
- The usernames and passwords for Cisco CloudCenter users that have API read permissions for each of the other components in the above list.

Creating Credentials for High-Availability Deployments

To configure SL1 to monitor HA Cisco CloudCenter deployments, you must create the following credentials:

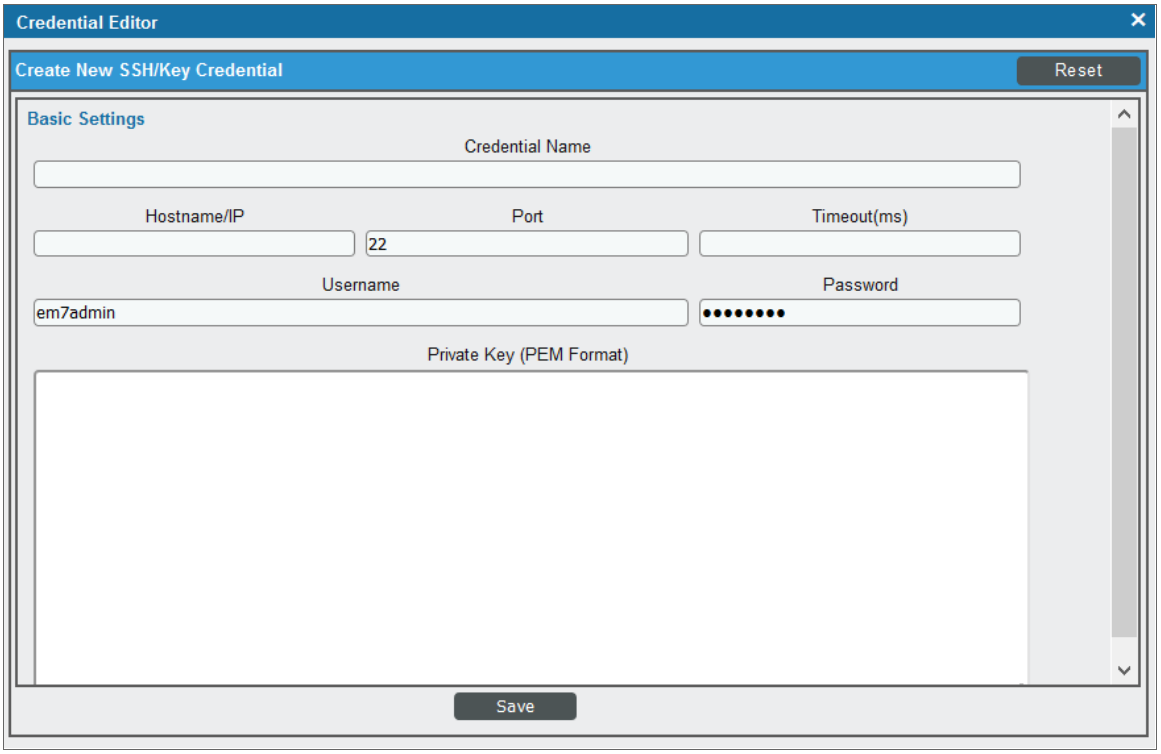
- *SSH/Key credentials for CloudCenter Components*
- *A Basic/Snippet credential for RabbitMQ*
- *A "master" SOAP/XML credential* that references the CloudCenter Manager and RabbitMQ credentials and that you will use for discovering the high-availability CloudCenter deployment

Creating SSH/Key Credentials for CloudCenter Components

To configure SL1 to monitor HA Cisco CloudCenter deployments, you must create SSH/Key credentials that allow the Dynamic Applications in the *Cisco: CloudCenter* PowerPack to connect with the various components in your HA CloudCenter.

To create an SSH/Key credential to access a CloudCenter component:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click **[Actions]**, and then select *Create SSH/Key Credential*.
3. Complete the following fields:



Port: 22

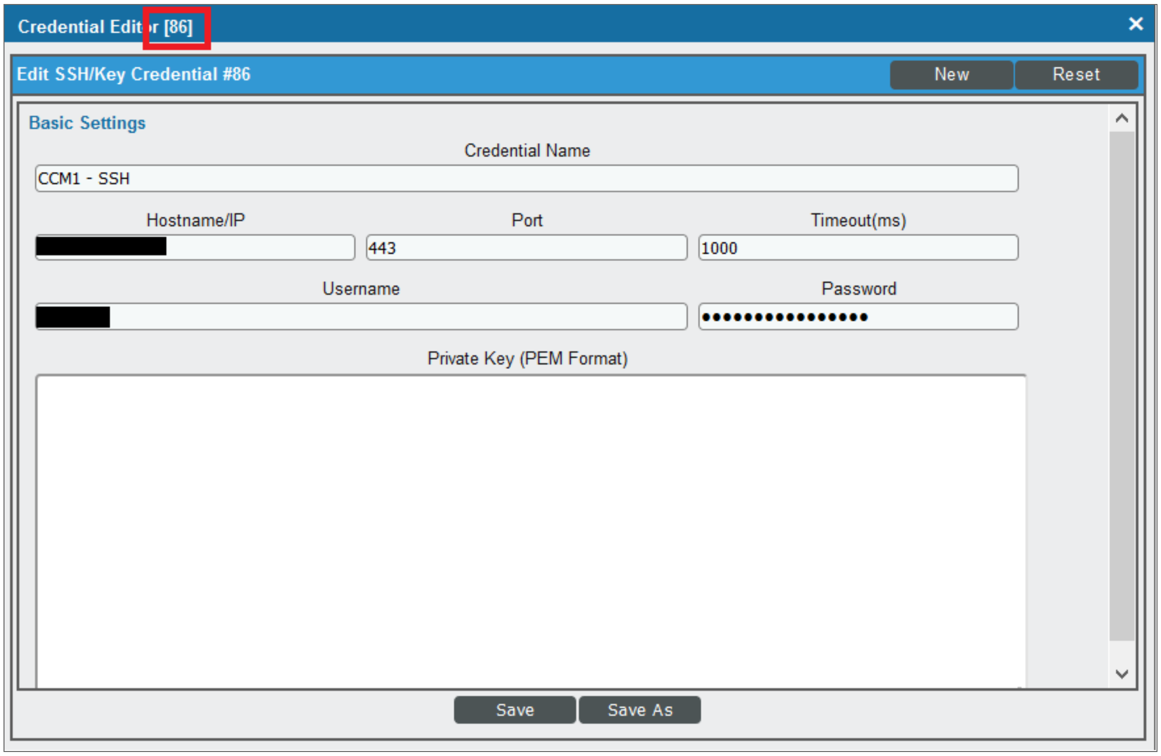
Username: em7admin

Password: ••••••••

- ***Credential Name***. Type a name for the credential.
- ***Hostname/IP***. Type the IP address for the component. **Do not use "%D".**
- ***Port***. Type the port number required to access the component.
- ***Timeout(ms)***. Type the time, in milliseconds, after which SL1 will stop trying to communicate with the component.

- ***Username***. Type the username for a user that has root tenant administration privileges for CloudCenter Manager, or read privileges for other components. This account must be an API user, not a GUI user.
- ***Password***. Type the API key for the user you entered in the ***Username*** field.
- ***Private Key (PEM Format)***. Leave this field blank.

4. Click **[Save]**.
5. SL1 assigns the credential an ID number. Take note of the ID number that appears in the Credential Editor heading, as you will need this when ***creating the master SOAP/XML credential***.



Credential Editor [86]

Edit SSH/Key Credential #86

Basic Settings

Credential Name: CCM1 - SSH

Hostname/IP: [redacted]

Port: 443

Timeout(ms): 1000

Username: [redacted]

Password: ••••••••••••••••

Private Key (PEM Format):

6. Repeat these steps for each major component in your HA CloudCenter deployment.

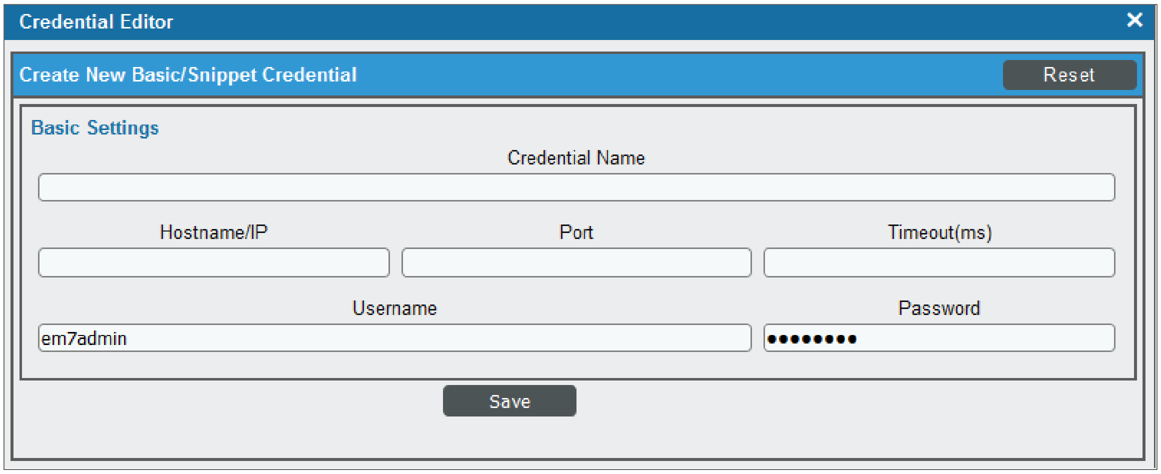
Creating a Basic/Snippet Credential for RabbitMQ

In addition to an SSH/Key credential that allows the Dynamic Applications in the *Cisco: CloudCenter* PowerPack to communicate with your RabbitMQ system, you must also create a Basic/Snippet credential for RabbitMQ. When you discover your HA CloudCenter deployment, these Dynamic Applications will discover and model the CloudCenter RabbitMQ components. These components will later be merged with the physical devices once they are discovered.

NOTE: When monitoring a high-availability CloudCenter deployment, the use of Basic/Snippet credentials will cause RabbitMQ Dynamic Applications to align to RabbitMQ devices, but those Dynamic Applications will not collect data. This is because SL1 discovers the RabbitMQ load balancer devices as the RabbitMQ components, rather than the actual RabbitMQ components themselves. This means that, even if you manually discover the RabbitMQ components, the *Cisco: CloudCenter* PowerPack has no way of linking them with the load balancers. If you would like to collect data for the non-load balancer RabbitMQ components, you can manually align the appropriate credentials.

To create a Basic/Snippet credential to access a RabbitMQ system:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click **[Actions]**, and then select *Create Basic/Snippet Credential*.
3. Complete the following fields:



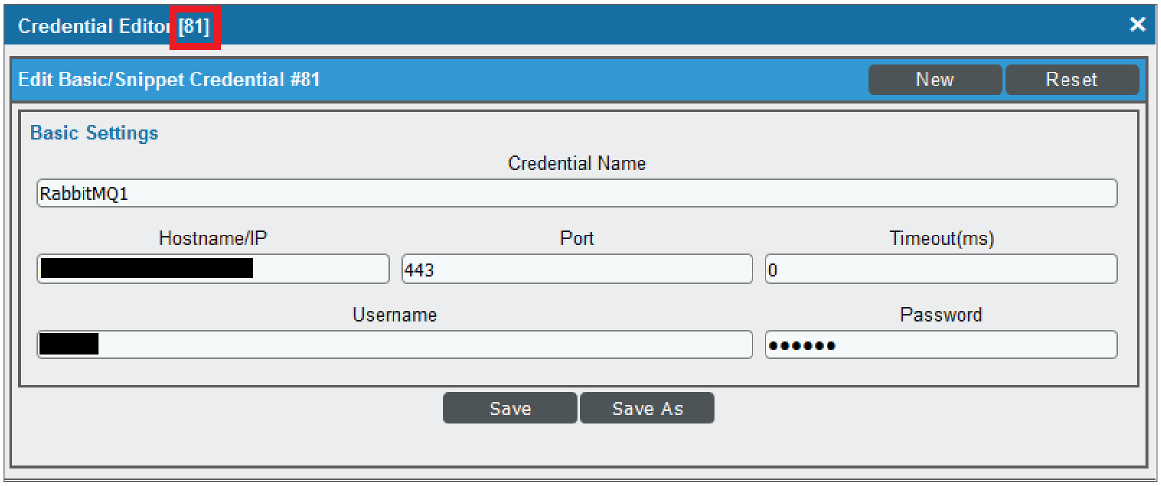
Username: em7admin

Password: ••••••••

- ***Profile Name***. Type a name for the RabbitMQ credential.
- ***Hostname/IP***. Type the hostname or IP address for the RabbitMQ server.
- ***Port***. Type the port number required to access the RabbitMQ server.
- ***Timeout(ms)***.Type the time, in milliseconds, after which SL1 will stop trying to communicate with the RabbitMQ server.
- ***Username***. Type the username for a RabbitMQ user that has read permission to the RabbitMQ API.
- ***Password***. Type the password for the user you entered in the ***Username*** field.

4. Click **[Save]**.

5. SL1 assigns the credential an ID number. Take note of the ID number that appears in the Credential Editor heading, as you will need this when *creating the master SOAP/XML credential*.



Credential Editor [81]

Edit Basic/Snippet Credential #81

Basic Settings

Credential Name: RabbitMQ1

Hostname/IP: [redacted]

Port: 443

Timeout(ms): 0

Username: [redacted]

Password: ●●●●●●

Creating the Master SOAP/XML Credential for High-Availability Discovery

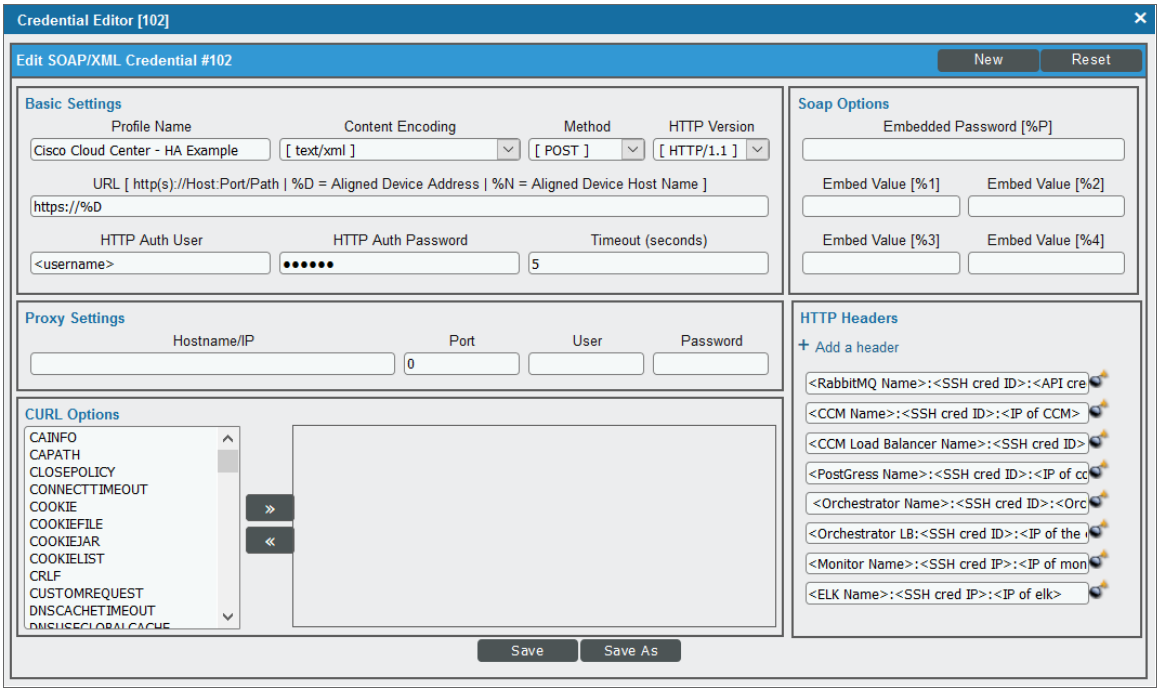
After you have created the *SSH/Key* and *Basic/Snippet* credentials for the various components in your HA CloudCenter, you must create the SOAP/XML credential that will be used as the master credential to discover and model your HA CloudCenter deployment.

A sample credential (**Cisco CloudCenter - HA Example**) that you can use is included in the *Cisco: CloudCenter* PowerPack.

To create a SOAP/XML credential for discovering HA Cisco CloudCenter deployments:

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

2. Locate the **Cisco CloudCenter - HA Example** credential and then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears:



Profile Name: Cisco Cloud Center - HA Example

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://%D

HTTP Auth User: <username>

HTTP Auth Password: ••••••

Timeout (seconds): 5

Embedded Password [%P]:

Embed Value [%1]:

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

Hostname/IP:

Port: 0

User:

Password:

<RabbitMQ Name>:<SSH cred ID>:<API cre

<CCM Name>:<SSH cred ID>:<IP of CCM>

<CCM Load Balancer Name>:<SSH cred ID>

<PostGress Name>:<SSH cred ID>:<IP of cc

<Orchestrator Name>:<SSH cred ID>:<Orc

<Orchestrator LB:<SSH cred ID>:<IP of the

<Monitor Name>:<SSH cred IP>:<IP of mon

<ELK Name>:<SSH cred IP>:<IP of elk>

3. Complete the following fields:

Basic Settings

- ***Profile Name***. Type a new name for the credential.
- ***HTTP Auth User***. Type the username for a CloudCenter Manager user that has root tenant administration privileges. This account must be an API user, not a GUI user.
- ***HTTP Auth Password***. Type the API key for the user you entered in the ***HTTP Auth User*** field.

HTTP Headers

- ***HTTP Headers***. Type the following information for each of the CloudCenter components, creating a separate header for each component:
  - **RabbitMQ:** Type the header in the following format:

    <Component Name>:<SSH/Key Credential ID>:<Basic/Snippet Credential ID>:<RabbitMQ IP address>:<RabbitMQ Load Balancer IP Address>

    > ***Example:*** If the RabbitMQ has an SSH/Key credential with the ID 60, a Basic/Snippet Credential with the ID 70, an IP address of 10.123.34.45, and a load balancer IP address of 10.22.33.45, then you would type "RabbitMQ:60:70:10.123.34.45:10.22.33.45".

- **CloudCenter Manager:** Type the header in the following format:

  <Component Name>:<SSH/Key Credential ID>:<IP address>

  > ***Example:*** If the CloudCenter Manager has an SSH/Key credential with the ID 80 and an IP address of 10.11.23.45, then you would type "CCM:80:10.11.23.45".

- **CloudCenter Manager Load Balancer:** Type the header in the following format:

  <Component Name>:<SSH/Key Credential ID>:<IP address>

  > ***Example:*** If the CloudCenter Manager Load Balancer has an SSH/Key credential with the ID 90 and an IP address of 10.22.12.34, then you would type "CCMLB:90:10.22.12.34".

- **PostgreSQL Database:** Type the header in the following format:

  <Component Name>:<SSH/Key Credential ID>:<IP address>

  > ***Example:*** If the PostgreSQL database has an SSH/Key credential with the ID 105 and an IP address of 10.32.54.76, then you would type "PostgreSQL:105:10.32.54.76".

- **CloudCenter Orchestrator:** Type the header in the following format:

  <Component Name>:<SSH/Key Credential ID>:<Orchestrator IP address>:<Orchestrator Load Balancer IP Address>

  > ***Example:*** If the CloudCenter Orchestrator has an SSH/Key credential with the ID 120, an IP address of 10.33.22.11, and a load balancer IP address of 10.99.88.77, then you would type "CCO:120:10.33.22.11:10.99.88.77".

- **CloudCenter Orchestrator Load Balancer:** Type the header in the following format:

  <Component Name>:<SSH/Key Credential ID>:<IP address>

  > ***Example:*** If the CloudCenter Orchestrator Load Balancer has an SSH/Key credential with the ID 120 and an IP address of 10.99.88.77, then you would type "CCOLB:120:10.99.88.77".

- **CloudCenter Health Monitor:** Type the header in the following format:

  <Component Name>:<SSH/Key Credential ID>:<IP address>

  > ***Example:*** If the Health Monitor has an SSH/Key credential with the ID 135 and an IP address of 10.56.77.89, then you would type "Monitor:135:10.56.77.89".

- **CloudCenter ELK Components:** Type the header in the following format:

  <ELK Name>:<SSH/Key Credential ID>:<IP address>

  > ***Example:*** If the ELK component has an SSH/Key credential with the ID 85 and an IP address of 10.13.24.57, then you would type "ELK:85:10.13.24.57".

NOTE: If you have more than one of the same component, then you can add numbers to the component name. For example: "CCM1", "CCM2", etc.

NOTE: Component names for load balancers must include "LB".

NOTE: If any of your components use a hostname instead of an IP address, you should include the hostname in place of the IP address.

CAUTION: The IP address or hostname used in the header for a given component must match the IP address or hostname in the discovery payload. If any of the headers for any of the components are incorrect, SL1 will be unable to discover and model your HA CloudCenter deployment.

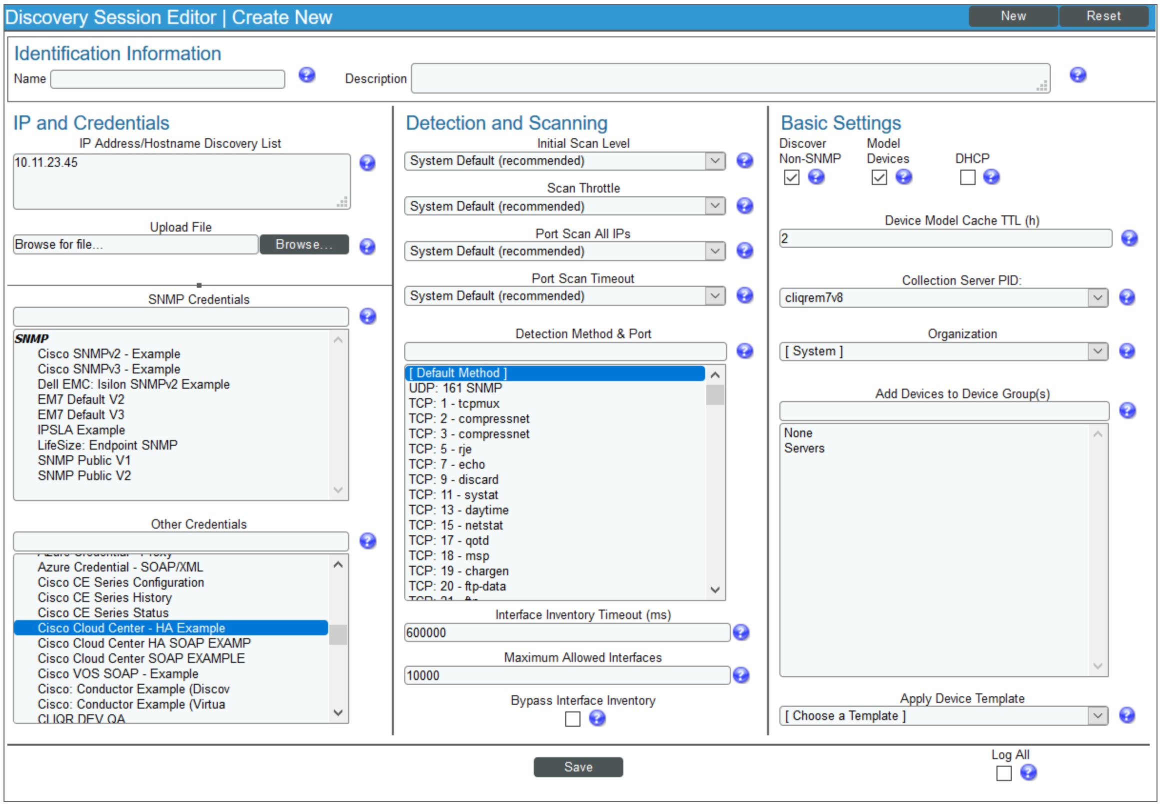
4. For all other fields, use the default values.
5. Click **[Save As]**.
6. In the confirmation message, click **[OK]**.

Discovering Cisco CloudCenter High-Availability Deployments

To discover a Cisco CloudCenter HA deployment:

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:



IP Address/Hostname Discovery List: 10.11.23.45

SNMP: Cisco SNMPv2 - Example, Cisco SNMPv3 - Example, Dell EMC: Isilon SNMPv2 Example, EM7 Default V2, EM7 Default V3, IPSLA Example, LifeSize: Endpoint SNMP, SNMP Public V1, SNMP Public V2

Other Credentials: Azure Credential - SOAP/XML, Cisco CE Series Configuration, Cisco CE Series History, Cisco CE Series Status, Cisco Cloud Center - HA Example (selected), Cisco Cloud Center HA SOAP EXAMP, Cisco Cloud Center SOAP EXAMPLE, Cisco VOS SOAP - Example, Cisco: Conductor Example (Discov, Cisco: Conductor Example (Virtua, CLIQR DEV QA

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] (selected), 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, TCP: 17 - qotd, TCP: 18 - msp, TCP: 19 - chargen, TCP: 20 - ftp-data

Interface Inventory Timeout (ms): 600000

Maximum Allowed Interfaces: 10000

Bypass Interface Inventory ☐

Discover Non-SNMP ☑ Model Devices ☑ DHCP ☐

Device Model Cache TTL (h): 2

Collection Server PID: cliqrem7v8

Organization: [System]

Add Devices to Device Group(s): None, Servers

Apply Device Template: [Choose a Template]

Log All ☐

- ***Name***. Type a name for the discovery session.
- ***IP Address/Hostname Discovery List***. Type the IP address for the CloudCenter Manager.
- ***Other Credentials***. Select the *SOAP/XML credential* you created for the HA CloudCenter deployment.
- ***Discover Non-SNMP***. 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.

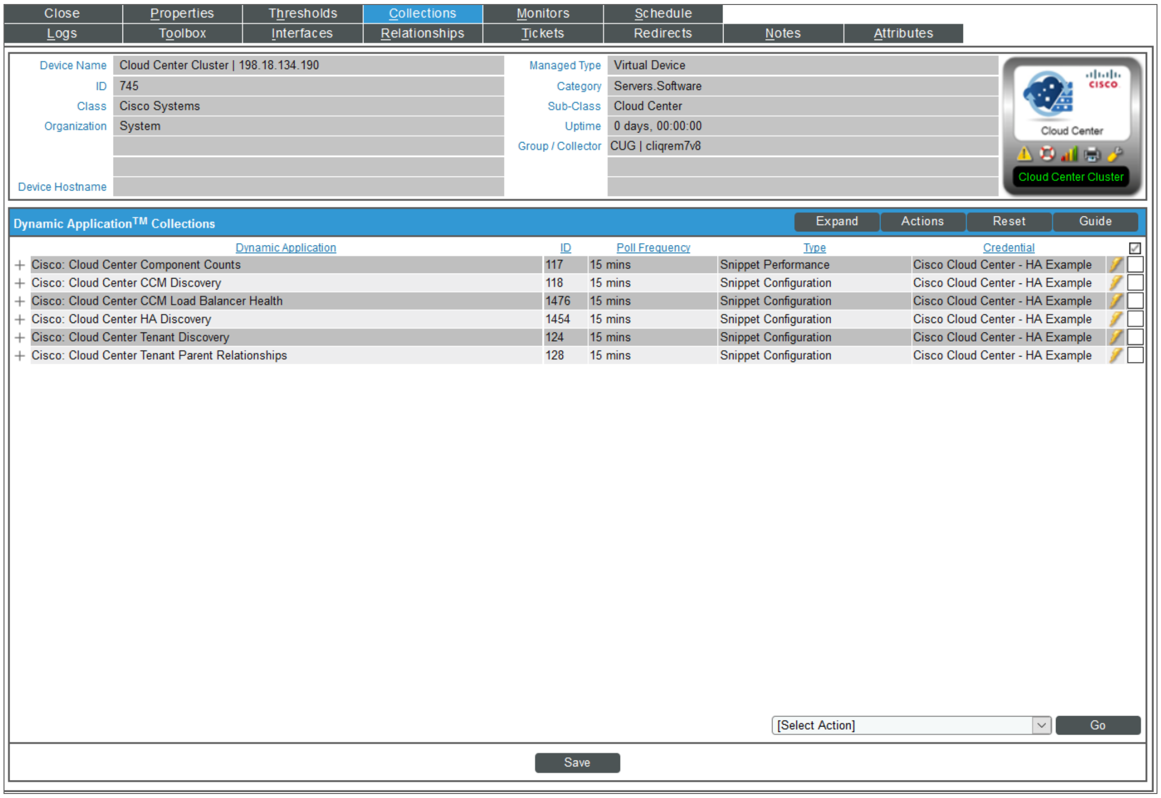
7. The **Discovery Session** window appears. When the device is discovered, click the device icon (🖥) to view the **Device Properties** page for the device.

Verifying Discovery and Dynamic Application Alignment

To verify that SL1 automatically aligned the correct Dynamic Applications during discovery:

1. From the **Device Properties** page for the CloudCenter HA root device, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. All applicable Dynamic Applications for the CloudCenter root device 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	Cloud Center Cluster | 198.18.134.190	Managed Type	Virtual Device
ID	745	Category	Servers.Software
Class	Cisco Systems	Sub-Class	Cloud Center
Organization	System	Uptime	0 days, 00:00:00
		Group / Collector	CUG | cliqrem7v8
Device Hostname			

Dynamic Application^{TM} Collections

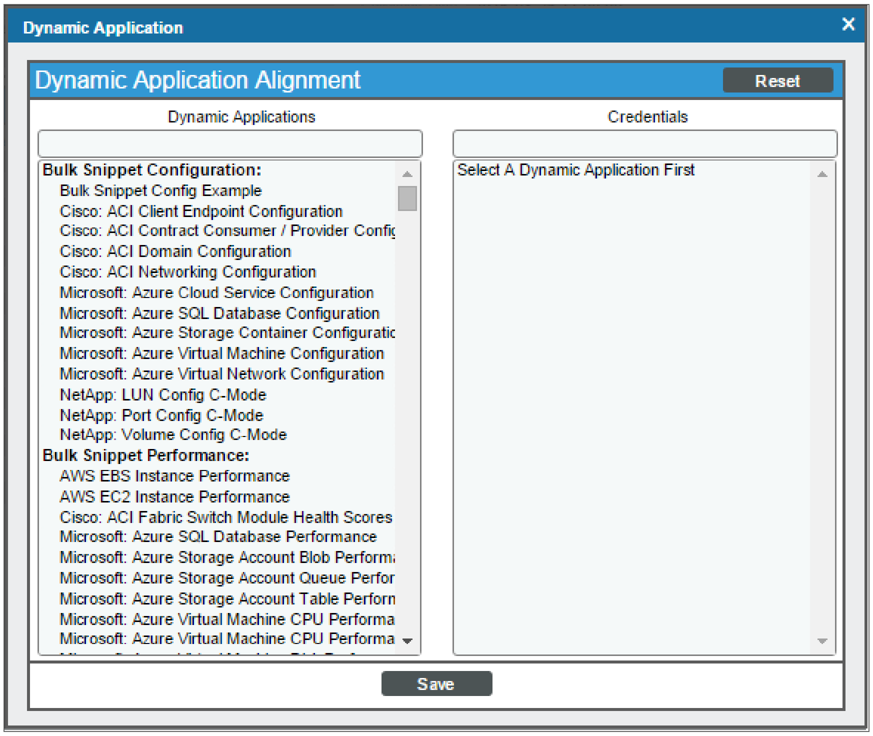
Dynamic Application	ID	Poll Frequency	Type	Credential	☑
+ Cisco: Cloud Center Component Counts	117	15 mins	Snippet Performance	Cisco Cloud Center - HA Example	□
+ Cisco: Cloud Center CCM Discovery	118	15 mins	Snippet Configuration	Cisco Cloud Center - HA Example	□
+ Cisco: Cloud Center CCM Load Balancer Health	1476	15 mins	Snippet Configuration	Cisco Cloud Center - HA Example	□
+ Cisco: Cloud Center HA Discovery	1454	15 mins	Snippet Configuration	Cisco Cloud Center - HA Example	□
+ Cisco: Cloud Center Tenant Discovery	124	15 mins	Snippet Configuration	Cisco Cloud Center - HA Example	□
+ Cisco: Cloud Center Tenant Parent Relationships	128	15 mins	Snippet Configuration	Cisco Cloud Center - HA Example	□

The following Dynamic Applications should be aligned to the device:

- Cisco: CloudCenter Component Counts
- Cisco: CloudCenter CCM Discovery
- Cisco: CloudCenter CCM Load Balancer Health
- Cisco: CloudCenter HA Discovery
- Cisco: CloudCenter Tenant Discovery
- Cisco: CloudCenter Tenant Parent Relationships

If the listed Dynamic Applications have not been automatically aligned during discovery, you can align them manually. To do so, perform the following steps:

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

Bulk Snippet Configuration:
Bulk Snippet Config Example
Cisco: ACI Client Endpoint Configuration
Cisco: ACI Contract Consumer / Provider Config
Cisco: ACI Domain Configuration
Cisco: ACI Networking Configuration
Microsoft: Azure Cloud Service Configuration
Microsoft: Azure SQL Database Configuration
Microsoft: Azure Storage Container Configuratic
Microsoft: Azure Virtual Machine Configuration
Microsoft: Azure Virtual Network Configuration
NetApp: LUN Config C-Mode
NetApp: Port Config C-Mode
NetApp: Volume Config C-Mode
Bulk Snippet Performance:
AWS EBS Instance Performance
AWS EC2 Instance Performance
Cisco: ACI Fabric Switch Module Health Scores
Microsoft: Azure SQL Database Performance
Microsoft: Azure Storage Account Blob Performa
Microsoft: Azure Storage Account Queue Perfor
Microsoft: Azure Storage Account Table Perforn
Microsoft: Azure Virtual Machine CPU Performa
Microsoft: Azure Virtual Machine CPU Performa

Credentials

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 *SOAP/XML credential* you created for CloudCenter.
4. Click the **[Save]** button.
5. Repeat steps 1-4 for the other unaligned Dynamic Applications.

Discovering Multiple Tenants for High-Availability CloudCenter Deployments

The *Cisco: CloudCenter* PowerPack can be used to monitor an HA CloudCenter deployment that includes multiple tenants. To discover multiple tenants, you must follow the steps in the following sections for each tenant in order (in other words, parents must be discovered before their children):

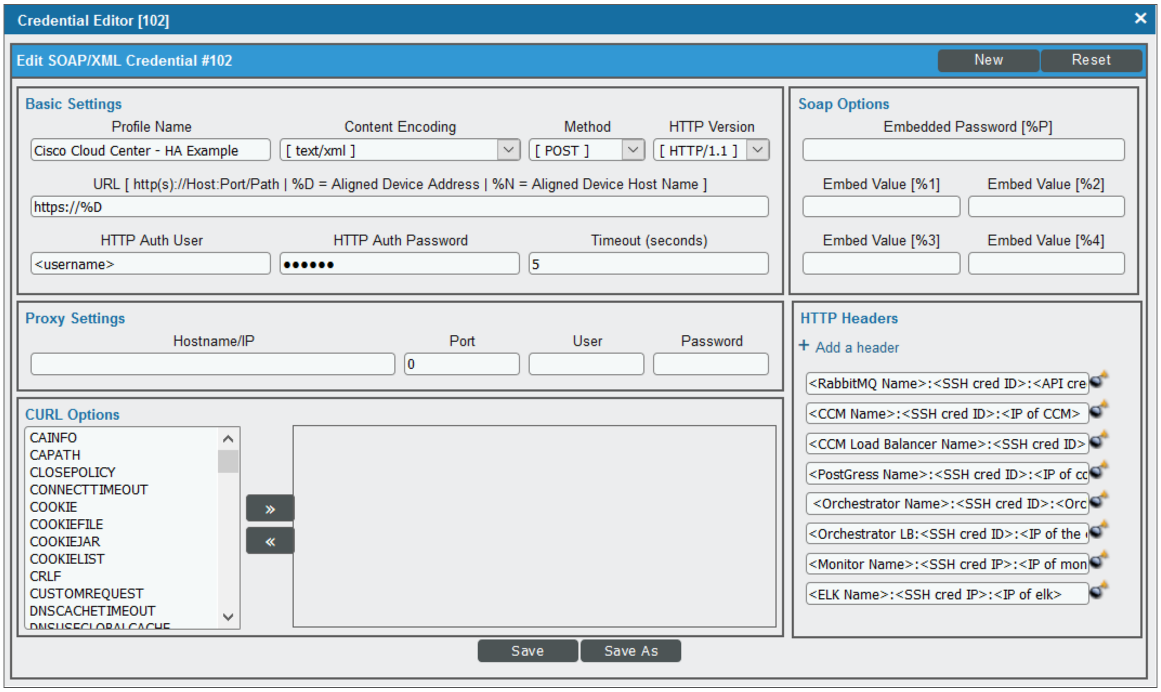
- *Creating a Credential for an HA CloudCenter Manager Tenant*
- *Discovering an additional HA CloudCenter Manager Tenant*

> **NOTE:** For each tenant, you must use the administrator account for that tenant when you create the credential.

Creating a Credential for a High-Availability CloudCenter Tenant

To configure a SOAP/XML credential to access an additional HA CloudCenter tenant:

1. Create any additional *SSH/Key* and *Basic/Snippet* credentials that you might need to reference in the SOAP/XML credential headers.
2. Go to the **Credential Management** page (System > Manage > Credentials).
3. Locate the credential you used to discover the root device for your HA deployment, and then click its wrench icon (). The **Edit SOAP/XML Credential** modal appears.
4. Enter values in the following fields:



Credential Editor [102]

Edit SOAP/XML Credential #102

Basic Settings

Profile Name: Cisco Cloud Center - HA Example

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://%D

HTTP Auth User: <username>

HTTP Auth Password: ••••••

Timeout (seconds): 5

Proxy Settings

Hostname/IP:

Port: 0

User:

Password:

Soap Options

Embedded Password [%P]:

Embed Value [%1]:

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

HTTP Headers

<RabbitMQ Name>:<SSH cred ID>:<API cre

<CCM Name>:<SSH cred ID>:<IP of CCM>

<CCM Load Balancer Name>:<SSH cred ID>

<PostGress Name>:<SSH cred ID>:<IP of cc

<Orchestrator Name>:<SSH cred ID>:<Orc

<Orchestrator LB:<SSH cred ID>:<IP of the

<Monitor Name>:<SSH cred IP>:<IP of mon

<ELK Name>:<SSH cred IP>:<IP of elk>

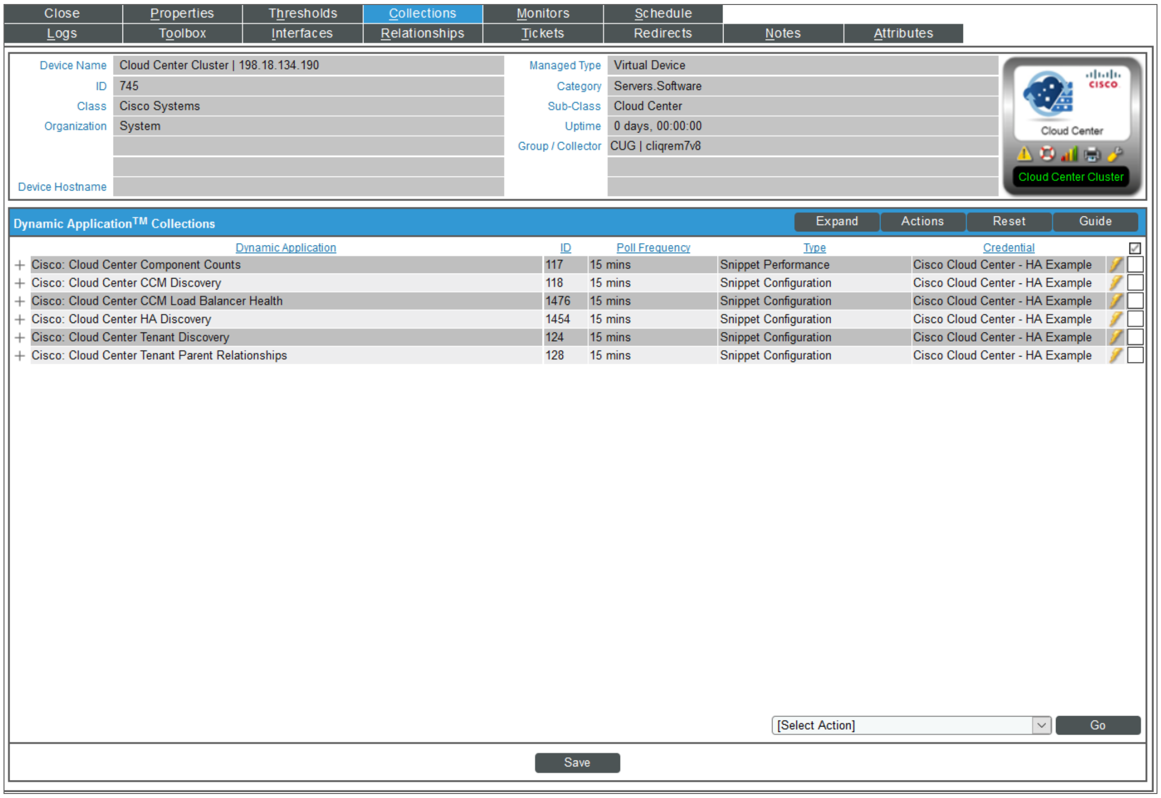
- ***Profile Name***. Enter a new name for the credential.
- For all other fields, follow the instructions described in the *Creating a SOAP/XML Credential for High-Availability Discovery* section.

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

Discovering an Additional High-Availability CloudCenter Tenant

To discover an additional tenant:

1. From the **Device Properties** page for the CloudCenter HA root device, click the **[Collections]** tab. The **Dynamic Application Collections** page appears:



Device Name	Cloud Center Cluster | 198.18.134.190	Managed Type	Virtual Device
ID	745	Category	Servers.Software
Class	Cisco Systems	Sub-Class	Cloud Center
Organization	System	Uptime	0 days, 00:00:00
		Group / Collector	CUG | cliqrem7v8
Device Hostname			

Dynamic Application^{TM} Collections

Dynamic Application	ID	Poll Frequency	Type	Credential	☑
+ Cisco: Cloud Center Component Counts	117	15 mins	Snippet Performance	Cisco Cloud Center - HA Example	□
+ Cisco: Cloud Center CCM Discovery	118	15 mins	Snippet Configuration	Cisco Cloud Center - HA Example	□
+ Cisco: Cloud Center CCM Load Balancer Health	1476	15 mins	Snippet Configuration	Cisco Cloud Center - HA Example	□
+ Cisco: Cloud Center HA Discovery	1454	15 mins	Snippet Configuration	Cisco Cloud Center - HA Example	□
+ Cisco: Cloud Center Tenant Discovery	124	15 mins	Snippet Configuration	Cisco Cloud Center - HA Example	□
+ Cisco: Cloud Center Tenant Parent Relationships	128	15 mins	Snippet Configuration	Cisco Cloud Center - HA Example	□

2. Select the checkbox for the "Cisco: CloudCenter Tenant Discovery" Dynamic Application.
3. In the ***Select Action*** drop-down list, select the SOAP/XML credential you created for the tenant.
4. Click **[Go]**.

Merging RabbitMQ and CloudCenter Orchestrator Devices

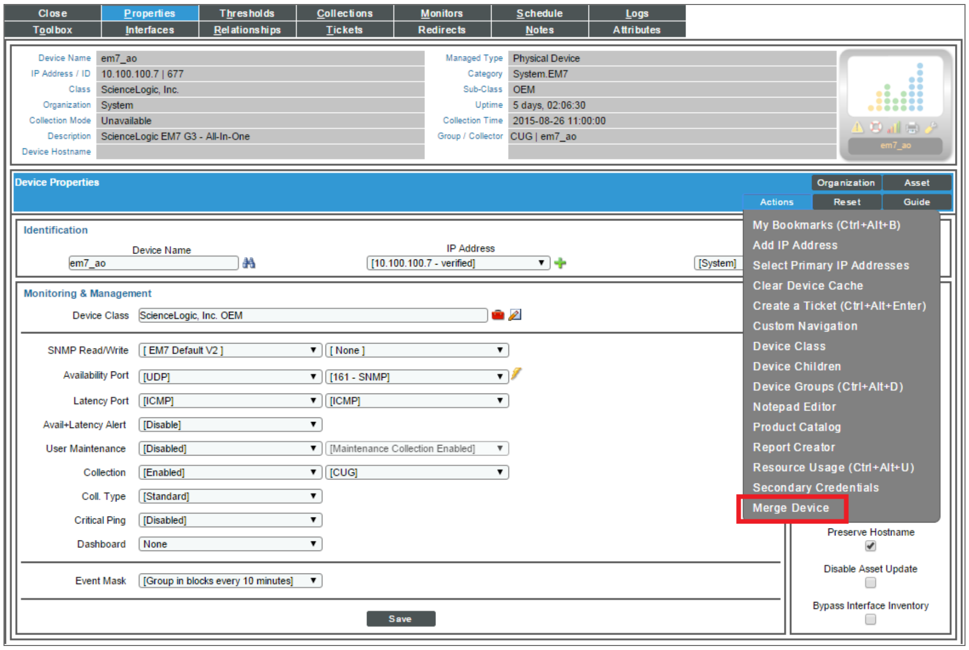
The Dynamic Applications in the *Cisco: CloudCenter*PowerPack create component devices for the RabbitMQ system and CloudCenter Manager. Optionally, you can discover these devices as physical SNMP devices and merge the component device record and physical device record. For information about discovering and monitoring a RabbitMQ system, see the ***Monitoring RabbitMQ Systems*** manual.

To merge individual devices:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).

2. Click the wrench icon (🔧) for the physical device that you want to merge with a component device.

3. On the **Device Properties** page, click the **[Actions]** menu and then select *Merge Device*.



Device Name	em7_ao	Managed Type	Physical Device
IP Address / ID	10.100.100.7 | 677	Category	System.EM7
Class	ScienceLogic, Inc.	Sub-Class	OEM
Organization	System	Uptime	5 days, 02:06:30
Collection Mode	Unavailable	Collection Time	2015-08-26 11:00:00
Description	ScienceLogic EM7 G3 - All-In-One	Group / Collector	CUG | em7_ao
Device Hostname			

Identification

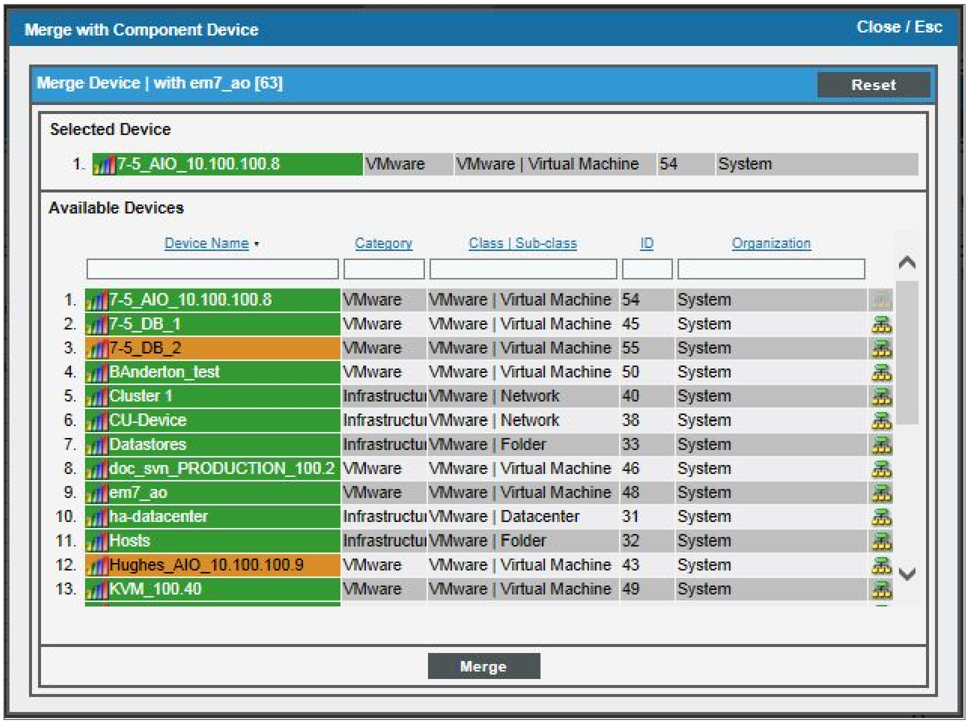
Device Name: em7_ao
IP Address: [10.100.100.7 - verified]
[System]

Monitoring & Management

Device Class: ScienceLogic, Inc. OEM
SNMP Read/Write: [EM7 Default V2] [None]
Availability Port: [UDP] [161 - SNMP]
Latency Port: [ICMP] [ICMP]
Avail+Latency Alert: [Disable]
User Maintenance: [Disabled] [Maintenance Collection Enabled]
Collection: [Enabled] [CUG]
Coll. Type: [Standard]
Critical Ping: [Disabled]
Dashboard: None
Event Mask: [Group in blocks every 10 minutes]

Preserve Hostname ☑
Disable Asset Update ☐
Bypass Interface Inventory ☐

4. A list of component devices that are available for merging with the physical device displays. Click the merge icon (品) for the component device you want to merge with the physical device. Information for the component device then displays in the **Selected Device** panel.



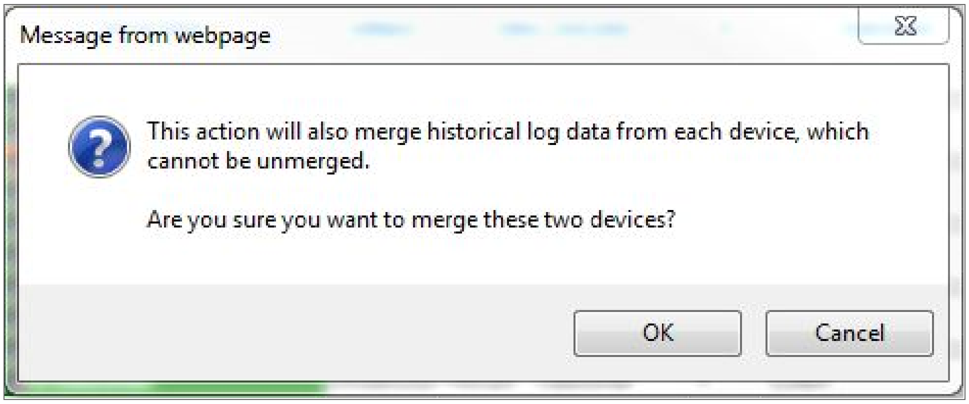
Selected Device

	Device Name	Category	Class | Sub-class	ID	Organization
1.	7-5_AIO_10.100.100.8	VMware	VMware | Virtual Machine	54	System

Available Devices

	Device Name	Category	Class | Sub-class	ID	Organization	
1.	7-5_AIO_10.100.100.8	VMware	VMware | Virtual Machine	54	System	品
2.	7-5_DB_1	VMware	VMware | Virtual Machine	45	System	品
3.	7-5_DB_2	VMware	VMware | Virtual Machine	55	System	品
4.	BAnderton_test	VMware	VMware | Virtual Machine	50	System	品
5.	Cluster 1	Infrastructu	VMware | Network	40	System	品
6.	CU-Device	Infrastructu	VMware | Network	38	System	品
7.	Datastores	Infrastructu	VMware | Folder	33	System	品
8.	doc_svn_PRODUCTION_100.2	VMware	VMware | Virtual Machine	46	System	品
9.	em7_ao	VMware	VMware | Virtual Machine	48	System	品
10.	ha-datacenter	Infrastructu	VMware | Datacenter	31	System	品
11.	Hosts	Infrastructu	VMware | Folder	32	System	品
12.	Hughes_AIO_10.100.100.9	VMware	VMware | Virtual Machine	43	System	品
13.	KVM_100.40	VMware	VMware | Virtual Machine	49	System	品

5. Click the **[Merge]** button. A pop-up message appears that asks you to confirm the merge.



Message from webpage

This action will also merge historical log data from each device, which cannot be unmerged.

Are you sure you want to merge these two devices?

6. Click the **[OK]** button.

NOTE: To view an updated list of devices that includes your merged devices, click the **[Reset]** button on the **Device Manager** page.

Relationships Between Component Devices

SL1 can automatically build relationships between CloudCenter component devices and other associated devices:

- If you discover an ACI system using the Dynamic Applications in the *Cisco: ACI* PowerPack version 106 or later, SL1 will automatically create relationships between CloudCenter Applications and ACI Application Network Profiles.
- If you discover an AWS account using the Dynamic Applications in the *Amazon Web Services* PowerPack version 103 or later, SL1 will automatically create relationships between CloudCenter Applications and AWS EC2 Instances.
- If you discover an Azure account using the Dynamic Applications in the *Microsoft: Azure* PowerPack version 103 or later, SL1 will automatically create relationships between CloudCenter Applications and Azure Virtual Machines.
- If you discover a vCenter device using the Dynamic Applications in the *VMware: vSphere Base Pack* PowerPack version 207 or later, SL1 will automatically create relationships between CloudCenter Applications and VMware Virtual Machines.

Chapter 11

Cisco: Contact Center Enterprise

Overview

The following sections describe how to configure and discover Cisco Unified Contact Center Enterprise services for monitoring by SL1 using the *Cisco: Contact Center Enterprise* PowerPack:

NOTE: For more information about the *Cisco: Contact Center Enterprise* PowerPack, see the ***Monitoring Cisco Unified Contact Center Enterprise*** manual.

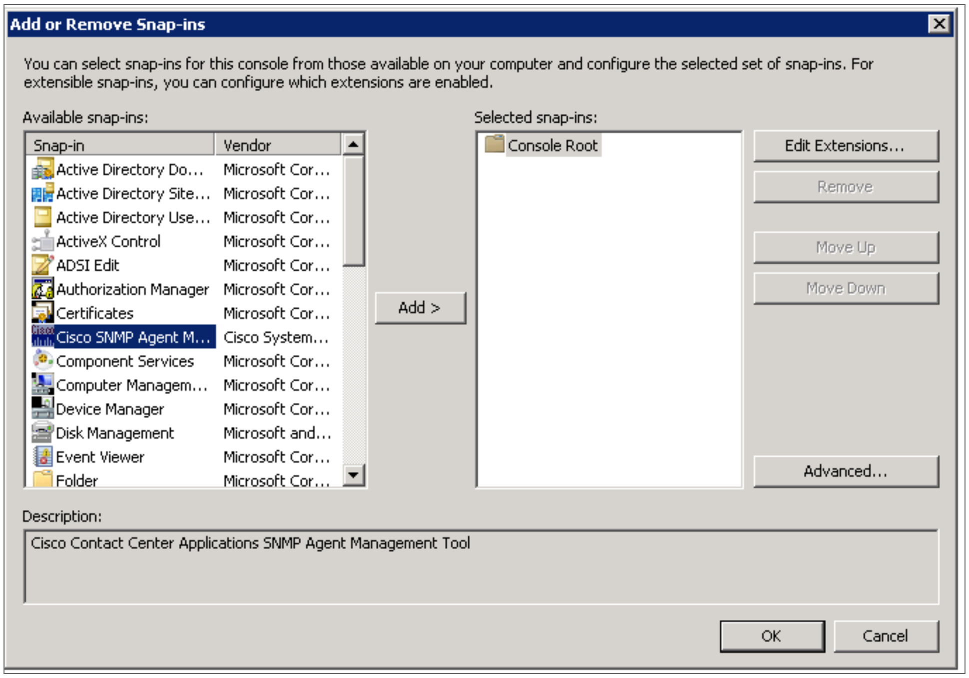
Configuring Unified Contact Center Enterprise Monitoring Using SNMP

Before you can discover and monitor Cisco Unified Contact Center Enterprise (UCCE) devices in SL1, you must first configure SNMP community strings in each of the UCCE services that you will monitor with SL1. You can then create an SNMP credential in SL1 that enables it to collect data from the UCCE services. Finally, you must compile several Management Information Bases (MIBs) that are required for monitoring UCCE.

Enabling SNMP in Cisco Unified Contact Center Enterprise

To enable SNMP in Cisco Unified Contact Center Enterprise, perform the following steps:

1. Log in to the Cisco Unified Contact Center Enterprise Server as an administrator.
2. Open Microsoft Management Console (32-bit).
3. Click **[File]**, then select *Add/Remove Snap-In*. The **Add or Remove Snap-ins** page appears.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Cisco SNMP Agent M...	Cisco System...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...

Selected snap-ins:

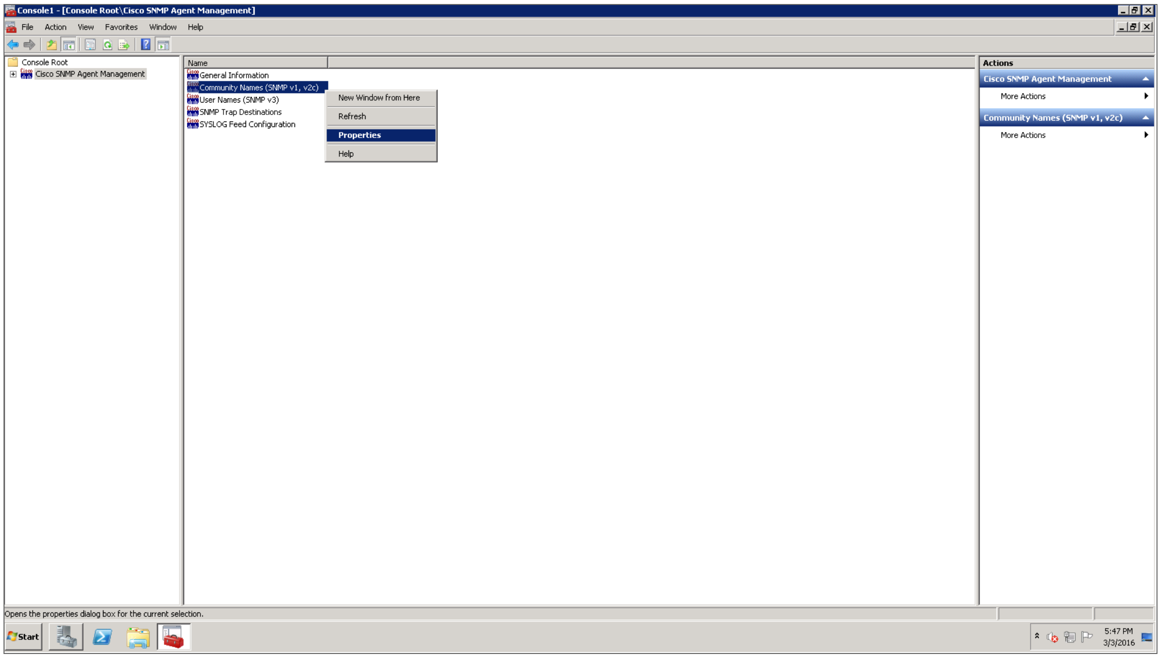
Console Root

Description:

Cisco Contact Center Applications SNMP Agent Management Tool

4. In the ***Available snap-ins*** field, select **Cisco SNMP Agent Management**, then click **[Add >]** to move it to the ***Selected snap-ins*** field.
5. Click **[OK]**.

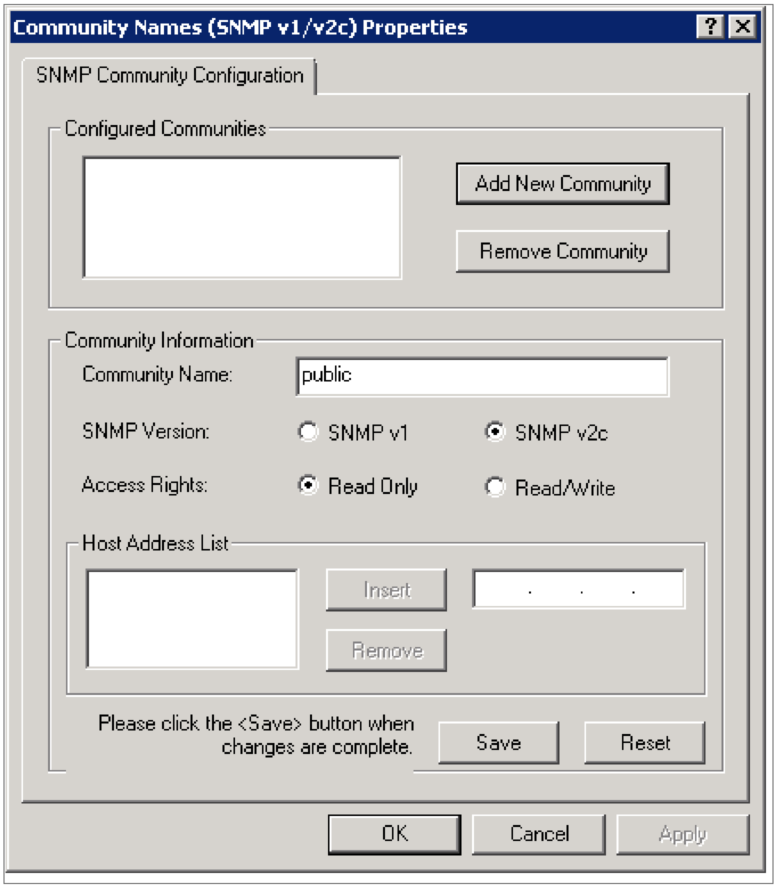
6. In the left panel of the Microsoft Management Console, click **Cisco SNMP Agent Management**. Then, in the right panel, right-click **Community Names (SNMP v1, v2c)** and select *Properties*.



Opens the properties dialog box for the current selection.

7. In the **Community Names (SNMP v1/v2c) Properties** modal page, click the **[Add New Community]** button to enable the fields on the page.

8. Make entries in the following fields:



Community Names (SNMP v1/v2c) Properties

SNMP Community Configuration

Configured Communities

Community Information

Community Name: public

SNMP Version: ○ SNMP v1 ● SNMP v2c

Access Rights: ● Read Only ○ Read/Write

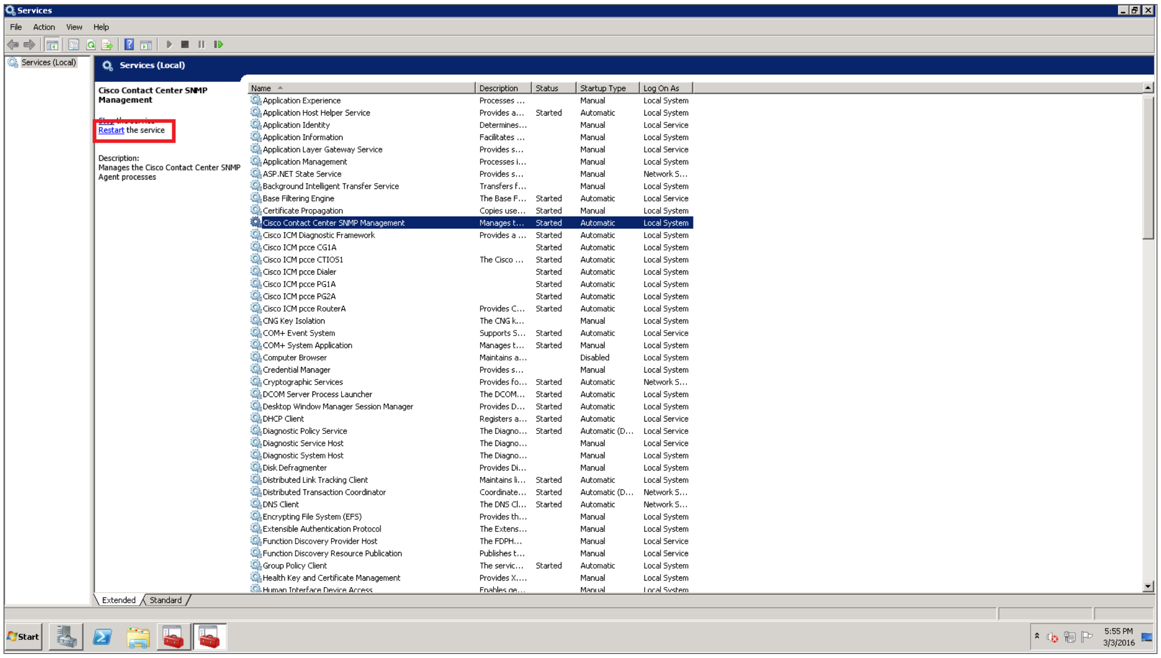
Host Address List

Please click the <Save> button when changes are complete.

- ***Community Name***. Enter a name for the new community string.
- ***SNMP Version***. Select *SNMP v2c*.
- ***Access Rights***. Select *Read Only*.

9. Click **[Save]**, and then click **[OK]**.
10. Close the Microsoft Management Console.
11. Open the Microsoft Windows Services console.

12. In the Microsoft Windows Services console, select **Cisco Contact Center SNMP Management** from the list of local services, then click the **Restart** hyperlink to restart the service.



Cisco Contact Center SNMP Management

Stop the service
Restart the service

Description:
Manages the Cisco Contact Center SNMP Agent processes

Name	Description	Status	Startup Type	Log On As
Application Experience	Processes ...		Manual	Local System
Application Host Helper Service	Provides a...	Started	Automatic	Local System
Application Identity	Determines...		Manual	Local Service
Application Information	Facilitates ...		Manual	Local System
Application Layer Gateway Service	Provides s...		Manual	Local Service
Application Management	Processes i...		Manual	Local System
ASP.NET State Service	Provides s...		Manual	Network S...
Background Intelligent Transfer Service	Transfers f...		Manual	Local System
Base Filtering Engine	The Base F...	Started	Automatic	Local Service
Certificate Propagation	Copies use...	Started	Manual	Local System
Cisco Contact Center SNMP Management	Manages t...	Started	Automatic	Local System
Cisco ICM Diagnostic Framework	Provides a ...	Started	Automatic	Local System
Cisco ICM pcce CG1A		Started	Automatic	Local System
Cisco ICM pcce CTIOS1	The Cisco ...	Started	Automatic	Local System
Cisco ICM pcce Dialer		Started	Automatic	Local System
Cisco ICM pcce PG1A		Started	Automatic	Local System
Cisco ICM pcce PG2A		Started	Automatic	Local System
Cisco ICM pcce RouterA	Provides C...	Started	Automatic	Local System
CNG Key Isolation	The CNG k...		Manual	Local System
COM+ Event System	Supports S...	Started	Automatic	Local Service
COM+ System Application	Manages t...	Started	Manual	Local System
Computer Browser	Maintains a...		Disabled	Local System
Credential Manager	Provides s...		Manual	Local System
Cryptographic Services	Provides fo...	Started	Automatic	Network S...
DCOM Server Process Launcher	The DCOM...	Started	Automatic	Local System
Desktop Window Manager Session Manager	Provides D...	Started	Automatic	Local System
DHCP Client	Registers a...	Started	Automatic	Local Service
Diagnostic Policy Service	The Diagno...	Started	Automatic (D...	Local Service
Diagnostic Service Host	The Diagno...		Manual	Local Service
Diagnostic System Host	The Diagno...		Manual	Local System
Disk Defragmenter	Provides Di...		Manual	Local System
Distributed Link Tracking Client	Maintains li...	Started	Automatic	Local System
Distributed Transaction Coordinator	Coordinate...	Started	Automatic (D...	Network S...
DNS Client	The DNS Cl...	Started	Automatic	Network S...
Encrypting File System (EFS)	Provides th...		Manual	Local System
Extensible Authentication Protocol	The Extens...		Manual	Local System
Function Discovery Provider Host	The FDPH...		Manual	Local Service
Function Discovery Resource Publication	Publishes t...		Manual	Local Service
Group Policy Client	The servic...	Started	Automatic	Local System
Health Key and Certificate Management	Provides X....		Manual	Local System
Human Interface Device Access	Enables ge...		Manual	Local System

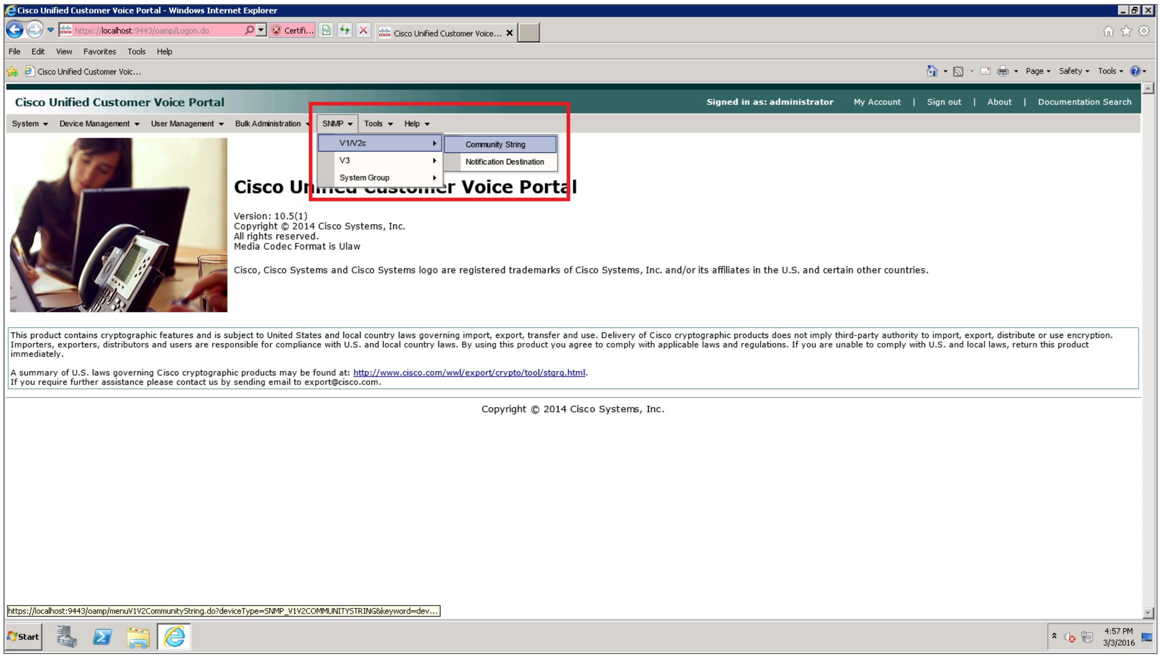
13. Close the Microsoft Windows Services console.
14. Click the Windows **[Start]** menu, then go to Control Panel > System and Security > Windows Firewall.
15. In the left panel, click the **Turn Windows Firewall on or off** hyperlink. The **Customize Settings** page appears.
16. Under **Domain network location settings**, select *Turn off Windows Firewall*, then click **[OK]**.
17. To enable SNMP in Cisco Unified Contact Center Enterprise Data Server, log in to Cisco Unified Contact Center Enterprise Data Server as an administrator and repeat steps 2-16.

Enabling SNMP in Cisco Unified Customer Voice Portal (CVP)

To enable SNMP in Cisco Unified Customer Voice Portal, perform the following steps:

1. Log in to Cisco Unified Customer Voice Portal as an administrator.

2. Click the **[SNMP]** tab, then select *V1/V2c > Community String*.



Cisco Unified Customer Voice Portal - Windows Internet Explorer
https://localhost:9443/oamp/Logon.do
File Edit View Favorites Tools Help
Cisco Unified Customer Voice Portal
Signed in as: administrator
My Account | Sign out | About | Documentation Search
System Device Management User Management Bulk Administration SNMP Tools Help
V1/V2c
V3
System Group
Community String
Notification Destination
4:57 PM
3/3/2016

Cisco Unified Customer Voice Portal

Version: 10.5(1)
Copyright © 2014 Cisco Systems, Inc.
All rights reserved.
Media Codec Format is Ulaw

Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

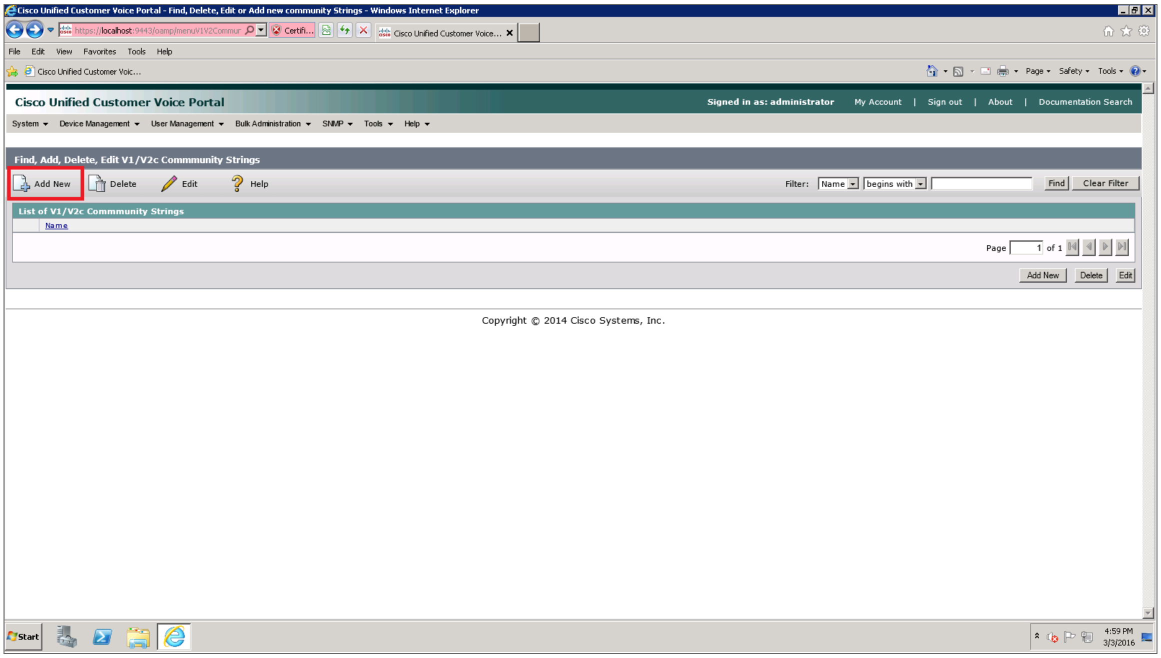
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html.
If you require further assistance please contact us by sending email to export@cisco.com.

Copyright © 2014 Cisco Systems, Inc.

https://localhost:9443/oamp/menuV1V2CommunityString.do?deviceType=SNMP_V1V2COMMUNITYSTRING&keyword=dev...

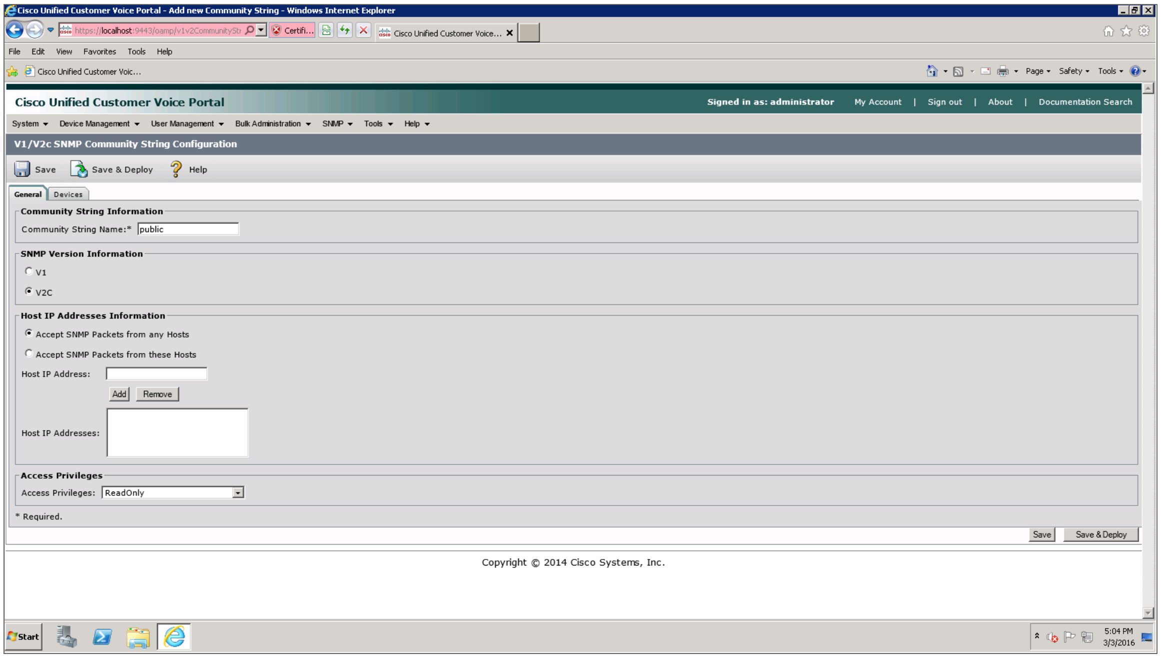
3. On the **Find, Add, Delete, Edit V1/V2c Community Strings** page, click the **[Add New]** button.



Cisco Unified Customer Voice Portal - Find, Delete, Edit or Add new community Strings - Windows Internet Explorer
https://localhost:9443/oamp/menuV1V2Commur
File Edit View Favorites Tools Help
Cisco Unified Customer Voice Portal
Signed in as: administrator
My Account | Sign out | About | Documentation Search
System Device Management User Management Bulk Administration SNMP Tools Help
Find, Add, Delete, Edit V1/V2c Commmunity Strings
Add New
Delete
Edit
Help
Filter: Name begins with
Find
Clear Filter
List of V1/V2c Commmunity Strings
Name
Page 1 of 1
Add New
Delete
Edit
4:59 PM
3/3/2016

Copyright © 2014 Cisco Systems, Inc.

4. The **V1/V2c SNMP Community String Configuration** page appears. Make entries in the following fields:


Cisco Unified Customer Voice Portal - Add new Community String - Windows Internet Explorer
Cisco Unified Customer Voice Portal
Signed in as: administrator | My Account | Sign out | About | Documentation Search
System | Device Management | User Management | Bulk Administration | SNMP | Tools | Help
Save | Save & Deploy | Help
General | Devices
Add | Remove
Save | Save & Deploy

V1/V2c SNMP Community String Configuration

Community String Information

Community String Name:* public

SNMP Version Information

○ V1

● V2C

Host IP Addresses Information

● Accept SNMP Packets from any Hosts

○ Accept SNMP Packets from these Hosts

Host IP Address:

Host IP Addresses:

Access Privileges

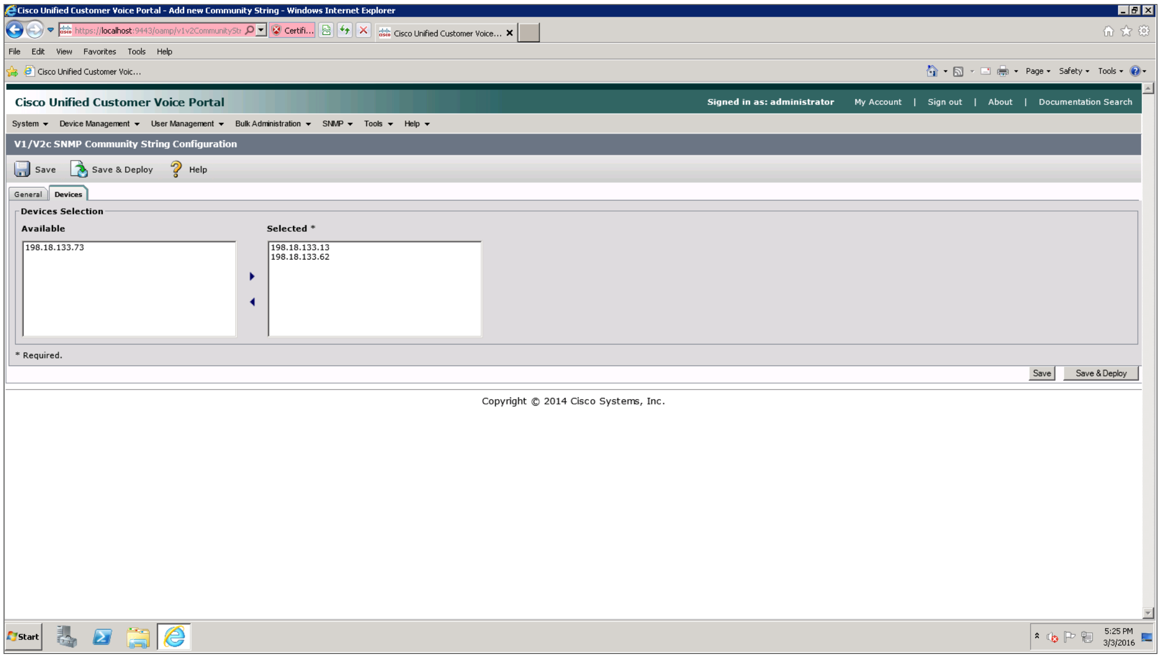
Access Privileges: ReadOnly

* Required.

Copyright © 2014 Cisco Systems, Inc.

- ***Community String Name***. Enter a name for the new community string.
- ***SNMP Version Information***. Select *V2C*.
- For the other fields on the page, use the default values.

5. Click the **[Devices]** tab.


Cisco Unified Customer Voice Portal - Add new Community String - Windows Internet Explorer
Cisco Unified Customer Voice Portal
Signed in as: administrator | My Account | Sign out | About | Documentation Search
System | Device Management | User Management | Bulk Administration | SNMP | Tools | Help
Save | Save & Deploy | Help
General | Devices
Save | Save & Deploy

V1/V2c SNMP Community String Configuration

Devices Selection

Available	Selected *
198.18.133.73	198.18.133.13 198.18.133.62

* Required.

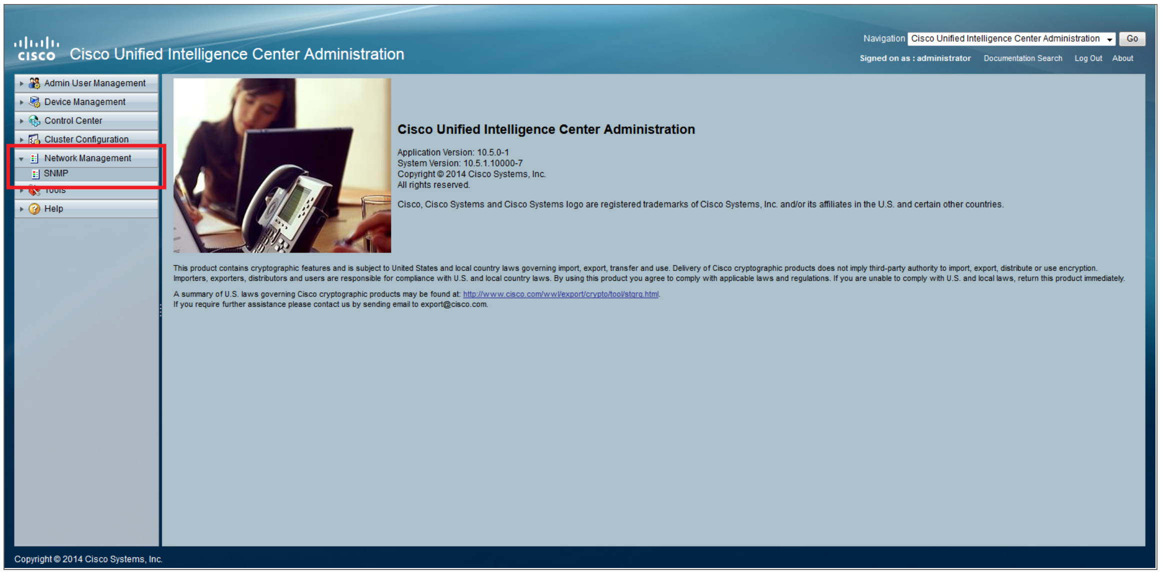
Copyright © 2014 Cisco Systems, Inc.

6. Select one or more of the devices in the ***Available*** field, then click the right-arrow icon to move the selected device(s) to the ***Selected*** field.
7. Click the **[Save & Deploy]** button. A message confirms that the configuration of the SNMP community string was successfully applied to the selected device(s).

Enabling SNMP in Cisco Unified Intelligence Center (CUIC)

To enable SNMP in Cisco Unified Intelligence Center, perform the following steps:

1. Log in to Cisco Unified Intelligence Center as an administrator.
2. In the left panel, click **[Network Management]**, then select *SNMP*.



Cisco Unified Intelligence Center Administration

Application Version: 10.5.0-1
System Version: 10.5.1.10000-7
Copyright © 2014 Cisco Systems, Inc.
All rights reserved.

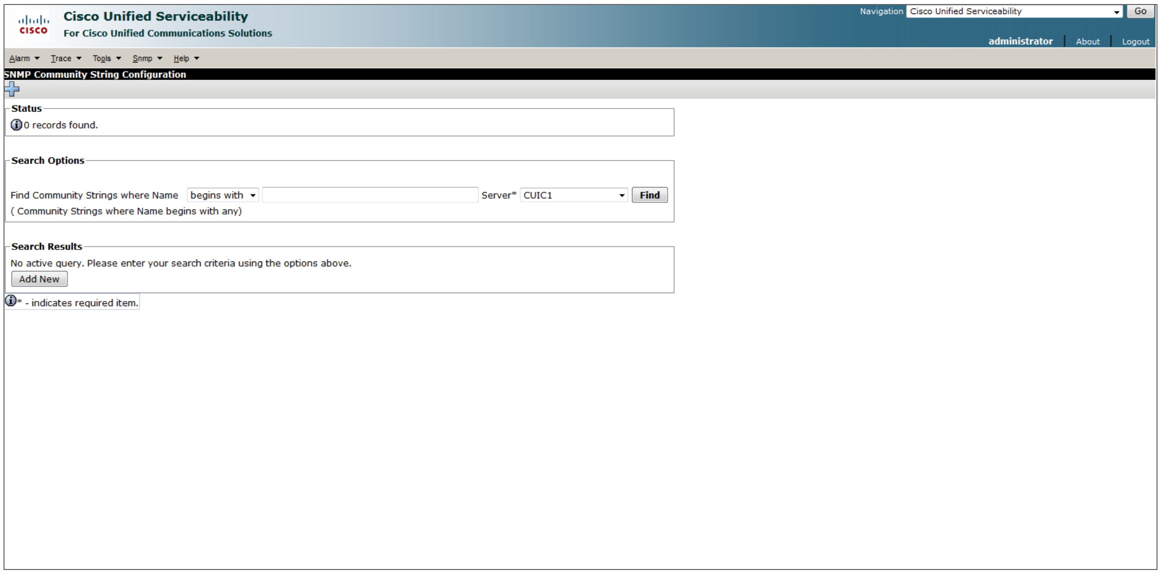
Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html.
If you require further assistance please contact us by sending email to export@cisco.com.

Copyright © 2014 Cisco Systems, Inc.

3. On the **SNMP Community String Configuration** page, under **Search Options**, click **[Find]**. The **Search Results** section appears.


Cisco Unified Serviceability
For Cisco Unified Communications Solutions
Navigation Cisco Unified Serviceability Go
administrator About Logout
Alarm Trace Tools Snmp Help
SNMP Community String Configuration

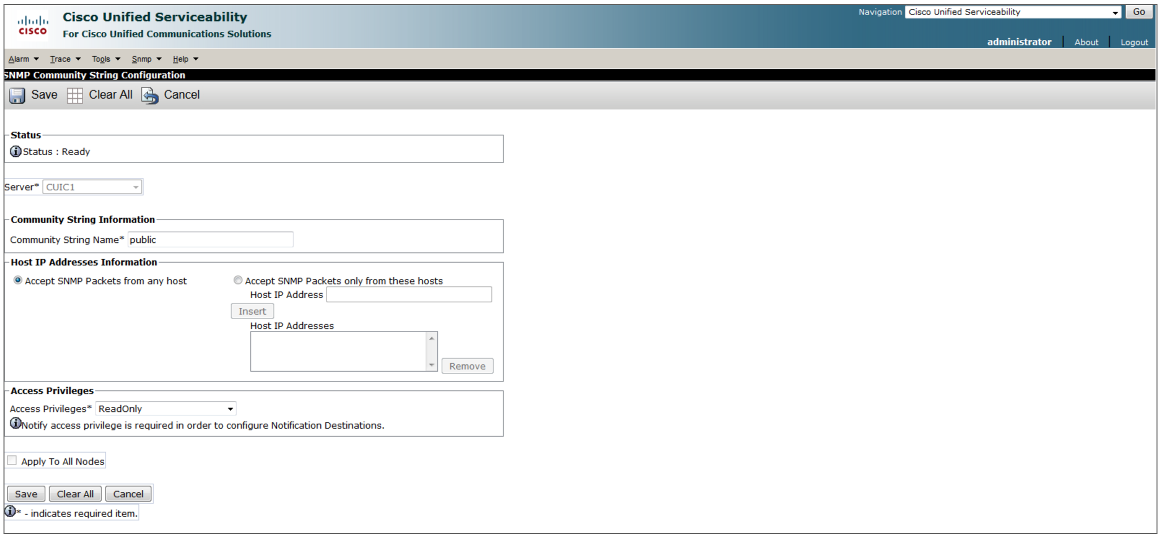
Status
0 records found.

Search Options
Find Community Strings where Name begins with Server* CUIC1 Find
(Community Strings where Name begins with any)

Search Results
No active query. Please enter your search criteria using the options above.
Add New

* - indicates required item.

4. Under **Search Results**, click **[Add New]**.
5. Enter values in the following fields:


Cisco Unified Serviceability
For Cisco Unified Communications Solutions
Navigation Cisco Unified Serviceability Go
administrator About Logout
Alarm Trace Tools Snmp Help
SNMP Community String Configuration
Save Clear All Cancel

Status
Status : Ready

Server* CUIC1

Community String Information
Community String Name* public

Host IP Addresses Information
● Accept SNMP Packets from any host
○ Accept SNMP Packets only from these hosts
Host IP Address
Insert
Host IP Addresses
Remove

Access Privileges
Access Privileges* ReadOnly
Notify access privilege is required in order to configure Notification Destinations.

□ Apply To All Nodes

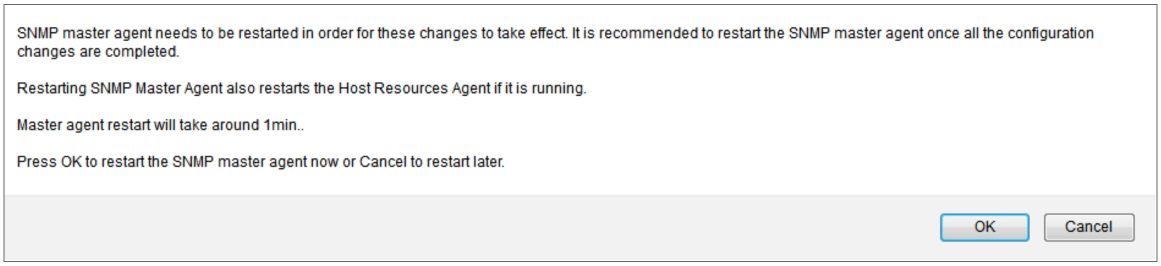
Save Clear All Cancel

* - indicates required item.

- ***Community String Name***. Enter a name for the new community string.
- ***Access Privileges***. Select *ReadOnly*.
- For the other fields on the page, use the default values.

6. Click **[Save]**.

7. Click **[OK]** to restart the SNMP master agent.



SNMP master agent needs to be restarted in order for these changes to take effect. It is recommended to restart the SNMP master agent once all the configuration changes are completed.

Restarting SNMP Master Agent also restarts the Host Resources Agent if it is running.

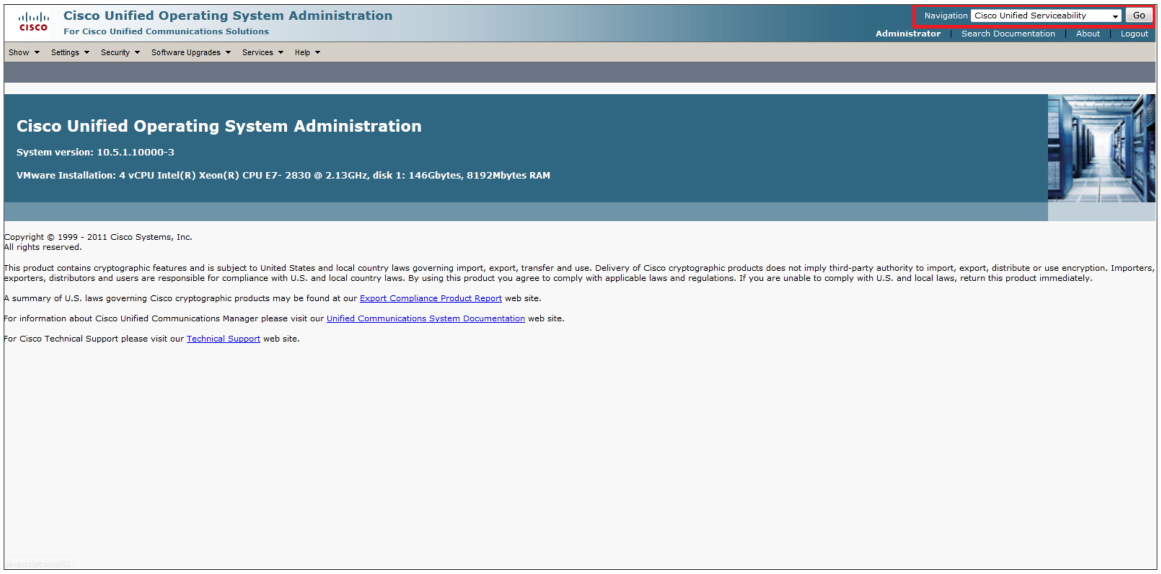
Master agent restart will take around 1min..

Press OK to restart the SNMP master agent now or Cancel to restart later.

Enabling SNMP in Cisco Finesse Server

To enable SNMP in Cisco Finesse Server, perform the following steps:

1. Log in to Cisco Unified Operating System Administration as an administrator.
2. In the top-right corner of the page, in the ***Navigation*** field, select *Cisco Unified Serviceability* and then click **[Go]**.



Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Navigation
Cisco Unified Serviceability
Go
Administrator
Search Documentation
About
Logout
Show
Settings
Security
Software Upgrades
Services
Help

Cisco Unified Operating System Administration

System version: 10.5.1.10000-3

VMware Installation: 4 vCPU Intel(R) Xeon(R) CPU E7- 2830 @ 2.13GHz, disk 1: 146Gbytes, 8192Mbytes RAM

Copyright © 1999 - 2011 Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

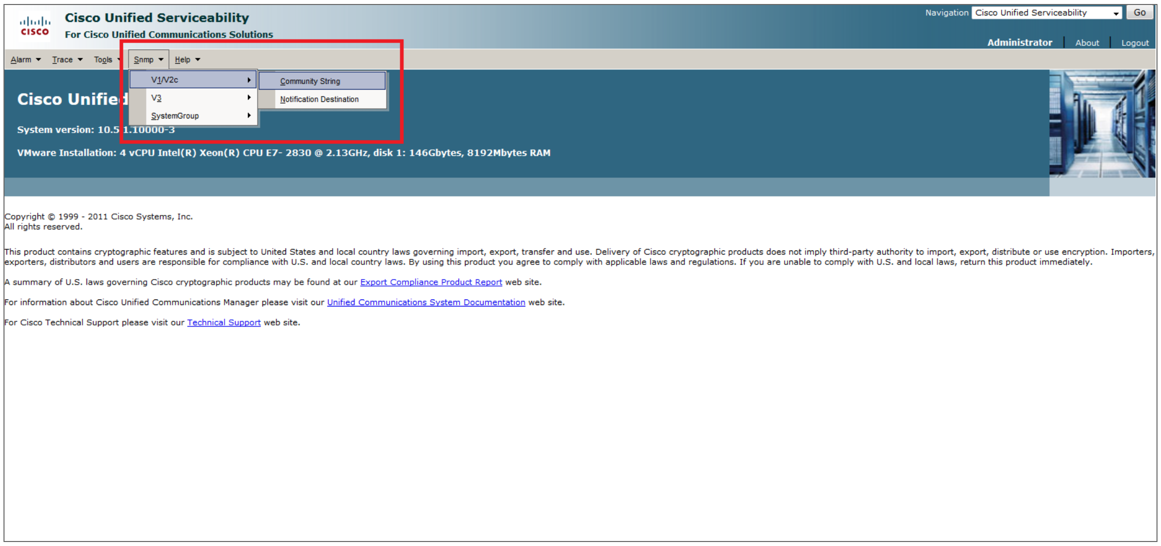
A summary of U.S. laws governing Cisco cryptographic products may be found at our Export Compliance Product Report web site.

For information about Cisco Unified Communications Manager please visit our Unified Communications System Documentation web site.

For Cisco Technical Support please visit our Technical Support web site.

NOTE: You might be required to enter your login credentials again before proceeding.

3. Click the **[SNMP]** tab, then select *V1/V2c > Community String*.



System version: 10.5 1.10000-3

VMware Installation: 4 vCPU Intel(R) Xeon(R) CPU E7- 2830 @ 2.13GHz, disk 1: 146Gbytes, 8192Mbytes RAM

Copyright © 1999 - 2011 Cisco Systems, Inc.
All rights reserved.

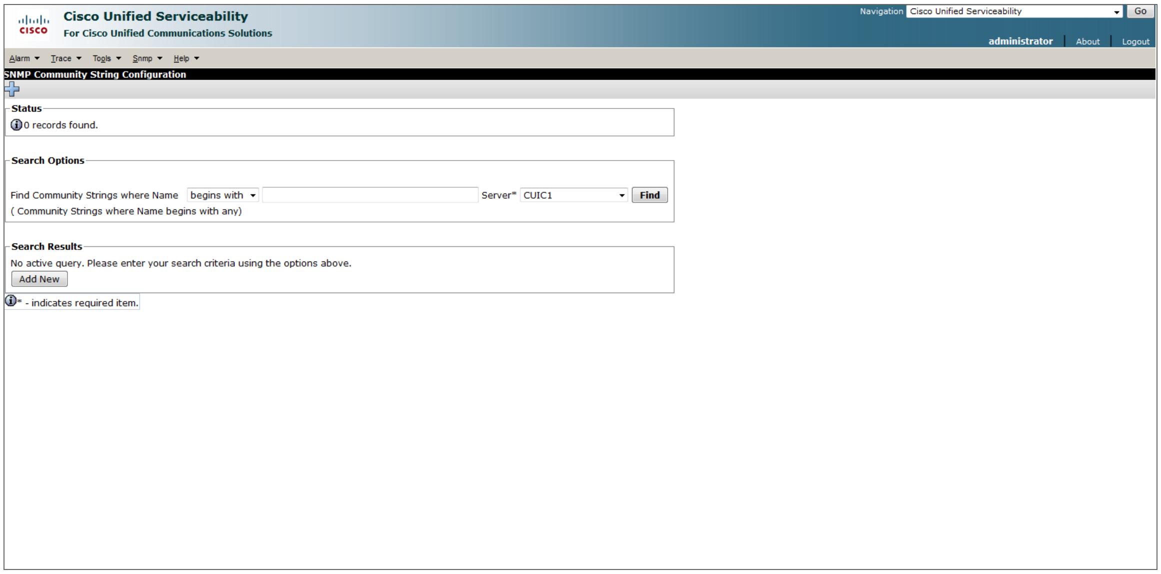
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our Export Compliance Product Report web site.

For information about Cisco Unified Communications Manager please visit our Unified Communications System Documentation web site.

For Cisco Technical Support please visit our Technical Support web site.

4. On the **SNMP Community String Configuration** page, under **Search Options**, click **[Find]**. The **Search Results** section appears.


Cisco Unified Serviceability
For Cisco Unified Communications Solutions
Navigation
Cisco Unified Serviceability
Go
administrator
About
Logout
Alarm
Trace
Tools
Snmp
Help
Find
Add New

SNMP Community String Configuration

Status

0 records found.

Search Options

Find Community Strings where Name begins with Server* CUIC1
(Community Strings where Name begins with any)

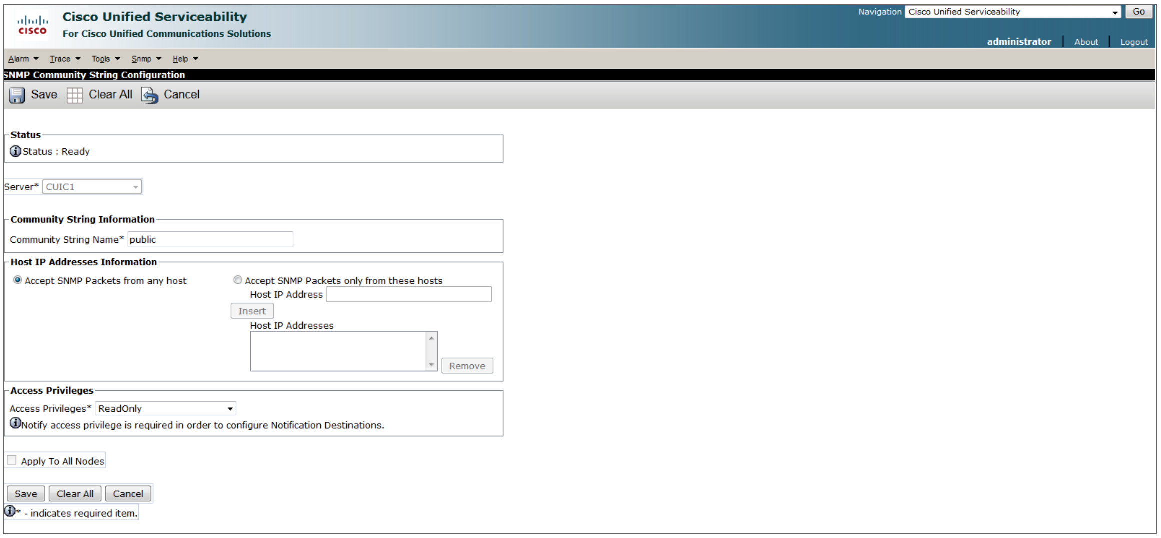
Search Results

No active query. Please enter your search criteria using the options above.

* - indicates required item.

5. Under **Search Results**, click **[Add New]**.

6. Enter values in the following fields:


Cisco Unified Serviceability
For Cisco Unified Communications Solutions
Navigation Cisco Unified Serviceability
Go
administrator
About
Logout
Alarm
Trace
Tools
Snmp
Help
Save
Clear All
Cancel
Insert
Remove
Save
Clear All
Cancel

SNMP Community String Configuration

Status

Status : Ready

Server* CUIC1

Community String Information

Community String Name* public

Host IP Addresses Information

● Accept SNMP Packets from any host

○ Accept SNMP Packets only from these hosts

Host IP Address

Host IP Addresses

Access Privileges

Access Privileges* ReadOnly

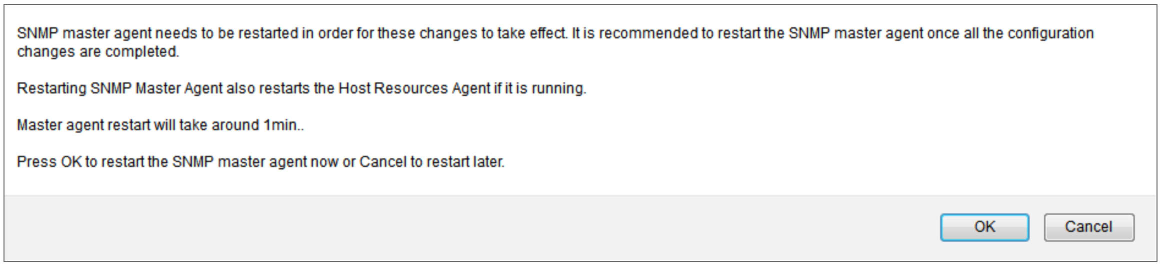
Notify access privilege is required in order to configure Notification Destinations.

□ Apply To All Nodes

* - indicates required item.

- ***Community String Name***. Enter a name for the new community string.
- ***Access Privileges***. Select *ReadOnly*.
- For the other fields on the page, use the default values.

7. Click **[Save]**.
8. Click **[OK]** to restart the SNMP master agent.



SNMP master agent needs to be restarted in order for these changes to take effect. It is recommended to restart the SNMP master agent once all the configuration changes are completed.

Restarting SNMP Master Agent also restarts the Host Resources Agent if it is running.

Master agent restart will take around 1min..

Press OK to restart the SNMP master agent now or Cancel to restart later.

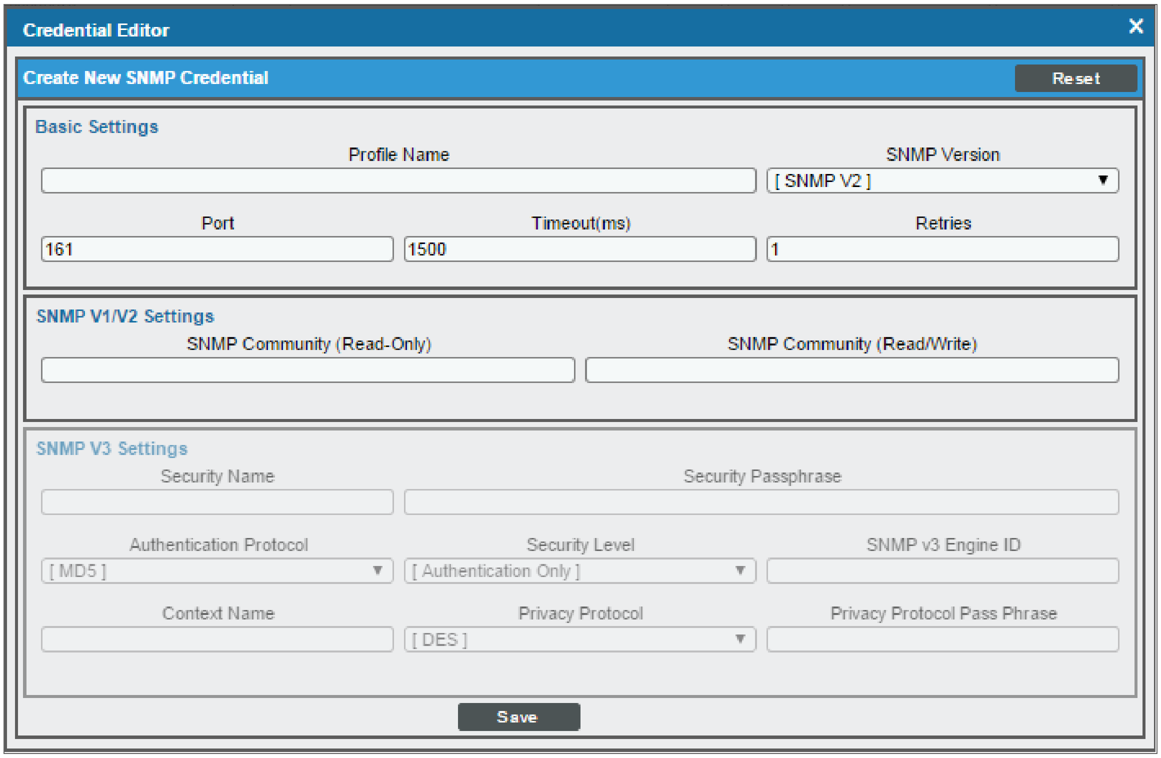
Creating an SNMP Credential for Unified Contact Center Enterprise

To configure SL1 to monitor Cisco Unified Contact Center Enterprise (UCCE), you must create an SNMP credential. This credential allows the Dynamic Applications in the *Cisco: Contact Center Enterprise* PowerPack to communicate with your UCCE account.

To configure an SNMP credential for UCCE:

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:



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:

4. In the ***Profile Name*** field, enter a name for the credential.
5. In the ***SNMP Version*** field, select *SNMP V2*.
6. In the ***SNMP Community (Read Only)*** field, enter the community string for the UCCE services.
7. Optionally, supply values in the other fields in this page. In most cases, you can use the default values for the other fields.
8. Click the **[Save]** button.

Compiling SNMP MIBs for Unified Contact Center Enterprise

You must manually compile some of the Management Information Base (MIB) files that are required for monitoring Cisco Unified Contact Center Enterprise in SL1. To compile these MIBs, perform the following steps:

1. Go to the **MIB Compiler** page (System > Tools > MIB Compiler).
2. Locate the CISCO-CONTACT-CENTER-APPS-MIB and then click its lightning bolt icon (⚡).
3. Repeat step 2 for the CISCO-CUICAPPS-MIB and the CISCO-CVP-MIB.

> **NOTE:** The MIB Compiler page displays "Yes" in the Compiled column for the MIBs before these steps are completed. However, you must still compile the MIBs manually using the lightning bolt icon (⚡).

If the message "MIB File Missing" appears when you click the lightning bolt icon (⚡), you must download and import the MIB(s) before compiling them. To do so:

1. Download the MIB(s) you need:
   - CISCO-CONTACT-CENTER-APPS-MIB: ftp://ftp.cisco.com/pub/mibs/v2/CISCO-CONTACT-CENTER-APPS-MIB.my
   - CISCO-CUICAPPS-MIB: ftp://ftp.cisco.com/pub/mibs/v2/CISCO-CUICAPPS-MIB.my
   - CISCO-CVP-MIB: ftp://ftp.cisco.com/pub/mibs/v2/CISCO-CVP-MIB.my
2. Go to the **MIB Compiler** page (System > Tools > MIB Compiler).
3. Click the **[Import]** button.
4. Click the **[Browse]** button to locate the downloaded MIB. Select the MIB, and then click the **[Import]** button.
5. Click **[OK]** to confirm.
6. On the **MIB Compiler** page, locate the imported MIB and click its lightning bolt icon (⚡) to compile it.
7. If you downloaded more than one MIB, repeat steps 2-6 for the additional MIB(s) that need to be imported and compiled.

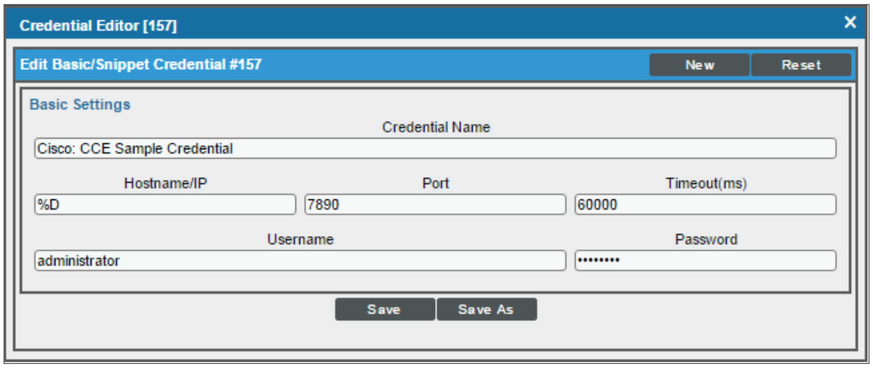
Configuring Unified Contact Center Enterprise Monitoring Using REST API

Some Dynamic Applications in the *Cisco: Contact Center Enterprise* PowerPack collect data from Cisco Unified Contact Center Enterprise (UCCE) using the UCCE REST API. These Dynamic Applications require a Basic/Snippet credential to enable SL1 to communicate with your UCCE account. An example Basic/Snippet credential that you can edit for your own use is included in the *Cisco: Contact Center Enterprise* PowerPack.

To create a Basic/Snippet credential to monitor UCCE:

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

3. Enter values in the following fields:



Credential Name: Cisco: CCE Sample Credential
Hostname/IP: %D
Port: 7890
Timeout(ms): 60000
Username: administrator
Password: ••••••••

- ***Credential Name***. Enter a new name for the credential.
- ***Hostname/IP***. Enter "%D".
- ***Port***. Enter "7890".
- ***Timeout***. Enter "60000".
- ***Username***. Enter the username for a user with administrator access to the UCCE system.
- ***Password***. Enter the password for the UCCE administrator account.

4. Click the **[Save As]** button.
5. When the confirmation message appears, click **[OK]**.

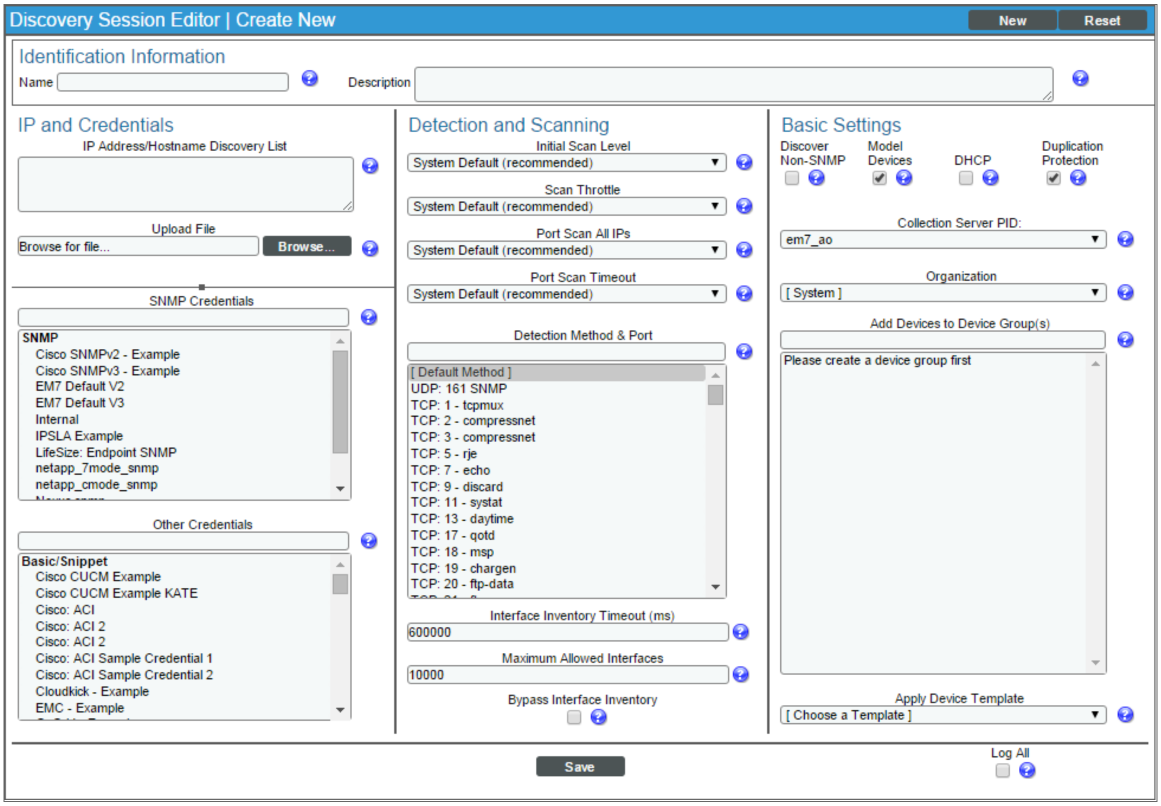
Discovering Component Devices in Cisco Unified Contact Center Enterprise

When you discover your Cisco Unified Contact Center Enterprise (UCCE) instance with SL1, SL1 auto-aligns a series of Dynamic Applications to discover, configure, and monitor UCCE, Customer Voice Portal (CVP), Cisco Unified Intelligence Center (CUIC), and/or Finesse services, and all the associated component devices.

To discover your UCCE instance, perform the following steps:

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

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



Discovery Session Editor | Create New

Identification Information

Name:

Description:

IP and Credentials

IP Address/Hostname Discovery List:

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

SNMP Credentials:

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

Other Credentials:

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

Detection and Scanning

Initial Scan Level: System Default (recommended)

Scan Throttle: System Default (recommended)

Port Scan All IPs: System Default (recommended)

Port Scan Timeout: System Default (recommended)

Detection Method & Port:

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

Interface Inventory Timeout (ms): 600000

Maximum Allowed Interfaces: 10000

Bypass Interface Inventory ☐

Basic Settings

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

Collection Server PID: em7_ao

Organization: [System]

Add Devices to Device Group(s): Please create a device group first

Apply Device Template: [Choose a Template]

Log All ☐

3. Supply values in the following fields:

   - ***IP Address/Hostname Discovery List***. Enter the IP address(es) or the range of IP addresses for the UCCE, CVP, CUIC, and/or Finesse services you want to discover.
   - ***SNMP Credentials***. Select the *SNMP credential you created*.
   - ***Other Credentials***. Select the *Basic/Snippet credential you created*.

4. Optionally, supply values in the other fields in this page. For a description of the fields in this page, see the ***Discovery & Credentials*** manual.

5. Click the **[Save]** button.

6. The **Discovery Control Panel** page refreshes. Click the lightning bolt icon (⚡) for the discovery session you created.

7. In the pop-up window that appears, click the **[OK]** button. The **Discovery Session** page displays the progress of the discovery session.

Chapter 12

Cisco: Cloud Services Platform

Overview

The following sections describe how to configure and discover Cisco Cloud Services Platform (CSP) clusters for monitoring by SL1 using the *Cisco: Cloud Services Platform* PowerPack:

> NOTE: For more information about the *Cisco: Cloud Services Platform* PowerPack, see the ***Monitoring Cisco Cloud Services Platform 2100*** manual.

Prerequisites for Monitoring CSP Clusters

To configure the SL1 system to monitor CSP clusters using the *Cisco: Cloud Services Platform* PowerPack, you must have the following information about the clusters that you want to monitor:

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

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

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

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

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

Creating SNMP Credentials for CSP Clusters

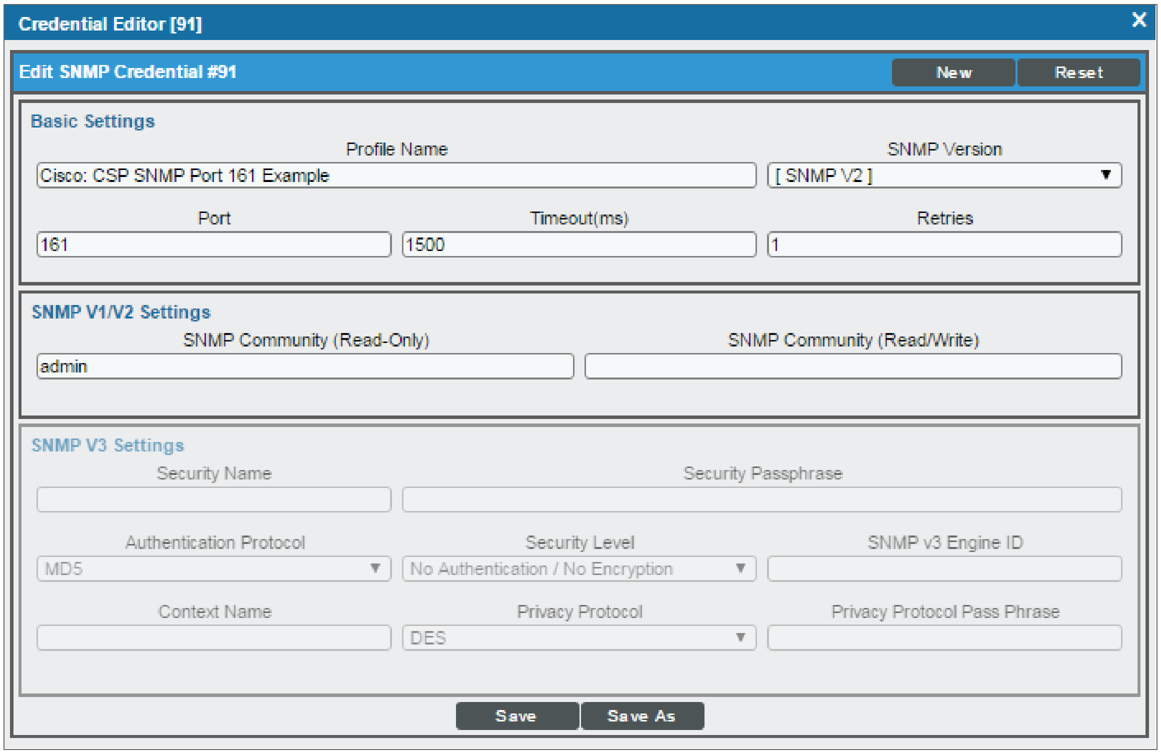
Before you can discover and monitor Cloud Services Platform (CSP) clusters in SL1, you must first create two SNMP credentials (one for port 161 and another for port 1610) in SL1. These credentials, along with a ***Basic/Snippet credential*** and ***SSH/Key credential*** that you must also create, enable SL1 to collect data from the clusters. Two example SNMP credentials that you can edit for your own use are included in the *Cisco: Cloud Services Platform* PowerPack.

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

To configure the port 161 SNMP credential for CSP:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **Cisco: CSP SNMP Port 161 Example** credential, then click its wrench icon (🔧). The **Edit SNMP Credential** modal page appears.

3. Make entries in the following fields:



Credential Editor [91]

Edit SNMP Credential #91

Basic Settings

Profile Name: Cisco: CSP SNMP Port 161 Example

SNMP Version: [SNMP V2]

Port: 161

Timeout(ms): 1500

Retries: 1

SNMP V1/V2 Settings

SNMP Community (Read-Only): admin

SNMP Community (Read/Write):

SNMP V3 Settings

Security Name:

Security Passphrase:

Authentication Protocol: MD5

Security Level: No Authentication / No Encryption

SNMP v3 Engine ID:

Context Name:

Privacy Protocol: DES

Privacy Protocol Pass Phrase:

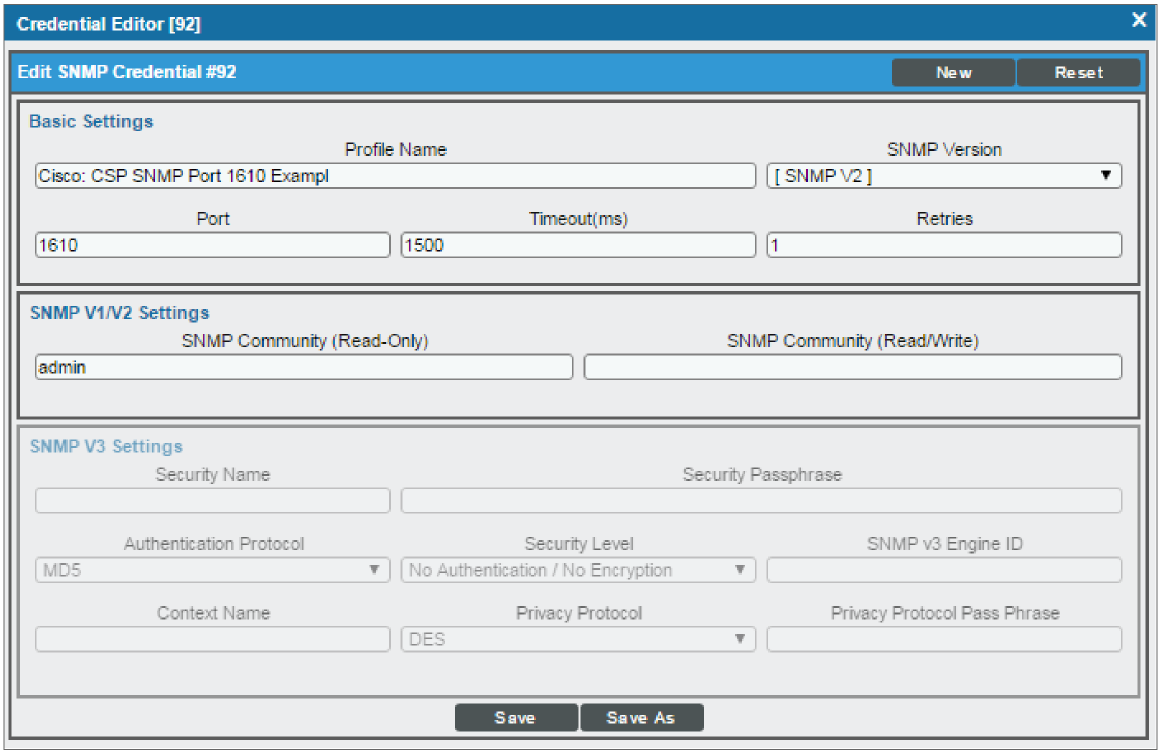
- ***Profile Name***. Enter a new name for the credential.
- ***SNMP Community (Read Only)***. Enter the port 161 community string for the CSP cluster.

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

To configure the port 1610 SNMP credential for CSP:

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

3. Make entries in the following fields:



Basic Settings

Profile Name: Cisco: CSP SNMP Port 1610 Exampl

SNMP Version: [SNMP V2]

Port: 1610

Timeout(ms): 1500

Retries: 1

SNMP V1/V2 Settings

SNMP Community (Read-Only): admin

SNMP Community (Read/Write):

SNMP V3 Settings

Security Name:

Security Passphrase:

Authentication Protocol: MD5

Security Level: No Authentication / No Encryption

SNMP v3 Engine ID:

Context Name:

Privacy Protocol: DES

Privacy Protocol Pass Phrase:

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

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

Creating a Basic/Snippet Credential for CSP Clusters

Some Dynamic Applications in the *Cisco: Cloud Services Platform* PowerPack collect data from CSP clusters using the REST API. These Dynamic Applications require a Basic/Snippet credential to enable SL1 to communicate with the cluster. An example Basic/Snippet credential that you can edit for your own use is included in the *Cisco: Cloud Services Platform* PowerPack.

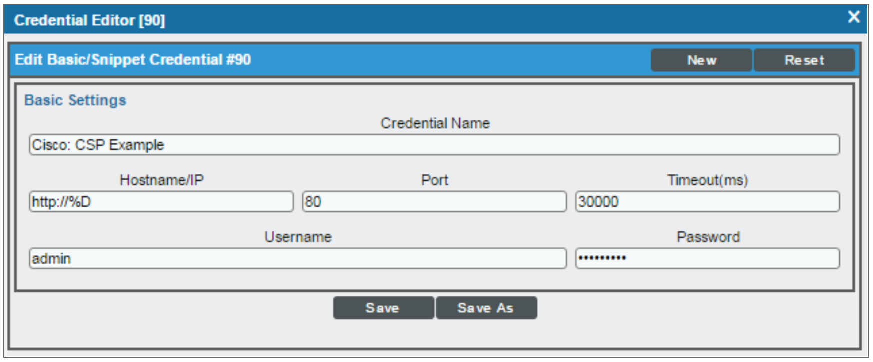
NOTE: For more information about the configuration required for the Basic/Snippet credential, see the ***Prerequisites*** section.

To create a Basic/Snippet credential to monitor CSP:

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

2. Locate the **Cisco: CSP Example** credential, and then click its wrench icon (🔧). The **Edit Basic/Snippet Credential** modal page appears.

3. Enter values in the following fields:



Credential Editor [90]

Edit Basic/Snippet Credential #90

Basic Settings

Credential Name: Cisco: CSP Example

Hostname/IP: http://%D

Port: 80

Timeout(ms): 30000

Username: admin

Password: •••••••••

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

4. Use the default values for the other fields on this page.

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

6. When the confirmation message appears, click **[OK]**.

Creating an SSH/Key Credential for CSP Clusters

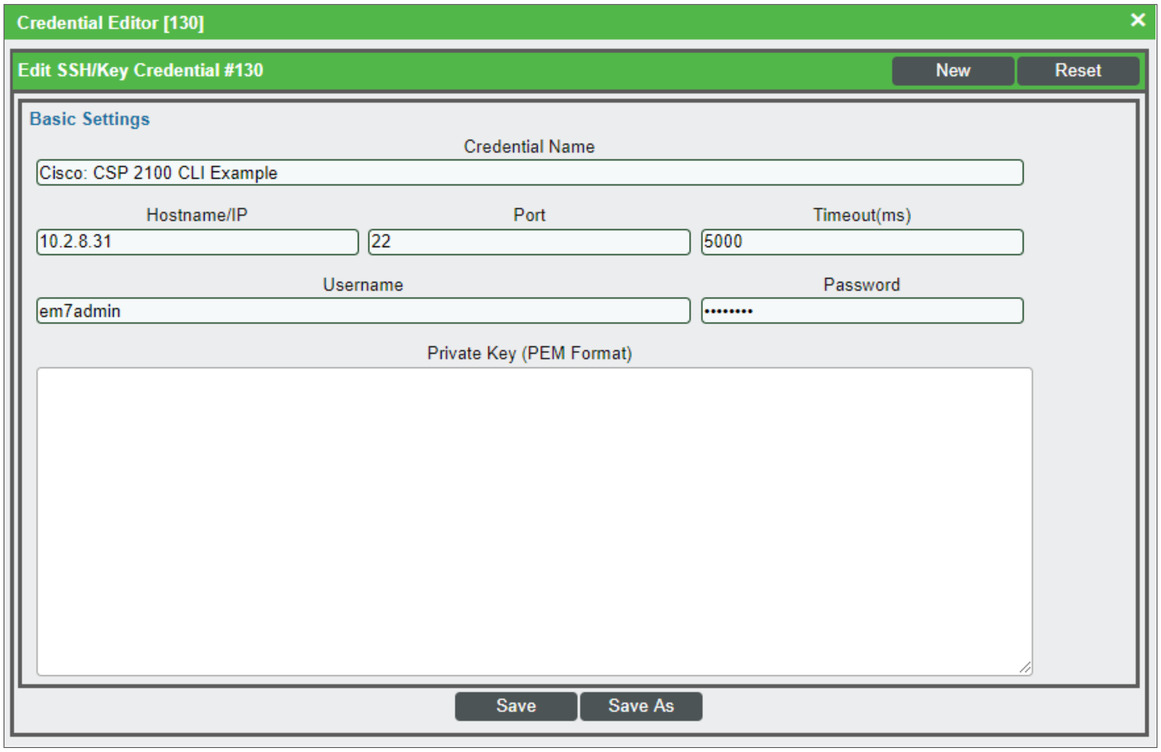
Some Dynamic Applications in the *Cisco: Cloud Services Platform* PowerPack collect data from CSP clusters from the command line interface instead of the API. These Dynamic Applications require an SSH/Key credential to enable SL1 to communicate with the cluster. An example SSH/Key credential that you can edit for your own use is included in the *Cisco: Cloud Services Platform* PowerPack.

> **NOTE:** This functionality utilizes MD5 password encryption. As such, it is not currently available for use in Federal Information Processing Standard (FIPS)-compliant installations of SL1. If you attempt to discover CSP cluster data using an SSH/Key credential in FIPS-compliant installations of SL1, the cluster component device will not be created and an exception error message appears in the system log.

To create an SSH/Key credential to monitor CSP:

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

2. Locate the **Cisco: CSP 2100 CLI Example** credential, and then click its wrench icon (🔧). The **Edit SSH/Key Credential** modal page appears.
3. Enter values in the following fields:



Credential Name: Cisco: CSP 2100 CLI Example

Hostname/IP: 10.2.8.31

Port: 22

Timeout(ms): 5000

Username: em7admin

Password: ••••••••

Private Key (PEM Format):

- ***Credential Name***. Type a new name for the credential.
- ***Hostname/IP***. Type the IP address or hostname of the CSP cluster you want to monitor.
- ***Port***. Type the SSH port number for the CSP cluster you want to monitor.
- ***Timeout(ms)***. Keep the default setting.
- ***Username***. Type the username for a user with administrator access to the CSP cluster command line interface.
- ***Password***. Type the user's password.
- ***Private Key (PEM Format)***. Keep this field blank.

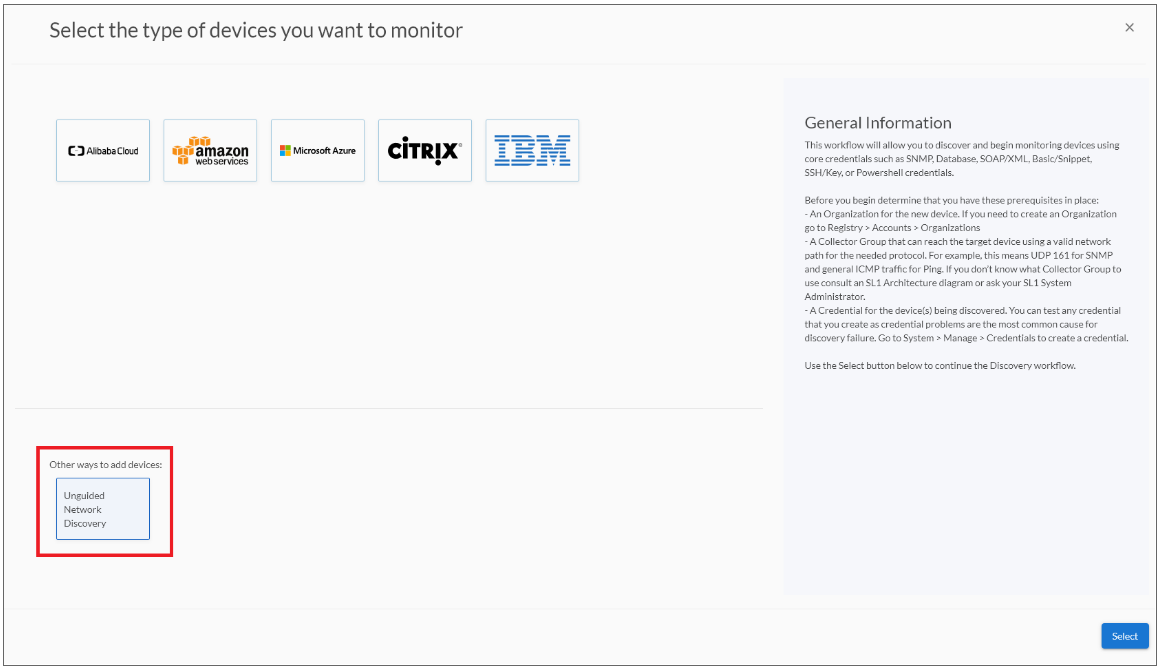
4. Click the **[Save As]** button.
5. When the confirmation message appears, click **[OK]**.

Discovering CSP Clusters

When you discover your Cloud Services Platform (CSP) cluster with SL1, SL1 auto-aligns a series of Dynamic Applications to discover, configure, and monitor the CSP cluster and all of its associated component devices.

To discover your CSP cluster, perform the following steps:

1. On the **Devices** page (🖥) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears:



Select the type of devices you want to monitor

General Information

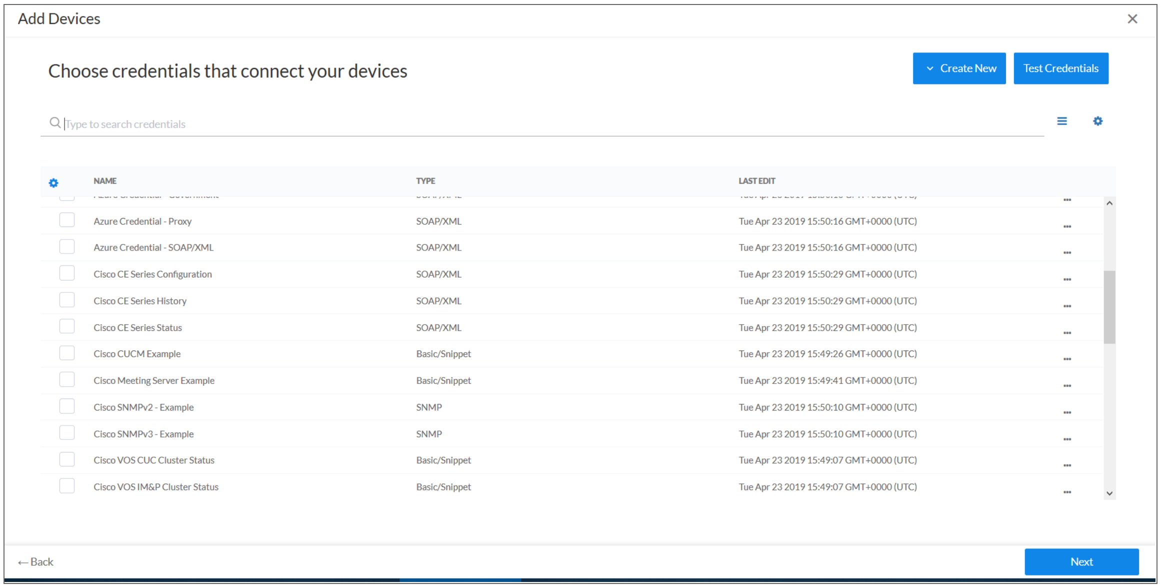
This workflow will allow you to discover and begin monitoring devices using core credentials such as SNMP, Database, SOAP/XML, Basic/Snippet, SSH/Key, or Powershell credentials.

Before you begin determine that you have these prerequisites in place:
- An Organization for the new device. If you need to create an Organization go to Registry > Accounts > Organizations
- A Collector Group that can reach the target device using a valid network path for the needed protocol. For example, this means UDP 161 for SNMP and general ICMP traffic for Ping. If you don't know what Collector Group to use consult an SL1 Architecture diagram or ask your SL1 System Administrator.
- A Credential for the device(s) being discovered. You can test any credential that you create as credential problems are the most common cause for discovery failure. Go to System > Manage > Credentials to create a credential.

Use the Select button below to continue the Discovery workflow.

2. Click the **[Unguided Network Discovery]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.
3. Click **[Select]**. The **Add Devices** page appears:
4. Complete the following fields:
   - ***Name***. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.
   - ***Description***. Optional. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **[Discovery Sessions]** tab.
   - ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered devices.

5. Click **[Next]**. The **Credentials** page of the **Add Devices** wizard appears:



Choose credentials that connect your devices

Type to search credentials

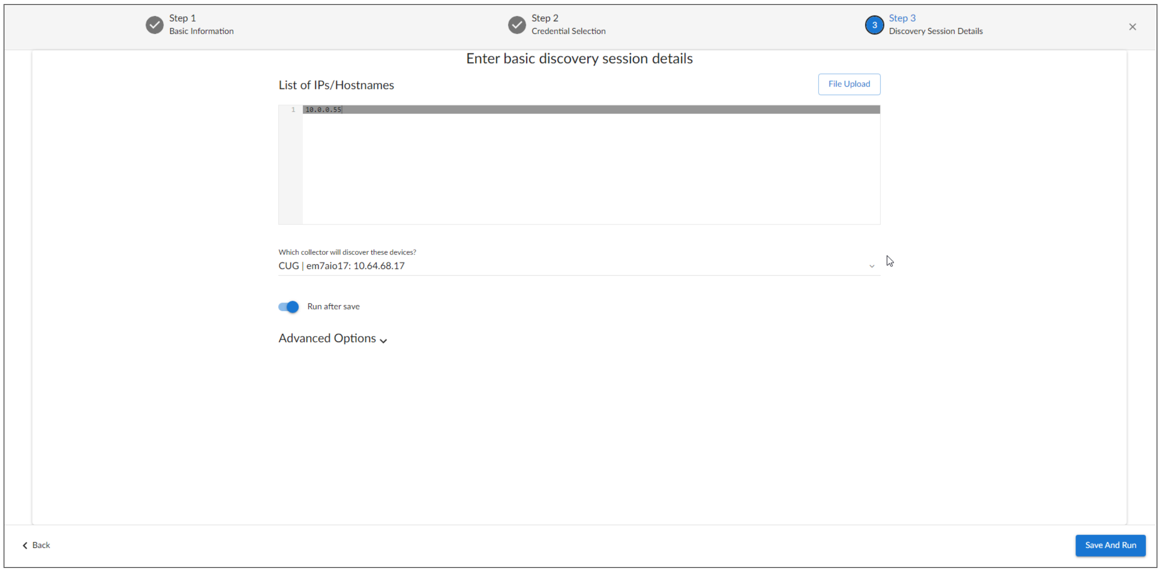
	NAME	TYPE	LAST EDIT	
☐	Azure Credential - Proxy	SOAP/XML	Tue Apr 23 2019 15:50:16 GMT+0000 (UTC)	...
☐	Azure Credential - SOAP/XML	SOAP/XML	Tue Apr 23 2019 15:50:16 GMT+0000 (UTC)	...
☐	Cisco CE Series Configuration	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)	...
☐	Cisco CE Series History	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)	...
☐	Cisco CE Series Status	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)	...
☐	Cisco CUCM Example	Basic/Snippet	Tue Apr 23 2019 15:49:26 GMT+0000 (UTC)	...
☐	Cisco Meeting Server Example	Basic/Snippet	Tue Apr 23 2019 15:49:41 GMT+0000 (UTC)	...
☐	Cisco SNMPv2 - Example	SNMP	Tue Apr 23 2019 15:50:10 GMT+0000 (UTC)	...
☐	Cisco SNMPv3 - Example	SNMP	Tue Apr 23 2019 15:50:10 GMT+0000 (UTC)	...
☐	Cisco VOS CUC Cluster Status	Basic/Snippet	Tue Apr 23 2019 15:49:07 GMT+0000 (UTC)	...
☐	Cisco VOS IM&P Cluster Status	Basic/Snippet	Tue Apr 23 2019 15:49:07 GMT+0000 (UTC)	...

6. On the **Credentials** page, locate and select the two SNMP credentials that you created (one for port 161 and the other for port 1610), and the Basic/Snippet credential and the SSH/Key credential for each of the CSP nodes you want to discover.

> NOTE: You must include a minimum of three credentials (one SNMP credential and two Basic/Snippet credentials) for each CSP node with unique credential information.

> NOTE: If you are running a Federal Information Processing Standard (FIPS)-compliant installations of the SL1 platform, then you should **not** select an SSH/Key credential.

7. Click **[Next]**. The **Discovery Session Details** page of the **Add Devices** wizard appears:



Enter basic discovery session details

List of IPs/Hostnames

```
10.0.0.55
```

Which collector will discover these devices?
CUG | em7aio17: 10.64.68.17

● Run after save

Advanced Options ⌄

8. Complete the following fields:

   - ***List of IPs/Hostnames***. Type the IP address of each CSP node you want to discover.
   - ***Which collector will monitor these devices?***. Select an existing collector to monitor the discovered devices. Required.
   - ***Run after save***. Select this option to run this discovery session as soon as you click **[Save and Close]**.

     In the **Advanced options** section, click the down arrow icon (⌄) to complete the following fields:

     - ***Discover Non-SNMP***. Enable this setting.

9. Click **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.
10. If you selected the **Run after save** option on this page, the discovery session runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page includes a link to the **Device Investigator** page for the discovered device.

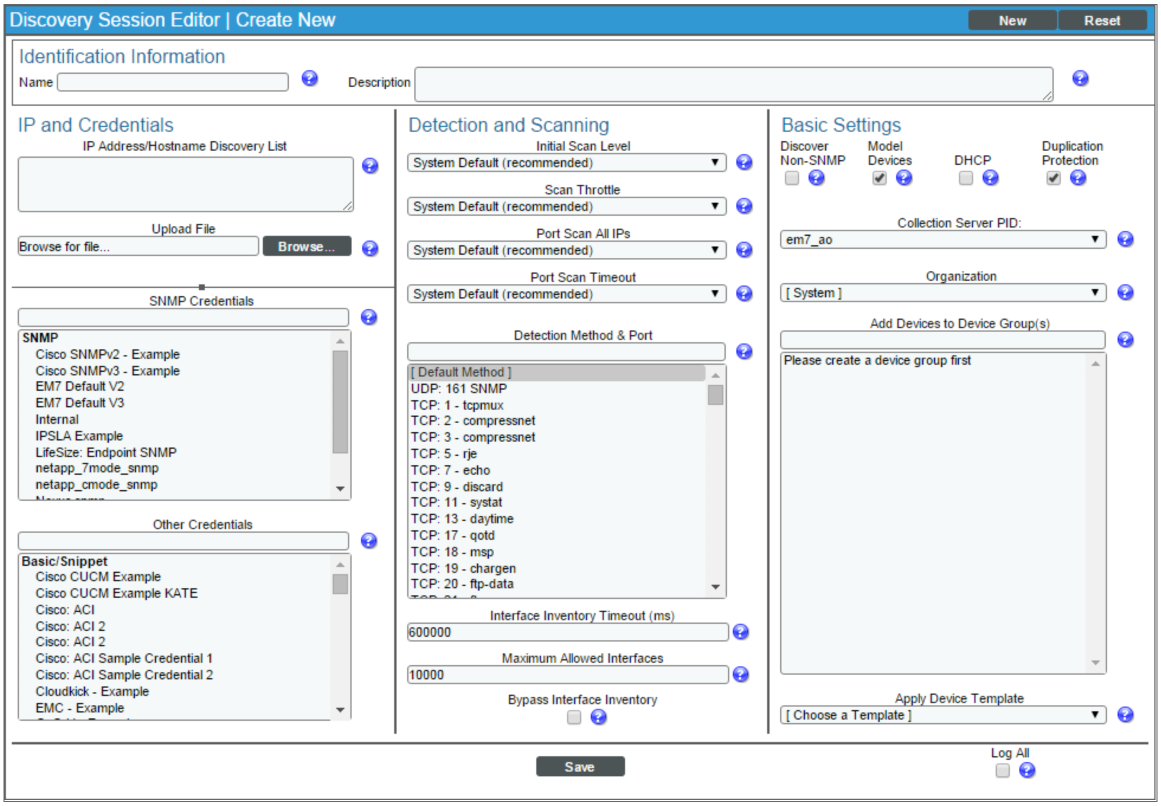
Discovering CSP Clusters in the SL1 Classic User Interface

When you discover your Cloud Services Platform (CSP) cluster with SL1, SL1 auto-aligns a series of Dynamic Applications to discover, configure, and monitor the CSP cluster and all of its associated component devices.

To discover your CSP cluster, perform the following steps:

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

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



Discovery Session Editor | Create New

New Reset

Identification Information

Name

Description

IP and Credentials

IP Address/Hostname Discovery List

Upload File

Browse for file... Browse...

SNMP Credentials

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

Other Credentials

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

Detection and Scanning

Initial Scan Level: System Default (recommended)

Scan Throttle: System Default (recommended)

Port Scan All IPs: System Default (recommended)

Port Scan Timeout: System Default (recommended)

Detection Method & Port

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

Interface Inventory Timeout (ms): 600000

Maximum Allowed Interfaces: 10000

Bypass Interface Inventory □

Basic Settings

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

Collection Server PID: em7_ao

Organization: [System]

Add Devices to Device Group(s): Please create a device group first

Apply Device Template: [Choose a Template]

Save

Log All □

3. Supply values in the following fields:

- ***IP Address/Hostname Discovery List***. Enter the IP address of each CSP node you want to discover.
- ***SNMP Credentials***. Select the two SNMP credentials that you created (one for port 161 and the other for port 1610) for each of the CSP nodes you want to discover.
- ***Other Credentials***. Select the Basic/Snippet credential and the SSH/Key credential for each of the CSP nodes you want to discover.
- ***Discover Non-SNMP***. Select this checkbox.

NOTE: You must include a minimum of three credentials (one SNMP credential and two Basic/Snippet credentials) for each CSP node with unique credential information.

NOTE: If you are running a Federal Information Processing Standard (FIPS)-compliant installations of the ScienceLogic platform, then you should not select an SSH/Key credential in the ***Other Credentials*** field.

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

Relationships Between Component Devices

In addition to parent/child relationships between component devices, SL1 also creates relationships between CSP-2100 nodes and Cisco UCS Standalone servers.

Chapter 13

Cisco: CUCM Unified Communications Manager

Overview

The following sections describe how to configure and discover a Cisco Unified Communications Manager (CM) system for monitoring by SL1 using the *Cisco: CUCM Unified Communications Manager* PowerPack:

NOTE: For more information about the *Cisco: CUCM Unified Communications Manager* PowerPack, see the ***Monitoring Cisco Unified Communications Manager*** manual.

Prerequisites for Monitoring CUCM

During the discovery process, SL1 automatically aligns the IP addresses and hostnames for each node in a Cisco Unified CM cluster via DNS.

If you do not have access to DNS for the Cisco Unified CM systems that you want to monitor with SL1, ensure that you know or have access to the following information about each node:

- IP address
- Hostname

Configuring the ScienceLogic Platform to Monitor CUCM

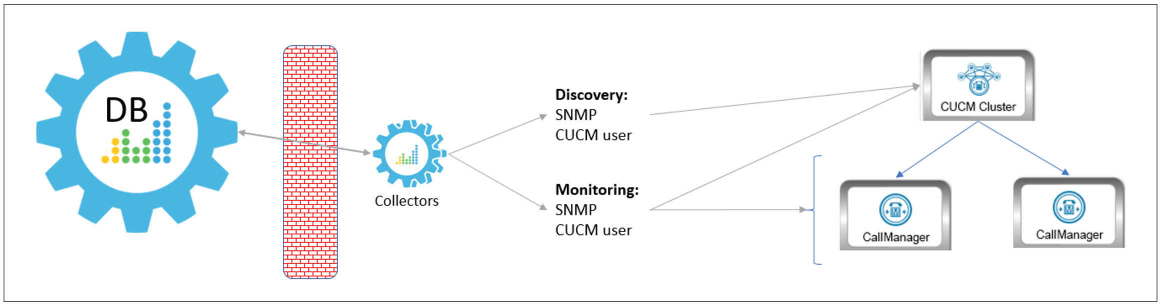
You can choose from several different possible configurations when using SL1 to monitor Cisco Unified CM:

- You can have the ScienceLogic Data Collector either in front of a firewall or behind a firewall.
- You can define the CallManager nodes either by hostname or by IP address in the Cisco Unified CM database.
- In some scenarios, you can also use network address translation (NAT) when defining the CallManagers.

These various methods are described in this section.

Method 1

In the first scenario, the Data Collector sits in front of the firewall and you define the CallManagers by hostname:

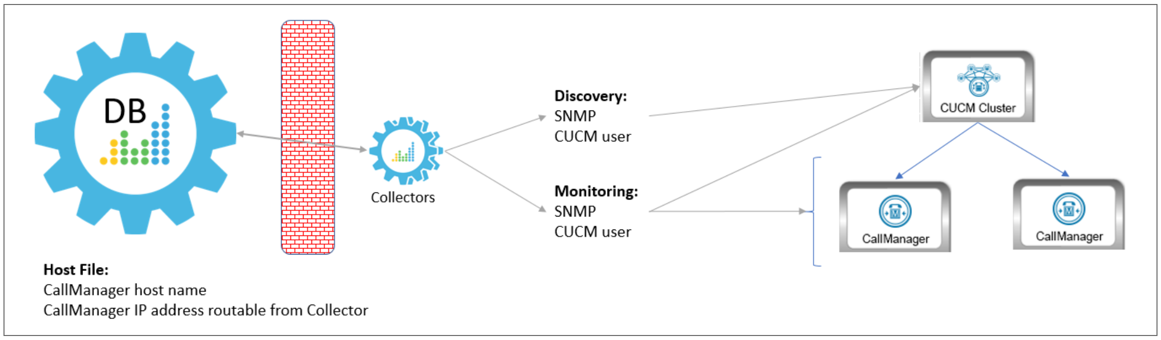


In this scenario, you must have the following ports open for the firewall:

Direction	Port	Protocol
ScienceLogic Database Server to the Data Collector	7707	TCP
PhoneHome Collector to the Database Server	7705	TCP

Method 2

In the second scenario, the Data Collector sits in front of the firewall and you define the CallManagers by IP address. This method requires you to ***create a host file*** that includes the CallManager hostname and IP address:

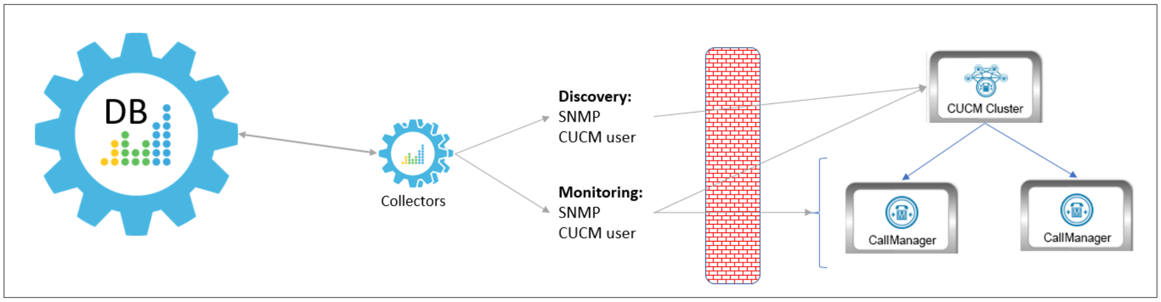


In this scenario, you must have the following ports open for the firewall:

Direction	Port	Protocol
ScienceLogic Database Server to the Data Collector	7707	TCP
PhoneHome Collector to the Database Server	7705	TCP

Method 3

In the third scenario, the Data Collector sits behind the firewall and you define the CallManagers by hostname:

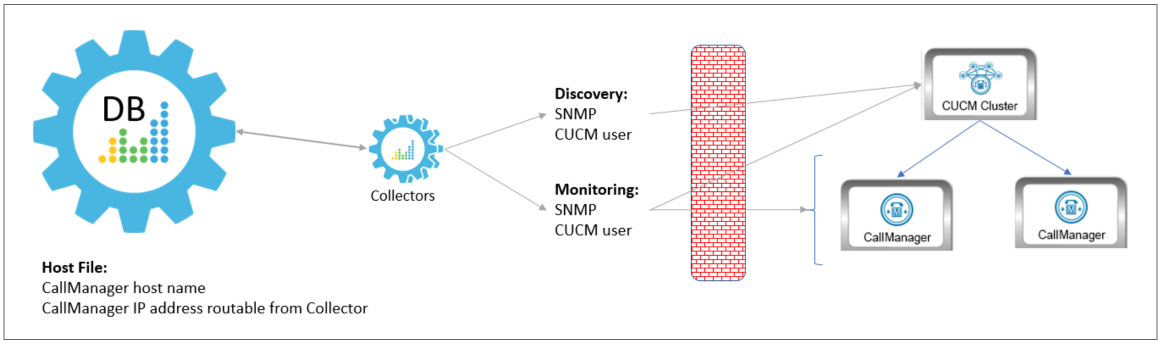


In this scenario, you must have the following ports open for the firewall:

Direction	Credential	Port	Protocol
ScienceLogic Data Collector to the Cisco Unified CM Cluster and CallManagers	SNMP	161	UDP
	Cisco Unified CM user	8443	TCP

Method 4

In the fourth scenario, the Data Collector sits behind the firewall and you define the CallManagers by hostname, with NAT. This method requires you to ***create a host file*** that includes the CallManager hostname and the IP address the Data Collector can use to access the device:

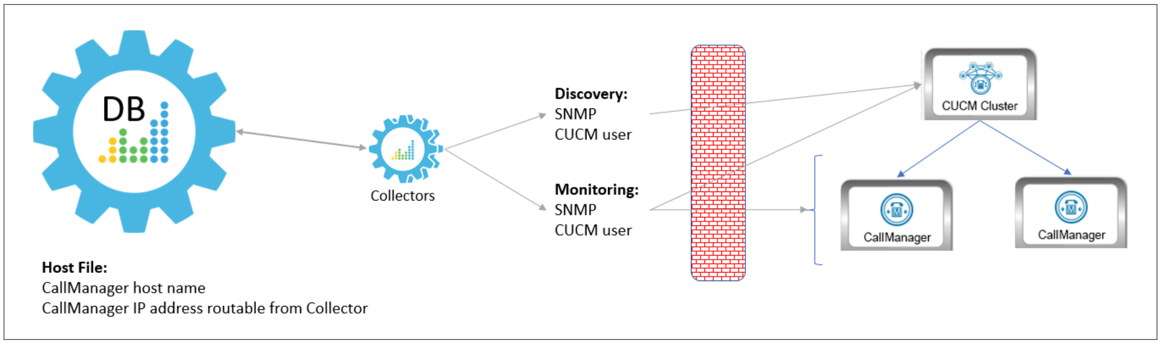


In this scenario, you must have the following ports open for the firewall:

Direction	Credential	Port	Protocol
ScienceLogic Data Collector to the Cisco Unified CM Cluster and CallManagers	SNMP	161	UDP
	Cisco Unified CM user	8443	TCP

Method 5

In the final scenario, the Data Collector sits behind the firewall and you define the CallManagers by IP address, with NAT. This method requires you to ***create a host file*** that includes the CallManager host name and IP address the Data Collector can use to access the device:



> **NOTE:** This method is not supported by versions of the *Cisco: CUCM Unified Communications Manager* PowerPack prior to version 109.

In this scenario, you must have the following ports open for the firewall:

Direction	Credential	Port	Protocol
ScienceLogic Data Collector to the Cisco Unified CM Cluster and CallManagers	SNMP	161	UDP
	Cisco Unified CM user	8443	TCP

Enabling the CUCM AXL Web Service

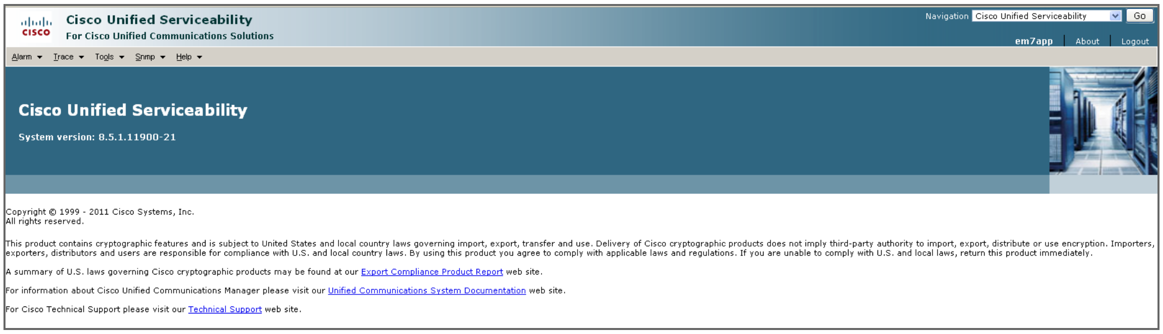
SL1 can monitor a Cisco Unified CM system by requesting detailed information about the system from the Cisco Unified CM AXL Web Service.

The Cisco Unified CM AXL web service is disabled by default. To enable the AXL web service, perform the following steps:

1. In a browser window, navigate to the following address:

   ```
   https://ip-address-of-CM-system:8443/ccmadmin/showHome.do
   ```

2. Log in to the Cisco Unified CM Administration site as an administrator.
3. In the ***Navigation*** drop-down list at the top-right corner of the page, select *Cisco Unified Serviceability*, and then click the **[Go]** button. The **Cisco Unified Serviceability** page appears:


Cisco Unified Serviceability
For Cisco Unified Communications Solutions
Navigation
Cisco Unified Serviceability
Go
em7app
About
Logout
Alarm
Trace
Tools
Snmp
Help

Cisco Unified Serviceability

System version: 8.5.1.11900-21

Copyright © 1999 - 2011 Cisco Systems, Inc.
All rights reserved.

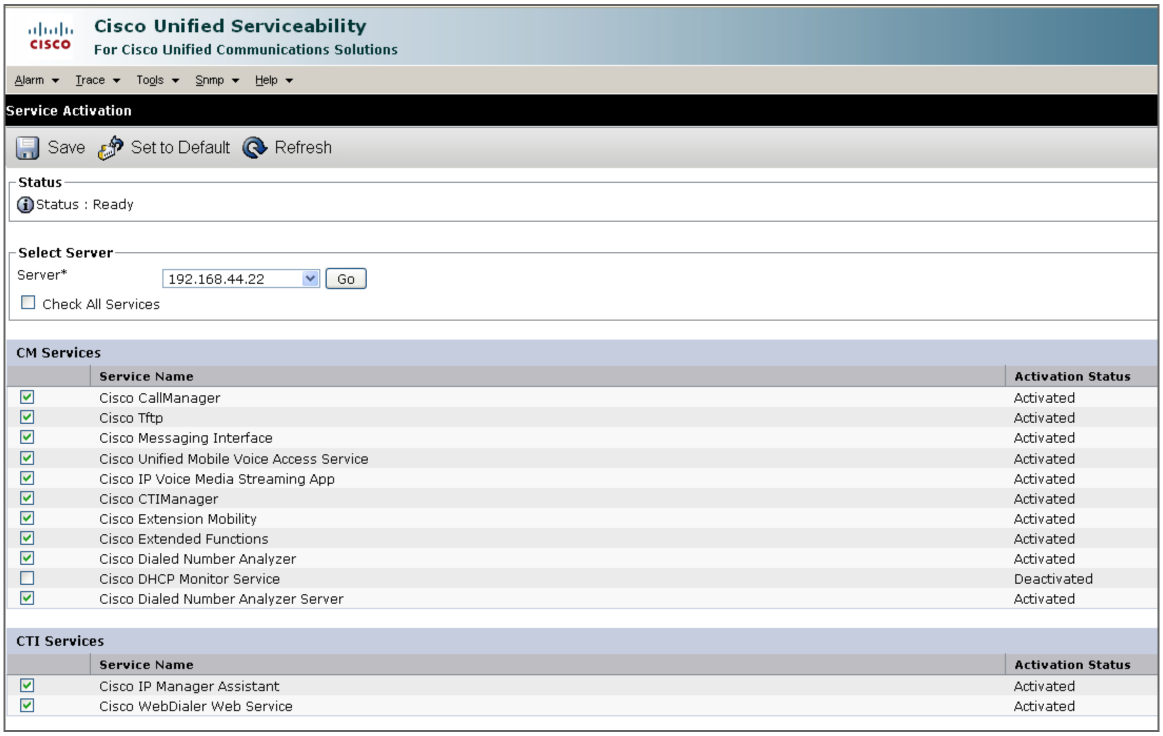
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our Export Compliance Product Report web site.

For information about Cisco Unified Communications Manager please visit our Unified Communications System Documentation web site.

For Cisco Technical Support please visit our Technical Support web site.

4. In the navigation bar at the top-left of the page, hover over ***Tools***, then select ***Service Activation***. The **Service Activation** page appears:


Cisco Unified Serviceability
For Cisco Unified Communications Solutions
Alarm
Trace
Tools
Snmp
Help
Service Activation
Save
Set to Default
Refresh

Status

Status : Ready

Select Server

Server* 192.168.44.22 Go

□ Check All Services

CM Services

	Service Name	Activation Status
☑	Cisco CallManager	Activated
☑	Cisco Tftp	Activated
☑	Cisco Messaging Interface	Activated
☑	Cisco Unified Mobile Voice Access Service	Activated
☑	Cisco IP Voice Media Streaming App	Activated
☑	Cisco CTIManager	Activated
☑	Cisco Extension Mobility	Activated
☑	Cisco Extended Functions	Activated
☑	Cisco Dialed Number Analyzer	Activated
□	Cisco DHCP Monitor Service	Deactivated
☑	Cisco Dialed Number Analyzer Server	Activated

CTI Services

	Service Name	Activation Status
☑	Cisco IP Manager Assistant	Activated
☑	Cisco WebDialer Web Service	Activated

5. In the ***Server*** drop-down list, select the Cisco Unified CM server for which you want to enable the AXL web service, and then click the **[Go]** button.

6. In the list of services, locate the **Database and Admin Services** section. If the *Activation Status* of the ***Cisco AXL Web Service*** is "Activated", the AXL web service is already enabled.

7. If the *Activation Status* of the ***Cisco AXL Web Service*** is not "Activated", select the checkbox for the **Cisco AXL Web Service**.

8. Click the **[Save]** button at the bottom of the page to save your changes, and then click the **[OK]** button in the pop-up window that appears.

Configuring a CUCM User Account

ScienceLogic recommends that you create a Cisco Unified CM user account that will be used only by SL1 to access the AXL web service. To create a user account in Cisco Unified CM that can access only the AXL web service, perform these two steps:

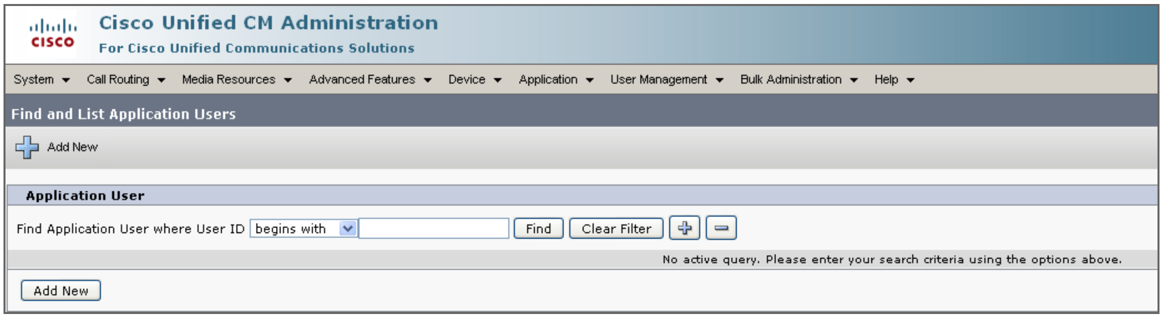
- Create a user account.
- Create a user group that includes the user account and has permission to access only the AXL web service.

To create a new Cisco Unified CM user group and user account, perform the following steps:

1. In a browser window, navigate to the following address:

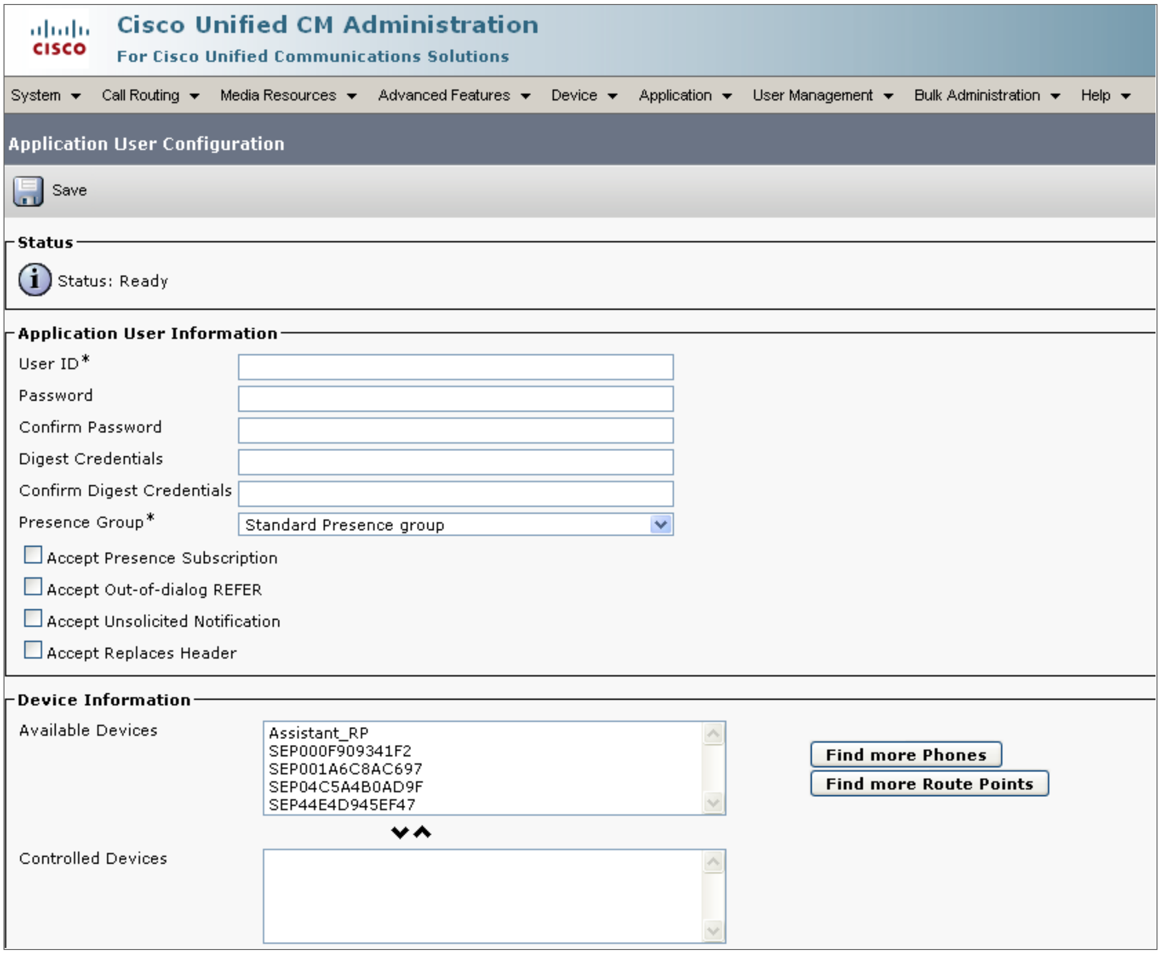
   `https://ip-address-of-CM-system:8443/ccmadmin/showHome.do`

2. Log in to the Cisco Unified CM Administration site as an administrator.
3. In the navigation bar at the top-left of the page, hover over ***User Management***, then select ***Application User***. The **Find and List Users** page appears:



No active query. Please enter your search criteria using the options above.

4. Click the **[+ Add New]** button. The **Application User Configuration** page appears:



Application User Configuration

Status

Status: Ready

Application User Information

User ID*

Password

Confirm Password

Digest Credentials

Confirm Digest Credentials

Presence Group* Standard Presence group

□ Accept Presence Subscription

□ Accept Out-of-dialog REFER

□ Accept Unsolicited Notification

□ Accept Replaces Header

Device Information

Available Devices

Assistant_RP
SEP000F909341F2
SEP001A6C8AC697
SEP04C5A4B0AD9F
SEP44E4D945EF47

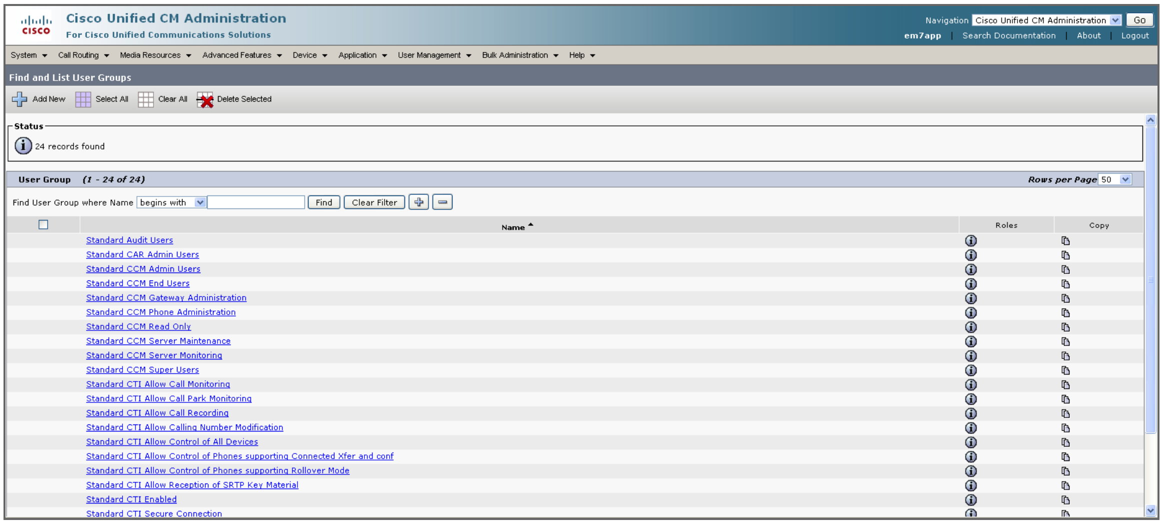
Controlled Devices

5. Supply values in the following fields:

- ***User ID***. Type a username for the new user.
- ***Password***. Type a password for the new user.
- ***Confirm Password***. Type the password for the new user again.

6. Click the **[Save]** button.

7. In the navigation bar at the top-left of the page, hover over ***User Management***, then select ***User Group***. The **Find and List User Groups** page appears:


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
em7app | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Add New Select All Clear All Delete Selected
Find User Group where Name begins with Find Clear Filter
Rows per Page 50

Find and List User Groups

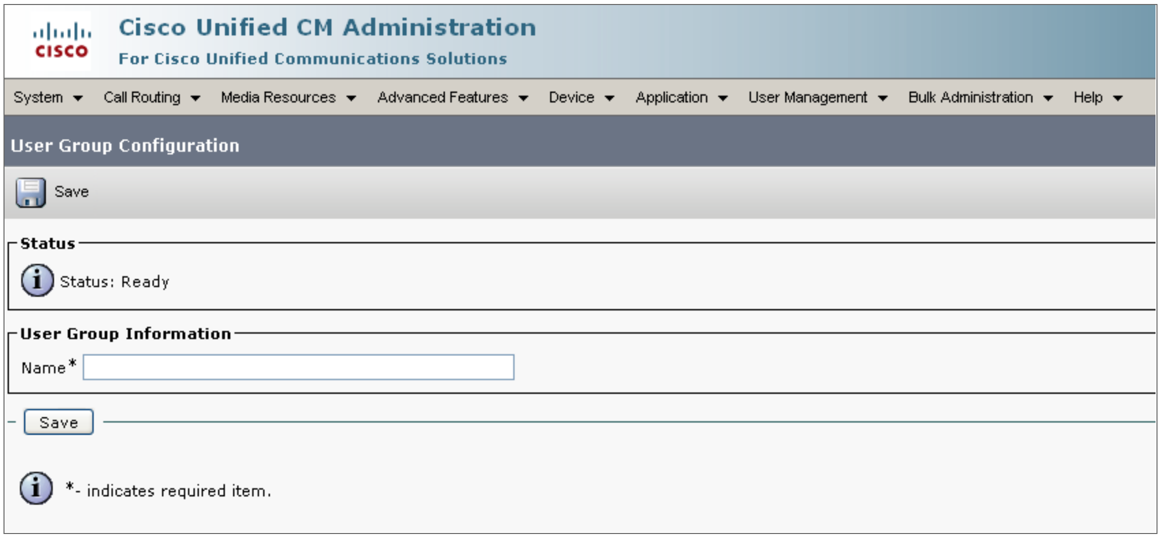
Status

24 records found

User Group (1 - 24 of 24)

□	Name ▲	Roles	Copy
	Standard Audit Users	ⓘ	⎘
	Standard CAR Admin Users	ⓘ	⎘
	Standard CCM Admin Users	ⓘ	⎘
	Standard CCM End Users	ⓘ	⎘
	Standard CCM Gateway Administration	ⓘ	⎘
	Standard CCM Phone Administration	ⓘ	⎘
	Standard CCM Read Only	ⓘ	⎘
	Standard CCM Server Maintenance	ⓘ	⎘
	Standard CCM Server Monitoring	ⓘ	⎘
	Standard CCM Super Users	ⓘ	⎘
	Standard CTI Allow Call Monitoring	ⓘ	⎘
	Standard CTI Allow Call Park Monitoring	ⓘ	⎘
	Standard CTI Allow Call Recording	ⓘ	⎘
	Standard CTI Allow Calling Number Modification	ⓘ	⎘
	Standard CTI Allow Control of All Devices	ⓘ	⎘
	Standard CTI Allow Control of Phones supporting Connected Xfer and conf	ⓘ	⎘
	Standard CTI Allow Control of Phones supporting Rollover Mode	ⓘ	⎘
	Standard CTI Allow Reception of SRTP Key Material	ⓘ	⎘
	Standard CTI Enabled	ⓘ	⎘
	Standard CTI Secure Connection	ⓘ	⎘

8. Click the **[+ Add New]** button. The **User Group Configuration** page appears:


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Save

User Group Configuration

Status

Status: Ready

User Group Information

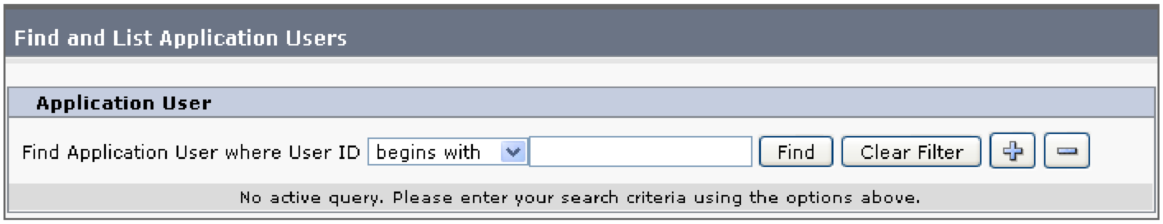
Name*

*- indicates required item.

9. In the ***Name*** field, type a name for the user group. For example, you could call the user group "AXL Access".

10. Click the **[Save]** button.

11. Click the **[Add App Users to Group]** button. The **Find and List Application Users** window appears:



Find and List Application Users

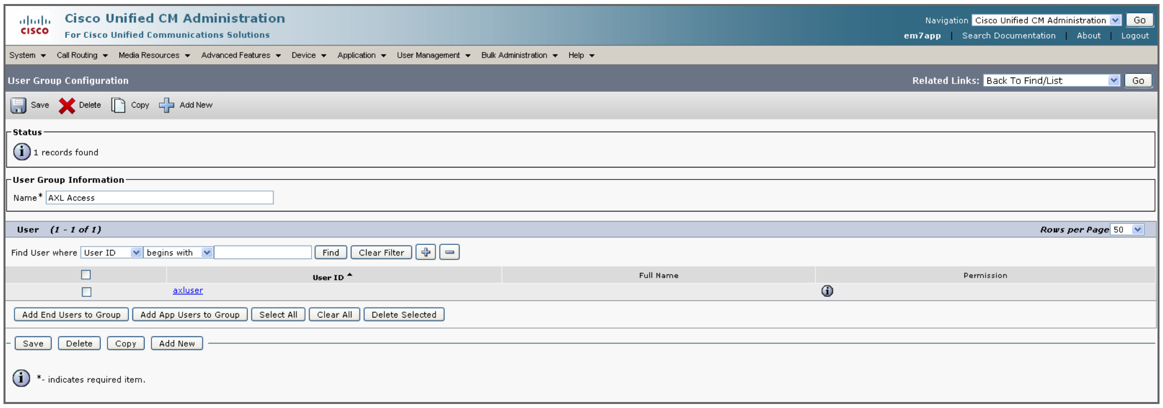
Application User

Find Application User where User ID begins with

No active query. Please enter your search criteria using the options above.

12. Click the **[Find]** button. In the list of users, select the checkbox for the user account that you created, then click the **[Add Selected]** button at the bottom of the page.

13. The **Find and List Application Users** window closes. In the **User Group Configuration** page, the user account is included in the list of users:



Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration

User Group Configuration

Related Links: Back To Find/List

Status

1 records found

User Group Information

Name* AXL Access

User (1 - 1 of 1)

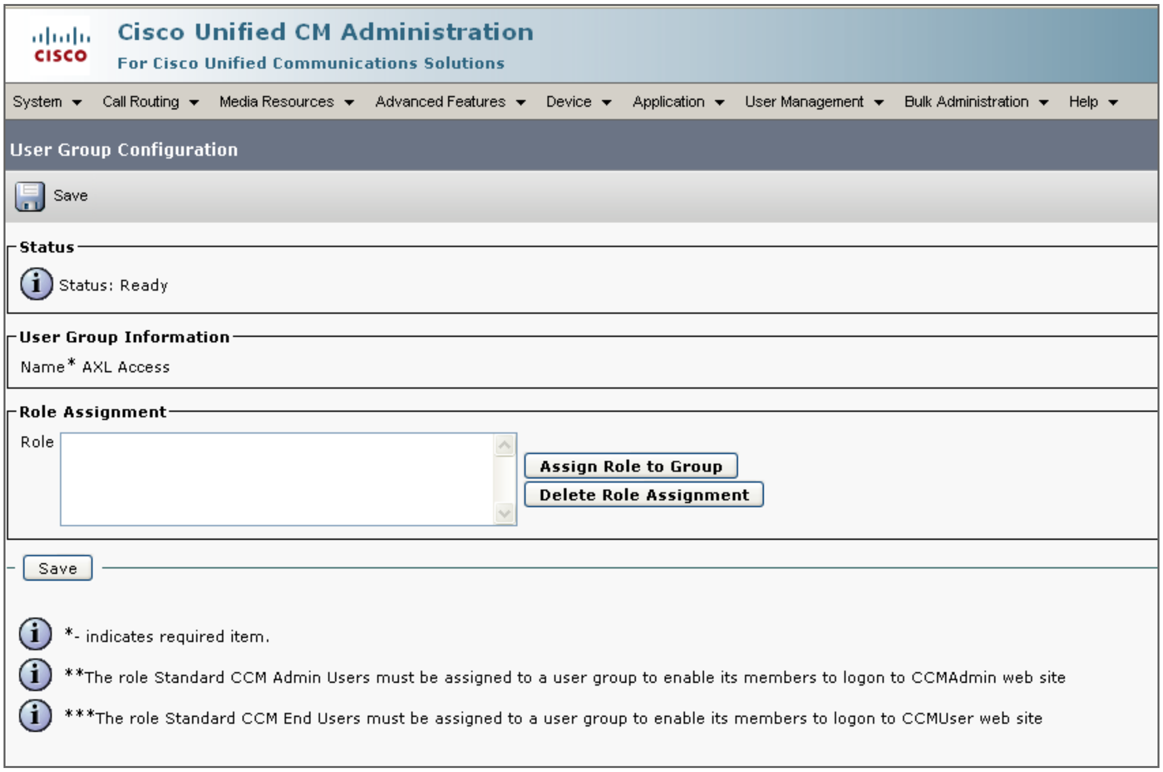
Rows per Page 50

Find User where User ID begins with

□	User ID	Full Name	Permission
□	axluser		

*- indicates required item.

14. In the ***Related Links*** drop-down list at the top-right hand corner of the page, select *Assign Role to User Group*, and then click the **[Go]** button. The **User Group Configuration** page appears:



User Group Configuration

Status

Status: Ready

User Group Information

Name* AXL Access

Role Assignment

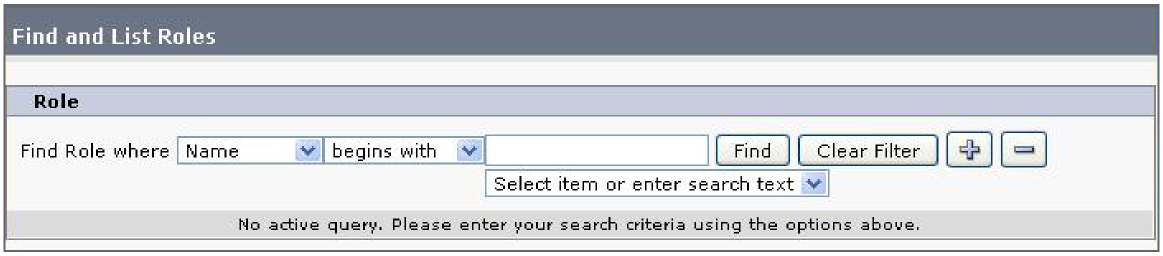
Role

*- indicates required item.

**The role Standard CCM Admin Users must be assigned to a user group to enable its members to logon to CCMAdmin web site

***The role Standard CCM End Users must be assigned to a user group to enable its members to logon to CCMUser web site

15. Click the **[Assign Role to Group]** button. The **Find and List Roles** window appears:



Find and List Roles

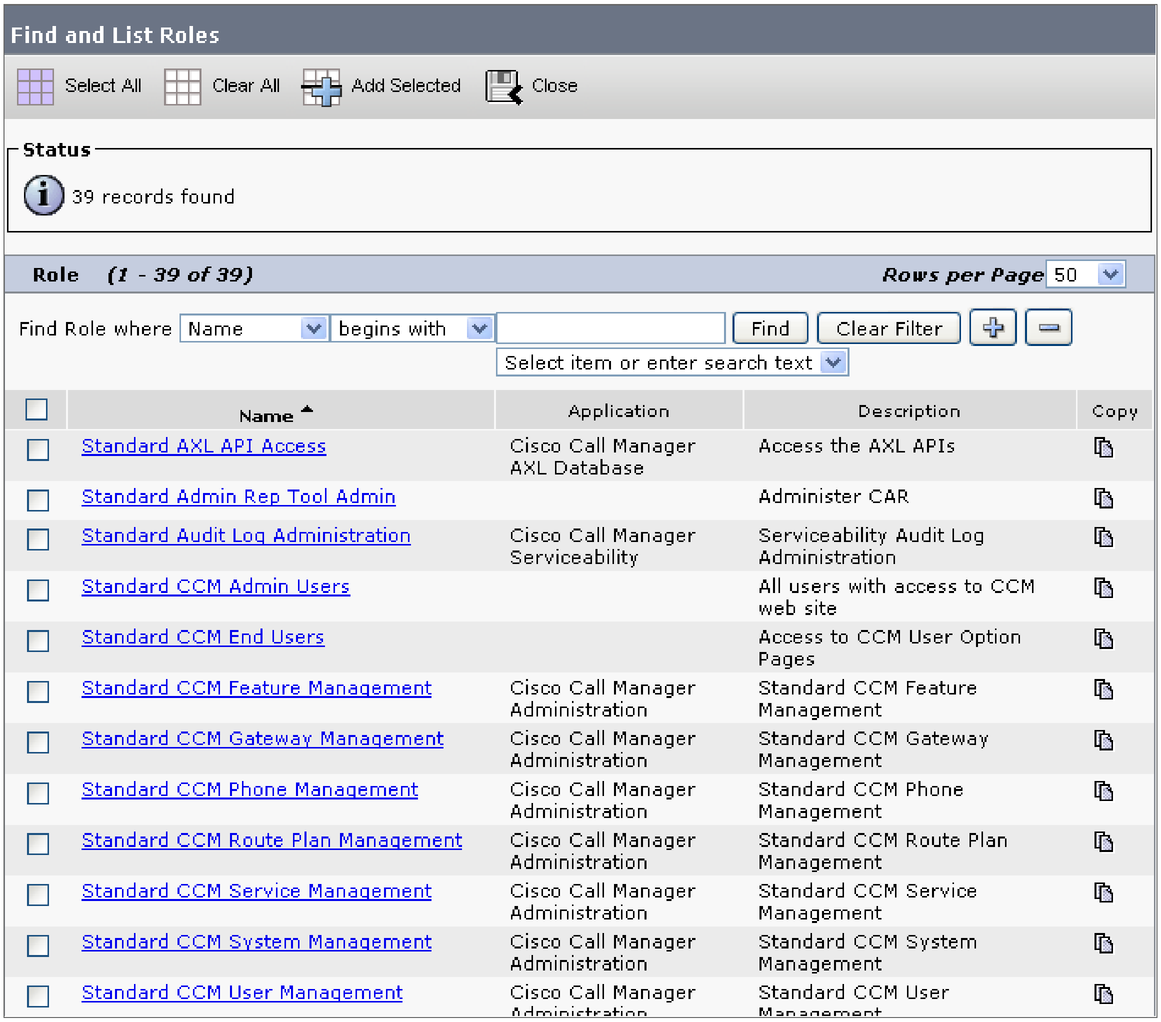
Role

Find Role where Name begins with

Select item or enter search text

No active query. Please enter your search criteria using the options above.

16. Click the **[Find]** button. A list of roles appears:



Find and List Roles

Status

39 records found

Role (1 - 39 of 39) Rows per Page 50

Find Role where Name begins with [ ] Select item or enter search text

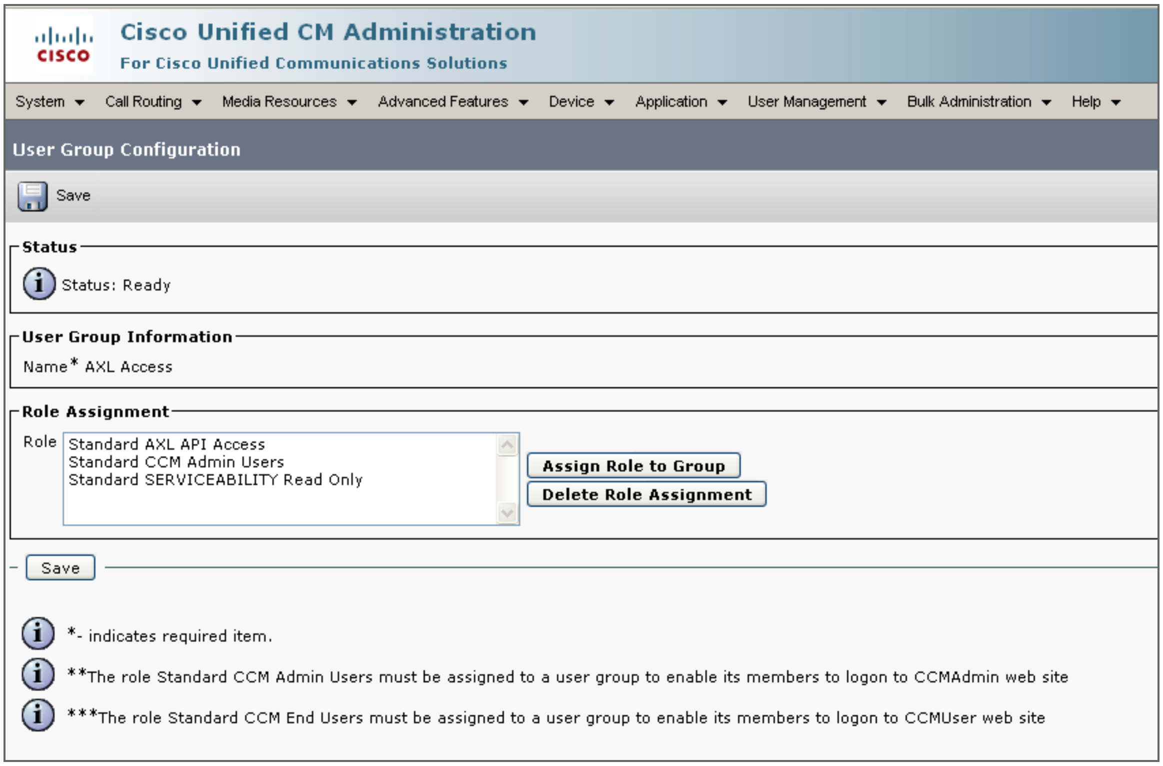
□	Name ▲	Application	Description	Copy
□	Standard AXL API Access	Cisco Call Manager AXL Database	Access the AXL APIs	
□	Standard Admin Rep Tool Admin		Administer CAR	
□	Standard Audit Log Administration	Cisco Call Manager Serviceability	Serviceability Audit Log Administration	
□	Standard CCM Admin Users		All users with access to CCM web site	
□	Standard CCM End Users		Access to CCM User Option Pages	
□	Standard CCM Feature Management	Cisco Call Manager Administration	Standard CCM Feature Management	
□	Standard CCM Gateway Management	Cisco Call Manager Administration	Standard CCM Gateway Management	
□	Standard CCM Phone Management	Cisco Call Manager Administration	Standard CCM Phone Management	
□	Standard CCM Route Plan Management	Cisco Call Manager Administration	Standard CCM Route Plan Management	
□	Standard CCM Service Management	Cisco Call Manager Administration	Standard CCM Service Management	
□	Standard CCM System Management	Cisco Call Manager Administration	Standard CCM System Management	
□	Standard CCM User Management	Cisco Call Manager Administration	Standard CCM User Management	

17. Select the checkboxes for the following roles:

- *Standard AXL API Access*
- *Standard CCM Admin Users*
- *Standard SERVICEABILITY Read Only*

18. Click the **[Add Selected]** button at the bottom of the page.

19. The **Find and List Roles** window closes. In the **User Group Configuration** page, the ***Roles*** field includes the *Standard AXL API Access* role:



User Group Configuration

Status

Status: Ready

User Group Information

Name* AXL Access

Role Assignment

Role
Standard AXL API Access
Standard CCM Admin Users
Standard SERVICEABILITY Read Only

*- indicates required item.

**The role Standard CCM Admin Users must be assigned to a user group to enable its members to logon to CCMAdmin web site

***The role Standard CCM End Users must be assigned to a user group to enable its members to logon to CCMUser web site

20. Click the **[Save]** button.

Configuring Prime License Manager

If you want to monitor Cisco Unified CM license information from Cisco Prime License Manager (PLM), you must create an administrator user account that SL1 can use to access PLM.

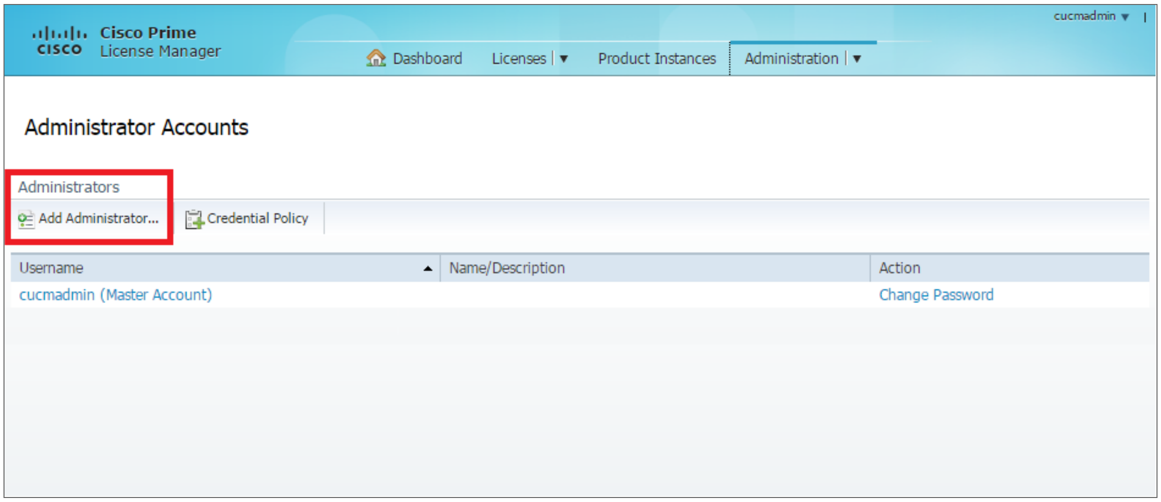
To create an administrator user in PLM:

1. In a browser window, navigate to the following address:

```
https://ip-address-of-plm-server/elm-admin/
```

2. Log in to the Cisco PLM site as an administrator.
3. In the ***Administration*** drop-down menu, select *Administrator Accounts*.

4. Click the **[Add Administrator]** button.

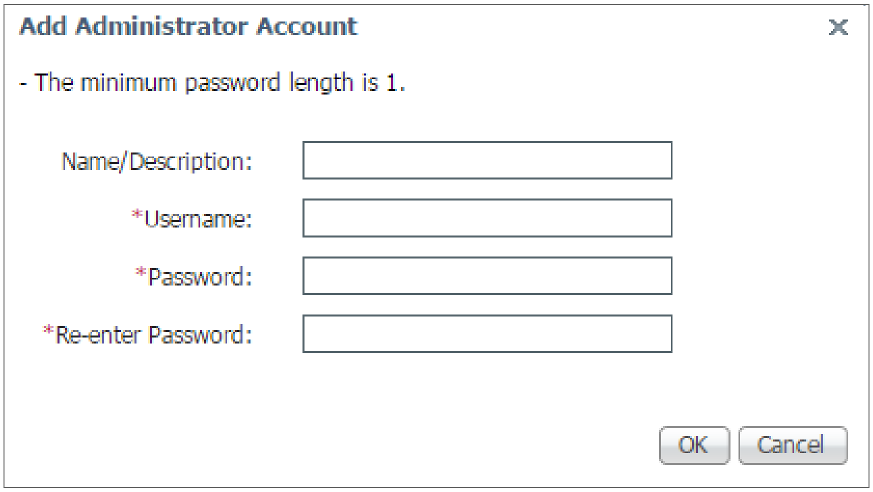


Administrator Accounts

Administrators

Username	Name/Description	Action
cucmadmin (Master Account)		Change Password

5. In the **Add Administrator Account** modal page, make entries in the following fields:



Add Administrator Account

- The minimum password length is 1.

Name/Description:

*Username:

*Password:

*Re-enter Password:

- ***Name/Description***. Type a name or description for the account.
- ***Username***. Type the account username.
- ***Password***. Type the account password.
- ***Re-enter Password***. Type the account password again.

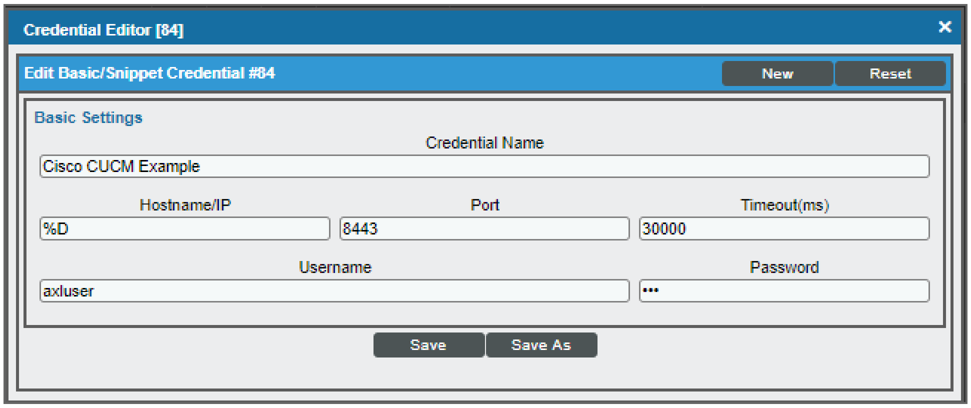
6. Click **[OK]**.

Creating a CUCM Credential

To use the Dynamic Applications in the *Cisco: CUCM Unified Communications Manager* PowerPack, you must first define a Basic/Snippet Cisco Unified CM credential in SL1. This credential allows SL1 to communicate with the Cisco Unified CM cluster. The *Cisco: CUCM Unified Communications Manager* PowerPack includes a template you can use to create this Basic/Snippet credential.

To modify the Cisco Unified CM Basic/Snippet Credential template for use with your Cisco Unified CM cluster:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the wrench icon (🔧) for the *Cisco CUCM Example* credential. The **Credential Editor** modal window appears:



Credential Name: Cisco CUCM Example

Hostname/IP: %D

Port: 8443

Timeout(ms): 30000

Username: axluser

Password: •••

3. Supply values in the following fields:
   - ***Credential Name***. Type a new name for the credential.
   - ***Hostname/IP***. Type the hostname or IP address, or you can type the variable "%D".
   - ***Port***. Type the port number.

> NOTE: The example credential included in older versions of the *Cisco: CUCM Unified Communications Manager* PowerPack used "80" as the default ***Port*** number. If your Cisco Unified CM credential specifies port 80, SL1 will automatically override that value and use port 8443 instead. If your Cisco Unified CM credential specifies any port other than 80, SL1 will use that specified port.

   - ***Timeout (ms)***. Type the timeout value of each request, in milliseconds. The default value is "30000".
   - ***Username***. Type the username for the Cisco Unified CM user account that you created to access the AXL web service. For details, see the ***Configuring a Cisco Unified CM User Account*** section.
   - ***Password***. Type the password for the username you entered in the ***Username*** field.
4. Click the **[Save As]** button.

NOTE: If you are monitoring Cisco Unified CM license information with the Cisco Prime License Manager (PLM) and your PLM administrator username and password are the same as the user account you created to access the AXL web service, then you can use the same credential to access PLM. However, if your PLM administrator user information is different, then repeat these steps to create a credential to access PLM.

NOTE: If SNMP is enabled on the Cisco Unified CM cluster, then you can also create an optional SNMP credential that will be used only during discovery to classify the cluster device class. If SNMP is not available on the Cisco Unified CM cluster, then you ***do not*** need an SNMP credential. For more information on SNMP credentials, see the ***Discovery and Credentials*** manual.

Testing the CUCM Credential

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

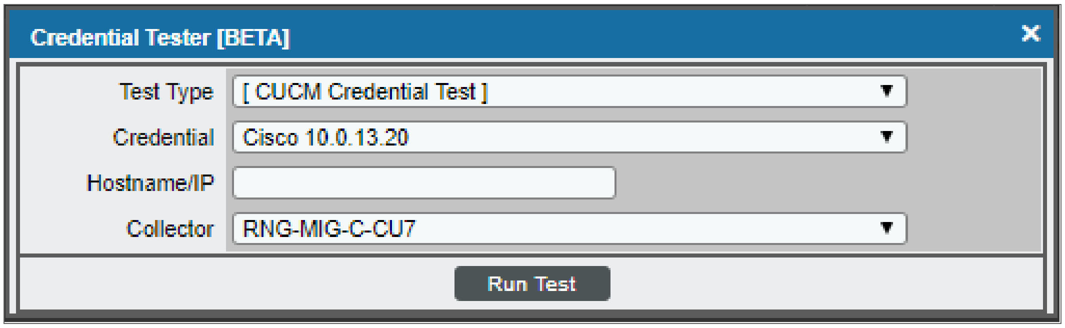
The CUCM Credential Test can be used to test a Basic/Snippet credential for monitoring Cisco Unified CM using the Dynamic Applications in the *Cisco: CUCM Unified Communications Manager* PowerPack. The CUCM Credential Test performs the following steps:

- ***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 Accessibility to Publisher***. Checks to see if the common API service URLs on the publisher device can be queried.
- ***Test Accessibility to Subscribers via Publisher***. Checks to see if data on a CUCM subscriber can be queried via the publisher.
- ***Test Accessibility to All Subscribers***. Checks to see if the status of services on a CUCM subscriber can be queried.

To test the CUCM credential:

1. Go to the **Credential Test Management** page (System > Customize > Credential Tests).

2. Locate the **CUCM Credential Test** and click its lightning bolt icon (⚡). The **Credential Tester** modal page appears:



Credential Tester [BETA]

Test Type: [CUCM Credential Test]

Credential: Cisco 10.0.13.20

Hostname/IP:

Collector: RNG-MIG-C-CU7

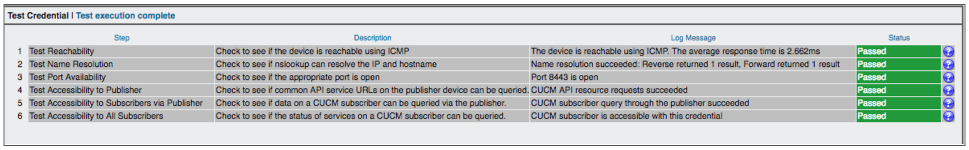
3. Supply values in the following fields:

- ***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:



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 2.662ms	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 appropriate port is open	Port 8443 is open	Passed	?
4	Test Accessibility to Publisher	Check to see if common API service URLs on the publisher device can be queried.	CUCM API resource requests succeeded	Passed	?
5	Test Accessibility to Subscribers via Publisher	Check to see if data on a CUCM subscriber can be queried via the publisher.	CUCM subscriber query through the publisher succeeded	Passed	?
6	Test Accessibility to All Subscribers	Check to see if the status of services on a CUCM subscriber can be queried.	CUCM subscriber is accessible with this credential	Passed	?

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".

Manually Creating Host File Entries for CUCM Nodes

During the discovery process, SL1 automatically aligns the IP addresses and hostnames for each CallManager server (node) in a Cisco Unified CM cluster via DNS.

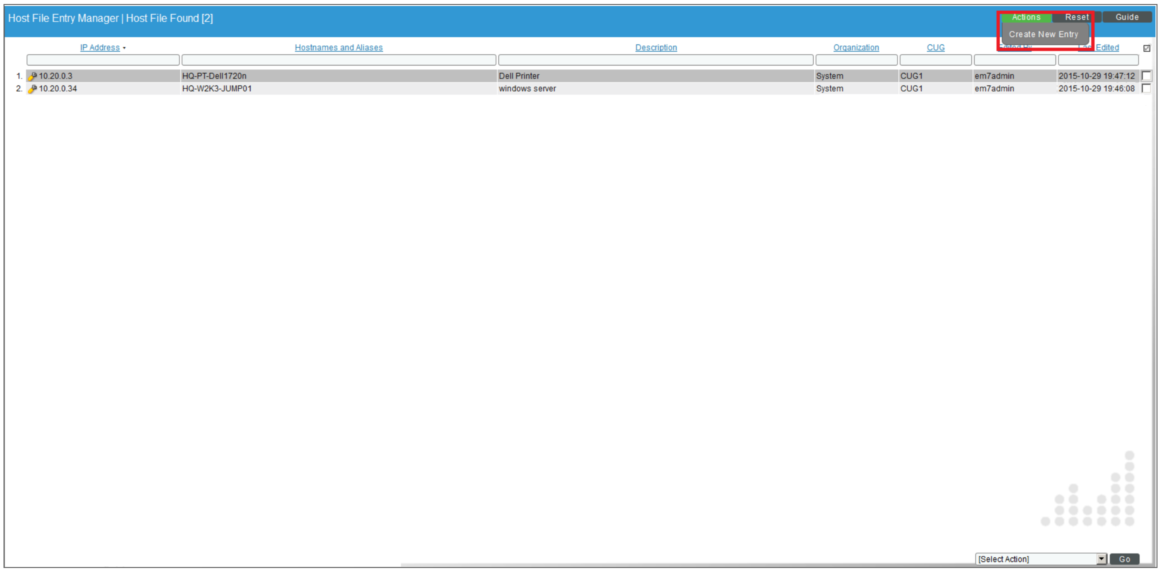
If you do not have access to DNS for the Cisco Unified CM system you want to monitor, you must manually create host file entries in SL1 for each node in the Cisco Unified CM cluster. Each host file entry must contain the IP address and hostname of a node in the Cisco Unified CM cluster.

> **NOTE:** If you have access to DNS for the Cisco Unified CM system you want to monitor with SL1, you do not need to perform the steps to manually configure host file entries. Continue to the section on ***Discovering a Cisco Unified CM Cluster***.

Repeat the following steps for each node in the Cisco Unified CM cluster.

To create a host file entry:

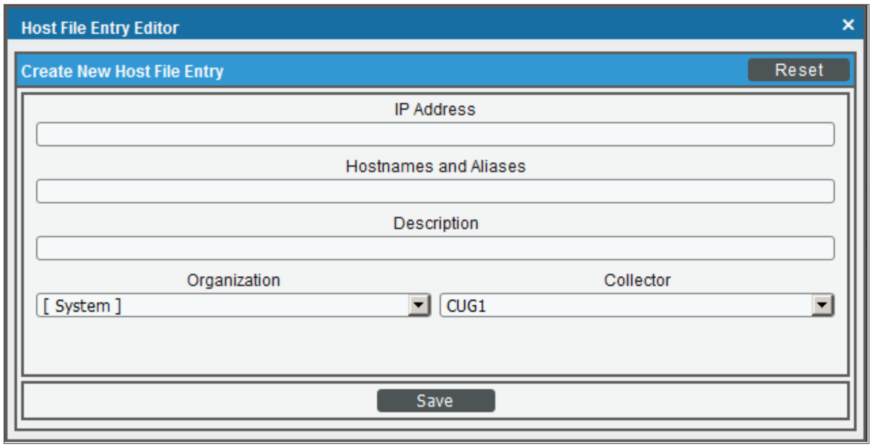
1. Go to the **Host File Entry Manager** page (System > Customize > Host Files).



Host File Entry Manager | Host File Found [2]

	IP Address	Hostnames and Aliases	Description	Organization	CUG	Edited By	Last Edited	☑
1.	10.20.0.3	HQ-PT-Dell1720n	Dell Printer	System	CUG1	em7admin	2015-10-29 19:47:12	□
2.	10.20.0.34	HQ-W2K3-JUMP01	windows server	System	CUG1	em7admin	2015-10-29 19:46:08	□

2. Click the **[Action]** menu and choose ***Create New Entry***. The **Create New Host File Entry** modal page appears.



Organization: [System]

Collector: CUG1

3. In the **Create New Host File Entry** modal page, supply values in the following fields:

    - ***IP Address***. The IP address to resolve with the hostname.

NOTE: Server hostnames should be aligned to external IP addresses when supporting Network Address Translation (NAT) environments.

- ***Hostnames and Aliases***. The hostname to align with the specified IP address. You can also include a space-delimited list of aliases for the host name.
- ***Description***. Description of the host entry. This field is not written to the host file. This field is for administrators to use when managing host file entries.
- ***Organization***. Organization associated with the host. You can select from a list of all existing organizations. This field is not written to the host file. This field is for administrators to use when managing host file entries. For example, a service provider could assign each customer its own organization and then use this field to manage host file entries for each customer.

4. Click the **[Save]** button to save the new host entry.

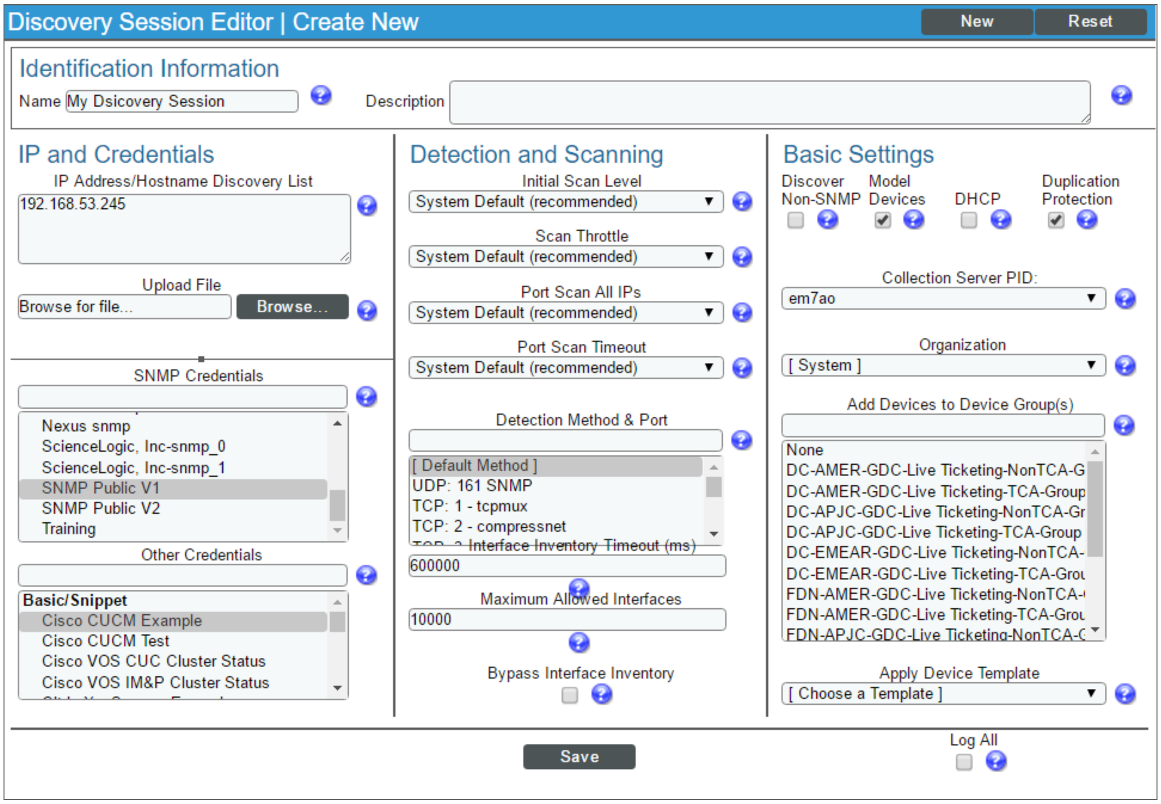
Discovering a Cisco Unified CM Cluster

When you use the *Cisco: CUCM Unified Communications Manager* PowerPack to discover Cisco Unified CM devices, SL1 creates a device representing your Cisco Unified CM cluster. This cluster device acts as the root device for the remaining servers and component devices in your Cisco Unified CM system.

To create and run a discovery session that will discover a Cisco Unified CM cluster:

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

2. Click the **[Create]** button to create a new discovery session. The **Discovery Session Editor** window appears:



Discovery Session Editor | Create New

Identification Information

Name: My Dsicovery Session

Description:

IP and Credentials

IP Address/Hostname Discovery List: 192.168.53.245

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

SNMP Credentials:
- Nexus snmp
- ScienceLogic, Inc-snmp_0
- ScienceLogic, Inc-snmp_1
- SNMP Public V1
- SNMP Public V2
- Training

Other Credentials:
- Basic/Snippet
- Cisco CUCM Example
- Cisco CUCM Test
- Cisco VOS CUC Cluster Status
- Cisco VOS IM&P Cluster Status

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

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: em7ao

Organization: [System]

Add Devices to Device Group(s):
- None
- DC-AMER-GDC-Live Ticketing-NonTCA-G
- DC-AMER-GDC-Live Ticketing-TCA-Group
- DC-APJC-GDC-Live Ticketing-NonTCA-Gr
- DC-APJC-GDC-Live Ticketing-TCA-Group
- DC-EMEAR-GDC-Live Ticketing-NonTCA-
- DC-EMEAR-GDC-Live Ticketing-TCA-Grou
- FDN-AMER-GDC-Live Ticketing-NonTCA-
- FDN-AMER-GDC-Live Ticketing-TCA-Grou
- FDN-APJC-GDC-Live Ticketing-NonTCA-C

Apply Device Template: [Choose a Template]

Log All: □

3. Enter values in the following fields:

- ***IP Address/Hostname Discovery List***. Type the IP addresses for the Cisco Unified CM Publishers.

NOTE: To monitor Cisco Unified CM servers that are registered by name within their clusters, you might need to go to the **Host File Entry Manager** page (System > Customize > Host Files) and map the server names to their IP addresses if you do not have access to DNS for the Cisco Unified CM system you want to monitor. For Network Address Translation (NAT) environments, server hostnames should be mapped to external IP addresses. For more information, see the section *Manually Creating Host File Entries for Cisco Unified CM Nodes*.

- ***SNMP Credential***. Select an SNMP credential to use with the Cisco Unified CM cluster. (For more information on SNMP credentials, see the ***Discovery and Credentials*** manual.)

NOTE: An SNMP credential is needed only to properly classify the devices in the cluster. If SNMP is not available on the Cisco Unified CM cluster, then you do not need to select an SNMP credential; in that scenario, the root device will be discovered as a pingable device and you must manually change it to a Cisco Unified CM cluster.

- ***Other Credentials***. Select the *Cisco Cisco Unified CM Example* credential that you edited in the section on ***Creating a Cisco Unified CM Credential***.

4. You can enter values in the other fields on this page, but are not required to and can simply accept the default values. For more information about the other fields on this page, see the ***Discovery and Credentials*** manual.
5. Click **[Save]** 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.
8. When the Cisco Unified CM cluster is discovered, click its device icon ( ) to view the **Device Properties** page for the Cisco Unified CM cluster.

Chapter 14

Cisco: ESA

Overview

The following sections describe how to configure and discover Cisco Email Security Appliances for monitoring by SL1 using the *Cisco: ESA* PowerPack:

NOTE: For more information about the *Cisco: ESA* PowerPack, see the ***Monitoring Cisco Email Security Appliances*** manual.

Prerequisites for Monitoring Cisco Email Security Appliances

To configure SL1 to monitor Cisco Email Security Appliances using the *Cisco: ESA* PowerPack, you must first have the following information about the appliance that you want to monitor:

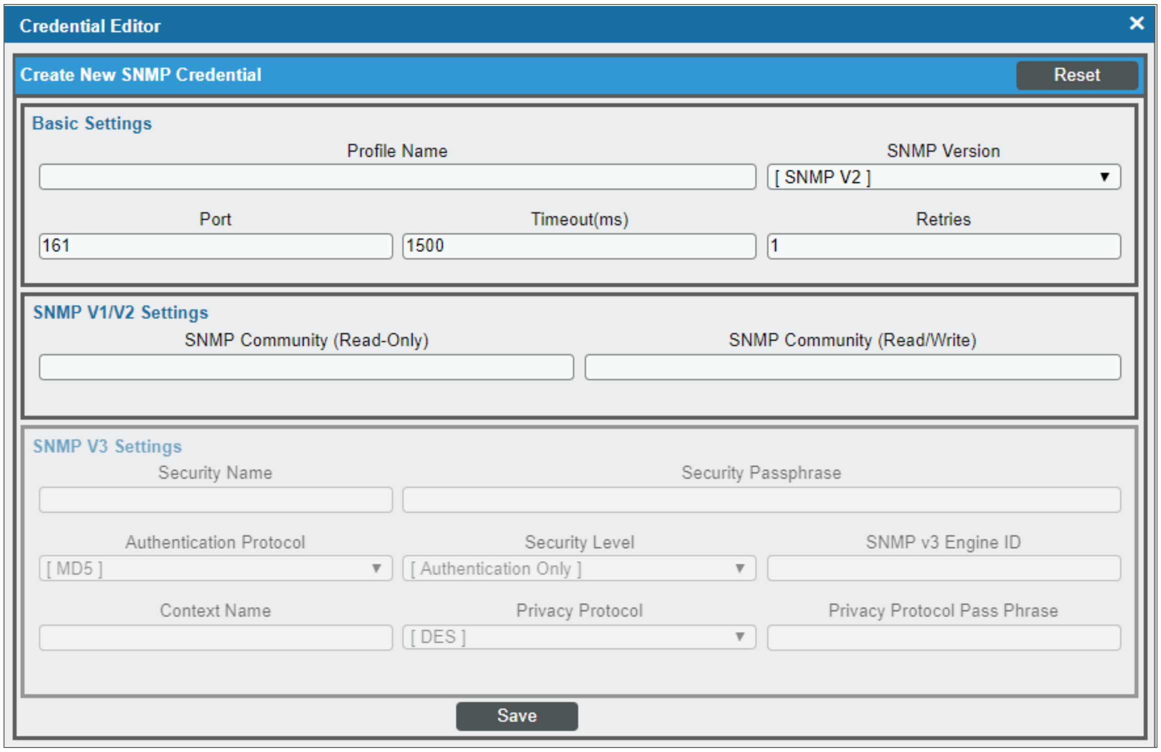
- The appliance's IP address.
- The appliance's SNMP community string.

Creating an SNMP Credential for Cisco ESA

To configure SL1 to monitor Cisco Email Security Appliances, you must create an SNMP credential. This credential allows the Dynamic Applications in the *Cisco: ESA* PowerPack to connect with the Cisco ESA and collect data from it.

To create an SNMP credential:

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



Profile Name:
SNMP Version: [SNMP V2]
Port: 161
Timeout(ms): 1500
Retries: 1
SNMP Community (Read-Only):
SNMP Community (Read/Write):
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.

SNMP V1/V2 Settings

These fields appear if you selected *SNMP V1* or *SNMP V2* in the ***SNMP Version*** field. Otherwise, these fields are grayed out.

- ***SNMP Community (Read Only)***. The SNMP community string (password) required for read-only access of SNMP data on the remote device or application. For SNMP V1 and SNMP V2 credentials, you must supply a community string, either in this field or in the ***SNMP Community (Read/Write)*** field.
- ***SNMP Community (Read/Write)***. The SNMP community string (password) required for read and write access of SNMP data on the remote device or application. For SNMP V1 and SNMP V2 credentials, you must supply a community string, either in this field or in the ***SNMP Community (Read Only)*** field.

SNMP V3 Settings

These fields appear if you selected *SNMP V3* in the ***SNMP Version*** field. Otherwise, these fields are grayed out.

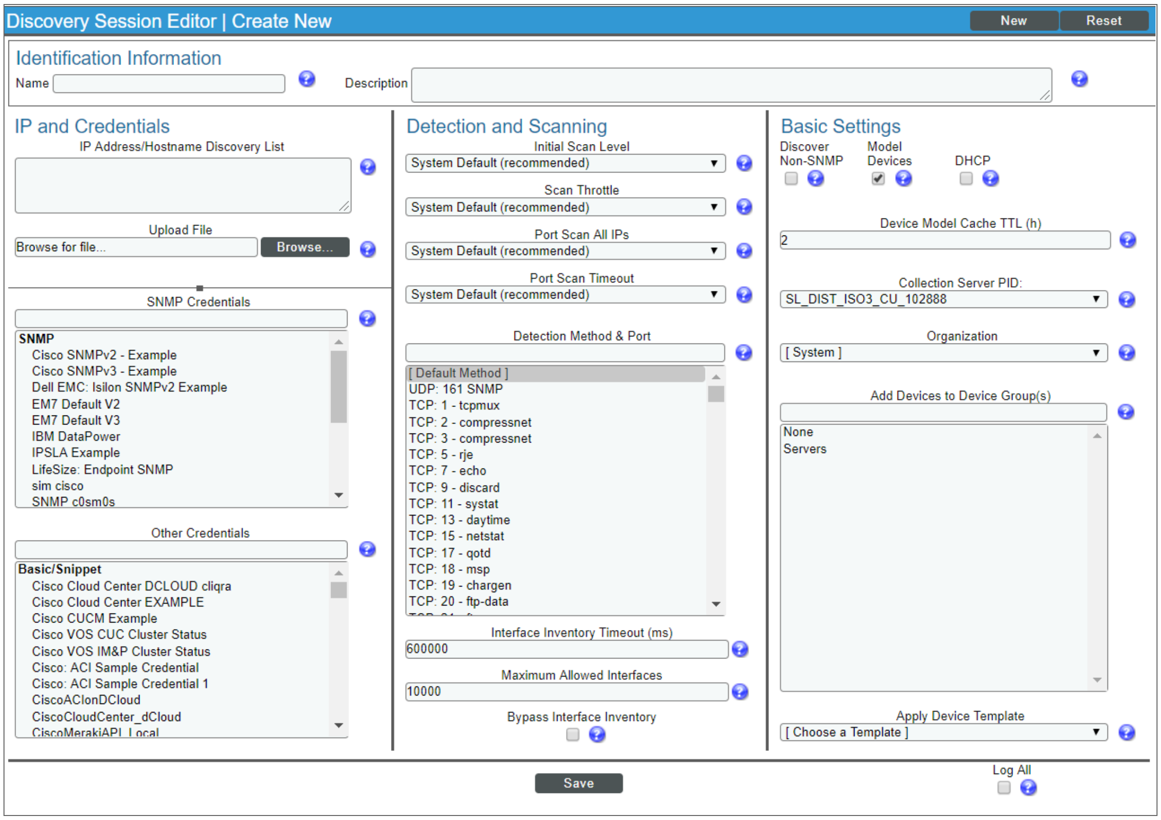
- ***Security Name***. Name for SNMP authentication. This field is required.
- ***Security Passphrase***. Password to authenticate the credential. This value must contain at least 8 characters. This value is required if you use a ***Security Level*** that includes authentication.
- ***Authentication Protocol***. Select an authentication algorithm for the credential. Choices are MD5 or SHA. The default value is *MD5*. This field is required.
- ***Security Level***. Specifies the combination of security features for the credentials. This field is required. Choices are:
    - *No Authentication / No Encryption*.
    - *Authentication Only*. This is the default value.
    - *Authentication and Encryption*.
- ***SNMP v3 Engine ID***. The unique engine ID for the SNMP agent you want to communicate with. (SNMPv3 authentication and encryption keys are generated based on the associated passwords and the engine ID.) This field is optional.
- ***Context Name***. A context is a mechanism within SNMPv3 (and AgentX) that allows you to use parallel versions of the same MIB objects. For example, one version of a MIB might be associated with SNMP Version 2 and another version of the same MIB might be associated with SNMP Version 3. For SNMP Version 3, specify the context name in this field. This field is optional.
- ***Privacy Protocol***. The privacy service encryption and decryption algorithm. Choices are *DES* or *AES*. The default value is *DES*. This field is required.
- ***Privacy Protocol Passphrase***. Privacy password for the credential. This field is optional.

4. Click **[Save]**.

Discovering a Cisco Email Security Appliance

To discover the Cisco ESA that you want to monitor:

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



Initial Scan Level: System Default (recommended)
Scan Throttle: System Default (recommended)
Port Scan All IPs: System Default (recommended)
Port Scan Timeout: System Default (recommended)
Interface Inventory Timeout (ms): 600000
Maximum Allowed Interfaces: 10000
Bypass Interface Inventory: □
Discover Non-SNMP: □
Model Devices: ☑
DHCP: □
Device Model Cache TTL (h): 2
Collection Server PID: SL_DIST_ISO3_CU_102888
Organization: [System]
Apply Device Template: [Choose a Template]
Log All: □

- ***Name***. Type a name for the discovery session.
- ***IP Address/Hostname Discovery List***. Type the IP address for the ESA device that you want to monitor.
- ***SNMP Credentials***. Select the SNMP credential you created for ESA.
- ***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 **[Save]**, 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. When the ESA is discovered, click its device icon (🖥) to view its **Device Properties** page.

Chapter 15

Cisco: Hyperflex

Overview

The following sections describe how to configure and discover Cisco HyperFlex data clusters for monitoring by SL1 using the *Cisco: Hyperflex* PowerPack:

NOTE: The *Cisco: Hyperflex* PowerPack supports only HyperFlex API version 2.5 and later.

NOTE: For more information about the *Cisco: Hyperflex* PowerPack, see the ***Monitoring Cisco Hyperflex*** manual.

Prerequisites for Monitoring Cisco HyperFlex

To configure SL1 to monitor Cisco HyperFlex using the *Cisco: Hyperflex* PowerPack, you must have the following information about the HyperFlex data clusters that you want to monitor:

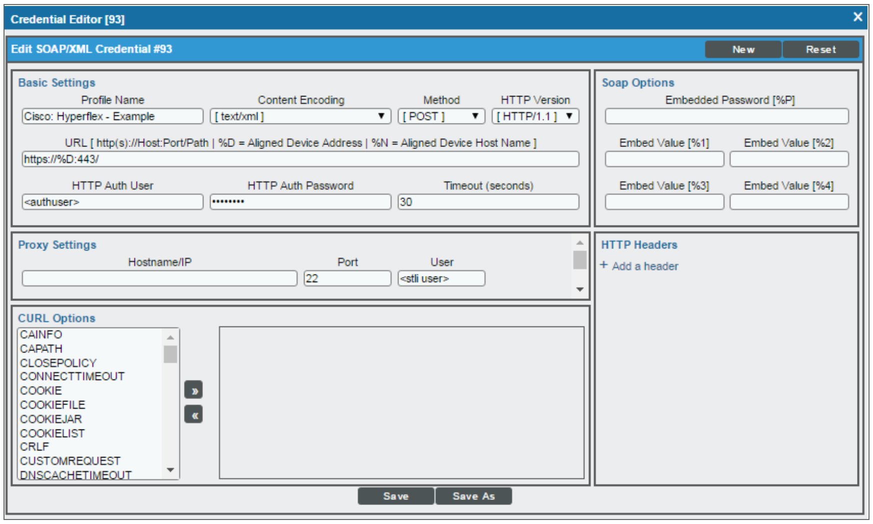
- The Hyperflex Cluster Management IP Address
- SNMP community strings for the voice mailboxes

Creating a SOAP/XML Credential for Cisco HyperFlex

To configure SL1 to monitor Cisco HyperFlex, you must first create a SOAP/XML credential. This credential allows SL1 (specifically, the Dynamic Applications in the *Cisco: HyperFlex* PowerPack) to connect with HyperFlex devices. An example SOAP/XML credential that you can edit for your own use is included in the *Cisco: HyperFlex* PowerPack.

To configure a SOAP/XML credential to access HyperFlex devices:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the sample credential included in the *Cisco: HyperFlex* PowerPack, called **Cisco: HyperFlex - Example**, then click its wrench icon (🔧).
3. Enter values in the following fields:



Credential Editor [93]

Edit SOAP/XML Credential #93

Basic Settings

Profile Name: Cisco: Hyperflex - Example

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://%D:443/

HTTP Auth User: <authuser>

HTTP Auth Password: ••••••••

Timeout (seconds): 30

Soap Options

Embedded Password [%P]:

Embed Value [%1]:

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

Proxy Settings

Hostname/IP:

Port: 22

User: <stli user>

HTTP Headers

CURL Options

Basic Settings

- ***Profile Name***. Enter a new name for the HyperFlex credential.
- ***Content Encoding***. Select *text/xml*.
- ***Method***. Select *POST*.
- ***HTTP Version***. Select *HTTP/1.1*.
- ***URL***. Keep the default value.
- ***HTTP Auth User***: Use the login credentials for the HyperFlex REST API Explorer:
  - *For users with HyperFlex Data Platform 3.0 and prior versions*, type "root"
  - *For users with Hyperflex Data Platform 3.5 and later versions*, type "admin"
- ***HTTP Auth Password***:

- *For users with HyperFlex Data Platform 3.0 and prior versions*, enter the password for "root"
- *For users with HyperFlex Data Platform 3.5 and later versions*, enter the HyperFlex administrator user's password

Proxy Settings

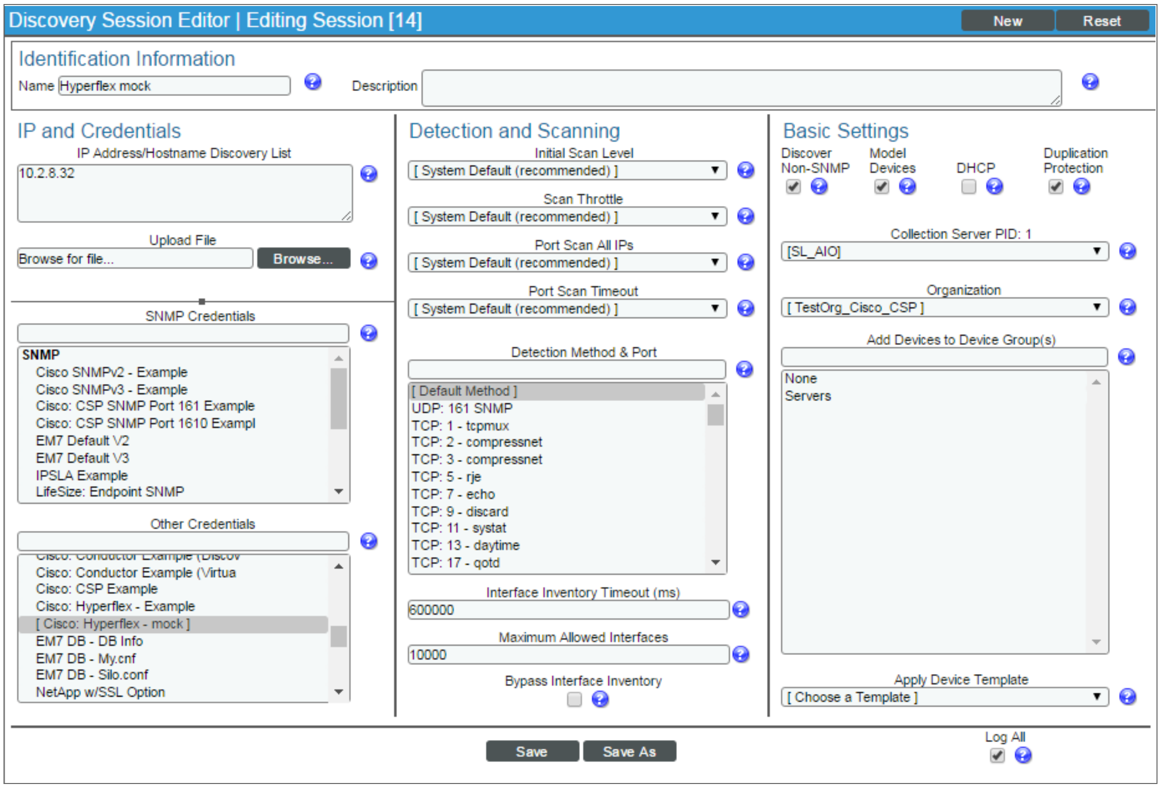
- ***Hostname/IP***. Leave this field blank.
- ***Port***. Keep the default value.
- ***User***. Enter the SSH username for the HyperFlex device(s).
- ***Password***. Enter the SSH password for the HyperFlex device(s).

4. Click **[Save As]**.
5. In the confirmation message, click **[OK]**.

Discovering Cisco HyperFlex Devices

To create and run a discovery session that will discover Cisco HyperFlex devices, perform the following steps:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. Click the **[Create]** button to create a new discovery session. The **Discovery Session Editor** page appears:



Discovery Session Editor | Editing Session [14]

Identification Information

Name: Hyperflex mock

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.2.8.32

Upload File: Browse for file...

SNMP Credentials

SNMP
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Cisco: CSP SNMP Port 161 Example
Cisco: CSP SNMP Port 1610 Exampl
EM7 Default V2
EM7 Default V3
IPSLA Example
LifeSize: Endpoint SNMP

Other Credentials

Cisco: Conductor Example (Discov
Cisco: Conductor Example (Virtua
Cisco: CSP Example
Cisco: Hyperflex - Example
[Cisco: Hyperflex - mock]
EM7 DB - DB Info
EM7 DB - My.cnf
EM7 DB - Silo.conf
NetApp w/SSL Option

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: 1: [SL_AIO]

Organization: [TestOrg_Cisco_CSP]

Add Devices to Device Group(s)

None
Servers

Apply Device Template: [Choose a Template]

Log All: ☑

3. Enter values in the following fields:

   - ***IP Address Discovery List***. Enter the IP address(es) for the Cisco HyperFlex device(s) you want to discover.
   - ***SNMP Credential***. Select the *SOAP/XML credential that you created for Cisco HyperFlex*.
   - ***Discover Non-SNMP***. Select this checkbox.

4. You can enter values in the other fields on this page, but are not required to and can simply accept the default values. For more information about the other fields on this page, see the ***Discovery and Credentials*** manual.
5. Click **[Save]** 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.
8. When the Cisco HyperFlex data cluster is discovered, click its device icon (🖥) to view its **Device Properties** page.

Chapter 16

Cisco: Meeting Server

Overview

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

NOTE: For more information about the *Cisco: Meeting Server* PowerPack, see the ***Monitoring Cisco Meeting Server*** manual.

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.

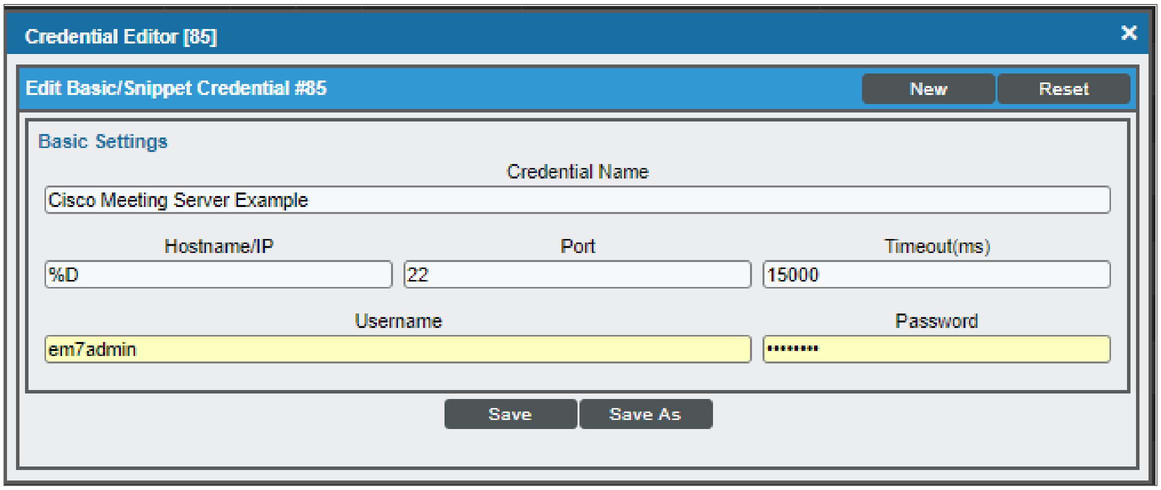
- If you can reach both of these through the same IP address, you can typically use a ***single Basic/Snippet credential***.
- If the two interfaces have separate IP addresses, or if the API is listening on a port other than 443, you must ***create two separate credentials***. In addition, you should 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: ••••••••

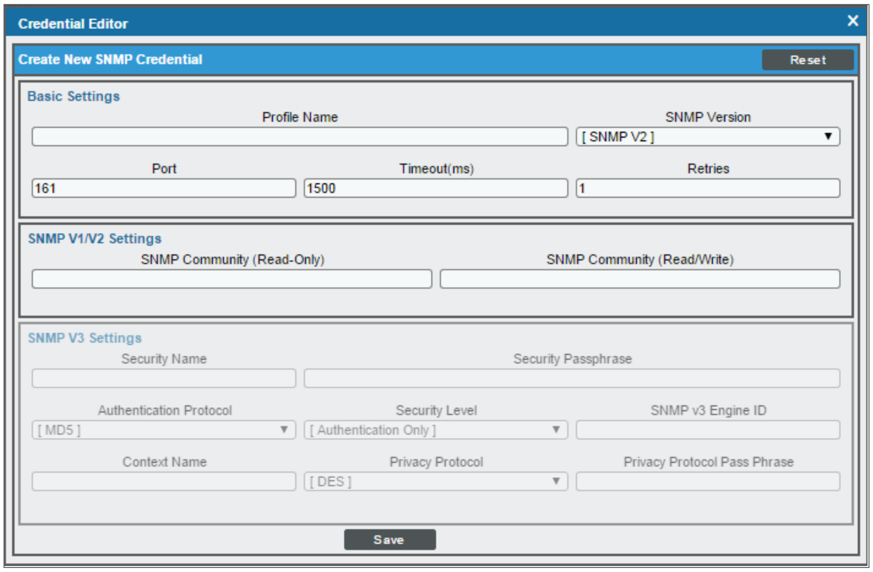
3. Supply values in the following fields:
   - ***Credential Name***. Type a new name for the credential.
   - ***Hostname/IP***. Type "%D".
   - ***Port***. Type "22".
   - ***Timeout(ms)***. Type "15000".

- ***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.



Credential Editor

Create New SNMP Credential

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.

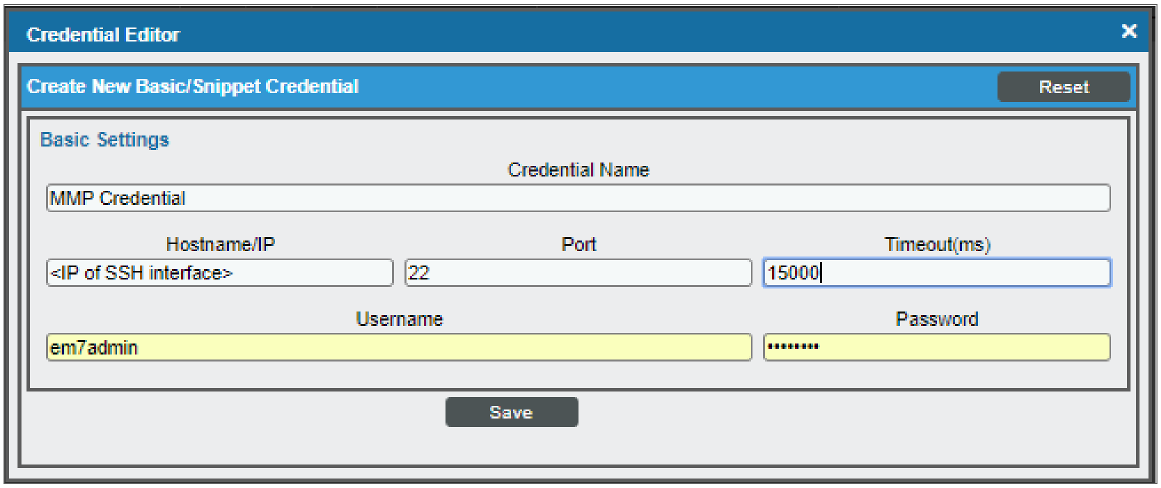
Creating Credentials for Cisco Meeting Server Systems Using More than One IP Address

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 Name: MMP Credential
Hostname/IP: <IP of SSH interface>
Port: 22
Timeout(ms): 15000
Username: em7admin
Password: ••••••••

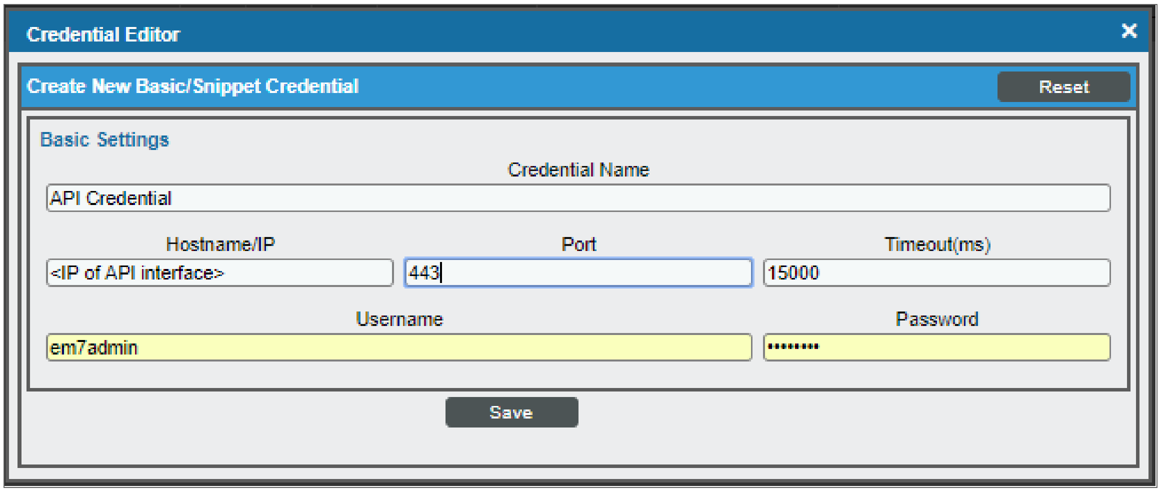
3. Supply values in the following fields:

   - ***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:

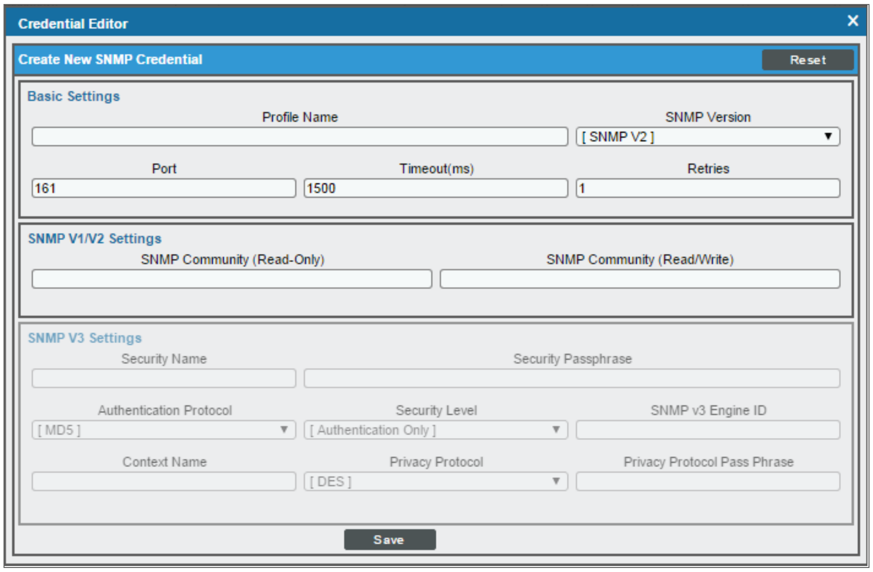
   - ***Credential Name***. Type a new name for the credential.
   - ***Hostname/IP***. Type the IP address of the API interface.
   - ***Port***. Type "443".
   - ***Timeout(ms)***. Type "15000". This value can be adjusted depending on your environment.
   - ***Username***. Type the username for the Cisco 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:



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.

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.

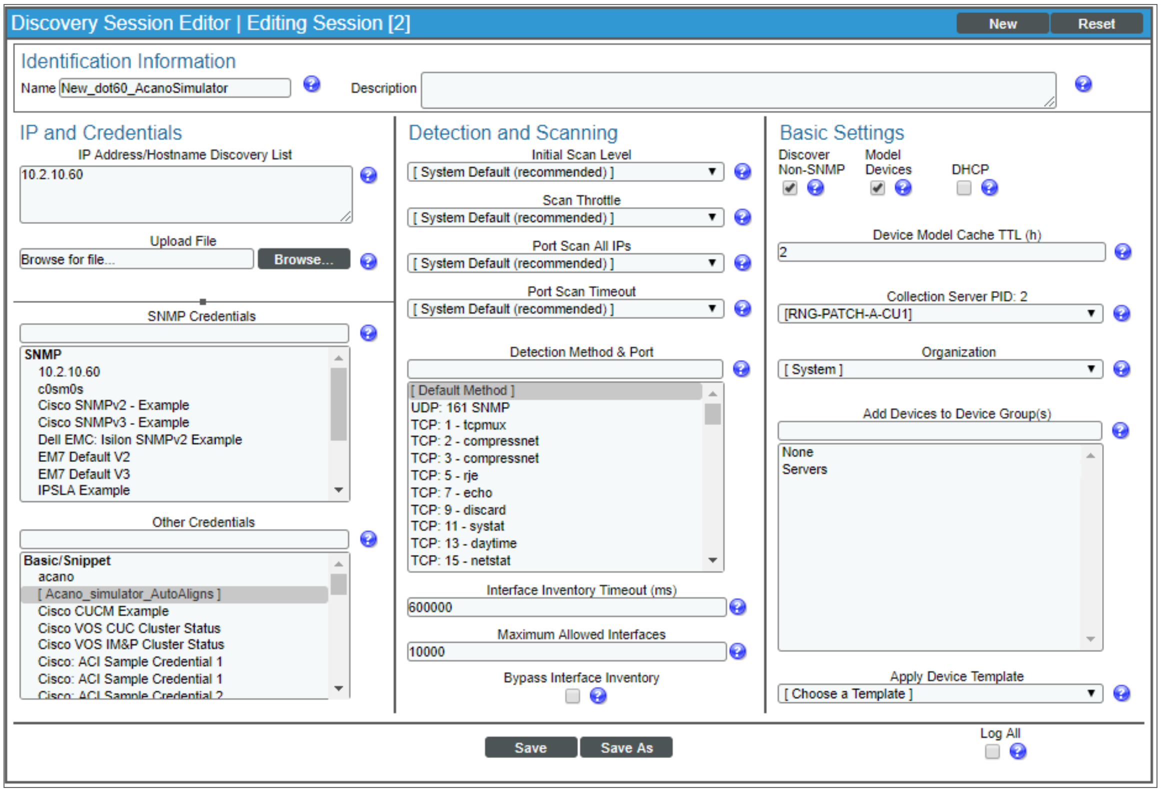
Discovering Cisco Meeting Server Devices That Use a Single IP Address

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 > Classic 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:



Name New_dot60_AcanoSimulator

Description

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

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 ☐

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

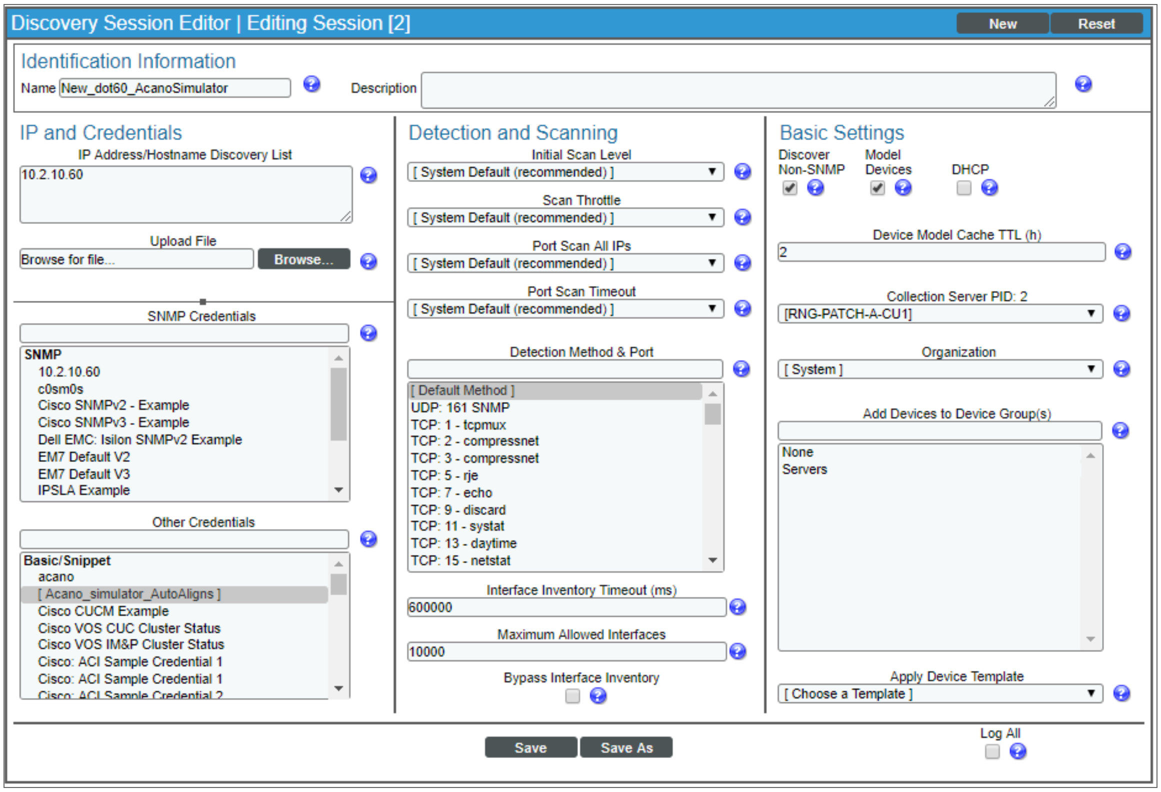
To model and monitor your Cisco Meeting Server devices, you must run a discovery session to discover the Cisco Meeting Server component devices that SL1 will use as the root devices for monitoring the applications.

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 > Classic 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... 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

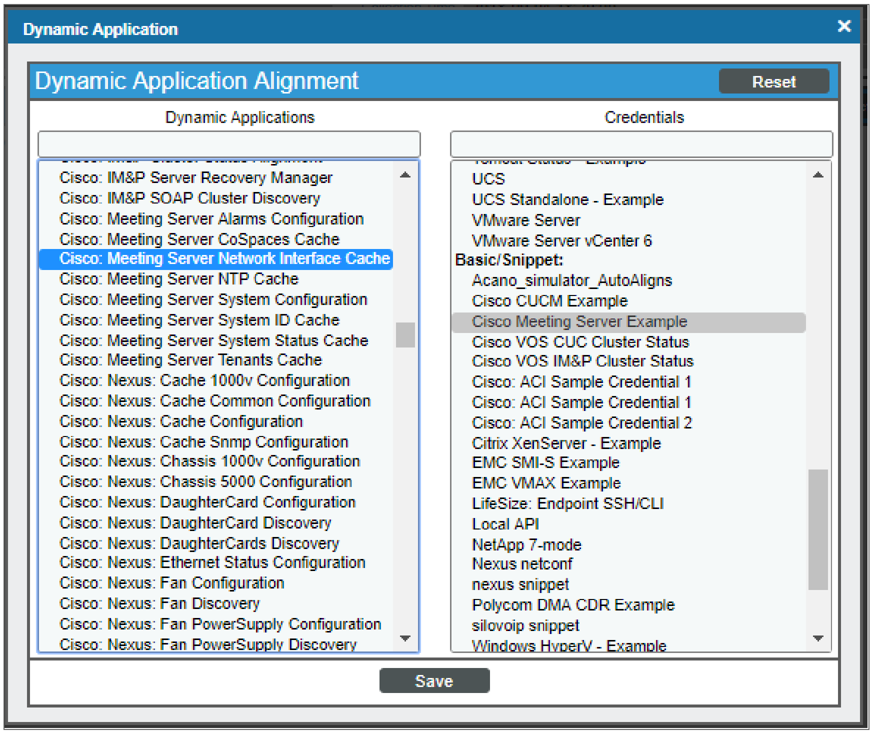
Apply Device Template: [Choose a Template]

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

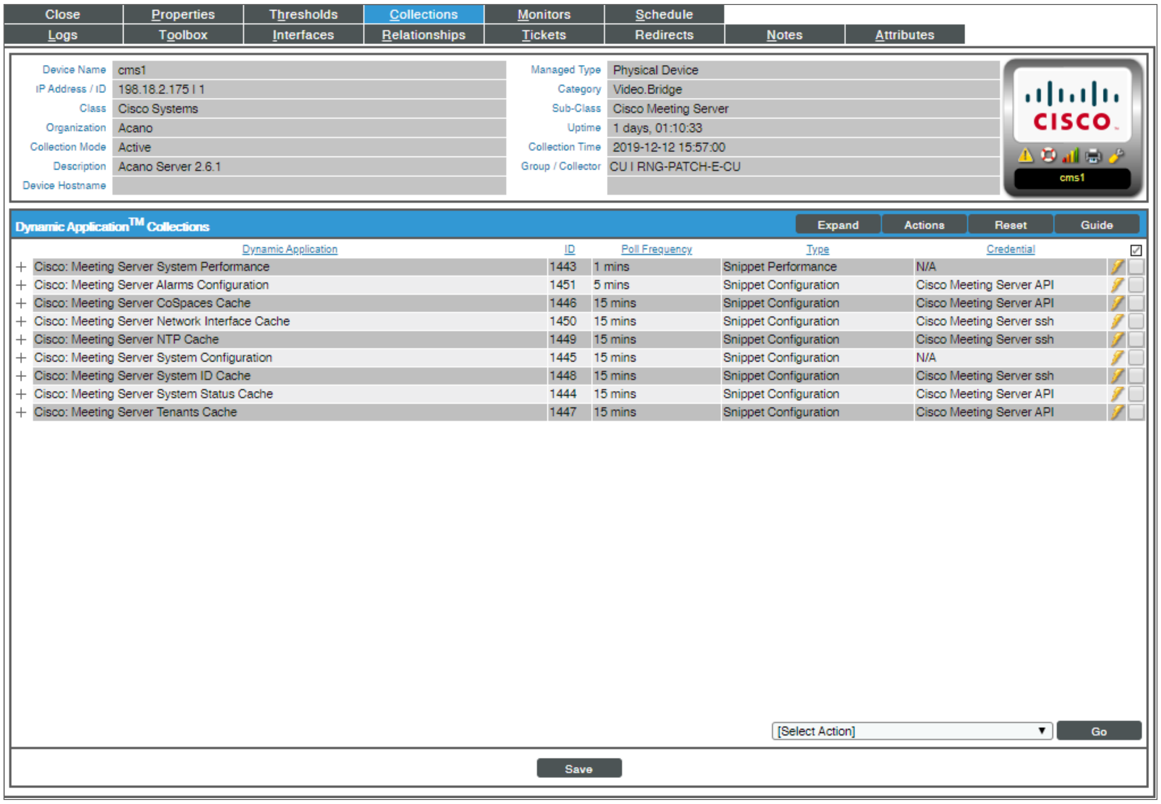
19. These applications do not require an associated credential.
20. Click **[Save]**. A few minutes after aligning the Dynamic Applications, SL1 will discover and model your Cisco Meeting Server and automatically align other Dynamic Applications to the devices in the system.

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	cms1	Managed Type	Physical Device
IP Address / ID	198.18.2.175 I 1	Category	Video.Bridge
Class	Cisco Systems	Sub-Class	Cisco Meeting Server
Organization	Acano	Uptime	1 days, 01:10:33
Collection Mode	Active	Collection Time	2019-12-12 15:57:00
Description	Acano Server 2.6.1	Group / Collector	CU I RNG-PATCH-E-CU
Device Hostname			

Dynamic Application^{TM} Collections

Dynamic Application	ID	Poll Frequency	Type	Credential	☑
+ Cisco: Meeting Server System Performance	1443	1 mins	Snippet Performance	N/A	□
+ Cisco: Meeting Server Alarms Configuration	1451	5 mins	Snippet Configuration	Cisco Meeting Server API	□
+ Cisco: Meeting Server CoSpaces Cache	1446	15 mins	Snippet Configuration	Cisco Meeting Server API	□
+ Cisco: Meeting Server Network Interface Cache	1450	15 mins	Snippet Configuration	Cisco Meeting Server ssh	□
+ Cisco: Meeting Server NTP Cache	1449	15 mins	Snippet Configuration	Cisco Meeting Server ssh	□
+ Cisco: Meeting Server System Configuration	1445	15 mins	Snippet Configuration	N/A	□
+ Cisco: Meeting Server System ID Cache	1448	15 mins	Snippet Configuration	Cisco Meeting Server ssh	□
+ Cisco: Meeting Server System Status Cache	1444	15 mins	Snippet Configuration	Cisco Meeting Server API	□
+ Cisco: Meeting Server Tenants Cache	1447	15 mins	Snippet Configuration	Cisco Meeting Server API	□

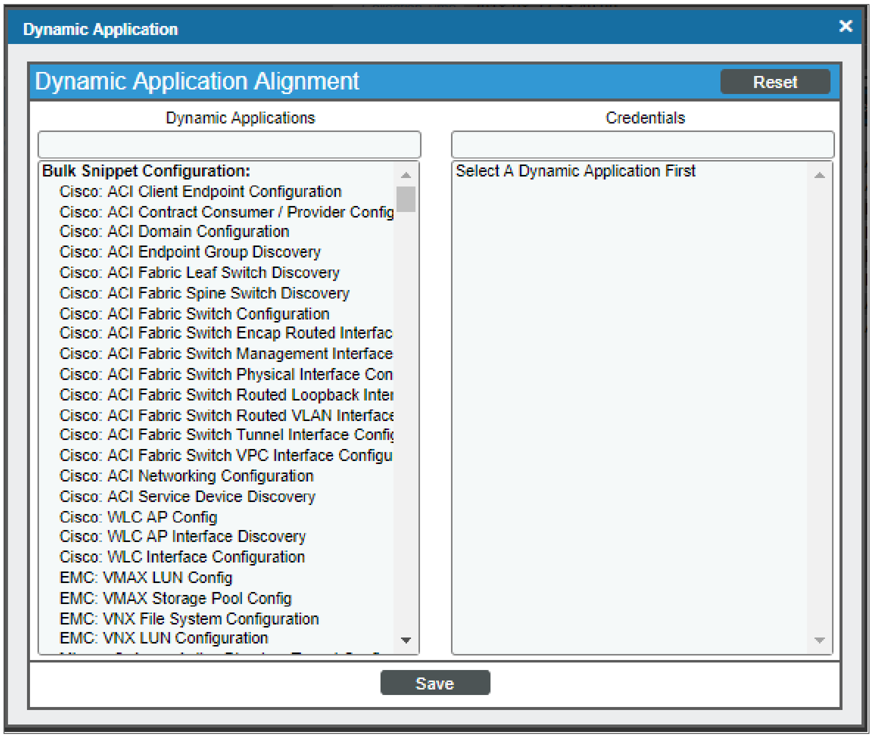
You should see the following Dynamic Applications aligned to the Cisco Meeting Server:

- 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:



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 Inte
- 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

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.

Chapter

17

Cisco: Meraki [API]

Overview

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

NOTE: For more information about the *Cisco: Meraki [API]* PowerPack, see the ***Monitoring Cisco Meraki (API)*** manual.

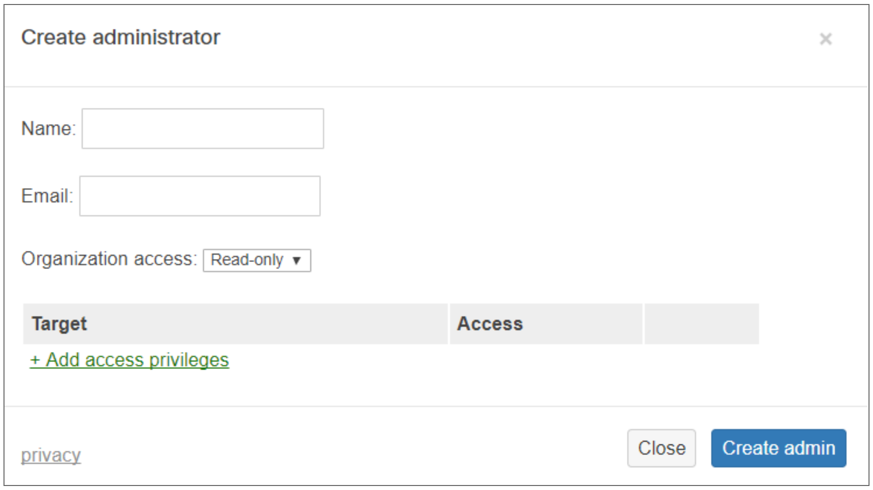
Generating a Cisco Meraki API Key

To configure Cisco Meraki for monitoring using the Meraki API, you must first generate an API key for a read-only Meraki user. You will then enter this user's API key in the ***Basic/Snippet credential*** you create in SL1 to monitor Meraki.

> NOTE: If the read-only user has access to multiple organizations, then SL1 can discover all of those organizations with a single discovery session. In this scenario, each organization is created as a separate Cloud Controller in SL1.
>
> However, if you want each Meraki organization to have its own corresponding ScienceLogic organization in SL1, ScienceLogic recommends creating a unique read-only user account and API key for each organization in Meraki. You can then create separate credentials in SL1 for each Meraki organization using those unique API keys, and then use those credentials to run separate discovery sessions for each organization.

To create a read-only user:

1. Log in to the Cisco Meraki web interface.
2. Go to **Organization > Administrators**, and then click the **[Add admin]** button.
3. On the **Create administrator** page, complete the following fields:


Create administrator

Name:

Email:

Organization access: Read-only

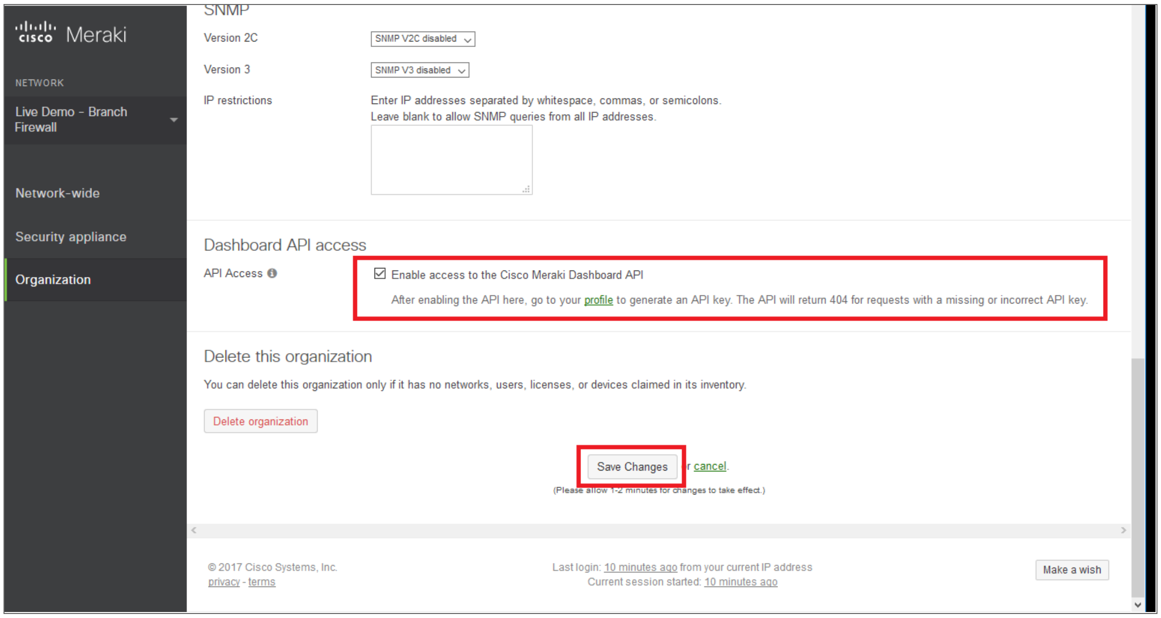
Target	Access	

- ***Name***. Type the user's name.
- ***Email***. Type the user's email address.
- ***Organization access***. Select *Read-only*.

4. Click **[Create admin]**. Cisco Meraki sends an email to the email address provided, describing how the user can complete the registration process. The user must complete those steps before generating the API key.

To generate a Cisco Meraki API key for that read-only user:

1. Log in to the Cisco Meraki web interface as the read-only user.
2. Go to **Organization > Settings**:



SNMP

Version 2C: SNMP V2C disabled

Version 3: SNMP V3 disabled

IP restrictions: Enter IP addresses separated by whitespace, commas, or semicolons. Leave blank to allow SNMP queries from all IP addresses.

Dashboard API access

API Access: ☑ Enable access to the Cisco Meraki Dashboard API

After enabling the API here, go to your profile to generate an API key. The API will return 404 for requests with a missing or incorrect API key.

Delete this organization

You can delete this organization only if it has no networks, users, licenses, or devices claimed in its inventory.

Save Changes r cancel.

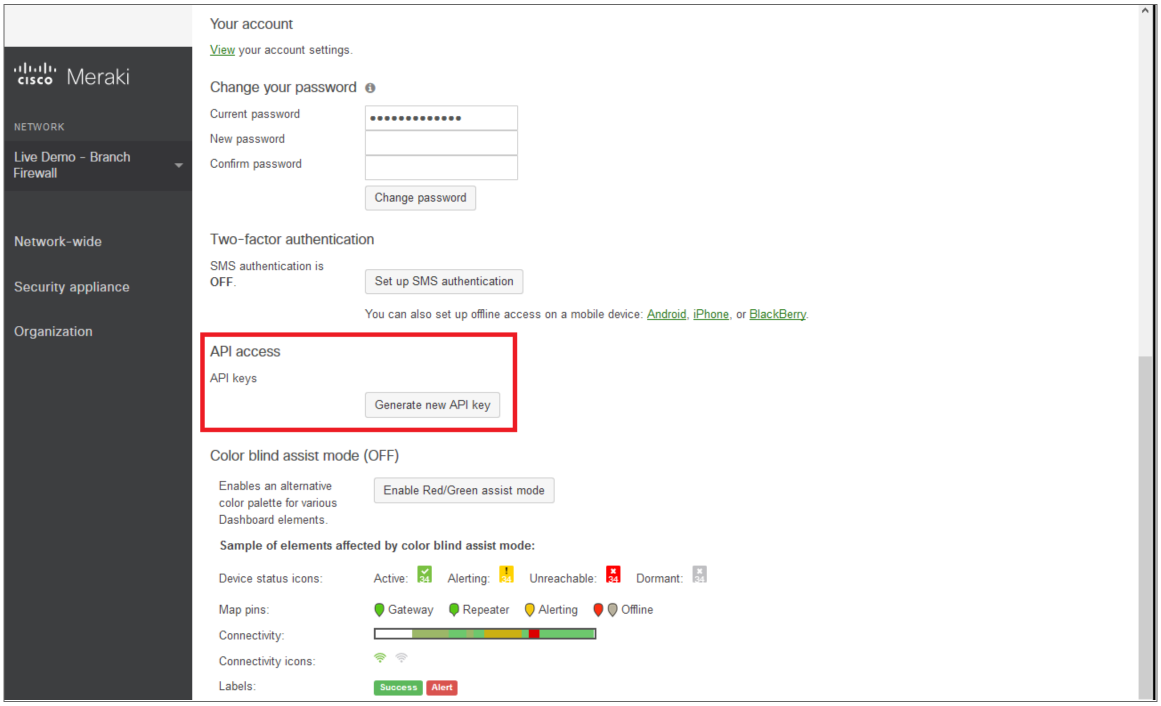
(Please allow 1-2 minutes for changes to take effect.)

© 2017 Cisco Systems, Inc.
privacy - terms

Last login: 10 minutes ago from your current IP address
Current session started: 10 minutes ago

3. In the **Dashboard API access** section, select the **Enable access to the Cisco Meraki Dashboard API** checkbox.
4. Click the **Save Changes** button.
5. Click the **profile** link in the **Dashboard API access** section.

6. In your user profile, navigate to the **API access** section and click the **Generate new API key** button.



Your account

View your account settings.

Change your password

Current password: ••••••••••••••

New password

Confirm password

Change password

Two-factor authentication

SMS authentication is **OFF**.

Set up SMS authentication

You can also set up offline access on a mobile device: Android, iPhone, or BlackBerry.

API access

API keys

Generate new API key

Color blind assist mode (OFF)

Enables an alternative color palette for various Dashboard elements.

Enable Red/Green assist mode

Sample of elements affected by color blind assist mode:

Device status icons: Active: Alerting: Unreachable: Dormant:

Map pins: Gateway Repeater Alerting Offline

Connectivity:

Connectivity icons:

Labels: Success Alert

7. In the **API access** section, the API key appears. Copy and save the key value.

NOTE: API keys are visible only to the user that created them.

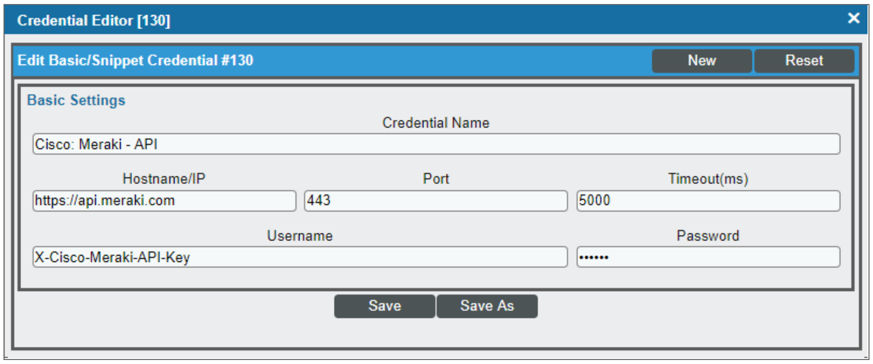
Creating a Basic/Snippet Credential

To configure SL1 to monitor Cisco Meraki systems using the Meraki API, you must create a Basic/Snippet credential. This credential allows the Dynamic Applications in the *Cisco: Meraki [API]* PowerPack to connect with the Cisco Meraki API. An example Basic/Snippet credential that you can edit for your own use is included in the PowerPack.

To create a Basic/Snippet credential:

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

2. Locate the **Cisco: Meraki - API** credential, and then click its wrench icon (). The **Edit Basic/Snippet Credential** modal page appears:



Credential Name: Cisco: Meraki - API

Hostname/IP: https://api.meraki.com

Port: 443

Timeout(ms): 5000

Username: X-Cisco-Meraki-API-Key

Password: ••••••

3. Complete the following fields:
   - ***Credential Name***. Type a new name for the credential.
   - ***Hostname/IP***. Keep the default value.

NOTE: You **must** use the default value in the ***Hostname/IP*** field.

   - ***Port***. Keep the default value.
   - ***Timeout(ms)***. Keep the default value.
   - ***Username***. Keep the default value.
   - ***Password***. Type the *Meraki API key*.

4. Click the **[Save As]** button.
5. When the confirmation message appears, click **[OK]**.

Creating an SNMP V3 Credential

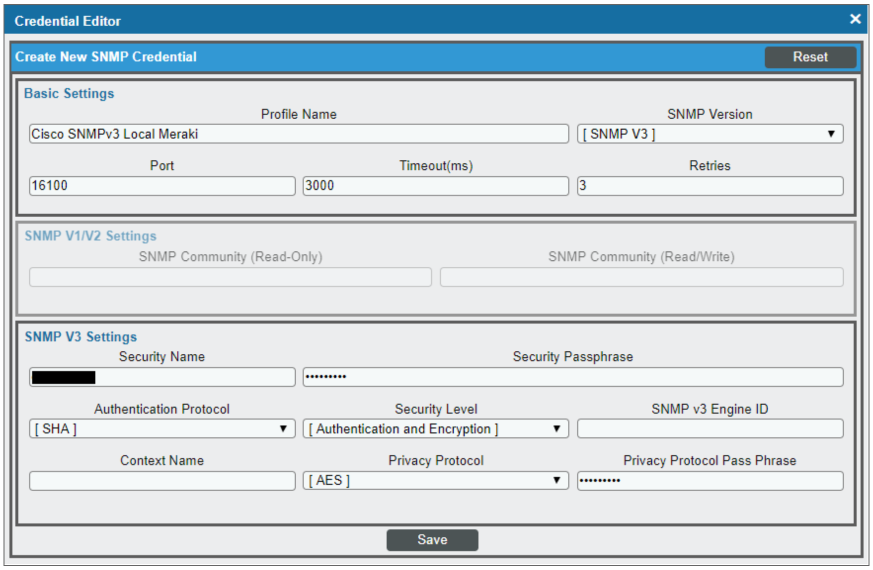
The Dynamic Applications in the *Cisco: Meraki [API]* PowerPack use SNMP to collect some data about Meraki component devices that is not available through the Meraki API. If your Meraki devices are configured for SNMP V3, then you must create an SNMP V3 credential that enables the PowerPack to connect with the devices through a series of Run Book Actions and Automations.

NOTE: If your Meraki system is configured for SNMP V2, you do not need to create an SNMP credential in SL1.

To create an SNMP V3 credential:

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

2. Click the **[Actions]** button, and then select *Create SNMP Credential*. The **Create New SNMP Credential** modal page appears:



Credential Editor ✕

Create New SNMP Credential — Reset

Basic Settings

Profile Name: Cisco SNMPv3 Local Meraki		SNMP Version: [SNMP V3] ▼
Port: 16100	Timeout(ms): 3000	Retries: 3

SNMP V1/V2 Settings

SNMP Community (Read-Only):	SNMP Community (Read/Write):

SNMP V3 Settings

Security Name: [redacted]	Security Passphrase: •••••••••	
Authentication Protocol: [SHA] ▼	Security Level: [Authentication and Encryption] ▼	SNMP v3 Engine ID:
Context Name:	Privacy Protocol: [AES] ▼	Privacy Protocol Pass Phrase: •••••••••

Save

3. Complete the following fields:
   - ***Profile Name***. Type a name for the credential.
   - ***SNMP Version***. Select *SNMP V3*.
   - ***Port***. Type "16100" for the port the platform will use to communicate with the device.
   - ***Timeout***. Type the amount of time, in milliseconds, after which the platform will stop trying to communicate with the device.
   - ***Retries***. Type the number of times the platform will try to authenticate and communicate with the device.
   - ***Security Name***. Type the Meraki device's SNMP V3 username.
   - ***Security Passphrase***. Type the Meraki device's SNMP V3 password.
   - ***Authentication Protocol***. *Select SHA*.
   - ***Security Level***. Select *Authentication and Encryption*.
   - ***SNMP v3 Engine ID***. Leave this field blank.
   - ***Context Name***. Leave this field blank.
   - ***Privacy Protocol***. Select *AES*.
   - ***Privacy Protocol Pass Phrase***. Type the Meraki device's AES privacy key.

4. Click **[Save]**.

Disabling Automatic SNMP V3 Credential Updates

If your Meraki devices are not configured for SNMP V3, you can disable the behavior in the *Cisco: Meraki [API]* PowerPack that searches for an SNMP V3 credential to use and triggers an event and Run Book Actions and Automations that automatically update the credential if one is found.

> **NOTE:** Disabling automatic SNMP V3 credential updates does not affect users whose Meraki devices are configured for SNMP V2.

To disable the automatic SNMP V3 credential update event:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
2. Locate the "Cisco: Meraki Network Discovery [API]" Dynamic Application and click its wrench icon (🔧).
3. Click the **[Snippets]** tab, and then click the wrench icon (🔧) for the "Network Discovery" snippet.
4. Edit the "Network Discovery" snippet to change `snmp_update=True` to `snmp_update=False`.
5. Click **[Save]**.

> CAUTION: If your Meraki devices are configured for SNMP V3 but you have the `snmp_update=False` value in the "Network Discovery" snippet, SL1 will not be able to collect the SNMP data for the "Cisco: Meraki Interface Performance [API]" and "Cisco: Meraki Device Configuration [API]" Dynamic Applications. If you want to collect this data, you will need to change the value back to `snmp_update=True` to enable SL1 to update the SNMP V3 credential and collect SNMP data from the Meraki devices.

Creating a SOAP/XML Credential

If you access Meraki systems through a third-party proxy server, you can create a SOAP/XML credential to enable the Dynamic Applications in the *Cisco: Meraki [API]* PowerPack to connect with the Cisco Meraki API via the proxy server.

Similarly, if you want to discover only some selected devices, you can create a SOAP/XML credential that specifies tag values that the Dynamic Applications in the *Cisco: Meraki [API]* PowerPack can use to determine which devices should be discovered.

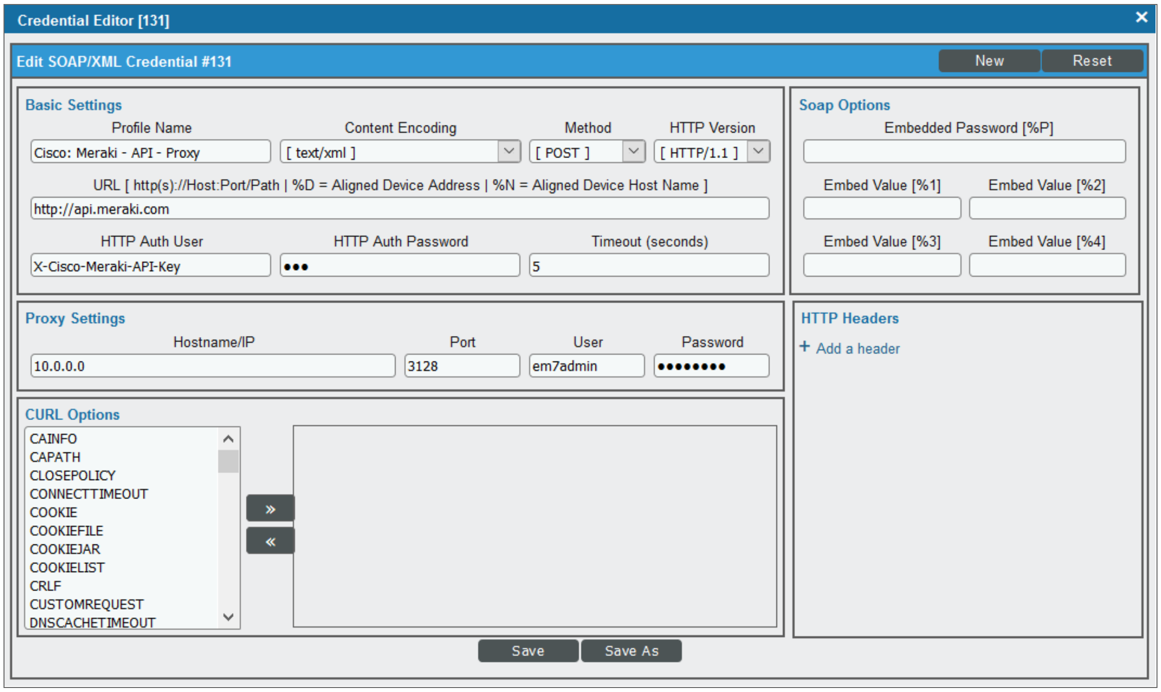
Two example SOAP/XML credentials that you can edit for your own use are included in the PowerPack:

- **Cisco: Meraki - API - Proxy**, for users who connect to Meraki through a third-party proxy server
- **Cisco: Meraki - API (Selective)**, for users who want to discover only some selected devices based on tag values

To define an SOAP/XML credential:

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

2. Locate the **Cisco: Meraki - API - Proxy** or **Cisco: Meraki - API (Selective)** credential and click its wrench icon ( ). The **Credential Editor** modal page appears:



Profile Name: Cisco: Meraki - API - Proxy

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: http://api.meraki.com

HTTP Auth User: X-Cisco-Meraki-API-Key

HTTP Auth Password: ●●●

Timeout (seconds): 5

Hostname/IP: 10.0.0.0

Port: 3128

User: em7admin

Password: ●●●●●●●●

3. Enter values in the following fields:

Basic Settings

- ***Profile Name***. Type a new name for your Meraki credential.
- ***HTTP Auth Password***. Type the *Meraki API key.*

> NOTE: You can use the default values for the remaining ***Basic Settings*** fields. You **must** use the default value in the **URL** field.

Proxy Settings

> NOTE: You must complete the ***Proxy Settings*** fields only if you connect to the Meraki API through a third-party proxy server. If you do not use a proxy to connect to Meraki, then you can leave these fields blank.

- ***Hostname/IP***. Type the server's hostname or IP address.
- ***Port***. Type the port on the proxy server to which you will connect.
- ***User***. Type the username used to access the proxy server.

- ***Password***. Type the password used to access the proxy server.

HTTP Headers

NOTE: You can add and complete the ***HTTP Headers*** fields if you want to discover only some selected devices based on tag values. If you want to discover all Meraki devices, then you can leave these fields blank.

- ***Add a header***. Click **[Add a header]** once if you want to include tag values for SL1 to match when it discovers Meraki devices, or click **[Add a header]** twice if you want to include tag values and specify that tag-matching should be case-insensitive. In the blank fields that appear, do one or both of the following:
  - Type "tags:" in the first field, followed by one or more tag values. You can include multiple tag values in a string, using comma separators and no spaces. For example: "tags:value1,value2,value3".
  - Type "regex:IGNORECASE" in the second field if you want SL1 to match the tag values regardless of case.

NOTE: If you are using a tag to discover a device and want to discover that device's network, the device and it's network must have the same tag applied.

NOTE: Tag values can include wildcard characters.

NOTE: After initial discovery, you can add more tag values and run discovery again to discover additional component devices. However, if you remove tag values and then run discovery again, the component devices that had been discovered based on the removed tag values will be updated to an unavailable state.

4. Click the **[Save As]** button, and then click **[OK]**.

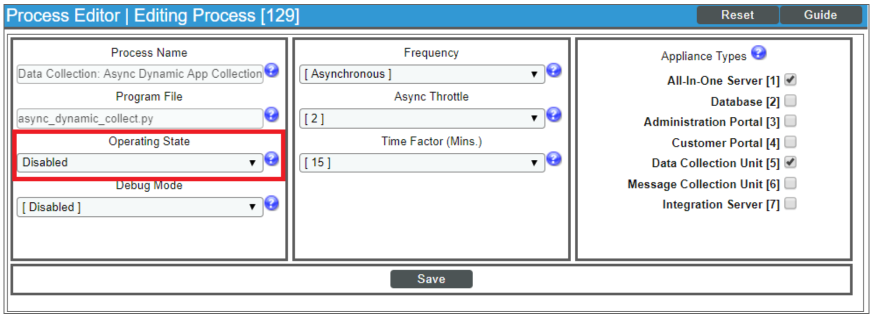
Disabling Asynchronous Dynamic Application Collection

If the Meraki system you want to monitor consists of more than 200 devices, you must disable the "Data Collection: Async Dynamic App Collection" process before discovering your Meraki system.

NOTE: Disabling asynchronous Dynamic Application collection increases the amount of time it takes the ScienceLogic platform to discover all of the component devices in your Meraki system.

To disable asynchronous Dynamic Application collection:

1. Go to the **Process Manager** page (System > Settings > Admin Processes, or System > Settings > Processes in the SL1 classic user interface).
2. Use the ***Process Name*** filter field to search for the "Data Collection: Async Dynamic App Collection" process, and then click its wrench icon ( ). The **Process Editor** page appears.



Process Editor | Editing Process [129]

Process Name: Data Collection: Async Dynamic App Collection

Program File: async_dynamic_collect.py

Operating State: Disabled

Debug Mode: [Disabled]

Frequency: [Asynchronous]

Async Throttle: [2]

Time Factor (Mins.): [15]

Appliance Types

- All-In-One Server [1] ☑
- Database [2] ☐
- Administration Portal [3] ☐
- Customer Portal [4] ☐
- Data Collection Unit [5] ☑
- Message Collection Unit [6] ☐
- Integration Server [7] ☐

3. In the ***Operating State*** field, select *Disabled*.
4. Click **[Save]**.

Re-enabling Asynchronous Dynamic Application Collection

If you no longer want to monitor Meraki devices in SL1 and you want to return the system to its original state with asynchronous Dynamic Application collection re-enabled, you must first delete all Meraki devices from the platform. You must then clear the Database Server or Data Collector of any asynchronous processes that are already queued. Failing to do these steps can result in the platform ceasing all data collection until those asynchronous processes are executed.

To re-enable asynchronous Dynamic Application collection:

1. Navigate to the Database Server by typing "<IP address>:8008" into your browser address bar.
2. Log in to the Database Server. The phpMyAdmin browser appears.
3. Select the database from the drop-down ***Database*** field, and then select the **master_logs** database.
4. In the **master_logs** database, select the **spool_process** table on the left menu, and then click the **[SQL]** tab.
5. Run the following query to clear out the processes on the database:

```
DELETE FROM 'spool_process' WHERE 'proc' = 129 AND 'state' != 0;
```

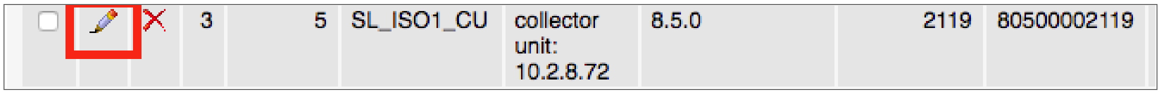
6. Click **[OK]** at the prompt. Many rows should have been deleted from the table.

   If you are using a distributed ScienceLogic system, continue with step 7. Otherwise, go to step 14.

7. In the left menu of the phpMyAdmin browser, select the Data Collector appliance where Meraki devices were discovered.

   If the IP address of the Data Collector appears in the upper left-hand corner of the phpMyAdmin browser, go to step 12. Otherwise, if you receive a MySQL error message that your access is denied, continue with step 8.

8. In the Database Server, navigate to the **Master** database and then select the **system_settings_licenses** table.
9. Click **[Browse]** in the upper left-hand side of the page and then identify the Data Collector appliance.
10. Click the **edit** button for the Data Collector:



□	✎	✕	3	5	SL_ISO1_CU	collector unit: 10.2.8.72	8.5.0	2119	80500002119

11. Locate the **db_user** and **db_pass** fields. In those fields, type the same credentials as the Database Server.
12. Click **[Go]**. Wait a few seconds before trying to access the Data Collector in the phpMyAdmin browser. When you do so, the IP address of the Data Collector should appear in the upper left-hand corner of the phpMyAdmin browser.
13. Repeat steps 3-6 on the Data Collector. If successful, many rows should have been deleted from the **spool_process** table.
14. In SL1, go to the **Process Manager** page (System > Settings > Admin Processes, or System > Settings > Processes in the SL1 classic user interface).
15. Use the ***Process Name*** filter field to search for the "Data Collection: Async Dynamic App Collection" process, and then click its wrench icon (🔧). The **Process Editor** page appears.
16. In the ***Operating State*** field, select *Enabled*, and then click **[Save]**.

Discovering Cisco Meraki Component Devices

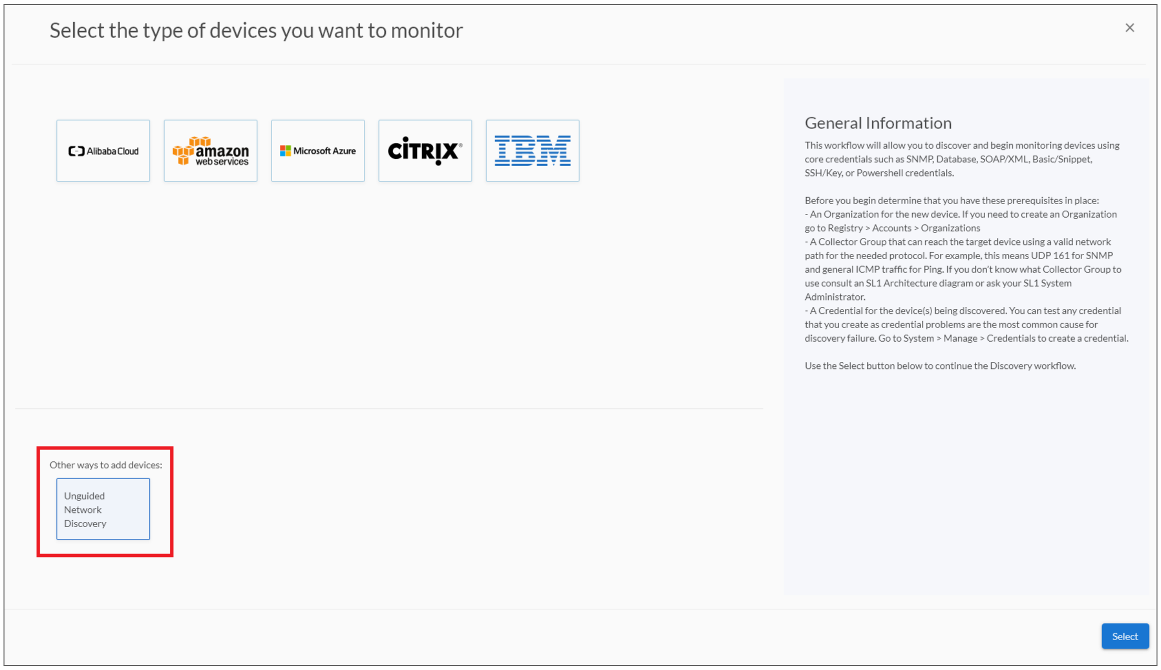
To model and monitor your Cisco Meraki devices, you must run a discovery session to discover your Meraki environment.

When the discovery session first completes, the Meraki system is initially discovered as a pingable physical device. The Run Book Action and Automation policies in the *Cisco: Meraki [API]* PowerPack then create a Meraki Cloud Controller virtual device that acts as the root device for your Meraki system. The Dynamic Applications included in the PowerPack then automatically align to the Cloud Controller virtual device to discover, model, and monitor the remaining Meraki devices.

NOTE: If you have a pre-existing device component with an identical name to a Meraki Organization, the "Cisco: Meraki Cloud Controller Discovery" Dynamic Application will show you a false positive message, indicating that the device component was created, but it will fail to create one. This is because the Dynamic Application checks for the existence of the component name and if it finds a matching one, a new component is not created.

To discover the Meraki devices that you want to monitor:

1. On the **Devices** page (🖳) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears:


Select the type of devices you want to monitor
×
Alibaba Cloud
amazon web services
Microsoft Azure
CITRIX
IBM
Other ways to add devices:
Unguided Network Discovery
Select

General Information

This workflow will allow you to discover and begin monitoring devices using core credentials such as SNMP, Database, SOAP/XML, Basic/Snippet, SSH/Key, or Powershell credentials.

Before you begin determine that you have these prerequisites in place:
- An Organization for the new device. If you need to create an Organization go to Registry > Accounts > Organizations
- A Collector Group that can reach the target device using a valid network path for the needed protocol. For example, this means UDP 161 for SNMP and general ICMP traffic for Ping. If you don't know what Collector Group to use consult an SL1 Architecture diagram or ask your SL1 System Administrator.
- A Credential for the device(s) being discovered. You can test any credential that you create as credential problems are the most common cause for discovery failure. Go to System > Manage > Credentials to create a credential.

Use the Select button below to continue the Discovery workflow.

2. Click the **[Unguided Network Discovery]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.

3. Click **[Select]**. The **Add Devices** page appears.

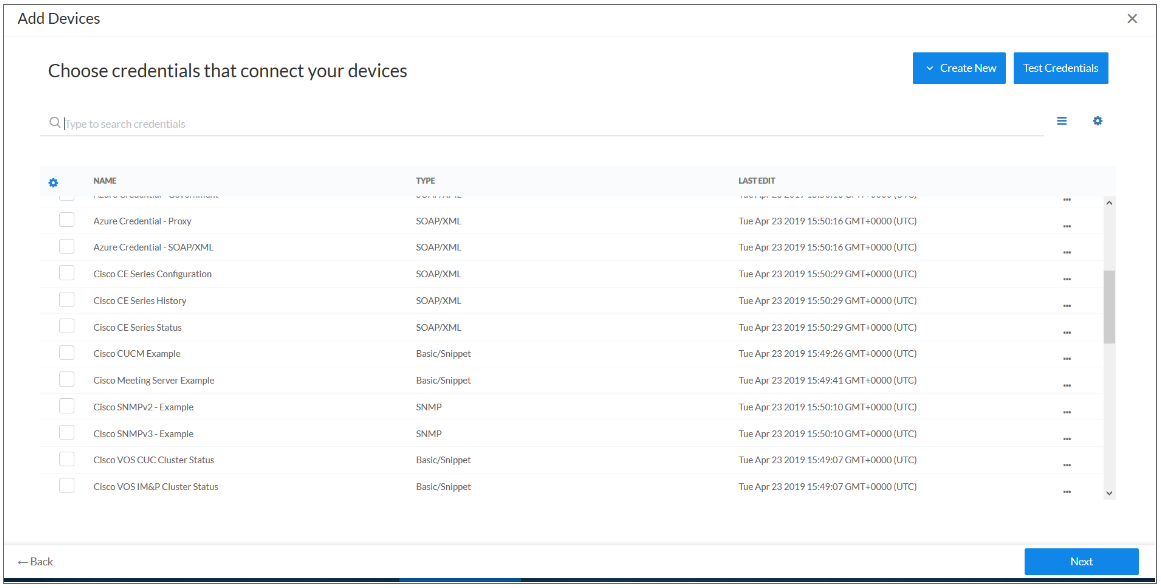
4. Complete the following fields:

   - ***Name***. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.

   - ***Description***. Optional. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **[Discovery Sessions]** tab.

   - ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered devices

5. Click **[Next]**. The **Credentials** page of the **Add Devices** wizard appears:



Add Devices

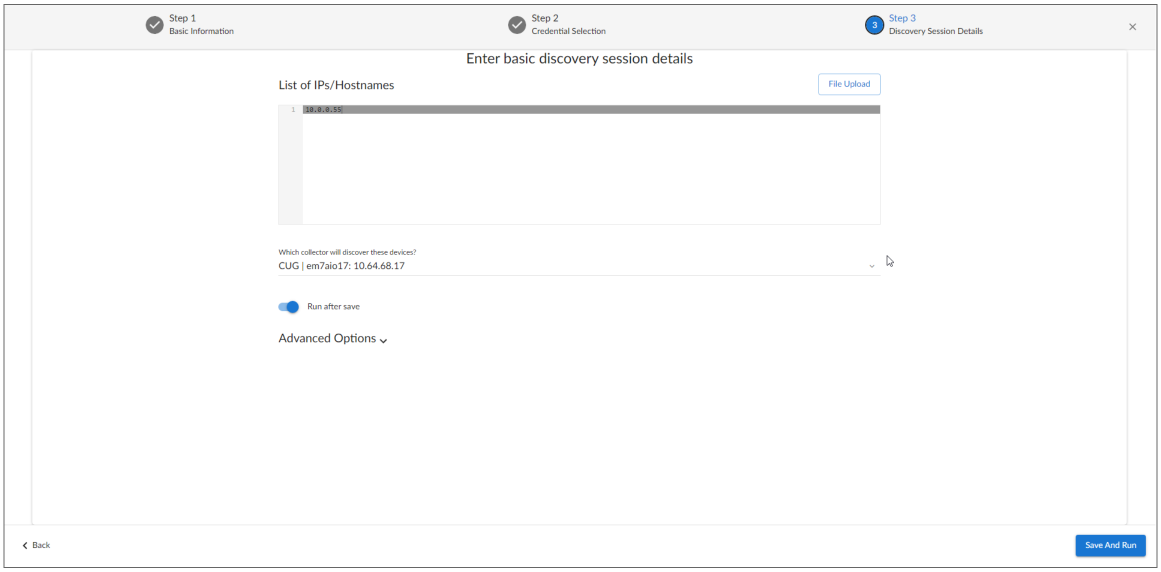
Choose credentials that connect your devices

	NAME	TYPE	LAST EDIT
□	Azure Credential - Proxy	SOAP/XML	Tue Apr 23 2019 15:50:16 GMT+0000 (UTC)
□	Azure Credential - SOAP/XML	SOAP/XML	Tue Apr 23 2019 15:50:16 GMT+0000 (UTC)
□	Cisco CE Series Configuration	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)
□	Cisco CE Series History	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)
□	Cisco CE Series Status	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)
□	Cisco CUCM Example	Basic/Snippet	Tue Apr 23 2019 15:49:26 GMT+0000 (UTC)
□	Cisco Meeting Server Example	Basic/Snippet	Tue Apr 23 2019 15:49:41 GMT+0000 (UTC)
□	Cisco SNMPv2 - Example	SNMP	Tue Apr 23 2019 15:50:10 GMT+0000 (UTC)
□	Cisco SNMPv3 - Example	SNMP	Tue Apr 23 2019 15:50:10 GMT+0000 (UTC)
□	Cisco VOS CUC Cluster Status	Basic/Snippet	Tue Apr 23 2019 15:49:07 GMT+0000 (UTC)
□	Cisco VOS IM&P Cluster Status	Basic/Snippet	Tue Apr 23 2019 15:49:07 GMT+0000 (UTC)

6. On the **Credentials** page, locate and select the *Basic/Snippet credential* you created for the Cisco Meraki devices.

NOTE: Do not select a credential in the ***SNMP Credentials*** field, even if you created an SNMP V3 credential for your Meraki devices. The Run Book Action and Automation policies included in the *Cisco: Meraki [API]* PowerPack automatically gather and use the necessary SNMP credential information during discovery.

7. Click **[Next]**. The **Discovery Session Details** page of the **Add Devices** wizard appears:



Enter basic discovery session details

List of IPs/Hostnames

```
10.0.0.55
```

Which collector will discover these devices?
CUG | em7aio17: 10.64.68.17

● Run after save

Advanced Options

8. Complete the following fields:

- ***List of IPs/Hostnames***. Type"api.meraki.com".
- ***Which collector will monitor these devices?***. Required. Select an existing collector to monitor the discovered devices.
- ***Run after save***. Select this option to run this discovery session as soon as you save the session.

  In the **Advanced options** section, click the down arrow icon (⌄) to complete the following fields:

  - ***Discover Non-SNMP***. Enable this setting.
  - ***Model Devices***. Enable this setting.

9. Click **[Save and Run]** if you enabled the Run after save setting, or **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.
10. If you selected the **Run after save** option on this page, the discovery session runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page includes a link to the **Device Investigator** page for the discovered device.
11. Repeat the above steps for every set of Cisco Meraki devices you want to monitor, using a different credential for each set of devices.

NOTE: ScienceLogic recommends that you delete the physical pingable Meraki device after the platform creates the Cloud Controller virtual device that serves as the Meraki system root device.

NOTE: You can edit the ***Device Name*** of the Meraki Cloud Controller virtual device from the **Device Investigator** page (**Devices** > select the device > click the **[Edit]** button) for that device. This enables you to change the root device's name so that it matches the organization name as the Meraki Controller defines it. The *Cisco: Meraki [API]* PowerPack cannot discover multiple organizations with the same name.

Discovering Cisco: Meraki Component Devices in the SL1 Classic User Interface

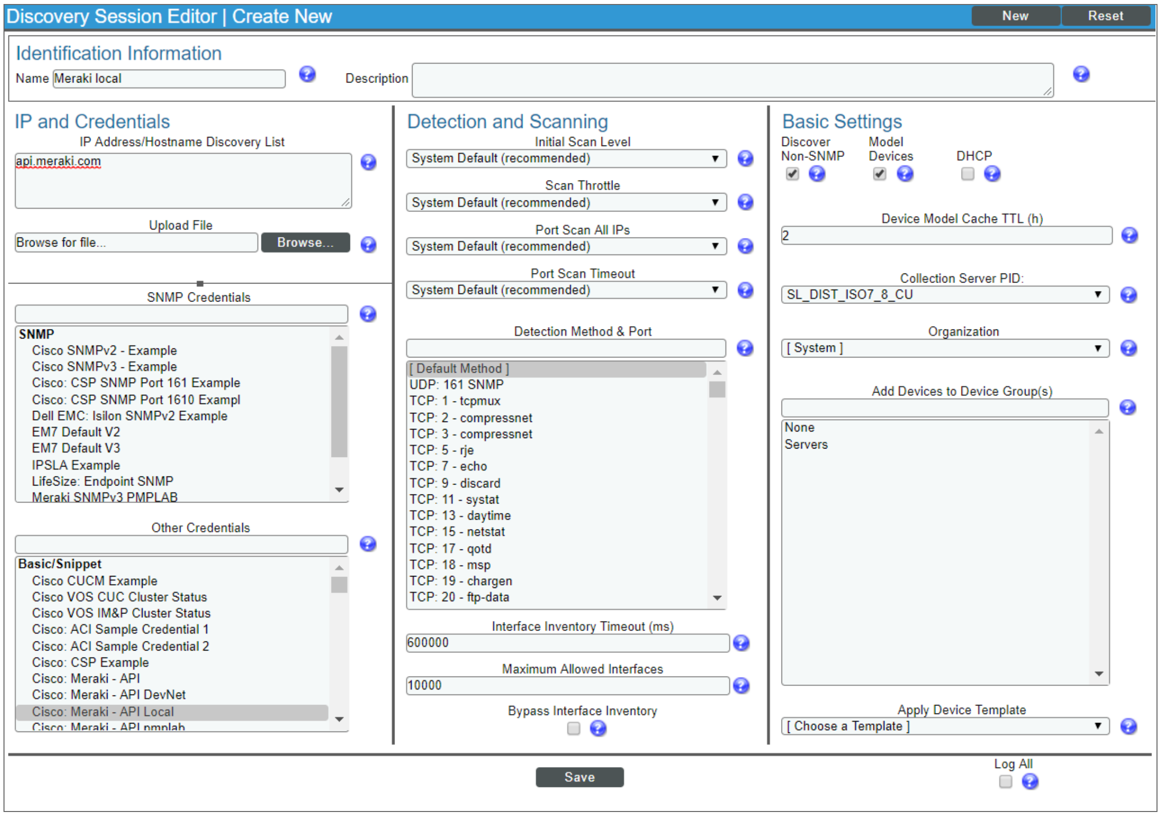
To model and monitor your Cisco Meraki devices, you must run a discovery session to discover your Meraki environment.

When the discovery session first completes, the Meraki system is initially discovered as a pingable physical device. The Run Book Action and Automation policies in the *Cisco: Meraki [API]* PowerPack then create a Meraki Cloud Controller virtual device that acts as the root device for your Meraki system. The Dynamic Applications included in the PowerPack then automatically align to the Cloud Controller virtual device to discover, model, and monitor the remaining Meraki devices.

NOTE: If you have a pre-existing device component with an identical name to a Meraki Organization, the "Cisco: Meraki Cloud Controller Discovery" Dynamic Application will show you a false positive message, indicating that the device component was created, but it will fail to create one. This is because the Dynamic Application checks for the existence of the component name and if it finds a matching one, a new component is not created.

To discover the Meraki devices that you want to monitor:

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



Discovery Session Editor | Create New

Identification Information

Name: Meraki local

Description:

IP and Credentials

IP Address/Hostname Discovery List: api.meraki.com

Upload File: Browse for file...

SNMP Credentials

SNMP
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Cisco: CSP SNMP Port 161 Example
Cisco: CSP SNMP Port 1610 Exampl
Dell EMC: Isilon SNMPv2 Example
EM7 Default V2
EM7 Default V3
IPSLA Example
LifeSize: Endpoint SNMP
Meraki SNMPv3 PMPLAB

Other Credentials

Basic/Snippet
Cisco CUCM Example
Cisco VOS CUC Cluster Status
Cisco VOS IM&P Cluster Status
Cisco: ACI Sample Credential 1
Cisco: ACI Sample Credential 2
Cisco: CSP Example
Cisco: Meraki - API
Cisco: Meraki - API DevNet
Cisco: Meraki - API Local
Cisco: Meraki - API pmplab

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
TCP: 17 - qotd
TCP: 18 - msp
TCP: 19 - chargen
TCP: 20 - ftp-data

Interface Inventory Timeout (ms): 600000

Maximum Allowed Interfaces: 10000

Bypass Interface Inventory: □

Basic Settings

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

Device Model Cache TTL (h): 2

Collection Server PID: SL_DIST_ISO7_8_CU

Organization: [System]

Add Devices to Device Group(s)

None
Servers

Apply Device Template: [Choose a Template]

Log All: □

- ***Name***. Type a name for the discovery session.
- ***IP Address/Hostname Discovery List***. Type "api.meraki.com".
- ***Other Credentials***. Select the Basic/Snippet credential you created for Meraki.
- ***Discover Non-SNMP***. Select this checkbox.
- ***Model Devices***. Select this checkbox.

NOTE: Do not select a credential in the ***SNMP Credentials*** field, even if you created an SNMP V3 credential for your Meraki devices. The Run Book Action and Automation policies included in the *Cisco: Meraki [API]* PowerPack automatically gather and use the necessary SNMP credential information during discovery.

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 **[Save]**, 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 virtual device is created and the Cisco Meraki devices are discovered, click the device icon ( ) to view the **Device Properties** page for each device.
8. Repeat steps 2-7 for every set of Cisco Meraki devices you want to monitor, using a different credential for each set of devices.

NOTE: ScienceLogic recommends that you delete the physical pingable Meraki device after the platform creates the Cloud Controller virtual device that serves as the Meraki system root device.

NOTE: You can edit the ***Device Name*** of the Meraki Cloud Controller virtual device from the **Device Properties** page (Registry > Devices > wrench icon). This enables you to change the root device's name so that it matches the organization name as the Meraki Controller defines it. The *Cisco: Meraki [API]* PowerPack cannot discover multiple organizations with the same name.

Creating Events from Cisco Meraki Emails

The *Cisco: Meraki [API]* PowerPack includes Event Policies that can generate events in SL1 based on emails that Cisco Meraki sends to SL1.

For SL1 to process events from inbound emails, you must configure your Meraki devices to send email to SL1 using certain formatting rules.

You must then enable SL1 to generate events from those inbound Meraki emails.

If configured properly, when SL1 domain receives an email with body text that matches a Meraki network component device name and a subject that matches the regular expression (RegEx) pattern of one of the PowerPack's Event Policies, SL1 will generate an event aligned to that network component device.

NOTE: Events from email are always aligned to network devices, even when the email includes references to one or more sub-component devices below the network device.

CAUTION: The email Event Policies included in the *Cisco: Meraki [API]* PowerPack each have an expiry delay setting that specifies the amount of time after which an active event is automatically cleared from SL1 if the event has not reoccurred. However, SL1 clearing an event for reaching its expiry delay setting does not mean that the initial condition that caused the event has been resolved.

Formatting Inbound Emails

Inbound emails must meet the following requirements to be processed as events by SL1:

- The email must be sent to the following address:

  ```
  notify@SL1-domain-name
  ```

  Where "SL1-domain-name" is one of the fully qualified domain names of the Database Server or All-In-One Appliance that is entered in the ***Authorized Email Domains*** field in the **Email Settings** (System > Settings > Email) page.

- The "from" address used by the external device must be "alerts-noreply@meraki.com" for non-maintenance events, "support-noreply@meraki.com" for maintenance events, or otherwise match an address defined in the ***Originator Address*** field in an email redirection policy on the **Emailer Redirection** page Events > Inbound Email, or Registry > Events > Inbound Email in the SL1 classic user interface).
- The email subject line must begin with "Alert for" or "Scheduled maintenance for" and match the regular expression (RegEx) pattern of one of the Event Policies included in the *Cisco: Meraki [API]* PowerPack.
- The email body must include the name of a network device monitored by the SL1 system.

  The following RegEx patterns are used:

  - For scheduled maintenance emails:

  ```
  (Scheduled maintenance for)\s((network\s|\d\snetworks\sin\sorganization\s)"([a-zA-Z0-9_\-\.]+).*")
  ```

  - For all other emails:

  ```
  (Alert for)\s*([a-zA-Z0-9_\-\.]+)\s*
  ```

NOTE: There must be a space between the RegEx pattern and the IP address, hostname, or device ID.

NOTE: The Event Policies included in the *Cisco: Meraki [API]* PowerPack ***do not*** include RegEx patterns "out of the box". Users can add or modify Event Policy RegEx patterns to best suit their needs.

NOTE: Emails that do not match the RegEx pattern of any Meraki Event Policy will generate a message in the system log. Emails that do not match the name of any component device in SL1 will not generate any events or messages.

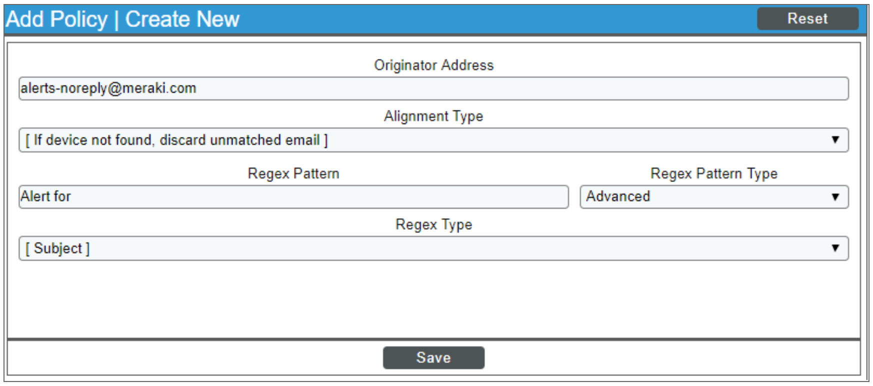
NOTE: You can specify how an Event from Email policy will match a RegEx to a device name in the **Behavior Settings** page (System > Settings > Behavior). For more information, see the ***Configuring Inbound Email*** manual.

Enabling Inbound Email Alerts

After you have ensured that inbound Meraki emails are formatted correctly, you must enable SL1 to generate events from the inbound Meraki emails.

To do so:

1. Go to the **Emailer Redirection** page (Events > Inbound Email, or Registry > Events > Inbound Email in the SL1 classic user interface), and then click the **[Create]** button. The **Add Policy** modal page appears.
2. Complete the following fields:



Add Policy | Create New

Originator Address: alerts-noreply@meraki.com

Alignment Type: [If device not found, discard unmatched email]

Regex Pattern: Alert for

Regex Pattern Type: Advanced

Regex Type: [Subject]

   - ***Originator Address***. Type "alerts-noreply@meraki.com".
   - ***Alignment Type***. Select *If device not found, discard unmatched email*.
   - ***Regex Pattern***. Type "Alert for" or "Scheduled maintenance for network".
   - ***Regex Pattern Type***. Select *Advanced*.
   - ***Regex Type***. Select *Subject*.

3. Click **[Save]**.

NOTE: For more information about generating events from inbound emails, see the ***Configuring Inbound Email*** manual.

Chapter 18

Cisco: Tetration

Overview

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

> NOTE: For more information about the *Cisco: Tetration* PowerPack, see the ***Monitoring Cisco Tetration Analytics*** manual.

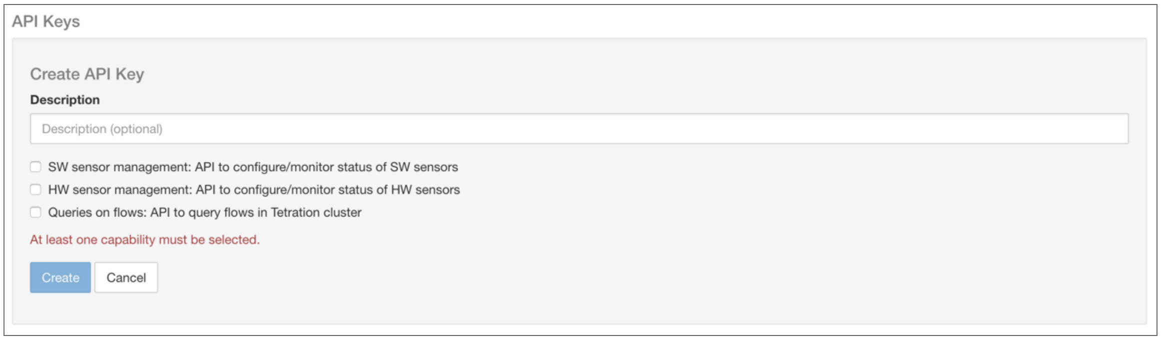
Configuring Cisco Tetration Analytics for Monitoring

Before you can use SL1 to monitor Cisco Tetration Analytics, you must first generate a Tetration Analytics API key and secret password. You will then use this API key and secret password to ***create a Basic/Snippet credential*** that enables SL1 to communicate with and monitor Tetration Analytics clusters.

To configure Cisco Tetration Analytics for monitoring:

1. Log in to the Cisco Tetration Analytics web interface with a **site_admin** or **customer_support** account.
2. Go to **Settings > API Keys**, and then click **[Create API Key]**.

3. Type a ***Description*** and select the checkbox of the appropriate API key capability.



API Keys

Create API Key

Description

Description (optional)

□ SW sensor management: API to configure/monitor status of SW sensors

□ HW sensor management: API to configure/monitor status of HW sensors

□ Queries on flows: API to query flows in Tetration cluster

At least one capability must be selected.

4. Click **[Create]**.
5. The API key appears. Copy and save the key value.

> **NOTE:** API keys are visible only to the user that created them.

6. The secret password appears. Copy and save the password value.

> WARNING: The secret password value appears only once and cannot be recovered. If you forget or lose the password value, you must generate a new API key with a different password value.

Creating a Basic/Snippet Credential for Cisco Tetration Analytics

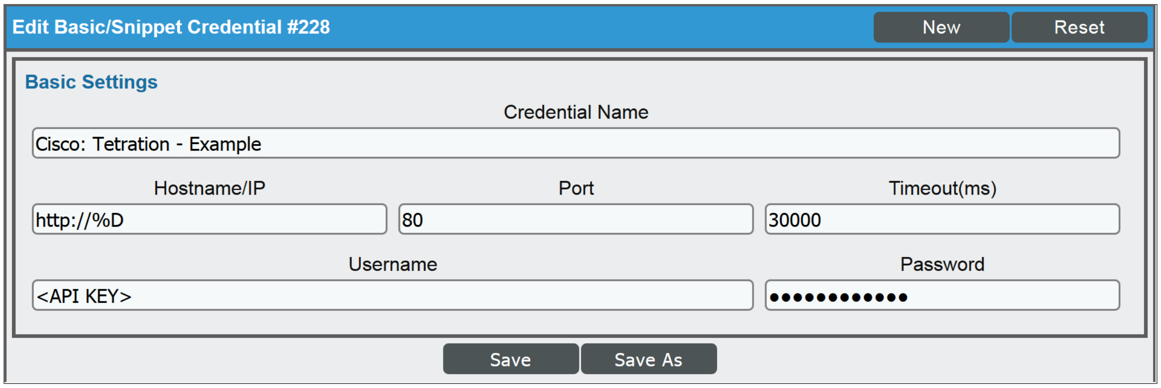
To monitor Cisco Tetration Analytics in SL1, you must configure a Basic/Snippet credential that SL1 can use to discover and communicate with Tetration Analytics clusters.

The *Cisco: Tetration* PowerPack includes an example credential (*Cisco: Tetration - Example*) that you can use to create a Basic/Snippet credential for monitoring Tetration Analytics.

To configure a credential for Cisco Tetration Analytics:

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

2. Click the wrench icon (🔧) for *Cisco: Tetration - Example*. The **Credential Editor** page appears:



Credential Name: Cisco: Tetration - Example

Hostname/IP: http://%D

Port: 80

Timeout(ms): 30000

Username: <API KEY>

Password: ●●●●●●●●●●●●

3. Supply values in the following fields:

   - ***Credential Name***. Type a new name for the credential.
   - ***Hostname/IP***. Type "http://%D".
   - ***Username***. Type the Tetration Analytics API key ***you previously generated.***
   - ***Password***. Type the Tetration Analytics API secret password you previously generated.

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

Discovering Cisco Tetration Analytics Devices

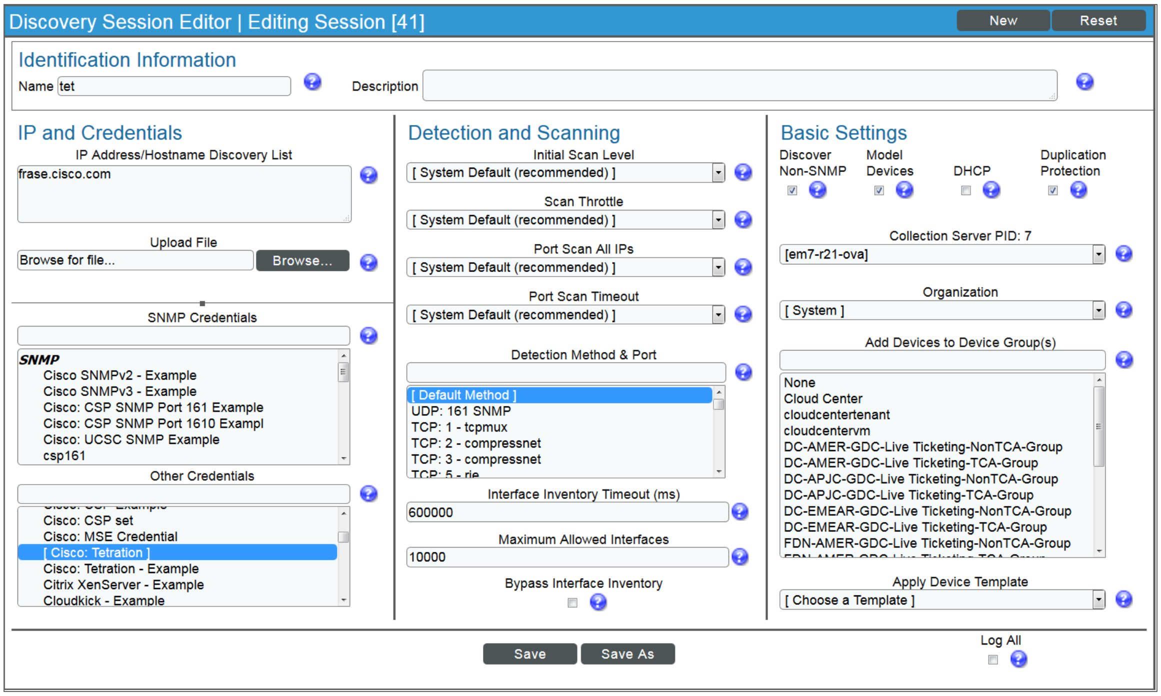
To monitor Cisco Tetration Analytics devices, you must run a discovery session to discover the Tetration Analytics clusters that SL1 will use as the root devices for monitoring the devices.

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

To discover the Tetration Analytics clusters that you want to monitor:

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

3. In the **Discovery Session Editor** page, define values in the following fields:



Discovery Session Editor | Editing Session [41]

Identification Information

Name: tet

Description:

IP and Credentials

IP Address/Hostname Discovery List: frase.cisco.com

Upload File: Browse for file...

SNMP Credentials

SNMP
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Cisco: CSP SNMP Port 161 Example
Cisco: CSP SNMP Port 1610 Exampl
Cisco: UCSC SNMP Example
csp161

Other Credentials

Cisco: CSP set
Cisco: MSE Credential
[Cisco: Tetration]
Cisco: Tetration - Example
Citrix XenServer - Example
Cloudkick - Example

Detection and Scanning

Initial Scan Level: [System Default (recommended)]

Scan Throttle: [System Default (recommended)]

Port Scan All IPs: [System Default (recommended)]

Port Scan Timeout: [System Default (recommended)]

Detection Method & Port

[Default Method]
UDP: 161 SNMP
TCP: 1 - tcpmux
TCP: 2 - compressnet
TCP: 3 - compressnet
TCP: 5 - rje

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: 7: [em7-r21-ova]

Organization: [System]

Add Devices to Device Group(s)

None
Cloud Center
cloudcentertenant
cloudcentervm
DC-AMER-GDC-Live Ticketing-NonTCA-Group
DC-AMER-GDC-Live Ticketing-TCA-Group
DC-APJC-GDC-Live Ticketing-NonTCA-Group
DC-APJC-GDC-Live Ticketing-TCA-Group
DC-EMEAR-GDC-Live Ticketing-NonTCA-Group
DC-EMEAR-GDC-Live Ticketing-TCA-Group
FDN-AMER-GDC-Live Ticketing-NonTCA-Group

Apply Device Template: [Choose a Template]

Log All: ☐

- ***IP Address/Hostname Discovery List***. Enter the IP address(es) or hostname(s) for the cluster root device(s) you want to discover.
- ***Other Credentials***. Select the *Basic/Snippet credential you created* for the device clusters.
- ***Discover Non-SNMP***. 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, you can click the device icon (🖥) to view the **Device Properties** page for each device.

Chapter

19

Cisco: UC Ancillary

Overview

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

NOTE: For more information about the *Cisco: UC Ancillary* PowerPack, see the ***Monitoring Cisco Unified Communications Ancillary Devices*** manual.

Prerequisites for Monitoring Ancillary Cisco Unified Communications Devices

To configure SL1 to monitor ancillary Cisco Unified Communications (UC) devices using the *Cisco: UC Ancillary* PowerPack, you must have already properly installed and configured the ancillary Cisco UC devices that you want to monitor. You must also note the following information, as appropriate, for each of the ancillary UC devices you want to monitor:

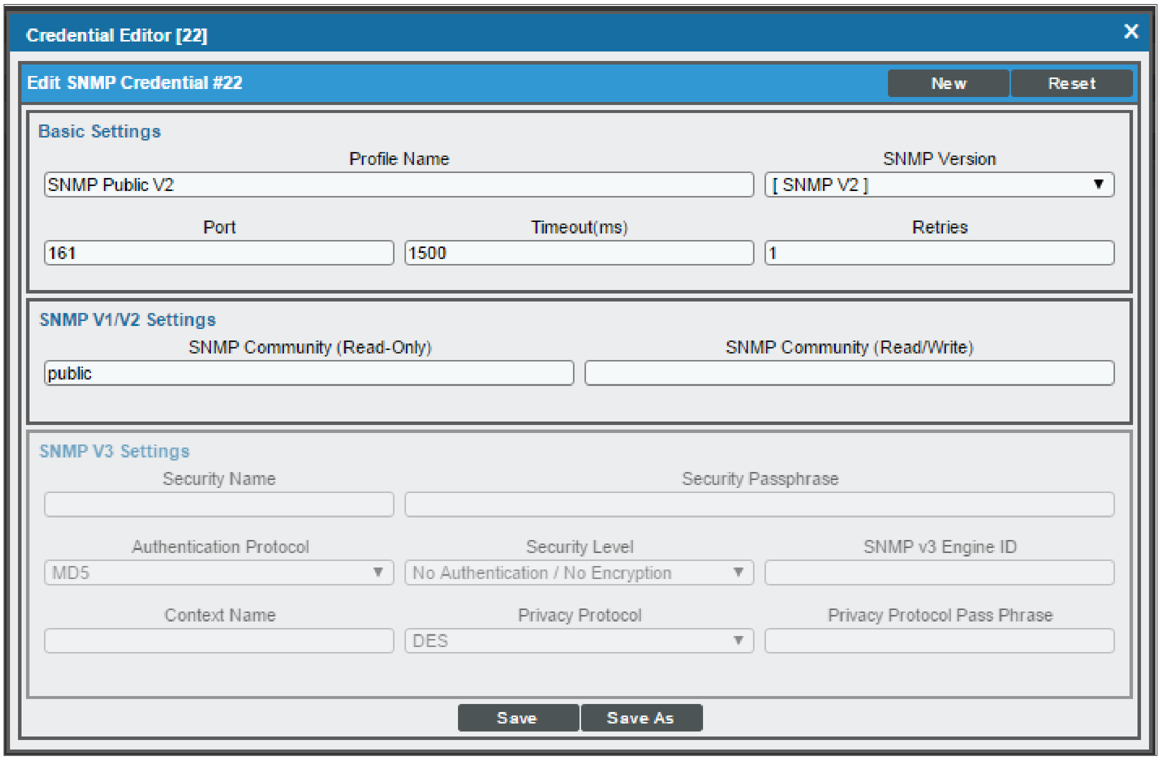
- SNMP community string
- Secure Shell (SSH) username and password to monitor Cisco voice components

Creating an SNMP Credential

SL1 uses SNMP to collect information about the devices that can be monitored using the Dynamic Applications in the *Cisco: UC Ancillary* PowerPack. To monitor these devices, you must first define an SNMP credential that enables SL1 to communicate with the devices.

To configure an SNMP credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click **[Create]**.
3. In the drop-down list that appears, select *SNMP Credential*. The **Credential Editor** page appears:



Credential Editor [22]

Edit SNMP Credential #22

Basic Settings

Profile Name: SNMP Public V2

SNMP Version: [SNMP V2]

Port: 161

Timeout(ms): 1500

Retries: 1

SNMP V1/V2 Settings

SNMP Community (Read-Only): public

SNMP Community (Read/Write):

SNMP V3 Settings

Security Name:

Security Passphrase:

Authentication Protocol: MD5

Security Level: No Authentication / No Encryption

SNMP v3 Engine ID:

Context Name:

Privacy Protocol: DES

Privacy Protocol Pass Phrase:

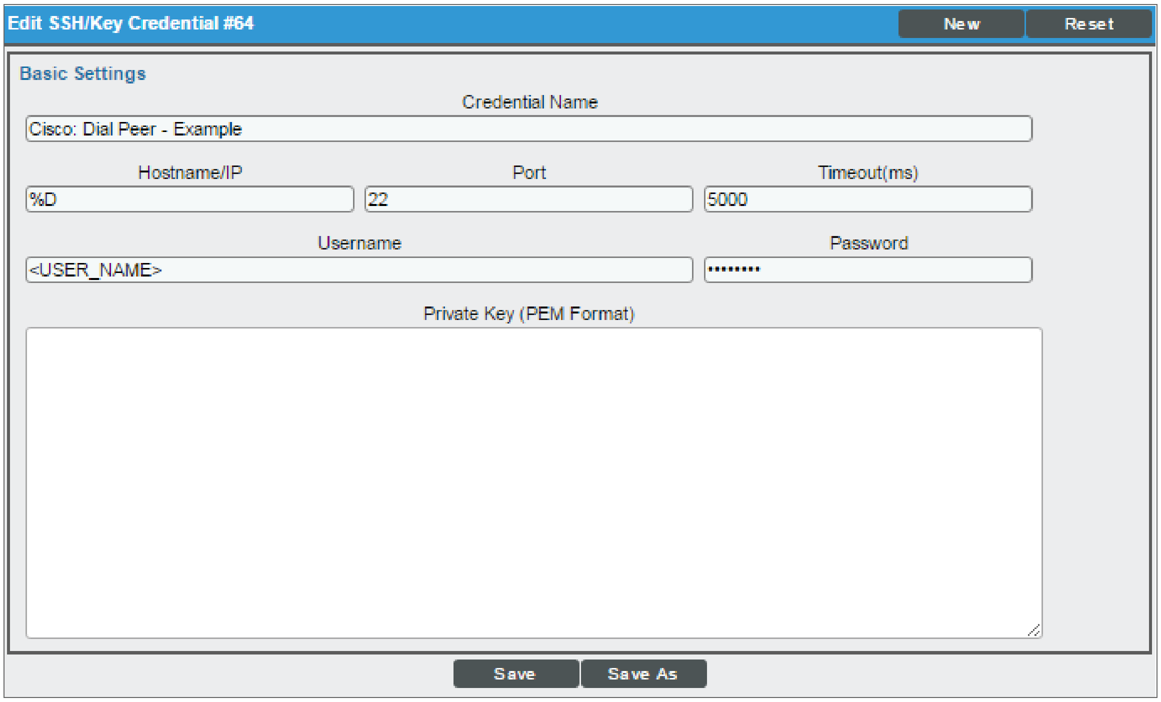
4. In the ***Profile Name*** field, type a name for the credential.
5. In the ***SNMP Version*** field, select *SNMP V2*.
6. In the ***SNMP Community (Read Only)*** field, type the community string for the device you want to monitor.
7. Optionally, supply values in the other fields in this page. In most cases, you can accept the default values for the other fields.
8. Click **[Save]**.

Creating an SSH/Key Credential

To configure SL1 to monitor Cisco voice devices, you must first create an SSH/Key credential that allows the Dynamic Applications in the *Cisco: UC Ancillary* PowerPack to connect with these devices. An example SSH/Key credential that you can edit for your own use is included in the *Cisco: UC Ancillary* PowerPack.

To create an SSH/Key credential to access Cisco voice devices:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **Cisco: Dial Peer - Example** credential, and then click its wrench icon (🔧). The **Edit SSH/Key Credential** modal page appears.
3. Type values in the following fields:



Credential Name		
Cisco: Dial Peer - Example		
Hostname/IP	Port	Timeout(ms)
%D	22	5000
Username		Password
<USER_NAME>		••••••••
Private Key (PEM Format)		

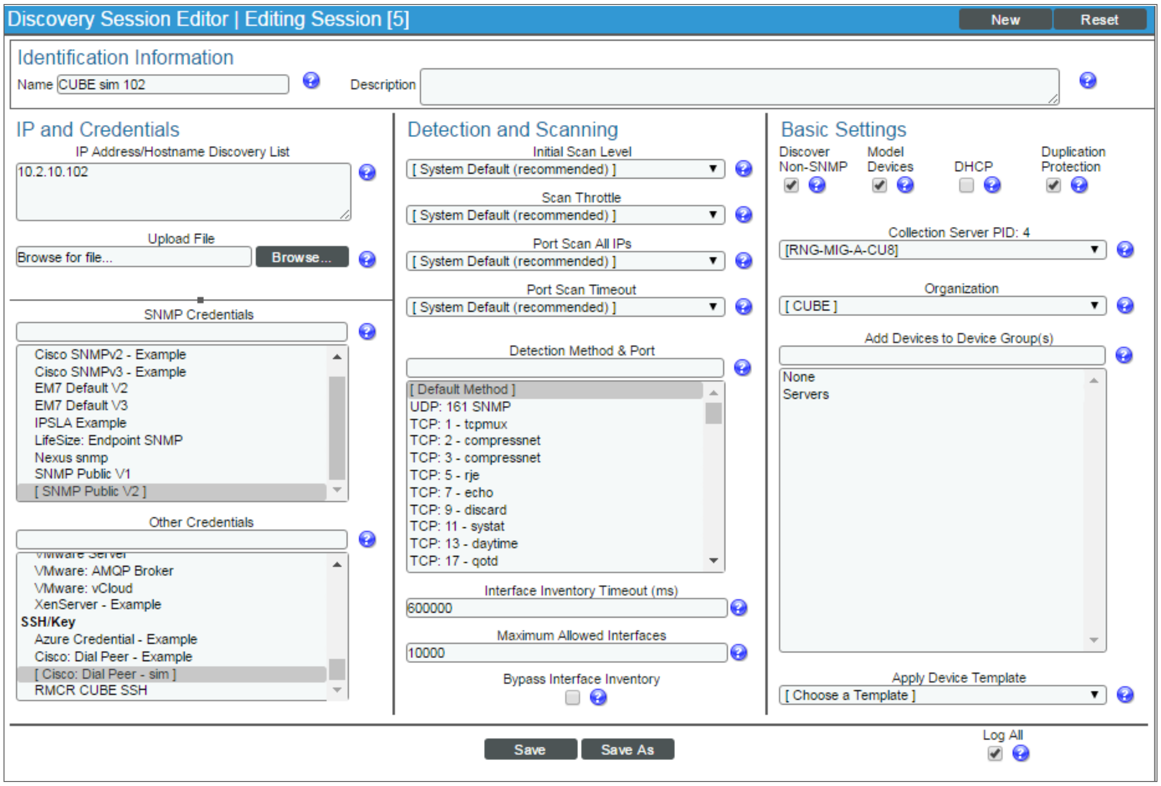
- ***Credential Name***. Type a new name for the credential.
- ***Hostname/IP***. Type "%D".
- ***Port***. Type "22".
- ***Username***. Type the administrator username used to connect to the dial peers via SSH.
- ***Password***. Type the password used to connect to the dial peers via SSH.
- ***Private Key (PEM Format)***. Leave this field blank.

4. Click **[Save As]**.
5. When the confirmation message appears, click **[OK]**.

Discovering Ancillary Cisco UC Devices

To create and run a discovery session that will discover ancillary Cisco UC devices, perform the following steps:

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



Discovery Session Editor | Editing Session [5]

Identification Information

Name: CUBE sim 102

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.2.10.102

Upload File: Browse for file...

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: VMware Server, VMware: AMQP Broker, VMware: vCloud, XenServer - Example, SSH/Key, Azure Credential - Example, Cisco: Dial Peer - Example, [Cisco: Dial Peer - sim], RMCR CUBE SSH

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: 4: [RNG-MIG-A-CU8]

Organization: [CUBE]

Add Devices to Device Group(s): None, Servers

Apply Device Template: [Choose a Template]

Log All: ☑

- ***IP Address/Hostname Discovery List***. Type the IP addresses for the devices you want to discover.
- ***SNMP Credentials***. Select the SNMP credential you created for the ancillary devices.
- ***Other Credentials***. Select the SSH/Key credential you created for the ancillary devices.
- ***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 **[Save]** 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 ancillary devices are discovered, click the device icon () to view the **Device Properties** page for each device.

Manually Aligning Dynamic Applications

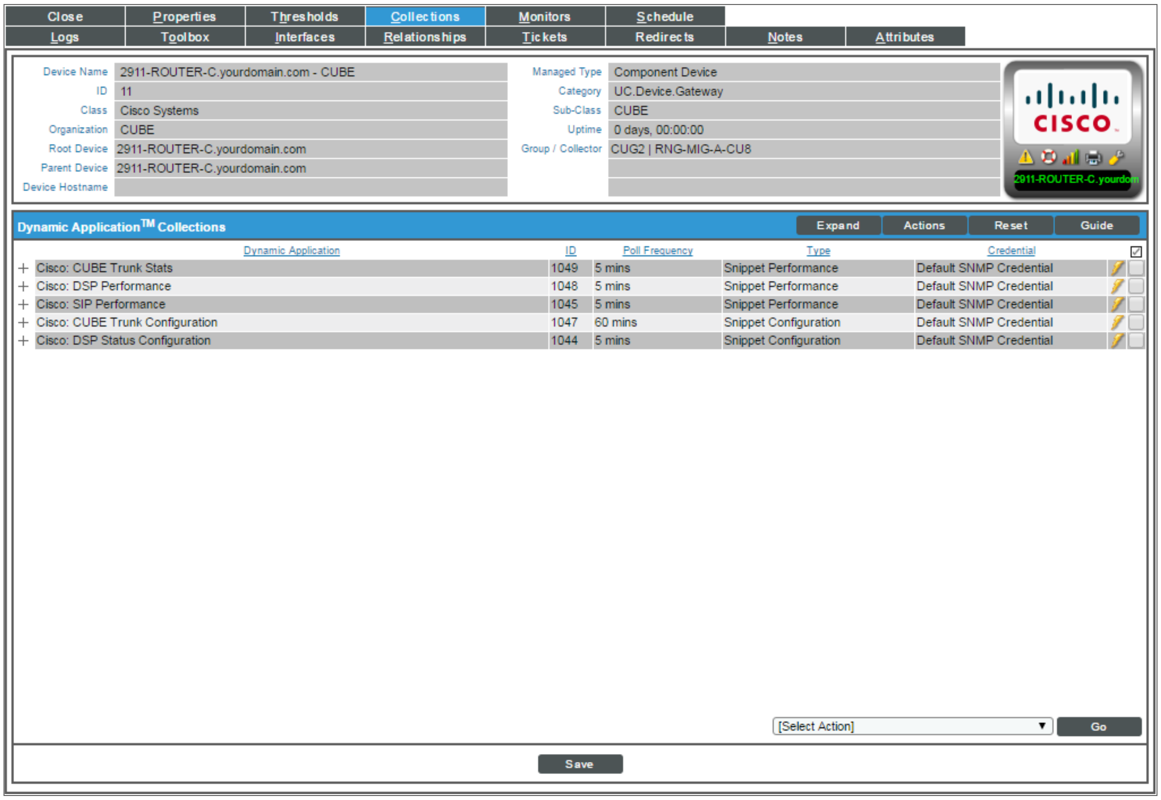
When you run the discovery session for ancillary UC devices, SL1 automatically aligns the necessary Dynamic Applications to the devices.

To verify that the Dynamic Applications aligned to the devices correctly:

1. After discovery has completed, click the device icon () for any of the discovered devices. The **Device Properties** page appears.
2. From the **Device Properties** page, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.

3. All applicable Dynamic Applications for the device 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	2911-ROUTER-C.yourdomain.com - CUBE	Managed Type	Component Device
ID	11	Category	UC.Device.Gateway
Class	Cisco Systems	Sub-Class	CUBE
Organization	CUBE	Uptime	0 days, 00:00:00
Root Device	2911-ROUTER-C.yourdomain.com	Group / Collector	CUG2 | RNG-MIG-A-CU8
Parent Device	2911-ROUTER-C.yourdomain.com		
Device Hostname			

Dynamic Application^{TM} Collections

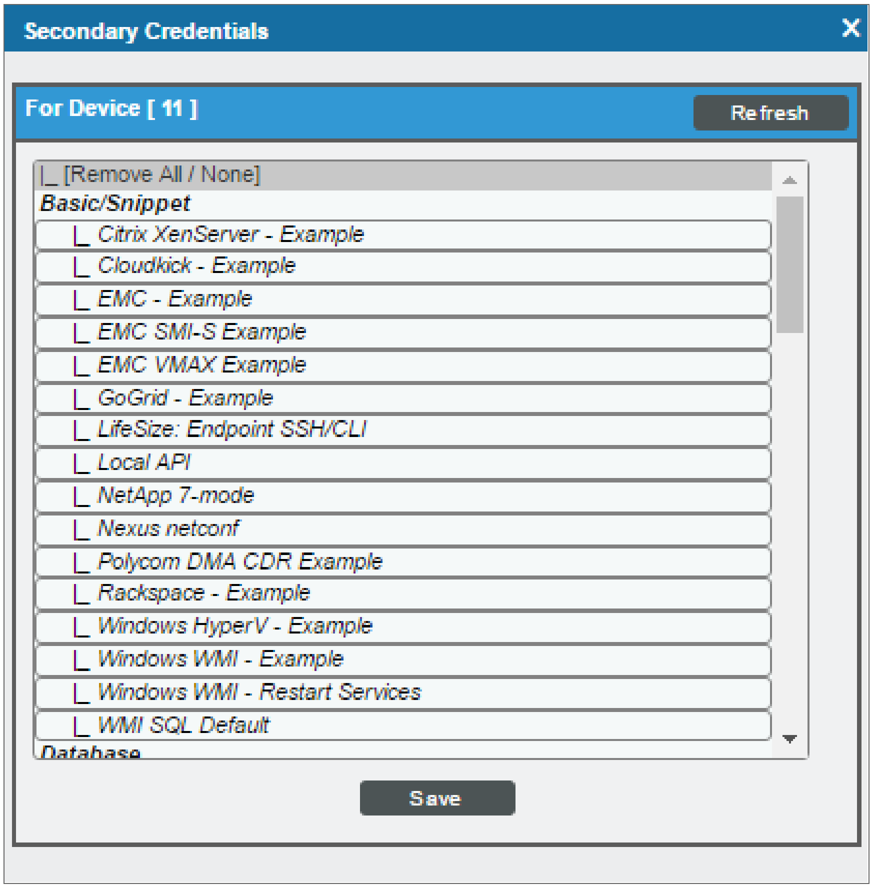
Dynamic Application	ID	Poll Frequency	Type	Credential	☑
+ Cisco: CUBE Trunk Stats	1049	5 mins	Snippet Performance	Default SNMP Credential	□
+ Cisco: DSP Performance	1048	5 mins	Snippet Performance	Default SNMP Credential	□
+ Cisco: SIP Performance	1045	5 mins	Snippet Performance	Default SNMP Credential	□
+ Cisco: CUBE Trunk Configuration	1047	60 mins	Snippet Configuration	Default SNMP Credential	□
+ Cisco: DSP Status Configuration	1044	5 mins	Snippet Configuration	Default SNMP Credential	□

If the "Cisco: Dial Peer Voice Summary" or "Cisco: Active Voice Call Legs Performance" Dynamic Applications did not automatically align to a voice device, you might need to manually align the SSH/Key credential to the device and then run discovery again.

To manually align the SSH/Key credential to the device:

1. From the **Device Properties** page (Registry > Devices > wrench icon), click the **[Actions]** button, and then select *Secondary Credentials* from the menu.

2. Select the SSH/Key credential you created for ancillary UC devices.



Secondary Credentials

For Device [11]

Refresh

|_ [Remove All / None]

Basic/Snippet

- |_ Citrix XenServer - Example
- |_ Cloudkick - Example
- |_ EMC - Example
- |_ EMC SMI-S Example
- |_ EMC VMAX Example
- |_ GoGrid - Example
- |_ LifeSize: Endpoint SSH/CLI
- |_ Local API
- |_ NetApp 7-mode
- |_ Nexus netconf
- |_ Polycom DMA CDR Example
- |_ Rackspace - Example
- |_ Windows HyperV - Example
- |_ Windows WMI - Example
- |_ Windows WMI - Restart Services
- |_ WMI SQL Default

Database

Save

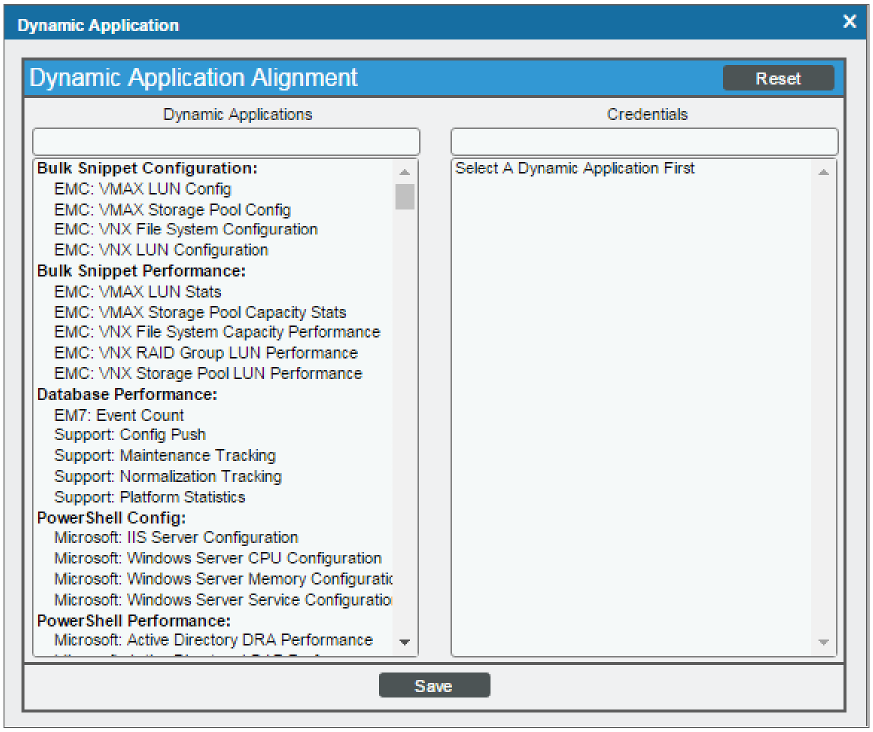
NOTE: If there are other credentials (for example, an SNMP credential) already aligned to the device, hold the <Ctrl> or <Command> key when selecting the SSH/Key credential to keep the other credentials aligned to the device as well.

3. Click **[Save]**.
4. Close the **Device Properties** page and go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
5. Locate the discovery session for ancillary UC devices and click its lightning bolt icon (⚡) to re-run the discovery session.

If any of the other Dynamic Applications did not automatically align to a device during discovery, you can align them manually to the device.

To manually align a Dynamic Application to a device:

1. From the **Dynamic Application Collections** page (Registry > Devices > wrench icon > Collections), click the **[Action]** button and then select *Add Dynamic Application*. The **Dynamic Application Alignment** page appears:



Bulk Snippet Configuration:
EMC: VMAX LUN Config
EMC: VMAX Storage Pool Config
EMC: VNX File System Configuration
EMC: VNX LUN Configuration
Bulk Snippet Performance:
EMC: VMAX LUN Stats
EMC: VMAX Storage Pool Capacity Stats
EMC: VNX File System Capacity Performance
EMC: VNX RAID Group LUN Performance
EMC: VNX Storage Pool LUN Performance
Database Performance:
EM7: Event Count
Support: Config Push
Support: Maintenance Tracking
Support: Normalization Tracking
Support: Platform Statistics
PowerShell Config:
Microsoft: IIS Server Configuration
Microsoft: Windows Server CPU Configuration
Microsoft: Windows Server Memory Configuratic
Microsoft: Windows Server Service Configuratio
PowerShell Performance:
Microsoft: Active Directory DRA Performance

Select A Dynamic Application First

2. In the ***Dynamic Applications*** field, select the Dynamic Application you want to align.
3. In the ***Credentials*** field, select one or more of the credentials you created for the ancillary UC devices.
4. Click **[Save]**.
5. Repeat steps 1-4 for any other unaligned Dynamic Applications.

Chapter

20

Cisco: UC VOS Applications

Overview

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

NOTE: For more information about the *Cisco: UC VOS Applications* PowerPack, see the ***Monitoring Cisco UC Voice Operating System (VOS) Applications*** manual.

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:

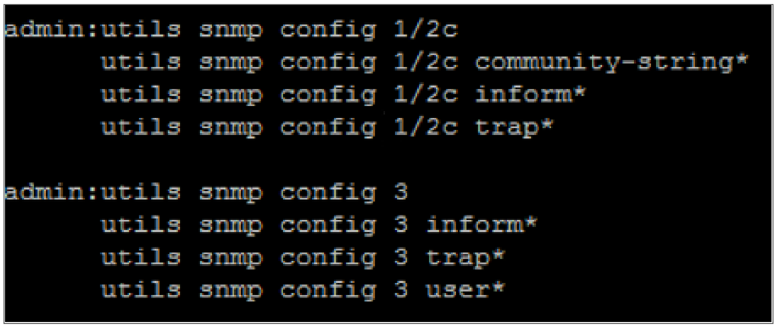
- Cisco Contact Center Express (CCX)
- Cisco Unity Connection (CUC) servers
- Cisco Hosted Collaboration Mediation for Fulfillment (HCM-F)
- Cisco HCS Intelligent Loader
- Cisco IM & Presence (IM&P) servers (optional)
- Cisco Emergency Responder
- Cisco Prime Collaboration Deployment (PCD) servers (optional,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

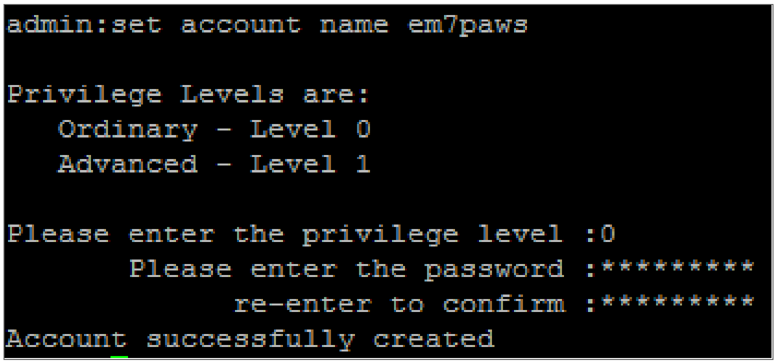
- Cisco Contact Center Express (CCX)
- Cisco Unity Connection (CUC) servers
- Cisco Hosted Collaboration Mediation for Fulfillment (HCM-F)
- Cisco HCS Intelligent Loader
- Cisco IM & Presence (IM&P) servers
- Cisco Unified Communications Manager (CUCM)
- Cisco Prime License Manager (PLM)
- Cisco Prime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

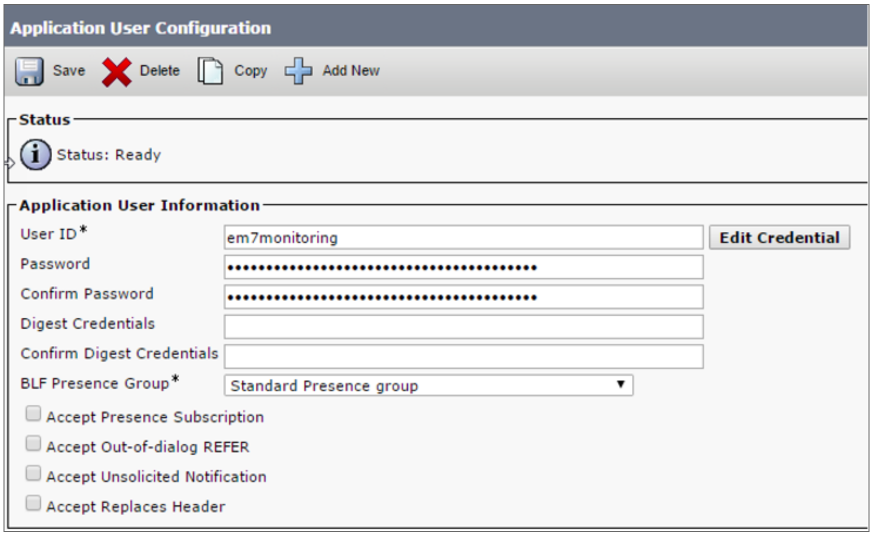
> **NOTE:** Because SL1 does not access the Administrative XML API for IM and Presence, the Standard AXL API Access role is not required.

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):



Application User Configuration

Status

Status: Ready

Application User Information

User ID*	em7monitoring
Password	••
Confirm Password	••
Digest Credentials	
Confirm Digest Credentials	
BLF Presence Group*	Standard Presence group

☐ Accept Presence Subscription

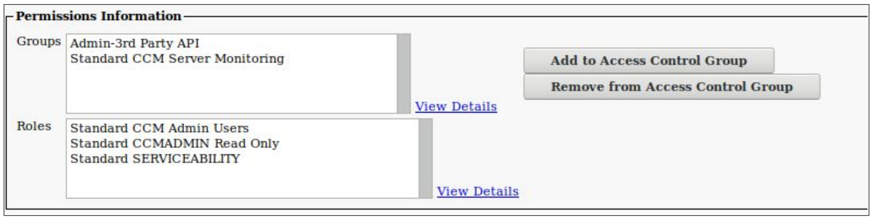
☐ Accept Out-of-dialog REFER

☐ Accept Unsolicited Notification

☐ Accept Replaces Header

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.



Permissions Information

Groups	Admin-3rd Party API Standard CCM Server Monitoring
Roles	Standard CCM Admin Users Standard CCMADMIN Read Only Standard SERVICEABILITY

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.

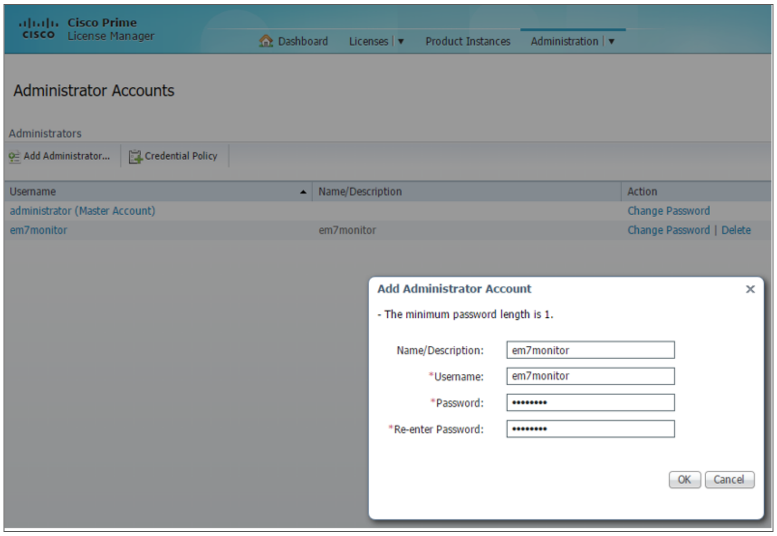
When Cisco Prime License Manager is installed as a standalone system, and is not co-resident with another Cisco product, you can only create administrative users for the application. You can use the existing administrator account or create a new account for monitoring.

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):



Administrator Accounts

Administrators

Username	Name/Description	Action
administrator (Master Account)		Change Password
em7monitor	em7monitor	Change Password | Delete

Add Administrator Account

- The minimum password length is 1.

Name/Description: em7monitor

*Username: em7monitor

*Password: ••••••••

*Re-enter Password: ••••••••

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***.

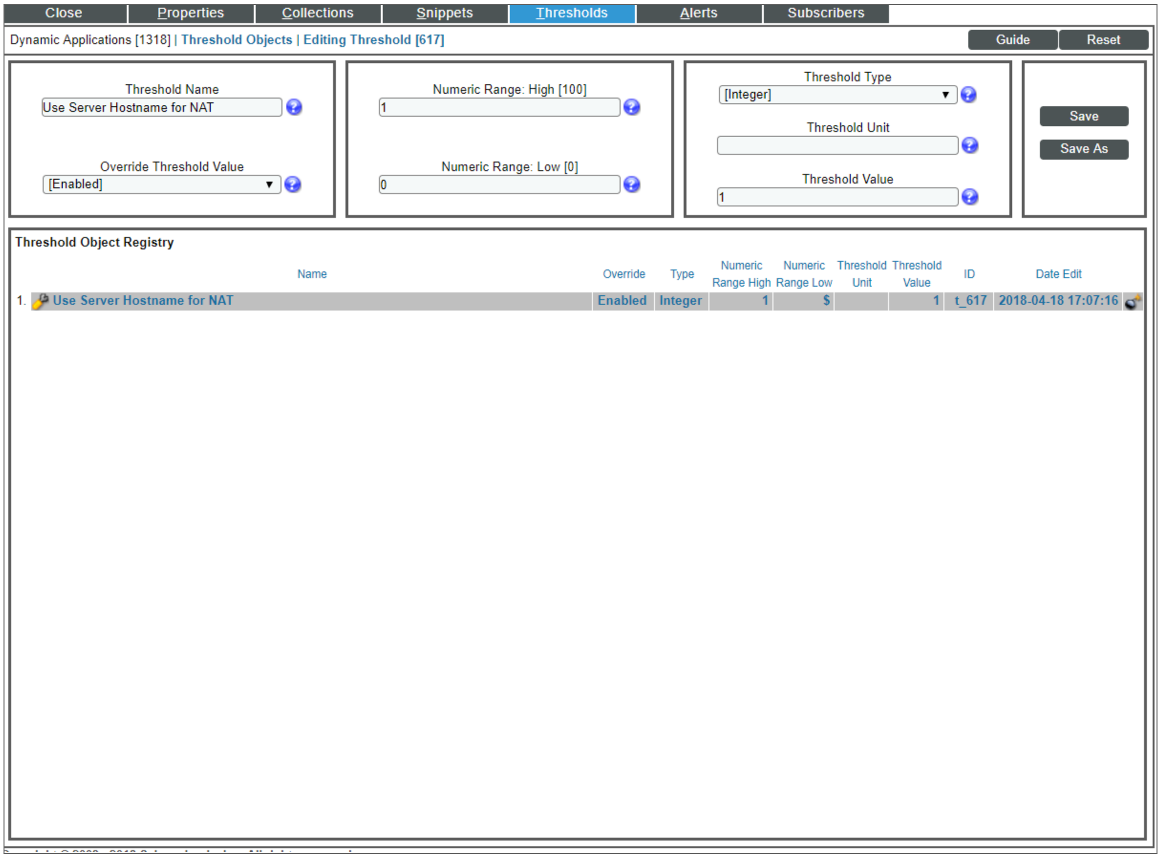
Enabling Network Address Translation (NAT) for Cisco UC VOS Devices

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.

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



Dynamic Applications [1318] | Threshold Objects | Editing Threshold [617]

Threshold Name: Use Server Hostname for NAT

Override Threshold Value: [Enabled]

Numeric Range: High [100]: 1

Numeric Range: Low [0]: 0

Threshold Type: [Integer]

Threshold Unit:

Threshold Value: 1

Threshold Object Registry

	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	$		1	t_617	2018-04-18 17:07:16

5. 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.

6. 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:

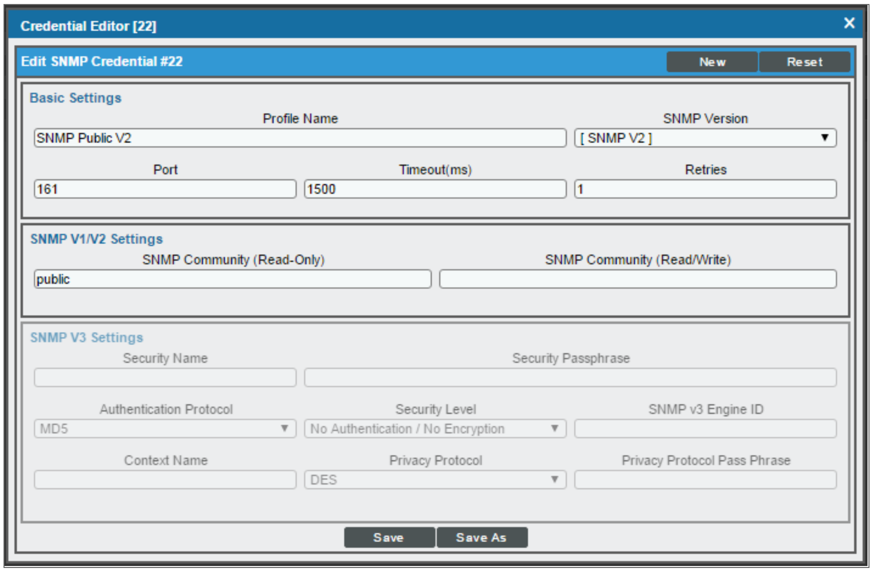
- Cisco Contact Center Express (CCX)
- Cisco Unity Connection (CUC) servers
- Cisco Hosted Collaboration Mediation for Fulfillment (HCM-F)
- Cisco HCS Intelligent Loader
- Cisco IM & Presence (IM&P) servers (optional)
- Cisco Emergency Responder
- Cisco Prime Collaboration Deployment (PCD) servers (optional,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



Basic Settings

Profile Name: SNMP Public V2

SNMP Version: [SNMP V2]

Port: 161

Timeout(ms): 1500

Retries: 1

SNMP V1/V2 Settings

SNMP Community (Read-Only): public

SNMP Community (Read/Write):

SNMP V3 Settings

Security Name:

Security Passphrase:

Authentication Protocol: MD5

Security Level: No Authentication / No Encryption

SNMP v3 Engine ID:

Context Name:

Privacy Protocol: DES

Privacy Protocol Pass Phrase:

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)***.

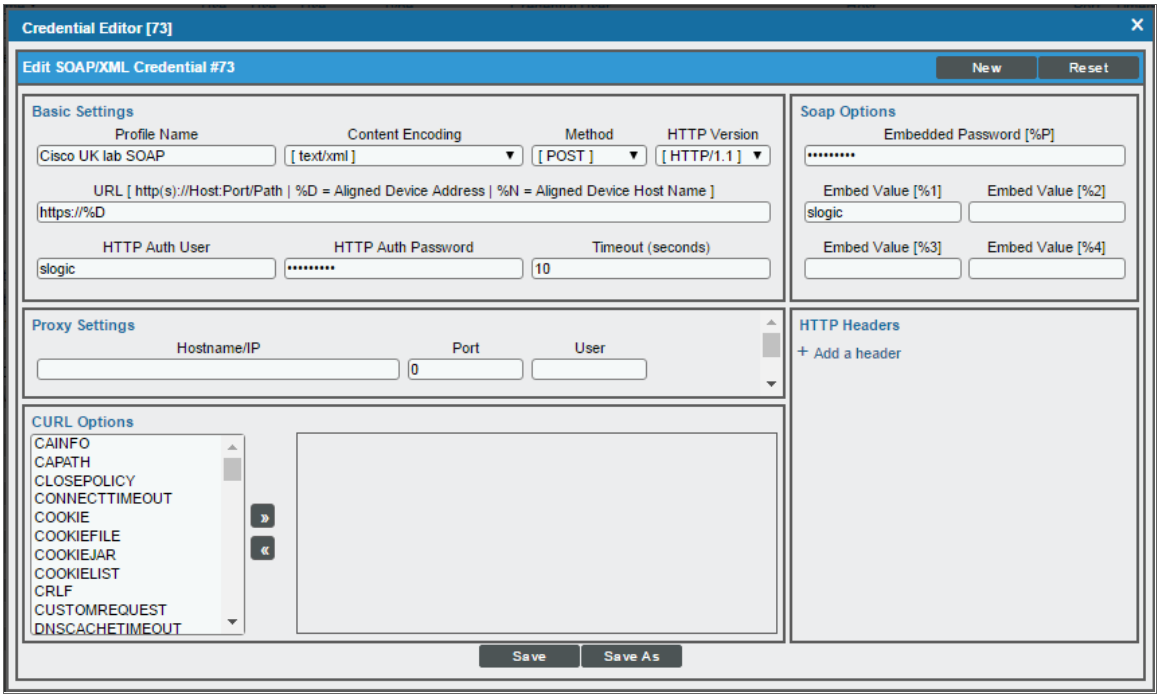
TIP: When possible, ScienceLogic recommends using the same login information with read access for all of the APIs required to monitor a particular application. Doing so enables you to create a single SOAP/XML credential for each application with only the "Basic Settings" configured.

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:



Profile Name: Cisco UK lab SOAP

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://%D

HTTP Auth User: slogic

HTTP Auth Password: •••••••••

Timeout (seconds): 10

Embedded Password [%P]: •••••••••

Embed Value [%1]: slogic

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

Hostname/IP:

Port: 0

User:

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)

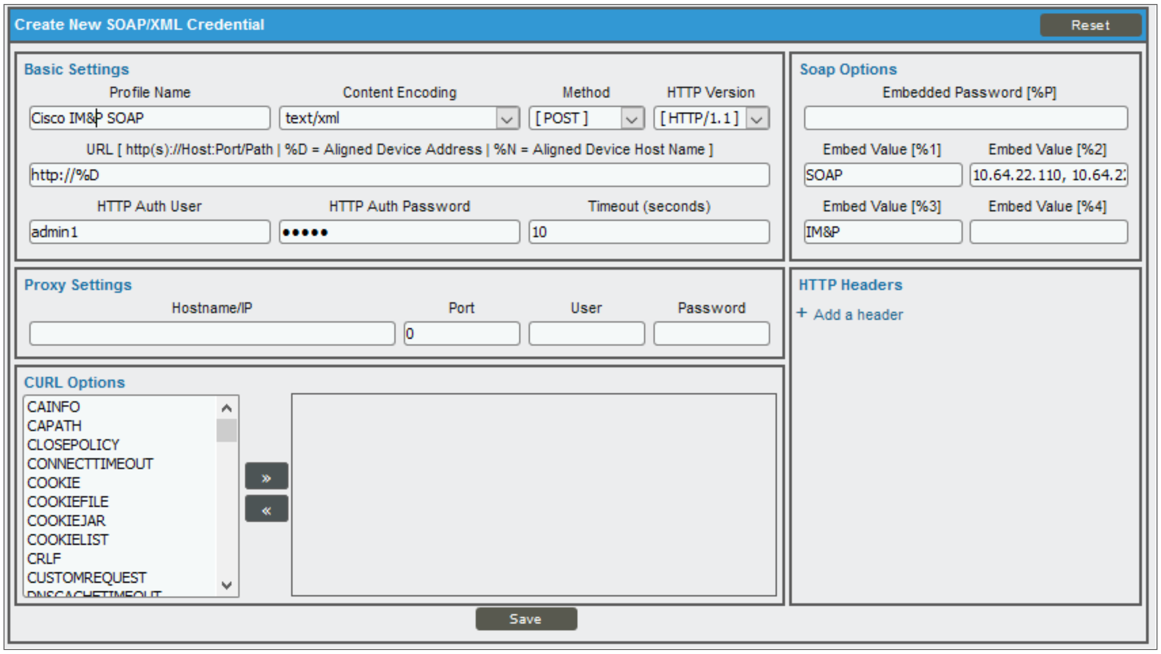
As a result, several of the Dynamic Applications (including all performance Dynamic Applications) in the *Cisco: UC VOS Applications* PowerPack must be aligned with a SOAP/XML credential that includes the SOAP API login information.

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:



Create New SOAP/XML Credential

Basic Settings

Profile Name	Content Encoding	Method	HTTP Version
Cisco IM&P SOAP	text/xml	[POST]	[HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: http://%D

HTTP Auth User	HTTP Auth Password	Timeout (seconds)
admin1	•••••	10

Soap Options

Embedded Password [%P]:

Embed Value [%1]	Embed Value [%2]
SOAP	10.64.22.110, 10.64.2

Embed Value [%3]	Embed Value [%4]
IM&P	

Proxy Settings

Hostname/IP	Port	User	Password
	0		

HTTP Headers

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.

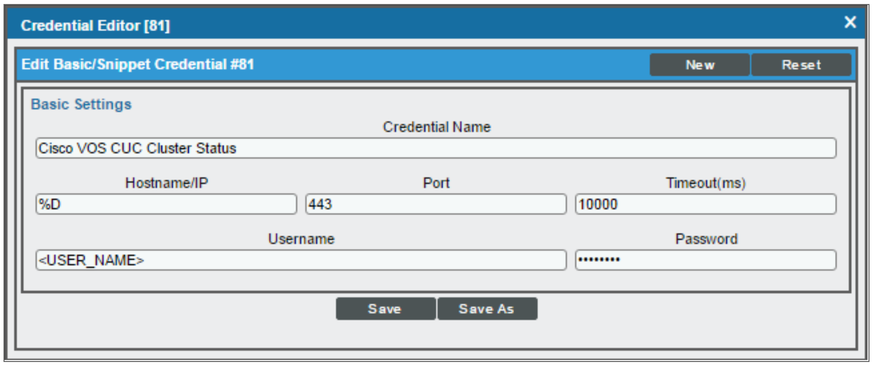
> **NOTE:** The steps below describe how to edit both example credentials, which you should do if the REST API login information is different for CUC and IM&P. However, if the REST API login information is the same for both applications, then a second Basic/Snippet credential is unnecessary.

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.

3. Update the following fields:



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

- ***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.

4. Click the **[Save As]** button.
5. When the confirmation message appears, click **[OK]**.
6. 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

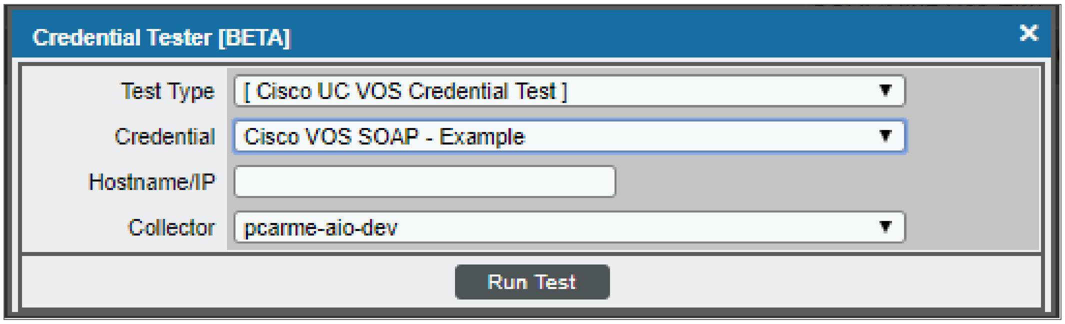
SL1 includes a Credential Test for Cisco UC VOS. Credential Tests define a series of steps that SL1 can execute on demand to validate whether a credential works as expected.

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:



Credential Tester [BETA]

Test Type: [Cisco UC VOS Credential Test]

Credential: Cisco VOS SOAP - Example

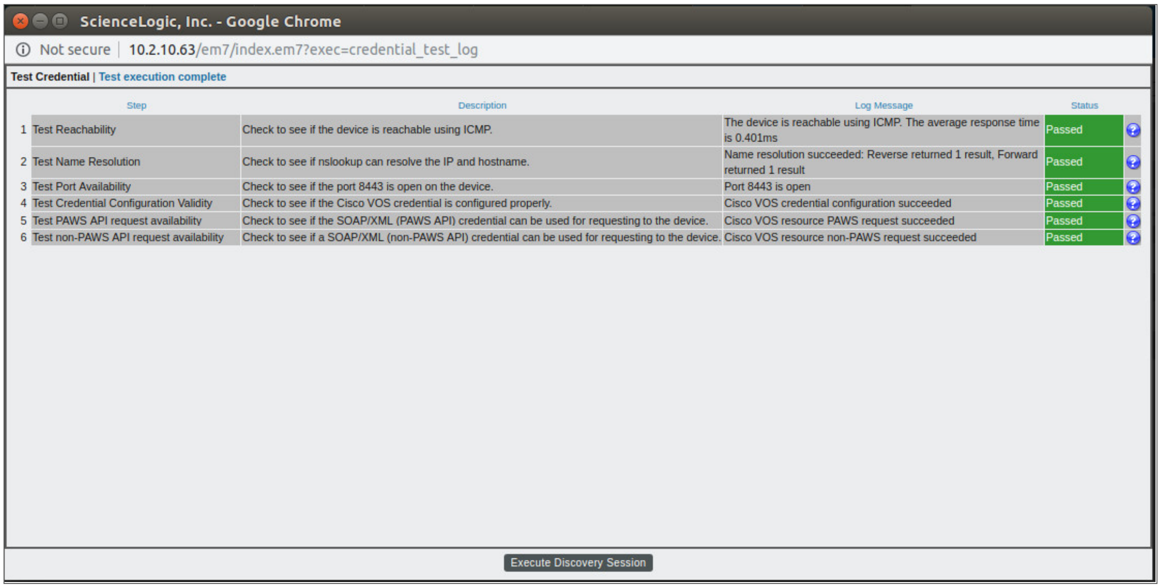
Hostname/IP:

Collector: pcarme-aio-dev

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	?

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".

Discovering VOS Devices

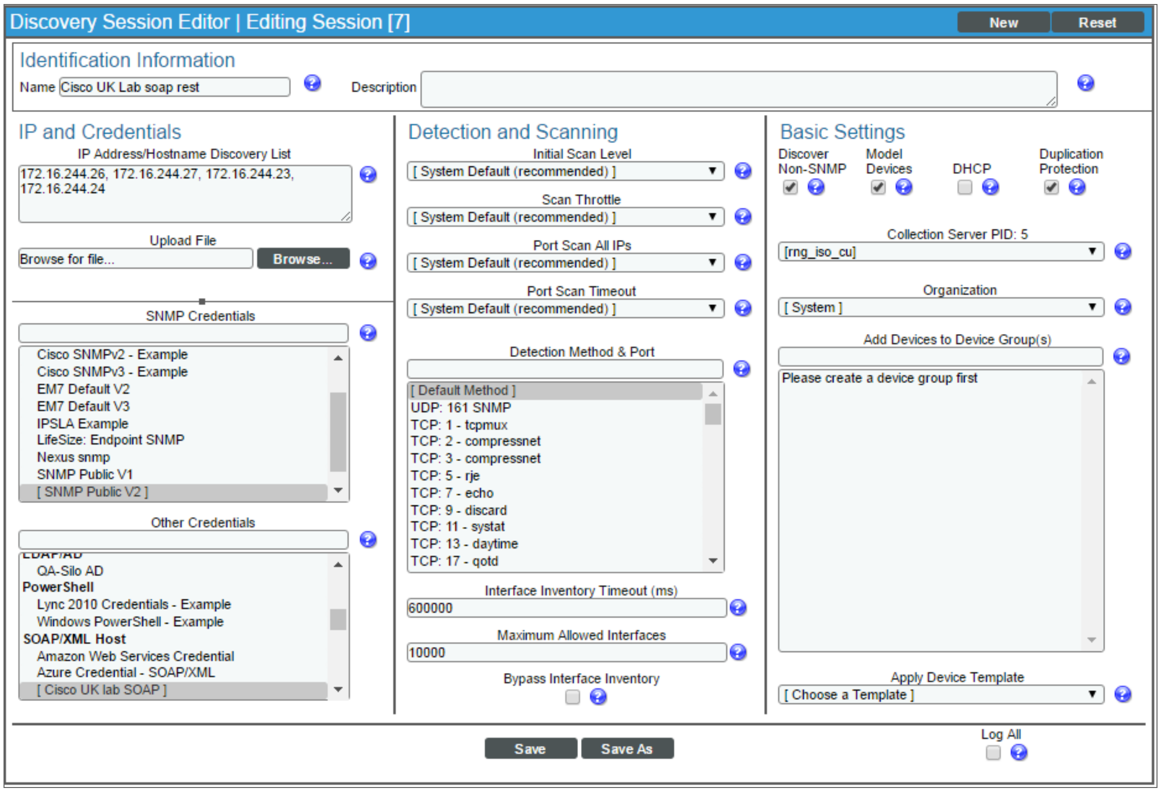
To model and monitor your VOS applications, run a discovery session to discover the VOS application clusters that SL1 will use as the root devices for monitoring the applications.

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:



Identification Information

Name: Cisco UK Lab soap rest

Description:

IP and Credentials

IP Address/Hostname Discovery List: 172.16.244.26, 172.16.244.27, 172.16.244.23, 172.16.244.24

Upload File: Browse for file...

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:
- LDAP/AD
  - 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: [rng_iso_cu]

Organization: [System]

Add Devices to Device Group(s): Please create a device group first

Apply Device Template: [Choose a Template]

Log All: □

- ***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.

Chapter 21

Cisco: UCS

Overview

The following sections describe how to configure and discover a Cisco Unified Computing System (UCS) Manager and component devices for monitoring by SL1 using the *Cisco: UCS* PowerPack:

NOTE: For more information about the *Cisco: UCS* PowerPack, see the ***Monitoring Cisco Unified Computing System (UCS) Manager*** manual.

Prerequisites for Monitoring Cisco UCS Manager

To use the Dynamic Component Mapping Dynamic Applications included in the *Cisco: UCS* PowerPack, you must log in to the UCS Manager GUI and create a user account that SL1 can use to access the UCS web service.

When the Dynamic Component Mapping Dynamic Applications are aligned to the UCS Manager, SL1 will collect information about all the components in the UCS system, such as UCS Chassis and Blades. SL1 will then create a device record for each component and automatically align other Dynamic Applications from the *Cisco: UCS* PowerPack to each component device.

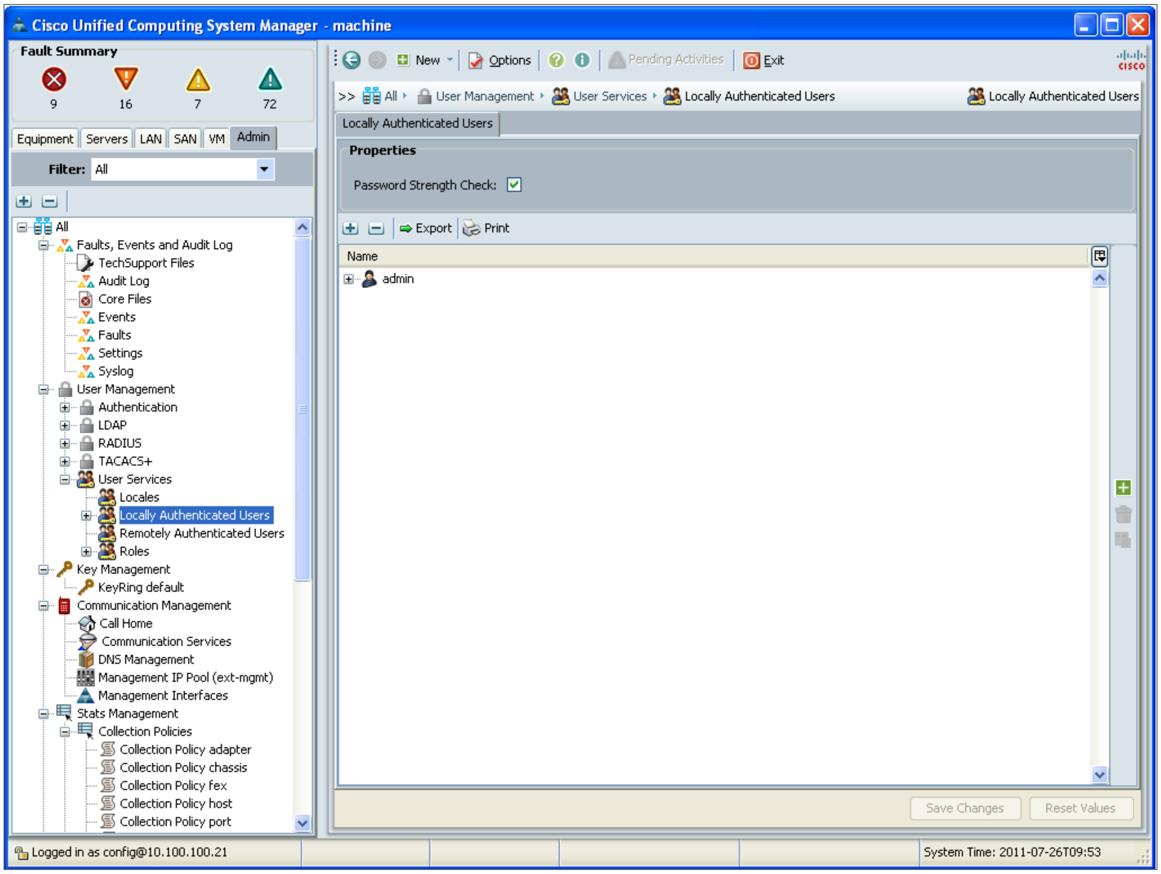
Configuring the UCS System

To configure a UCS system for monitoring by SL1, you must:

- Create a user account in UCS that SL1 can use to access the UCS web service
- Enable the CIM XML service

Perform the following steps to complete these tasks:

1. Log in to the UCS Manager GUI as an administrator.
2. At the top of the left pane, click the **[Admin]** tab.
3. In the left pane, go to All > User Management > User Services > Locally Authenticated Users. The **Locally Authenticated Users** page appears in the right pane:

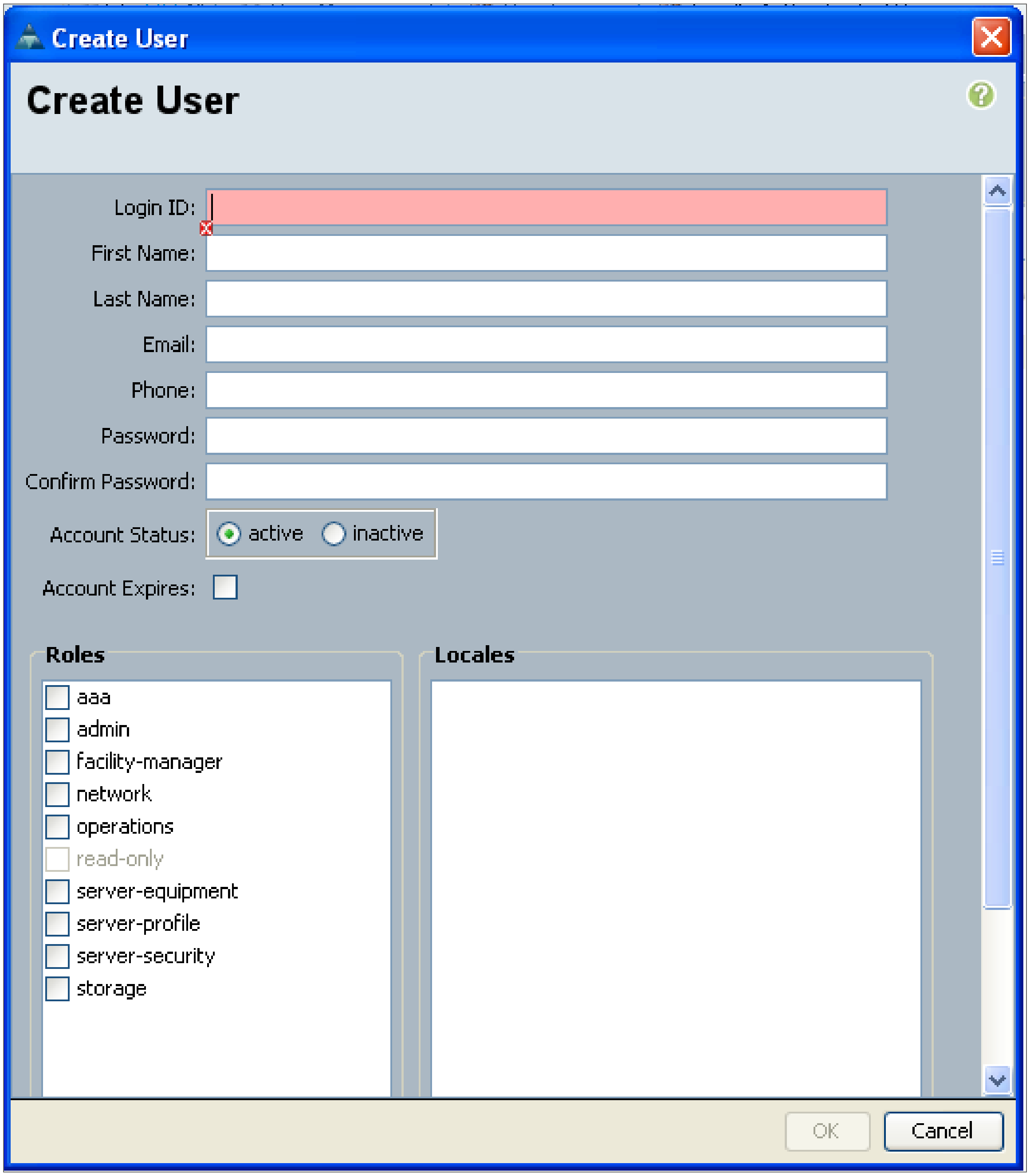


Password Strength Check: ☑

Logged in as config@10.100.100.21

System Time: 2011-07-26T09:53

4. Click the green plus icon on the right side of the **Locally Authenticated Users** page. The **Create User** window appears:



Create User

Create User

Login ID:

First Name:

Last Name:

Email:

Phone:

Password:

Confirm Password:

Account Status: ● active ○ inactive

Account Expires: □

Roles

□ aaa
□ admin
□ facility-manager
□ network
□ operations
□ read-only
□ server-equipment
□ server-profile
□ server-security
□ storage

Locales

5. Supply values in the following fields:

   - ***Login ID***. Enter a username for the user.
   - ***Password***. Enter a password for the user.
   - ***Confirm Password***. Re-enter the password you entered in the ***Password*** field.

- ***Account Status***. Select *active*.
- ***Account Expires***. Make sure that this checkbox is not selected.
- ***Roles***. To create a read-only user, do not select any checkboxes.

6. Click the **[OK]** button, and then click the **[OK]** button in the confirmation pop-up window.
7. In the left pane of the UCS Manager GUI, go to All > Communication Management > Communication Services. The **Communication Services** page appears in the right pane.
8. In the ***Admin State*** field in the **CIM XML** section, select *Enabled*.

NOTE: Older versions of the UCS software do not include the option to disable the CIM XML service. If the option to enable/disable the CIM XML service does not appear, the service is already enabled.

9. Click the **[Save Changes]** button.

NOTE: When blade servers are replaced in a UCS chassis, and the old blade servers are not properly decommissioned, UCS Manager does not assign new Internal IDs to the new blade servers when they are inserted in the chassis. Instead, UCS Manager assigns an Internal ID of "none" to the new blade servers. This does not cause an error in SL1 if it occurs with only a single blade; however, if more than one blade that you are monitoring is replaced without being decommissioned, multiple blades will have the same Internal ID of "none", which in turn can cause blades to appear under the incorrect chassis or not appear at all in SL1. If this occurs, decommission the affected blades and then reinsert them. For more information, see the section on "Guidelines for Removing and Decommissioning Blade Servers" in the Cisco UCS documentation.

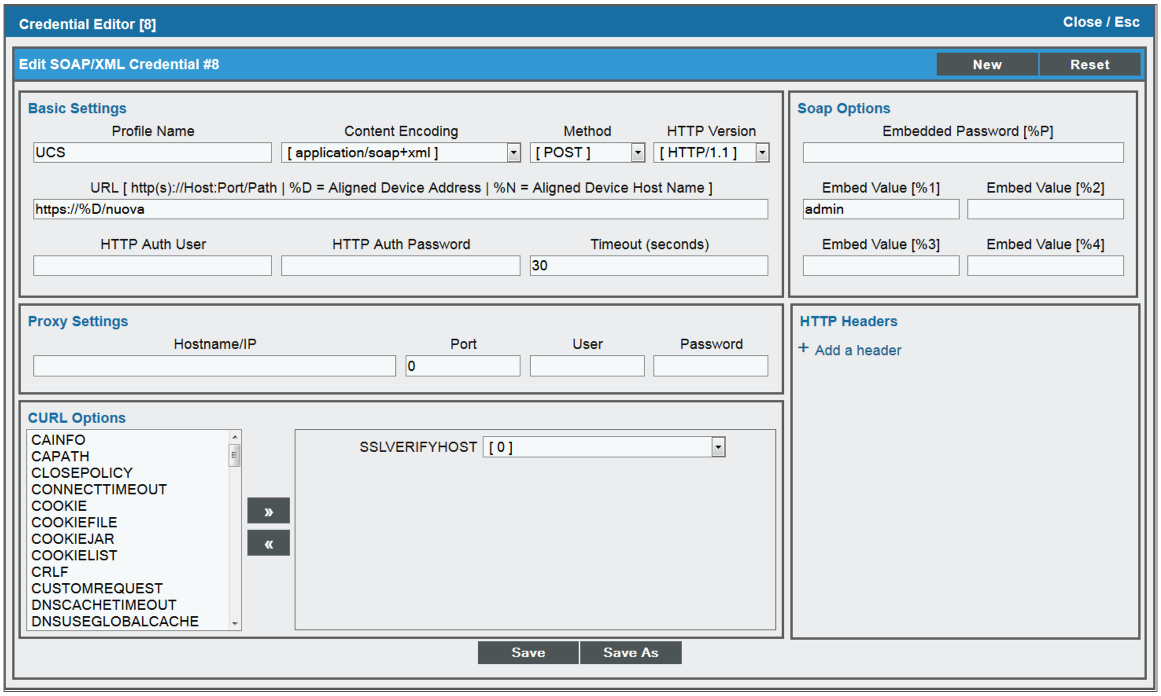
Creating a SOAP/XML Credential

To use the Dynamic Applications in the *Cisco: UCS* PowerPack, you must configure a SOAP/XML credential for the UCS Manager web service. The *Cisco: UCS* PowerPack includes a template for a SOAP/XML credential that you can edit for use with your UCS system.

To create a new UCS credential using the example credential:

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

2. Click the wrench icon () for the **UCS - Example** credential. The **Credential Editor** modal window appears:



Profile Name: UCS

Content Encoding: [application/soap+xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://%D/nuova

HTTP Auth User:

HTTP Auth Password:

Timeout (seconds): 30

Embedded Password [%P]:

Embed Value [%1]: admin

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

Hostname/IP:

Port: 0

User:

Password:

SSLVERIFYHOST [0]

3. Supply values in the following fields:

   - ***Profile Name***. Type a new name for the credential.
   - ***URL***. Keep the default value: **https://%D/nuova**
   - ***Embed Value [%1]***. Type the username for the user account that you configured in the UCS Manager.

> **NOTE:** If your user account does not use the default UCS Manager authentication realm, then you must prefix the username entered in this field with the authentication realm name for that user. In this scenario, the username should be in the following format: `ucs-[realm name]\[username]`.
>
> For example, if your UCS Manager username is "EM7admin" and it is authenticated in the "Local" realm (i.e., "Local" is the realm in which the user "EM7admin" is authenticated), you would enter the following value in this field:
>
> ```
> ucs-Local\EM7admin
> ```
>
> UCS Manager authentication realm names are case-sensitive.

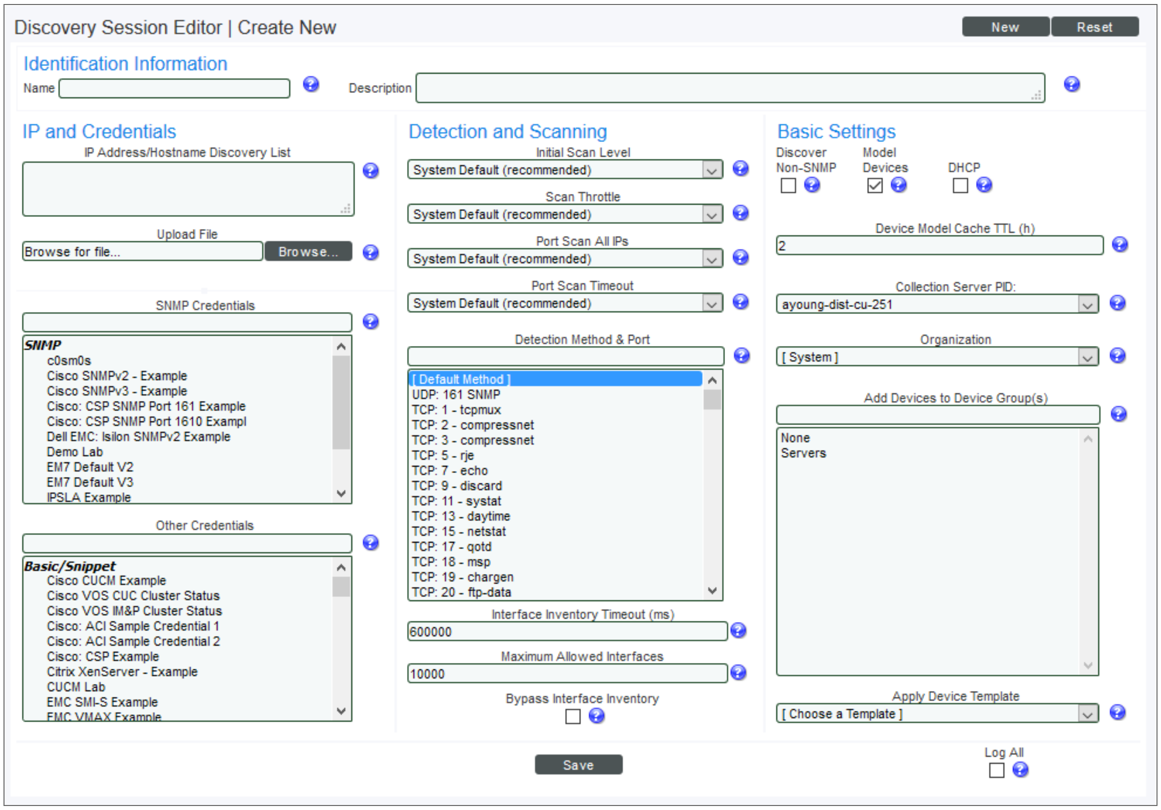
   - ***Embedded Password [%P]***. Type the password for the user account that you configured in the UCS Manager.

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

Discovering a UCS Manager

To create and run a discovery session that will discover a UCS Manager:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. Click the **[Create]** button to create a new discovery session. The **Discovery Session Editor** window appears:



Discovery Session Editor | Create New

New Reset

Identification Information

Name

Description

IP and Credentials

IP Address/Hostname Discovery List

Upload File

Browse for file... Browse...

SNMP Credentials

SNMP
c0sm0s
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Cisco: CSP SNMP Port 161 Example
Cisco: CSP SNMP Port 1610 Exampl
Dell EMC: Isilon SNMPv2 Example
Demo Lab
EM7 Default V2
EM7 Default V3
IPSLA Example

Other Credentials

Basic/Snippet
Cisco CUCM Example
Cisco VOS CUC Cluster Status
Cisco VOS IM&P Cluster Status
Cisco: ACI Sample Credential 1
Cisco: ACI Sample Credential 2
Cisco: CSP Example
Citrix XenServer - Example
CUCM Lab
EMC SMI-S Example
EMC VMAX Example

Detection and Scanning

Initial Scan Level: System Default (recommended)

Scan Throttle: System Default (recommended)

Port Scan All IPs: System Default (recommended)

Port Scan Timeout: System Default (recommended)

Detection Method & Port

[Default Method]
UDP: 161 SNMP
TCP: 1 - tcpmux
TCP: 2 - compressnet
TCP: 3 - compressnet
TCP: 5 - rje
TCP: 7 - echo
TCP: 9 - discard
TCP: 11 - systat
TCP: 13 - daytime
TCP: 15 - netstat
TCP: 17 - qotd
TCP: 18 - msp
TCP: 19 - chargen
TCP: 20 - ftp-data

Interface Inventory Timeout (ms): 600000

Maximum Allowed Interfaces: 10000

Bypass Interface Inventory □

Basic Settings

Discover Non-SNMP □

Model Devices ☑

DHCP □

Device Model Cache TTL (h): 2

Collection Server PID: ayoung-dist-cu-251

Organization: [System]

Add Devices to Device Group(s)

None
Servers

Apply Device Template: [Choose a Template]

Save

Log All □

3. Enter values in the following fields:
   - ***IP Address Discovery List***. Enter the IP address for the UCS Manager.
   - ***SNMP Credentials***. UCS Manager does not support SNMP. Do not select any credentials in this field.
   - ***Other Credentials***. Select the Cisco UCS credential you created.
   - ***Initial Scan Level***. Select 5. *Deep Discovery*. The *Cisco: UCS* PowerPack includes a "UCS Manager" device class. The "UCS Manager" device class is a **Non-SNMP** device class that is aligned only during deep discovery. If you do not select 5. *Deep Discovery* in this field, the UCS Manager will be discovered and assigned a device class for a Linux pingable device.

- ***Detection Method & Port***. Select *443 - HTTPS*. You can select additional ports, but must include port 443 - HTTPS.
- ***Discover Non-SNMP***. Because UCS Manager does not support SNMP, you must 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 will display 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.

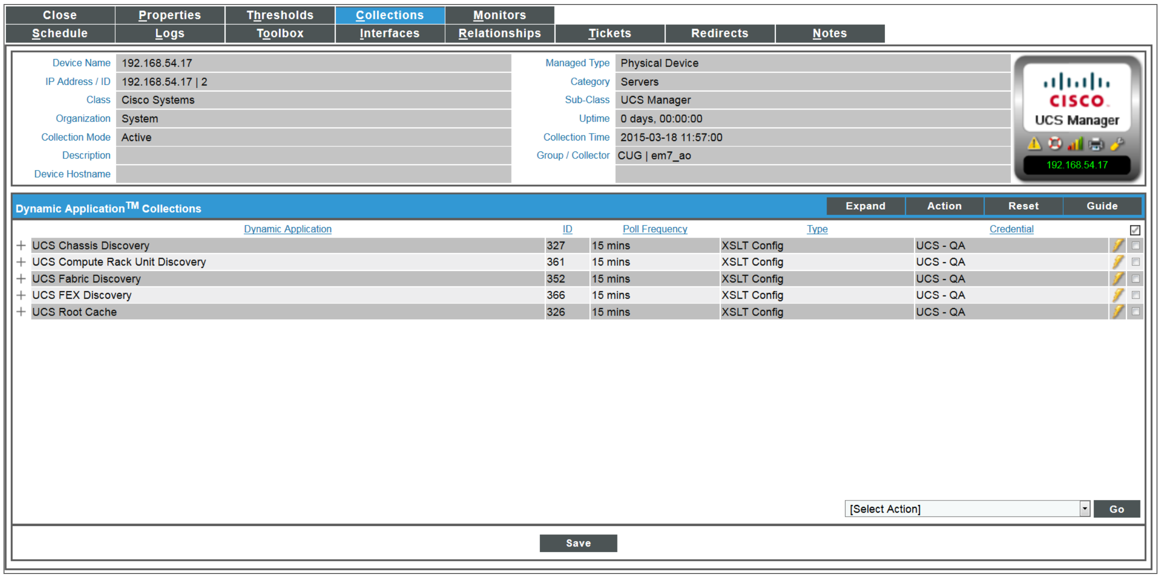
NOTE: After the discovery session completes, ScienceLogic recommends running the discovery session a second time to ensure that the "Cisco: UCS Cluster Information" Dynamic Application aligns with the UCS Manager root device.

8. When the UCS Manager is discovered, click its device icon (🖥) to view the **Device Properties** page for the UCS Manager server.

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

NOTE: It can take several minutes after discovery for Dynamic Applications to display on the **Dynamic Application Collections** page. If the listed Dynamic Applications do not display on this page, try clicking the **[Reset]** button.

1. From the **Device Properties** page for the UCS Manager, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.



Device Name	192.168.54.17	Managed Type	Physical Device
IP Address / ID	192.168.54.17 | 2	Category	Servers
Class	Cisco Systems	Sub-Class	UCS Manager
Organization	System	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2015-03-18 11:57:00
Description		Group / Collector	CUG | em7_ao
Device Hostname			

Dynamic Application™ Collections

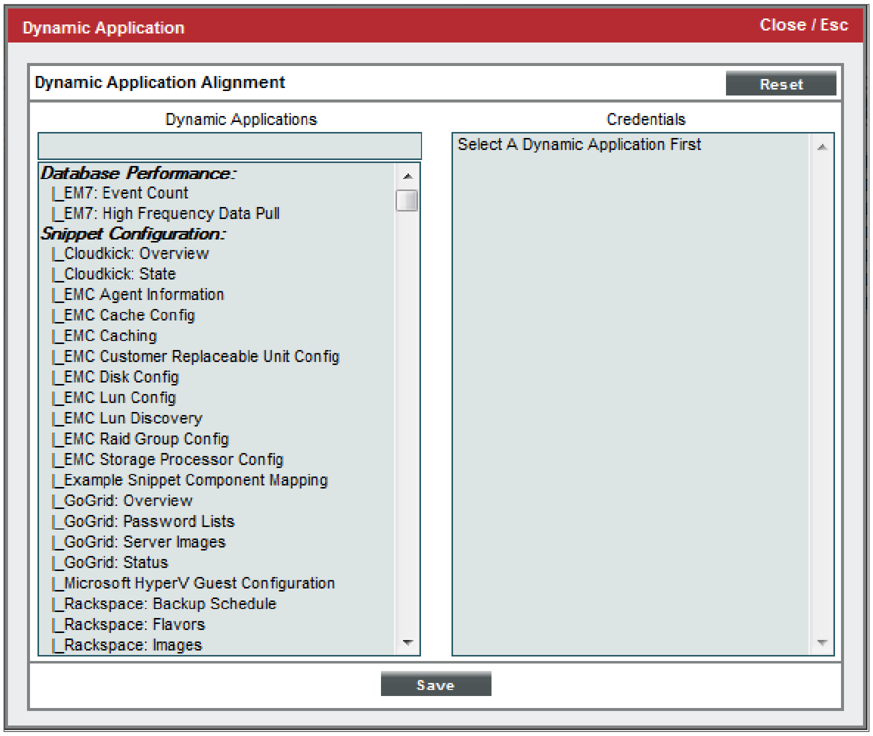
Dynamic Application	ID	Poll Frequency	Type	Credential	☑
+ UCS Chassis Discovery	327	15 mins	XSLT Config	UCS - QA	□
+ UCS Compute Rack Unit Discovery	361	15 mins	XSLT Config	UCS - QA	□
+ UCS Fabric Discovery	352	15 mins	XSLT Config	UCS - QA	□
+ UCS FEX Discovery	366	15 mins	XSLT Config	UCS - QA	□
+ UCS Root Cache	326	15 mins	XSLT Config	UCS - QA	□

2. The following Dynamic Applications should display in the list of Dynamic Applications aligned to the UCS Manager:

- "Cisco: UCS Chassis Discovery"
- "Cisco: UCS Compute Rack Unit Discovery"
- "Cisco: UCS Fabric Discovery"
- "Cisco: UCS FEX Discovery"
- "Cisco: UCS Root Cache"
- "Cisco: UCS Cluster Information"

If the listed Dynamic Applications have not been automatically aligned, you can align them manually. To do so:

1. For the "Cisco: UCS Root Cache" Dynamic Application, click the **[Action]** button in the **Dynamic Application Collections** page of the device and then select *Add Dynamic Application* from the menu. The **Dynamic Application Alignment** page appears.



2. In the ***Dynamic Applications*** field, select *Cisco: UCS Root Cache*.
3. In the ***Credentials*** field, select the SOAP/XML credential you configured for the UCS Manager.
4. Click the **[Save]** button.
5. Repeat steps 1–4 for the "Cisco: UCS Chassis Discovery" Dynamic Application.
6. Repeat steps 1–4 for the "Cisco: UCS Compute Rack Unit Discovery" Dynamic Application.
7. Repeat steps 1–4 for the "Cisco: UCS Fabric Discovery" Dynamic Application.
8. Repeat steps 1–4 for the "Cisco: UCS FEX Discovery" Dynamic Application.
9. Repeat steps 1-4 for the "Cisco: UCS Cluster Information" Dynamic Application.
10. After aligning the Dynamic Applications, click the **[Reset]** button and then click the plus icon (+) for the Dynamic Application. If collection for the Dynamic Application was successful, the graph icons (📊) for the Dynamic Application are enabled.
11. Click a graph icon (📊) to view the collected data. The **Configuration Report** page will display the number of components of each type and the total number of components managed by the device.

NOTE: In addition to the Dynamic Applications that might need to be manually aligned to the UCS Manager, you can also opt to manually align the "Cisco: UCS Fault Configuration" Dynamic Application to UCS C-Series Rack Mount Server component devices. Doing so allows fault alerts to appear in the device log for those rack units.

Availability for Component Devices

The Dynamic Applications that discover the component devices in a UCS system include collection objects that define the availability status of those component devices.

The following types of component devices are considered unavailable if the UCS system does not include information about those components in the appropriate response:

- Blade
- Chassis
- Compute Rack Unit
- Fabric Extender
- Fabric Interconnect
- IO Module
- Service Profile

Relationships with Other Types of Component Devices

In addition to the parent/child relationships between component devices, the Dynamic Applications in the *Cisco: UCS* PowerPack automatically create relationships between the following Cisco UCS component devices:

- UCS Blades and UCS IO Modules
- UCS Compute Rack Units and UCS Fabric Extenders
- UCS Fabric Interconnects and UCS Fabric Extenders
- UCS Fabric Interconnects and UCS IO Modules

Additionally, SL1 can automatically build relationships between Cisco UCS component devices and other associated devices. If you discover one or more of the following:

- A Cisco Hyperflex cluster using the Dynamic Applications in the *Cisco: Hyperflex* PowerPack
- A Cisco Nexus switch using the Dynamic Applications in the *Cisco Base Pack* PowerPack
- An EMC VNX LUN using the Dynamic Applications in the *EMC: VNX* PowerPack
- An EMC XtremIO LUN using the Dynamic Applications in the *Dell EMC: XtremIO* PowerPack
- A NetApp device using the Dynamic Applications in the *NetApp Base Pack* PowerPack
- A vCenter device using the Dynamic Applications in the *VMware vSphere Base Pack* PowerPack

SL1 will automatically create relationships between the following types of component devices, where appropriate:

- Cisco Hyperflex clusters and UCS Rack Servers
- Cisco Nexus switches and UCS Fabric Interconnects
- EMC VNX LUNs and UCS Service Profiles
- EMC XtremIO LUNs and UCS Service Profiles
- NetApp LUNs and UCS Service Profiles
- NetApp Volumes and UCS Service Profiles
- VMware Hosts and UCS Service Profiles

Chapter 22

Cisco: UCS Director

Overview

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

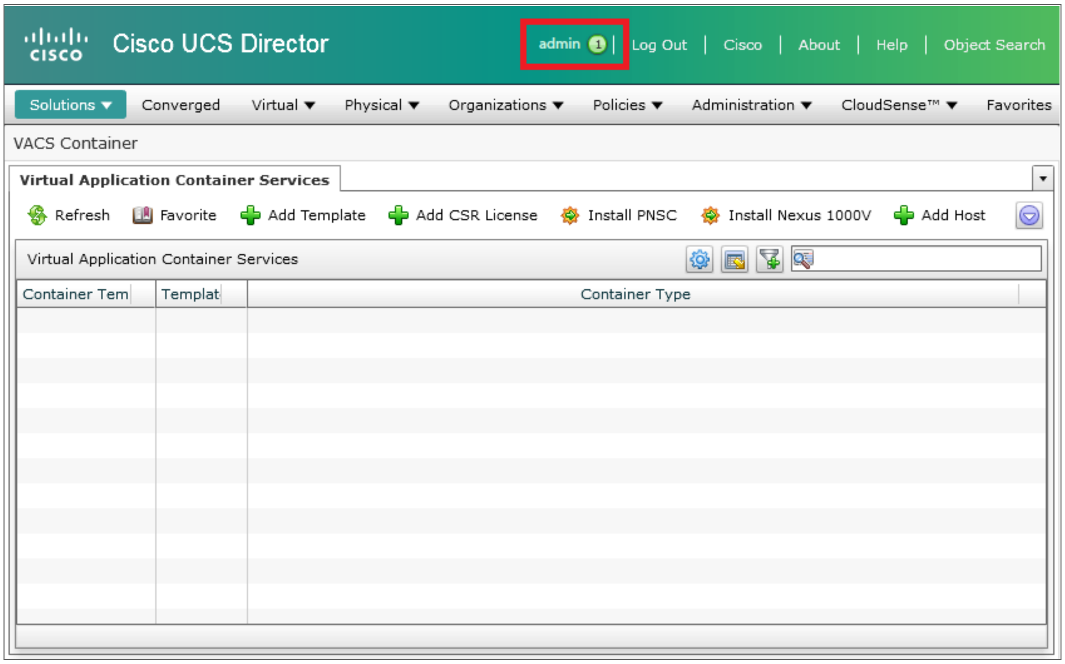
NOTE: For more information about the *Cisco: UCS Director* PowerPack, see the ***Monitoring Cisco Unified Computing System (UCS) Director*** manual.

Copying the REST API Access Key for a UCS Director Account

When *configuring the Basic/Snippet credential* that SL1 uses to discover and monitor UCS Director, you must include the REST API Access Key for a UCS Director administrator user account as the credential password.

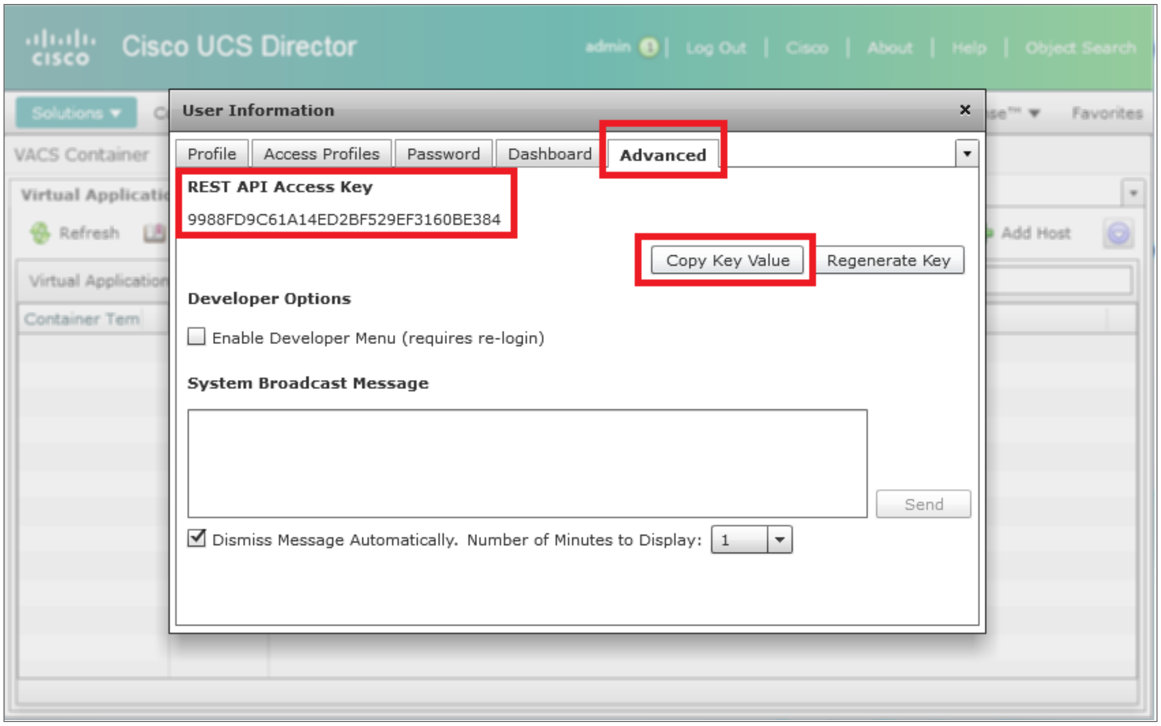
To locate and copy the REST API Access Key:

1. Log in to UCS Director as an administrator, and then click the username at the top of the page.



2. The **User Information** modal page appears. Click the **[Advanced]** tab.

3. Click the **[Copy Key Value]** button to copy the REST API Access Key.



User Information

REST API Access Key

9988FD9C61A14ED2BF529EF3160BE384

Developer Options

□ Enable Developer Menu (requires re-login)

System Broadcast Message

☑ Dismiss Message Automatically. Number of Minutes to Display: 1

Configuring a UCS Director Credential

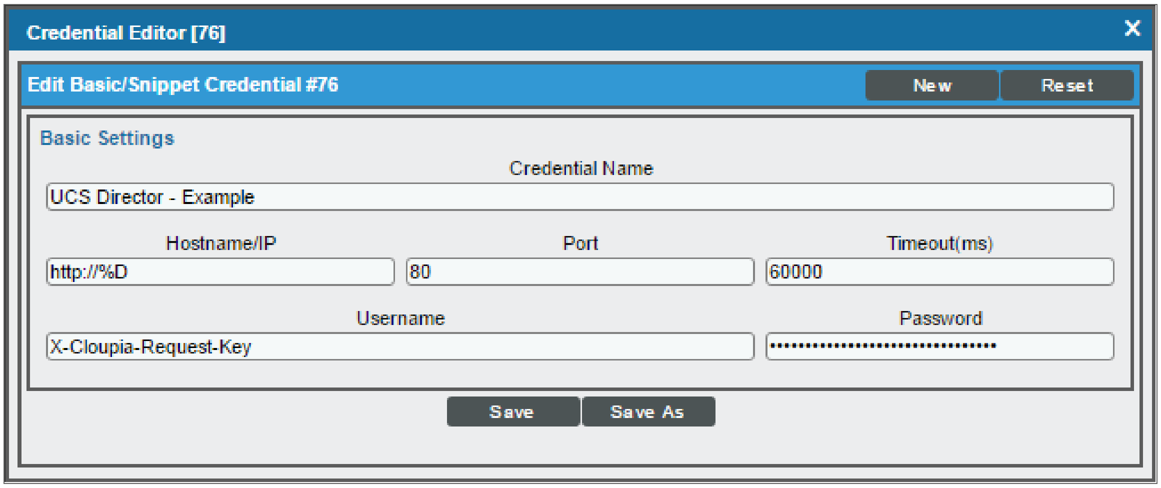
To configure SL1 to monitor UCS Director, you must first create a Basic/Snippet credential. This credential allows the Dynamic Applications in the *Cisco: UCS Director* PowerPack to connect with a UCS Director server. An example Basic/Snippet credential that you can edit for your own use is included in the *Cisco: UCS Director* PowerPack.

To create a Basic/Snippet credential to access a UCS Director server:

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

2. Locate the **UCS Director - Example** credential, then click its wrench icon (🔧). The **Edit Basic/Snippet Credential** modal page appears.

3. Enter values in the following fields:



Credential Editor [76]

Edit Basic/Snippet Credential #76

Basic Settings

Credential Name: UCS Director - Example

Hostname/IP: http://%D

Port: 80

Timeout(ms): 60000

Username: X-Cloupia-Request-Key

Password: ••••••••••••••••••••••••••••••••

- ***Credential Name***. Enter a new name for the UCS Director credential.
- ***Hostname/IP***. Enter "http://%D".
- ***Port***. Enter "80".
- ***Timeout***. Enter "60000".
- ***Username***. Keep the default value.
- ***Password***. Enter the REST API Access Key that you located in the section *Copying the REST API Access Key for a UCS Director Account*.

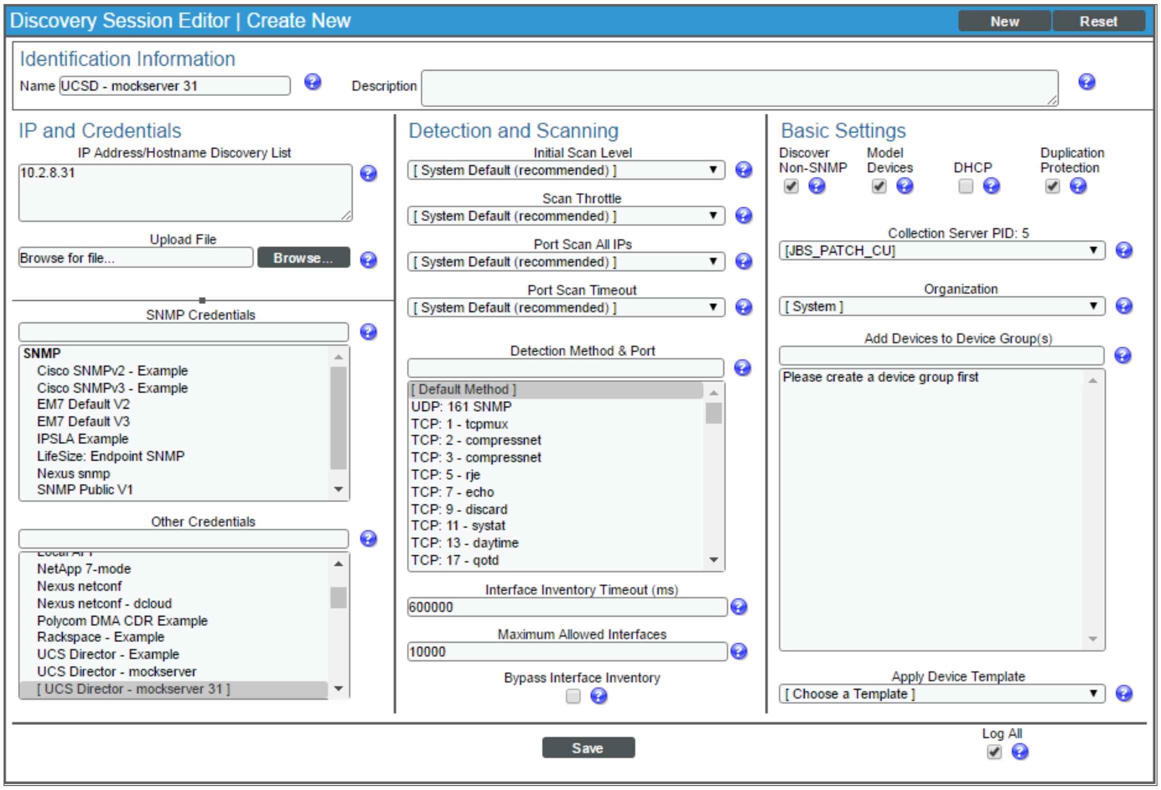
4. Click the **[Save As]** button.
5. When the confirmation message appears, click **[OK]**.

Discovering UCS Director

To create and run a discovery session that will discover UCS Director, perform the following steps:

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

2. Click the **[Create]** button to create a new discovery session. The **Discovery Session Editor** window appears:



Name: UCSD - mockserver 31

Description:

IP Address/Hostname Discovery List: 10.2.8.31

Upload File: Browse for file...

SNMP Credentials:
SNMP
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
EM7 Default V2
EM7 Default V3
IPSLA Example
LifeSize: Endpoint SNMP
Nexus snmp
SNMP Public V1

Other Credentials:
Local API
NetApp 7-mode
Nexus netconf
Nexus netconf - dcloud
Polycom DMA CDR Example
Rackspace - Example
UCS Director - Example
UCS Director - mockserver
[UCS Director - mockserver 31]

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: □

Discover Non-SNMP: ☑ | Model Devices: ☑ | DHCP: □ | Duplication Protection: ☑

Collection Server PID: 5: [JBS_PATCH_CU]

Organization: [System]

Add Devices to Device Group(s): Please create a device group first

Apply Device Template: [Choose a Template]

Log All: ☑

3. Edit the following fields in the **Discovery Session Editor** window:

   - ***Name***. Enter a name for the discovery session.
   - ***IP Address/Hostname Discovery List***. Enter the IP address for UCS Director.
   - ***Other Credentials***. Select the *Basic/Snippet credential that you created for UCS Director*.
   - ***Discover Non-SNMP***. 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. The **Discovery Session** window appears. When UCS Director is discovered, click its device icon (🖥) to view the **Device Properties** page for the UCS Director server.

Chapter 23

Cisco: UCS Standalone Rack Server

Overview

The following sections describe how to configure and discover a Cisco Unified Computing System (UCS) Rack Server for monitoring by SL1 using the *Cisco: UCS Standalone Rack Server* PowerPack:

NOTE: For more information about the *Cisco: UCS Standalone Rack Server* PowerPack, see the ***Monitoring Cisco Unified Computing System (UCS) Standalone Rack Servers*** manual.

Prerequisites for Monitoring Cisco UCS Standalone Rack Servers

In order to monitor Cisco UCS standalone rack servers in SL1 using the *Cisco: UCS Standalone Rack Server* PowerPack, you must know the username and password for a web service user on the rack servers you want to monitor.

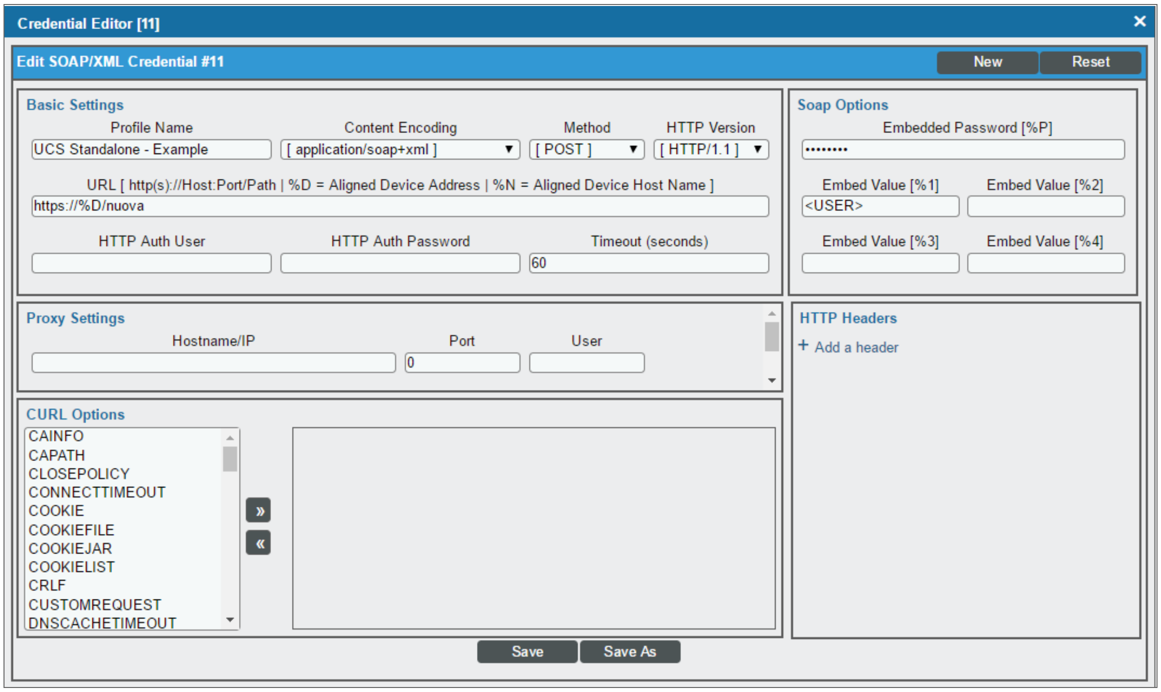
Configuring a SOAP/XML Credential

To monitor Cisco UCS rack servers, you must configure a SOAP/XML credential for the UCS web service. This credential enables the Dynamic Applications in the *Cisco: UCS Standalone Rack Server* PowerPack to automatically discover and align to your UCS rack servers.

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

To do so:

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



Credential Editor [11]

Edit SOAP/XML Credential #11

Basic Settings

Profile Name: UCS Standalone - Example
Content Encoding: [application/soap+xml]
Method: [POST]
HTTP Version: [HTTP/1.1]
URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://%D/nuova
HTTP Auth User:
HTTP Auth Password:
Timeout (seconds): 60

Soap Options

Embedded Password [%P]: ••••••••
Embed Value [%1]: <USER>
Embed Value [%2]:
Embed Value [%3]:
Embed Value [%4]:

Proxy Settings

Hostname/IP:
Port: 0
User:

HTTP Headers

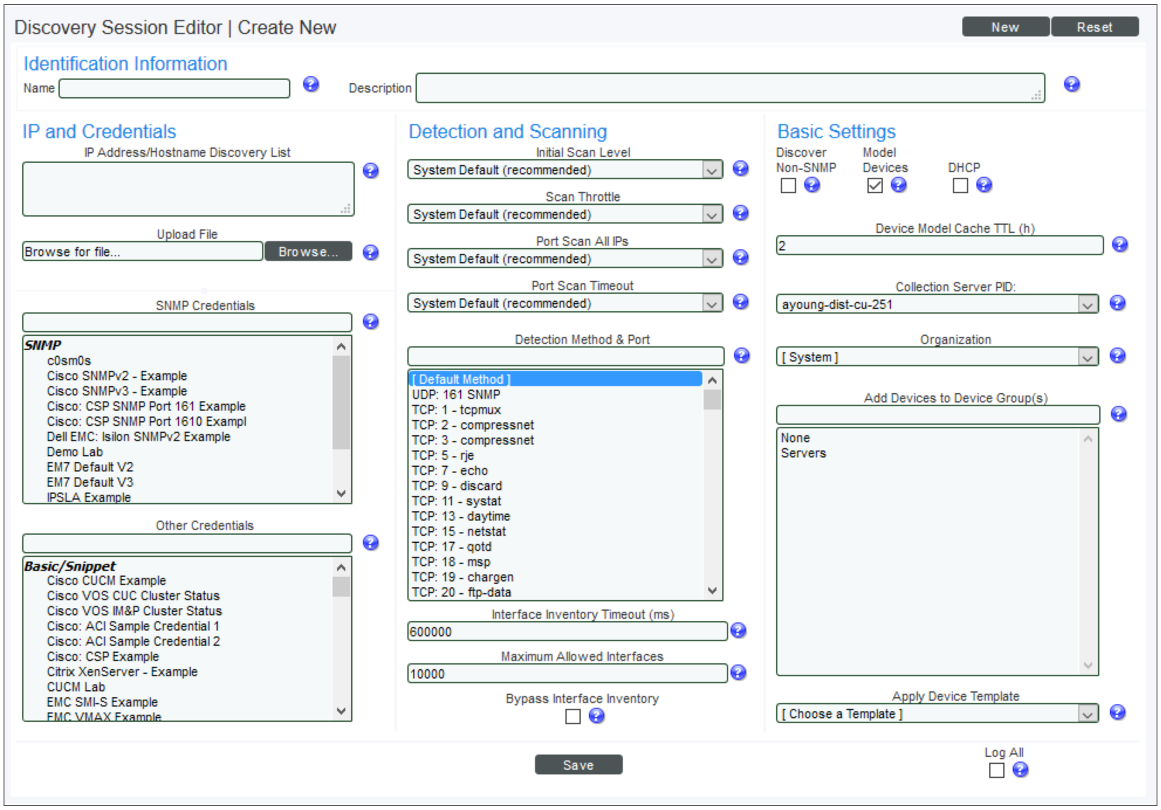
CURL Options

3. Supply values in the following fields:
   - ***Profile Name***. Type a name for the credential.
   - ***URL***. Type "https://%D/nuova".
   - ***Embed Value [%1]***. Type the username for a web service user on your UCS rack server.
   - ***Embedded Password [%P]***. Type the password for the user account on your UCS rack server.
4. Click the **[Save As]** button.

Discovering a UCS Rack Server

To create and run a discovery session that will discover a UCS Rack Server, perform the following steps:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. Click the **[Create]** button to create a new discovery session. The **Discovery Session Editor** window appears:



Discovery Session Editor | Create New

Identification Information

Name:

Description:

IP and Credentials

IP Address/Hostname Discovery List:

Upload File: Browse for file...

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]

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: ayoung-dist-cu-251

Organization: [System]

Add Devices to Device Group(s):

Apply Device Template: [Choose a Template]

Log All: □

3. Supply values in the following fields:
   - ***IP Address Discovery List***. Type the IP address for the UCS Rack Server.
   - ***Other Credentials***. Select the SOAP/XML credential that you created for the UCS Rack Server.
   - ***Initial Scan Level***. Select *5. Deep Discovery*.
   - ***Detection Method & Port***. Select *443 - HTTPS*. You can select additional ports, but you must include port 443 - HTTPS.
   - ***Discover Non-SNMP***. Select this checkbox.
4. Optionally, you can supply 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 displays 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. After several minutes, the UCS Rack Server should be discovered with the appropriate Dynamic Applications aligned to it. Click its device icon ( ) to view the **Device Properties** page for the UCS Rack Server server.

Chapter

24

Cisco: Unity Express

Overview

The following sections describe how to configure and discover Cisco Unity Express voice mailboxes for monitoring by SL1 using the *Cisco: Unity Express* PowerPack:

NOTE: For more information about the *Cisco: Unity Express* PowerPack, see the ***Monitoring Cisco Unity Express*** manual.

Prerequisites for Monitoring Cisco Unity Express

To configure the SL1 system to monitor Cisco Unity Express voice mailboxes using the *Cisco: Unity Express* PowerPack, you must first have the following information about the Unity Express voice mailboxes that you want to monitor:

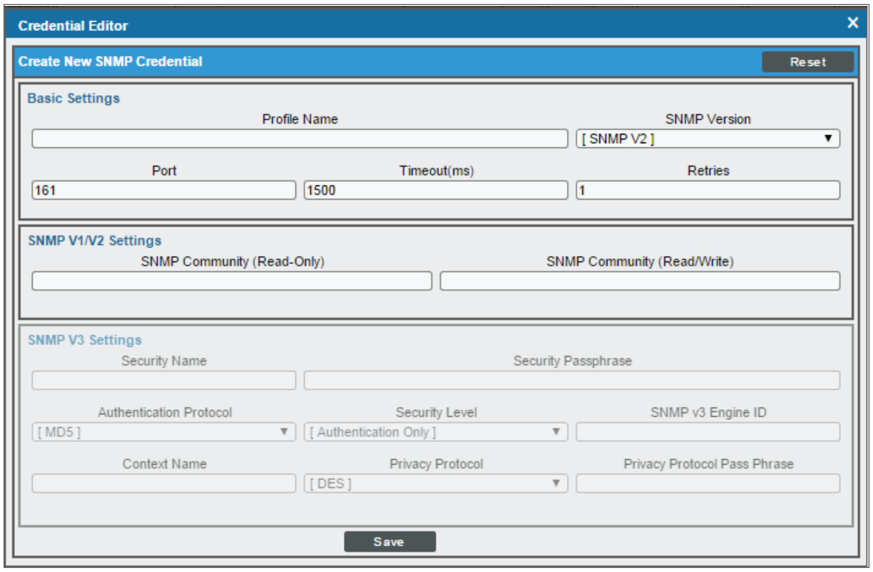
- IP addresses for the voice mailboxes
- SNMP community strings for the voice mailboxes

Creating an SNMP Credential for Cisco Unity Express

SL1 uses SNMP to collect information about Cisco Unity Express services. To monitor Unity Express, you must first create an SNMP credential that enables SL1 to communicate with these services.

To create an SNMP credential for Cisco Unity Express:

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:



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:

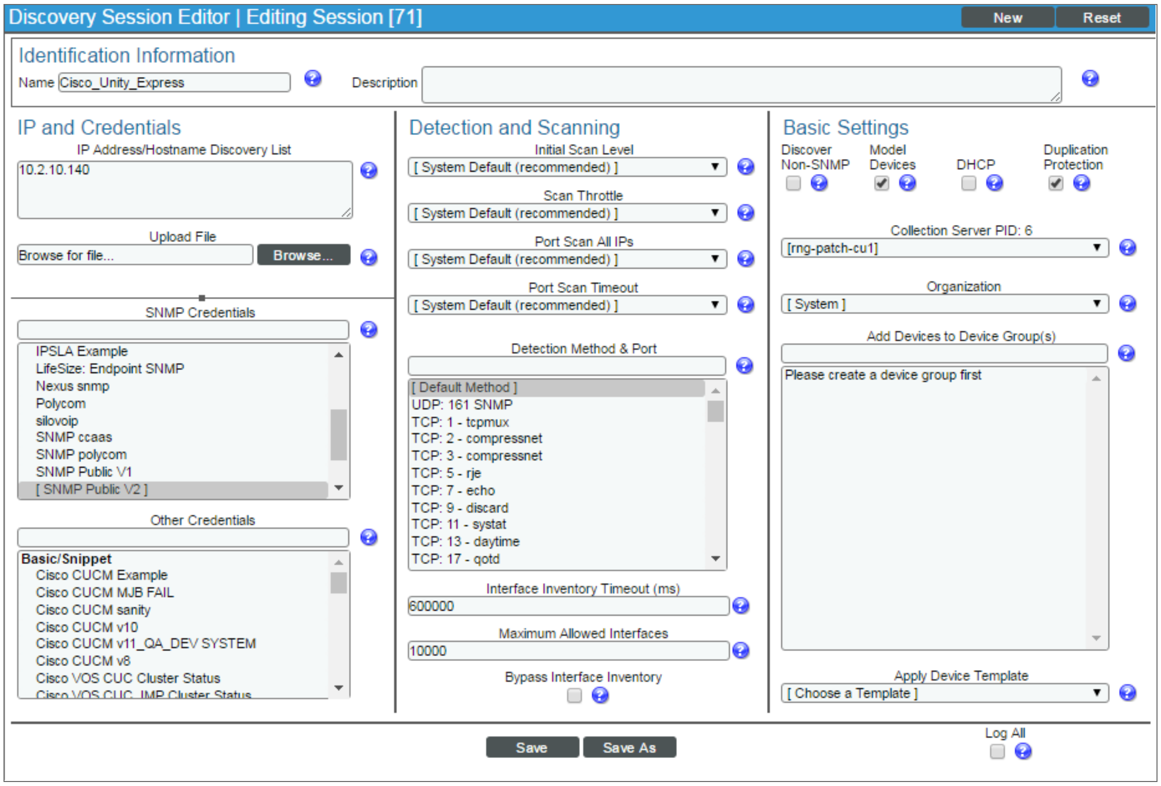
4. In the ***Profile Name*** field, enter a name for the credential.
5. In the ***SNMP Version*** field, select *SNMP V2*.
6. In the ***SNMP Community (Read Only)*** field, enter the community string for the Cisco Unity Express voice mailbox you want to monitor.
7. Optionally, supply values in the other fields in this page. In most cases, you can accept the default values for the other fields.
8. Click the **[Save]** button.

Discovering Cisco Unity Express Services

To create and run a discovery session that will discover Cisco Unity Express services, perform the following steps:

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

2. Click the **[Create]** button to create a new discovery session. The **Discovery Session Editor** page appears:



Discovery Session Editor | Editing Session [71]

Identification Information

Name: Cisco_Unity_Express

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.2.10.140

Upload File: Browse for file...

SNMP Credentials: IPSLA Example, LifeSize: Endpoint SNMP, Nexus snmp, Polycom, silovoip, SNMP ccaas, SNMP polycom, SNMP Public V1, [SNMP Public V2]

Other Credentials: Basic/Snippet: Cisco CUCM Example, Cisco CUCM MJB FAIL, Cisco CUCM sanity, Cisco CUCM v10, Cisco CUCM v11_QA_DEV SYSTEM, Cisco CUCM v8, Cisco VOS CUC Cluster Status, Cisco VOS CUC IMP Cluster Status

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: 6: [rng-patch-cu1]

Organization: [System]

Add Devices to Device Group(s): Please create a device group first

Apply Device Template: [Choose a Template]

Log All: □

3. Enter values in the following fields:

- ***IP Address Discovery List***. Enter the IP address(es) for the Cisco Unity Express voice mailbox(es).
- ***SNMP Credential***. Select the *SNMP credential that you created for Cisco Unity Express*.

4. You can enter values in the other fields on this page, but are not required to and can simply accept the default values. For more information about the other fields on this page, see the ***Discovery and Credentials*** manual.

5. Click **[Save]** 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.

8. When the Cisco Unity Express voice mailbox is discovered, click its device icon () to view its **Device Properties** page.

Chapter

25

Cisco: Viptela

Overview

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

NOTE: For more information about the *Cisco: Viptela*PowerPack, see the ***Monitoring Cisco Viptela*** manual.

Prerequisite for Monitoring Cisco Viptela

To configure the SL1 system to monitor Cisco Viptela resources using the *Cisco: Viptela* PowerPack, you must first know the credentials (username and password) for a user account that has access to the Cisco Viptela system. The user account must have read-all access.

Configuring a Credential for Cisco Viptela

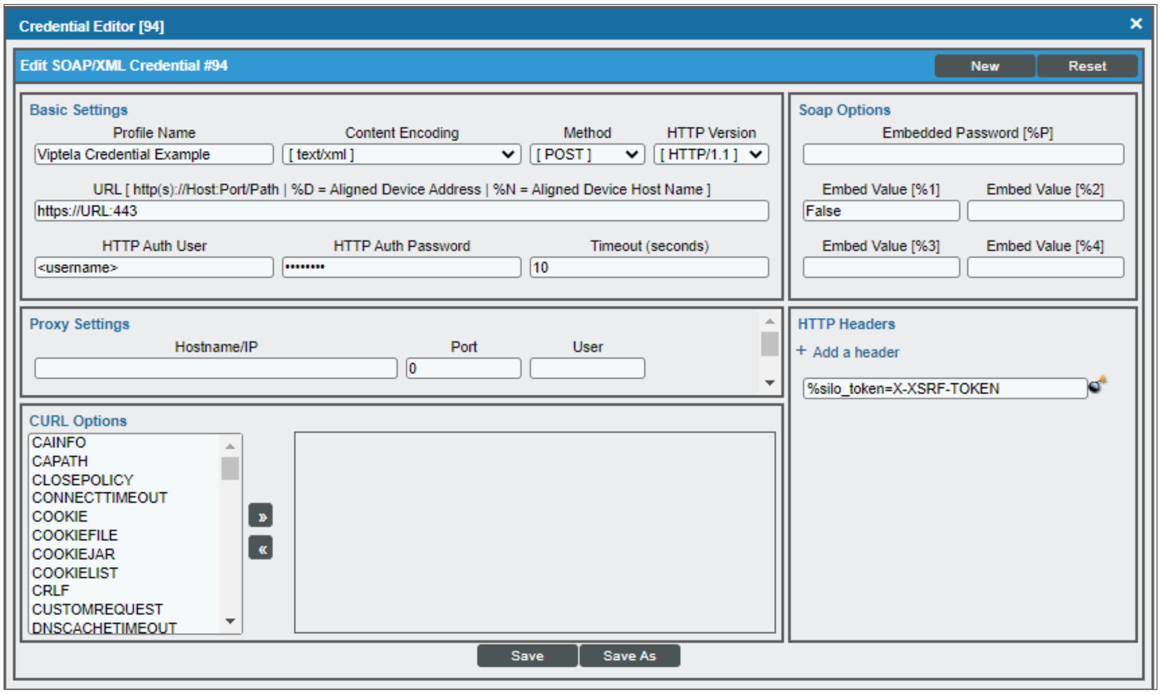
To configure SL1 to monitor Cisco: Viptela devices, you must first create a SOAP/XML credential. This credential allows the Dynamic Applications in the *Cisco: Viptela* PowerPack) to use your Cisco: Viptela user account to retrieve information from the *Cisco: Viptela* devices.

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

To configure a SOAP/XML credential to access Cisco: Viptela:

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

2. Locate the **Viptela Credential Example - SOAP/XML** credential, and then click its wrench icon (). The **Edit SOAP/XML Credential** modal page appears:



Edit SOAP/XML Credential #94

Profile Name: Viptela Credential Example

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://URL:443

HTTP Auth User: <username>

HTTP Auth Password: ••••••••

Timeout (seconds): 10

Embedded Password [%P]:

Embed Value [%1]: False

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

Hostname/IP:

Port: 0

User:

%silo_token=X-XSRF-TOKEN

CAINFO
CAPATH
CLOSEPOLICY
CONNECTTIMEOUT
COOKIE
COOKIEFILE
COOKIEJAR
COOKIELIST
CRLF
CUSTOMREQUEST
DNSCACHETIMEOUT

3. Complete the following fields:

   - ***Profile Name***. Type a name for the Cisco: Viptela credential.
   - ***Content Encoding***. Select *text/xml*.
   - ***Method***. Select POST.
   - ***HTTP Version***. Select HTTP/1.1.
   - ***URL***. Type the URL and port for the Cisco: Viptela system, using the following format: *https://URL:443*. For example, https://my.viptela.system:443.
   - ***HTTP Auth User***. Type the Cisco: Viptela account username.

- ***HTTP Auth Password***. Type the Cisco: Viptela account password.
- ***Timeout (seconds)***. Type "10".

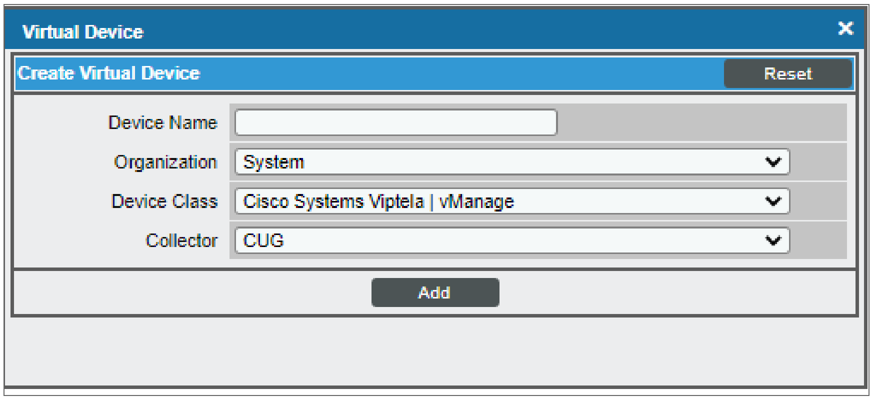
4. For the remaining fields, use the default values, and then click the **[Save As]** button.

Creating a Cisco Viptela Virtual Device

Because the Cisco: Viptela service does not have a static IP address, you cannot discover a Cisco: Viptela device using discovery. Instead, you must create a ***virtual device*** that represents the Cisco: Viptela service. A virtual device is a user-defined container that represents a device or service that cannot be discovered by SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications.

To create a virtual device that represents your Cisco: Viptela service:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Click the **[Actions]** button and select *Create Virtual Device* from the menu. The **Virtual Device** modal page appears:



Virtual Device

Create Virtual Device

Device Name	
Organization	System
Device Class	Cisco Systems Viptela | vManage
Collector	CUG

3. Complete the following fields:
   - ***Device Name***. Type a name for the device.
   - ***Organization***. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.
   - ***Device Class***. Select *Cisco Systems Viptela | vManage*.
   - ***Collector***. Select the collector group that will monitor the device.
4. Click **[Add]** to create the virtual device.

Aligning Dynamic Applications to the Virtual Device

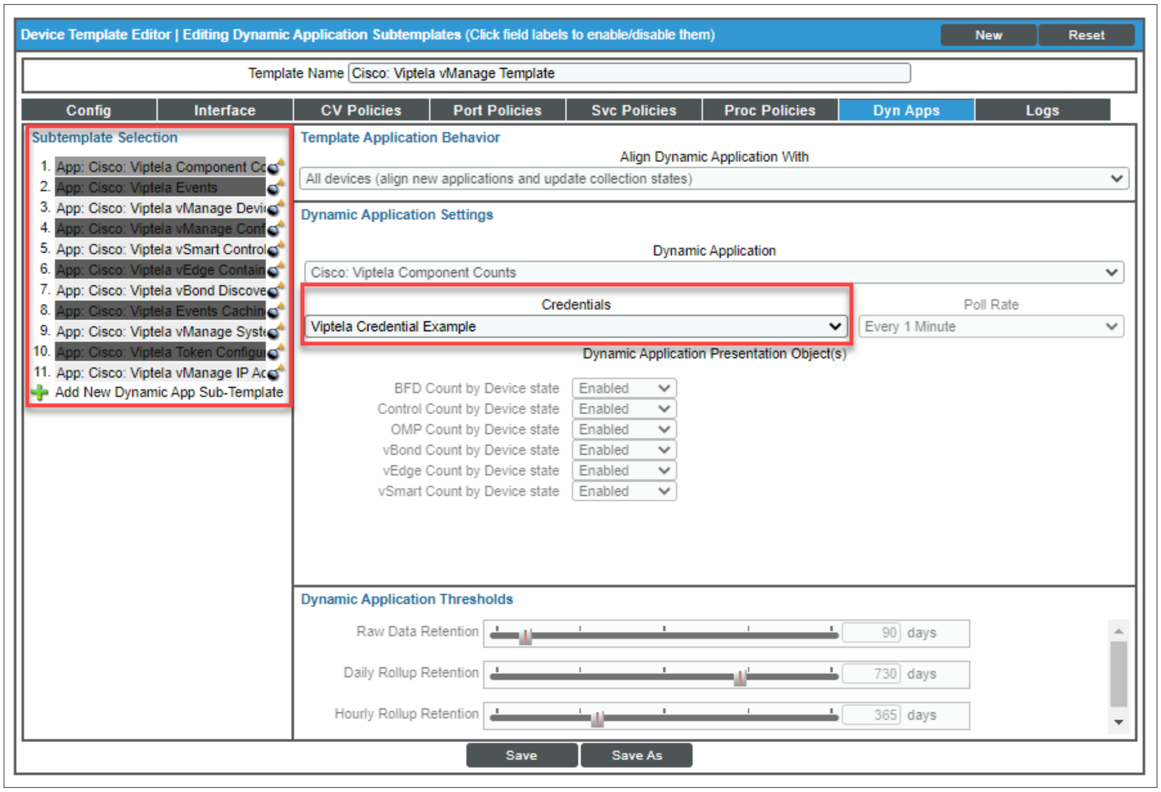
A ***device template*** allows you to save a device configuration and apply it to multiple devices. The *Cisco: Viptela* PowerPack includes the "Cisco: Viptela vManage Template," which enables the SL1 to align all Dynamic Applications to the root component device.

Configuring the Device Template

Before you can use the "Cisco: Viptela vManage Template," you need to configure the template so that each dynamic application in the template aligns with the ***credential you created earlier***.

To configure the Viptela device template:

1. Go to the **Configuration Templates** page (Registry > Devices > Templates).
2. Locate the "Cisco: Viptela vManage Template" and click its wrench icon (🔧). The **Device Template Editor** modal page appears.
3. Click the **[Dyn Apps]** tab. The **Editing Dynamic Application Subtemplates** page appears:



Device Template Editor | Editing Dynamic Application Subtemplates (Click field labels to enable/disable them)

Template Name: Cisco: Viptela vManage Template

Subtemplate Selection
1. App: Cisco: Viptela Component Co
2. App: Cisco: Viptela Events
3. App: Cisco: Viptela vManage Devic
4. App: Cisco: Viptela vManage Conf
5. App: Cisco: Viptela vSmart Control
6. App: Cisco: Viptela vEdge Contain
7. App: Cisco: Viptela vBond Discove
8. App: Cisco: Viptela Events Cachin
9. App: Cisco: Viptela vManage Syste
10. App: Cisco: Viptela Token Configu
11. App: Cisco: Viptela vManage IP Ac

Add New Dynamic App Sub-Template

Template Application Behavior

Align Dynamic Application With: All devices (align new applications and update collection states)

Dynamic Application Settings

Dynamic Application: Cisco: Viptela Component Counts

Credentials: Viptela Credential Example

Poll Rate: Every 1 Minute

Dynamic Application Presentation Object(s)

BFD Count by Device state	Enabled
Control Count by Device state	Enabled
OMP Count by Device state	Enabled
vBond Count by Device state	Enabled
vEdge Count by Device state	Enabled
vSmart Count by Device state	Enabled

Dynamic Application Thresholds

Raw Data Retention	90 days
Daily Rollup Retention	730 days
Hourly Rollup Retention	365 days

4. In the ***Credentials*** drop-down list, select the credential that you created for Viptela.
5. Click the next Dynamic Application listed in the **Subtemplate Selection** section on the left side of the page and then select the credential you created in the ***Credentials*** field.

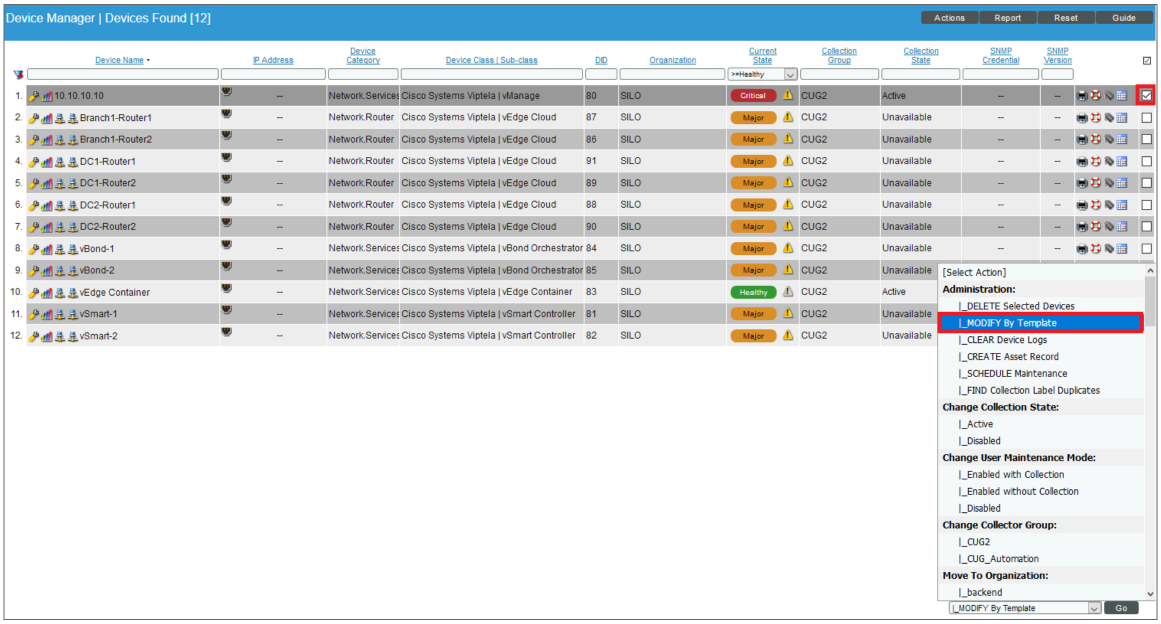
6. Repeat step 5 until you have selected that credential in the ***Credentials*** field for all of the Dynamic Applications listed in the **Subtemplate Selection** section.
7. Click **[Save]**.

Using the Device Template to Align Dynamic Applications to the Component Device

After you have configured the "Cisco: Viptela vManage Template" so that each dynamic application in the template aligns with the credential you created, you can use that template to align the Dynamic Applications to the root component device for Cisco: Viptela.

To use the "Viptela vManage Template" to align Dynamic Applications:

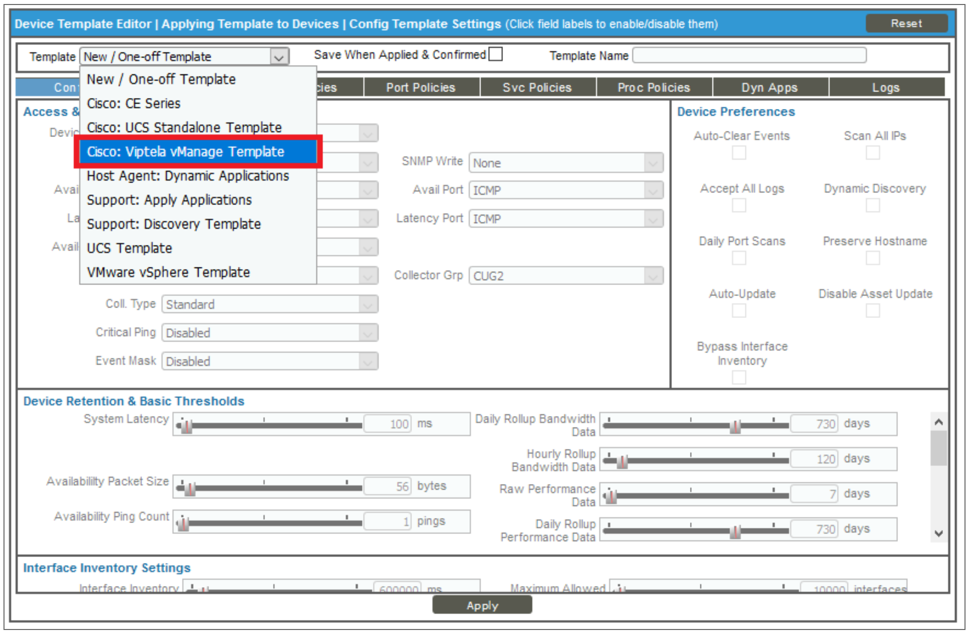
1. Go to the **Device Manager** page (Registry > Devices > Device Manager.
2. On the **Device Manager** page, select the checkbox for the root component device.



Device Manager | Devices Found [12]

	Device Name	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State	Collection Group	Collection State	SNMP Credential	SNMP Version	☑
							>=Healthy					
1.	10.10.10.10	--	Network.Services	Cisco Systems Viptela | vManage	80	SILO	Critical	CUG2	Active	--	--	☑
2.	Branch1-Router1	--	Network.Router	Cisco Systems Viptela | vEdge Cloud	87	SILO	Major	CUG2	Unavailable	--	--	☐
3.	Branch1-Router2	--	Network.Router	Cisco Systems Viptela | vEdge Cloud	86	SILO	Major	CUG2	Unavailable	--	--	☐
4.	DC1-Router1	--	Network.Router	Cisco Systems Viptela | vEdge Cloud	91	SILO	Major	CUG2	Unavailable	--	--	☐
5.	DC1-Router2	--	Network.Router	Cisco Systems Viptela | vEdge Cloud	89	SILO	Major	CUG2	Unavailable	--	--	☐
6.	DC2-Router1	--	Network.Router	Cisco Systems Viptela | vEdge Cloud	88	SILO	Major	CUG2	Unavailable	--	--	☐
7.	DC2-Router2	--	Network.Router	Cisco Systems Viptela | vEdge Cloud	90	SILO	Major	CUG2	Unavailable	--	--	☐
8.	vBond-1	--	Network.Services	Cisco Systems Viptela | vBond Orchestrator	84	SILO	Major	CUG2	Unavailable	--	--	☐
9.	vBond-2	--	Network.Services	Cisco Systems Viptela | vBond Orchestrator	85	SILO	Major	CUG2	Unavailable			
10.	vEdge Container	--	Network.Services	Cisco Systems Viptela | vEdge Container	83	SILO	Healthy	CUG2	Active			
11.	vSmart-1	--	Network.Services	Cisco Systems Viptela | vSmart Controller	81	SILO	Major	CUG2	Unavailable			
12.	vSmart-2	--	Network.Services	Cisco Systems Viptela | vSmart Controller	82	SILO	Major	CUG2	Unavailable			

3. In the ***Select Actions*** field, in the lower right, select the option *MODIFY by Template* and click the **[Go]** button. The **Device Template Editor** page appears:



Device Template Editor | Applying Template to Devices | Config Template Settings (Click field labels to enable/disable them)

Template: New / One-off Template

Save When Applied & Confirmed □

Template Name:

SNMP Write: None

Avail Port: ICMP

Latency Port: ICMP

Collector Grp: CUG2

Coll. Type: Standard

Critical Ping: Disabled

Event Mask: Disabled

System Latency: 100 ms

Availability Packet Size: 56 bytes

Availability Ping Count: 1 pings

Daily Rollup Bandwidth Data: 730 days

Hourly Rollup Bandwidth Data: 120 days

Raw Performance Data: 7 days

Daily Rollup Performance Data: 730 days

Interface Inventory: 600000 ms

Maximum Allowed: 10000 interfaces

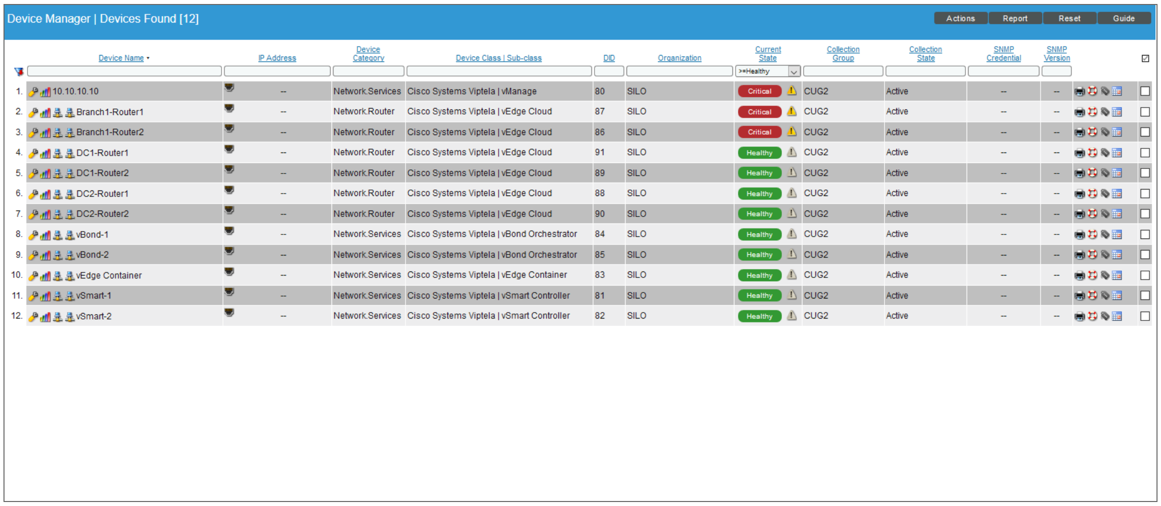
4. Complete the following fields:

   - In the ***Template*** drop-down list, select *Cisco: Viptela vManage Template*.
   - In the ***Credentials*** drop-down list, select the credential you created earlier.

5. Click the **[Apply]** button, and then click **[Confirm]** to align the Dynamic Applications to the root component device.

You can view all the devices, virtual devices, and component devices in the Cisco: Viptela system in the following places in the user interface:

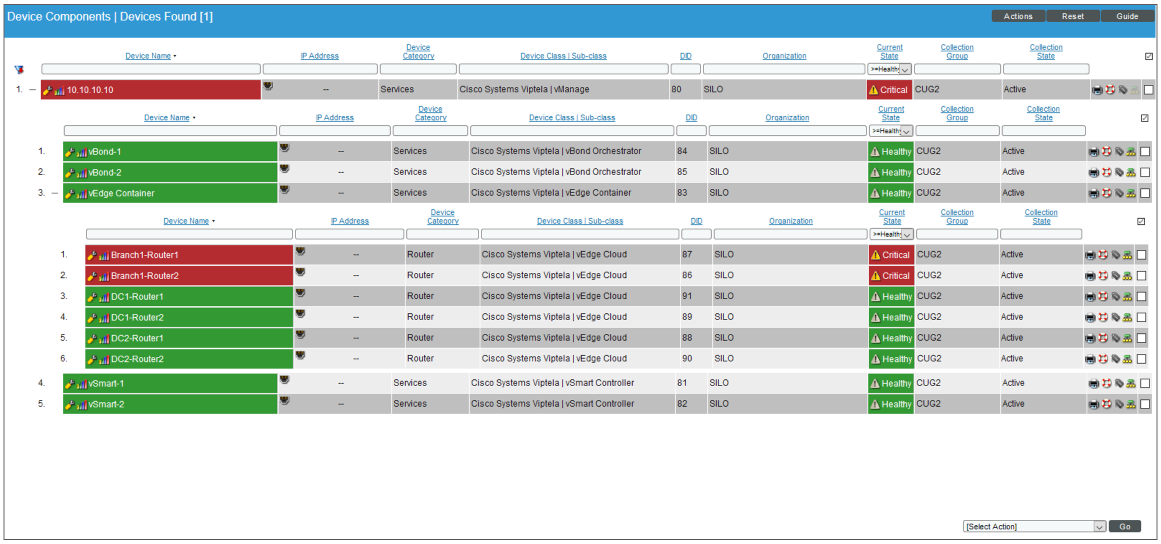
- All devices, virtual devices, and component devices appear in the **Device Manager** page (Registry > Devices > Device Manager).



Device Manager | Devices Found [12]

	Device Name	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State	Collection Group	Collection State	SNMP Credential	SNMP Version	☑
							>=Healthy					
1.	10.10.10.10	--	Network.Services	Cisco Systems Viptela | vManage	80	SILO	Critical	CUG2	Active	--	--	□
2.	Branch1-Router1	--	Network.Router	Cisco Systems Viptela | vEdge Cloud	87	SILO	Critical	CUG2	Active	--	--	□
3.	Branch1-Router2	--	Network.Router	Cisco Systems Viptela | vEdge Cloud	86	SILO	Critical	CUG2	Active	--	--	□
4.	DC1-Router1	--	Network.Router	Cisco Systems Viptela | vEdge Cloud	91	SILO	Healthy	CUG2	Active	--	--	□
5.	DC1-Router2	--	Network.Router	Cisco Systems Viptela | vEdge Cloud	89	SILO	Healthy	CUG2	Active	--	--	□
6.	DC2-Router1	--	Network.Router	Cisco Systems Viptela | vEdge Cloud	88	SILO	Healthy	CUG2	Active	--	--	□
7.	DC2-Router2	--	Network.Router	Cisco Systems Viptela | vEdge Cloud	90	SILO	Healthy	CUG2	Active	--	--	□
8.	vBond-1	--	Network.Services	Cisco Systems Viptela | vBond Orchestrator	84	SILO	Healthy	CUG2	Active	--	--	□
9.	vBond-2	--	Network.Services	Cisco Systems Viptela | vBond Orchestrator	85	SILO	Healthy	CUG2	Active	--	--	□
10.	vEdge Container	--	Network.Services	Cisco Systems Viptela | vEdge Container	83	SILO	Healthy	CUG2	Active	--	--	□
11.	vSmart-1	--	Network.Services	Cisco Systems Viptela | vSmart Controller	81	SILO	Healthy	CUG2	Active	--	--	□
12.	vSmart-2	--	Network.Services	Cisco Systems Viptela | vSmart Controller	82	SILO	Healthy	CUG2	Active	--	--	□

- 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 Cisco: Viptela, find the Cisco: Viptela root device and click its plus icon (**+**):



Device Components | Devices Found [1]

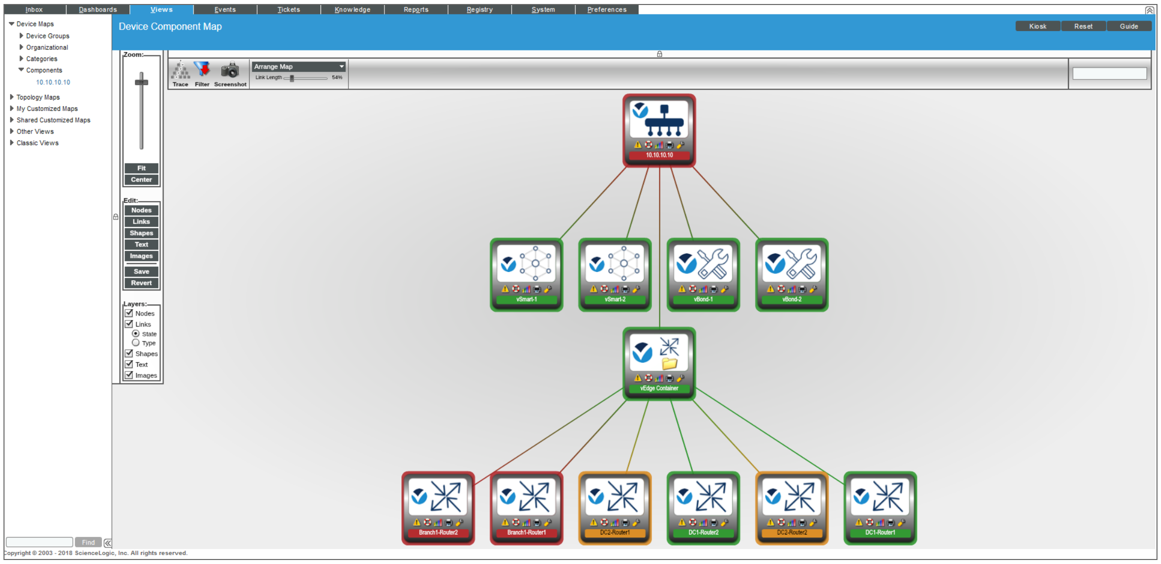
	Device Name	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State	Collection Group	Collection State	☑
							>=Healthy			
1. –	10.10.10.10	--	Services	Cisco Systems Viptela | vManage	80	SILO	Critical	CUG2	Active	□

	Device Name	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State	Collection Group	Collection State	☑
							>=Healthy			
1.	vBond-1	--	Services	Cisco Systems Viptela | vBond Orchestrator	84	SILO	Healthy	CUG2	Active	□
2.	vBond-2	--	Services	Cisco Systems Viptela | vBond Orchestrator	85	SILO	Healthy	CUG2	Active	□
3. –	vEdge Container	--	Services	Cisco Systems Viptela | vEdge Container	83	SILO	Healthy	CUG2	Active	□

	Device Name	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State	Collection Group	Collection State	☑
							>=Healthy			
1.	Branch1-Router1	--	Router	Cisco Systems Viptela | vEdge Cloud	87	SILO	Critical	CUG2	Active	□
2.	Branch1-Router2	--	Router	Cisco Systems Viptela | vEdge Cloud	86	SILO	Critical	CUG2	Active	□
3.	DC1-Router1	--	Router	Cisco Systems Viptela | vEdge Cloud	91	SILO	Healthy	CUG2	Active	□
4.	DC1-Router2	--	Router	Cisco Systems Viptela | vEdge Cloud	89	SILO	Healthy	CUG2	Active	□
5.	DC2-Router1	--	Router	Cisco Systems Viptela | vEdge Cloud	88	SILO	Healthy	CUG2	Active	□
6.	DC2-Router2	--	Router	Cisco Systems Viptela | vEdge Cloud	90	SILO	Healthy	CUG2	Active	□

	Device Name	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State	Collection Group	Collection State	
4.	vSmart-1	--	Services	Cisco Systems Viptela | vSmart Controller	81	SILO	Healthy	CUG2	Active	□
5.	vSmart-2	--	Services	Cisco Systems Viptela | vSmart Controller	82	SILO	Healthy	CUG2	Active	□

- The **Device 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 Cisco: Viptela devices, go to the **Component Map** page and select the map from the list in the left NavBar. To learn more about the **Component Map** page, see the ***Views*** manual.



Chapter 26

Cisco: Wireless

Overview

The following sections describe how to configure and discover Cisco wireless LAN controllers for monitoring by SL1 using the *Cisco: Wireless* PowerPack:

NOTE: For more information about the *Cisco: Wireless* PowerPack, see the ***Monitoring Cisco Wireless LAN Controllers*** manual.

Prerequisites for Monitoring Cisco WLC

Before you can monitor Cisco wireless LAN controllers using the *Cisco: Wireless* PowerPack, you must have the following information:

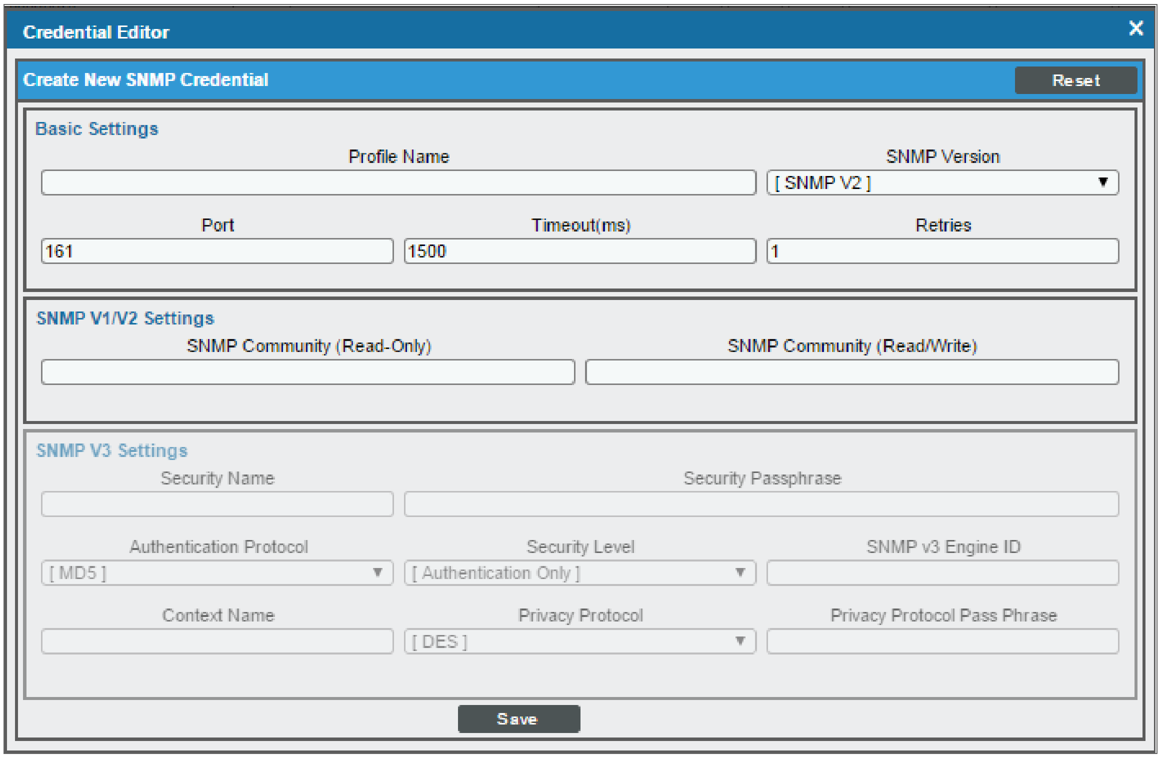
- The IP address of the WLC that you want to monitor with SL1
- The settings for an SNMP V2 or SNMP V3 credential that can be used to communicate with the WLC

Configuring a Cisco WLC SNMP Credential

To configure SL1 to monitor a Cisco WLC, you must first create a SNMP V2 or SNMP V3 credential. This credential allows the Dynamic Applications in the *Cisco: Wireless* PowerPack) to communicate with the WLC.

To create an SNMP credential for monitoring a WLC:

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



Credential Editor

Create New SNMP Credential

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. In the ***Profile Name*** field, type a name for the credential.
4. In the ***SNMP Version*** field, select *SNMP V2* or *SNMP V3*.

NOTE: Do not use an SNMP V1 credential for monitoring a WLC. Using an SNMP V1 credential will decrease the performance of the data collection process.

5. If you selected *SNMP V2*, then in the ***SNMP Community (Read Only)*** field, type the community string for the WLC.
6. If you selected *SNMP V3*, supply values in the following fields:

    - ***Security Name***. Type the SNMP user name for the WLC.

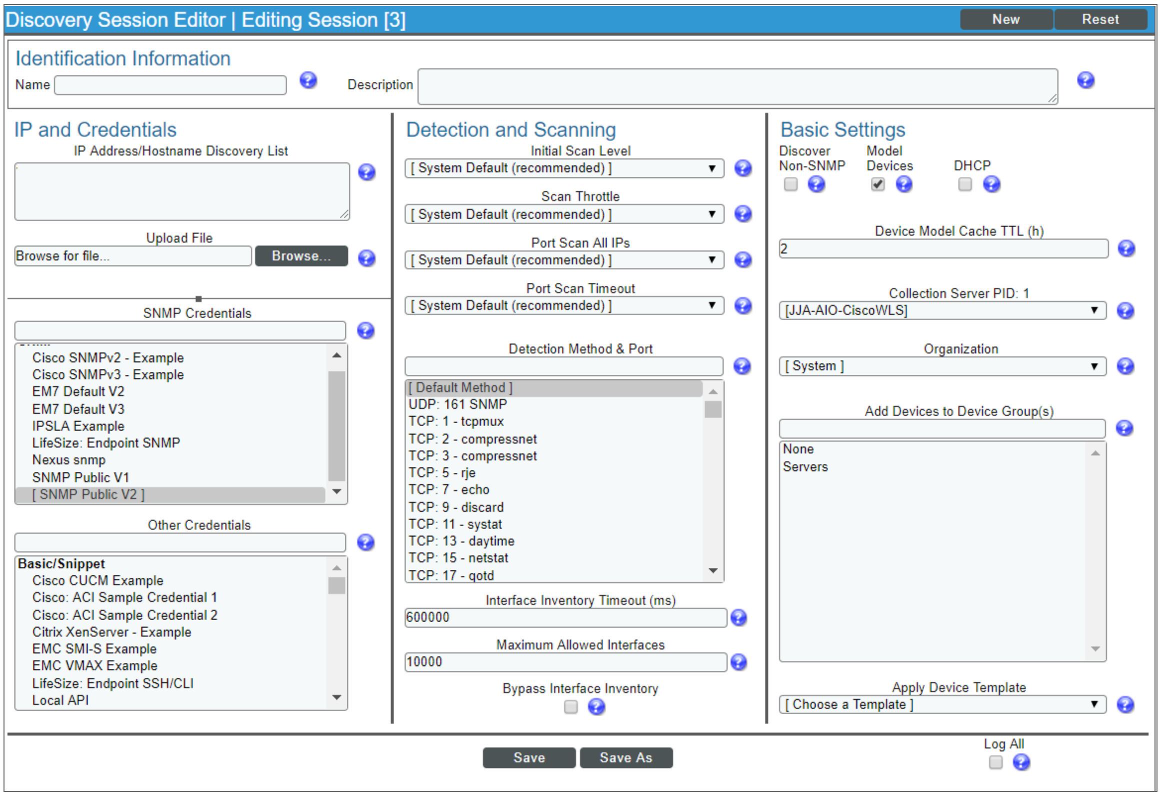
- ***Security Passphrase***. Type the passphrase for the SNMP user.
- ***Authentication Protocol***. If applicable, select the authentication protocol for the SNMP user.
- ***Security Level***. If applicable, select the security level that is applicable to the SNMP user.
- ***SNMP v3 Engine ID***. If applicable, type the SNMP V3 Engine ID for the SNMP user.
- ***Privacy Protocol***. If applicable, select the privacy protocol for the SNMP user.
- ***Privacy Protocol Pass Phrase***. If applicable, type the privacy protocol passphrase for the SNMP user.

7. Optionally, supply values in the other fields on this page. In most cases, you can use the default values for the other fields. For a description of the fields in this page, see the ***Discovery & Credentials*** manual.
8. Click **[Save]**.

Discovering Cisco WLC Devices

To discover Cisco WLC devices:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. Click the **[Create]** button. The **Discovery Session Editor** page appears:



Discovery Session Editor | Editing Session [3]

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]

Interface Inventory Timeout (ms): 600000

Maximum Allowed Interfaces: 10000

Bypass Interface Inventory: □

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

Device Model Cache TTL (h): 2

Collection Server PID: 1 [JJA-AIO-CiscoWLS]

Organization: [System]

Apply Device Template: [Choose a Template]

SNMP Credentials: [SNMP Public V2]

Log All: □

3. Supply values in the following fields:

   - ***Name***. Type a name for the discovery session.
   - ***IP Address Discovery List***. Type the IP address for the WLC.
   - ***SNMP Credentials***. Select the *SNMP credential you created for the WLC*.

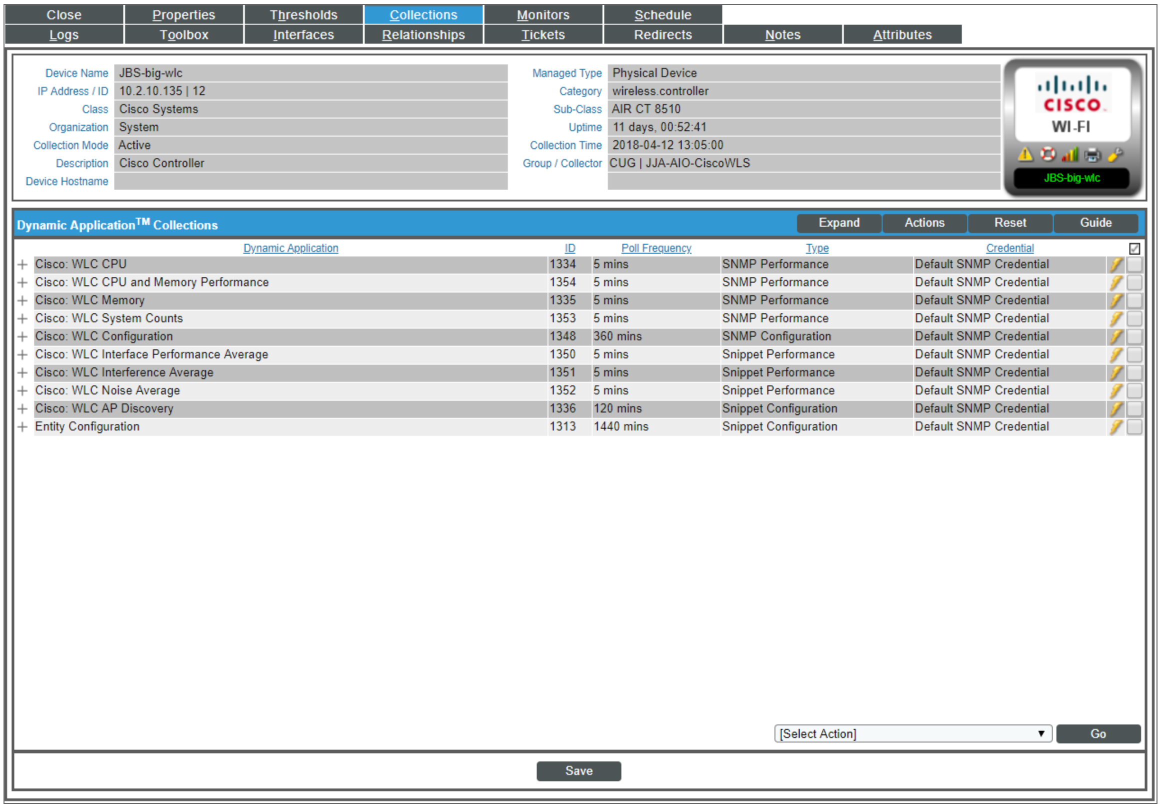
4. Optionally, supply values in the other fields in this page. In most cases, you can use the default values for the other fields. For a description of the fields in this page, see the ***Discovery & Credentials*** manual.
5. Click **[Save]**, then close the**Discovery Session Editor** page.
6. The **Discovery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

Verifying Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. In the **Discovery Session** page, click the device icon () for the newly discovered Cisco WLC device to view its **Device Properties** page.
2. From the **Device Properties** page for the Cisco WLC device, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.

3. The following Dynamic Applications should appear on the **Dynamic Application Collections** page for the WLC device:



Device Name	JBS-big-wlc	Managed Type	Physical Device
IP Address / ID	10.2.10.135 | 12	Category	wireless.controller
Class	Cisco Systems	Sub-Class	AIR CT 8510
Organization	System	Uptime	11 days, 00:52:41
Collection Mode	Active	Collection Time	2018-04-12 13:05:00
Description	Cisco Controller	Group / Collector	CUG | JJA-AIO-CiscoWLS
Device Hostname			

Dynamic Application^{TM} Collections

Dynamic Application	ID	Poll Frequency	Type	Credential	☑
Cisco: WLC CPU	1334	5 mins	SNMP Performance	Default SNMP Credential	□
Cisco: WLC CPU and Memory Performance	1354	5 mins	SNMP Performance	Default SNMP Credential	□
Cisco: WLC Memory	1335	5 mins	SNMP Performance	Default SNMP Credential	□
Cisco: WLC System Counts	1353	5 mins	SNMP Performance	Default SNMP Credential	□
Cisco: WLC Configuration	1348	360 mins	SNMP Configuration	Default SNMP Credential	□
Cisco: WLC Interface Performance Average	1350	5 mins	Snippet Performance	Default SNMP Credential	□
Cisco: WLC Interference Average	1351	5 mins	Snippet Performance	Default SNMP Credential	□
Cisco: WLC Noise Average	1352	5 mins	Snippet Performance	Default SNMP Credential	□
Cisco: WLC AP Discovery	1336	120 mins	Snippet Configuration	Default SNMP Credential	□
Entity Configuration	1313	1440 mins	Snippet Configuration	Default SNMP Credential	□

- *Cisco: WLC CPU*
- *Cisco: WLC CPU and Memory Performance*
- *Cisco: WLC Memory*
- *Cisco: WLC System Counts*
- *Cisco: WLC Configuration*
- *Cisco: WLC Interface Performance Average*
- *Cisco: WLC Interface Average*
- *Cisco: WLC Noise Average*
- *Cisco: WLC AP Discovery*

NOTE: It can take several minutes after discovery for Dynamic Applications to be automatically aligned to the controller device. If the listed Dynamic Applications do not display on this page, try clicking the **[Reset]** button.

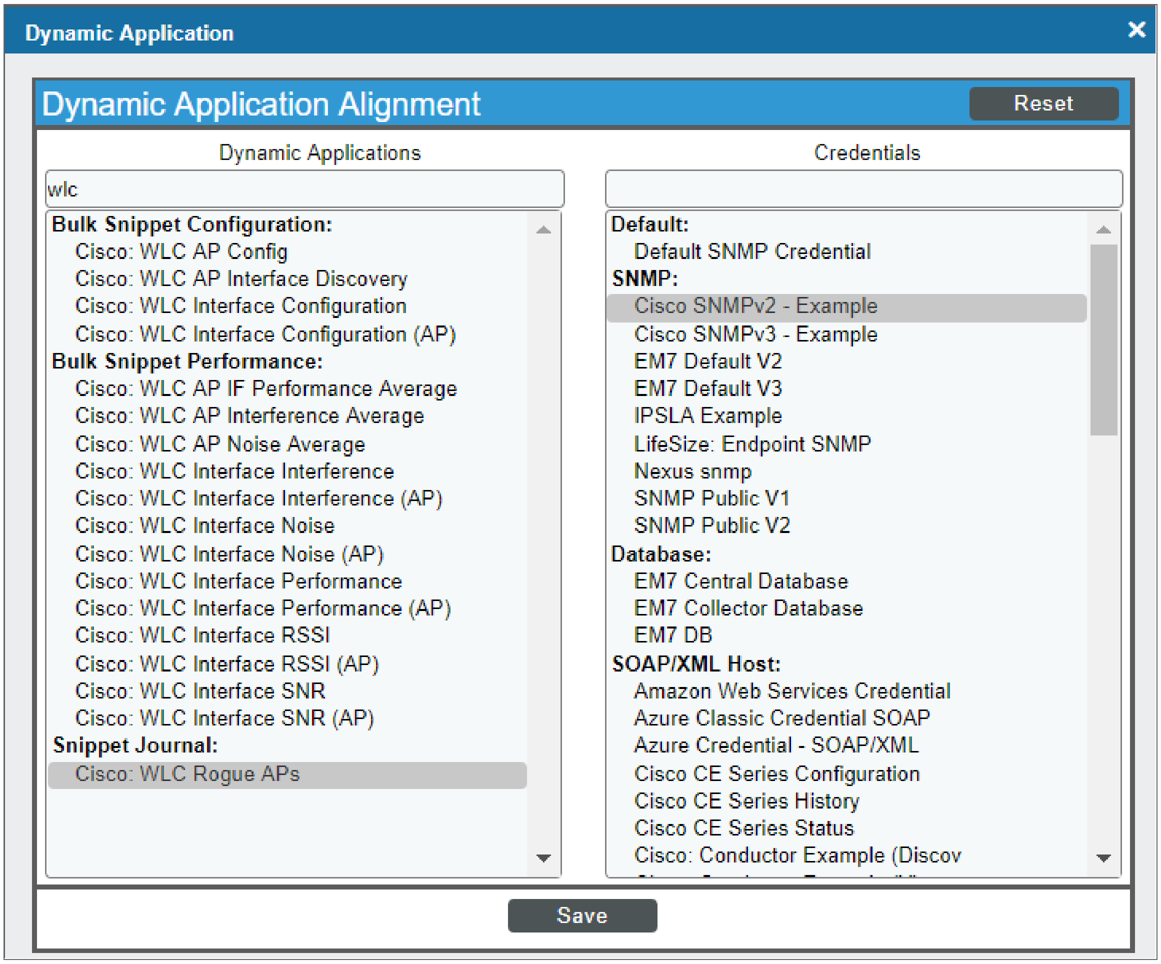
Manually Aligning Dynamic Applications

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

> **NOTE**: The "Cisco: WLC Rogue AP" Dynamic Application, which can be used to collect information about rogue access points, is not automatically aligned during discovery. To use the "Cisco: WLC Rogue AP" Dynamic Application, follow the instructions in this section.

To manually align Dynamic Applications:

1. From the **Device Properties** page for the Cisco WLC device, click the **[Collections]** tab.
2. Click the **[Actions]** button and then select *Add Dynamic Applications*. The **Dynamic Application Alignment** page appears:



Dynamic Applications

wlc

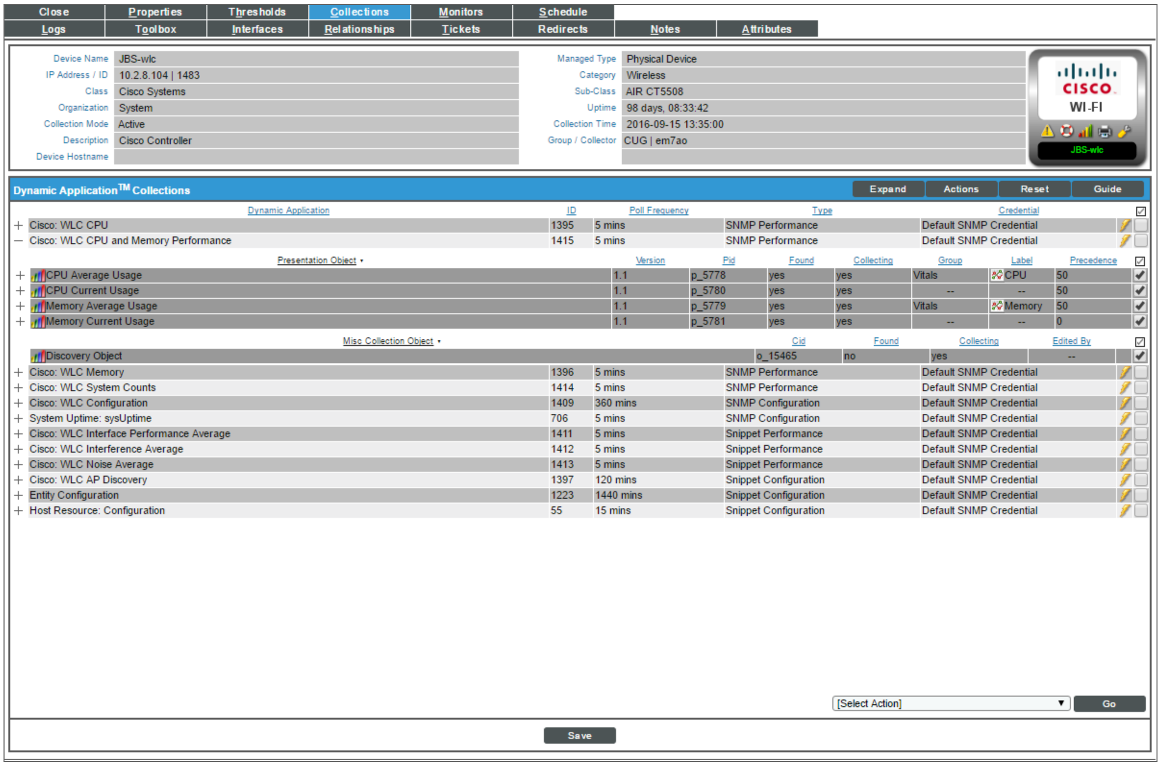
Bulk Snippet Configuration:
Cisco: WLC AP Config
Cisco: WLC AP Interface Discovery
Cisco: WLC Interface Configuration
Cisco: WLC Interface Configuration (AP)
Bulk Snippet Performance:
Cisco: WLC AP IF Performance Average
Cisco: WLC AP Interference Average
Cisco: WLC AP Noise Average
Cisco: WLC Interface Interference
Cisco: WLC Interface Interference (AP)
Cisco: WLC Interface Noise
Cisco: WLC Interface Noise (AP)
Cisco: WLC Interface Performance
Cisco: WLC Interface Performance (AP)
Cisco: WLC Interface RSSI
Cisco: WLC Interface RSSI (AP)
Cisco: WLC Interface SNR
Cisco: WLC Interface SNR (AP)
Snippet Journal:
Cisco: WLC Rogue APs

Credentials

Default:
Default SNMP Credential
SNMP:
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
Database:
EM7 Central Database
EM7 Collector Database
EM7 DB
SOAP/XML Host:
Amazon Web Services Credential
Azure Classic Credential SOAP
Azure Credential - SOAP/XML
Cisco CE Series Configuration
Cisco CE Series History
Cisco CE Series Status
Cisco: Conductor Example (Discov

3. In the ***Dynamic Applications*** field, select the Dynamic Application you want to align.
4. In the ***Credentials*** field, select the Cisco WLC SNMP credential.
5. Repeat steps 2-4 for the remaining Dynamic Applications you want to align with the device.

6. After aligning the Dynamic Applications, click the **[Reset]** button and then click the plus icon (+) for the Dynamic Application. If collection for the Dynamic Application was successful, the graph icons (📊) for the Dynamic Application are enabled:



Device Name	JBS-wlc	Managed Type	Physical Device
IP Address / ID	10.2.8.104 | 1483	Category	Wireless
Class	Cisco Systems	Sub-Class	AIR CT5508
Organization	System	Uptime	98 days, 08:33:42
Collection Mode	Active	Collection Time	2016-09-15 13:35:00
Description	Cisco Controller	Group / Collector	CUG | em7ao
Device Hostname			

Dynamic Application™ Collections

	Dynamic Application	ID	Poll Frequency	Type	Credential	☑
+	Cisco: WLC CPU	1395	5 mins	SNMP Performance	Default SNMP Credential	□
—	Cisco: WLC CPU and Memory Performance	1415	5 mins	SNMP Performance	Default SNMP Credential	□

	Presentation Object	Version	Pid	Found	Collecting	Group	Label	Precedence	☑
+	CPU Average Usage	1.1	p_5778	yes	yes	Vitals	CPU	50	✓
+	CPU Current Usage	1.1	p_5780	yes	yes	--	--	50	✓
+	Memory Average Usage	1.1	p_5779	yes	yes	Vitals	Memory	50	✓
+	Memory Current Usage	1.1	p_5781	yes	yes	--	--	0	✓

Misc Collection Object	Cid	Found	Collecting	Edited By	☑
Discovery Object	o_15465	no	yes	--	✓

	Dynamic Application	ID	Poll Frequency	Type	Credential	
+	Cisco: WLC Memory	1396	5 mins	SNMP Performance	Default SNMP Credential	□
+	Cisco: WLC System Counts	1414	5 mins	SNMP Performance	Default SNMP Credential	□
+	Cisco: WLC Configuration	1409	360 mins	SNMP Configuration	Default SNMP Credential	□
+	System Uptime: sysUptime	706	5 mins	SNMP Configuration	Default SNMP Credential	□
+	Cisco: WLC Interface Performance Average	1411	5 mins	Snippet Performance	Default SNMP Credential	□
+	Cisco: WLC Interference Average	1412	5 mins	Snippet Performance	Default SNMP Credential	□
+	Cisco: WLC Noise Average	1413	5 mins	Snippet Performance	Default SNMP Credential	□
+	Cisco: WLC AP Discovery	1397	120 mins	Snippet Configuration	Default SNMP Credential	□
+	Entity Configuration	1223	1440 mins	Snippet Configuration	Default SNMP Credential	□
+	Host Resource: Configuration	55	15 mins	Snippet Configuration	Default SNMP Credential	□

Chapter 27

Citrix: Xen

Overview

The following sections describe how to configure Citrix XenCenter systems and XenServer devices for monitoring by SL1 using the *Citrix: Xen* PowerPack:

NOTE: For more information about the *Citrix: Xen* PowerPack, see the ***Monitoring Citrix XenCenter*** manual.

Enabling Performance Metrics for XenServer 6.2.0 and Above

Most performance metrics are disabled by default in Citrix XenServer 6.2.0 and above. Therefore, if you are monitoring XenServer 6.2.0 or above with SL1, you must enable performance metrics on each XenServer host.

NOTE: Performance metrics are enabled by default in XenServer 6.1.0 and below. No additional steps are required to monitor those devices.

To enable performance metrics in XenServer 6.2.0 and above devices:

1. Open the XenServer command line interface.

2. For each XenServer host, enter the following command:

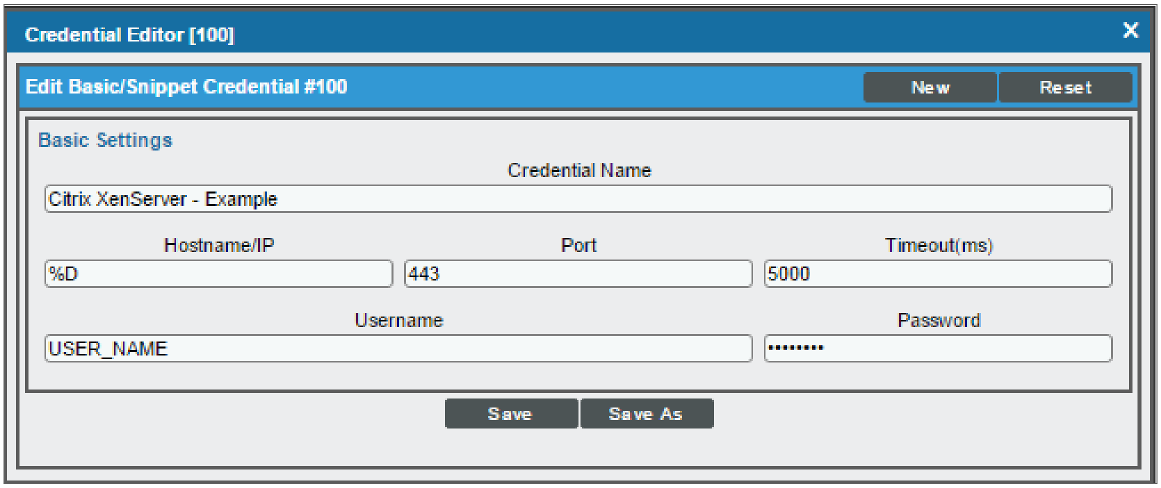
```
xe-enable-all-plugin-metrics true
```

Configuring a XenServer Credential

To use the Dynamic Applications in the *Citrix: Xen* PowerPack, you must first define a credential in SL1 that enables SL1 to communicate with your XenCenter system and XenServer devices. The *Citrix: Xen* PowerPack includes an example XenServer credential that you can modify for your own use.

To configure a XenServer credential:

1. Go to the **Credential Management** page (Credential Management).
2. Click the wrench icon (🔧) for the ***Citrix XenServer - Example*** credential. The **Credential Editor** modal window appears.



Credential Editor [100]

Edit Basic/Snippet Credential #100

Basic Settings

Credential Name: Citrix XenServer - Example

Hostname/IP: %D

Port: 443

Timeout(ms): 5000

Username: USER_NAME

Password: ••••••••

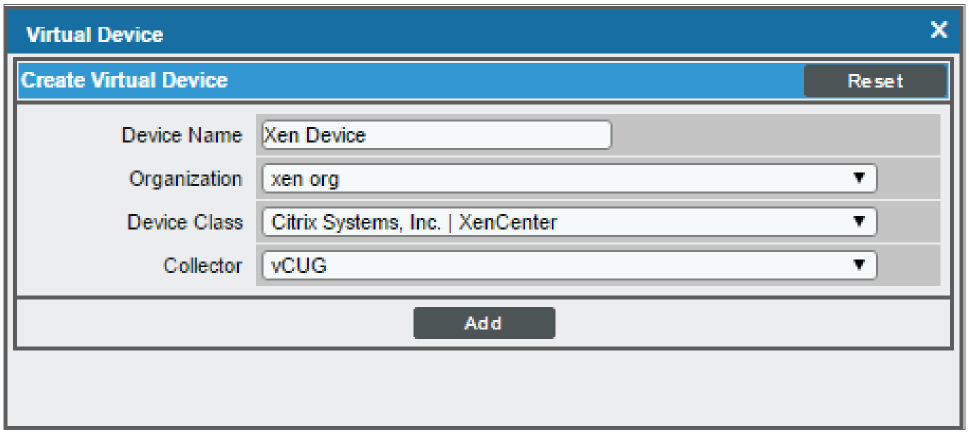
3. Enter values in the following fields:
   - ***Credential Name***. Enter a name for your XenServer credential.
   - ***Hostname/IP***. Enter the IP address of the XenServer.
   - ***Port***. Enter "443".
   - ***Timeout***. Enter "5000".
   - ***Username***. Enter the username that SL1 will use to connect to your XenServer.
   - ***Password***. Enter the password for the XenServer username.
4. Click the **[Save As]** button.

Creating a XenCenter Virtual Device

Because the XenCenter system does not have an IP address, you cannot discover XenCenter using discovery. Instead, you must create a ***virtual device*** that represents the root device for the XenCenter system. A virtual device is a user-defined container that represents a device or service that cannot be discovered by SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications.

To create a virtual device that represents your XenCenter system:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Click the **[Actions]** button, then select *Create Virtual Device*. The **Create Virtual Device** modal page appears:



Device Name: Xen Device
Organization: xen org
Device Class: Citrix Systems, Inc. | XenCenter
Collector: vCUG

3. Enter values in the following fields:

   - ***Device Name***. Enter a name for the device. For example, you could enter "XenCenter" in this field.
   - ***Organization***. Select the organization for this device. When you assign an organization to the device, only organization members and users with administrator privileges are allowed to view and edit the device.
   - ***Device Class***. Select *Citrix Systems, Inc. | XenCenter*.
   - ***Collector Group***. Select the collector group that will monitor the device.

4. Click the **[Add]** button to create the virtual device.

Aligning the Discovery Dynamic Application

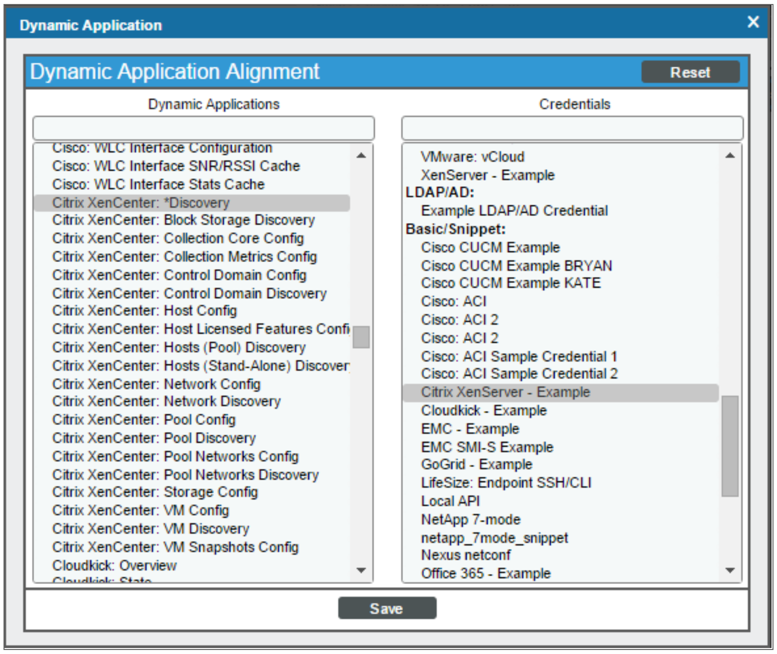
To discover your XenCenter system, you must manually align the "Citrix XenCenter: *Discovery" Dynamic Application to the XenCenter virtual device. To do so, perform the following steps:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).

2. Click the wrench icon (🔧) for your virtual device.

3. In the **Device Administration** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.

4. Click the **[Actions]** button and select *Add Dynamic Application* from the menu. The **Dynamic Application Alignment** modal page appears:


Dynamic Application
×
Dynamic Application Alignment
Reset
Dynamic Applications
Credentials
Cisco: WLC Interface Configuration
Cisco: WLC Interface SNR/RSSI Cache
Cisco: WLC Interface Stats Cache
Citrix XenCenter: *Discovery
Citrix XenCenter: Block Storage Discovery
Citrix XenCenter: Collection Core Config
Citrix XenCenter: Collection Metrics Config
Citrix XenCenter: Control Domain Config
Citrix XenCenter: Control Domain Discovery
Citrix XenCenter: Host Config
Citrix XenCenter: Host Licensed Features Confi
Citrix XenCenter: Hosts (Pool) Discovery
Citrix XenCenter: Hosts (Stand-Alone) Discover
Citrix XenCenter: Network Config
Citrix XenCenter: Network Discovery
Citrix XenCenter: Pool Config
Citrix XenCenter: Pool Discovery
Citrix XenCenter: Pool Networks Config
Citrix XenCenter: Pool Networks Discovery
Citrix XenCenter: Storage Config
Citrix XenCenter: VM Config
Citrix XenCenter: VM Discovery
Citrix XenCenter: VM Snapshots Config
Cloudkick: Overview
Cloudkick: State
VMware: vCloud
XenServer - Example
LDAP/AD:
Example LDAP/AD Credential
Basic/Snippet:
Cisco CUCM Example
Cisco CUCM Example BRYAN
Cisco CUCM Example KATE
Cisco: ACI
Cisco: ACI 2
Cisco: ACI 2
Cisco: ACI Sample Credential 1
Cisco: ACI Sample Credential 2
Citrix XenServer - Example
Cloudkick - Example
EMC - Example
EMC SMI-S Example
GoGrid - Example
LifeSize: Endpoint SSH/CLI
Local API
NetApp 7-mode
netapp_7mode_snippet
Nexus netconf
Office 365 - Example
Save

- In the ***Dynamic Applications*** field, select *Citrix XenCenter: *Discovery*.
- In the ***Credentials*** field, select the credential *you created for this Xen cluster*.

5. Click the **[Save]** button to align the Dynamic Application.

Chapter

28

CouchBase

Overview

The following sections describe how to configure Couchbase servers for monitoring by SL1 using the *CouchBase* PowerPack:

NOTE: For more information about the *CouchBase* PowerPack, see the ***Monitoring Couchbase*** manual.

Prerequisites for Monitoring Couchbase

To configure SL1 to monitor Couchbase servers and component devices using the *CouchBase* PowerPack, you must have the login credentials for a user with administrative access to the Couchbase server.

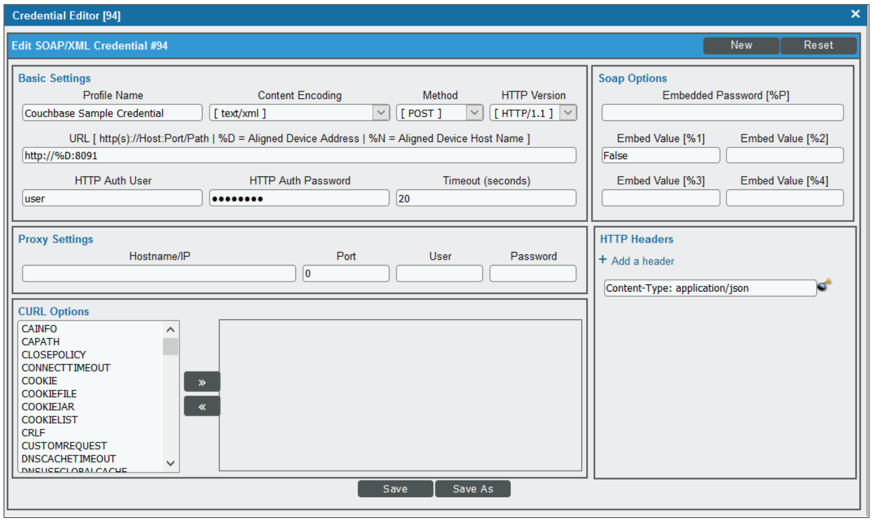
Creating a Couchbase Credential

To use the Dynamic Applications in the *CouchBase* PowerPack, you must first define a credential in SL1. This credential enables the Dynamic Applications in the *CouchBase* PowerPack to monitor your Couchbase component devices. The PowerPack includes a sample SOAP/XML credential (**Couchbase Sample Credential**) that you can use as a template.

To define a Couchbase credential:

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

2. Click the wrench icon ( ) for the **Couchbase Sample Credential**. The **Credential Editor** modal page appears:



Profile Name: Couchbase Sample Credential
Content Encoding: [text/xml]
Method: [POST]
HTTP Version: [HTTP/1.1]
URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: http://%D:8091
HTTP Auth User: user
HTTP Auth Password: ••••••••
Timeout (seconds): 20
Embedded Password [%P]:
Embed Value [%1]: False
Embed Value [%2]:
Embed Value [%3]:
Embed Value [%4]:
Hostname/IP:
Port: 0
User:
Password:
Content-Type: application/json

3. Enter values in the following fields:

    - ***Profile Name***. Type a new name for your Couchbase credential.
    - ***URL***. Type the URL for the Couchbase server, or use the default value.
    - ***HTTP Auth User***. Type the username for a user with administrative access to the Couchbase server.
    - ***HTTP Auth Password***. Type the Couchbase administrator user's password.

    Use the default values for the remaining fields.

4. Click the **[Save As]** button, and then click **[OK]**.

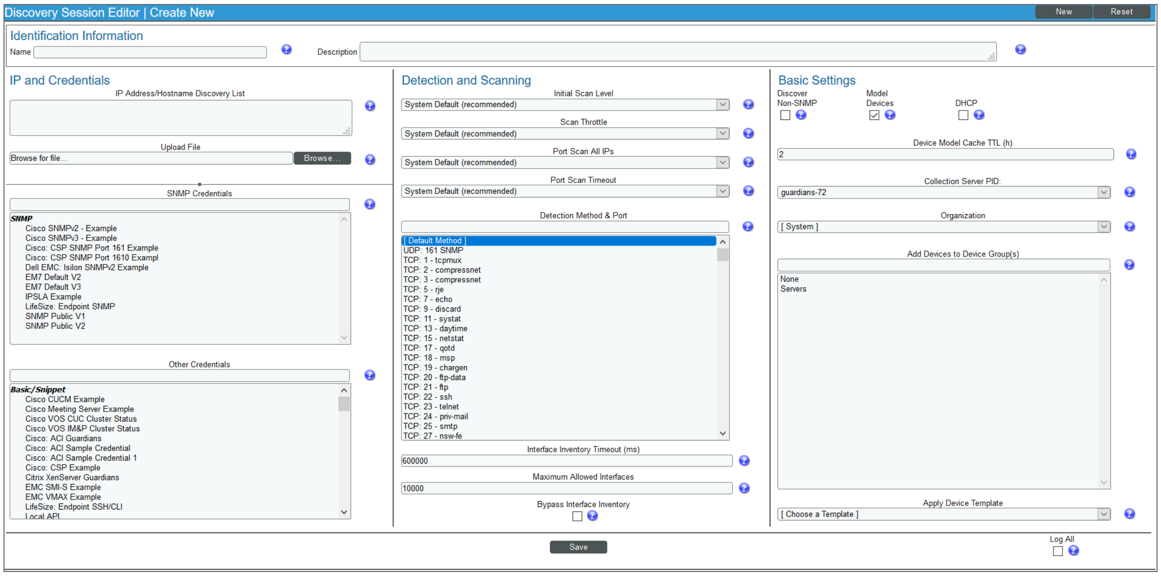
Discovering Couchbase Devices

To discover Couchbase devices, you must create and run a discovery session that will discover the Couchbase server. You must then manually align the "Couchbase: Pool Discovery" Dynamic Application to the Couchbase server device.

To discover Couchbase devices:

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

2. Click the **[Create]** button to create a new discovery session. The **Discovery Session Editor** window appears:



Initial Scan Level: System Default (recommended)

Scan Throttle: System Default (recommended)

Port Scan All IPs: System Default (recommended)

Port Scan Timeout: System Default (recommended)

SNMP Credentials:

SNMP
- Cisco SNMPv2 - Example
- Cisco SNMPv3 - Example
- Cisco: CSP SNMP Port 161 Example
- Cisco: CSP SNMP Port 1610 Exampl
- Dell EMC: Isilon SNMPv2 Example
- EM7 Default V2
- EM7 Default V3
- IPSLA Example
- LifeSize: Endpoint SNMP
- SNMP Public V1
- SNMP Public V2

Other Credentials:

Basic/Snippet
- Cisco CUCM Example
- Cisco Meeting Server Example
- Cisco VOS CUC Cluster Status
- Cisco VOS IM&P Cluster Status
- Cisco: ACI Guardians
- Cisco: ACI Sample Credential
- Cisco: ACI Sample Credential 1
- Cisco: CSP Example
- Citrix XenServer Guardians
- EMC SMI-S Example
- EMC VMAX Example
- LifeSize: Endpoint SSH/CLI
- Local API

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
- TCP: 17 - qotd
- TCP: 18 - msp
- TCP: 19 - chargen
- TCP: 20 - ftp-data
- TCP: 21 - ftp
- TCP: 22 - ssh
- TCP: 23 - telnet
- TCP: 24 - priv-mail
- TCP: 25 - smtp
- TCP: 27 - nsw-fe

Interface Inventory Timeout (ms): 600000

Maximum Allowed Interfaces: 10000

Bypass Interface Inventory: □

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

Device Model Cache TTL (h): 2

Collection Server PID: guardians-72

Organization: [System]

Add Devices to Device Group(s):
- None
- Servers

Apply Device Template: [Choose a Template]

Log All: □

3. Edit the following fields in the **Discovery Session Editor** window:

   - ***Name***. Type a name for the discovery session.
   - ***IP Address/Hostname Discovery List***. Type the IP address for the Couchbase server.
   - ***Other Credentials***. Select the SOAP/XML credential you created for Couchbase.
   - ***Discover Non-SNMP***. 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.

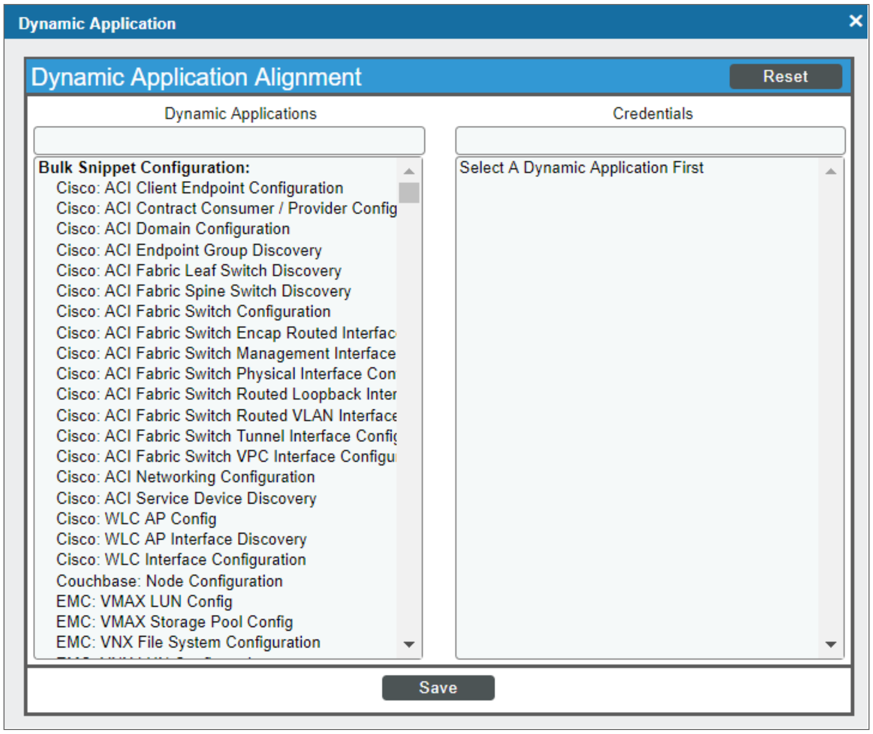
5. Click the **[Save]** button and then close the **Discovery Session Editor** window.

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. The **Discovery Session** window appears. When Couchbase is discovered, click its device icon ( ) to view the **Device Properties** page for the Couchbase server.

8. From the **Device Properties** page, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.

9. On theDynamic Application Collections page, click the **[Actions]** button and then select *Add Dynamic Application*. The **Dynamic Application Alignment** pane appears.



Dynamic Application ×

Dynamic Application Alignment

Reset

Dynamic Applications

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
Couchbase: Node Configuration
EMC: VMAX LUN Config
EMC: VMAX Storage Pool Config
EMC: VNX File System Configuration

Credentials

Select A Dynamic Application First

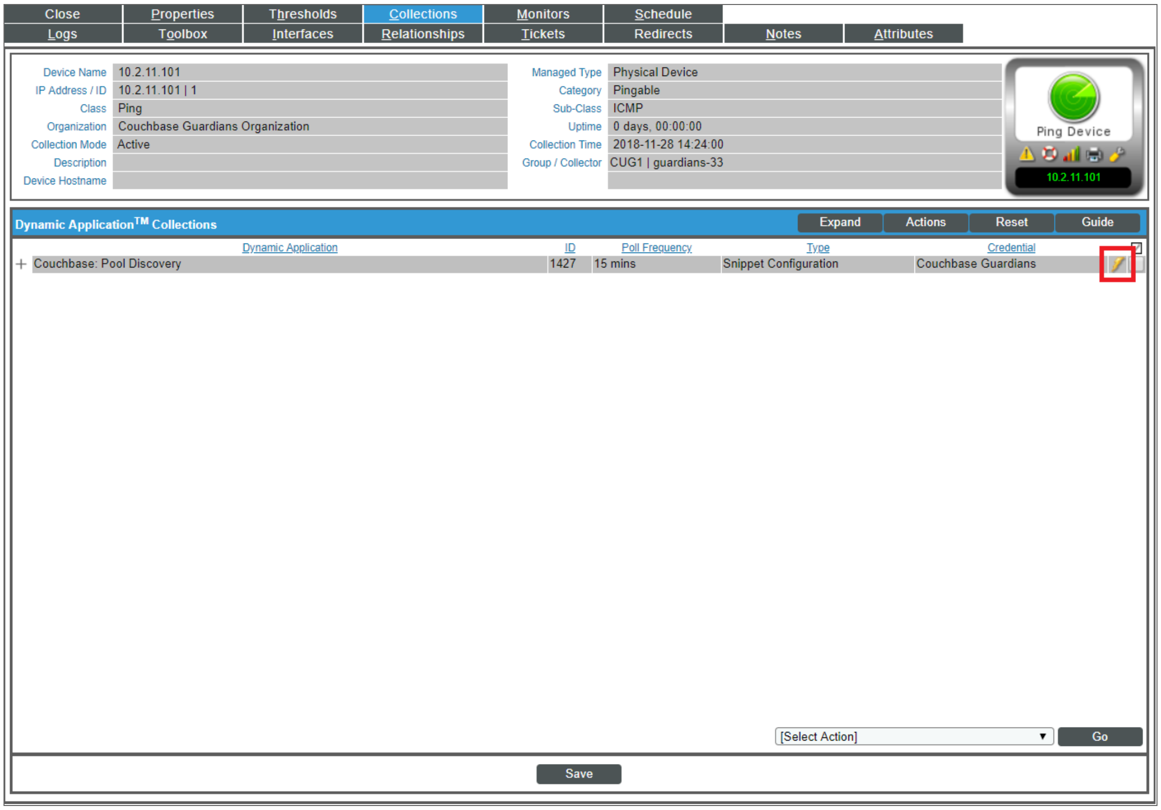
Save

10. In the ***Dynamic Applications*** field, select *Couchbase: Pool Discovery*.

11. In the ***Credentials*** field, select the SOAP/XML credential you created for Couchbase.

12. Click **[Save]**. The Dynamic Application appears on the **Dynamic Application Collections** page.

13. To run the "Couchbase: Pool Discovery" Dynamic Application immediately, click its lightning bolt icon (⚡).



Device Name	10.2.11.101	Managed Type	Physical Device
IP Address / ID	10.2.11.101 | 1	Category	Pingable
Class	Ping	Sub-Class	ICMP
Organization	Couchbase Guardians Organization	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2018-11-28 14:24:00
Description		Group / Collector	CUG1 | guardians-33
Device Hostname			

Dynamic Application^{TM} Collections

Dynamic Application	ID	Poll Frequency	Type	Credential
Couchbase: Pool Discovery	1427	15 mins	Snippet Configuration	Couchbase Guardians

Chapter 29

Dell EMC: Isilon

Overview

The following sections describe how to configure and discover Dell EMC Isilon storage arrays for monitoring by SL1 using the *Dell EMC: Isilon* PowerPack:

NOTE: For more information about the *Dell EMC: Isilon* PowerPack, see the ***Monitoring Dell EMC Isilon*** manual.

Prerequisites for Monitoring Dell EMC Isilon

To configure the SL1 system to monitor Dell EMC Isilon storage arrays using the *Dell EMC: Isilon* PowerPack, you must have already installed and configured the storage arrays that you want to monitor.

If you are using a Secure Sockets Layer (SSL) certificate to communicate with the Isilon storage arrays you are monitoring, you must add an Isilon SSL certificate on your SL1 appliance in the following file:

```
/var/lib/em7/content/silo_core_rest/certs.crt
```

> NOTE: If you are not using an SSL certificate to communicate with the Isilon storage arrays, then you do not need to add a certificate. For more information about installing an SSL certificate, see the manual ***Installing an SSL Certificate***.

Additionally, you should take note of the SNMP community string used by the Isilon storage arrays you want to monitor.

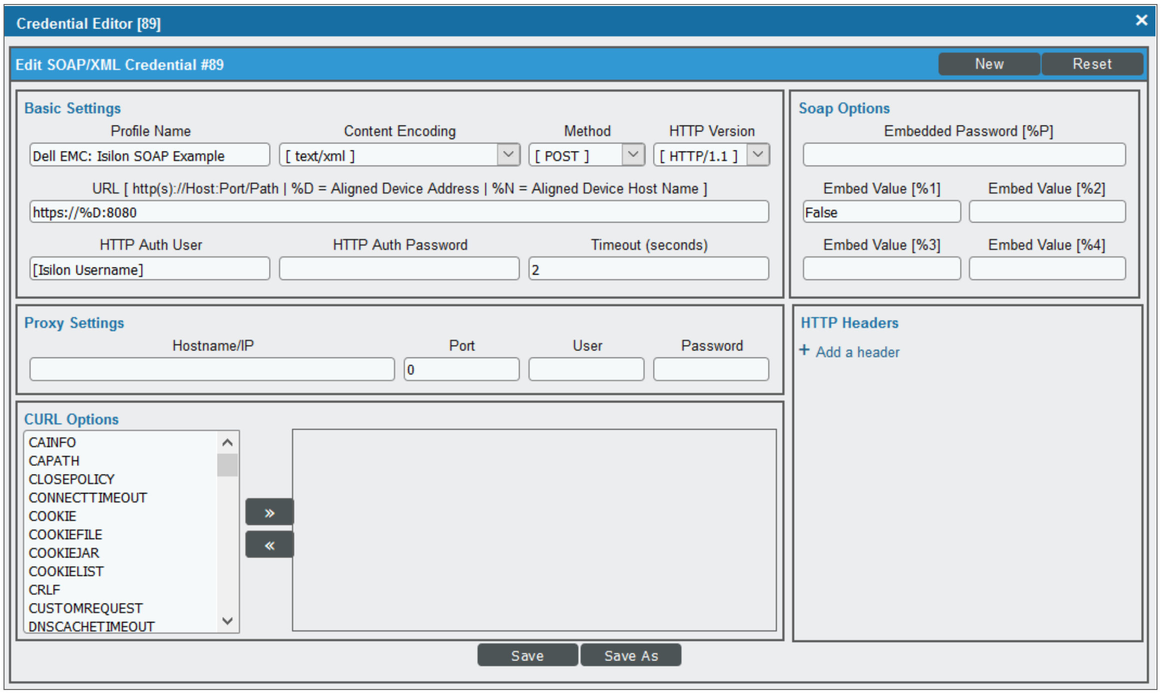
Creating a SOAP/XML Credential for Dell EMC Isilon

To configure SL1 to monitor Dell EMC Isilon storage arrays, you must first create a credential that allows the Dynamic Applications in the *Dell EMC: Isilon* PowerPack to communicate with your Isilon storage devices. The PowerPack includes an example SOAP/XML credential that you can edit for your own use.

To configure the SOAP/XML credential to access Dell EMC Isilon devices:

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

2. Locate the **Dell EMC: Isilon SOAP Example** credential, and then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears.



Credential Editor [89]

Edit SOAP/XML Credential #89

Basic Settings

Profile Name	Content Encoding	Method	HTTP Version
Dell EMC: Isilon SOAP Example	[text/xml]	[POST]	[HTTP/1.1]

URL [http(s)://Host:Port/Path \| %D = Aligned Device Address \| %N = Aligned Device Host Name]: https://%D:8080

HTTP Auth User	HTTP Auth Password	Timeout (seconds)
[Isilon Username]		2

Soap Options

Embedded Password [%P]:

Embed Value [%1]	Embed Value [%2]
False	

Embed Value [%3]	Embed Value [%4]

Proxy Settings

Hostname/IP	Port	User	Password
	0		

HTTP Headers

CURL Options

3. Update the values in the following fields:

Basic Settings

- ***Profile Name***. Type a new name for the credential.
- ***HTTP Auth User***. Type the Isilon administrator username.
- ***HTTP Auth Password***. Type the Isilon administrator password.

SOAP Options

- ***Embed Value [%1]***. Do one of the following:
    - Type "True" to enable verification of the storage array's SSL certificate.
    - Type "False" or leave this field blank to disable SSL verification.

NOTE: This field is not case-sensitive.

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

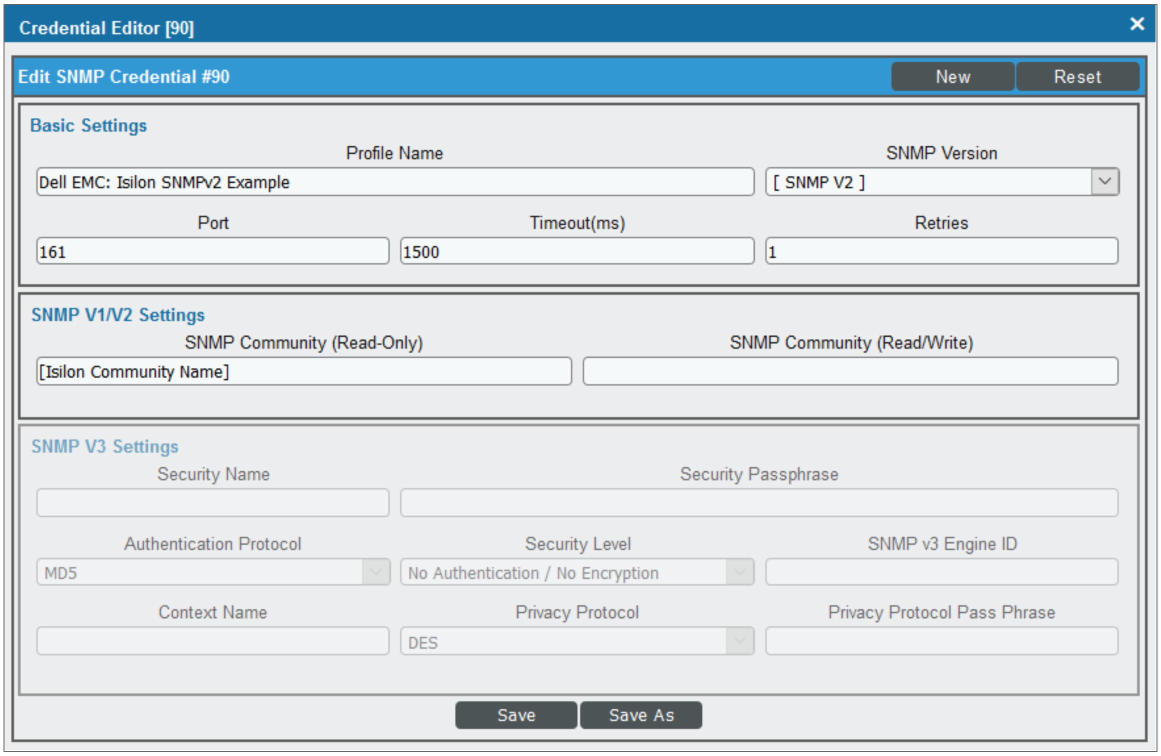
Creating an SNMP Credential for Dell EMC Isilon

In addition to the SOAP/XML credential, you will also need to configure an SNMP credential to enable SL1 to monitor Dell EMC Isilon storage arrays. The *Dell EMC: Isilon* PowerPack includes an example SNMP credential that you can edit for your own use.

To configure the SNMP credential to access Dell EMC Isilon devices:

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

2. Locate the **Dell EMC: Isilon SNMPv2 Example** credential, and then click its wrench icon (). The **Edit SNMP Credential** modal page appears.



Credential Editor [90]

Edit SNMP Credential #90

Basic Settings

Profile Name: Dell EMC: Isilon SNMPv2 Example

SNMP Version: [SNMP V2]

Port: 161

Timeout(ms): 1500

Retries: 1

SNMP V1/V2 Settings

SNMP Community (Read-Only): [Isilon Community Name]

SNMP Community (Read/Write):

SNMP V3 Settings

Security Name:

Security Passphrase:

Authentication Protocol: MD5

Security Level: No Authentication / No Encryption

SNMP v3 Engine ID:

Context Name:

Privacy Protocol: DES

Privacy Protocol Pass Phrase:

3. Update the values in the following fields:

Basic Settings

- *Profile Name*. Type a new name for the credential.

SNMP V1/V2 Settings

- *SNMP Community (Read-Only)*. Type the Isilon storage array's SNMP community string.

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

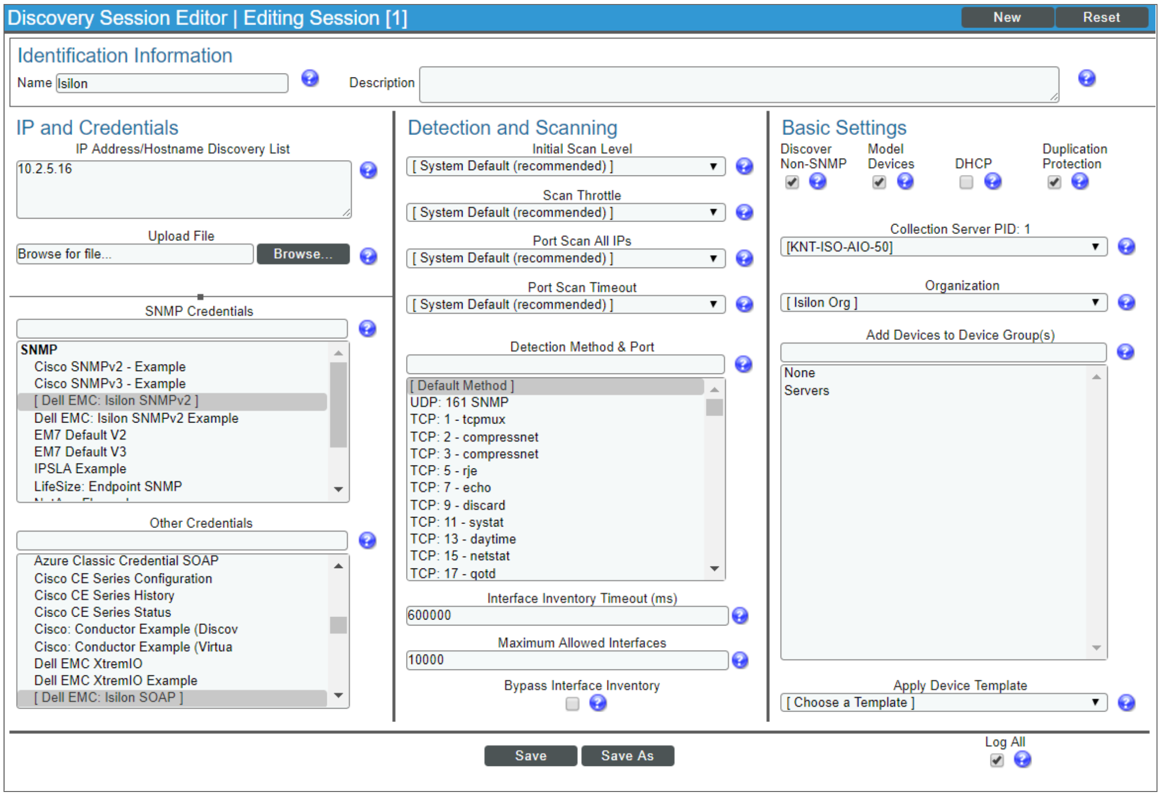
Discovering Dell EMC Isilon Component Devices

To model and monitor your Dell EMC Isilon storage arrays, you must run a discovery session to discover the storage arrays that SL1 will use as the root devices for monitoring the Isilon storage system.

After the discovery session completes, the Dynamic Applications in the *Dell EMC: Isilon* PowerPack automatically align to the storage array device, and then the PowerPack discovers, models, and monitors the remaining Isilon storage devices.

To discover the Isilon arrays that you want to monitor, perform the following steps:

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



Discovery Session Editor | Editing Session [1]

Identification Information

Name: Isilon

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.2.5.16

Upload File: Browse for file...

SNMP Credentials: SNMP, Cisco SNMPv2 - Example, Cisco SNMPv3 - Example, [Dell EMC: Isilon SNMPv2], Dell EMC: Isilon SNMPv2 Example, EM7 Default V2, EM7 Default V3, IPSLA Example, LifeSize: Endpoint SNMP

Other Credentials: Azure Classic Credential SOAP, Cisco CE Series Configuration, Cisco CE Series History, Cisco CE Series Status, Cisco: Conductor Example (Discov, Cisco: Conductor Example (Virtua, Dell EMC XtremIO, Dell EMC XtremIO Example, [Dell EMC: Isilon 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: 15 - netstat, 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: 1 [KNT-ISO-AIO-50]

Organization: [Isilon Org]

Add Devices to Device Group(s): None, Servers

Apply Device Template: [Choose a Template]

Log All: ☑

3. Supply values in the following fields:

    - ***IP Address/Hostname Discovery List***. Type the IP address or hostname for the Isilon storage array or arrays that you want to discover.
    - ***SNMP Credentials***. Select the SNMP credential that you created for Isilon devices.
    - ***Other Credentials***. Select the SOAP/XML credential that you created for Isilon devices.
    - ***Discover Non-SNMP***. Select this checkbox.
    - ***Model Devices***. Select this checkbox.
    - ***Duplication Protection***. 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.

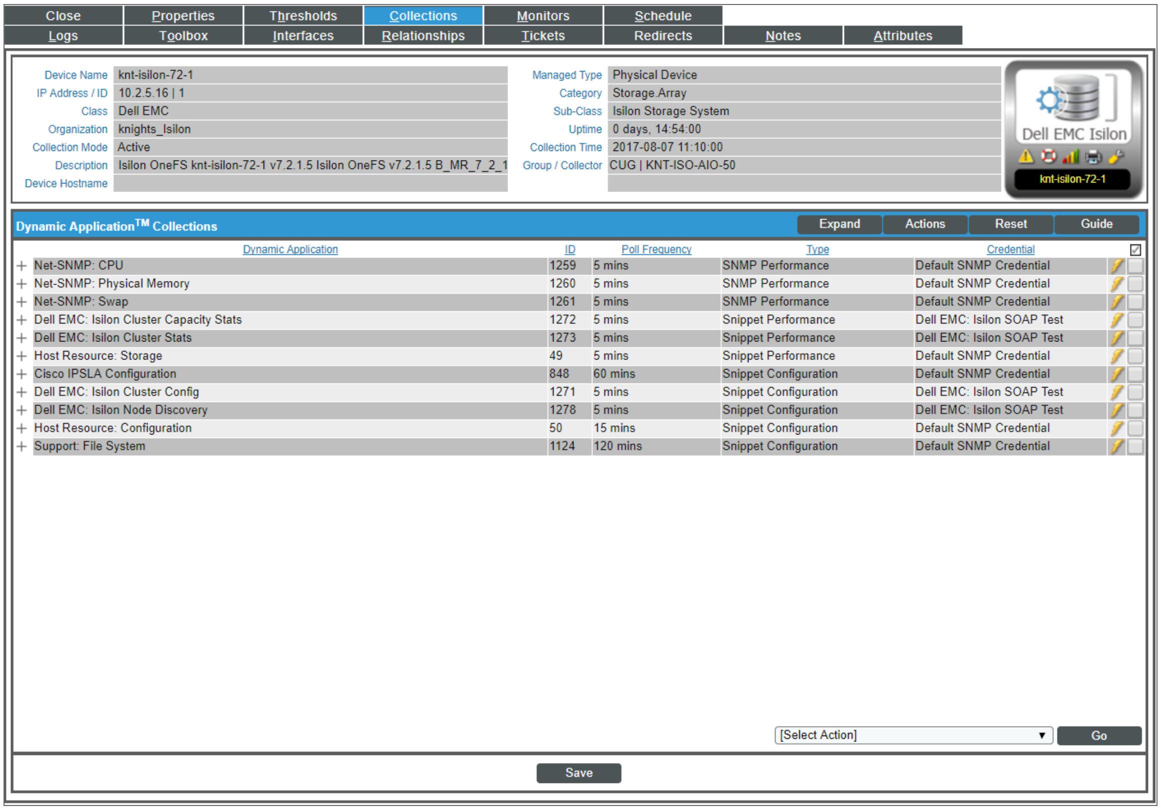
7. The **Discovery Session** window appears. After the devices are discovered, click the device icon ( ) to view the **Device Properties** page for each device.

Verifying Discovery andDynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. After discovery has completed, click the device icon for the Isilon Storage Array device ( ).
2. From the **Device Properties** page for the array device, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
3. All applicable Dynamic Applications for the storage array device 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: knt-isilon-72-1
IP Address / ID: 10.2.5.16 | 1
Class: Dell EMC
Organization: knights_Isilon
Collection Mode: Active
Description: Isilon OneFS knt-isilon-72-1 v7.2.1.5 Isilon OneFS v7.2.1.5 B_MR_7_2_1
Device Hostname:
Managed Type: Physical Device
Category: Storage.Array
Sub-Class: Isilon Storage System
Uptime: 0 days, 14:54:00
Collection Time: 2017-08-07 11:10:00
Group / Collector: CUG | KNT-ISO-AIO-50

Dynamic Application^{TM} Collections

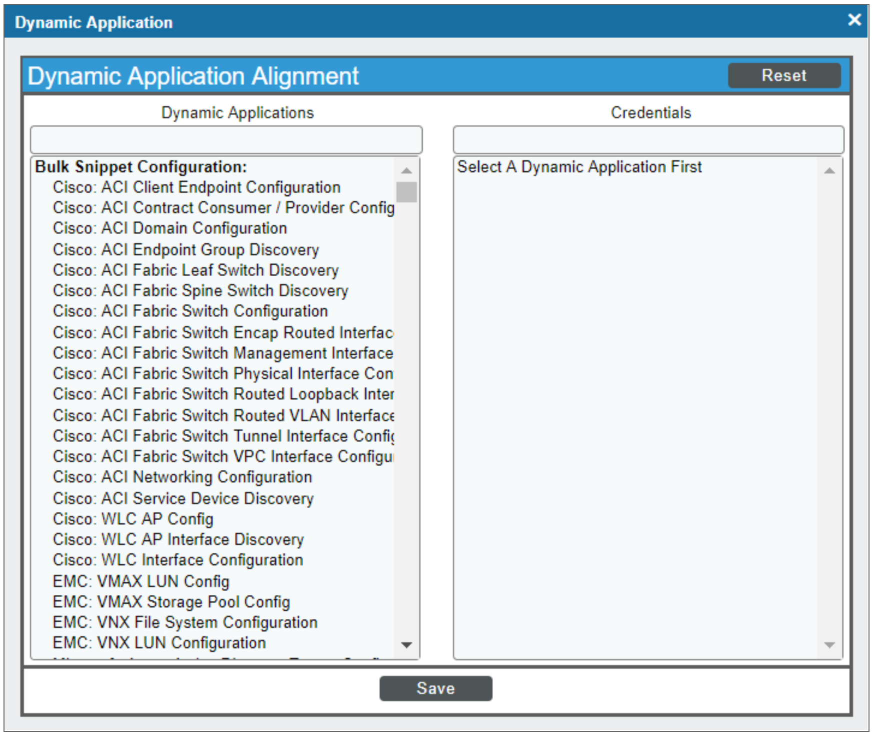
Dynamic Application	ID	Poll Frequency	Type	Credential
Net-SNMP: CPU	1259	5 mins	SNMP Performance	Default SNMP Credential
Net-SNMP: Physical Memory	1260	5 mins	SNMP Performance	Default SNMP Credential
Net-SNMP: Swap	1261	5 mins	SNMP Performance	Default SNMP Credential
Dell EMC: Isilon Cluster Capacity Stats	1272	5 mins	Snippet Performance	Dell EMC: Isilon SOAP Test
Dell EMC: Isilon Cluster Stats	1273	5 mins	Snippet Performance	Dell EMC: Isilon SOAP Test
Host Resource: Storage	49	5 mins	Snippet Performance	Default SNMP Credential
Cisco IPSLA Configuration	848	60 mins	Snippet Configuration	Default SNMP Credential
Dell EMC: Isilon Cluster Config	1271	5 mins	Snippet Configuration	Dell EMC: Isilon SOAP Test
Dell EMC: Isilon Node Discovery	1278	5 mins	Snippet Configuration	Dell EMC: Isilon SOAP Test
Host Resource: Configuration	50	15 mins	Snippet Configuration	Default SNMP Credential
Support: File System	1124	120 mins	Snippet Configuration	Default SNMP Credential

You should see the following Dynamic Applications aligned to the storage array device:

Dynamic Application	Credential Type
Dell EMC: Isilon Cluster Capacity Stats	SOAP/XML
Dell EMC: Isilon Cluster Config	SOAP/XML
Dell EMC: Isilon Cluster Stats	SOAP/XML
Dell EMC: Isilon Node Discovery	SOAP/XML
Host Resource: Configuration	SNMP
Host Resource: Storage	SNMP
Net-SNMP: CPU	SNMP
Net-SNMP: Physical Memory	SNMP
Net-SNMP: Swap	SNMP
Support: File System	SNMP

If the listed Dynamic Applications have not been automatically aligned during discovery, you can align them manually. To do so, perform the following steps:

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



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

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.

Chapter

30

Dell EMC: Unity

Overview

The following sections describe how to configure and discover Dell EMC Unity storage arrays for monitoring by SL1 using the *Dell EMC: Unity* PowerPack:

NOTE: For more information about the *Dell EMC: Unity* PowerPack, see the ***Monitoring Dell EMC Unity*** manual.

Prerequisites for Monitoring Dell EMC Unity

Before you can monitor Dell EMC Unity systems using the *Dell EMC: Unity* PowerPack, you must have the following information about the Unisphere REST API:

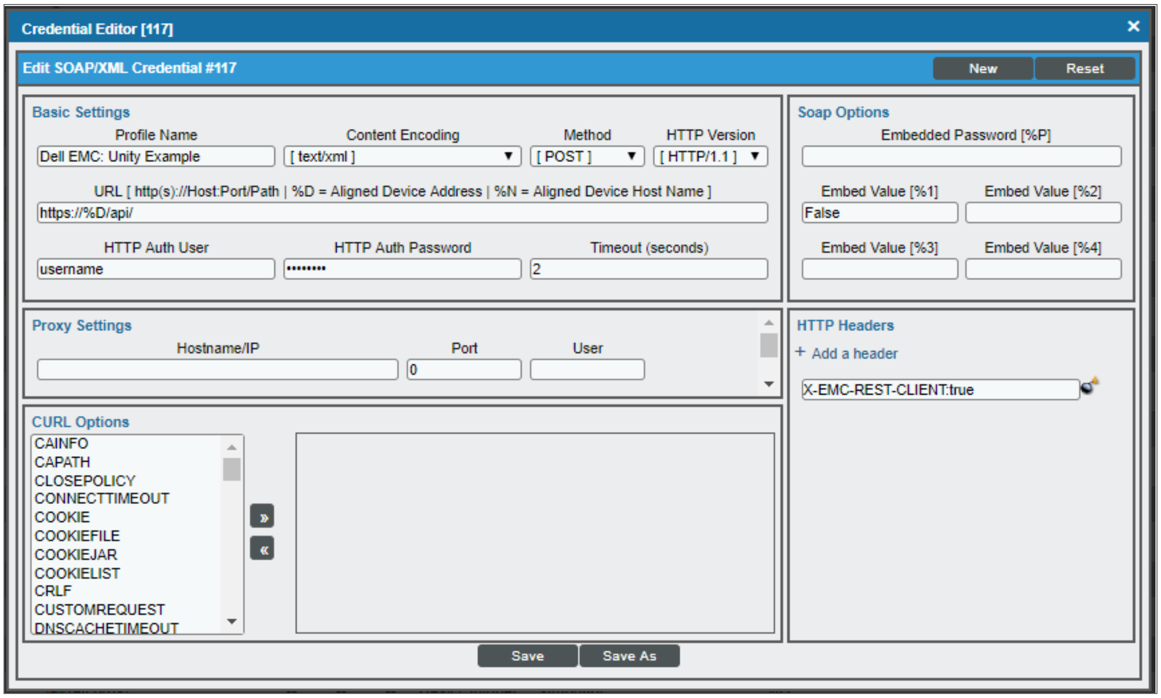
- Username and password for a user with access to the Unisphere REST API
- IP address for the Unisphere REST API

Creating a SOAP/XML Credential for Dell EMC Unity

To configure SL1 to monitor Dell EMC Unity storage arrays, you must first create a SOAP/XML credential. This credential allows the Dynamic Applications in the *Dell EMC: Unity* PowerPack to use the Unisphere REST API. An example SOAP/XML credential that you can edit for your own use is included in the *Dell EMC: Unity* PowerPack.

To configure the SOAP/XML credential to access the Unisphere REST API:

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



Credential Editor [117]

Edit SOAP/XML Credential #117

Basic Settings

Profile Name: Dell EMC: Unity Example

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://%D/api/

HTTP Auth User: username

HTTP Auth Password: ••••••••

Timeout (seconds): 2

Soap Options

Embedded Password [%P]:

Embed Value [%1]: False

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

Proxy Settings

Hostname/IP:

Port: 0

User:

HTTP Headers

X-EMC-REST-CLIENT:true

CURL Options

3. Complete the following fields:
   - ***Profile Name***. Type a new name for the credential.
   - ***HTTP Auth User***. Type the username for a user with access to the Unisphere REST API.
   - ***HTTP Auth Password***. Type the password for the user you specified in the ***HTTP Auth User*** field.

NOTE: The HTTP Headers that are included in the example credential are required to receive a response from the Unisphere REST API. Do not delete or edit them.

4. Click **[Save As]**.
5. When the confirmation message appears, click **[OK]**.

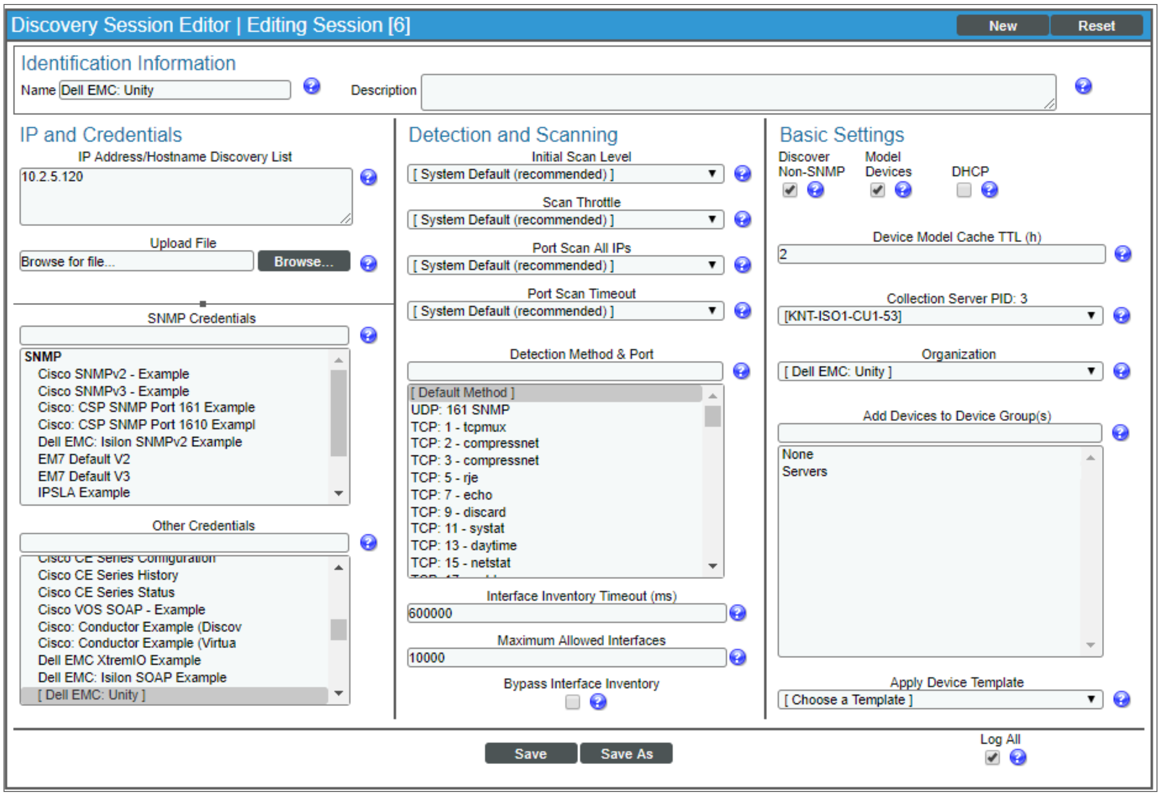
Discovering Dell EMC Unity Component Devices

To model and monitor your Dell EMC Unity storage arrays, you must run a discovery session to discover the Unisphere that SL1 will use as the root device for monitoring the Unity storage system.

After the discovery session completes, the Dynamic Applications in the *Dell EMC: Unity* PowerPack automatically align to the storage array device, and then the PowerPack discovers, models, and monitors the remaining Unity component devices.

To discover the Unity arrays that you want to monitor, perform the following steps:

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



Discovery Session Editor | Editing Session [6]

Identification Information

Name: Dell EMC: Unity

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.2.5.120

Upload File: Browse for file...

SNMP Credentials: SNMP — Cisco SNMPv2 - Example, Cisco SNMPv3 - Example, Cisco: CSP SNMP Port 161 Example, Cisco: CSP SNMP Port 1610 Exampl, Dell EMC: Isilon SNMPv2 Example, EM7 Default V2, EM7 Default V3, IPSLA Example

Other Credentials: Cisco CE Series Configuration, Cisco CE Series History, Cisco CE Series Status, Cisco VOS SOAP - Example, Cisco: Conductor Example (Discov, Cisco: Conductor Example (Virtua, Dell EMC XtremIO Example, Dell EMC: Isilon SOAP Example, [Dell EMC: Unity]

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: 3: [KNT-ISO1-CU1-53]

Organization: [Dell EMC: Unity]

Add Devices to Device Group(s): None, Servers

Apply Device Template: [Choose a Template]

Log All: ☑

3. Complete the following fields:

- ***IP Address/Hostname Discovery List***. Type the IP address for the Unisphere.
- ***Other Credentials***. Select the SOAP/XML credential that you created for Unity devices.
- ***Discover Non-SNMP***. Select this checkbox.
- ***Model Devices***. Select this checkbox.

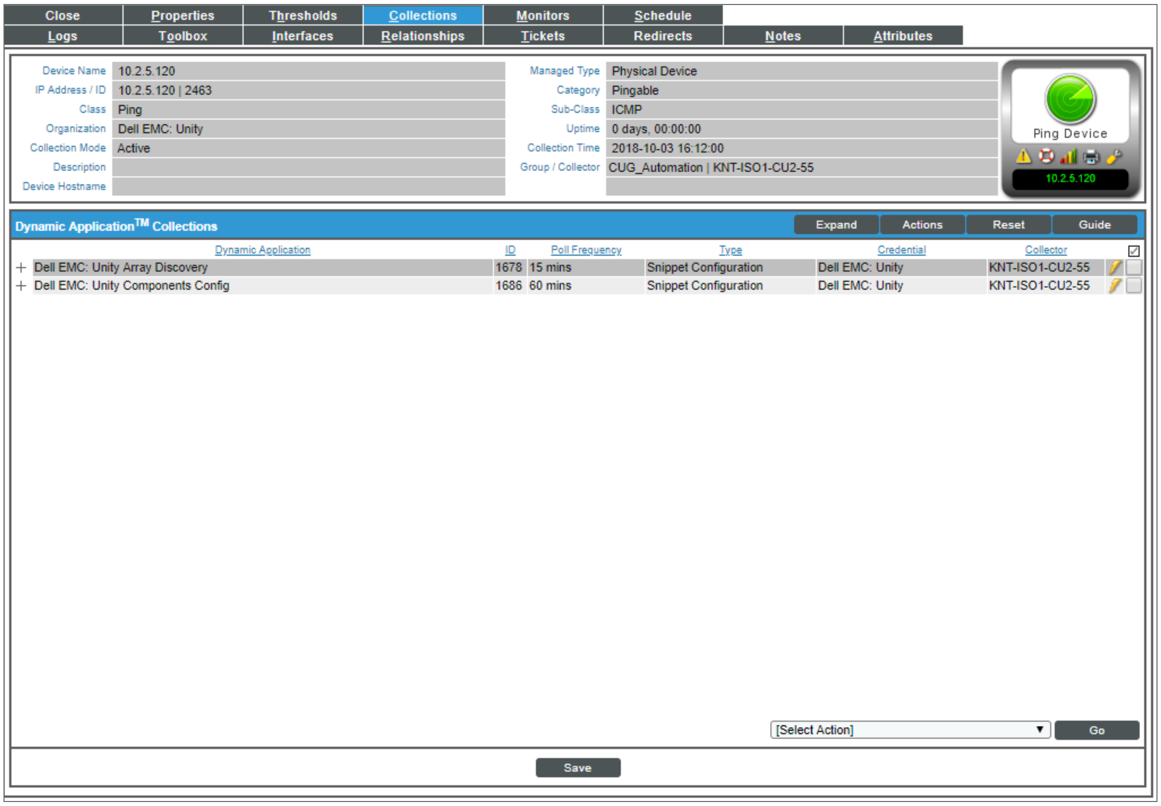
4. Optionally, you can enter values in the other fields on this page. For more information about the other fields on this page, see the ***Discovery & Credentials*** manual.
5. Click the **[Save]** button to save the discovery session and then close the **Discovery Session Editor** window.
6. The discovery 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. After the devices are discovered, click the device icon ( ) to view the **Device Properties** page for each device.

Verifying Discovery andDynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. After discovery has completed, click the device icon for the root device ( ).
2. From the **Device Properties** page for the array device, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
3. All applicable Dynamic Applications for the device 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	10.2.5.120	Managed Type	Physical Device
IP Address / ID	10.2.5.120 | 2463	Category	Pingable
Class	Ping	Sub-Class	ICMP
Organization	Dell EMC: Unity	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2018-10-03 16:12:00
Description		Group / Collector	CUG_Automation | KNT-ISO1-CU2-55
Device Hostname			

10.2.5.120

Dynamic Application™ Collections

Dynamic Application	ID	Poll Frequency	Type	Credential	Collector	☑
+ Dell EMC: Unity Array Discovery	1678	15 mins	Snippet Configuration	Dell EMC: Unity	KNT-ISO1-CU2-55	☐
+ Dell EMC: Unity Components Config	1686	60 mins	Snippet Configuration	Dell EMC: Unity	KNT-ISO1-CU2-55	☐

The "Dell EMC: Unity Array Discovery" and "Dell EMC: Unity Components Config" Dynamic Applications are automatically aligned to the root device, after which the rest of the Dynamic Applications in the PowerPack will be aligned.

Chapter 31

Dell EMC: VMAX and PowerMax Unisphere API

Overview

The following sections describe how to configure and discover Dell EMC VMAX and PowerMax systems for monitoring by SL1 using the *Dell EMC: VMAX and PowerMax Unisphere API* PowerPack:

> NOTE: For more information about the *Dell EMC: VMAX and PowerMax Unisphere API* PowerPack, see the ***Monitoring Dell EMC VMAX and PowerMax Unisphere API*** manual.

Prerequisites for Monitoring Dell EMC VMAX and PowerMax Systems

Before you can monitor Dell EMC VMAX and PowerMax systems using the *Dell EMC: VMAX and PowerMax Unisphere API* PowerPack, you must have the following information about the Unisphere API that has already been properly configured:

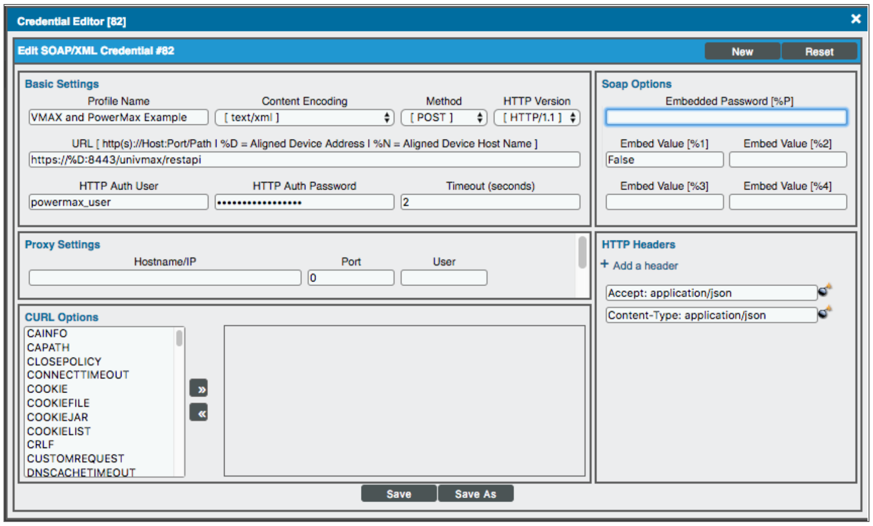
- Username and password for a user with access to the Unisphere REST API
- IP address and port for the Unisphere

Creating a Credential for Dell EMC VMAX and PowerMax Systems

To configure SL1 to monitor Dell EMC VMAX and PowerMax storage systems, you must first create a SOAP/XML credential. This credential allows the Dynamic Applications in the *Dell EMC: VMAX and PowerMax Unisphere API* PowerPack to use the Unisphere REST API. An example SOAP/XML credential that you can edit for your own use is included in the *Dell EMC: VMAX and PowerMax Unisphere API* PowerPack.

To create a SOAP/XML credential to access the Unisphere REST API:

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



Profile Name: VMAX and PowerMax Example
Content Encoding: [text/xml]
Method: [POST]
HTTP Version: [HTTP/1.1]
URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://%D:8443/univmax/restapi
HTTP Auth User: powermax_user
HTTP Auth Password: •••••••••••••••••
Timeout (seconds): 2
Embedded Password [%P]:
Embed Value [%1]: False
Embed Value [%2]:
Embed Value [%3]:
Embed Value [%4]:
Hostname/IP:
Port: 0
User:
Accept: application/json
Content-Type: application/json

- ***Profile Name***. Type a new name for the Dell EMC VMAX or PowerMax credential.
- ***HTTP Auth User***. Type the username for a user with access to the Unisphere REST API.
- ***HTTP Auth Password***. Type the password for the user you specified in the ***HTTP Auth User*** field.

NOTE: The ***HTTP Headers*** that are included in the example are required to receive a response from the Unisphere REST API. Do not delete or edit them.

4. Click the **[Save As]** button.
5. When the confirmation message appears, click **[OK]**.

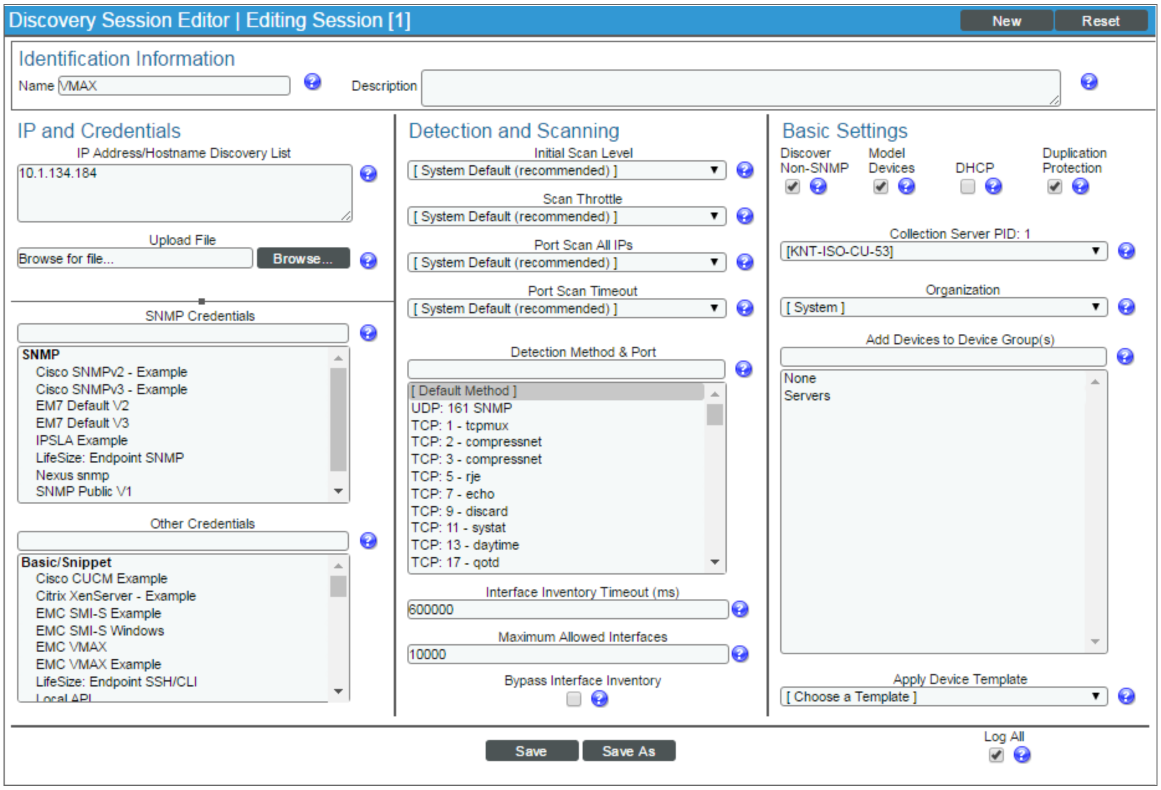
Discovering Dell EMC VMAX and PowerMax Systems

To model and monitor your Dell EMC VMAX and Powermax systems, you must run a discovery session to discover the Unisphere that SL1 will use as the root device for monitoring the VMAX or PowerMax system.

The discovery session will discover the Unisphere as a pingable device using *the SOAP/XML credential that you created*. The Dynamic Applications will automatically align to the Unisphere root device to enable SL1 to discover, model, and monitor the remaining component devices in your VMAX or PowerMax system.

To discover your VMAX or PowerMax storage system in SL1:

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



Discovery Session Editor | Editing Session [1]

Identification Information

Name: VMAX

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.1.134.184

Upload File: Browse for file...

SNMP Credentials

SNMP
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
EM7 Default V2
EM7 Default V3
IPSLA Example
LifeSize: Endpoint SNMP
Nexus snmp
SNMP Public V1

Other Credentials

Basic/Snippet
Cisco CUCM Example
Citrix XenServer - Example
EMC SMI-S Example
EMC SMI-S Windows
EMC VMAX
EMC VMAX Example
LifeSize: Endpoint SSH/CLI
Local API

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: 1: [KNT-ISO-CU-53]

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 for the Unisphere.
- ***Other Credentials***. Select the SOAP/XML credential you created for the VMAX or PowerMax system.
- ***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 **[Save]** to save the discovery session and then close the **Discovery Session Editor** window.
6. The discovery session you created will display at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon (⚡) to run the discovery session.

Chapter 32

Dell EMC: XtremIO

Overview

The following sections describe how to configure and discover Dell EMC XtremIO storage devices for monitoring by SL1 using the *Dell EMC: XtremIO* PowerPack:

NOTE: For more information about the *Dell EMC: XtremIO* PowerPack, see the ***Monitoring Dell EMC XtremIO*** manual.

Prerequisites for Monitoring Dell EMC XtremIO

Before you can monitor Dell EMC XtremIO storage devices in SL1 using the *Dell EMC: XtremIO* PowerPack, you must have already properly installed and configured the XtremIO storage devices that you want to monitor.

In addition, you must create a read-only user in the XtremIO Management Server (XMS) with the following user permissions:

- ***User Name***: Type the XMS user's name.
- ***Authentication***. Select the ***By Password*** checkbox.
- ***Password***: Type and then confirm the XMS user's password.

You can also configure LDAP authentication for this account.

Finally, take note of the SNMP community string used by the XtremIO storage devices you want to monitor.

For more information about these configuration processes, see the Dell EMC XtremIO documentation.

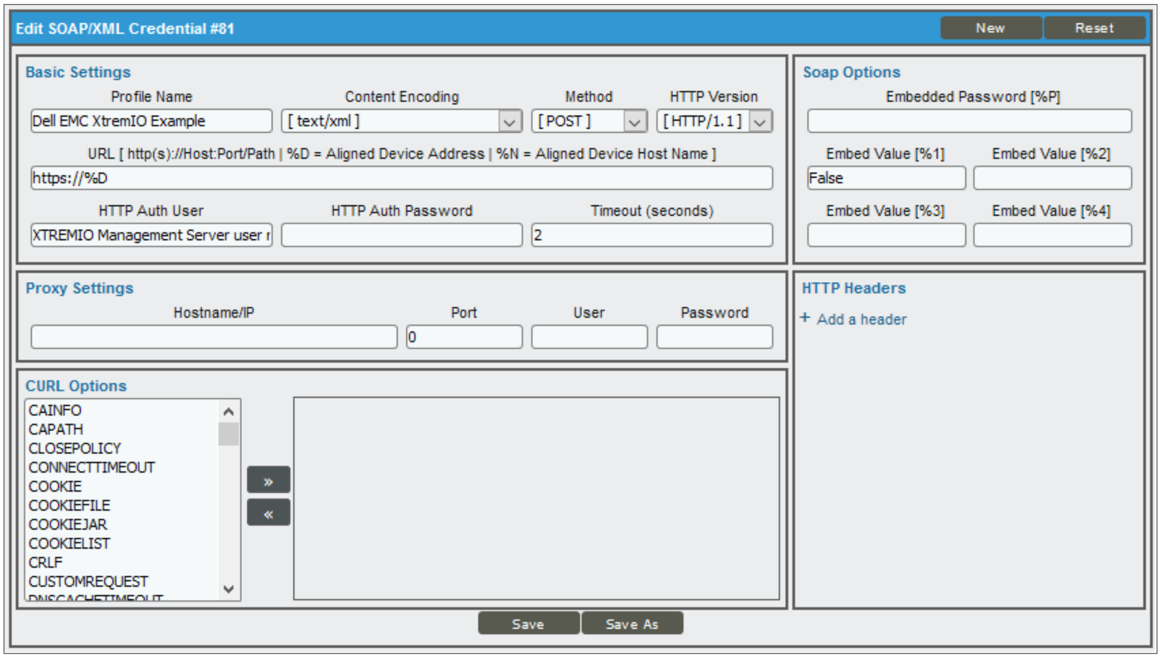
Creating a SOAP/XML Credential for Dell EMC XtremIO

To configure SL1 to monitor Dell EMC XtremIO storage devices, you must create a credential that allows the Dynamic Applications in the *Dell EMC: XtremIO* PowerPack to communicate with your XtremIO storage devices. The PowerPack includes an example SOAP/XML credential that you can edit for your own use.

To configure the SOAP/XML credential to access Dell EMC XtremIO devices:

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

2. Locate the **Dell EMC XtremIO Example - SOAP/XML** credential, and then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears.



Edit SOAP/XML Credential #81

Basic Settings

Profile Name: Dell EMC XtremIO Example
Content Encoding: [text/xml]
Method: [POST]
HTTP Version: [HTTP/1.1]
URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://%D
HTTP Auth User: XTREMIO Management Server user r
HTTP Auth Password:
Timeout (seconds): 2

Soap Options

Embedded Password [%P]:
Embed Value [%1]: False
Embed Value [%2]:
Embed Value [%3]:
Embed Value [%4]:

Proxy Settings

Hostname/IP:
Port: 0
User:
Password:

HTTP Headers

3. Update the values in the following fields:

Basic Settings

- ***Profile Name***. Type a name for the credential.
- ***Content Encoding***. Select *text/xml*.
- ***Method***. Select POST.
- ***HTTP Version***. Select HTTP/1.1.
- ***URL***. Type the device IP address or the host name for your XtremIO devices.
- ***HTTP Auth User***. Type the XtremIO administrator username.
- ***HTTP Auth Password***. Type the XtremIO administrator password.
- ***Timeout (seconds)***. Type "2".

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 "True" to enable verification of the storage array's self-signed certificate. Since the certificate is self-signed, you will need to determine if you trust the certificate and, if so, add it to a file. Append the applicable XMS root certificates to the file located at `/var/lib/em7/content/silo_rest/root_cert/xms_root_ca.crt` for any XMS being monitored. Type "False" or leave this field blank to disable SSL verification. This field is not case-sensitive.
- ***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.

Configuring Traps with Dell EMC XtremIO

To send alerts to SL1, SNMP traps must be enabled and configured on the Dell EMC XtremIO storage array. When configuring these traps, use the IP address of the ScienceLogic Message Collector, Data Collector, or All-In-One Appliance responsible for monitoring the system as the destination IP.

For more information, see the Dell EMC XtremIO documentation.

Discovering Dell EMC XtremIO Component Devices

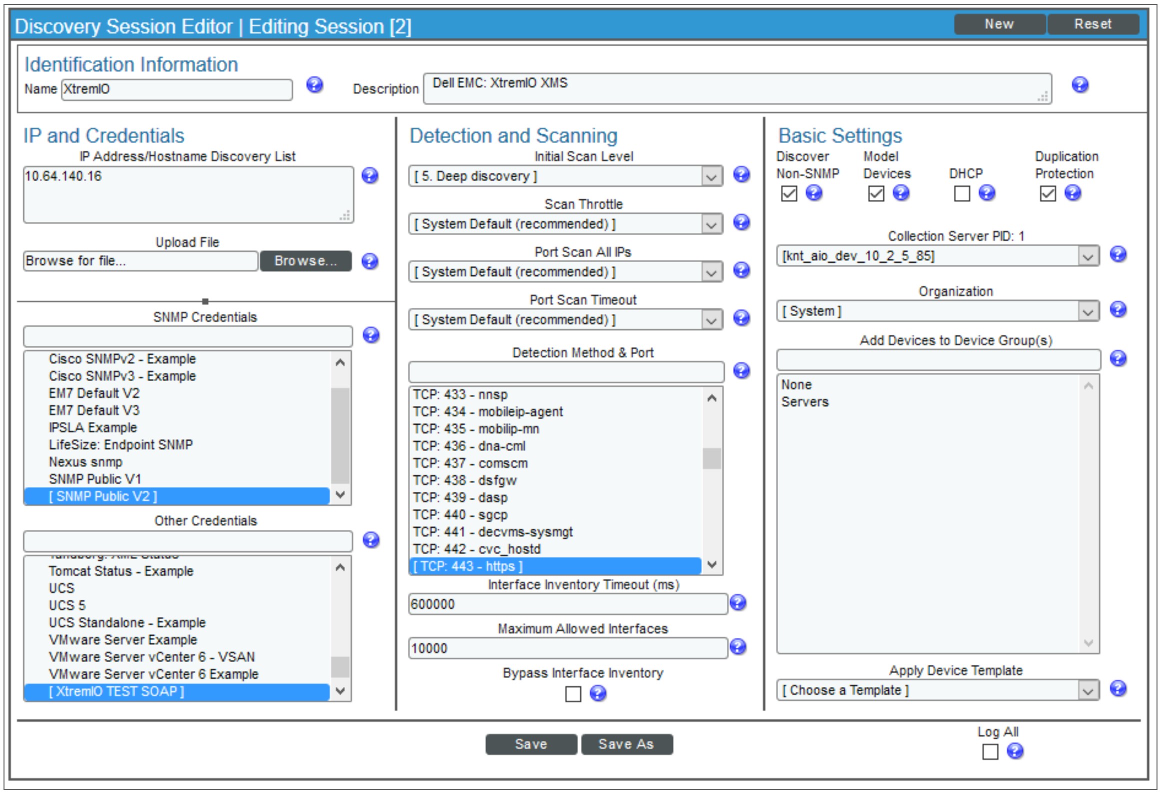
To model and monitor your Dell EMC XtremIO storage devices, you must run a discovery session to discover the XtremIO Management Server (XMS) device and XtremIO clusters that SL1 will use as the root devices for monitoring the applications.

After the discovery session completes, the Dynamic Applications in the *Dell EMC: XtremIO* PowerPack automatically align to the XMS device, and then the PowerPack discovers, models, and monitors the remaining XtremIO storage devices.

To discover the XtremIO devices that you want to monitor, perform the following steps:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic 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: XtremIO

Description: Dell EMC: XtremIO XMS

IP and Credentials

IP Address/Hostname Discovery List: 10.64.140.16

SNMP Credentials: [SNMP Public V2]

Other Credentials: [XtremIO TEST SOAP]

Detection and Scanning

Initial Scan Level: [5. Deep discovery]

Scan Throttle: [System Default (recommended)]

Port Scan All IPs: [System Default (recommended)]

Port Scan Timeout: [System Default (recommended)]

Detection Method & Port: [TCP: 443 - https]

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: 1 [knt_aio_dev_10_2_5_85]

Organization: [System]

Add Devices to Device Group(s): None, Servers

Apply Device Template: [Choose a Template]

Log All: □

- ***IP Address/Hostname Discovery List***. Enter the IP address or hostname for the XtremIO storage device or devices that you want to discover.
- ***SNMP Credentials***. Select the SNMP credential that you are using for XtremIO.
- ***Other Credentials***. Select the Basic/Snippet or SOAP/XML credential that you created for your XtremIO storage devices.
- ***Initial Scan Level***. Select *5. Deep Discovery*.
- **Detection Method & Port**: Select *TCP: 443 - https*.
- ***Discover Non-SNMP***. Select this checkbox.
- ***Model Devices***. Select this checkbox.
- ***Duplication Protection***. 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.

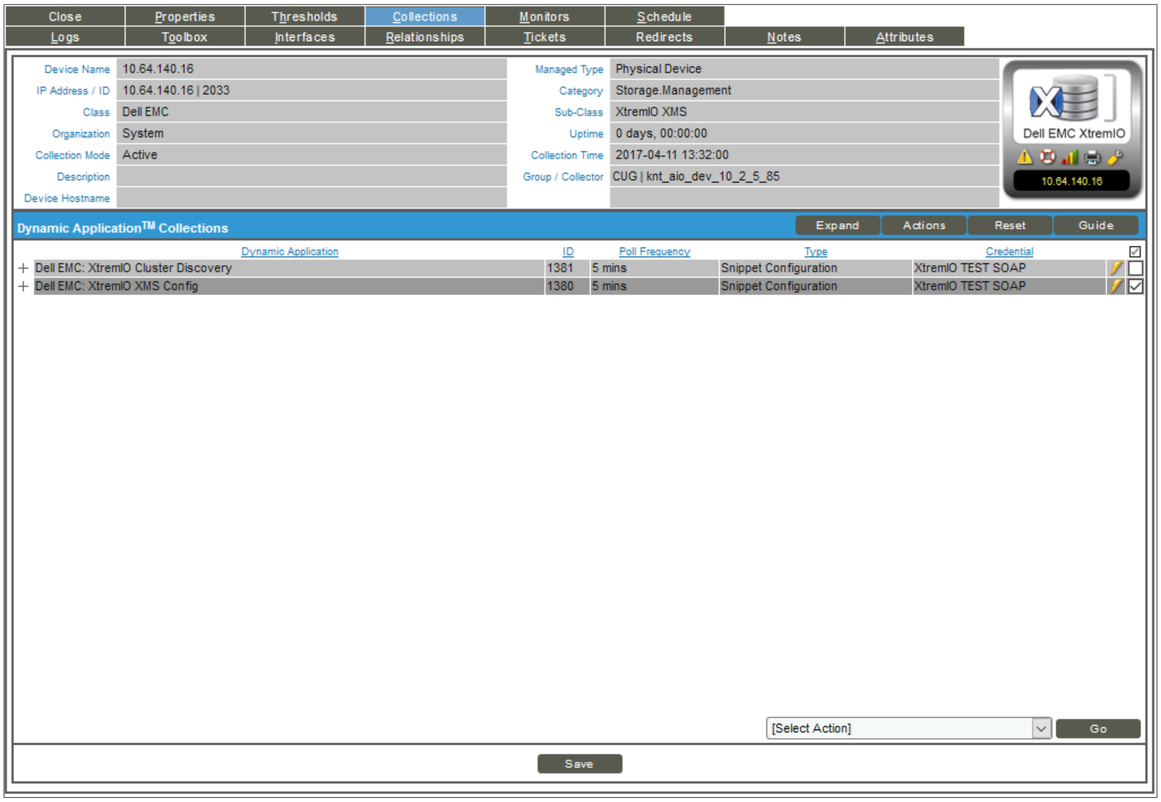
7. The **Discovery Session** window appears. After the devices are discovered, click the device icon ( ) to view the **Device Properties** page for each device.

Verifying Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. After discovery has completed, click the device icon for the XMS device ( ). From the **Device Properties** page for the XMS device, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. All applicable Dynamic Applications for the XMS device 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	10.64.140.16	Managed Type	Physical Device
IP Address / ID	10.64.140.16 | 2033	Category	Storage.Management
Class	Dell EMC	Sub-Class	XtremIO XMS
Organization	System	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2017-04-11 13:32:00
Description		Group / Collector	CUG | knt_aio_dev_10_2_5_85
Device Hostname			

Dynamic Application^{TM} Collections

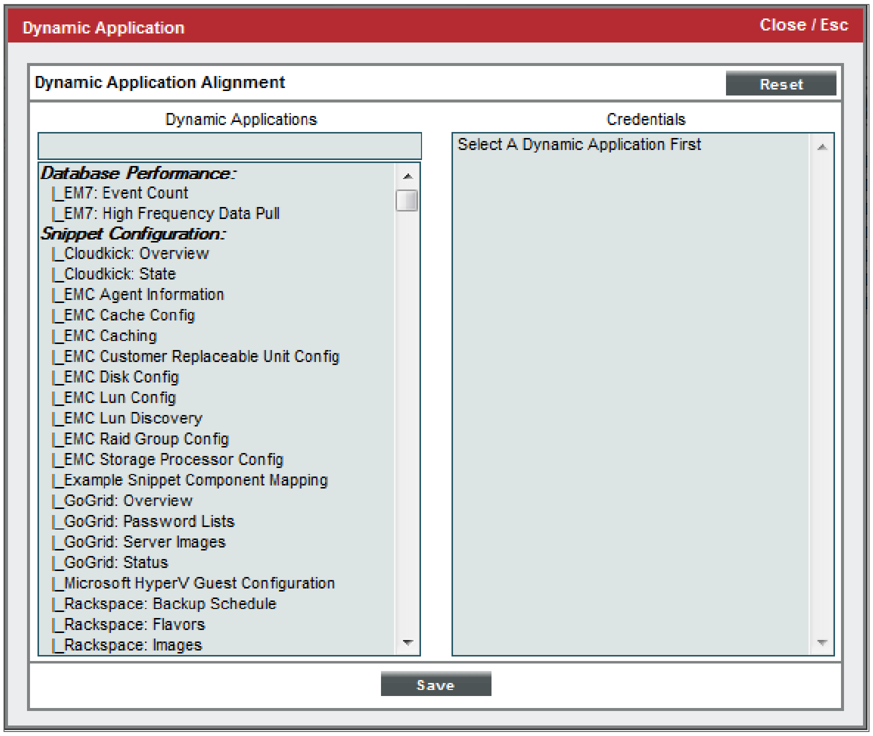
	Dynamic Application	ID	Poll Frequency	Type	Credential	☑
+	Dell EMC: XtremIO Cluster Discovery	1381	5 mins	Snippet Configuration	XtremIO TEST SOAP	☐
+	Dell EMC: XtremIO XMS Config	1380	5 mins	Snippet Configuration	XtremIO TEST SOAP	☑

You should see the following Dynamic Applications aligned to the XMS device:

Dynamic Application	Credential Type
Dell EMC: XtremIO Cluster Discovery	SOAP/XML
Dell EMC: XtremIO XMS Config	SOAP/XML

If the listed Dynamic Applications have not been automatically aligned during discovery, you can align them manually. To do so, perform the following steps:

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 credential specified in the table.
4. Click the **[Save]** button.
5. Repeat steps 1-4 for the other unaligned Dynamic Applications.

Chapter

32

Docker

Overview

The following sections describe how to configure and discover the Docker platform and its component devices for monitoring by SL1 using the *Docker* PowerPack:

NOTE: For more information about the *Docker* PowerPack, see the ***Monitoring Docker*** manual.

Prerequisites for Monitoring Docker

If you are using Secure Shell (SSH) to monitor Docker or Kubernetes nodes in conjunction with the *Kubernetes* PowerPack, you must install cURL 7.40 or greater on all of the Docker hosts that you want to monitor, prior to discovery. You must then run the following cURL commands on each of those hosts:

- `curl --unix-socket /var/run/docker.sock http://docker/containers/json`
- `curl --unix-socket /var/run/docker.sock http://docker/containers/\[container_id]/json`
- `curl --unix-socket /var/run/docker.sock http://docker/containers/\[container_id]/stats?stream=0`

If you are using a Basic/Snippet credential, before you can monitor the Docker platform and its component devices in SL1 using the *Docker* PowerPack, you must first follow the instructions in the ***Enabling the Docker API*** section. These steps enable the Dynamic Applications in the *Docker* PowerPack to communicate with and gather data from the Docker API.

NOTE: You do not need to enable the API if you are using SSH to monitor Docker.

WARNING: If you choose to enable the API when monitoring Docker versions through 18.06.1-ce-rc2, be aware that a vulnerability exists. The API endpoints behind the 'docker cp' command are vulnerable to a symlink-exchange attack. (CVE-2018-15664).

Enabling the Docker API

Before you discover Docker components using the *Docker* PowerPack, you must first enable the Docker API. This section describes how to do so for Windows, CentOS, Red Hat Enterprise Linux (RHEL), and Oracle Linux operating systems.

NOTE: If you are using SSH to monitor Docker, skip this section and go to the ***Creating an SSH/Key Credential*** section.

Windows

To enable the Docker API for Windows using the Docker Toolbox:

1. Start Docker Quickstart Terminal.
2. To determine the IP address of the Docker host machine, type the following command:

   ```
   $ docker-machine ip
   ```

3. Log in to the host machine:

   ```
   $ docker-machine ssh
   ```

4. Navigate to Boot2Docker:

   ```
   $ cd /var/lib/boot2docker
   ```

5. Edit the Boot2Docker profile:

```
$ sudo vi profile
```

6. In the profile, change "DOCKER_HOST" to "DOCKER_HOST='-H tcp://0.0.0.0:*[port number]*'", and set DOCKER_TLS=no.
7. Exit the SSH session, and then restart Docker:

```
$ exit
$ docker-machine restart
```

8. To verify that the Docker API is accessible, open a browser and navigate to http:*[IP address]*:*[port number]*/version.

   If the Docker API is successfully enabled, the version returns something similar to the following:

```
{"Version":"17.10.0-ce","ApiVersion":"1.33","MinAPIVersion":"1.12","GitCommit":
"f4ffd25","GoVersion":"go1.8.3","Os":"linux","Arch":"amd64","KernelVersion":
"4.4.93-boot2docker","BuildTime":"2017-10-17T19:05:23.000000000+00:00"}
```

CentOS

To enable the Docker API for CentOS:

1. Log in to the command-line interface of the server running Docker and navigate to systemd/system:

```
$ cd /etc/systemd/system
```

2. Create a new "docker.service.d" folder, then navigate to that folder:

```
$ mkdir docker.service.d
$ cd docker.service.d
```

3. Create a new docker.conf file:

```
$ vi docker.conf
```

4. Type the following:

```
INSERT
[Service]
ExecStart=
ExecStart=/usr/bin/dockerd -H tcp://0.0.0.0:[port number] -H
unix://var/run/docker.sock
```

5. Reload daemon, restart Docker, and open the port on the firewall by typing the following:

```
$ systemctl daemon-reload
$ systemctl restart docker
$ firewall-cmd --add-port=[port number]/tcp
```

6. Verify that the Docker API is accessible by typing the following:

```
$ *curl http://localhost:[port number]/version*
```

If the Docker API is successfully enabled, the version returns something similar to the following:

```
{"Version":"17.06.1-ce","ApiVersion":"1.30","MinAPIVersion":"1.12","GitCommit"
:"874a737","GoVersion":"go1.8.3","Os":"linux","Arch":"amd64","KernelVersion":
"3.10.0-514.26.2.el7.x86_64","BuildTime":"2017-08-17T23:01:50.155177940+00:00"}
```

RHEL 7 and Oracle Linux 7

To enable the Docker API for RHEL 7 or Oracle Linux 7:

1. Log in to the command-line interface of the server running Docker and navigate to systemd/system:

```
$ cd /etc/systemd/system
```

2. Edit the service.docker file:

```
$ sudo vi docker.service
```

3. Create or edit the file to ensure that it has a [Service] section and a line that starts with "`ExecStart=/usr/bin/dockerd`". Add "`-H tcp://0.0.0.0:[port number] -H unix:///var/run/docker.sock`" so that the updated line looks like this:

```
ExecStart=/usr/bin/dockerd -H tcp://0.0.0.0:4243 -H unix:///var/run/docker.sock
```

4. Open the firewall port, if needed, and then reload daemon and restart restart Docker by typing the following:

```
$ sudo firewall-cmd --add-port=[port number]/tcp
$ sudo firewall-cmd --reload
$ sudo systemctl daemon-reload
$ sudo systemctl restart docker
```

5. Verify that the Docker API is accessible by typing the following:

```
$ curl http://[IP address]:[port number]/version
```

If the Docker API is successfully enabled, the version returns something similar to the following:

```
{"Version":"17.06.2-ee-4","ApiVersion":"1.30","MinAPIVersion":"1.12","GitCommit":
"dd2c358","GoVersion":"go1.8.3","Os":"linux","Arch":"amd64","KernelVersion":
"3.10.0-514.el7.x86_64","BuildTime":"2017-10-12T16:19:56.386620861+00:00"}
```

Configuring a Docker Credential

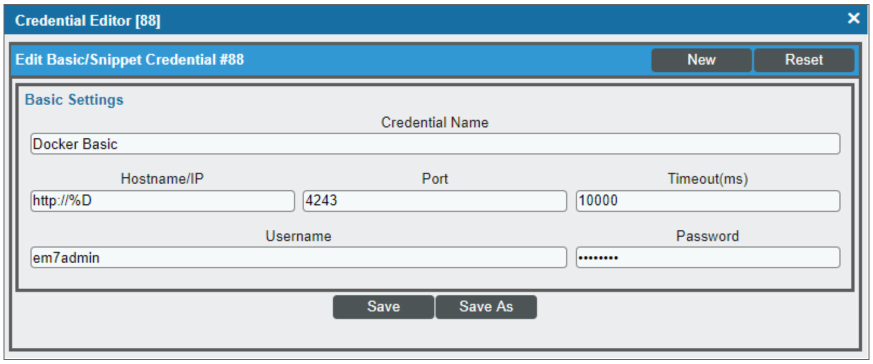
The *Docker* PowerPack includes an example Basic/Snippet Credential and an example SSH/Key Credential for your use. You can modify these to create your own Credentials that will enable SL1 to discover your Docker devices.

Creating a Basic/Snippet Credential

To configure SL1 to monitor the Docker platform using the Docker API, you must create a Basic/Snippet credential that allows the Dynamic Applications in the *Docker* PowerPack to connect with Docker hosts or swarms. An example Basic/Snippet credential that you can edit for your own use is included in the *Docker* PowerPack.

To create a Basic/Snippet credential to access Docker hosts or swarms:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the example **Docker Basic** credential, and then click its wrench icon (🔧). The **Edit Basic/Snippet Credential** modal page appears.
3. Complete the following fields:



Credential Name	Docker Basic	
Hostname/IP	Port	Timeout(ms)
http://%D	4243	10000
Username	Password	
em7admin	••••••••	

- ***Credential Name***. Type a new name for the Docker credential.
- ***Hostname/IP***. Type "%D".
- ***Port***. Type the port number you specified when you ***enabled the Docker API***.
- ***Timeout(ms)***. Type "10000".
- ***Username***. Type a value for the username.
- ***Password***. Type a value for the password.

NOTE: The Docker platform does not require a specific username and password to access the platform, but SL1 does require the ***Username*** and ***Password*** fields to have values when using Basic/Snippet credentials to monitor Docker. Therefore, those fields must have entries, but the values themselves do not matter.

4. Click the **[Save As]** button.
5. When the confirmation message appears, click **[OK]**.

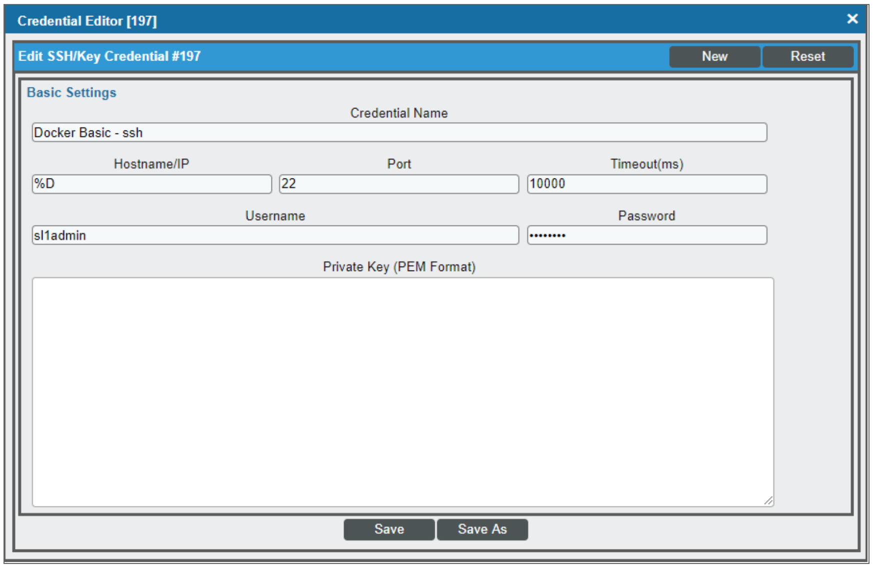
Creating an SSH/Key Credential

If you are using SSH to monitor Docker swarms, then you must create an SSH/Key credential that allows the Dynamic Applications in the *Docker* PowerPack to connect with Docker swarms. An example SSH/Key credential that you can edit for your own use is included in the *Docker* PowerPack.

> NOTE: You can also use an SSH credential in conjunction with the *Kubernetes* PowerPack to monitor the Docker infrastructure for a Kubernetes cluster.

To create an SSH/Key credential to monitor Docker containers:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the example **Docker Basic - SSH** credential, and then click its wrench icon (🔧). The **Edit SSH/Key Credential** modal page appears.
3. Complete the following fields:



Credential Name: Docker Basic - ssh

Hostname/IP: %D

Port: 22

Timeout(ms): 10000

Username: sl1admin

Password: ••••••••

Private Key (PEM Format):

- ***Credential Name***. Type a new name for the Docker credential.
- ***Hostname/IP***. Type "%D".
- ***Port***. Type the SSH port number for the Docker swarm you want to monitor.
- ***Timeout(ms)***. Type "10000".
- ***Username***. Type the username for a user with SSH access to the Docker swarm command line interface.
- ***Password***. Type the user's password.
- ***Private Key (PEM Format)***. Keep this field blank.

4. Click the **[Save As]** button.
5. When the confirmation message appears, click **[OK]**.

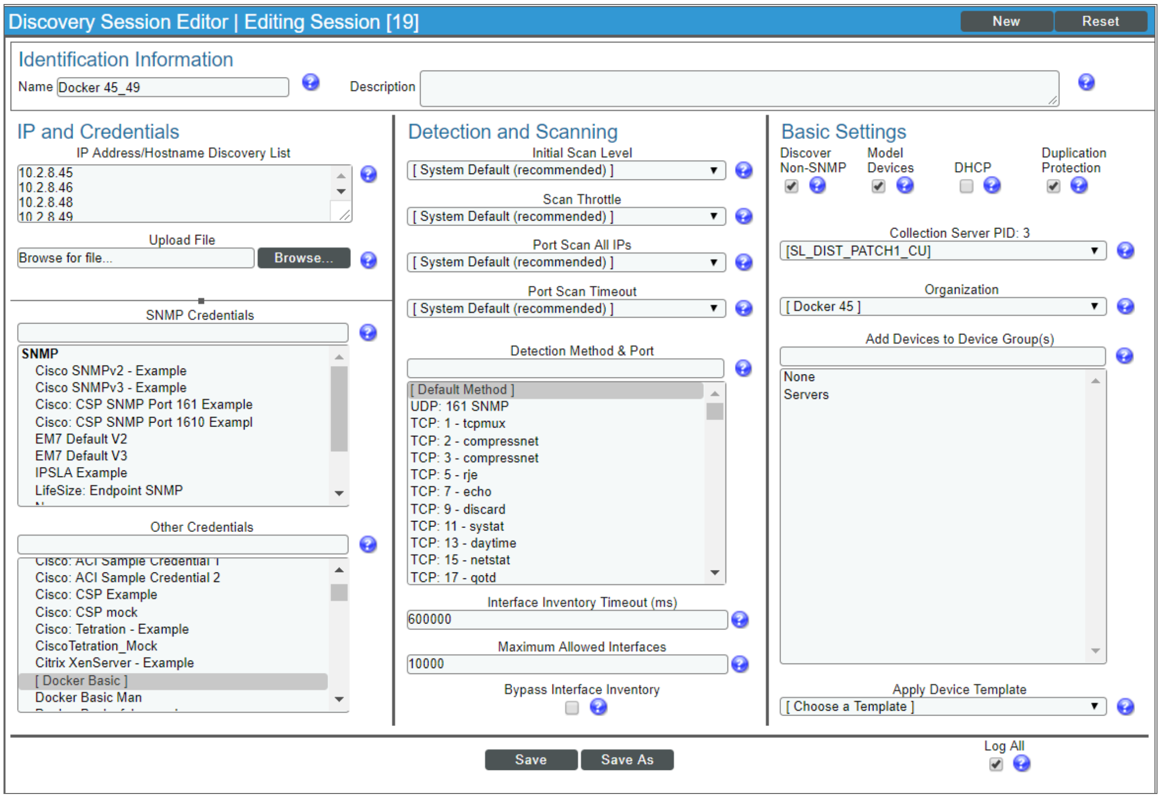
Discovering Docker Components

To discover and model your Docker component devices for monitoring, you must run a discovery session. The discovery session will discover the Docker hosts and swarms that SL1 will use as the root devices for monitoring the Docker components.

Several minutes after the discovery session has completed, the Dynamic Applications in the *Docker* PowerPack will automatically align to the Docker root devices. These Dynamic Applications will discover, model, and monitor the remaining components in your Docker system.

To discover Docker components, perform the following steps:

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



Discovery Session Editor | Editing Session [19]

Identification Information

Name: Docker 45_49
Description:

IP and Credentials

IP Address/Hostname Discovery List:
10.2.8.45
10.2.8.46
10.2.8.48
10.2.8.49

Upload File: Browse for file...

SNMP Credentials:
SNMP
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Cisco: CSP SNMP Port 161 Example
Cisco: CSP SNMP Port 1610 Exampl
EM7 Default V2
EM7 Default V3
IPSLA Example
LifeSize: Endpoint SNMP

Other Credentials:
Cisco: ACI Sample Credential 1
Cisco: ACI Sample Credential 2
Cisco: CSP Example
Cisco: CSP mock
Cisco: Tetration - Example
CiscoTetration_Mock
Citrix XenServer - Example
[Docker Basic]
Docker Basic Man

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
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: 3: [SL_DIST_PATCH1_CU]
Organization: [Docker 45]

Add Devices to Device Group(s):
None
Servers

Apply Device Template: [Choose a Template]

Log All: ☑

- ***Name***. Type a name for your discovery session.

- ***IP Address/Hostname Discovery List***. Type the IP addresses for all of the Docker hosts in the swarm that you want to discover.

> **NOTE:** Swarms are created only when the swarm leader is discovered.

- ***Other Credentials***. Select the *Basic/Snippet or SSH/Key credential(s)* you created for Docker.
- ***Discover Non-SNMP***. Select this checkbox.
- ***Model Devices***. Select this checkbox.

3. 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.
4. Click the **[Save]** button to save the discovery session, and then close the **Discovery Session Editor** window.
5. The discovery session you created displays at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon (⚡) to run the discovery session.
6. The **Discovery Session** window appears. When a root device is discovered, click its device icon (🖥) to view the **Device Properties** page for that device.

Manually Aligning Dynamic Applications

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

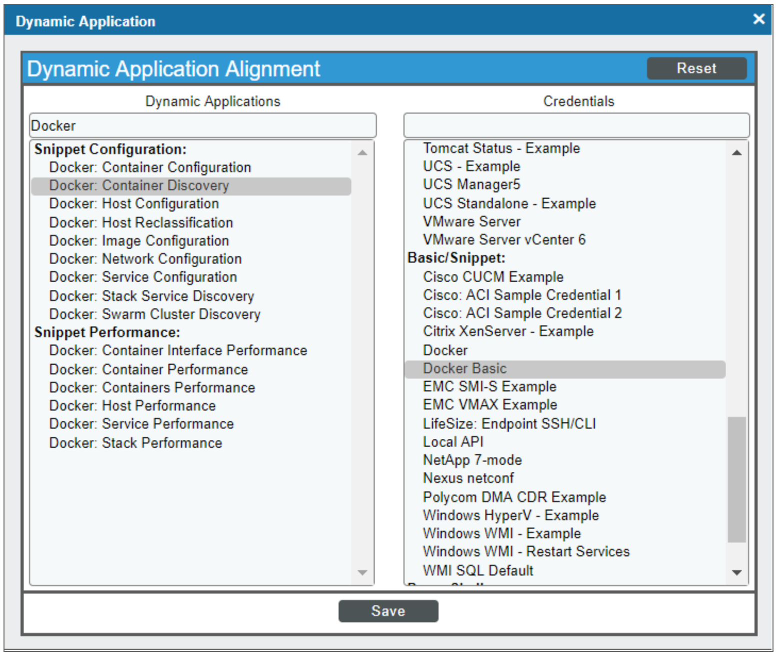
1. From the **Device Properties** page (Registry > Devices > wrench icon (🔧)) for the Docker root device, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. The following Dynamic Applications should appear in the list of aligned Dynamic Applications:
   - For Docker Hosts:
     - Docker: Container Discovery
     - Docker: Containers Performance
     - Docker: Host Configuration
     - Docker: Host Performance
     - Docker: Host Reclassification
     - Docker: Image Configuration
     - Docker: Image Performance
     - Docker: Network Configuration
     - Docker: Swarm Cluster Discovery
   - For Docker Swarms:
     - Docker: Stack Discovery

- Docker: Swarm Configuration
- Docker: Swarm Performance
- Docker: Swarm Service Discovery

> NOTE: It can take several minutes after discovery for Dynamic Applications to display on the **Dynamic Application Collections** page. If the listed Dynamic Applications do not display on this page, try clicking the **[Reset]** button.

If the Dynamic Applications have not been automatically aligned, you can align them manually. To do so, perform the following steps:

1. Go to the **Device Properties** page (Registry > Devices > wrench icon()) for the Docker root device and click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. On the **Dynamic Application Collections** page, click the **[Action]** button and then select *Add Dynamic Application* from the menu. The **Dynamic Application Alignment** page appears.


Dynamic Application
×
Dynamic Application Alignment
Reset
Dynamic Applications
Credentials
Docker
Snippet Configuration:
Docker: Container Configuration
Docker: Container Discovery
Docker: Host Configuration
Docker: Host Reclassification
Docker: Image Configuration
Docker: Network Configuration
Docker: Service Configuration
Docker: Stack Service Discovery
Docker: Swarm Cluster Discovery
Snippet Performance:
Docker: Container Interface Performance
Docker: Container Performance
Docker: Containers Performance
Docker: Host Performance
Docker: Service Performance
Docker: Stack Performance
Tomcat Status - Example
UCS - Example
UCS Manager5
UCS Standalone - Example
VMware Server
VMware Server vCenter 6
Basic/Snippet:
Cisco CUCM Example
Cisco: ACI Sample Credential 1
Cisco: ACI Sample Credential 2
Citrix XenServer - Example
Docker
Docker Basic
EMC SMI-S Example
EMC VMAX Example
LifeSize: Endpoint SSH/CLI
Local API
NetApp 7-mode
Nexus netconf
Polycom DMA CDR Example
Windows HyperV - Example
Windows WMI - Example
Windows WMI - Restart Services
WMI SQL Default
Save

3. In the ***Dynamic Applications*** field, select a Dynamic Application to align.
4. In the ***Credentials*** field, select the ***Basic/Snippet credential*** you created for Docker.
5. Click the **[Save]** button.
6. Repeat steps 2-5 as needed to align any additional Dynamic Applications.

Relationships Between Component Devices

In addition to parent/child relationships between component devices, SL1 also creates relationships between the following component devices:

- Swarms and Nodes
- Services and Containers

You can also use the *Docker* PowerPack in conjunction with the *Kubernetes* PowerPack when monitoring Kubernetes systems. When you do so, SL1 creates relationships between Docker Swarms and Containers and their underlying Kubernetes Nodes.

Chapter 33

Dynatrace

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 and discover Dynatrace resources for monitoring by SL1 using the *Dynatrace* PowerPack:

NOTE: For more information about the *Dynatrace* PowerPack, see the ***Monitoring Dynatrace*** manual.

Generating a Dynatrace API Token

To configure the SL1 system to monitor Dynatrace resources using the *Dynatrace*PowerPack, you must first generate a Dynatrace API token.

To do so:

1. Log in to your Dynatrace portal. On the left menu, click **Settings > Integration > Dynatrace API**. The **Dynatrace API** page appears.
2. Click the **[Generate Token]** button.
3. In the blank box that appears, type a token name, and then activate (at a minimum) the "Access problem and event feed, metrics, topology, and RUM JavaScript tag management" permission.
4. Click **[Generate]** to generate the API token.

TIP: You can click the **[Copy]** button next to the generated token to copy the token to your computer's clipboard.

5. The newly generated API token appears in your list of API tokens. Ensure that the ***Disable/enable*** switch is activated.
6. Optionally, if you want to verify the token, you can use an API tool like Postman or cURL to send a GET request for your Dynatrace environment, and then attach the token to the Api-Token realm for the Authorization HTTP header. For example:

```
curl --request GET \
  --url https://<Hostname>/e/<Environment-ID>.live.dynatrace.com/api/v1/time \
  --header 'Authorization: Api-Token <generated API token>' \
```

Configuring Dynatrace Credentials

To configure SL1 to monitor Dynatrace devices, you must first create a SOAP/XML credential. This credential allows the Dynamic Applications in the *Dynatrace* PowerPack to use your Dynatrace user account to retrieve information from the *Dynatrace* environment and component devices.

The PowerPack includes an example SOAP/XML credential (**Dynatrace Credential Example**) that you can edit for your own use.

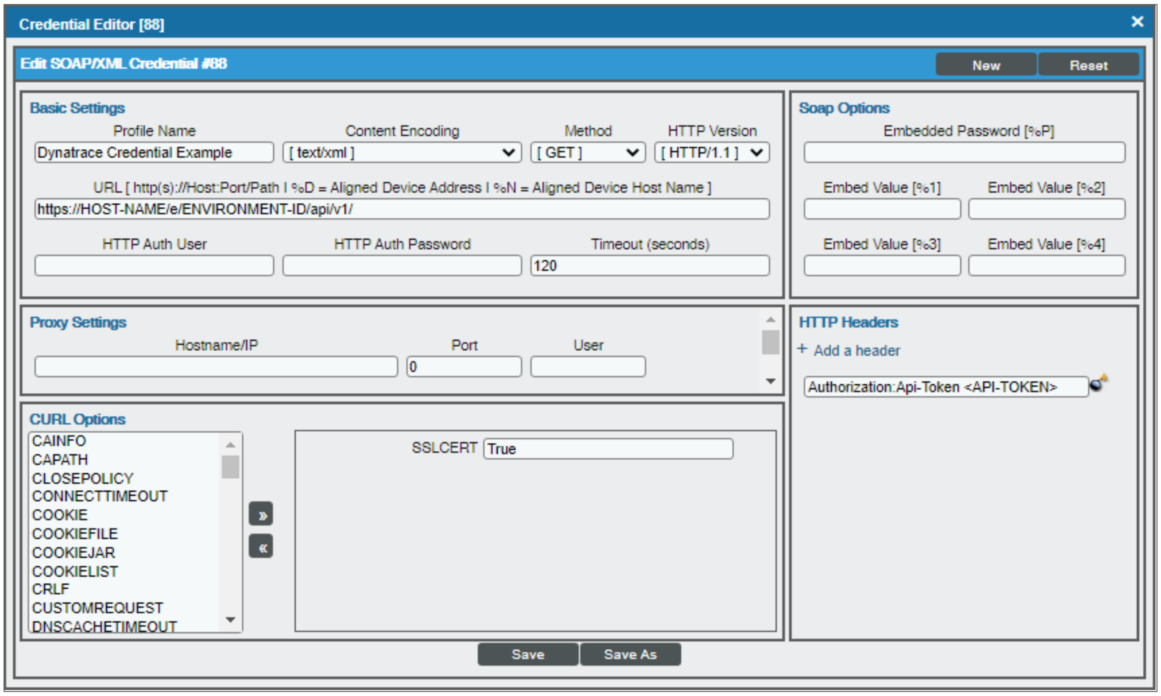
To configure SL1 to monitor Dynatrace devices, you must first create a SOAP/XML credential. This credential allows the Dynamic Applications in the *Dynatrace* PowerPack to use your Dynatrace user account to retrieve information from the *Dynatrace* environment and component devices.

The PowerPack includes example SOAP/XML credentials that you can edit for your own use:

- ***Dynatrace Credential Example***. The standard credential for monitoring Dynatrace.
- ***Dynatrace Cred MZFilter Example***. Use this credential for filtering hosts and services by Management Zone.
- ***Dynatrace Cred TagFilter Example***. Use this credential for filtering hosts and services by Tag Key.

To configure a SOAP/XML credential to access Dynatrace:

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



Basic Settings

Profile Name: Dynatrace Credential Example

Content Encoding: [text/xml]

Method: [GET]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://HOST-NAME/e/ENVIRONMENT-ID/api/v1/

HTTP Auth User:

HTTP Auth Password:

Timeout (seconds): 120

Soap Options

Embedded Password [%P]:

Embed Value [%1]:

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

Proxy Settings

Hostname/IP:

Port: 0

User

HTTP Headers

+ Add a header

Authorization:Api-Token <API-TOKEN>

CURL Options

CAINFO
CAPATH
CLOSEPOLICY
CONNECTTIMEOUT
COOKIE
COOKIEFILE
COOKIEJAR
COOKIELIST
CRLF
CUSTOMREQUEST
DNSCACHETIMEOUT

SSLCERT: True

3. Complete the following fields:

Basic Settings

- ***Profile Name***. Type a new name for the Dynatrace credential.
- ***URL***. Type your URL in the following format, replacing <Hostname> with your Dynatrace hostname and <Environment-ID> with your Dynatrace environment ID:

  https://<Hostname>/e/<Environment-ID>/api/v1/

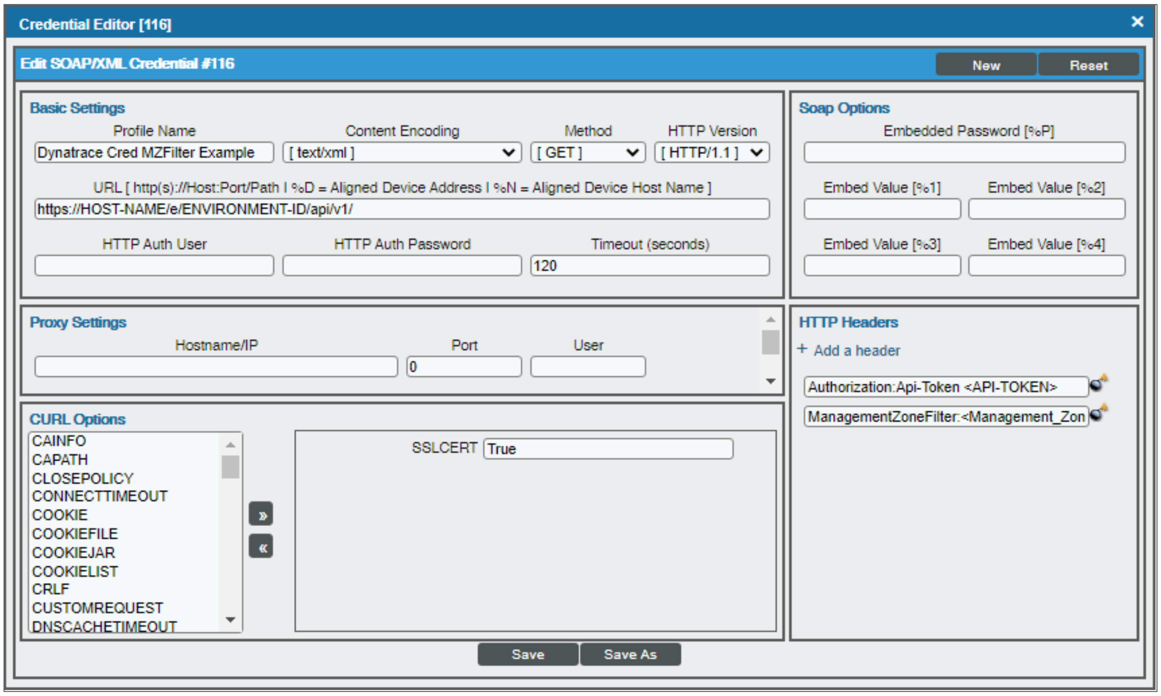
- ***HTTP Auth User***. This field must be blank.
- ***HTTP Auth Password***. This field must be blank.

HTTP Headers

- Type your authorization API token in the following format, replacing <API-Token> with your actual API token:

  Authorization: Api-Token <API-Token>

- If you want to filter hosts and services by Management Zone or Tag Key, the HTTP headers for these filters will appear in the " Dynatrace Cred MZFilter Example" and "Dynatrace Cred TagFilter Example" credentials.



Profile Name: Dynatrace Cred MZFilter Example

Content Encoding: [text/xml]

Method: [GET]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://HOST-NAME/e/ENVIRONMENT-ID/api/v1/

Timeout (seconds): 120

Port: 0

SSLCERT: True

Authorization:Api-Token <API-TOKEN>

ManagementZoneFilter:<Management_Zon

Update the headers in the following format:

ManagementZoneFilter: <Management_Zone_ID>

TagFilter: <TagName>

NOTE: You can filter only one Management Zone or Tag Key at a time.

CURL Options

- *SSLCERT*. Keep the default value of "True".

4. For the remaining fields, use the default values.
5. Click the **[Save As]** button.

Discovering Dynatrace Devices

To discover and monitor your Dynatrace environment, you must do the following:

- Create a virtual device representing the environment
- Configure the Dynatrace device template that is included in the *Dynatrace* PowerPack
- Align the device template to the Dynatrace virtual device

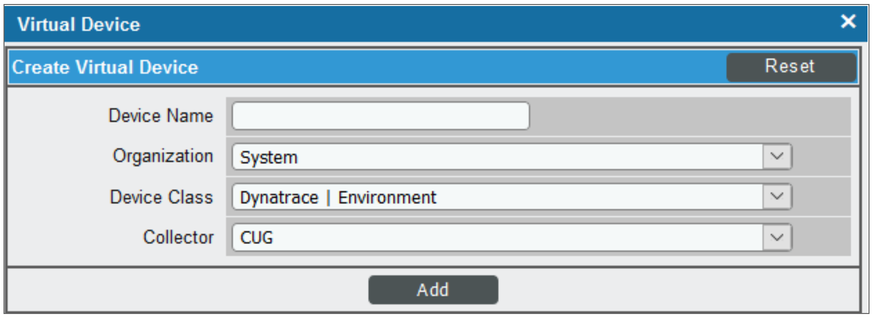
Each of these steps is documented in the following sections.

Creating a Dynatrace Virtual Device

Because the Dynatrace environment does not have a static IP address, you cannot discover a Dynatrace device by running a discovery session. Instead, you must create a ***virtual device*** that represents the Dynatrace environment. A virtual device is a user-defined container that represents a device or service that cannot be discovered by SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications.

To create a virtual device that represents your Dynatrace environment:

1. Go to the **Device Manager** page (Devices > Device Manager or Registry > Devices > Device Manager in the SL1 classic user interface).
2. Click the **[Actions]** button and select *Create Virtual Device* from the menu. The **Virtual Device** modal page appears:



Device Name
Organization: System
Device Class: Dynatrace | Environment
Collector: CUG

3. Complete the following fields:
   - ***Device Name***. Type a name for the device.
   - ***Organization***. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.
   - ***Device Class***. Select *Dynatrace | Environment*.
   - ***Collector***. Select the collector group that will monitor the device.
4. Click **[Add]** to create the virtual device.

Configuring the Dynatrace Device Template

A ***device template*** allows you to save a device configuration and apply it to multiple devices. The *Dynatrace* PowerPack includes the "Dynatrace Template," which enables SL1 to align all of the necessary Dynamic Applications to the environment root component device.

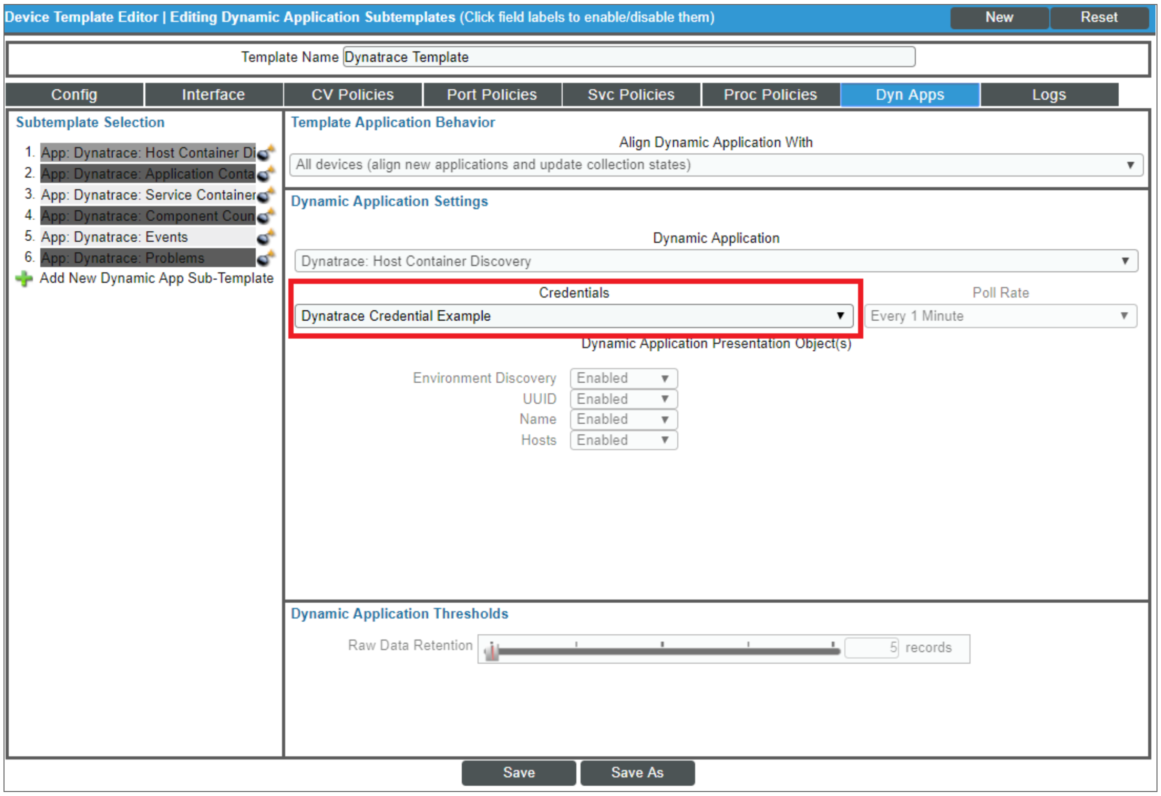
Before you can use the "Dynatrace Template", you must configure the template so that each Dynamic Application in the template aligns with the ***credential you created earlier***.

To configure the Dynatrace device template:

1. Go to the **Configuration Templates** page (Devices > Templates or Registry > Devices > Templates in the SL1 classic user interface).

2. Locate the "Dynatrace Template" and click its wrench icon (🔧). The **Device Template Editor** modal page appears.

3. Click the **[Dyn Apps]** tab. The **Editing Dynamic Application Subtemplates** page appears:



Device Template Editor | Editing Dynamic Application Subtemplates (Click field labels to enable/disable them)

Template Name: Dynatrace Template

Subtemplate Selection

1. App: Dynatrace: Host Container Di
2. App: Dynatrace: Application Conta
3. App: Dynatrace: Service Container
4. App: Dynatrace: Component Coun
5. App: Dynatrace: Events
6. App: Dynatrace: Problems

Add New Dynamic App Sub-Template

Template Application Behavior

Align Dynamic Application With: All devices (align new applications and update collection states)

Dynamic Application Settings

Dynamic Application: Dynatrace: Host Container Discovery

Credentials: Dynatrace Credential Example

Poll Rate: Every 1 Minute

Dynamic Application Presentation Object(s)

Environment Discovery: Enabled
UUID: Enabled
Name: Enabled
Hosts: Enabled

Dynamic Application Thresholds

Raw Data Retention: 5 records

4. In the ***Credentials*** drop-down list, select the credential that you created for Dynatrace.

5. Click the next Dynamic Application listed in the **Subtemplate Selection** section on the left side of the page and then select the credential you created in the ***Credentials*** field.

6. Repeat step 5 until you have selected your Dynatrace credential in the ***Credentials*** field for all of the

Dynamic Applications listed in the **Subtemplate Selection** section.

7. Click **[Save]**.

> NOTE: To maintain a "clean" version of the template, type a new name in the ***Template Name*** field and then click **[Save As]** instead of **[Save]**.

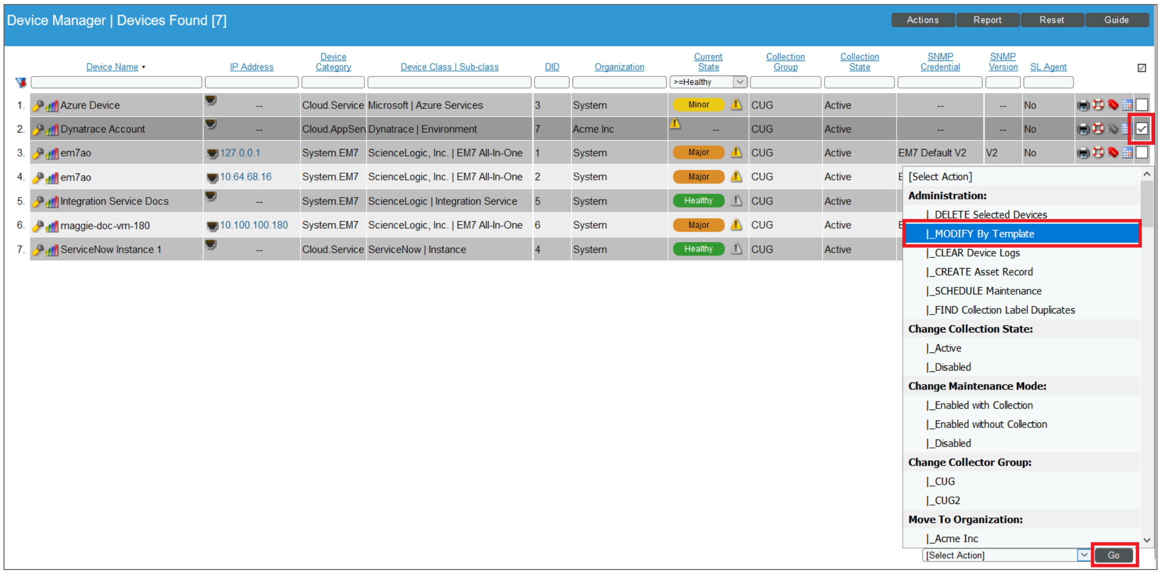
> NOTE: The "Dynatrace: Events" Dynamic Application is disabled by default in the *Dynatrace* PowerPack. To collect Dynatrace events, you must enable it. To do so, go to the **Dynamic Applications Manager** page (System > Manage > Applications), locate the "Dynatrace: Events" Dynamic Application and click its wrench icon (🔧), change the ***Operational State*** setting to *Enabled*, and then click **[Save]**.

Aligning the Device Template to Your Dynatrace Virtual Device

After you have configured the Dynatrace device template so that each Dynamic Application in the template aligns with your Dynatrace credential, you can use that template to align the Dynamic Applications to the virtual device that you created to act as the root device for your Dynatrace environment. When you do so, SL1 discovers and models all of the components in your Dynatrace environment.

To align the Dynatrace device template to the Dynatrace virtual device:

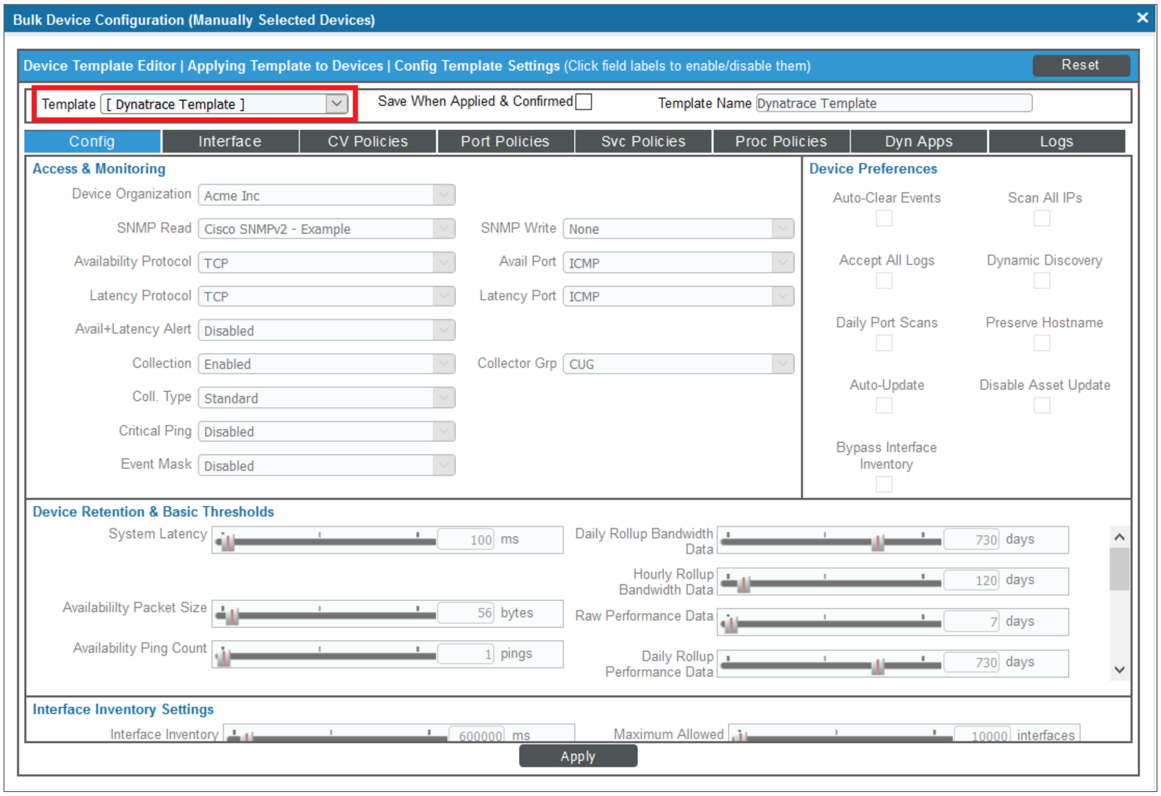
1. Go to the **Device Manager** page (Devices > Device Manager or Registry > Devices > Device Manager in the SL1 classic user interface).
2. On the **Device Manager** page, select the checkbox for the Dynatrace virtual device.
3. In the ***Select Actions*** field, in the lower right corner of the page, select the option *MODIFY by Template* and then click the **[Go]** button. The **Device Template Editor** page appears.



Device Manager | Devices Found [7]

	Device Name	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State	Collection Group	Collection State	SNMP Credential	SNMP Version	SL Agent	☑
							>=Healthy						
1.	Azure Device	--	Cloud.Service	Microsoft | Azure Services	3	System	Minor	CUG	Active	--	--	No	□
2.	Dynatrace Account	--	Cloud.AppSen	Dynatrace | Environment	7	Acme Inc	--	CUG	Active	--	--	No	☑
3.	em7ao	127.0.0.1	System.EM7	ScienceLogic, Inc. | EM7 All-In-One	1	System	Major	CUG	Active	EM7 Default V2	V2	No	□
4.	em7ao	10.64.68.16	System.EM7	ScienceLogic, Inc. | EM7 All-In-One	2	System	Major	CUG	Active	E			
5.	Integration Service Docs	--	System.EM7	ScienceLogic | Integration Service	5	System	Healthy	CUG	Active				
6.	maggie-doc-vm-180	10.100.100.180	System.EM7	ScienceLogic, Inc. | EM7 All-In-One	6	System	Major	CUG	Active	E			
7.	ServiceNow Instance 1	--	Cloud.Service	ServiceNow | Instance	4	System	Healthy	CUG	Active				

4. In the ***Template*** drop-down list, select your Dynatrace device template.



Bulk Device Configuration (Manually Selected Devices)

Device Template Editor | Applying Template to Devices | Config Template Settings (Click field labels to enable/disable them)

Template [Dynatrace Template]

Save When Applied & Confirmed □

Template Name Dynatrace Template

Access & Monitoring

Device Organization	Acme Inc		
SNMP Read	Cisco SNMPv2 - Example	SNMP Write	None
Availability Protocol	TCP	Avail Port	ICMP
Latency Protocol	TCP	Latency Port	ICMP
Avail+Latency Alert	Disabled		
Collection	Enabled	Collector Grp	CUG
Coll. Type	Standard		
Critical Ping	Disabled		
Event Mask	Disabled		

Device Preferences

Auto-Clear Events □	Scan All IPs □
Accept All Logs □	Dynamic Discovery □
Daily Port Scans □	Preserve Hostname □
Auto-Update □	Disable Asset Update □
Bypass Interface Inventory □	

Device Retention & Basic Thresholds

System Latency	100 ms	Daily Rollup Bandwidth Data	730 days
		Hourly Rollup Bandwidth Data	120 days
Availabililty Packet Size	56 bytes	Raw Performance Data	7 days
Availability Ping Count	1 pings	Daily Rollup Performance Data	730 days

Interface Inventory Settings

Interface Inventory	600000 ms	Maximum Allowed	10000 interfaces

5. Click the **[Apply]** button, and then click **[Confirm]** to align the Dynamic Applications to the root component device.

Filtering Partitions from Host Components

You can filter out partitions from host components in the "Dynatrace: Host Disk Performance" Dynamic Application. To do this, perform the following steps:

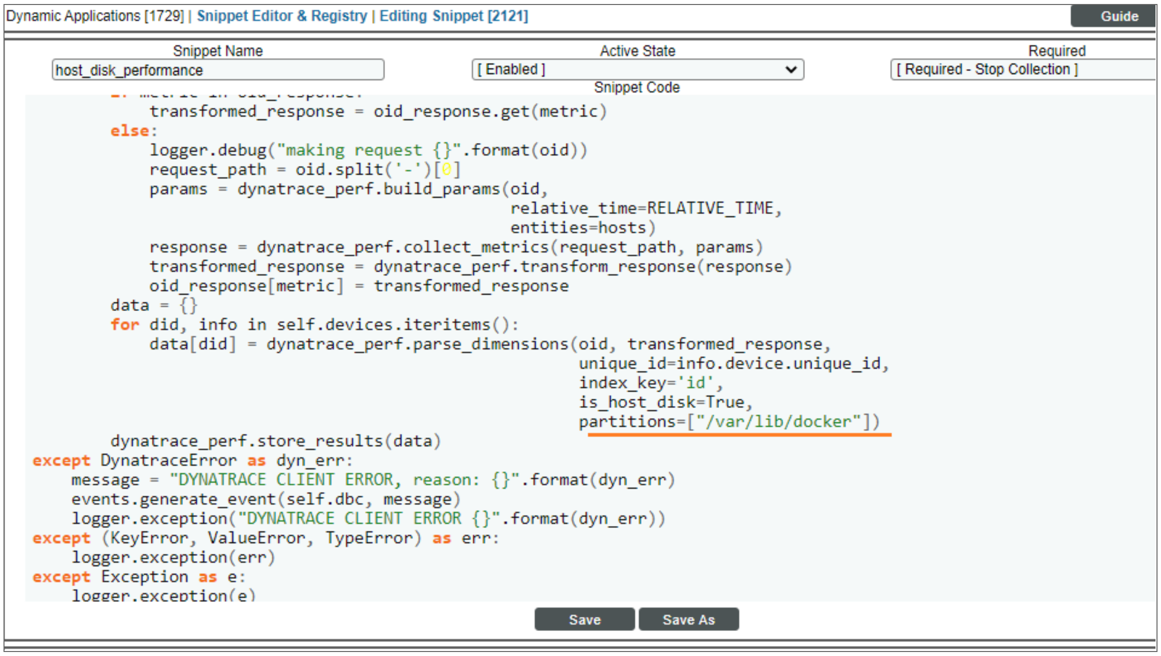
1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).

2. Locate the "Dynatrace: Host Disk Performance" Dynamic Application and click its wrench icon (🔧).

3. Click on the **[Snippets]** tab.

4. In the **Snippet Editor & Registry** page, click the wrench icon (🔧) for the "host_disk_performance" snippet.

5. Edit the `partitions=["/var/lib/docker"])` line to specify the partition(s) you want to filter out. You can specify more than one partition by separating them with commas and enclosing the partitions in quotation marks. Remove the partition if you want to collect data for it.


Dynamic Applications [1729] | Snippet Editor & Registry | Editing Snippet [2121]
Guide

Snippet Name: host_disk_performance

Active State: [Enabled]

Required: [Required - Stop Collection]

Snippet Code

```
        if metric in oid_response:
            transformed_response = oid_response.get(metric)
        else:
            logger.debug("making request {}".format(oid))
            request_path = oid.split('-')[0]
            params = dynatrace_perf.build_params(oid,
                                                 relative_time=RELATIVE_TIME,
                                                 entities=hosts)
            response = dynatrace_perf.collect_metrics(request_path, params)
            transformed_response = dynatrace_perf.transform_response(response)
            oid_response[metric] = transformed_response
        data = {}
        for did, info in self.devices.iteritems():
            data[did] = dynatrace_perf.parse_dimensions(oid, transformed_response,
                                                        unique_id=info.device.unique_id,
                                                        index_key='id',
                                                        is_host_disk=True,
                                                        partitions=["/var/lib/docker"])
        dynatrace_perf.store_results(data)
except DynatraceError as dyn_err:
    message = "DYNATRACE CLIENT ERROR, reason: {}".format(dyn_err)
    events.generate_event(self.dbc, message)
    logger.exception("DYNATRACE CLIENT ERROR {}".format(dyn_err))
except (KeyError, ValueError, TypeError) as err:
    logger.exception(err)
except Exception as e:
    logger.exception(e)
```

NOTE: The snippet will revert to default values each time the PowerPack is updated. You will need to update the snippet again each time you update the PowerPack.

Relationships Between Component Devices

In addition to parent/child relationships between component devices, SL1 also creates relationships between the following Dynatrace component devices:

- Hosts and Services
- Services and Applications

Additionally, the platform can automatically build relationships between Dynatrace component devices and other associated devices:

- If you discover Azure devices using the Dynamic Applications in the *Microsoft: Azure* PowerPack version 108 or later, SL1 will automatically create relationships between the following device types:
  - Dynatrace Hosts and Azure Virtual Machines
  - Dynatrace Hosts and Azure Virtual Machine Scale Sets
- If you discover Linux devices using the Dynamic Applications in the *Linux Base Pack* PowerPack version 102 or later, SL1 will automatically create relationships between Dynatrace Hosts and Linux Servers.
- If you discover VMware devices using the Dynamic Applications in the *VMware: vSphere Base Pack* PowerPack version 210 or later, SL1 will automatically create relationships between Dynatrace Hosts and VMware Virtual Machines.

- If you discover Windows devices using the Dynamic Applications in the *Microsoft: Windows Server* PowerPack version 107 or later or the *Microsoft Base Pack* PowerPack version 106 or later, SL1 will automatically create relationships between Dynatrace Hosts and Windows Servers.

Chapter 34

ELK: AWS CloudTrail

Overview

The following sections describe how to configure AWS component devices in ELK stacks for monitoring by SL1 using the *ELK: AWS CloudTrail* PowerPack:

NOTE: For more information about the *ELK: AWS CloudTrail* PowerPack, see the ***Monitoring Amazon Web Services ELK Stacks*** manual.

Prerequisites for Monitoring AWS ELK Stacks

To configure SL1 to monitor AWS component devices in ELK stacks using the *ELK: AWS CloudTrail* PowerPack, you must first:

- Install the *Amazon Web Services* PowerPack.
- Create a virtual device in SL1 to represent your AWS service.
- Discover AWS component devices by manually aligning the "AWS Account Discovery" Dynamic Application to the virtual device.
- Ensure that your AWS CloudTrail bucket is properly configured for all read/write events.

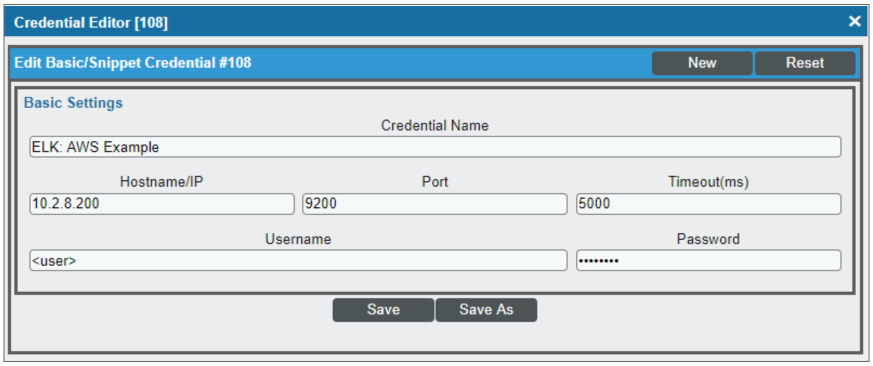
NOTE: For more information about the *Amazon Web Services* PowerPack, including how to install the PowerPack and discover AWS devices, see the ***Monitoring Amazon Web Services*** manual.

Creating an AWS ELK Credential

To use the Dynamic Applications in the *ELK: AWS CloudTrail* PowerPack, you must first define a credential in SL1. This credential enables the Dynamic Applications in the *ELK: AWS CloudTrail* PowerPack to monitor your AWS component devices in ELK stacks. The PowerPack includes a sample Basic/Snippet credential (**ELK: AWS Example**) that you can use as a template.

To define an AWS ELK credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the wrench icon (🔧) for the **ELK: AWS Example** credential. The **Credential Editor** modal page appears:



Credential Editor [108]

Edit Basic/Snippet Credential #108

Basic Settings

Credential Name: ELK: AWS Example

Hostname/IP: 10.2.8.200

Port: 9200

Timeout(ms): 5000

Username: <user>

Password: ••••••••

3. Enter values in the following fields:
   - ***Credential Name***. Type a new name for your AWS ELK credential.
   - ***Hostname/IP***. Type the IP address or hostname for the Logstash server that collects data for the AWS components in your ELK stack.
   - ***Port***. Type "9200".

   Use the default values for the remaining fields.

NOTE: The Basic/Snippet credential requires values in the ***Username*** and ***Password*** fields, but the values themselves do not matter.

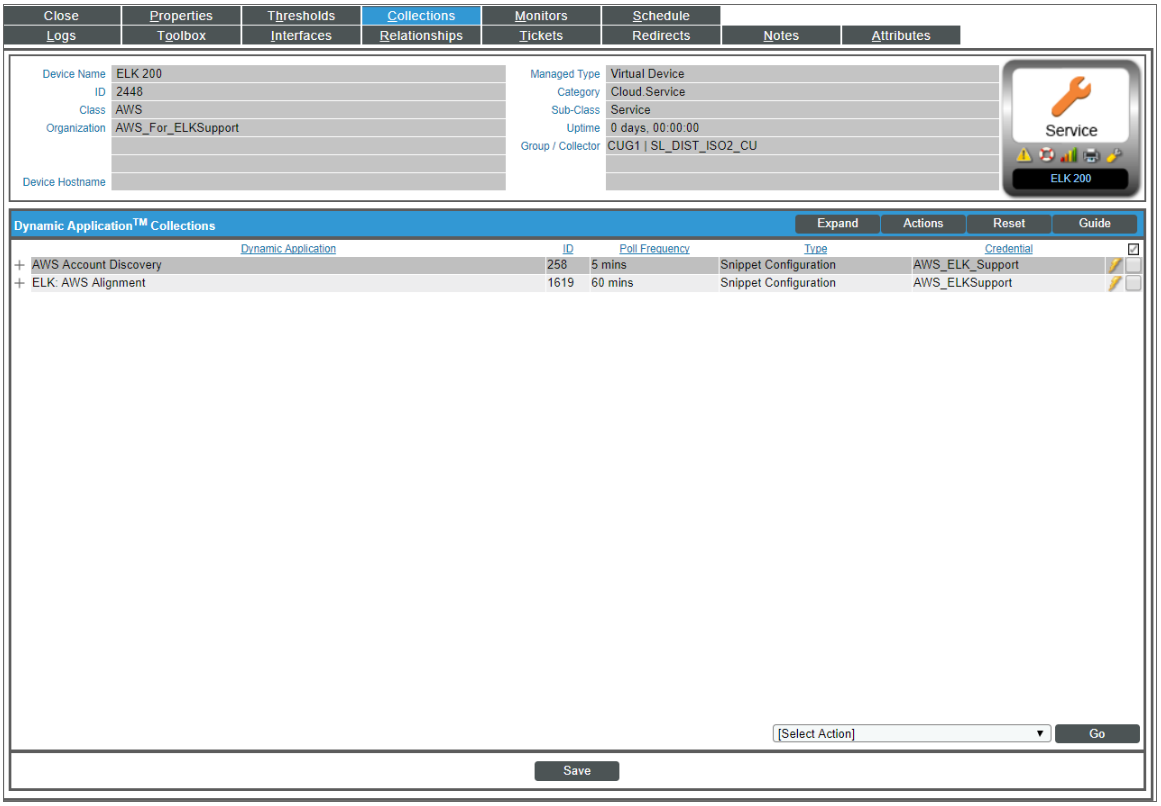
4. Click the **[Save As]** button, and then click **[OK]**.

Aligning the AWS ELK Dynamic Applications

To monitor your AWS component devices in ELK stacks, you must manually align the "ELK: AWS Alignment" Dynamic Application with the AWS virtual device. When you do so, the remaining Dynamic Applications from the *ELK: AWS CloudTrail* PowerPack automatically align to the appropriate AWS component devices.

To manually align the "ELK: AWS Alignment" Dynamic Application to your virtual device:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Locate your AWS virtual device and click its wrench icon (🔧).
3. In the **Device Administration** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.



Device Name ELK 200
ID 2448
Class AWS
Organization AWS_For_ELKSupport
Device Hostname
Managed Type Virtual Device
Category Cloud.Service
Sub-Class Service
Uptime 0 days, 00:00:00
Group / Collector CUG1 | SL_DIST_ISO2_CU

Dynamic Application^{TM} Collections

Dynamic Application	ID	Poll Frequency	Type	Credential	☑
+ AWS Account Discovery	258	5 mins	Snippet Configuration	AWS_ELK_Support	□
+ ELK: AWS Alignment	1619	60 mins	Snippet Configuration	AWS_ELKSupport	□

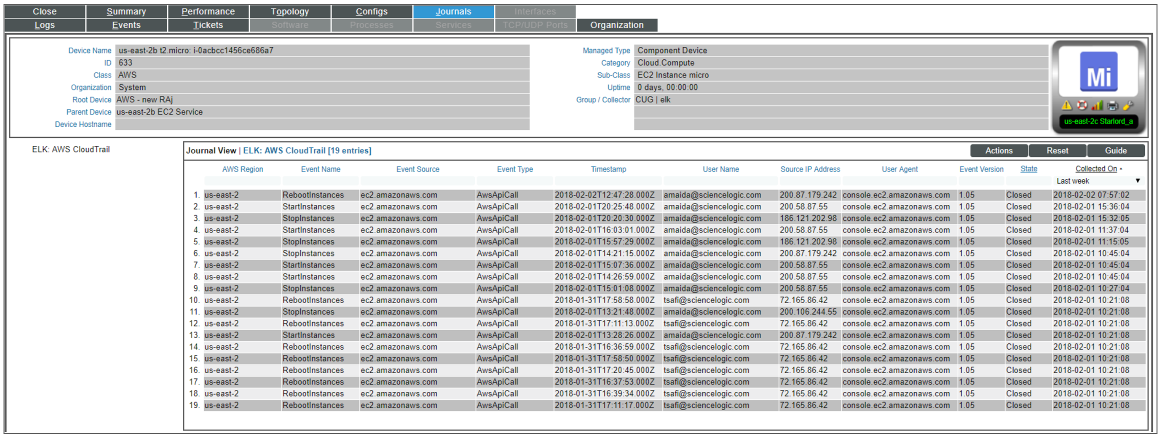
4. Click the **[Actions]** button, and then select *Add Dynamic Application* from the menu.
5. In the **Dynamic Application Alignment** modal page, select *ELK: AWS Alignment* in the ***Dynamic Applications*** field.
6. In the ***Credentials*** field, select the *credential you created for your AWS ELK components*.
7. Click **[Save]**.

NOTE: By default, the "ELK: AWS Alignment" Dynamic Application begins collecting data after 60 minutes. If you want to begin collecting data immediately, click the lightning bolt icon (⚡) for the "ELK: AWS Alignment" Dynamic Application on the **Dynamic Application Collections** page.

When you align the "ELK: AWS Alignment" Dynamic Application to the AWS root device, SL1 then aligns the following Dynamic Application from the *ELK: AWS CloudTrail* PowerPack to the appropriate component devices:

- ELK: AWS CloudTrail
- ELK: AWS CloudTrail EC2 Stats

To view the data collected by the "ELK: AWS CloudTrail" Dynamic Application, navigate to the **Journal View** page (Registry > Devices > Device Manager > bar-graph icon > Journals) and click **ELK: AWS CloudTrail** on the left menu:

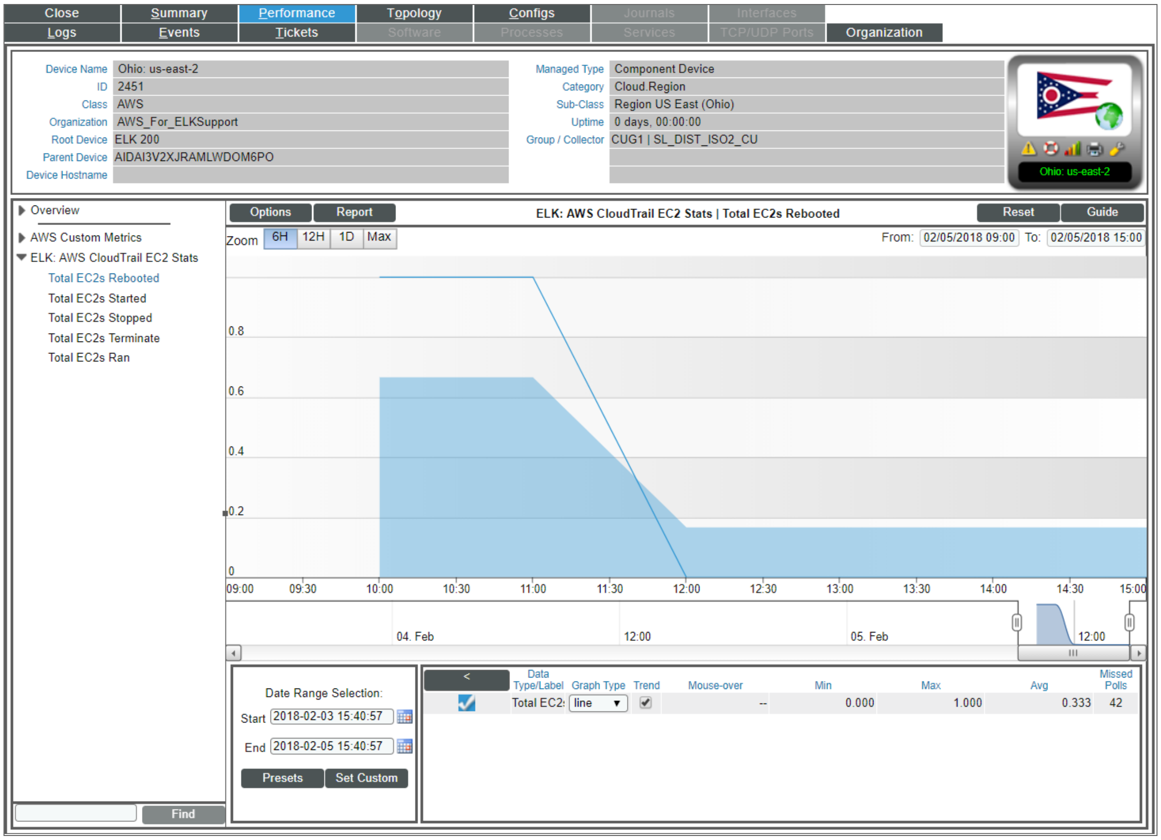


Device Name	us-east-2b t2.micro: i-0acbcc1456ce686a7	Managed Type	Component Device
ID	633	Category	Cloud.Compute
Class	AWS	Sub-Class	EC2 Instance micro
Organization	System	Uptime	0 days, 00:00:00
Root Device	AWS - new RAj	Group / Collector	CUG | elk
Parent Device	us-east-2b EC2 Service		
Device Hostname			

Journal View | ELK: AWS CloudTrail [19 entries]

	AWS Region	Event Name	Event Source	Event Type	Timestamp	User Name	Source IP Address	User Agent	Event Version	State	Collected On
											Last week
1.	us-east-2	RebootInstances	ec2.amazonaws.com	AwsApiCall	2018-02-02T12:47:28.000Z	amaida@sciencelogic.com	200.87.179.242	console.ec2.amazonaws.com	1.05	Closed	2018-02-02 07:57:02
2.	us-east-2	StartInstances	ec2.amazonaws.com	AwsApiCall	2018-02-01T20:25:48.000Z	amaida@sciencelogic.com	200.58.87.55	console.ec2.amazonaws.com	1.05	Closed	2018-02-01 15:36:04
3.	us-east-2	StopInstances	ec2.amazonaws.com	AwsApiCall	2018-02-01T20:20:30.000Z	amaida@sciencelogic.com	186.121.202.98	console.ec2.amazonaws.com	1.05	Closed	2018-02-01 15:32:05
4.	us-east-2	StartInstances	ec2.amazonaws.com	AwsApiCall	2018-02-01T16:03:01.000Z	amaida@sciencelogic.com	200.58.87.55	console.ec2.amazonaws.com	1.05	Closed	2018-02-01 11:37:04
5.	us-east-2	StopInstances	ec2.amazonaws.com	AwsApiCall	2018-02-01T15:57:29.000Z	amaida@sciencelogic.com	186.121.202.98	console.ec2.amazonaws.com	1.05	Closed	2018-02-01 11:15:05
6.	us-east-2	StopInstances	ec2.amazonaws.com	AwsApiCall	2018-02-01T14:21:15.000Z	amaida@sciencelogic.com	200.87.179.242	console.ec2.amazonaws.com	1.05	Closed	2018-02-01 10:45:04
7.	us-east-2	StartInstances	ec2.amazonaws.com	AwsApiCall	2018-02-01T15:07:36.000Z	amaida@sciencelogic.com	200.58.87.55	console.ec2.amazonaws.com	1.05	Closed	2018-02-01 10:45:04
8.	us-east-2	StartInstances	ec2.amazonaws.com	AwsApiCall	2018-02-01T14:26:59.000Z	amaida@sciencelogic.com	200.58.87.55	console.ec2.amazonaws.com	1.05	Closed	2018-02-01 10:45:04
9.	us-east-2	StopInstances	ec2.amazonaws.com	AwsApiCall	2018-02-01T15:01:08.000Z	amaida@sciencelogic.com	200.58.87.55	console.ec2.amazonaws.com	1.05	Closed	2018-02-01 10:27:04
10.	us-east-2	RebootInstances	ec2.amazonaws.com	AwsApiCall	2018-01-31T17:58:58.000Z	tsafi@sciencelogic.com	72.165.86.42	console.ec2.amazonaws.com	1.05	Closed	2018-02-01 10:21:08
11.	us-east-2	StopInstances	ec2.amazonaws.com	AwsApiCall	2018-02-01T13:21:48.000Z	amaida@sciencelogic.com	200.106.244.55	console.ec2.amazonaws.com	1.05	Closed	2018-02-01 10:21:08
12.	us-east-2	RebootInstances	ec2.amazonaws.com	AwsApiCall	2018-01-31T17:11:13.000Z	tsafi@sciencelogic.com	72.165.86.42	console.ec2.amazonaws.com	1.05	Closed	2018-02-01 10:21:08
13.	us-east-2	StartInstances	ec2.amazonaws.com	AwsApiCall	2018-02-01T13:28:26.000Z	amaida@sciencelogic.com	200.87.179.242	console.ec2.amazonaws.com	1.05	Closed	2018-02-01 10:21:08
14.	us-east-2	RebootInstances	ec2.amazonaws.com	AwsApiCall	2018-01-31T16:36:59.000Z	tsafi@sciencelogic.com	72.165.86.42	console.ec2.amazonaws.com	1.05	Closed	2018-02-01 10:21:08
15.	us-east-2	RebootInstances	ec2.amazonaws.com	AwsApiCall	2018-01-31T17:58:50.000Z	tsafi@sciencelogic.com	72.165.86.42	console.ec2.amazonaws.com	1.05	Closed	2018-02-01 10:21:08
16.	us-east-2	RebootInstances	ec2.amazonaws.com	AwsApiCall	2018-01-31T17:20:45.000Z	tsafi@sciencelogic.com	72.165.86.42	console.ec2.amazonaws.com	1.05	Closed	2018-02-01 10:21:08
17.	us-east-2	RebootInstances	ec2.amazonaws.com	AwsApiCall	2018-01-31T16:37:53.000Z	tsafi@sciencelogic.com	72.165.86.42	console.ec2.amazonaws.com	1.05	Closed	2018-02-01 10:21:08
18.	us-east-2	RebootInstances	ec2.amazonaws.com	AwsApiCall	2018-01-31T16:39:34.000Z	tsafi@sciencelogic.com	72.165.86.42	console.ec2.amazonaws.com	1.05	Closed	2018-02-01 10:21:08
19.	us-east-2	RebootInstances	ec2.amazonaws.com	AwsApiCall	2018-01-31T17:11:17.000Z	tsafi@sciencelogic.com	72.165.86.42	console.ec2.amazonaws.com	1.05	Closed	2018-02-01 10:21:08

To view the data collected by the "ELK: AWS CloudTrail EC2 Stats" Dynamic Application, navigate to the **Device Performance** page (Registry > Devices > Device Manager > bar-graph icon > Performance) and click **ELK: AWS CloudTrail** on the left menu:



Device Name	Ohio: us-east-2
ID	2451
Class	AWS
Organization	AWS_For_ELKSupport
Root Device	ELK 200
Parent Device	AIDAI3V2XJRAMLWDOM6PO
Device Hostname	
Managed Type	Component Device
Category	Cloud.Region
Sub-Class	Region US East (Ohio)
Uptime	0 days, 00:00:00
Group / Collector	CUG1 | SL_DIST_ISO2_CU

ELK: AWS CloudTrail EC2 Stats | Total EC2s Rebooted

From: 02/05/2018 09:00 To: 02/05/2018 15:00

Date Range Selection:

Start 2018-02-03 15:40:57

End 2018-02-05 15:40:57

<	Data Type/Label	Graph Type	Trend	Mouse-over	Min	Max	Avg	Missed Polls
☑	Total EC2:	line	☑	--	0.000	1.000	0.333	42

Chapter 35

ELK: Azure Activity Log

Overview

The following sections describe how to configure Azure component devices in ELK stacks for monitoring by SL1 using the *ELK: Azure Activity Log* PowerPack:

NOTE: For more information about the *ELK: Azure Activity Log* PowerPack, see the ***Monitoring Microsoft Azure ELK Stacks*** manual.

Prerequisites for Monitoring Azure ELK Stacks

To configure SL1 to monitor Azure component devices in ELK stacks using the *ELK: Azure Activity Log* PowerPack, you must first:

1. Install the *Microsoft: Azure*PowerPack.
2. Create a virtual device in SL1 to represent your Azure service.
3. Discover Azure component devices by manually aligning the "Microsoft: Azure Account Discovery" Dynamic Application to the virtual device.
4. Ensure that your Azure Activity Log is properly configured for all read/write events.

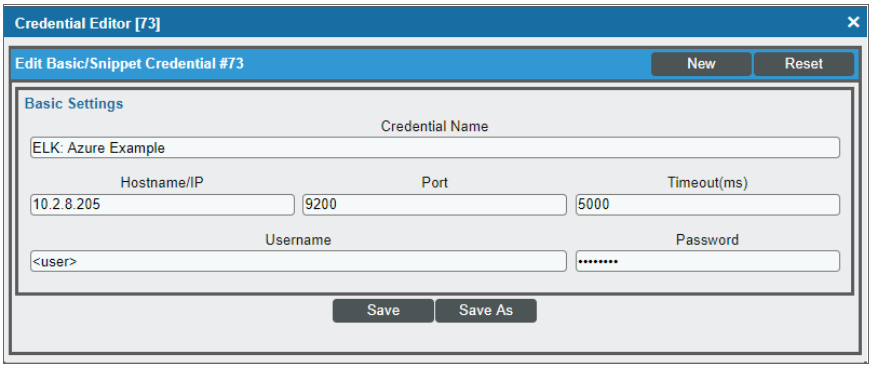
NOTE: For more information about the *Microsoft: Azure* PowerPack, including how to install the PowerPack and discover Azure devices, see the ***Monitoring Microsoft Azure*** manual.

Creating an Azure ELK Credential

To use the Dynamic Applications in the *ELK: Azure Activity Log* PowerPack, you must first define a credential in SL1. This credential enables the Dynamic Applications in the *ELK: Azure Activity Log* PowerPack to monitor your Azure component devices in ELK stacks. The PowerPack includes a sample Basic/Snippet credential (**ELK: Azure Example**) that you can use as a template.

To define an Azure ELK credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the wrench icon (🔧) for the **ELK: Azure Example** credential. The **Credential Editor** modal page appears:



Credential Editor [73]

Edit Basic/Snippet Credential #73

Basic Settings

Credential Name: ELK: Azure Example

Hostname/IP: 10.2.8.205

Port: 9200

Timeout(ms): 5000

Username: <user>

Password: ••••••••

3. Enter values in the following fields:

- ***Credential Name***. Type a new name for your Azure ELK credential.
- ***Hostname/IP***. Type the IP address or hostname for the Logstash server that collects data for the Azure components in your ELK stack.
- ***Port***. Type "9200".
- ***Timeout(ms)***. Type a timeout value, in milliseconds.
- ***Username***. Type the username of a user with access to the Azure Logstash server.
- ***Password***. Type the password associated with the ***Username***.

NOTE: If the Logstash server that collects data for your Azure components is not password-protected, you must still enter values in the ***Username*** and ***Password*** fields, as they are required fields. However, in this scenario, the values you enter do not matter.

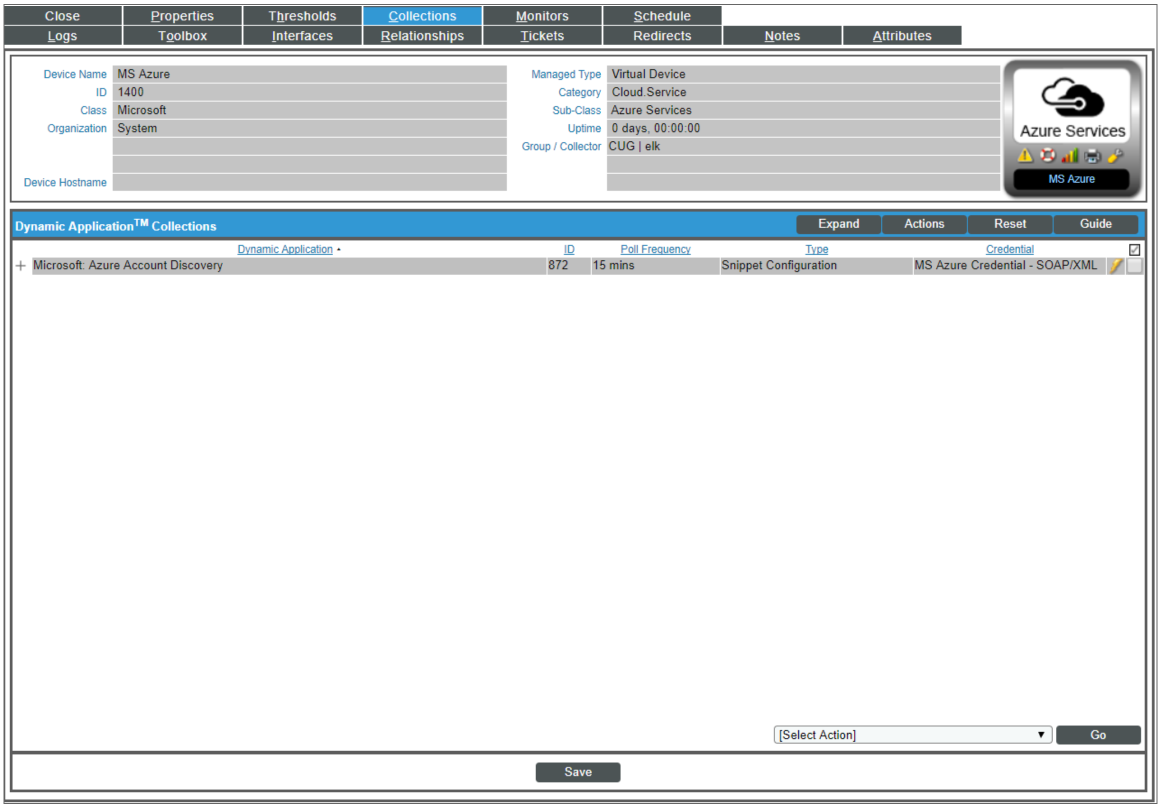
4. Click the **[Save As]** button, and then click **[OK]**.

Aligning the Azure ELK Dynamic Applications

To monitor your Azure component devices in ELK stacks, you must manually align the "ELK: Azure Alignment" Dynamic Application with the Azure virtual device. When you do so, the remaining Dynamic Applications from the *ELK: Azure Activity Log* PowerPack automatically align to the appropriate Azure component devices.

To manually align the "ELK: Azure Alignment" Dynamic Application to your virtual device:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Locate your Azure virtual device and click its wrench icon (🔧).
3. In the **Device Administration** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.



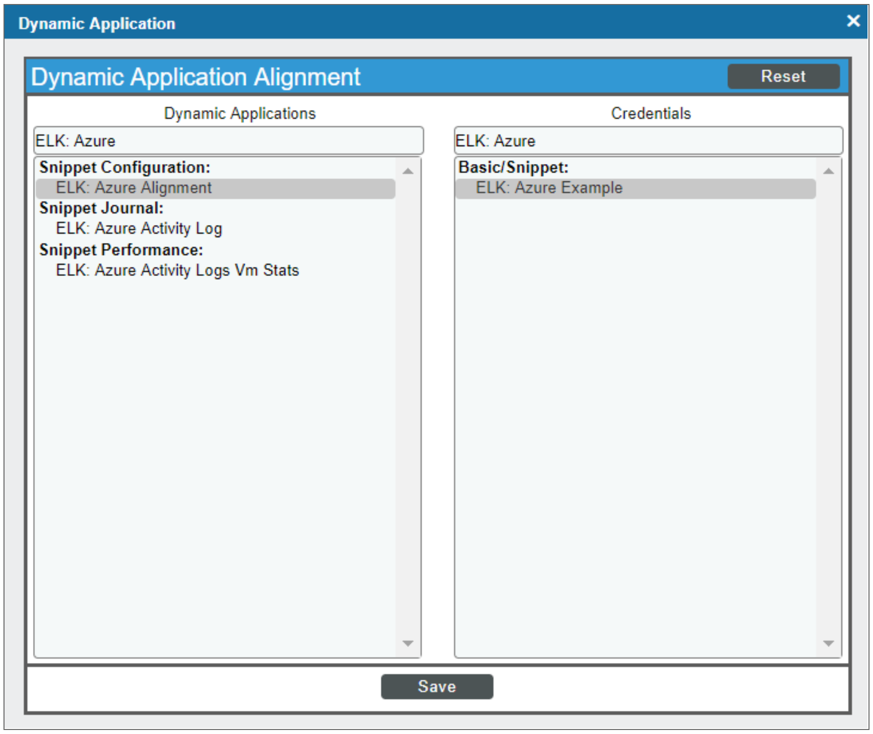
Device Name	MS Azure	Managed Type	Virtual Device
ID	1400	Category	Cloud.Service
Class	Microsoft	Sub-Class	Azure Services
Organization	System	Uptime	0 days, 00:00:00
		Group / Collector	CUG | elk
Device Hostname			

Dynamic Application^{TM} Collections

Dynamic Application •	ID	Poll Frequency	Type	Credential
+ Microsoft: Azure Account Discovery	872	15 mins	Snippet Configuration	MS Azure Credential - SOAP/XML

4. Click the **[Actions]** button, and then select *Add Dynamic Application* from the menu.
5. In the **Dynamic Application Alignment** modal page, select *ELK: Azure Alignment* in the ***Dynamic Applications*** field.

6. In the ***Credentials*** field, select the *credential you created for your Azure ELK components*.



ELK: Azure

Snippet Configuration:
ELK: Azure Alignment
Snippet Journal:
ELK: Azure Activity Log
Snippet Performance:
ELK: Azure Activity Logs Vm Stats

ELK: Azure

Basic/Snippet:
ELK: Azure Example

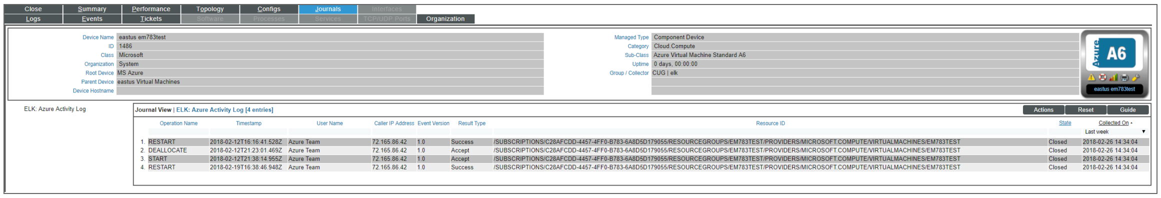
7. Click **[Save]**.

NOTE: By default, the "ELK: Azure Alignment" Dynamic Application begins collecting data after 60 minutes. If you want to begin collecting data immediately, click the lightning bolt icon (⚡) for the "ELK: Azure Alignment" Dynamic Application on the **Dynamic Application Collections** page.

When you align the "ELK: Azure Alignment" Dynamic Application to the Azure root device, SL1 then aligns the following Dynamic Application from the *ELK: Azure Activity Log* PowerPack to the appropriate component devices:

- ELK: Azure Activity Log
- ELK: Azure Activity Logs Vm Stats

To view the data collected by the "ELK: Azure Activity Log" Dynamic Application, navigate to the **Journal View** page (Registry > Devices > Device Manager > bar-graph icon > Journals) and click **ELK: Azure Activity Log** on the left menu:



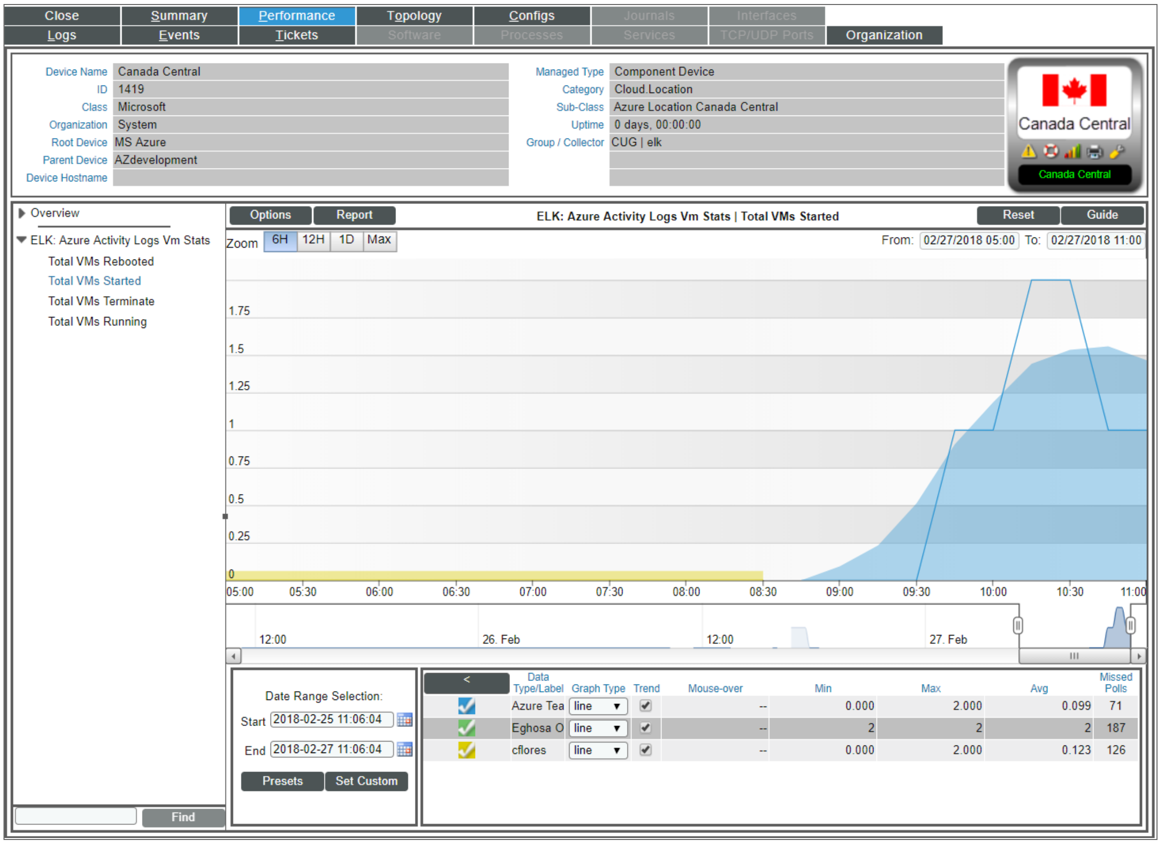
Device Name	eastus em783test	Managed Type	Component Device
ID	1486	Category	Cloud.Compute
Class	Microsoft	Sub-Class	Azure Virtual Machine Standard A6
Organization	System	Uptime	0 days, 00:00:00
Root Device	MS Azure	Group / Collector	CUG | elk
Parent Device	eastus Virtual Machines		
Device Hostname			

ELK: Azure Activity Log

Journal View | ELK: Azure Activity Log [4 entries]

	Operation Name	Timestamp	User Name	Caller IP Address	Event Version	Result Type	Resource ID	State	Collected On
1.	RESTART	2018-02-12T16:16:41.528Z	Azure Team	72.165.86.42	1.0	Success	/SUBSCRIPTIONS/C28AFCDD-4457-4FF0-B783-6A8D5D179055/RESOURCEGROUPS/EM783TEST/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/EM783TEST	Closed	2018-02-26 14:34:04
2.	DEALLOCATE	2018-02-12T21:23:01.469Z	Azure Team	72.165.86.42	1.0	Accept	/SUBSCRIPTIONS/C28AFCDD-4457-4FF0-B783-6A8D5D179055/RESOURCEGROUPS/EM783TEST/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/EM783TEST	Closed	2018-02-26 14:34:04
3.	START	2018-02-12T21:38:14.955Z	Azure Team	72.165.86.42	1.0	Accept	/SUBSCRIPTIONS/C28AFCDD-4457-4FF0-B783-6A8D5D179055/RESOURCEGROUPS/EM783TEST/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/EM783TEST	Closed	2018-02-26 14:34:04
4.	RESTART	2018-02-19T16:38:46.948Z	Azure Team	72.165.86.42	1.0	Success	/SUBSCRIPTIONS/C28AFCDD-4457-4FF0-B783-6A8D5D179055/RESOURCEGROUPS/EM783TEST/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/EM783TEST	Closed	2018-02-26 14:34:04

To view the data collected by the "ELK: Azure Activity Logs Vm Stats" Dynamic Application, navigate to the **Device Performance** page (Registry > Devices > Device Manager > bar-graph icon > Performance) and click **ELK: Azure Activity Logs Vm Stats** on the left menu:



Device Name	Canada Central	Managed Type	Component Device
ID	1419	Category	Cloud.Location
Class	Microsoft	Sub-Class	Azure Location Canada Central
Organization	System	Uptime	0 days, 00:00:00
Root Device	MS Azure	Group / Collector	CUG | elk
Parent Device	AZdevelopment		
Device Hostname			

ELK: Azure Activity Logs Vm Stats | Total VMs Started

From: 02/27/2018 05:00 To: 02/27/2018 11:00

Date Range Selection:

Start 2018-02-25 11:06:04

End 2018-02-27 11:06:04

	Data Type/Label	Graph Type	Trend	Mouse-over	Min	Max	Avg	Missed Polls
☑	Azure Tea	line	☑	--	0.000	2.000	0.099	71
☑	Eghosa O	line	☑	--	2	2	2	187
☑	cflores	line	☑	--	0.000	2.000	0.123	126

Chapter 36

EMC: VMAX

Overview

The following sections describe how to configure and discover Dell EMC VMAX systems for monitoring by SL1 using the *EMC: VMAX* PowerPack:

NOTE: For more information about the *EMC: VMAX* PowerPack, see the ***Monitoring Dell EMC VMAX*** manual.

Prerequisites for Monitoring Dell EMC VMAX

Before you can monitor Dell EMC VMAX systems using the *EMC: VMAX* PowerPack, you must have the following information about an EMC SMI-S Provider that has already been properly installed and configured:

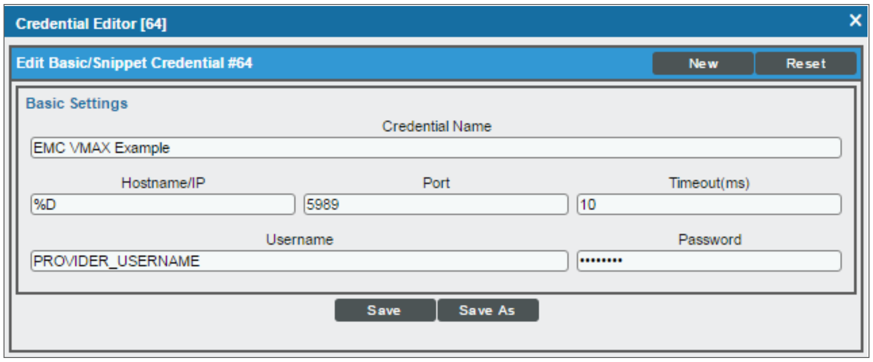
- Username and password for a user with access to the SMI-S Provider
- IP address and port for the SMI-S Provider

Creating a Credential for Dell EMC VMAX

To configure SL1 to monitor Dell EMC VMAX storage systems, you must first create a Basic/Snippet credential. This credential allows the Dynamic Applications in the *EMC: VMAX* PowerPack) to connect with a VMAX SMI-S Provider. An example Basic/Snippet credential that you can edit for your own use is included in the *EMC: VMAX* PowerPack.

To create a Basic/Snippet credential to access a VMAX SMI-S Provider:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **EMC VMAX Example** credential, then click its wrench icon (🔧). The **Edit Basic/Snippet Credential** modal page appears.
3. Enter values in the following fields:


Credential Editor [64]

Edit Basic/Snippet Credential #64

Basic Settings

Credential Name: EMC VMAX Example

Hostname/IP: %D

Port: 5989

Timeout(ms): 10

Username: PROVIDER_USERNAME

Password: ••••••••

- ***Credential Name***. Enter a new name for the Dell EMC VMAX credential.
- ***Hostname/IP***. Enter "%D".
- ***Port***. Enter "5988" for an HTTP connection or "5989" for an HTTPS connection.
- ***Timeout***. Enter "10".
- ***Username***. Enter the username for a user with access to the VMAX SMI-S Provider.
- ***Password***. Enter the password for the user you specified in the ***Username*** field.

4. Click the **[Save As]** button.
5. When the confirmation message appears, click **[OK]**.

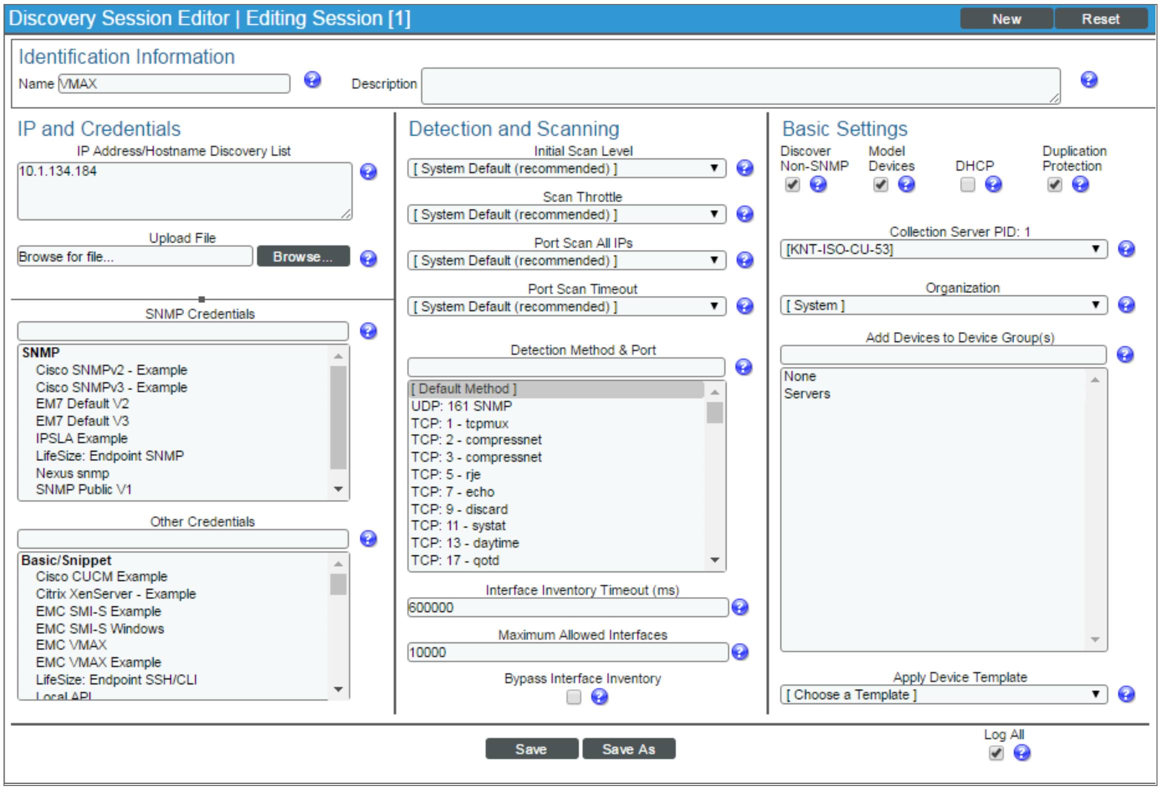
Discovering Dell EMC VMAX Devices

To model and monitor your Dell EMC VMAX system, you must run a discovery session to discover the SMI-S Provider that SL1 will use as the root device for monitoring the VMAX system.

The discovery session will discover the SMI-S Provider as a pingable device using ***the Basic/Snippet credential that you created***. You must then manually align the "EMC: VMAX Array Discovery" and "EMC: VMAX Statistics Cache" Dynamic Applications to the SMI-S Provider root device to enable SL1 to discover, model, and monitor the remaining component devices in your VMAX system.

To discover your VMAX storage system in SL1:

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



Discovery Session Editor | Editing Session [1]

Identification Information

Name: VMAX

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.1.134.184

Upload File: Browse for file...

SNMP Credentials:

SNMP
- Cisco SNMPv2 - Example
- Cisco SNMPv3 - Example
- EM7 Default V2
- EM7 Default V3
- IPSLA Example
- LifeSize: Endpoint SNMP
- Nexus snmp
- SNMP Public V1

Other Credentials:

Basic/Snippet
- Cisco CUCM Example
- Citrix XenServer - Example
- EMC SMI-S Example
- EMC SMI-S Windows
- EMC VMAX
- EMC VMAX Example
- LifeSize: Endpoint SSH/CLI
- Local API

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: 1: [KNT-ISO-CU-53]

Organization: [System]

Add Devices to Device Group(s):
- None
- Servers

Apply Device Template: [Choose a Template]

Log All ☑

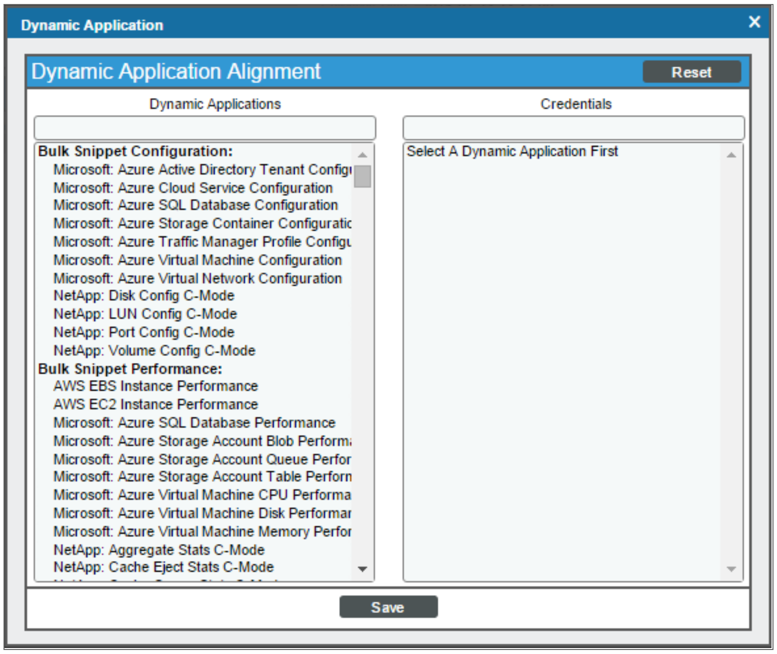
- ***IP Address Discovery List***. Enter the IP address for the VMAX SMI-S Provider.
- ***Other Credentials***. Select the Basic/Snippet credential you created for the VMAX SMI-S Provider.
- ***Discover Non-SNMP***. Select this checkbox.
- ***Model Devices***. Select this checkbox.

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 **[Save]** to save the discovery session and then close the **Discovery Session Editor** window.
6. The discovery session you created will display at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon (⚡) to run the discovery session.

7. The **Discovery Session** window will appear. When the root device is discovered, click its device icon ( ). The **Device Properties** page appears.

8. 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
Bulk Snippet Configuration:
Microsoft: Azure Active Directory Tenant Config
Microsoft: Azure Cloud Service Configuration
Microsoft: Azure SQL Database Configuration
Microsoft: Azure Storage Container Configuratic
Microsoft: Azure Traffic Manager Profile Configu
Microsoft: Azure Virtual Machine Configuration
Microsoft: Azure Virtual Network Configuration
NetApp: Disk Config C-Mode
NetApp: LUN Config C-Mode
NetApp: Port Config C-Mode
NetApp: Volume Config C-Mode
Bulk Snippet Performance:
AWS EBS Instance Performance
AWS EC2 Instance Performance
Microsoft: Azure SQL Database Performance
Microsoft: Azure Storage Account Blob Perform
Microsoft: Azure Storage Account Queue Perfor
Microsoft: Azure Storage Account Table Perforn
Microsoft: Azure Virtual Machine CPU Performa
Microsoft: Azure Virtual Machine Disk Performar
Microsoft: Azure Virtual Machine Memory Perfor
NetApp: Aggregate Stats C-Mode
NetApp: Cache Eject Stats C-Mode
Select A Dynamic Application First
Save

10. In the ***Dynamic Applications*** field, select *EMC: VMAX Array Discovery*.

11. In the ***Credentials*** field, select the Basic/Snippet credential you configured for the VMAX SMI-S Provider.

12. Click **[Save]**. A few minutes after aligning the Dynamic Application, SL1 will discover and model your VMAX system and automatically align other Dynamic Applications to the devices in the system.

13. Repeat steps 8-12 to manually align the "EMC: VMAX Statistics Cache" Dynamic Application to the SMI-S Provider.

Chapter 37

EMC: VNX

Overview

The following sections describe how to configure and discover Dell EMC VNX systems for monitoring by SL1 using the *EMC: VNX* PowerPack:

NOTE: For more information about the *EMC: VNX* PowerPack, see the ***Monitoring Dell EMC VNX*** manual.

Prerequisites for Monitoring Dell EMC VNX

Before you can monitor Dell EMC VNX storage systems using the *EMC: VNX* PowerPack, you must have the following information about an EMC SMI-S Provider that has already been properly installed and configured:

- Username and password for a user with access to the SMI-S Provider
- IP address and port for the SMI-S Provider

Additionally, statistics logging must be enabled on each Dell EMC VNX storage system that will be monitored. To do so:

1. Log in to Unisphere.

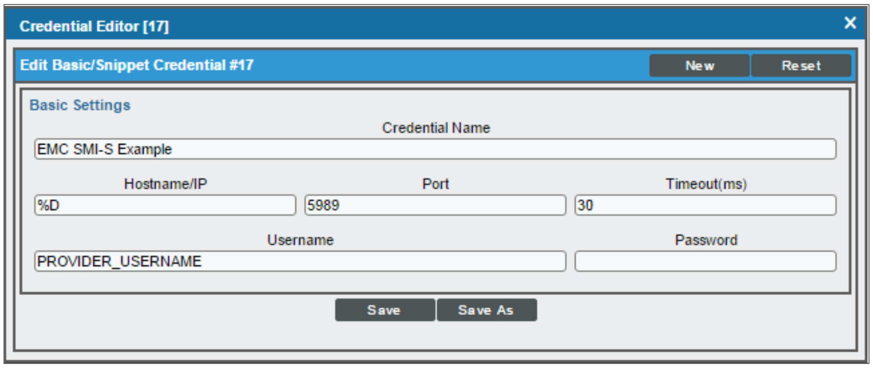
2. Select a Dell EMC VNX storage array from the list, and then click the **[System]** tab.
3. In the **System Management** menu, click **System Properties**.
4. On the **Storage System Properties** dialog box, click the **[General]** tab.
5. Select the *Statistics Logging* checkbox, and then click **[OK]**.

Creating a Credential for Dell EMC VNX

To configure SL1 to monitor Dell EMC VNX systems, you must first create a Basic/Snippet credential. This credential allows the Dynamic Applications in the *EMC: VNX* PowerPack to connect with an EMC SMI-S Provider. An example Basic/Snippet credential that you can edit for your own use is included in the *EMC: VNX* PowerPack.

To create a Basic/Snippet credential to access an EMC SMI-S Provider:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **EMC SMI-S Example** credential, and then click its wrench icon (🔧). The **Edit Basic/Snippet Credential** modal page appears.
3. Enter values in the following fields:



Credential Editor [17]

Edit Basic/Snippet Credential #17

Basic Settings

Credential Name: EMC SMI-S Example		
Hostname/IP: %D	Port: 5989	Timeout(ms): 30
Username: PROVIDER_USERNAME		Password:

- ***Credential Name***. Type a new name for the Dell EMC VNX credential.
- ***Hostname/IP***. Type the IP address of the SMI-S Provider.
- ***Port***. Type "5988" for an HTTP connection or "5989" for an HTTPS connection.
- ***Timeout***. Type "30".
- ***Username***. Type the username for a user with access to the SMI-S Provider.
- ***Password***. Type the password for the SMI-S Provider account username.

4. Click the **[Save As]** button.
5. When the confirmation message appears, click **[OK]**.

> **NOTE:** To monitor VNX arrays and file systems that have different login credentials, create a separate Basic/Snippet credential for each.

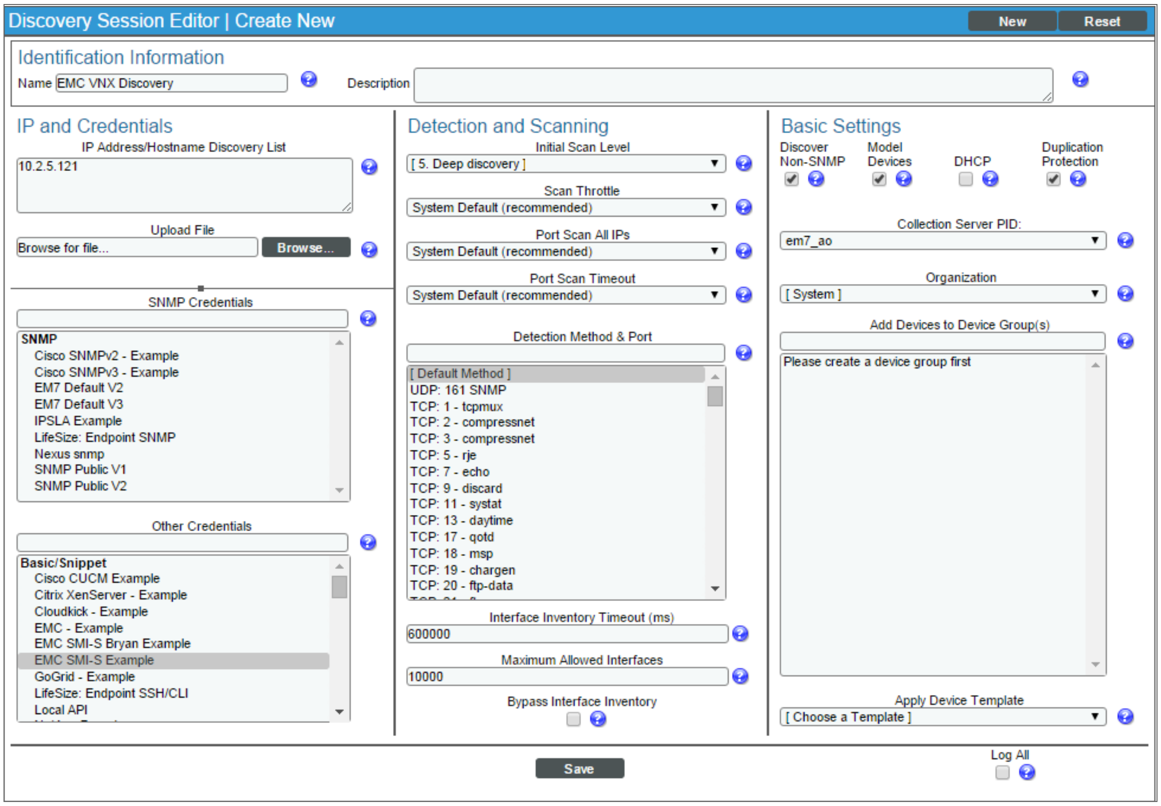
Discovering Dell EMC VNX Devices

To model and monitor your Dell EMC VNX system, you must run a discovery session to discover the EMC SMI-S Provider that SL1 will use as the root device for monitoring the VNX system.

The discovery session will discover the SMI-S Provider as a pingable device using ***the Basic/Snippet credential that you created***. Several minutes after the discovery session has completed, the Dynamic Applications in the *EMC: VNX* PowerPack should automatically align to the SMI-S Provider root device to discover, model, and monitor the remaining component devices in your VNX system.

To discover the SMI-S Provider for the Dell EMC VNX system 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:



Discovery Session Editor | Create New

Identification Information

Name: EMC VNX Discovery
Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.2.5.121

Upload File: Browse for file...

SNMP Credentials:
SNMP
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:
Basic/Snippet
Cisco CUCM Example
Citrix XenServer - Example
Cloudkick - Example
EMC - Example
EMC SMI-S Bryan Example
EMC SMI-S Example
GoGrid - Example
LifeSize: Endpoint SSH/CLI
Local API

Detection and Scanning

Initial Scan Level: [5. Deep discovery]
Scan Throttle: System Default (recommended)
Port Scan All IPs: System Default (recommended)
Port Scan Timeout: System Default (recommended)

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

Interface Inventory Timeout (ms): 600000
Maximum Allowed Interfaces: 10000
Bypass Interface Inventory: ☐

Basic Settings

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

Collection Server PID: em7_ao
Organization: [System]
Add Devices to Device Group(s): Please create a device group first
Apply Device Template: [Choose a Template]

Log All: ☐

- ***IP Address Discovery List***. Enter the IP address for the SMI-S Provider.

   - ***SNMP Credentials***. Do not select any credentials in this field.
   - ***Other Credentials***. Select the Basic/Snippet credential you created for the SMI-S Provider.
   - ***Initial Scan Level***. Select 5. *Deep Discovery*. The *EMC: VNX* PowerPack includes non-SNMP device classes that are aligned only during deep discovery. If you do not select 5. *Deep Discovery* in this field, the SMI-S Provider will be discovered and assigned a device class for a pingable device.
   - ***Discover Non-SNMP***. You must select this checkbox.
   - ***Model Devices***. You must 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 will display at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon (⚡) to run the discovery session.
7. The **Discovery Session** window will appear. When the SMI-S Provider is discovered, click its device icon (🖥) to view the **Device Properties** page for the SMI-S Provider.

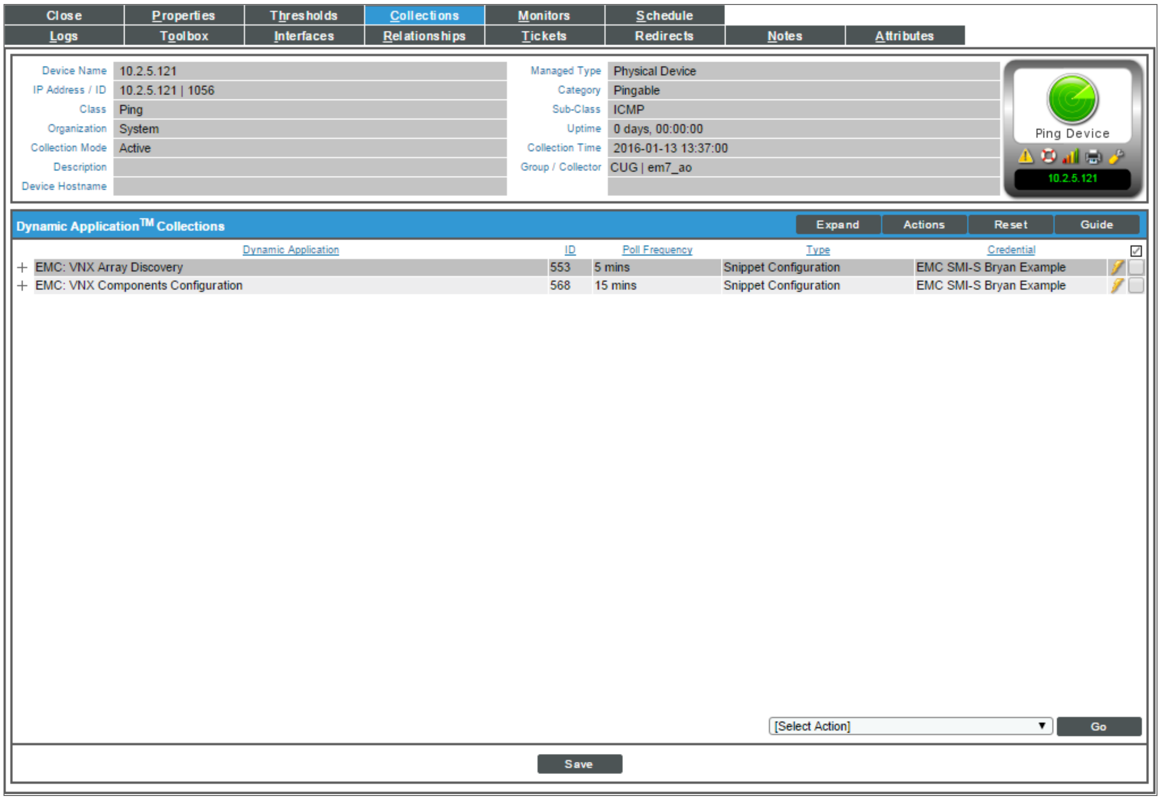
NOTE: To monitor VNX storage arrays and file systems that have different IP addresses and/or credentials, create and run a separate discovery session for each.

Manually Aligning Dynamic Applications

NOTE: It can take several minutes after discovery for Dynamic Applications to display on the **Dynamic Application Collections** page. If the listed Dynamic Applications do not display on this page, try clicking the **[Reset]** button.

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. From the **Device Properties** page (Registry > Devices > wrench icon(🔧)) for the SMI-S Provider, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.



Device Name	10.2.5.121	Managed Type	Physical Device
IP Address / ID	10.2.5.121 | 1056	Category	Pingable
Class	Ping	Sub-Class	ICMP
Organization	System	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2016-01-13 13:37:00
Description		Group / Collector	CUG | em7_ao
Device Hostname			

Dynamic Application™ Collections

Dynamic Application	ID	Poll Frequency	Type	Credential
+ EMC: VNX Array Discovery	553	5 mins	Snippet Configuration	EMC SMI-S Bryan Example
+ EMC: VNX Components Configuration	568	15 mins	Snippet Configuration	EMC SMI-S Bryan Example

2. If the SMI-S Provider that you are monitoring is a storage area network (SAN) device, then the following Dynamic Applications should display in the list of aligned Dynamic Applications:

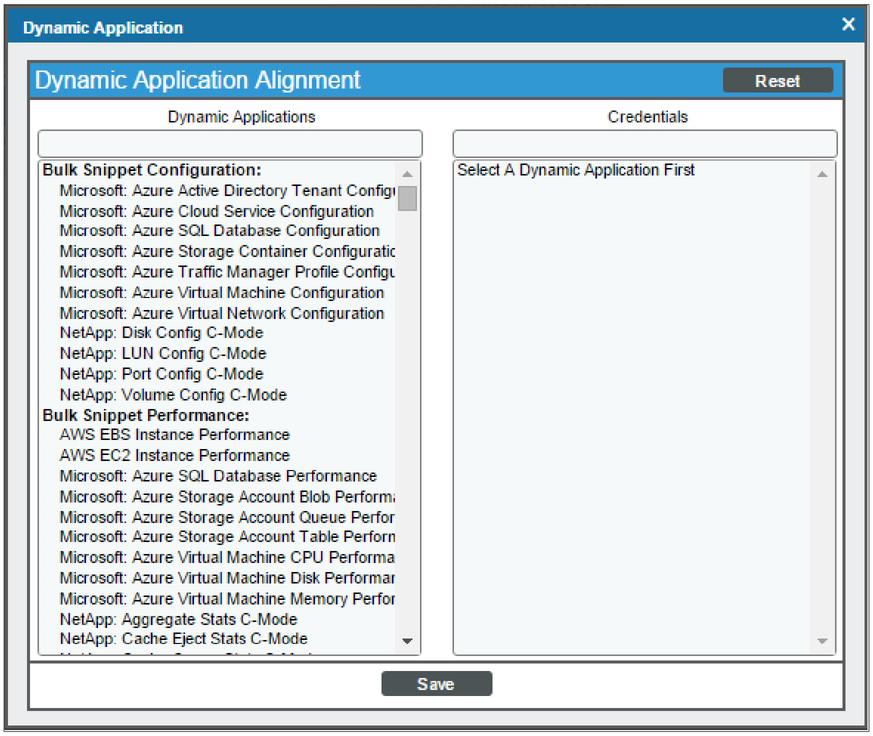
   - EMC: VNX Array Discovery
   - EMC: VNX Components Configuration
   - EMC: VNX LUN Cache

   If the SMI-S Provider that you are monitoring is a network-attached storage (NAS) device, then the following Dynamic Application should display in the list of aligned Dynamic Applications:

   - EMC: VNX File Discovery

If the listed Dynamic Applications have not been automatically aligned, you can align them manually. To do so, perform the following steps:

1. For the "EMC: VNX Array Discovery" Dynamic Application, click the **[Action]** button on the **Dynamic Application Collections** page of the SMI-S Provider device and then select *Add Dynamic Application* from the menu. The **Dynamic Application Alignment** page appears.


Dynamic Application
×
Dynamic Application Alignment
Reset
Dynamic Applications
Credentials
Bulk Snippet Configuration:
Microsoft: Azure Active Directory Tenant Config
Microsoft: Azure Cloud Service Configuration
Microsoft: Azure SQL Database Configuration
Microsoft: Azure Storage Container Configuratic
Microsoft: Azure Traffic Manager Profile Configu
Microsoft: Azure Virtual Machine Configuration
Microsoft: Azure Virtual Network Configuration
NetApp: Disk Config C-Mode
NetApp: LUN Config C-Mode
NetApp: Port Config C-Mode
NetApp: Volume Config C-Mode
Bulk Snippet Performance:
AWS EBS Instance Performance
AWS EC2 Instance Performance
Microsoft: Azure SQL Database Performance
Microsoft: Azure Storage Account Blob Perform
Microsoft: Azure Storage Account Queue Perfor
Microsoft: Azure Storage Account Table Perforn
Microsoft: Azure Virtual Machine CPU Performa
Microsoft: Azure Virtual Machine Disk Performar
Microsoft: Azure Virtual Machine Memory Perfor
NetApp: Aggregate Stats C-Mode
NetApp: Cache Eject Stats C-Mode
Select A Dynamic Application First
Save

2. In the ***Dynamic Applications*** field, select *EMC: VNX Array Discovery*.
3. In the ***Credentials*** field, select the Basic/Snippet credential you configured for the SMI-S Provider.
4. Click the **[Save]** button.
5. Repeat steps 1–4 for the other Dynamic Applications, as needed.
6. After aligning the Dynamic Applications, click the **[Reset]** button and then click the plus icon (+) for the Dynamic Applications. If collection for the Dynamic Applications was successful, the graph icons (📊) for the Dynamic Applications are enabled.
7. Click the graph icon (📊) for the "EMC: VNX Components Configuration" Dynamic Application to view the collected data. The **Configuration Report** page will display the number of components of each type and the total number of components managed by the device.

Relationships with Other Types of Component Devices

SL1 can automatically build relationships between Dell EMC VNX component devices and other associated devices. If you discover a vCenter device using the Dynamic Applications in the *VMware: vSphere Base Pack* PowerPack and/or a UCS device using the Dynamic Applications in the *Cisco: UCS* PowerPack, SL1 will automatically create relationships between the following types of component devices, where appropriate:

- Dell EMC VNX LUNs and VMware Datastores
- Dell EMC VNX LUNs and UCS Service Profiles

Chapter 38

F5 BIG-IP

Overview

The following sections describe how to configure and discover F5 BIG-IP Local Traffic Manager (LTM) services for monitoring by SL1 using the *F5 BIG-IP* PowerPack:

NOTE: For more information about the *F5 BIG-IP* PowerPack, see the ***Monitoring F5 BIG-IP*** manual.

Prerequisites for Monitoring F5 BIG-IP

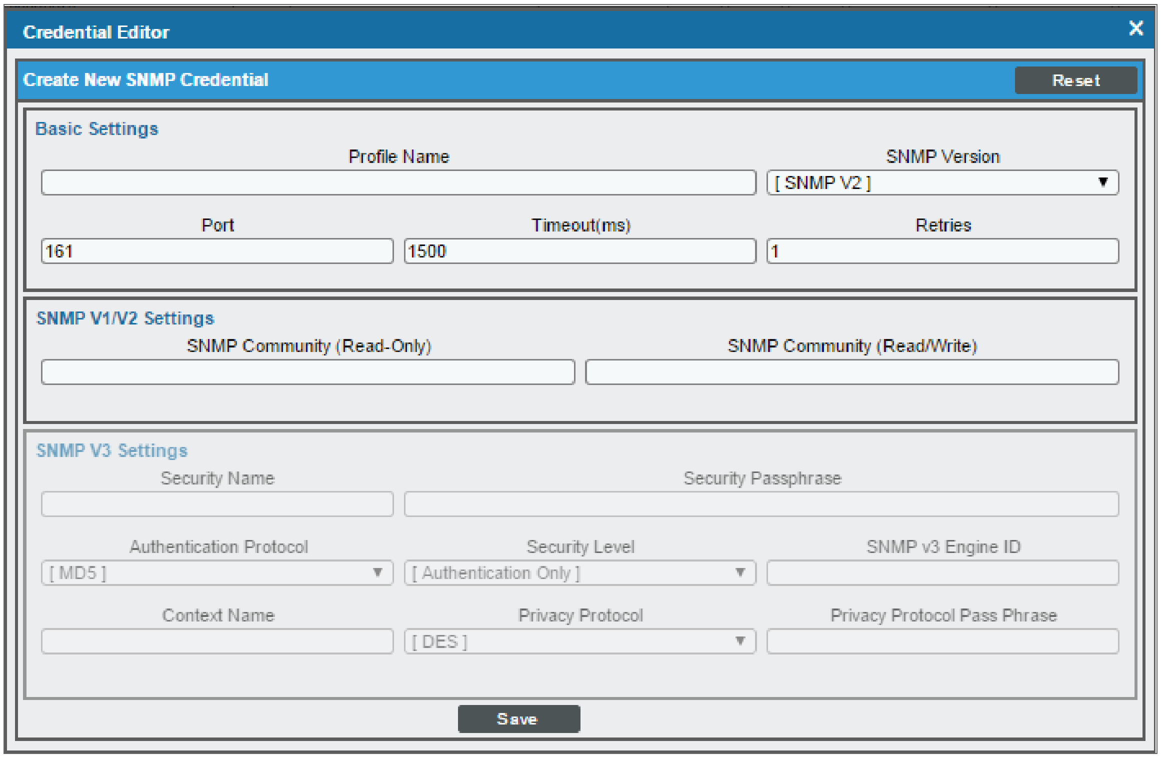
Before you can monitor F5 BIG-IP services using the *F5 BIG-IP* PowerPack, you must ensure that SL1 can communicate with BIG-IP using SNMP and you must know the SNMP community string for the BIG-IP system. SL1 can then use the data collected from BIG-IP to create device records for all components managed by BIG-IP.

Creating an SNMP Credential for F5 BIG-IP

To use the Dynamic Applications in the *F5 BIG-IP* PowerPack, you must first define an SNMP credential in SL1. This credential allows SL1 to communicate with the BIG-IP system.

To configure an SNMP credential for F5 BIG-IP:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the **[Actions]** button.
3. In the drop-down list that appears, select *Create SNMP Credential*. The **Credential Editor** page appears:



Credential Editor

Create New SNMP Credential

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:

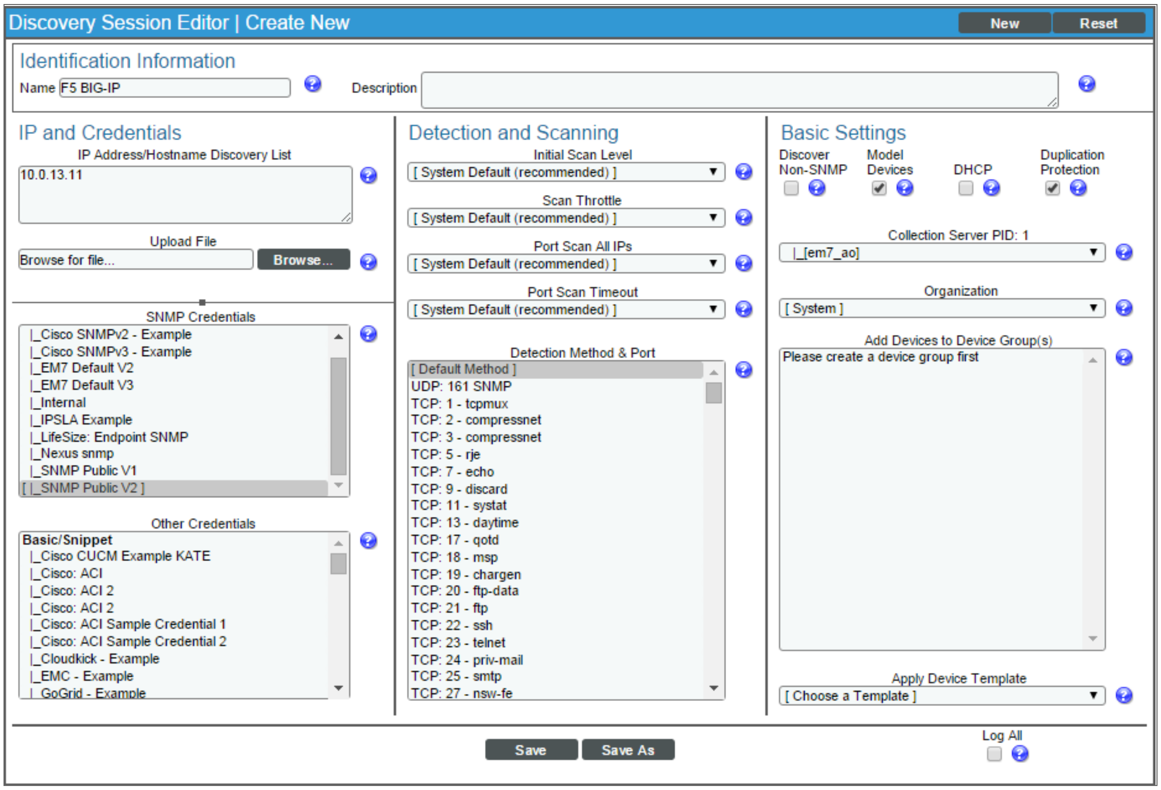
4. In the ***SNMP Version*** field, select *SNMP V2*.
5. In the ***Profile Name*** field, enter a name for the credential.
6. In the ***SNMP Community (Read Only)*** field, enter the community string for the BIG-IP system.
7. Optionally, supply values in the other fields in this page. In most cases, you can use the default values for the other fields.
8. Click the **[Save]** button.

Discovering an F5 BIG-IP System

After you have created an SNMP credential for the F5 BIG-IP system that you want to monitor, you can create and run a discovery session that will discover the BIG-IP system and automatically align Dynamic Applications with the BIG-IP system.

To do so, perform the following steps:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. Click the **[Create]** button to create a new discovery session. The **Discovery Session Editor** window appears:



Discovery Session Editor | Create New

Identification Information

Name: F5 BIG-IP

IP Address/Hostname Discovery List: 10.0.13.11

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]

SNMP Credentials: [|_SNMP Public V2]

Discover Non-SNMP: □

Model Devices: ☑

DHCP: □

Duplication Protection: ☑

Collection Server PID: 1: |_[em7_ao]

Organization: [System]

Add Devices to Device Group(s): Please create a device group first

Apply Device Template: [Choose a Template]

Log All: □

3. Enter values in the following fields:

   - ***IP Address Discovery List***. Enter the IP address for the BIG-IP system.
   - ***SNMP Credentials***. Select the SNMP Credential for the BIG-IP system.

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 will appear 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 BIG-IP system is discovered, you can click its device icon () to view the system device's properties.

Aligning F5 BIG-IP Dynamic Applications

The Dynamic Applications in the *F5 BIG-IP* PowerPack are divided into four types:

- ***Count***. These Dynamic Applications poll BIG-IP to determine the number of component devices monitored by SL1.
- ***Discovery***. These Dynamic Applications poll BIG-IP for new instances of component devices or changes to existing instances of component devices.
- ***Configuration***. These Dynamic Applications retrieve configuration information about each component device and retrieve any changes to that configuration information.
- ***Performance***. These Dynamic Applications poll BIG-IP for performance metrics.

The following Dynamic Applications are aligned automatically to the F5 BIG-IP system when you run discovery:

- F5: Viprion Chassis Slot Status
- F5 BIG-IP: Cluster Status
- F5 BIG-IP: CPU Configuration
- F5 BIG-IP: Disk Array Status
- F5 BIG-IP: Fan Status
- F5 BIG-IP: Interface Usage (64Bit)
- F5 BIG-IP: Performance
- F5 BIG-IP: Power Supply Status
- F5 BIG-IP: System Configuration
- F5 BIG-IP: Temperature
- F5 BIG-IP: vCMP VM Configuration
- F5 BIG-IP LTM: Node Configuration
- F5 BIG-IP LTM: Node Discovery
- F5 BIG-IP LTM: Node Performance
- F5 BIG-IP LTM: Pool Configuration
- F5 BIG-IP LTM: Pool Discovery: Non-Default Pools
- F5 BIG-IP LTM: Pool Discovery: Virtual Server Default Pools
- F5 BIG-IP LTM: Pool Member Configuration
- F5 BIG-IP LTM: Pool Member Discovery

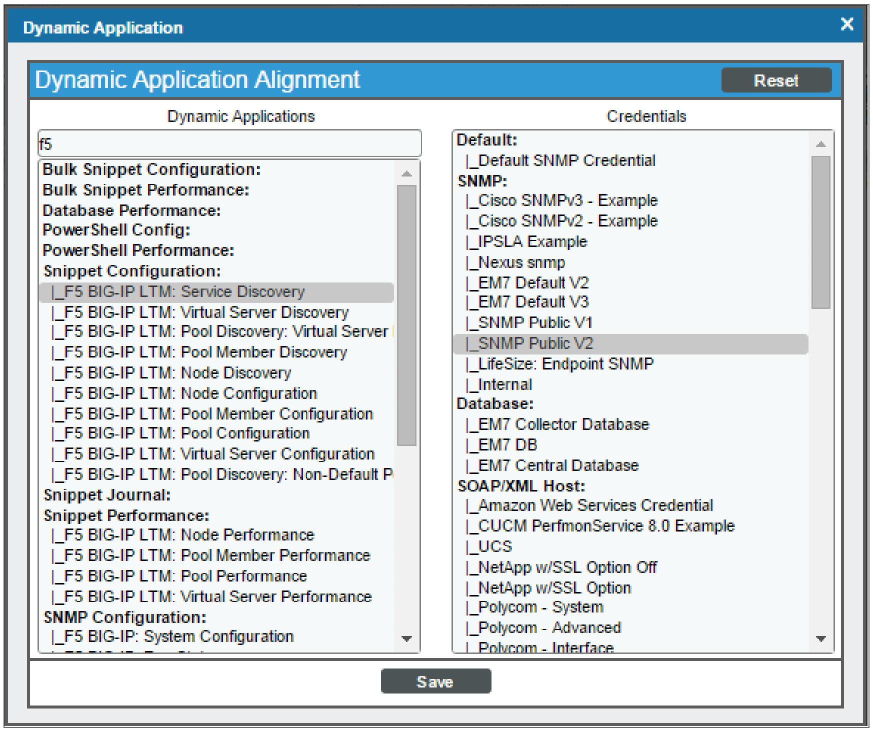
- F5 BIG-IP LTM: Pool Member Performance
- F5 BIG-IP LTM: Pool Performance
- F5 BIG-IP LTM: Virtual Server Configuration
- F5 BIG-IP LTM: Virtual Server Discovery
- F5 BIG-IP LTM: Virtual Server Performance
- Host Resource: Configuration
- Net SNMP: CPU
- Net SNMP: Physical Memory
- Net SNMP: Swap

CAUTION: To discover all of the component devices in the BIG-IP system, you must ***manually align*** the "F5 BIG-IP LTM: Service Discovery" Dynamic Application with the BIG-IP root device. For instructions on how to do this, see the section on ***Manually Aligning the Dynamic Application with the BIG-IP Root Device***.

If these Dynamic Applications are not aligned during discovery, perform the following steps to add them manually:

1. Go to the **Device Properties** page (Registry > Devices > wrench icon) for the BIG-IP system.
2. Click the **[Collections]** tab. The **Dynamic Application Collections** page appears.

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



Dynamic Application

Dynamic Application Alignment

Reset

Dynamic Applications

f5

Bulk Snippet Configuration:
Bulk Snippet Performance:
Database Performance:
PowerShell Config:
PowerShell Performance:
Snippet Configuration:
|_F5 BIG-IP LTM: Service Discovery
|_F5 BIG-IP LTM: Virtual Server Discovery
|_F5 BIG-IP LTM: Pool Discovery: Virtual Server
|_F5 BIG-IP LTM: Pool Member Discovery
|_F5 BIG-IP LTM: Node Discovery
|_F5 BIG-IP LTM: Node Configuration
|_F5 BIG-IP LTM: Pool Member Configuration
|_F5 BIG-IP LTM: Pool Configuration
|_F5 BIG-IP LTM: Virtual Server Configuration
|_F5 BIG-IP LTM: Pool Discovery: Non-Default P
Snippet Journal:
Snippet Performance:
|_F5 BIG-IP LTM: Node Performance
|_F5 BIG-IP LTM: Pool Member Performance
|_F5 BIG-IP LTM: Pool Performance
|_F5 BIG-IP LTM: Virtual Server Performance
SNMP Configuration:
|_F5 BIG-IP: System Configuration

Credentials

Default:
|_Default SNMP Credential
SNMP:
|_Cisco SNMPv3 - Example
|_Cisco SNMPv2 - Example
|_IPSLA Example
|_Nexus snmp
|_EM7 Default V2
|_EM7 Default V3
|_SNMP Public V1
|_SNMP Public V2
|_LifeSize: Endpoint SNMP
|_Internal
Database:
|_EM7 Collector Database
|_EM7 DB
|_EM7 Central Database
SOAP/XML Host:
|_Amazon Web Services Credential
|_CUCM PerfmonService 8.0 Example
|_UCS
|_NetApp w/SSL Option Off
|_NetApp w/SSL Option
|_Polycom - System
|_Polycom - Advanced
|_Polycom - Interface

Save

4. In the ***Dynamic Applications*** field, select the Dynamic Application that you want to align to the BIG-IP system.

5. In the ***Credentials*** field, select the SNMP credential for the BIG-IP system.

6. Click the **[Save]** button.

Manually Aligning the "F5 BIG IP LTM: Service Discovery" Dynamic Application with the BIG-IP Root Device

When you run discovery, the "F5 BIG-IP LTM: Component Counts" Dynamic Application is automatically aligned with the F5 BIG-IP system. This Dynamic Application enables you to determine the number of component devices in your BIG-IP system that will be discovered.

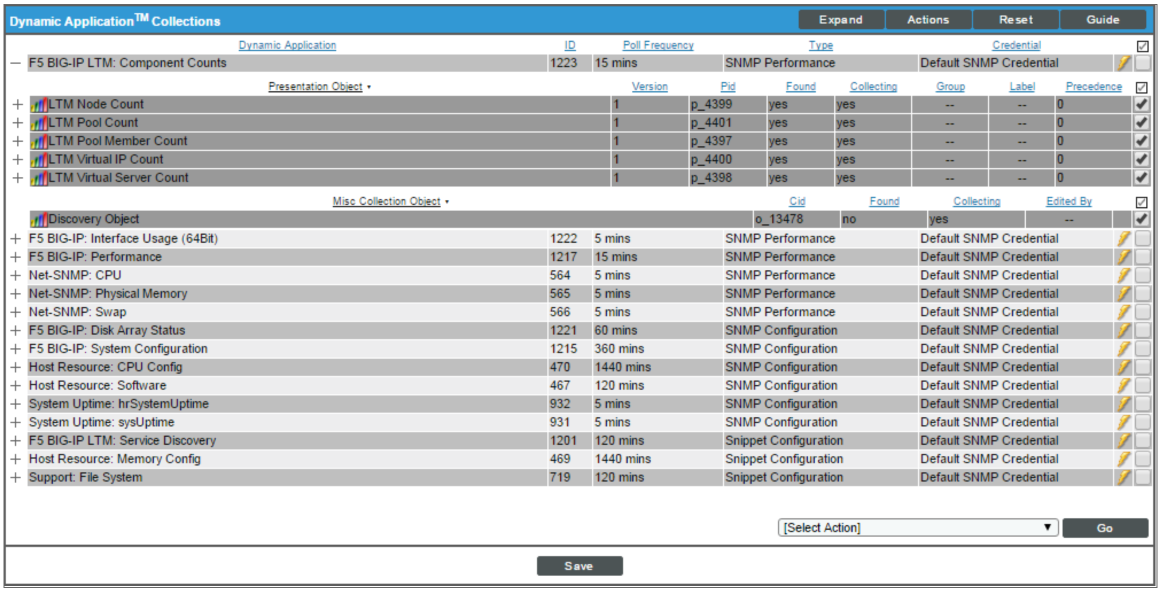
To determine the BIG-IP component device count:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).

2. Click the wrench icon ( ) for the BIG-IP system.

3. In the **Device Administration** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page displays.

4. Click the plus icon (+) for the "F5 BIG-IP LTM: Component Counts" Dynamic Application. If collection for the Dynamic Application was successful, the graph icons (📊) for the "F5 BIG-IP LTM: Component Counts" presentation objects are enabled:



Dynamic Application™ Collections

	Dynamic Application	ID	Poll Frequency	Type	Credential		☑
—	F5 BIG-IP LTM: Component Counts	1223	15 mins	SNMP Performance	Default SNMP Credential	✎	□

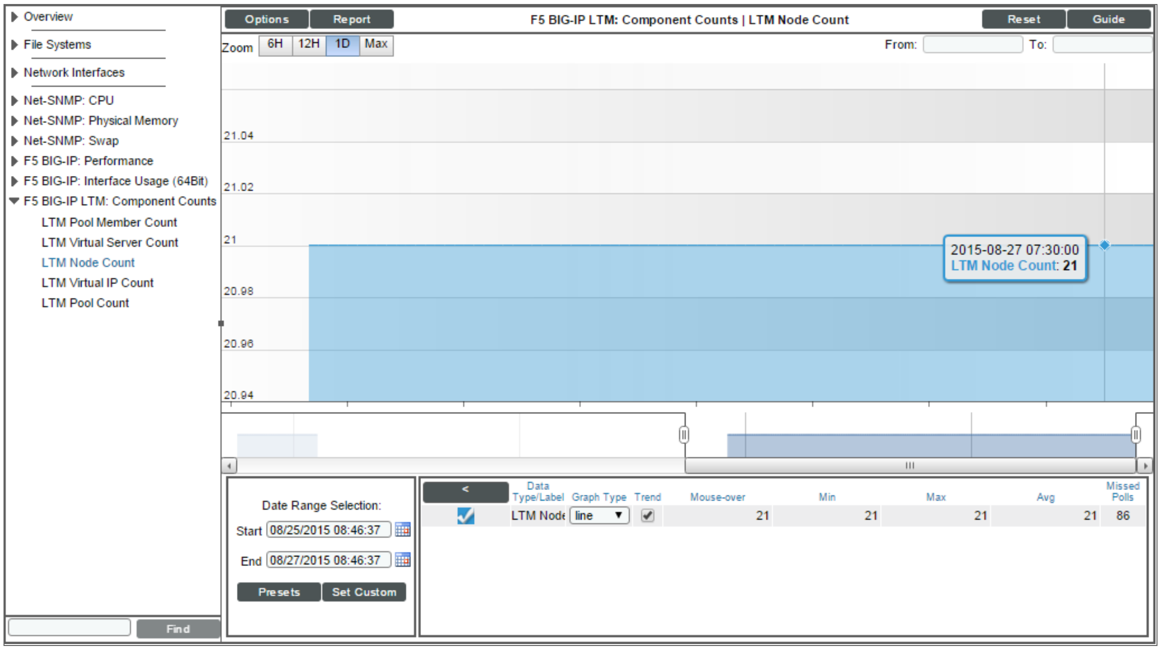
	Presentation Object ▾	Version	Pid	Found	Collecting	Group	Label	Precedence	☑
+	📊LTM Node Count	1	p_4399	yes	yes	--	--	0	✓
+	📊LTM Pool Count	1	p_4401	yes	yes	--	--	0	✓
+	📊LTM Pool Member Count	1	p_4397	yes	yes	--	--	0	✓
+	📊LTM Virtual IP Count	1	p_4400	yes	yes	--	--	0	✓
+	📊LTM Virtual Server Count	1	p_4398	yes	yes	--	--	0	✓

Misc Collection Object ▾	Cid	Found	Collecting	Edited By	☑
📊Discovery Object	o_13478	no	yes	--	✓

	Dynamic Application	ID	Poll Frequency	Type	Credential		
+	F5 BIG-IP: Interface Usage (64Bit)	1222	5 mins	SNMP Performance	Default SNMP Credential	✎	□
+	F5 BIG-IP: Performance	1217	15 mins	SNMP Performance	Default SNMP Credential	✎	□
+	Net-SNMP: CPU	564	5 mins	SNMP Performance	Default SNMP Credential	✎	□
+	Net-SNMP: Physical Memory	565	5 mins	SNMP Performance	Default SNMP Credential	✎	□
+	Net-SNMP: Swap	566	5 mins	SNMP Performance	Default SNMP Credential	✎	□
+	F5 BIG-IP: Disk Array Status	1221	60 mins	SNMP Configuration	Default SNMP Credential	✎	□
+	F5 BIG-IP: System Configuration	1215	360 mins	SNMP Configuration	Default SNMP Credential	✎	□
+	Host Resource: CPU Config	470	1440 mins	SNMP Configuration	Default SNMP Credential	✎	□
+	Host Resource: Software	467	120 mins	SNMP Configuration	Default SNMP Credential	✎	□
+	System Uptime: hrSystemUptime	932	5 mins	SNMP Configuration	Default SNMP Credential	✎	□
+	System Uptime: sysUptime	931	5 mins	SNMP Configuration	Default SNMP Credential	✎	□
+	F5 BIG-IP LTM: Service Discovery	1201	120 mins	Snippet Configuration	Default SNMP Credential	✎	□
+	Host Resource: Memory Config	469	1440 mins	Snippet Configuration	Default SNMP Credential	✎	□
+	Support: File System	719	120 mins	Snippet Configuration	Default SNMP Credential	✎	□

[Select Action] ▾ Go

5. Click a graph icon (📊) for any of the "F5 BIG-IP LTM: Component Counts" presentation objects to view the collected data for that presentation object. The **Device Performance** page displays the number of components that are being monitored.



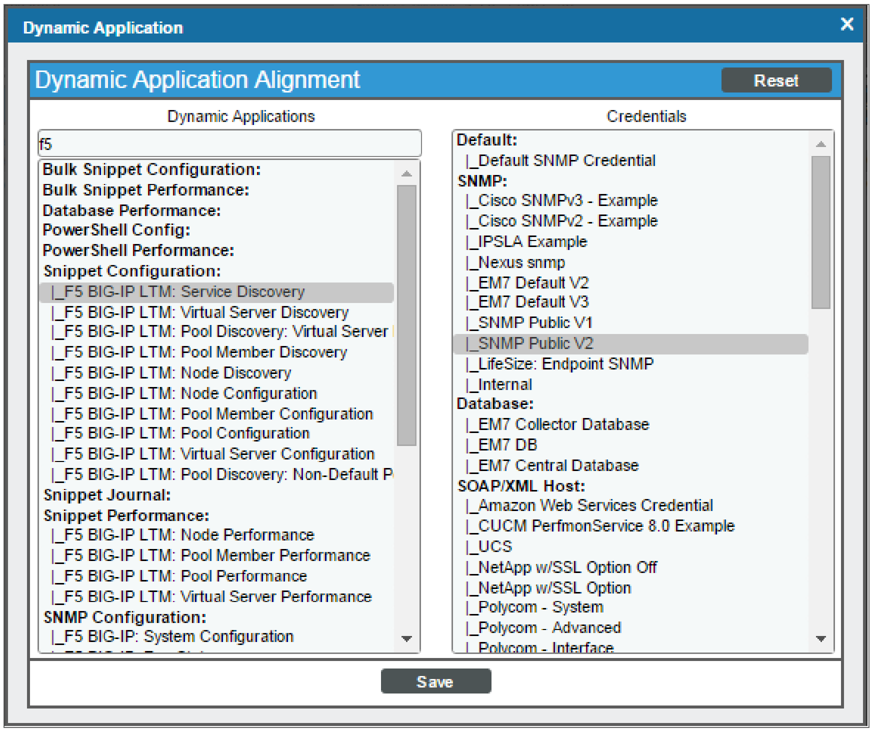
F5 BIG-IP LTM: Component Counts | LTM Node Count

Date Range Selection:
Start 08/25/2015 08:46:37
End 08/27/2015 08:46:37

	Data Type/Label	Graph Type	Trend	Mouse-over	Min	Max	Avg	Missed Polls
☑	LTM Node	line ▾	☑	21	21	21	21	86

After verifying the number of component devices that will be discovered, perform the following steps to start component device discovery by aligning the "F5 BIG-IP LTM: Service Discovery" Dynamic Application with the BIG-IP root system:

1. Go to the **Device Properties** page (Registry > Devices > wrench icon) for the BIG-IP system.
2. Click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
3. Click the **[Actions]** button and then select *Add Dynamic Application*. The **Dynamic Application Alignment** page appears:


Dynamic Application
Dynamic Application Alignment
Reset
Dynamic Applications
f5
Bulk Snippet Configuration:
Bulk Snippet Performance:
Database Performance:
PowerShell Config:
PowerShell Performance:
Snippet Configuration:
|_F5 BIG-IP LTM: Service Discovery
|_F5 BIG-IP LTM: Virtual Server Discovery
|_F5 BIG-IP LTM: Pool Discovery: Virtual Server
|_F5 BIG-IP LTM: Pool Member Discovery
|_F5 BIG-IP LTM: Node Discovery
|_F5 BIG-IP LTM: Node Configuration
|_F5 BIG-IP LTM: Pool Member Configuration
|_F5 BIG-IP LTM: Pool Configuration
|_F5 BIG-IP LTM: Virtual Server Configuration
|_F5 BIG-IP LTM: Pool Discovery: Non-Default P
Snippet Journal:
Snippet Performance:
|_F5 BIG-IP LTM: Node Performance
|_F5 BIG-IP LTM: Pool Member Performance
|_F5 BIG-IP LTM: Pool Performance
|_F5 BIG-IP LTM: Virtual Server Performance
SNMP Configuration:
|_F5 BIG-IP: System Configuration
Credentials
Default:
|_Default SNMP Credential
SNMP:
|_Cisco SNMPv3 - Example
|_Cisco SNMPv2 - Example
|_IPSLA Example
|_Nexus snmp
|_EM7 Default V2
|_EM7 Default V3
|_SNMP Public V1
|_SNMP Public V2
|_LifeSize: Endpoint SNMP
|_Internal
Database:
|_EM7 Collector Database
|_EM7 DB
|_EM7 Central Database
SOAP/XML Host:
|_Amazon Web Services Credential
|_CUCM PerfmonService 8.0 Example
|_UCS
|_NetApp w/SSL Option Off
|_NetApp w/SSL Option
|_Polycom - System
|_Polycom - Advanced
|_Polycom - Interface
Save

4. In the ***Dynamic Applications*** field, select *F5 BIG-IP LTM: Service Discovery*.
5. In the ***Credentials*** field, select the SNMP credential for the BIG-IP system.
6. Click the **[Save]** button.

Chapter

39

F5: BIG-IP DNS

Overview

The following sections describe how to configure and discover F5 BIG-IP DNS services for monitoring by SL1 using the *F5: BIG-IP DNS* PowerPack:

NOTE: For more information about the *F5: BIG-IP DNS* PowerPack, see the ***Monitoring F5 BIG-IP DNS*** manual.

Prerequisites for Monitoring F5 BIG-IP DNS

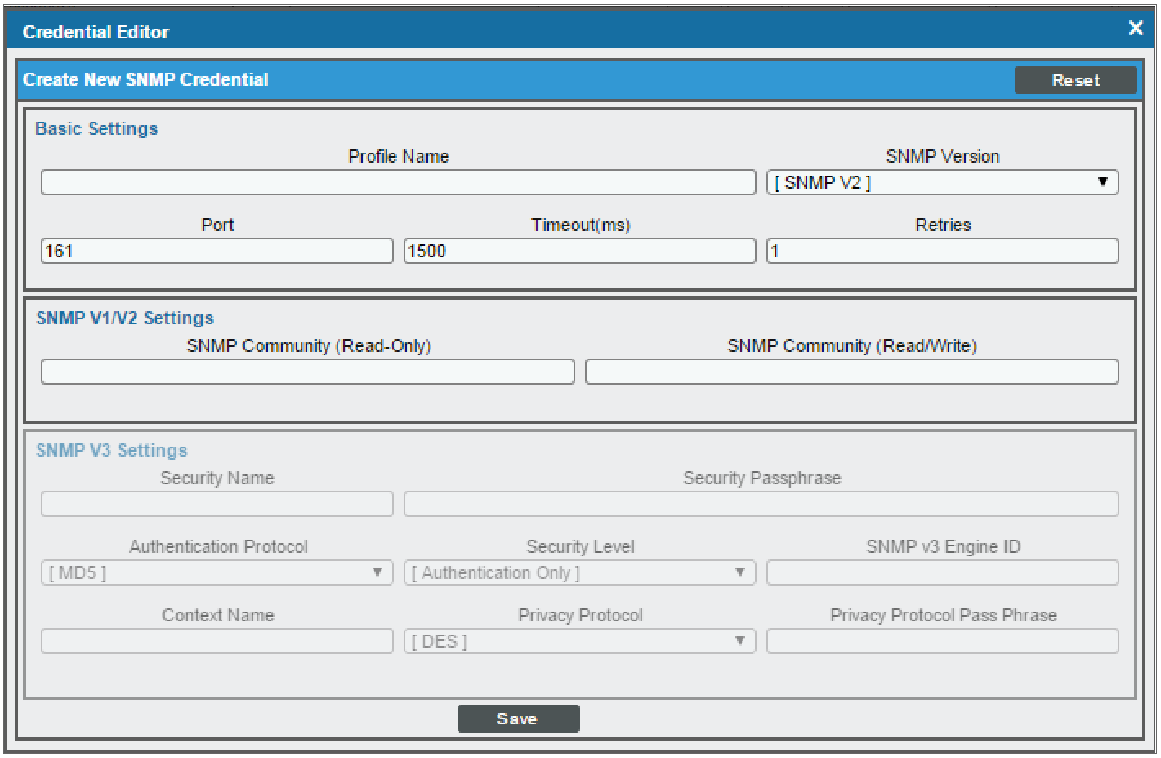
Before you can monitor F5 BIG-IP DNS services using the *F5: BIG-IP DNS* PowerPack, you must ensure that SL1 can communicate with BIG-IP DNS using SNMP and you must know the SNMP community string for the BIG-IP DNS system. SL1 can then use the data collected from BIG-IP DNS to create device records for all DNS components.

Creating an SNMP Credential for F5 BIG-IP DNS

To use the Dynamic Applications in the *F5: BIG-IP DNS* PowerPack, you must first define an SNMP credential in SL1. This credential allows SL1 to communicate with the BIG-IP DNS system.

To configure an SNMP credential for F5 BIG-IP DNS:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the **[Actions]** button.
3. In the drop-down list that appears, select *Create SNMP Credential*. The **Credential Editor** page appears:



Credential Editor

Create New SNMP Credential

Reset

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:

Save

4. In the ***Profile Name*** field, type a name for the credential.
5. In the ***SNMP Version*** field, select *SNMP V2*.
6. In the ***SNMP Community (Read Only)*** field, type the community string for the BIG-IP DNS system.
7. Optionally, supply values in the other fields in this page. In most cases, you can use the default values for the other fields.
8. Click the **[Save]** button.

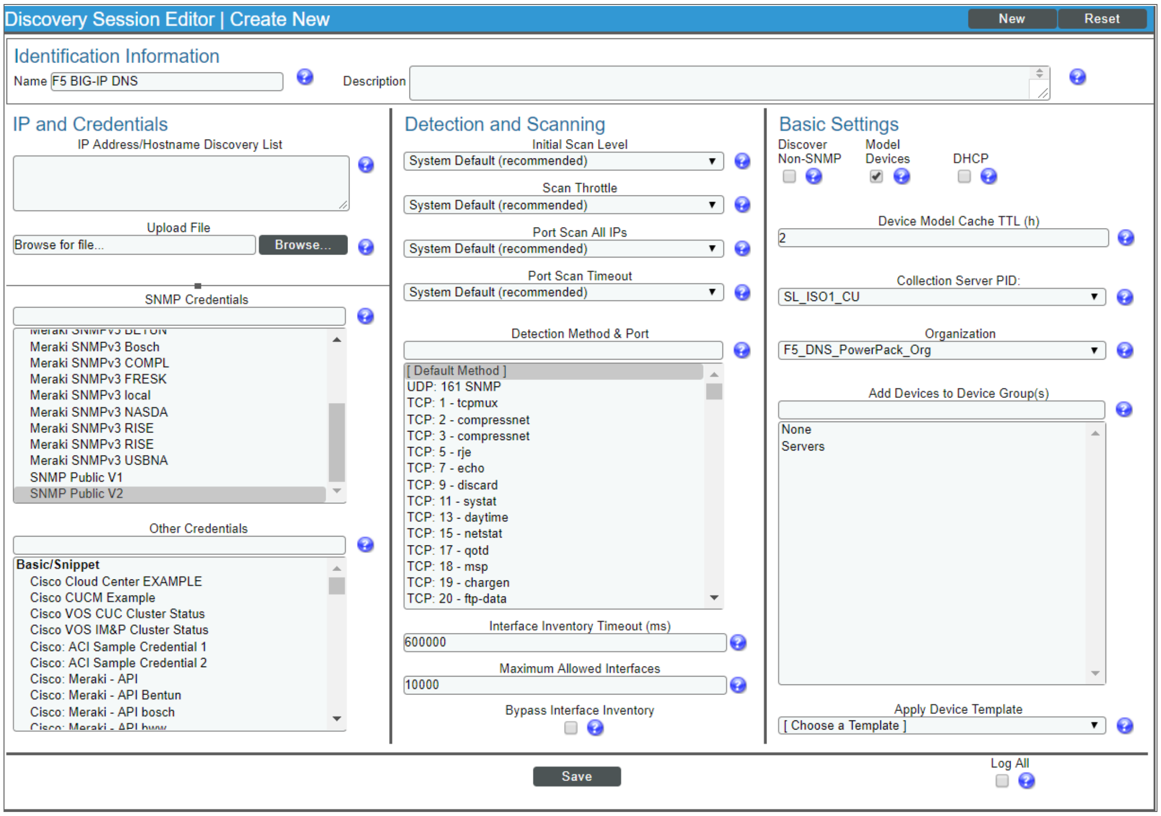
Discovering an F5 BIG-IP System

After you have created an SNMP credential for the F5 BIG-IP DNS system that you want to monitor, you can create and run a discovery session that will discover your BIG-IP DNS system.

> CAUTION: The *F5: BIG-IP DNS* PowerPack enables you to discover and monitor a maximum of 1,500 component devices.

To discover your BIG-IP DNS system:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. Click the **[Create]** button to create a new discovery session. The **Discovery Session Editor** window appears:



Discovery Session Editor | Create New

Identification Information

Name: F5 BIG-IP DNS

Description:

IP and Credentials

IP Address/Hostname Discovery List:

Upload File: Browse for file...

SNMP Credentials:

Meraki SNMPv3 BETON
Meraki SNMPv3 Bosch
Meraki SNMPv3 COMPL
Meraki SNMPv3 FRESK
Meraki SNMPv3 local
Meraki SNMPv3 NASDA
Meraki SNMPv3 RISE
Meraki SNMPv3 RISE
Meraki SNMPv3 USBNA
SNMP Public V1
SNMP Public V2

Other Credentials:

Basic/Snippet
Cisco Cloud Center EXAMPLE
Cisco CUCM Example
Cisco VOS CUC Cluster Status
Cisco VOS IM&P Cluster Status
Cisco: ACI Sample Credential 1
Cisco: ACI Sample Credential 2
Cisco: Meraki - API
Cisco: Meraki - API Bentun
Cisco: Meraki - API bosch
Cisco: Meraki - API hww

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
TCP: 17 - qotd
TCP: 18 - msp
TCP: 19 - chargen
TCP: 20 - ftp-data

Interface Inventory Timeout (ms): 600000

Maximum Allowed Interfaces: 10000

Bypass Interface Inventory: □

Basic Settings

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

Device Model Cache TTL (h): 2

Collection Server PID: SL_ISO1_CU

Organization: F5_DNS_PowerPack_Org

Add Devices to Device Group(s):

None
Servers

Apply Device Template: [Choose a Template]

Log All: □

3. Complete the following fields:

- ***Name***. Type a name for the discovery session.
- ***IP Address/Hostname Discovery List***. Type the IP address for the BIG-IP DNS system.
- ***SNMP Credentials***. Select the SNMP Credential for the BIG-IP DNS system.

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 will appear 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 BIG-IP DNS root device is discovered, you can click its device icon () to view the system device's properties.

NOTE: SL1 might take several minutes to discover the component devices for your BIG-IP DNS service.

Chapter

40

Google Cloud Platform *BETA*

Overview

The following sections describe how to configure and discover Google Cloud Platform resources for monitoring by SL1 using the *Google Cloud Platform *BETA** PowerPack:

NOTE: For more information about the *Google Cloud Platform *BETA** PowerPack, see the ***Monitoring Google Cloud Platform*** manual.

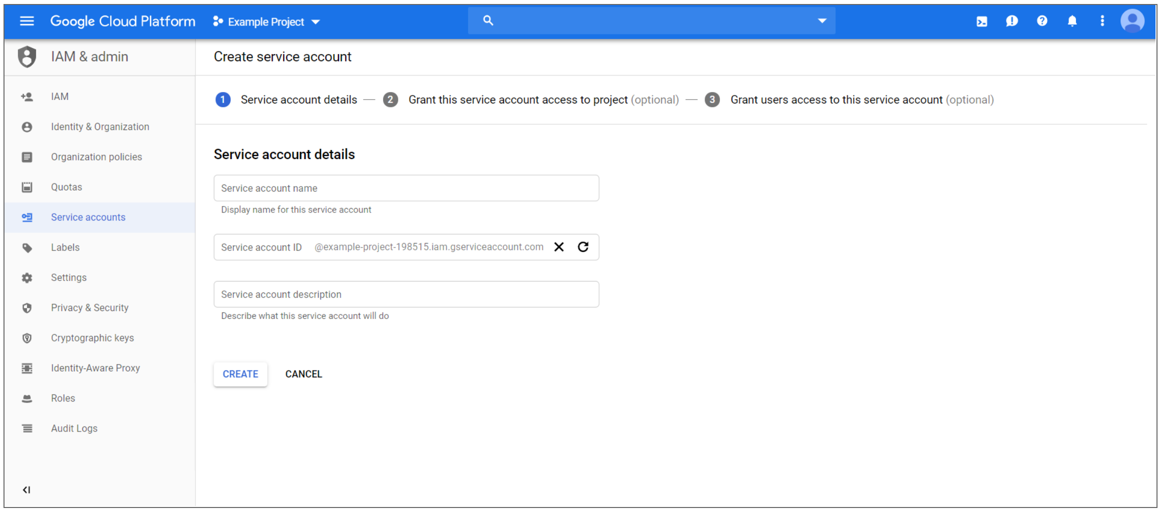
Creating a Google Cloud Platform Service Account

To monitor Google Cloud Platform (GCP) resources with SL1, you must first create a GCP ***service account*** for SL1 in the GCP Console. This service account belongs to SL1 instead of an individual end user, and enables SL1 to communicate with Google APIs when monitoring your GCP resources.

This service account's credentials will include a unique email address and a secret JSON key. You will include this email address and key information when you create the SOAP/XML credential that enables SL1 to monitor your GCP resources.

To create a GCP service account:

1. Log in to the GCP Console and go to the **Service accounts** page. If prompted, select a project.
2. Click the **[CREATE SERVICE ACCOUNT]** button.
3. Complete the following fields on the **Create service account** page:

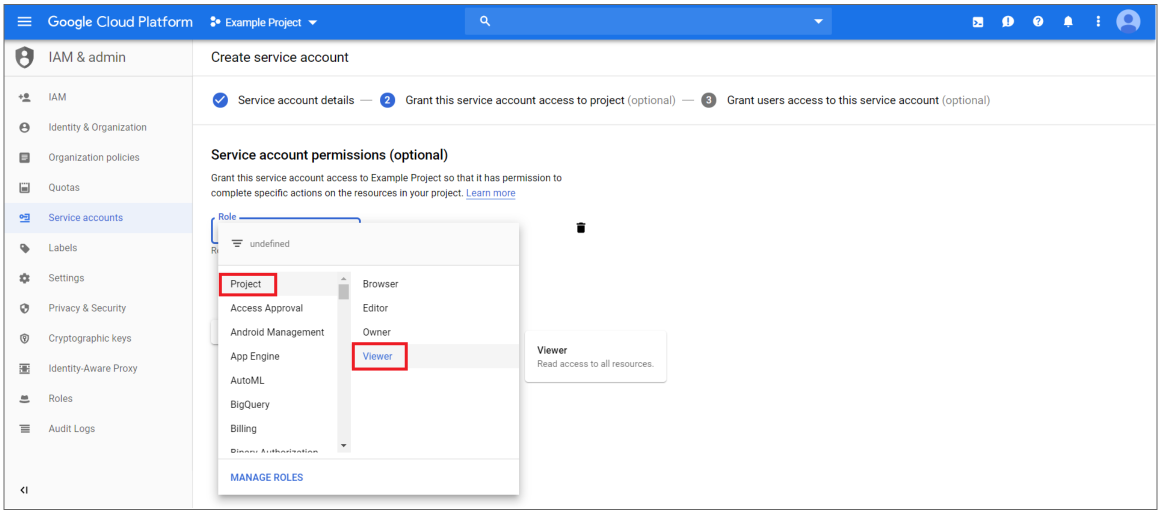


Google Cloud Platform
Example Project
IAM & admin
Create service account
IAM
Identity & Organization
Organization policies
Quotas
Service accounts
Labels
Settings
Privacy & Security
Cryptographic keys
Identity-Aware Proxy
Roles
Audit Logs
1 Service account details — 2 Grant this service account access to project (optional) — 3 Grant users access to this service account (optional)
Service account details
Service account name
Display name for this service account
Service account ID @example-project-198515.iam.gserviceaccount.com
Service account description
Describe what this service account will do
CREATE
CANCEL

   - ***Service account name.*** Type a name for the service account.
   - ***Service account ID.*** This field auto-populates with a service account ID that is based on your ***Service account name***.
   - ***Service account description.*** Type a description for the service account.

4. Click **[Create]**. Your service account is created, and the **Service account permissions** page displays.

5. Complete the following fields on the **Service account permissions** page:



Create service account

Service account details — 2 Grant this service account access to project (optional) — 3 Grant users access to this service account (optional)

Service account permissions (optional)

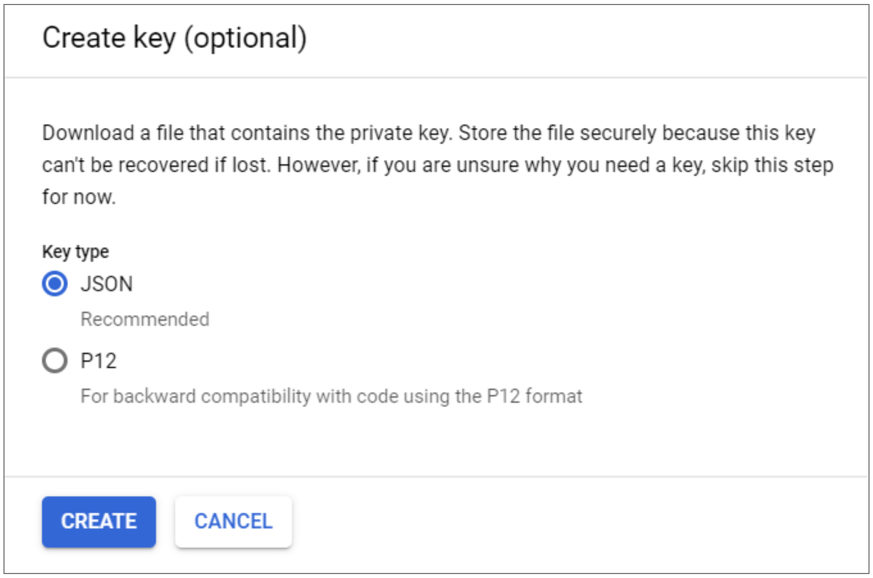
Grant this service account access to Example Project so that it has permission to complete specific actions on the resources in your project. Learn more

Viewer
Read access to all resources.

- ***Role***. Select *Project* > *Viewer*.

NOTE: At a minimum, the service account must have a role of "Project" with "Viewer" permissions for the GCP service that you want to monitor.

6. Click **[Continue]**. The **Grant users access to this service account** page displays.
7. Click **[Create Key]**. The **Create key** pane appears.
8. On the **Create key** pane, select the JSON radio button and then click **[Create]**. The private JSON key is saved to your computer.



Create key (optional)

Download a file that contains the private key. Store the file securely because this key can't be recovered if lost. However, if you are unsure why you need a key, skip this step for now.

Key type

● JSON
Recommended

○ P12
For backward compatibility with code using the P12 format

9. Click **[Close]**, and then click **[Done]**.
10. Open the JSON file that was downloaded to your computer and copy the following information:

    - client_email
    - private_key

> **TIP:** When you copy the private key from the JSON file, it must include the "BEGIN PRIVATE KEY" and "END PRIVATE KEY" lines, including all leading and ending dashes.

If you are discovering GCP resources at the Project level, then you can skip the following steps and continue on to the ***Enabling Google Cloud APIs*** section.

However, ***if you are discovering GCP resources at the Organization level***, then you must also do the following:

11. In the GCP Console, go to the **IAM** page and select your organization.
12. Click **[Add]**.
13. Add your service account as a member of the organization, and then add the following mandatory roles:
    - Role > Project > Viewer
    - Role > Resource Manager >Folder Viewer
    - Role > Resource Manager > Organization Viewer
14. When you are finished, click **[Save]**.

Enabling Google Cloud Platform APIs

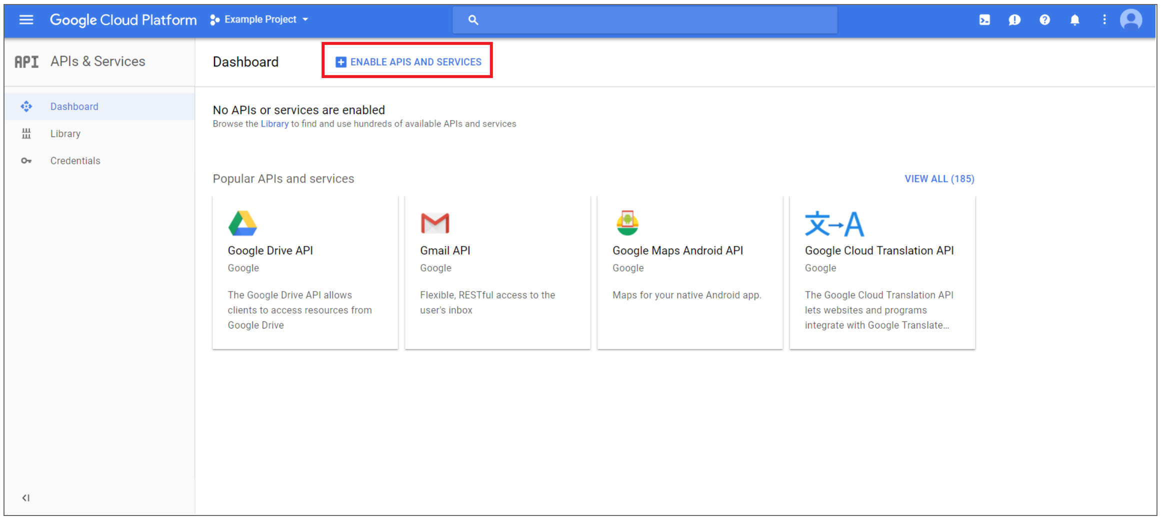
Before SL1 can monitor GCP, you must also enable two APIs in the GCP portal:

- Cloud Resource Manager API
- Compute Engine API

To enable these GCP APIs:

1. Log in to the GCP Console for your project and go to the **API & Services Dashboard** page.

2. Click **[ENABLE APIS AND SERVICES]**. The **API Library** page appears.



No APIs or services are enabled

Browse the Library to find and use hundreds of available APIs and services

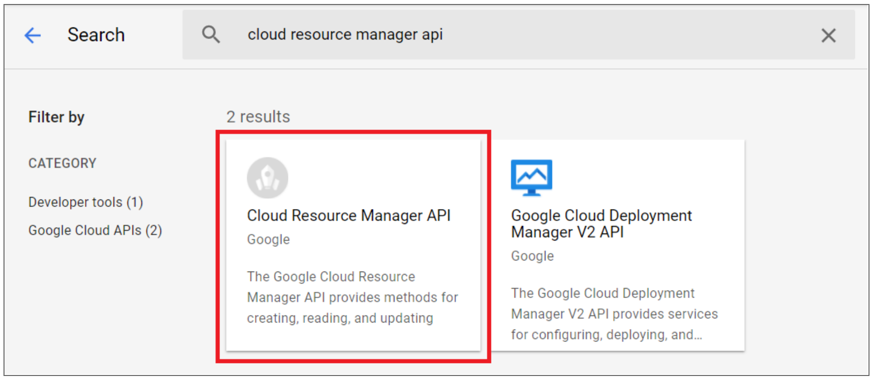
Google Drive API
Google
The Google Drive API allows clients to access resources from Google Drive

Gmail API
Google
Flexible, RESTful access to the user's inbox

Google Maps Android API
Google
Maps for your native Android app.

Google Cloud Translation API
Google
The Google Cloud Translation API lets websites and programs integrate with Google Translate...

3. In the search bar, type "Cloud Resource Manager API". The page will filter search results while you type.
4. Click the **Cloud Resource Manager API** box.



Cloud Resource Manager API
Google
The Google Cloud Resource Manager API provides methods for creating, reading, and updating

Google Cloud Deployment Manager V2 API
Google
The Google Cloud Deployment Manager V2 API provides services for configuring, deploying, and...

5. On the **Cloud Resource Manager API** page, click the **[Enable]** button.
6. Click **[Dashboard]** on the **API & Services** left menu and then repeat steps 2-5 to enable the **Compute Engine API**.

Creating a SOAP/XML Credential for Google Cloud Platform

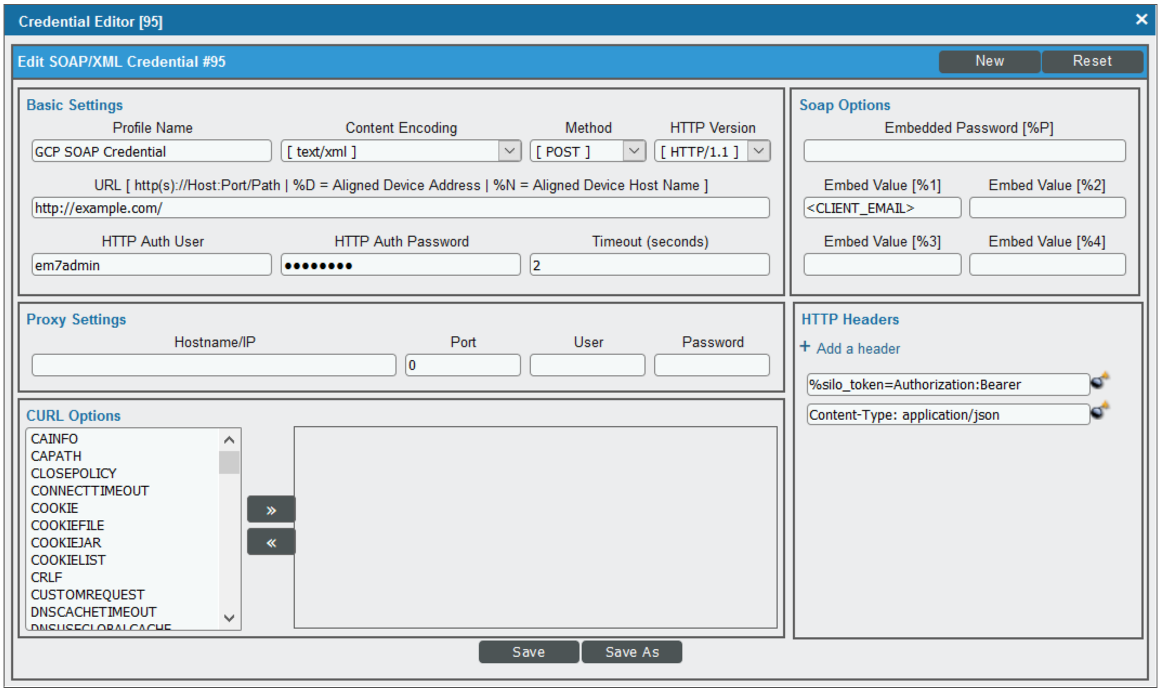
To configure SL1 to monitor GCP, you must create a SOAP/XML credential that allows the Dynamic Applications in the *Google Cloud Platform *BETA** PowerPack to connect with your GCP service. An example SOAP/XML credential that you can edit for your own use is included in the *Google Cloud Platform *BETA** PowerPack.

To create a SOAP/XML credential to access GCP:

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

2. Locate the **GCP SOAP Credential** and then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears.

3. Complete the following fields:



Credential Editor [95]

Edit SOAP/XML Credential #95

Basic Settings

Profile Name: GCP SOAP Credential

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: http://example.com/

HTTP Auth User: em7admin

HTTP Auth Password: ●●●●●●●●

Timeout (seconds): 2

Soap Options

Embedded Password [%P]:

Embed Value [%1]: <CLIENT_EMAIL>

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

Proxy Settings

Hostname/IP:

Port: 0

User:

Password:

HTTP Headers

%silo_token=Authorization:Bearer

Content-Type: application/json

CURL Options

CAINFO
CAPATH
CLOSEPOLICY
CONNECTTIMEOUT
COOKIE
COOKIEFILE
COOKIEJAR
COOKIELIST
CRLF
CUSTOMREQUEST
DNSCACHETIMEOUT
DNSUSEGLOBALCACHE

Basic Settings

- ***Profile Name***. Type a new name for the credential.

SOAP Options

- ***Embedded Password [%P]***. Paste the "private_key" value from the private key JSON file.
- ***Embed Value [%1]***. Type the "client_email" value from the private key JSON file. For example: myprojectid@myaccount.iam.gserviceaccount.com.

TIP: When you copy the "private_key" from the JSON file, it must include the "BEGIN PRIVATE KEY" and "END PRIVATE KEY" lines, including all leading and ending dashes.

4. For all remaining fields, use the default values.

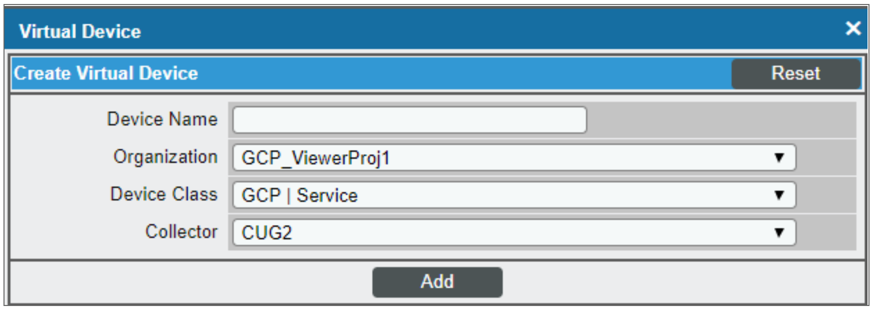
5. Click the **[Save As]** button, and then click **[OK]**.

Creating a Google Cloud Platform Virtual Device

Because the GCP service does not have a static IP address, you cannot discover GCP devices using a regular discovery session. Instead, you must create a ***virtual device*** that represents the GCP service. A virtual device is a user-defined container that represents a device or service that cannot be discovered by SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications.

To create a virtual device that represents your GCP service:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Click the **[Actions]** button and select *Create Virtual Device* from the menu. The **Virtual Device** modal page appears.
3. Complete the following fields:



Device Name
Organization: GCP_ViewerProj1
Device Class: GCP | Service
Collector: CUG2

   - ***Device Name***. Type a name for the device.
   - ***Organization***. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.
   - ***Device Class***. Select *GCP | Service*.
   - ***Collector***. Select the collector group that will monitor the device.

4. Click **[Add]** to create the virtual device.

Aligning the Google Cloud Platform Dynamic Applications

The Dynamic Applications in the *Google Cloud Platform *BETA** PowerPack are divided into the following types:

- ***Discovery***. These Dynamic Applications poll GCP for new instances of services or changes to existing instances of services.
- ***Configuration***. These Dynamic Applications retrieve configuration information about each service instance and retrieve any changes to that configuration information.
- ***Performance***. These Dynamic Applications poll GCP for performance metrics.

When configuring SL1 to monitor GCP services, you must manually align Dynamic Applications to discover GCP component devices.

Discovering Google Cloud Platform Component Devices

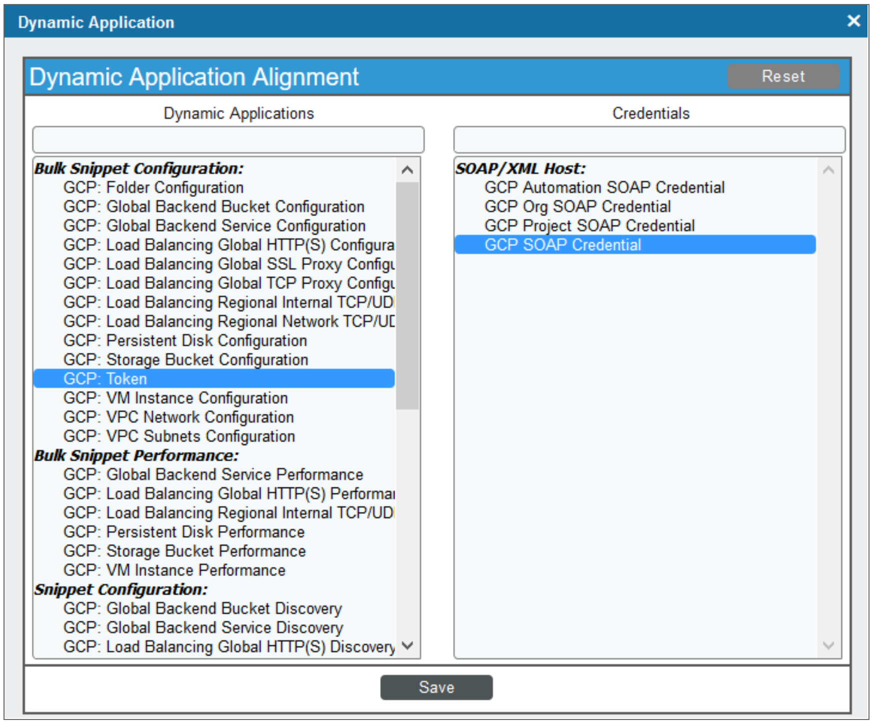
To discover all the components of your GCP service, you must manually align two Dynamic Applications with the GCP virtual device. The specific Dynamic Applications that you must align to the virtual device vary based on whether you are discovering GCP resources from the Organization level or the Project level.

- If you are discovering an Organization, you must align the following Dynamic Applications:
  - GCP: Token
  - GCP: Organization Discovery
- If you are discovering GCP resources from the Project level, you must align the following Dynamic Applications:
  - GCP: Token
  - GCP: Project Discovery

To manually align these Dynamic Applications:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Click the wrench icon (🔧) for your GCP virtual device.
3. In the ***Device Administration*** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
4. Click the **[Actions]** button and select *Add Dynamic Application* from the menu.

5. In the **Dynamic Application Alignment** modal:


Dynamic Application
Dynamic Application Alignment
Reset
Dynamic Applications
Credentials
Bulk Snippet Configuration:
GCP: Folder Configuration
GCP: Global Backend Bucket Configuration
GCP: Global Backend Service Configuration
GCP: Load Balancing Global HTTP(S) Configura
GCP: Load Balancing Global SSL Proxy Configu
GCP: Load Balancing Global TCP Proxy Configu
GCP: Load Balancing Regional Internal TCP/UD
GCP: Load Balancing Regional Network TCP/UD
GCP: Persistent Disk Configuration
GCP: Storage Bucket Configuration
GCP: Token
GCP: VM Instance Configuration
GCP: VPC Network Configuration
GCP: VPC Subnets Configuration
Bulk Snippet Performance:
GCP: Global Backend Service Performance
GCP: Load Balancing Global HTTP(S) Performa
GCP: Load Balancing Regional Internal TCP/UD
GCP: Persistent Disk Performance
GCP: Storage Bucket Performance
GCP: VM Instance Performance
Snippet Configuration:
GCP: Global Backend Bucket Discovery
GCP: Global Backend Service Discovery
GCP: Load Balancing Global HTTP(S) Discovery
SOAP/XML Host:
GCP Automation SOAP Credential
GCP Org SOAP Credential
GCP Project SOAP Credential
GCP SOAP Credential
Save

- In the ***Dynamic Applications*** field, select *GCP Token*.
- In the ***Credentials*** field, select the credential you created for your GCP service.

6. Click **[Save]** to align the Dynamic Application with the GCP virtual device.
7. Repeat steps 2-6 to align the "GCP Project Discovery" or "GCP Project Discovery" Dynamic Application, depending on whether you are discovering an Organization or a Project.

NOTE: You must align the "GCP: Token" Dynamic Application ***before*** you align the "GCP: Organization Discovery" or "GCP: Project Discovery" Dynamic Application.

When you align the Dynamic Applications with the virtual device representing your GCP service, SL1 creates a component device representing your GCP Organization or Project.

SL1 then automatically aligns several other Dynamic Applications to that component device. These Dynamic Applications discover and create additional component devices representing your GCP resources.

NOTE: SL1 might take several minutes to align these Dynamic Applications and create the component devices in your GCP service.

Relationships Between Component Devices

In addition to parent/child relationships between component devices, SL1 also creates relationships between the following component devices:

- Compute Instances and Storage Persistent Disks
- Compute Instances and Subnets
- Compute Instances and VPC Networks
- Load Balancing Global HTTPS and Backend Buckets
- Load Balancing Global HTTPS and Backend Services
- Load Balancing Global HTTPS and Default Backend Services
- Load Balancing Global SSL Proxy and Backend Services
- Load Balancing Global TCP Proxy and Backend Services
- Load Balancing Regional Network TCP/UDP and Compute Instances
- VPC Subnets and VPC Networks

NOTE: If an instance is configured in GCP to automatically delete any associated read-write persistent disks when the instance is deleted, then that behavior will also occur in SL1: If the instance is deleted, its related persistent disks will also be deleted. This behavior is controlled in GCP on the **VM Instances** page by the *Delete boot disk when instance is deleted* checkbox for boot disks and the ***When deleting instance*** field for additional disks.

Additionally, SL1 can also build relationships between GCP VM Instances and Kubernetes Nodes, for users who also have the *Kubernetes* PowerPack installed.

Chapter 41

Hitachi Data Systems: VSP

Overview

The following sections describe how to configure and discover Hitachi Virtual Storage Platform (VSP) systems for monitoring by SL1 using the *Hitachi Data Systems: VSP* PowerPack:

> NOTE: For more information about the *Hitachi Data Systems: VSP* PowerPack, see the ***Monitoring Hitachi Data Systems*** manual.

Prerequisites for Monitoring Hitachi VSP Systems

Before you can monitor Hitachi VSP storage arrays using the *Hitachi Data Systems: VSP* PowerPack, you must have the following information about an Hitachi SMI-S Provider that has already been properly installed and configured:

- IP address and port for the SMI-S Provider
- Username and password for a user with access to the SMI-S Provider

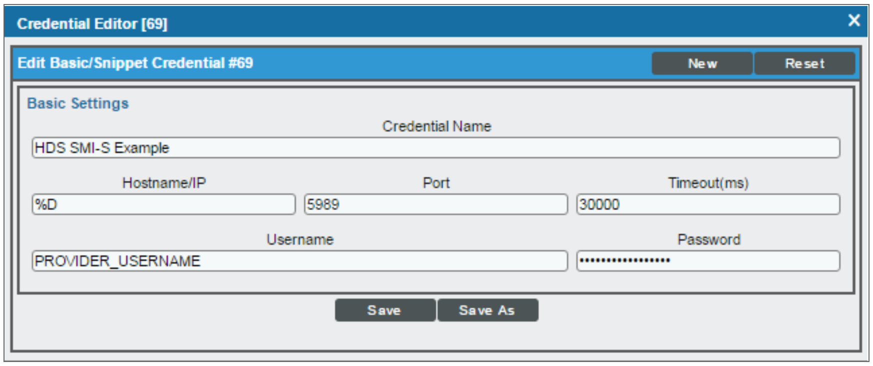
The SMI-S Provider will act as the root device during discovery by SL1.

Creating a Credential for Hitachi VSP Systems

To configure SL1 to monitor Hitachi VSP systems, you must first create a Basic/Snippet credential. This credential allows the Dynamic Applications in the *Hitachi Data Systems: VSP* PowerPack to connect with an Hitachi SMI-S Provider. An example Basic/Snippet credential that you can edit for your own use is included in the *Hitachi Data Systems: VSP* PowerPack.

To create a Basic/Snippet credential to access an Hitachi SMI-S Provider:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **HDS SMI-S Example** credential, then click its wrench icon (🔧). The **Edit Basic/Snippet Credential** modal page appears.
3. Enter values in the following fields:



Credential Name: HDS SMI-S Example

Hostname/IP: %D

Port: 5989

Timeout(ms): 30000

Username: PROVIDER_USERNAME

Password: ••••••••••••••••

- ***Credential Name***. Enter a new name for the Hitachi VSP credential.
- ***Hostname/IP***. Enter "%D".
- ***Port***. Enter "5989" for an HTTPS connection.
- ***Timeout***. Enter "30000".
- ***Username***. Enter the username for a user with access to the SMI-S Provider.
- ***Password***. Enter the password for the SMI-S Provider account username.

4. Click the **[Save As]** button.
5. When the confirmation message appears, click **[OK]**.

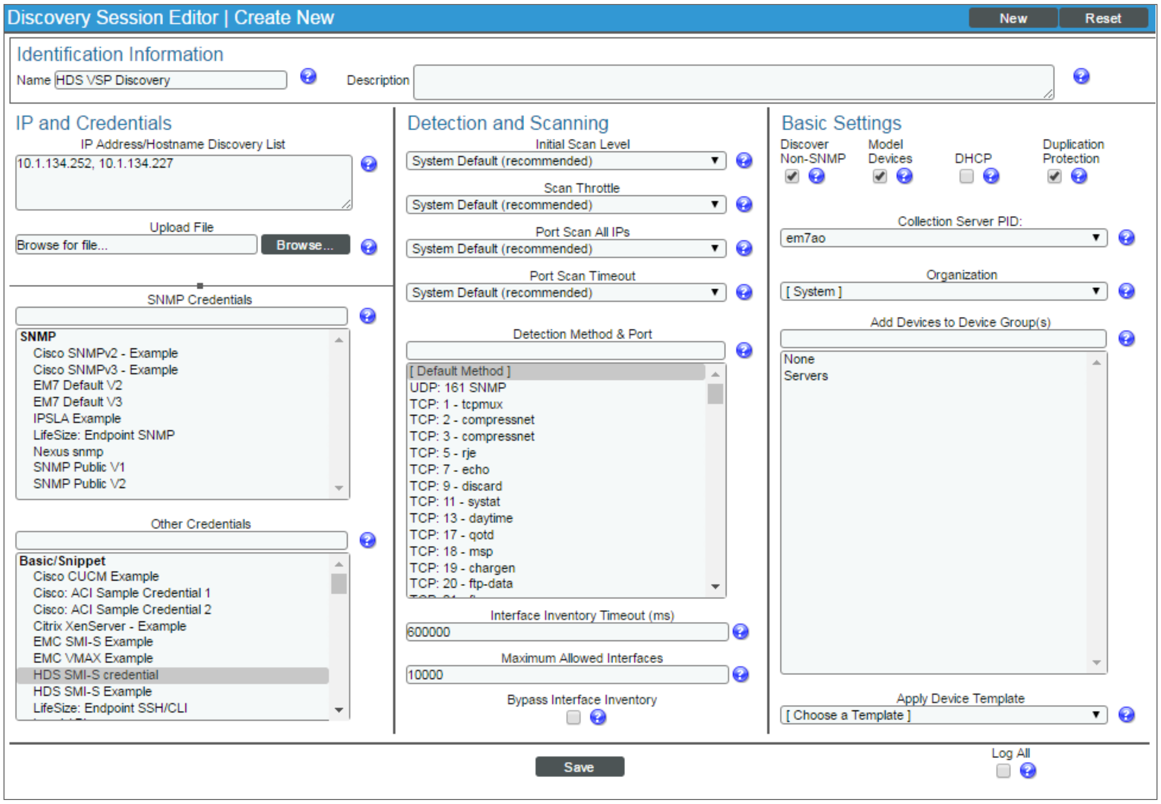
Discovering Hitachi VSP Devices

To model and monitor your Hitachi VSP system, you must first run a discovery session to discover the Hitachi SMI-S Provider. SL1 will use the Hitachi SMI-S Provider as the root device for monitoring the VSP system.

The discovery session will discover the SMI-S Provider as a pingable device using *the Basic/Snippet credential that you created*. You must then manually align the "HDS: VSP Array Discovery" Dynamic Application to the SMI-S Provider pingable device. When you do so, SL1 will discover, model, and monitor the remaining component devices in your VSP system.

To discover the Hitachi VSP system 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. On this page, define values in the following fields:



Discovery Session Editor | Create New

Identification Information

Name: HDS VSP Discovery

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.1.134.252, 10.1.134.227

Upload File: Browse for file...

Other Credentials: HDS SMI-S credential

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]

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: em7ao

Organization: [System]

Add Devices to Device Group(s):

Apply Device Template: [Choose a Template]

Log All: □

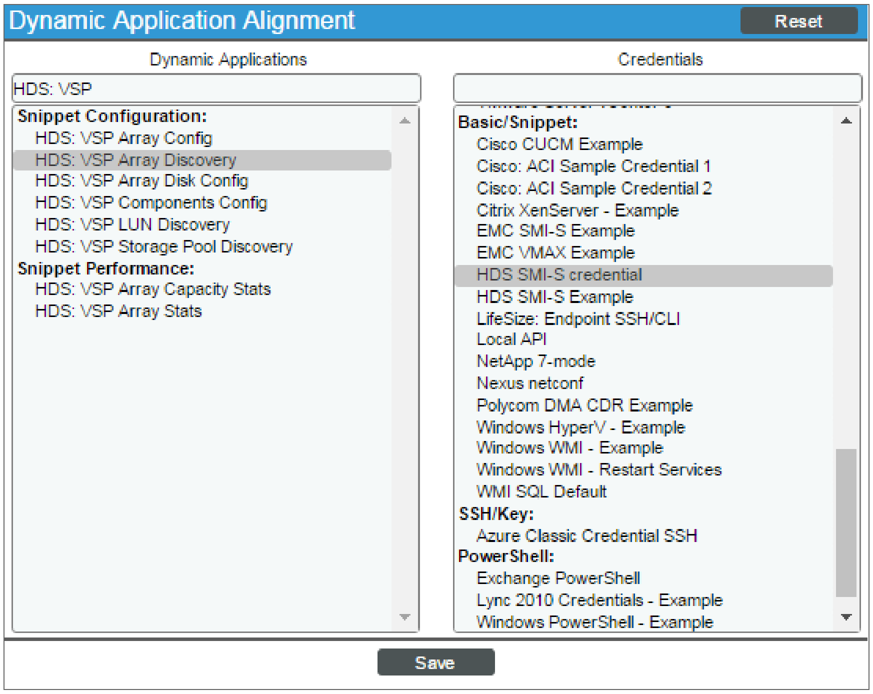
- ***IP Address Discovery List***. Enter the IP address for the SMI-S Provider.
- ***Other Credentials***. Select the Basic/Snippet credential you created for the SMI-S Provider.
- ***Discover Non-SNMP***. Select this checkbox.
- ***Model Devices***. Select this checkbox.

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 SMI-S Provider is discovered, click its device icon () to view the **Device Properties** page for the SMI-S Provider.

8. From the **Device Properties** page for the SMI-S Provider, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.

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

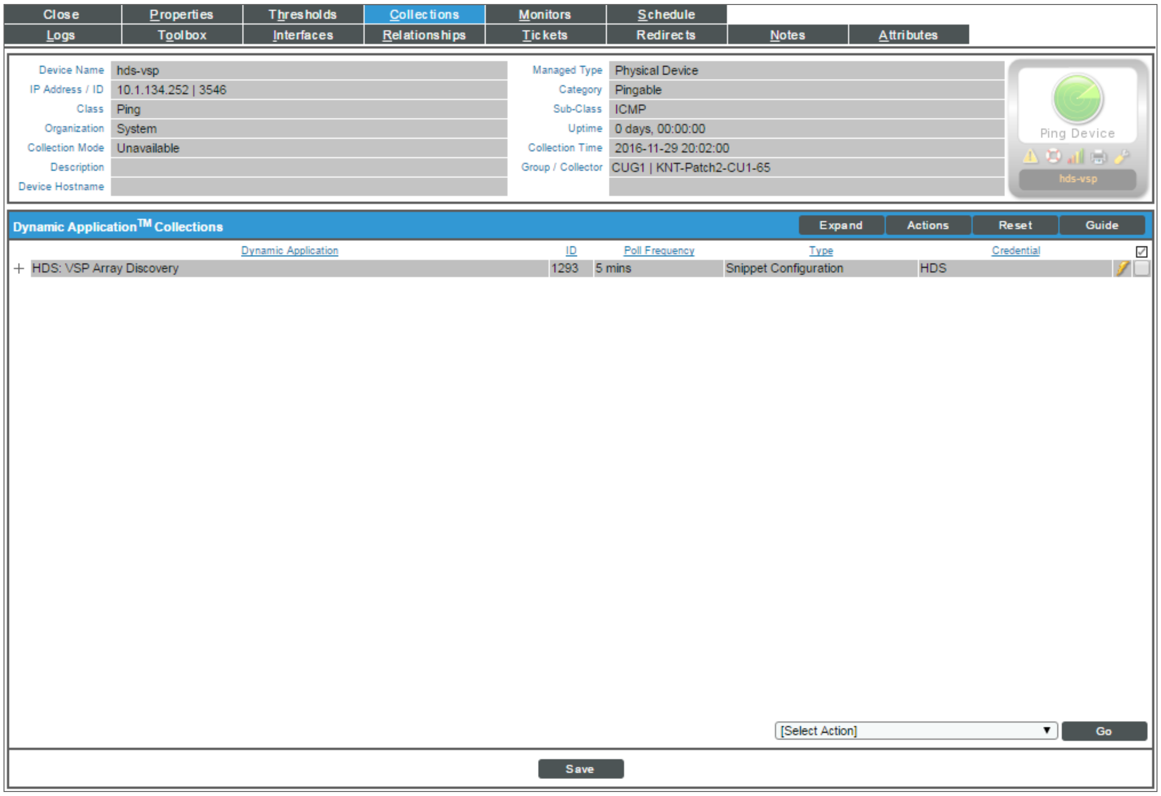


10. In the ***Dynamic Applications*** field, select *HDS: VSP Array Discovery*.

11. In the ***Credentials*** field, select the Basic/Snippet credential you configured for the SMI-S Provider.

12. Click the **[Save]** button.

13. The "HDS: VSP Array Discovery" Dynamic Application appears on the **Dynamic Application Collections** page and begins auto-aligning the other Dynamic Applications in the *Hitachi Data Systems: VSP* PowerPack to the SMI-S Provider and discovering the other component devices in the VSP system.



Device Name	hds-vsp	Managed Type	Physical Device
IP Address / ID	10.1.134.252 | 3546	Category	Pingable
Class	Ping	Sub-Class	ICMP
Organization	System	Uptime	0 days, 00:00:00
Collection Mode	Unavailable	Collection Time	2016-11-29 20:02:00
Description		Group / Collector	CUG1 | KNT-Patch2-CU1-65
Device Hostname			

Dynamic Application™ Collections

Dynamic Application	ID	Poll Frequency	Type	Credential
+ HDS: VSP Array Discovery	1293	5 mins	Snippet Configuration	HDS

NOTE: It might take several minutes after manually aligning the discovery Dynamic Application for SL1 to discover and model the remaining component devices in the VSP system.

Chapter 42

IBM: DataPower

Overview

The following sections describe how to configure and discover IBM DataPower gateways for monitoring by SL1 using the *IBM: DataPower* PowerPack:

NOTE: For more information about the *IBM: DataPower* PowerPack, see the ***Monitoring IBM DataPower Gateway*** manual.

Prerequisites for Monitoring IBM DataPower Gateways

Before you can monitor IBM DataPower gateways in SL1 using the *IBM: DataPower* PowerPack, you must first enable SNMP and configure SNMP community strings in each of the DataPower gateways that you will monitor with SL1.

Creating an SNMP Credential for IBM DataPower Gateway

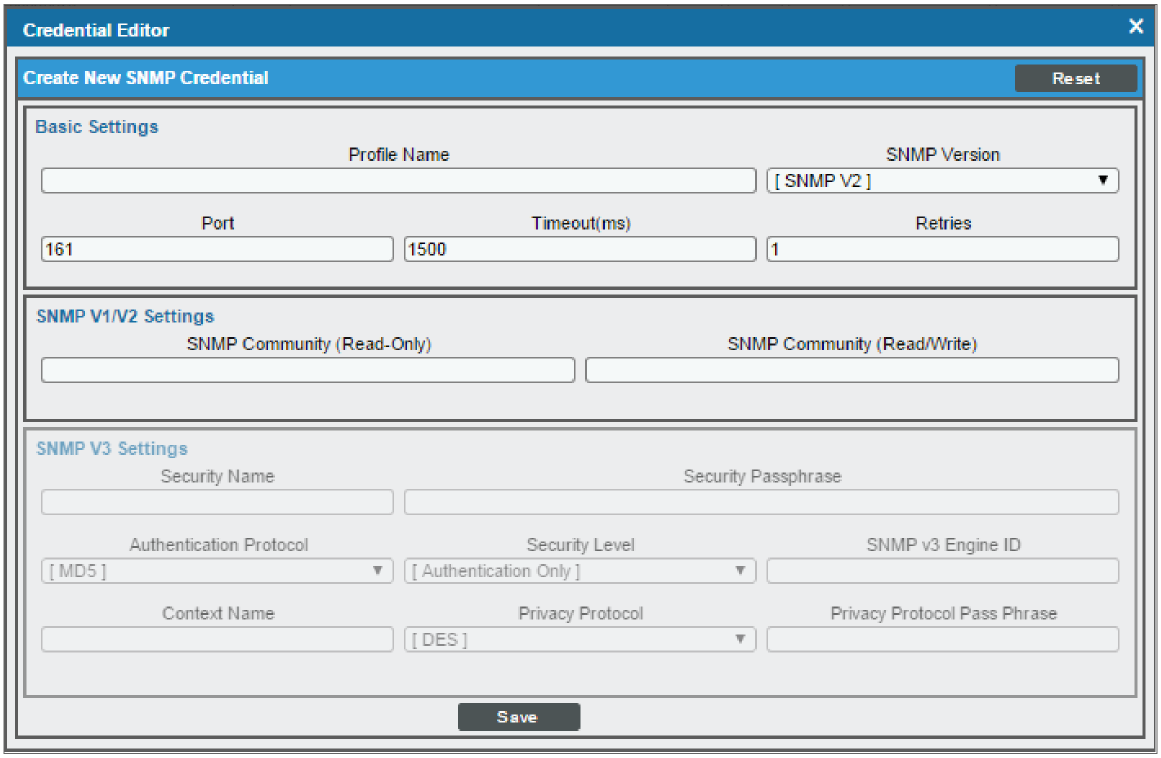
To configure SL1 to monitor IBM DataPower gateways, you must first create an SNMP credential. This credential allows the Dynamic Applications in the *IBM: DataPower* PowerPack to connect with a DataPower gateway.

To configure an SNMP credential to connect with a DataPower gateway:

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:



Credential Editor

Create New SNMP Credential

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:

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

5. In the ***SNMP Version*** field, select *SNMP V2*.

6. In the ***SNMP Community (Read Only)*** field, enter the community string for the DataPower gateway.

7. Optionally, supply values in the other fields in this page. In most cases, you can use the default values for the other fields.

8. Click the **[Save]** button.

Discovering IBM DataPower Gateways

To discover an IBM DataPower gateway:

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

2. In the **Discovery Control Panel**, click the **[Create]** button. The **Discovery Session Editor** page appears.

3. In the **Discovery Session Editor** page, complete the following fields:

    - ***Name***. Type a name for the discovery session.

- ***IP Address/Hostname Discovery List***. Type the IP address for the DataPower gateway.
- ***SNMP Credentials***. Select the SNMP credential that you created for the DataPower gateway.
- ***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 gateway device is discovered, click the device icon (🖥) to view the **Device Properties** page for the gateway device.

Chapter 43

IBM: Db2

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 and discover IBM Db2 databases for monitoring by SL1 using the *IBM: Db2* PowerPack:

> NOTE: For more information about the *IBM: Db2* PowerPack, see the ***Monitoring IBM Db2*** manual.

Prerequisites for Monitoring IBM Db2

To configure the SL1 system to monitor IBM Db2 databases using the *IBM: Db2* PowerPack, you must first perform the following prerequisites based on your operating system:

Prerequisites for Linux/Unix Users

1. Create a shell session and SSH into the Db2 database you want to monitor.
2. Create a new group to monitor by entering the following command:

```
sudo groupadd <group_name>
```

2. Create a new user for the group you created by entering the following command:

```
sudo useradd -u <user_id> -g <group_name> -m -d /home/<user_name> <user_name>
```

3. Set a password for the user you created by entering the following command:

```
sudo passwd <user_name>
```

4. Log in with the instance admin user. For example: `su - db2inst1`
5. Run the following commands:

```
db2 update database manager configuration using SYSMON_GROUP <group_name>

db2stop

db2start
```

6. Connect to your database with the following command:

```
db2 connect to <db_name>
```

7. Run the following command to grant the DATAACCESS privilege to the user:

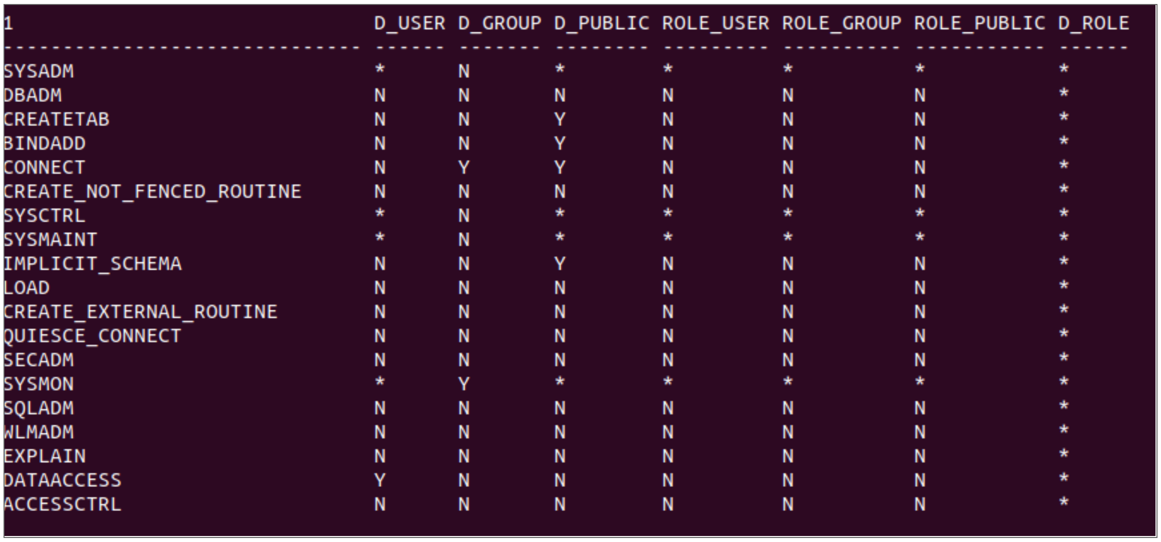
```
db2 "grant DATAACCESS ON DATABASE TO USER <user_name>"
```

8. Verify permissions with the following commands:

```
db2 connect to <db_name> user <user_name> using <user_password>

db2 "select SUBSTR(AUTHORITY,1,30), D_USER, D_GROUP, D_PUBLIC, ROLE_USER, ROLE_
GROUP, ROLE_PUBLIC, D_ROLE from table (sysproc.auth_list_authorities_for_authid
(CURRENT_USER, 'U'))"
```

> **NOTE:** Repeat steps 4 - 7 for each Db2 instance.



```
1                              D_USER D_GROUP D_PUBLIC ROLE_USER ROLE_GROUP ROLE_PUBLIC D_ROLE
------------------------------ ------ ------- -------- --------- ---------- ----------- ------
SYSADM                         *      N       *        *         *          *           *
DBADM                          N      N       N        N         N          N           *
CREATETAB                      N      N       Y        N         N          N           *
BINDADD                        N      N       Y        N         N          N           *
CONNECT                        N      Y       Y        N         N          N           *
CREATE_NOT_FENCED_ROUTINE      N      N       N        N         N          N           *
SYSCTRL                        *      N       *        *         *          *           *
SYSMAINT                       *      N       *        *         *          *           *
IMPLICIT_SCHEMA                N      N       Y        N         N          N           *
LOAD                           N      N       N        N         N          N           *
CREATE_EXTERNAL_ROUTINE        N      N       N        N         N          N           *
QUIESCE_CONNECT                N      N       N        N         N          N           *
SECADM                         N      N       N        N         N          N           *
SYSMON                         *      Y       *        *         *          *           *
SQLADM                         N      N       N        N         N          N           *
WLMADM                         N      N       N        N         N          N           *
EXPLAIN                        N      N       N        N         N          N           *
DATAACCESS                     Y      N       N        N         N          N           *
ACCESSCTRL                     N      N       N        N         N          N           *
```

NOTE: The user you create will likely need to use KornShell (for Unix systems) or Bash (for Linux systems).

If you are unsure of the shell directory, you can use the command `which ksh` to determine the KornShell directory, or `which bash` to determine the Bash directory.

After you have determined shell directory, run the following commands, replacing <*shell_directory*> with the KornShell or Bash directory:

```
sudo useradd -u <user_id> -g <group_name> -s <shell_directory> -m -d
/home/<user_name> <user_name>
```

You ***should not*** use Shell (sh) as the shell for the user. Using Shell for the user shell could result in shell-related errors appearing in the Device Log.

Prerequisites for Windows Users

NOTE: Before performing the steps for the Windows prerequisites, ensure that you have followed the steps in the *Configuring Windows Servers for Monitoring with PowerShell*section of the ***Monitoring Windows Systems with PowerShell*** manual.

Windows users will need to create a local user and group for the Db2 database. If you have already done so, proceed to ***adding the group to the instance database manager***. To create the user and group, perform the following steps:

1. Click **[Start]** and select ***Run***.
2. In the **Run** window, enter `lusrmgr.msc` and click **[OK]**.
3. In the **Local Users and Groups** pane, select the ***Users*** folder.

4. Click the ***Action*** menu and select *New User...*. Enter the new user's information in the **New User** window and click **[Create]**.
5. In the **Local Users and Groups** pane, select the ***Groups*** folder.
6. Click the ***Action*** menu and select *New Group...*. Enter the new group's information in the **New Group** window and click **[Create]**.
7. To add the new user to the group, double-click on the group name.
8. Click the **[Add...]** button under the **Members** window and enter the username. Click **[OK]**.

NOTE: You may need to add the user to the Administrators group in order to use PowerShell remoting if you don't have a PowerShell group/policy in place for non-adminstrative users.

Next, you will need to add the group you created to the instance database manager:

1. Log in to the Db2 database as the instance admin user.
2. Open the Db2 admin shell.
3. Run the following commands:

```
db2 update database manager configuration using SYSMON_GROUP <group_name>

db2stop

db2start
```

Next, you will grant the DATAACCESS privilege to the new user:

1. Log in to the Db2 database as the instance admin user.
2. Open the Db2 admin shell.
3. Run the following commands:

```
db2 connect to <database>

db2 "grant DATAACCESS on database to user <user_name>"
```

NOTE: You will need to grant this access to each database.

NOTE: Perform the steps to add the group to the instance database manager and to grant the DATAACCESS privilege for each Db2 instance that you will monitor.

Creating Credentials for IBM Db2

To monitor Db2 databases using SL1, you must create two credentials. These credentials enable SL1 to collect data from your Db2 databases. The types of credentials that are required for monitoring depend on the type of database being monitored:

- Linux and Unix users must use an ***SSH/Key credential*** and a ***SOAP/XML credential***
- Windows users must use a ***PowerShell credential*** and a ***SOAP/XML credential***

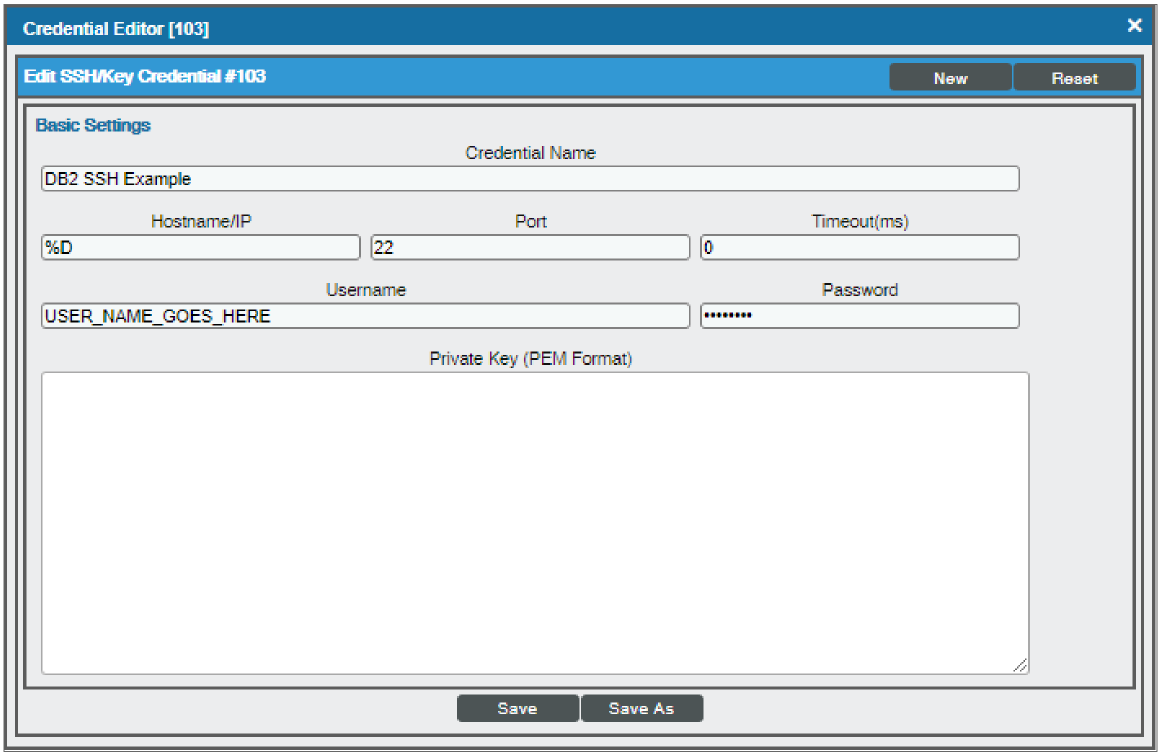
In addition, if the password has changed for the account with access to the Db2 database, you will need to update the corresponding ***Database credential***.

Creating an SSH/Key Credential (Linux and Unix Users)

Linux and Unix users must create an SSH/Key credential.

To create an SSH/Key credential :

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the wrench icon (🔧) for the "DB2 SSH Example" credential. The **Credential Editor** modal page appears:



Credential Name: DB2 SSH Example

Hostname/IP: %D

Port: 22

Timeout(ms): 0

Username: USER_NAME_GOES_HERE

Password: ••••••••

Private Key (PEM Format):

3. Supply values in the following fields:

   - ***Credential Name***. Type a new name for the credential.
   - ***Hostname/IP***. Type the IP address or hostname of the Db2 database you want to monitor.
   - ***Port***. Keep the default setting.
   - ***Timeout(ms)***. Keep the default setting.
   - ***Username***. Type the username for a user with access to the Db2 database.
   - ***Password***. Type the password for the account with access to the Db2 database.
   - ***Private Key (PEM Format)***. Optional. Use if required for SSH authentication.

NOTE: If your SSH access to the Db2 database allows you to only use a PEM key and prevents you from using a username and password, enter a PEM key in the SSH/Key credential and then include a username and password in the SOAP/XML credential instead.

4. Click the **[Save As]** button.
5. When the confirmation message appears, click **[OK]**.

NOTE: The credential ID will appear at the top of the window after it has been saved. Take note of the ID as you will need it when creating the SOAP/XML credential.

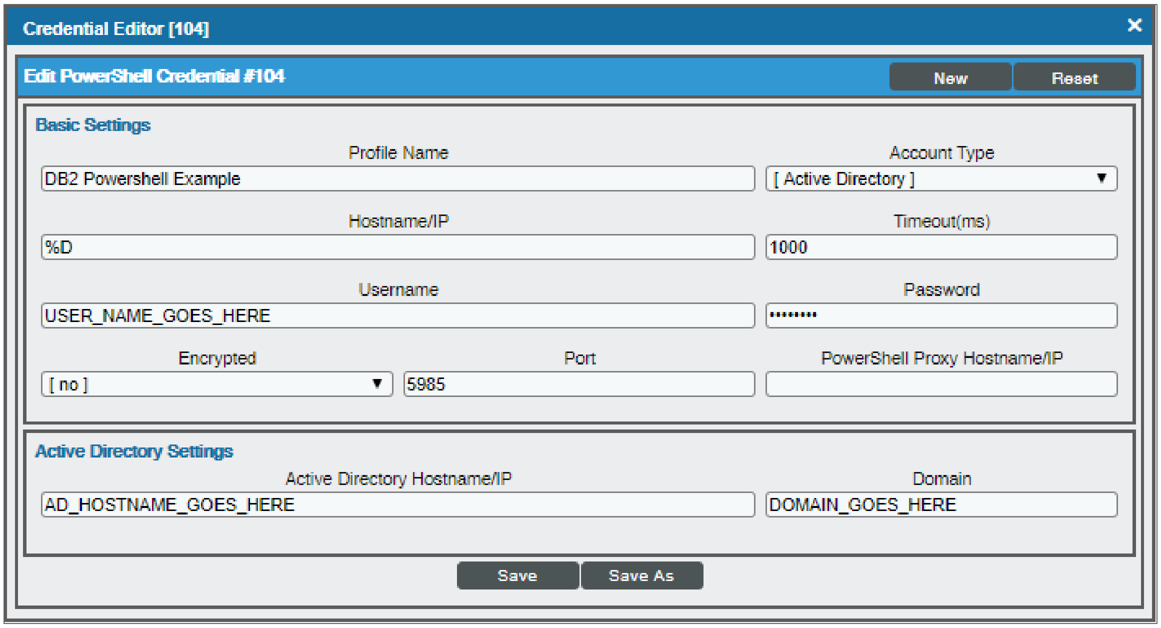
Creating a PowerShell Credential (Windows Users)

Windows users must create a PowerShell credential.

To create a PowerShell credential:

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

2. Click the wrench icon () for the "DB2 Powershell Example" credential. The **Credential Editor** modal page appears:



Basic Settings

Profile Name: DB2 Powershell Example

Account Type: [Active Directory]

Hostname/IP: %D

Timeout(ms): 1000

Username: USER_NAME_GOES_HERE

Password: ••••••••

Encrypted: [no]

Port: 5985

PowerShell Proxy Hostname/IP:

Active Directory Settings

Active Directory Hostname/IP: AD_HOSTNAME_GOES_HERE

Domain: DOMAIN_GOES_HERE

3. Supply values in the following fields:

   - ***Profile Name***. Type a new name for the credential. Can be any combination of alphanumeric characters.
   - ***Account Type***. Select the type of authentication for the username and password in this credential. Choices are:
     - *Active Directory*. On the device, Active Directory will authenticate the username and password in this credential.
     - *Local*. Local security on the device will authenticate the username and password in this credential.
   - ***Hostname/IP***. Type the IP address of the Db2 database from which you want to retrieve data, or enter the variable **%D**.
   - ***Timeout (ms)***. Type the time, in milliseconds, after which SL1 will stop trying to collect data from the authenticating server. For collection to be successful, SL1 must connect to the authenticating server, execute the PowerShell command, and receive a response within the amount of time specified in this field.

- ***Username***. Type the username for a user with access to the Db2 database to be monitored.
- ***Password***. Type the password for the user account with access to the Db2 database to be monitored.
- ***Encrypted***. Select whether SL1 will communicate with the device using an encrypted connection. Choices are:
    - *yes*. When communicating with the Windows server, SL1 will use a local user account with authentication of type "Basic Auth". You must then use HTTPS and can use a Microsoft Certificate or a self-signed certificate.
    - *no*. When communicating with the Windows server, SL1 will not encrypt the connection.
- ***Port***. Leave as default value.
- ***PowerShell Proxy Hostname/IP***. Leave this field blank.

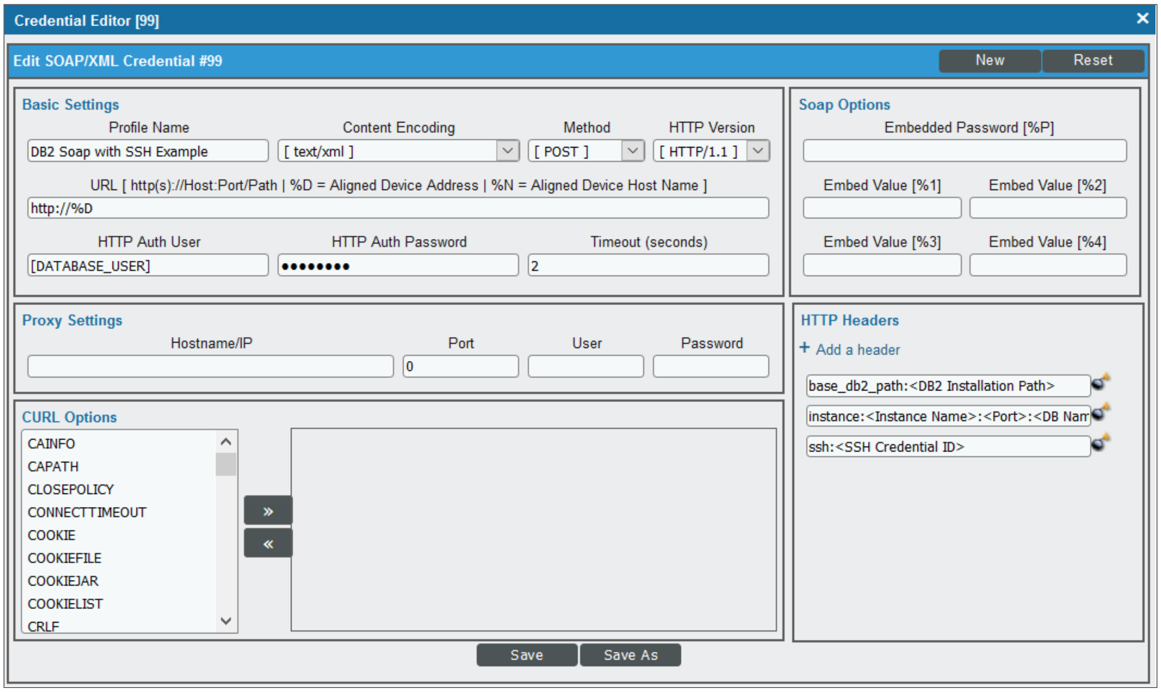
4. Click the **[Save As]** button.

Creating a SOAP/XML Credential (Linux and Unix Users)

After configuring the SSH/Key credential, you must then create a SOAP/XML credential.

To create the SOAP/XML credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the wrench icon () for either the "DB2 Soap with SSH Example" credential for Linux users. The **Credential Editor** modal page appears:



Credential Editor [99]

Edit SOAP/XML Credential #99

Basic Settings

Profile Name: DB2 Soap with SSH Example

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: http://%D

HTTP Auth User: [DATABASE_USER]

HTTP Auth Password: ••••••••

Timeout (seconds): 2

Soap Options

Embedded Password [%P]:

Embed Value [%1]:

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

Proxy Settings

Hostname/IP:

Port: 0

User:

Password:

HTTP Headers

base_db2_path:<DB2 Installation Path>

instance:<Instance Name>:<Port>:<DB Nam

ssh:<SSH Credential ID>

3. Update the values in the following fields:

Basic Settings

- ***Profile Name***. Type a new name for the credential.
- ***URL***. Leave the default value of https://%D.
- ***HTTP Auth User***. If your SSH access to the Db2 database allows you to only use a PEM key and prevents you from using a username and password, type the username for a user with access to the Db2 database in this field. Otherwise, if you are inserting the database username and password in the SSH/Key credential, leave this field blank.
- ***HTTP Auth Password***. If your SSH access to the Db2 database allows you to only use a PEM key and prevents you from using a username and password, type the password for the account with access to the Db2 database in this field. Otherwise, if you are inserting the database username and password in the SSH/Key credential, leave this field blank.

NOTE: If the ***HTTP Auth User*** and ***HTTP Auth Password*** fields are blank, then the Dynamic Applications in the *IBM: Db2* PowerPack will use the credentials provided in the SSH/Key credential.

HTTP Headers

- ***HTTP Headers***. Add the following headers by clicking ***+ Add a header***:
  - `base_db2_path:<DB2 Installation Path>`. For example: `base_db2_path:/opt/ibm/db2/V11.5`
  - `instance:<Instance Name>:<Port>:<DB Name>` For example: `instance:db2inst1:50000:ONE`
  - `instance:<Instance Name2>:<Port2>:<DB Name2>` For example: `instance:db2inst2:50000:TWO`
  - `ssh:<SSH Credential ID>`

NOTE: You can create a header for each Db2 instance you have.

NOTE: During the discovery process, these headers will either find an existing Database credential that matches the user, password, port, and default database, or it will create a new Database credential.

NOTE: By default, the SOAP/XML credential deletes any white space before and after the colon (:) in the credential headers. If you want to include paths with white spaces in the credential, surround the path with double quotes after the colon. For example: <base_db2_path:"/opt/folder name/program files">

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

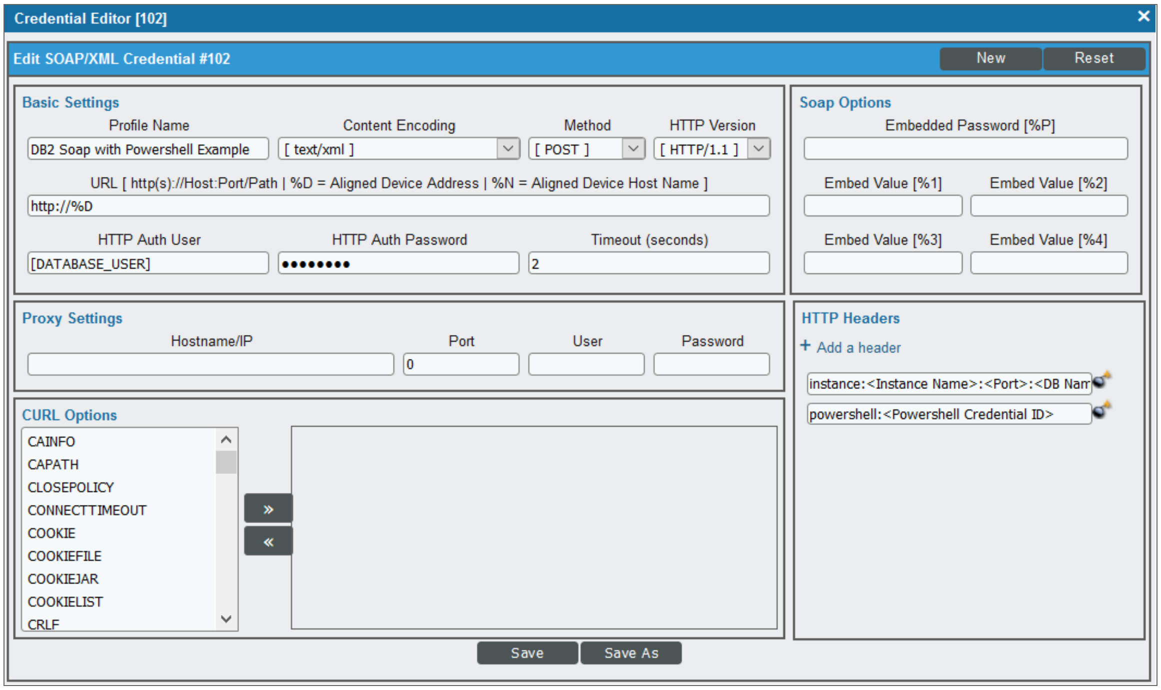
Creating a SOAP/XML Credential (Windows Users)

After configuring the PowerShell credential, you must then create a SOAP/XML credential.

To create the SOAP/XML credential:

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

2. Click the wrench icon (🔧) for either the "DB2 Soap with PowerShell Example" credential for Windows users. The **Credential Editor** modal page appears:



Credential Editor [102]

Edit SOAP/XML Credential #102

Basic Settings

Profile Name: DB2 Soap with Powershell Example

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: http://%D

HTTP Auth User: [DATABASE_USER]

HTTP Auth Password: ••••••••

Timeout (seconds): 2

Soap Options

Embedded Password [%P]:

Embed Value [%1]:

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

Proxy Settings

Hostname/IP:

Port: 0

User:

Password:

CURL Options

CAINFO
CAPATH
CLOSEPOLICY
CONNECTTIMEOUT
COOKIE
COOKIEFILE
COOKIEJAR
COOKIELIST
CRLF

HTTP Headers

+ Add a header

instance:<Instance Name>:<Port>:<DB Nam

powershell:<Powershell Credential ID>

3. Update the values in the following fields:

Basic Settings

- ***Profile Name***. Type a new name for the credential.
- ***URL***. Leave the default value of https://%D.

HTTP Headers

- *HTTP Headers*. Add the following headers by clicking **+ *Add a header***:
  - `instance:<Instance Name>:<Port>:<DB Name>` For example: `instance:db2inst1:50000:ONE`
  - `instance:<Instance Name2>:<Port2>:<DB Name2>` For example: `instance:db2inst2:50000:TWO`
  - `powershell:<PowerShell Credential ID>`

NOTE: You can create a header for each Db2 instance you have.

NOTE: During the discovery process, these headers will either find an existing Database credential that matches the user, password, port, and default database, or it will create a Database credential.

NOTE: By default, the SOAP/XML credential deletes any white space before and after the colon (:) in the credential headers. If you want to include paths with white spaces in the credential, surround the path with double quotes after the colon. For example: <base_db2_path:"/opt/folder name/program files">

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

Updating the Database Credential

If the password has changed for the account with access to the Db2 database, you must also update the corresponding Database credential in SL1. Otherwise, you can skip this section.

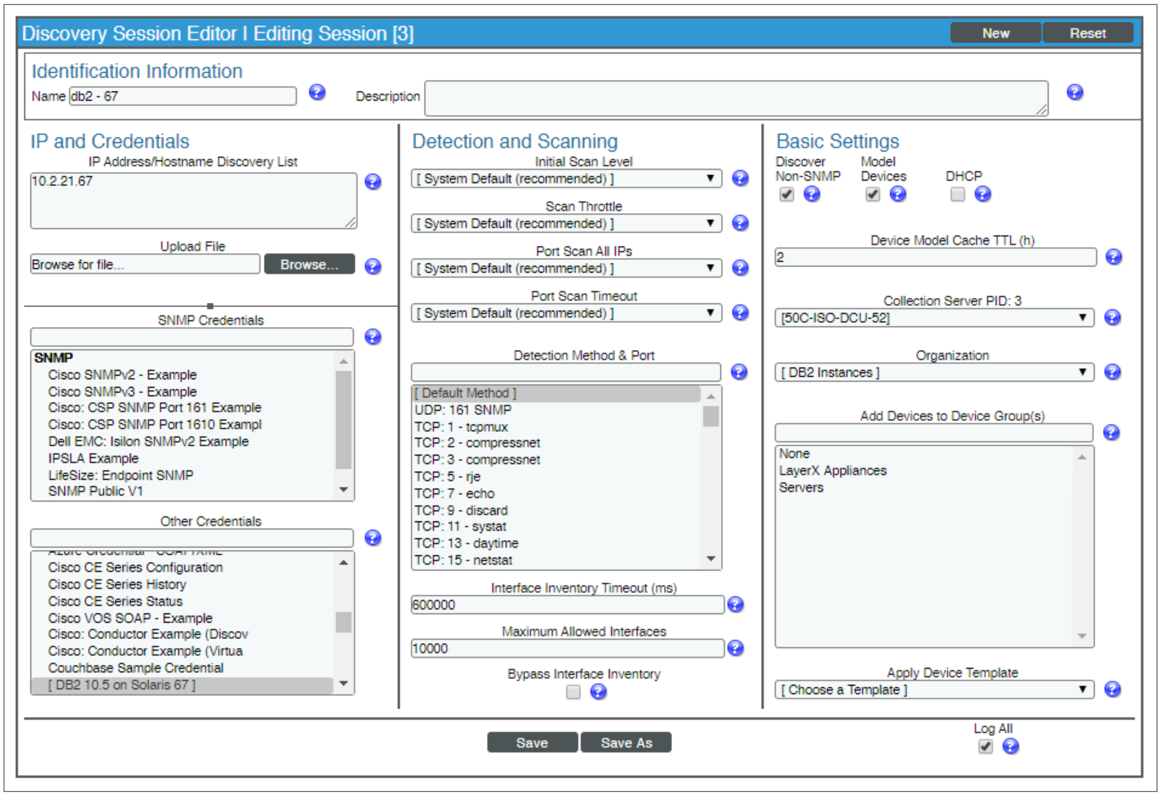
To update the Database credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. In the ***Type*** column filter, type "Database". This filters the list so that only Database credentials appear on the page.
3. Search for and locate the credential that includes the name and port of the database with the updated password, then click the credential's wrench icon (🔧).
4. On the **Credential Editor** modal page that appears, type the new password in the Password field.
5. Click **[Save]**.

Discovering IBM Db2 Component Devices

To discover an IBM Db2 database:

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



Discovery Session Editor | Editing Session [3]

Identification Information

Name: db2 - 67

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.2.21.67

Upload File: Browse for file...

SNMP Credentials:

SNMP
- Cisco SNMPv2 - Example
- Cisco SNMPv3 - Example
- Cisco: CSP SNMP Port 161 Example
- Cisco: CSP SNMP Port 1610 Exampl
- Dell EMC: Isilon SNMPv2 Example
- IPSLA Example
- LifeSize: Endpoint SNMP
- SNMP Public V1

Other Credentials:

- Azure Credential - SOAP/XML
- Cisco CE Series Configuration
- Cisco CE Series History
- Cisco CE Series Status
- Cisco VOS SOAP - Example
- Cisco: Conductor Example (Discov
- Cisco: Conductor Example (Virtua
- Couchbase Sample Credential
- [DB2 10.5 on Solaris 67]

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: 3: [50C-ISO-DCU-52]

Organization: [DB2 Instances]

Add Devices to Device Group(s):

- None
- LayerX Appliances
- Servers

Apply Device Template: [Choose a Template]

Log All: ☑

3. In the **Discovery Session Editor** page, complete the following fields:

   - ***Name***. Type a name for the discovery session.
   - ***IP Address/Hostname Discovery List***. Type the IP address for the Db2 database.
   - ***Other Credentials***. Select the SOAP/XML credential you created for the Db2 database.
   - ***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.

Verifying Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. After the discovery session has completed, go to the **Device Manager** (Registry > Devices > Device Manager) page and find the device(s) you discovered. When you have located the device in the **Device Manager**, click on its edit icon ().
2. In the **Device Properties** page, click the **[Collections]** tab.
3. All applicable Dynamic Applications for the Db2 devices 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.

To verify alignment of the IBM Db2 Dynamic Applications:

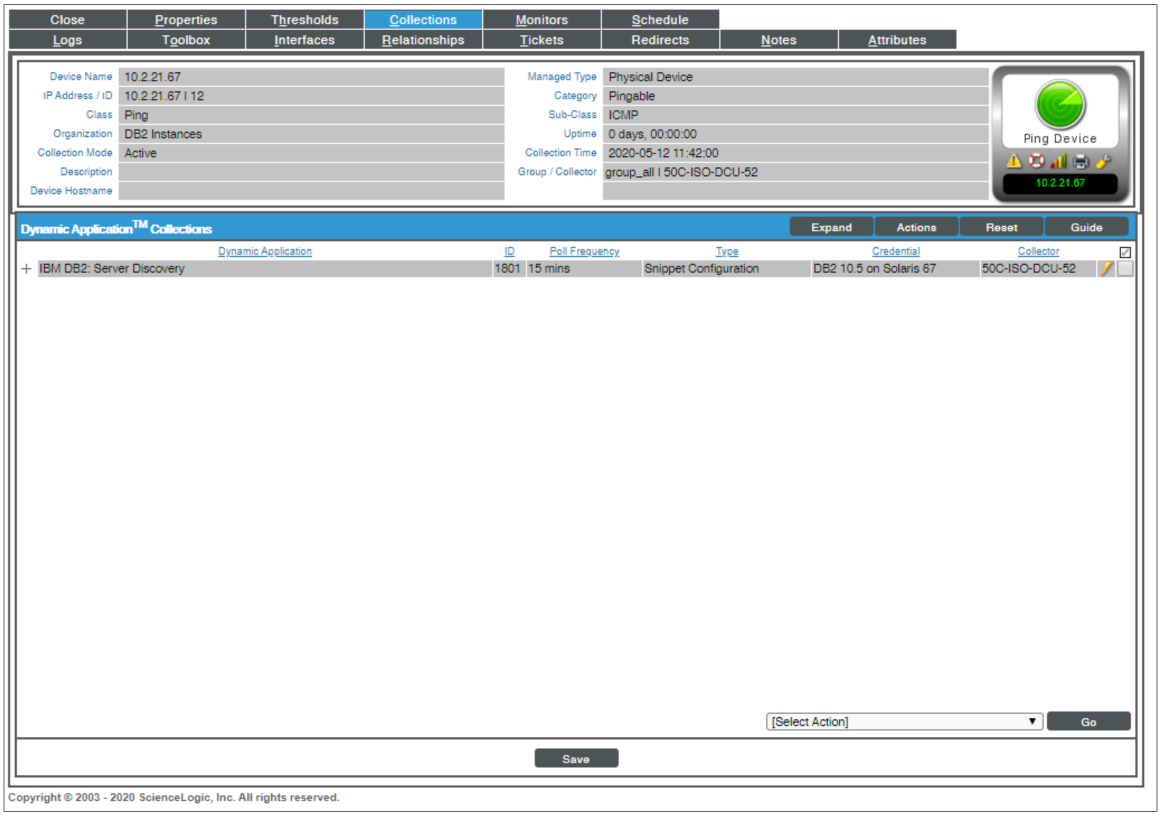
1. After discovery has completed, click the device icon for the IBM Db2 device (). From the **Device Properties** page for the IBM Db2 device, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.

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

2. All applicable Dynamic Applications are automatically aligned to the root device and component devices during discovery:

You should see the following Dynamic Application aligned to the root device:

- IBM DB2: Server Discovery



Device Name	10.2.21.67	Managed Type	Physical Device
IP Address / ID	10.2.21.67 I 12	Category	Pingable
Class	Ping	Sub-Class	ICMP
Organization	DB2 Instances	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2020-05-12 11:42:00
Description		Group / Collector	group_all I 50C-ISO-DCU-52
Device Hostname			

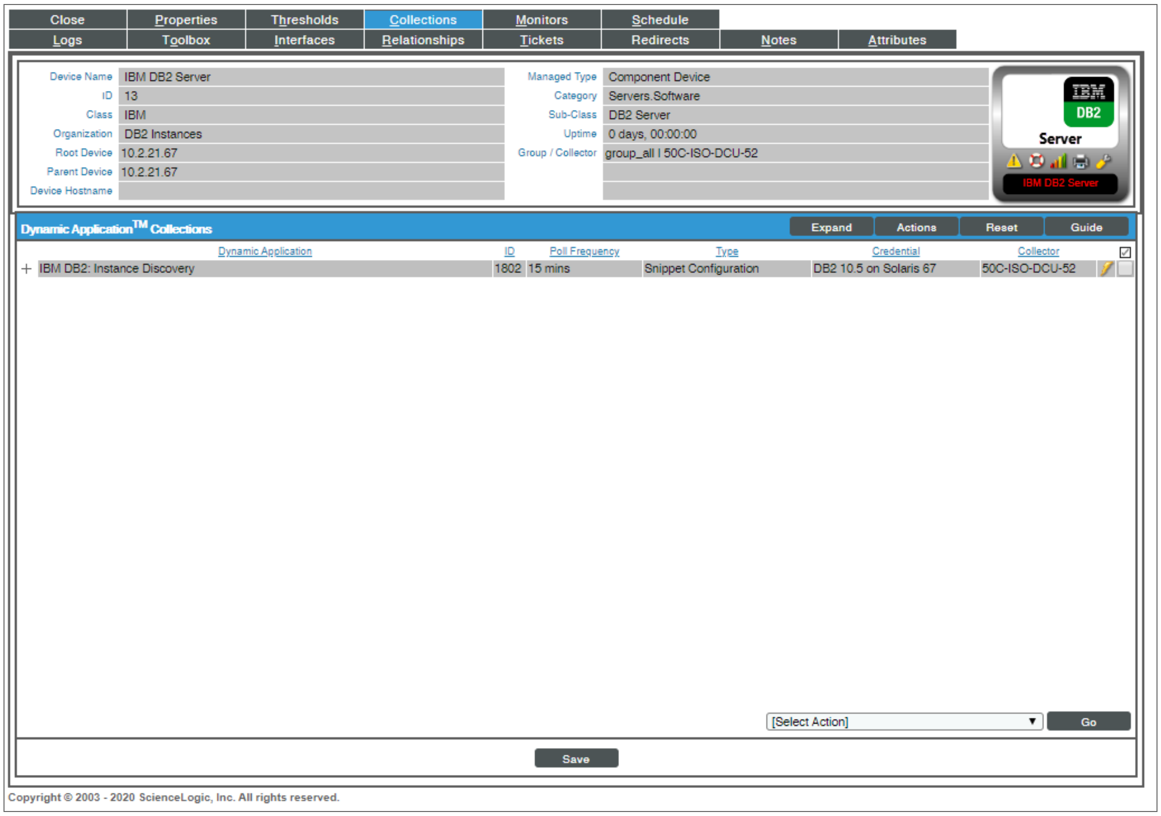
Dynamic Application™ Collections

Dynamic Application	ID	Poll Frequency	Type	Credential	Collector	☑
+ IBM DB2: Server Discovery	1801	15 mins	Snippet Configuration	DB2 10.5 on Solaris 67	50C-ISO-DCU-52	□

Copyright © 2003 - 2020 ScienceLogic, Inc. All rights reserved.

You should see the following Dynamic Application aligned to the Db2 server:

- IBM DB2: Instance Discovery



Device Name: IBM DB2 Server
ID: 13
Class: IBM
Organization: DB2 Instances
Root Device: 10.2.21.67
Parent Device: 10.2.21.67
Device Hostname:

Managed Type: Component Device
Category: Servers.Software
Sub-Class: DB2 Server
Uptime: 0 days, 00:00:00
Group / Collector: group_all I 50C-ISO-DCU-52

Dynamic Application™ Collections

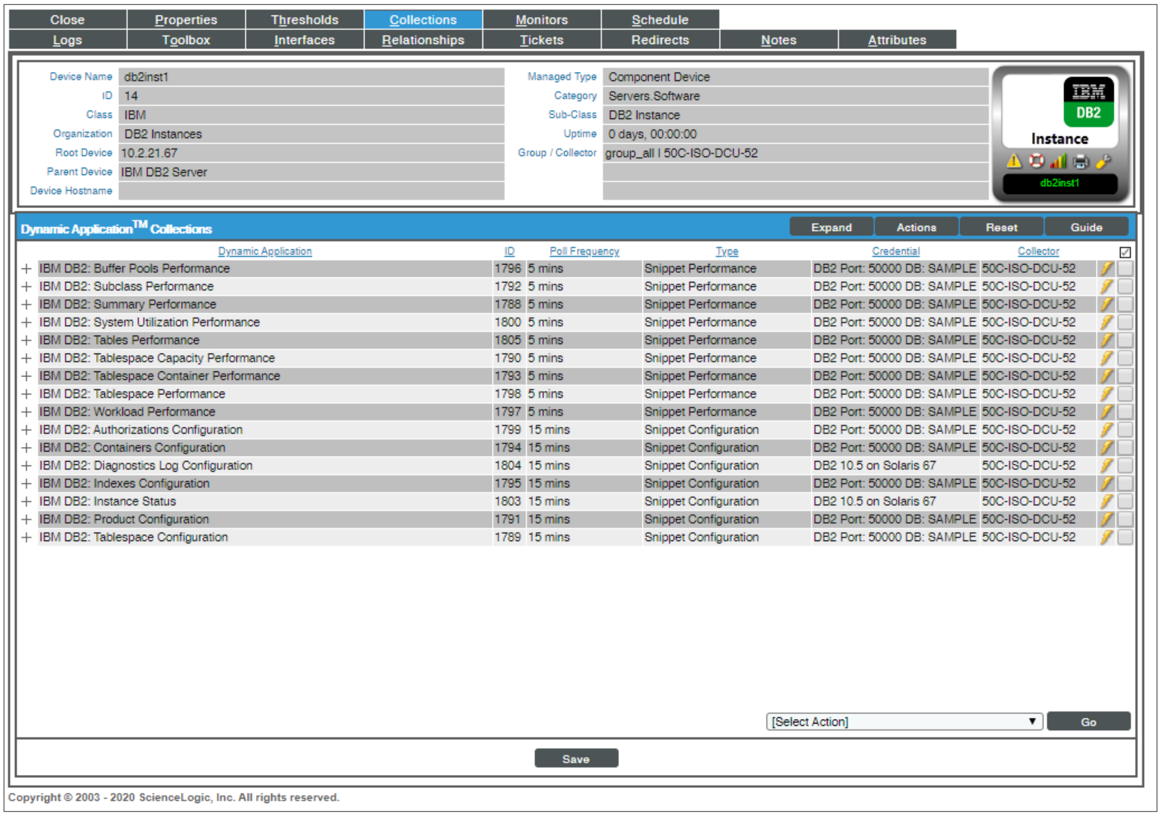
Dynamic Application	ID	Poll Frequency	Type	Credential	Collector	☑
+ IBM DB2: Instance Discovery	1802	15 mins	Snippet Configuration	DB2 10.5 on Solaris 67	50C-ISO-DCU-52	□

Copyright © 2003 - 2020 ScienceLogic, Inc. All rights reserved.

You should see the following Dynamic Application aligned to the Db2 instances:

- IBM DB2: Authorizations Configuration
- IBM DB2: Buffer Pools Performance
- IBM DB2: Containers Configuration
- IBM DB2: Diagnostics Log Configuration
- IBM DB2: Indexes Configuration
- IBM DB2: Instance Status
- IBM DB2: Product Configuration
- IBM DB2: Subclass Performance
- IBM DB2: Summary Performance
- IBM DB2: System Utilization Performance
- IBM DB2: Tables Performance
- IBM DB2: Tablespace Capacity Performance
- IBM DB2: Tablespace Configuration
- IBM DB2: Tablespace Container Performance

- IBM DB2: Tablespace Performance
- IBM DB2: Workload Performance



Device Name	db2inst1	Managed Type	Component Device
ID	14	Category	Servers.Software
Class	IBM	Sub-Class	DB2 Instance
Organization	DB2 Instances	Uptime	0 days, 00:00:00
Root Device	10.2.21.67	Group / Collector	group_all I 50C-ISO-DCU-52
Parent Device	IBM DB2 Server		
Device Hostname			

Dynamic Application™ Collections

Dynamic Application	ID	Poll Frequency	Type	Credential	Collector
IBM DB2: Buffer Pools Performance	1796	5 mins	Snippet Performance	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52
IBM DB2: Subclass Performance	1792	5 mins	Snippet Performance	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52
IBM DB2: Summary Performance	1788	5 mins	Snippet Performance	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52
IBM DB2: System Utilization Performance	1800	5 mins	Snippet Performance	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52
IBM DB2: Tables Performance	1805	5 mins	Snippet Performance	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52
IBM DB2: Tablespace Capacity Performance	1790	5 mins	Snippet Performance	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52
IBM DB2: Tablespace Container Performance	1793	5 mins	Snippet Performance	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52
IBM DB2: Tablespace Performance	1798	5 mins	Snippet Performance	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52
IBM DB2: Workload Performance	1797	5 mins	Snippet Performance	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52
IBM DB2: Authorizations Configuration	1799	15 mins	Snippet Configuration	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52
IBM DB2: Containers Configuration	1794	15 mins	Snippet Configuration	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52
IBM DB2: Diagnostics Log Configuration	1804	15 mins	Snippet Configuration	DB2 10.5 on Solaris 67	50C-ISO-DCU-52
IBM DB2: Indexes Configuration	1795	15 mins	Snippet Configuration	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52
IBM DB2: Instance Status	1803	15 mins	Snippet Configuration	DB2 10.5 on Solaris 67	50C-ISO-DCU-52
IBM DB2: Product Configuration	1791	15 mins	Snippet Configuration	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52
IBM DB2: Tablespace Configuration	1789	15 mins	Snippet Configuration	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52

NOTE: The *IBM Db2* PowerPack uses db2ilist to discover all Db2 instances, but the Dynamic Applications will be aligned to only the instances specified in the SOAP/XML credential headers.

Chapter 43

IBM: MQ

Overview

The following sections describe how to configure and discover IBM MQ messaging systems for monitoring by SL1 using the *IBM: MQ* PowerPack:

NOTE: For more information about the *IBM: MQ* PowerPack, see the ***Monitoring IBM MQ*** manual.

Prerequisites for Monitoring IBM MQ

To configure the SL1 system to monitor IBM MQ messaging systems using the *IBM: MQ* PowerPack, you must first perform the following:

- ***Install the IBM MQ PowerShell Snap-in for Monitoring on Windows Servers***
- Give all users the "mgm" group permission

Installing the IBM MQ PowerShell Snap-In for Monitoring on Windows Servers

NOTE: Users monitoring MQ on Linux servers do not need to perform these steps.

NOTE: On 64-bit versions of Microsoft Windows, both 32-bit and 64-bit versions of Windows PowerShell are installed. SL1's collection processes using Windows PowerShell will default to using the version of powershell.exe whose folder exists first in the PATH environment variable. Because this will vary from system to system, these steps ensure the WebSphereMQ.dll file is registered for both Windows PowerShell environments.

1. Download the Windows PowerShell library package (mo74.zip) for IBM MQ from the following location: https://www.ibm.com/support/pages/mo74-websphere-mq-windows-powershell-library#:~:text=Download%20Description,queue%20managers%20from%20the%20PowerShell
2. Extract the contents of the zip file to your Windows server, and find the "manual" subfolder from the extracted files (under the mo74_v2.0.1_x86_x64 folder). Create a new folder on your desktop and move the files in the "manual" subfolder to that folder.
3. Register the IBM WebSphere MQ library for use by both 32-bit and 64-bit Windows PowerShell. To do this:

   - Start a 32-bit Windows PowerShell console window (this will be the Windows PowerShell (x86) application if running on a 64-bit version of Microsoft Windows) using "Run as adminstrator", run the following:

   ```
   %WINDIR%\Microsoft.NET\Framework\v4.0.30319\installutil <Directory where
   WebsphereMQ.dll resides>\WebSphereMQ.dll
   ```

   - Start a 64-bit Windows PowerShell console window (this will be the Windows PowerShell application without (x86) in its program name on a 64-bit version of Microsoft Windows) using "Run as adminstrator" and run the following:

   ```
   %WINDIR%\Microsoft.NET\Framework64\v4.0.30319\installutil <Directory where
   WebsphereMQ.dll resides>\WebSphereMQ.dll
   ```

4. Open your Windows PowerShell console and add the WebSphere MQ for PowerShell snap-in by running the following command:

   ```
   Add-PSSnapin IBM.PowerShell.WebSphereMQ
   ```

Creating a PowerShell Credential for IBM MQ on Windows Systems

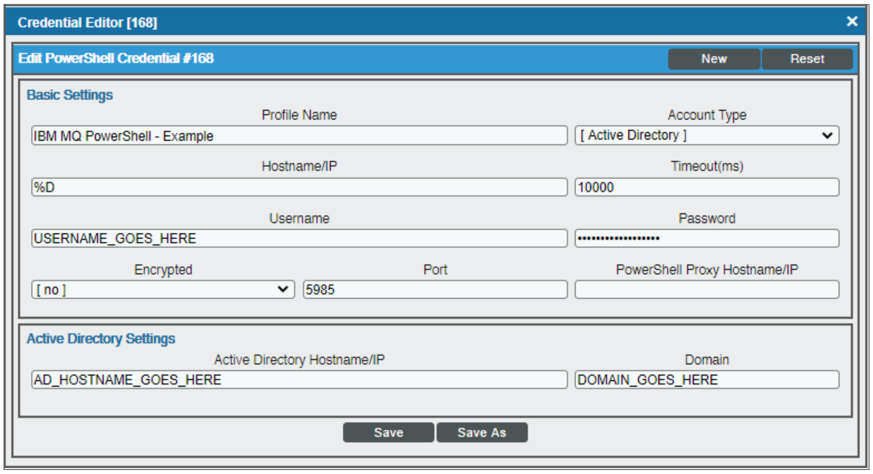
To configure SL1 to monitor IBM MQ messaging systems on Windows systems, you must first create a PowerShell credential. This credential allows the Dynamic Applications in the *IBM: MQ* PowerPack to connect with an IBM MQ system.

The PowerPack includes an example PowerShell credential that you can edit for your own use.

To configure a PowerShell credential to access an IBM MQ system:

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

2. Locate the **IBM MQ PowerShell - Example** credential, then click its wrench icon (). The **Edit PowerShell Credential** modal page appears:



Profile Name: IBM MQ PowerShell - Example
Account Type: [Active Directory]
Hostname/IP: %D
Timeout(ms): 10000
Username: USERNAME_GOES_HERE
Password: ••••••••••••••••••
Encrypted: [no]
Port: 5985
PowerShell Proxy Hostname/IP:
Active Directory Hostname/IP: AD_HOSTNAME_GOES_HERE
Domain: DOMAIN_GOES_HERE

3. Complete the following fields:

   - ***Credential Name***. Type a name for the IBM MQ credential.
   - ***Hostname/IP***. Leave at the default value of '%D'.
   - ***Username***. Type the username for a user with administrator access to the IBM MQ messaging system.
   - ***Password***. Type the password for the IBM MQ system account username.

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

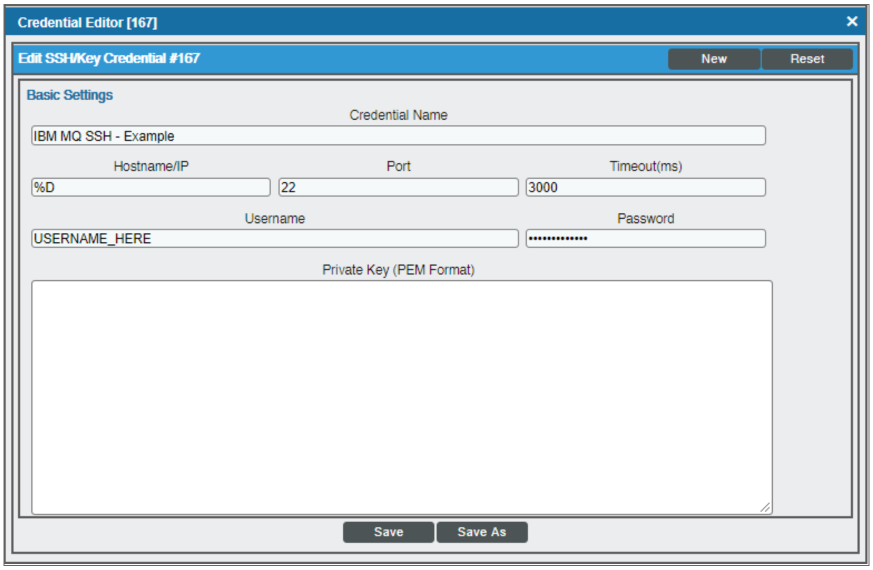
Creating an SSH/Key Credential for IBM MQ on Linux Systems

To configure SL1 to monitor IBM MQ messaging systems on Linux systems, you must first create an SSH/Key credential. This credential allows the Dynamic Applications in the *IBM: MQ* PowerPack to connect with an IBM MQ system.

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

To configure an SSH/Key credential to access an IBM MQ system:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **IBM MQ SSH - Example** credential, then click its wrench icon (🔧). The **Edit SSH/Key Credential** modal page appears:



Credential Name: IBM MQ SSH - Example

Hostname/IP: %D

Port: 22

Timeout(ms): 3000

Username: USERNAME_HERE

Password: ••••••••••••••

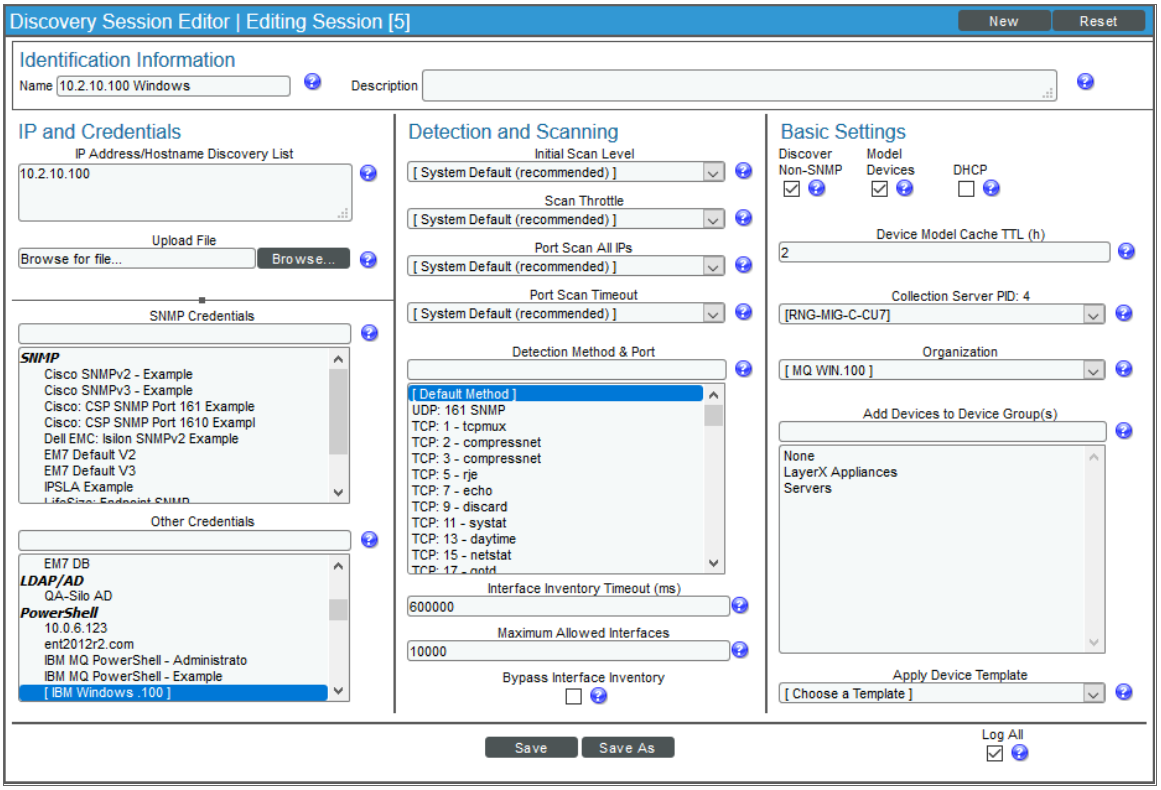
Private Key (PEM Format):

3. Complete the following fields:
   - ***Credential Name***. Type a name for the IBM MQ credential.
   - ***Hostname/IP***. Leave at the default value of '%D'.
   - ***Username***. Type the username for a user with administrator access, and who is a member of the "mgm" group, to the IBM MQ messaging system.
   - ***Password***. Type the password for the IBM MQ system account username.
4. Click the **[Save As]** button.

Discovering IBM MQ Component Devices

To discover an IBM MQ messaging system:

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



Discovery Session Editor | Editing Session [5]

Identification Information

Name: 10.2.10.100 Windows

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.2.10.100

Upload File: Browse for file...

SNMP Credentials:

- *SNMP*
  - Cisco SNMPv2 - Example
  - Cisco SNMPv3 - Example
  - Cisco: CSP SNMP Port 161 Example
  - Cisco: CSP SNMP Port 1610 Exampl
  - Dell EMC: Isilon SNMPv2 Example
  - EM7 Default V2
  - EM7 Default V3
  - IPSLA Example

Other Credentials:

- EM7 DB
- *LDAP/AD*
  - QA-Silo AD
- *PowerShell*
  - 10.0.6.123
  - ent2012r2.com
  - IBM MQ PowerShell - Administrato
  - IBM MQ PowerShell - Example
  - [IBM Windows .100]

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: 4: [RNG-MIG-C-CU7]

Organization: [MQ WIN.100]

Add Devices to Device Group(s):

- None
- LayerX Appliances
- Servers

Apply Device Template: [Choose a Template]

Log All: ☑

3. In the **Discovery Session Editor** page, complete the following fields:

   - ***Name***. Type a name for the discovery session.
   - ***IP Address/Hostname Discovery List***. Type the IP address for the IBM MQ messaging system.
   - ***Other Credentials***. Select the PowerShell or SSH/Key credential you created for the IBM MQ messaging system.
   - ***Discover Non-SNMP***. Select this checkbox.
   - ***Model Devices***. Select this checkbox.

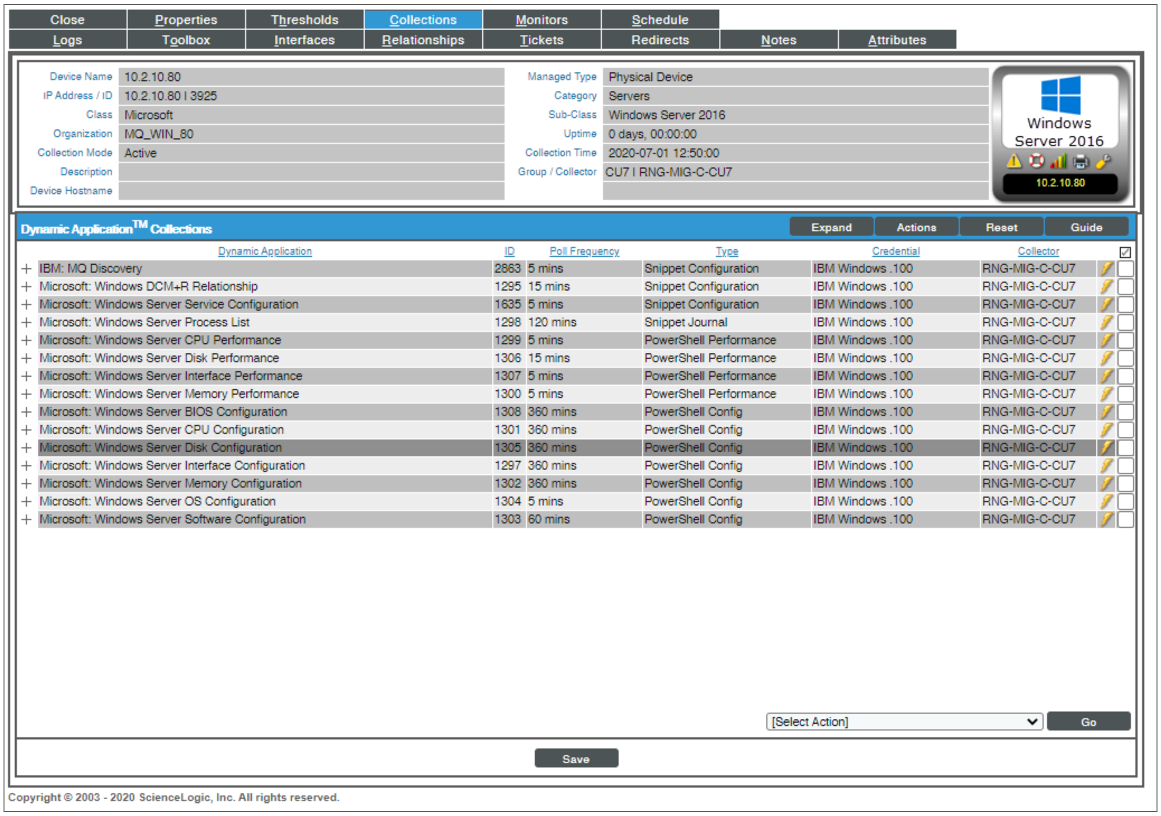
4. Optionally, you can enter values in the other fields on this page. For more information about the other fields on this page, see the ***Discovery & Credentials*** manual.
5. Click the **[Save]** button to save the discovery session and then close the **Discovery Session Editor** window.
6. The discovery 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.

Verifying Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. After discovery has completed, click the device icon for the IBM MQ device (). From the **Device Properties** page for the IBM MQ device, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. All applicable Dynamic Applications for the device 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	10.2.10.80	Managed Type	Physical Device
IP Address / ID	10.2.10.80 I 3925	Category	Servers
Class	Microsoft	Sub-Class	Windows Server 2016
Organization	MQ_WIN_80	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2020-07-01 12:50:00
Description		Group / Collector	CU7 I RNG-MIG-C-CU7
Device Hostname			

Dynamic Application™ Collections

	Dynamic Application	ID	Poll Frequency	Type	Credential	Collector	☑
+	IBM: MQ Discovery	2863	5 mins	Snippet Configuration	IBM Windows .100	RNG-MIG-C-CU7	□
+	Microsoft: Windows DCM+R Relationship	1295	15 mins	Snippet Configuration	IBM Windows .100	RNG-MIG-C-CU7	□
+	Microsoft: Windows Server Service Configuration	1635	5 mins	Snippet Configuration	IBM Windows .100	RNG-MIG-C-CU7	□
+	Microsoft: Windows Server Process List	1298	120 mins	Snippet Journal	IBM Windows .100	RNG-MIG-C-CU7	□
+	Microsoft: Windows Server CPU Performance	1299	5 mins	PowerShell Performance	IBM Windows .100	RNG-MIG-C-CU7	□
+	Microsoft: Windows Server Disk Performance	1306	15 mins	PowerShell Performance	IBM Windows .100	RNG-MIG-C-CU7	□
+	Microsoft: Windows Server Interface Performance	1307	5 mins	PowerShell Performance	IBM Windows .100	RNG-MIG-C-CU7	□
+	Microsoft: Windows Server Memory Performance	1300	5 mins	PowerShell Performance	IBM Windows .100	RNG-MIG-C-CU7	□
+	Microsoft: Windows Server BIOS Configuration	1308	360 mins	PowerShell Config	IBM Windows .100	RNG-MIG-C-CU7	□
+	Microsoft: Windows Server CPU Configuration	1301	360 mins	PowerShell Config	IBM Windows .100	RNG-MIG-C-CU7	□
+	Microsoft: Windows Server Disk Configuration	1305	360 mins	PowerShell Config	IBM Windows .100	RNG-MIG-C-CU7	□
+	Microsoft: Windows Server Interface Configuration	1297	360 mins	PowerShell Config	IBM Windows .100	RNG-MIG-C-CU7	□
+	Microsoft: Windows Server Memory Configuration	1302	360 mins	PowerShell Config	IBM Windows .100	RNG-MIG-C-CU7	□
+	Microsoft: Windows Server OS Configuration	1304	5 mins	PowerShell Config	IBM Windows .100	RNG-MIG-C-CU7	□
+	Microsoft: Windows Server Software Configuration	1303	60 mins	PowerShell Config	IBM Windows .100	RNG-MIG-C-CU7	□

Copyright © 2003 - 2020 ScienceLogic, Inc. All rights reserved.

You should see the following Dynamic Applications aligned to the IBM MQ root device:

- IBM: MQ Discovery

You should see the following Dynamic Applications aligned to the IBM MQ server:

- IBM: MQ Queue Manager Discovery

You should see the following Dynamic Applications aligned to the IBM MQ queue managers:

- IBM: MQ Cluster Channel Configuration

NOTE: For Windows users, in the "IBM: MQ Cluster Channel Configuration" Dynamic Application, when a channel is configured with a cluster and that cluster is deleted, the status for that cluster cannot be returned.

NOTE: For Windows users, in the "IBM: MQ Cluster Channel Configuration" Dynamic Application, the "CLUSSDRA" and "CLUSSDRB" are shown as "CLUSSDR".

- IBM: MQ Channel Configuration
- IBM: MQ Queue Discovery

NOTE: For Windows users, the "IBM: MQ Discovery" Dynamic Application currently does not return "Connections", "Parent Queue Manager", or "Start Date" metrics. On some MQ installations, SL1 may be unable to collect the "Standby Host" property.

- IBM: MQ Queue Manager Configuration

NOTE: For Windows users, the "IBM: MQ Queue Manager Configuration" Dynamic Application currently does not return "Connections", "Parent Queue Manager", or "Start Date" metrics.

You should see the following Dynamic Applications aligned to the IBM MQ queues:

- IBM: MQ Queue Configuration
- IBM: MQ Queue Performance

If the listed Dynamic Applications have not been automatically aligned during discovery, you can align them manually. To do so, perform the following steps:

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 credential specified in the table.
4. Click the **[Save]** button.
5. Repeat steps 1-4 for the other unaligned Dynamic Applications.

Configuring the IBM: MQ Queue Discovery Snippet

The "IBM: MQ Queue Discovery" Dynamic Application snippet allows you to customize the list of queue names and types of queues that SL1 will discover. Up to 20 queue names can be specified, and those names will be discovered under each queue manager where they are found.

For specifying queue types, an integer can be specified as one item in the list, and the allowed values for type are:

1 : Dead letter queue will be discovered

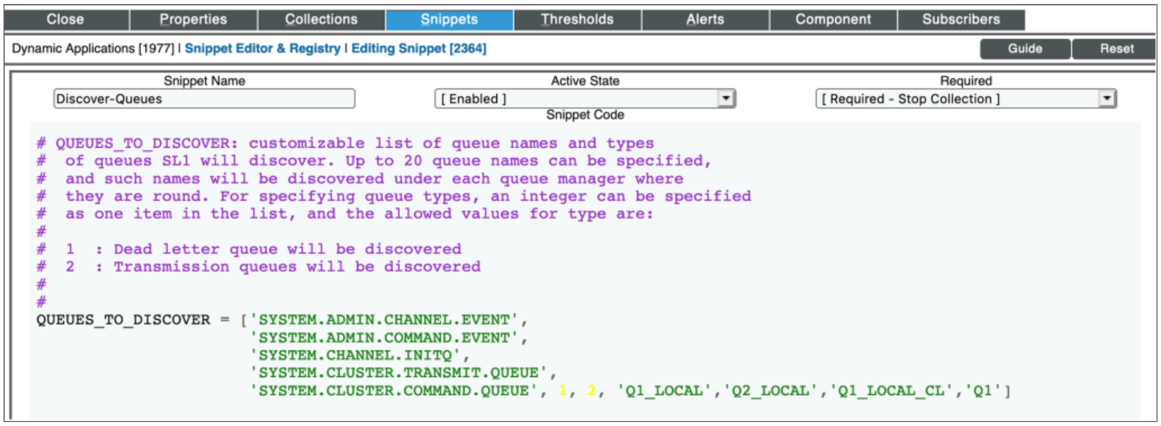
2 : Transmission queues will be discovered

To edit the snippet:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
2. Find the "IBM: MQ Discovery" Dynamic Application and click its wrench icon (🔧).
3. In the **Dynamic Applications Properties Editor**, click the **[Snippets]** tab.
4. In the **Dynamic Applications Snippet Editor & Registry** page, click the wrench icon (🔧) of the "Discover-QueueManagers" snippet.
5. The content of the snippet will appear. Add the following text to the snippet to customize the list of queue names and queue types that can be discovered:

   ```
   QUEUES_TO_DISCOVER = ['<queue name>','<queue name>','<queue type>']
   ```

   Use commas to separate queue names and queue types.


Close
Properties
Collections
Snippets
Thresholds
Alerts
Component
Subscribers
Dynamic Applications [1977] | Snippet Editor & Registry | Editing Snippet [2364]
Guide
Reset

Snippet Name: Discover-Queues

Active State: [Enabled]

Required: [Required - Stop Collection]

Snippet Code

```
# QUEUES_TO_DISCOVER: customizable list of queue names and types
#  of queues SL1 will discover. Up to 20 queue names can be specified,
#  and such names will be discovered under each queue manager where
#  they are round. For specifying queue types, an integer can be specified
#  as one item in the list, and the allowed values for type are:
#
#  1  : Dead letter queue will be discovered
#  2  : Transmission queues will be discovered
#
#
QUEUES_TO_DISCOVER = ['SYSTEM.ADMIN.CHANNEL.EVENT',
                      'SYSTEM.ADMIN.COMMAND.EVENT',
                      'SYSTEM.CHANNEL.INITQ',
                      'SYSTEM.CLUSTER.TRANSMIT.QUEUE',
                      'SYSTEM.CLUSTER.COMMAND.QUEUE', 1, 2, 'Q1_LOCAL','Q2_LOCAL','Q1_LOCAL_CL','Q1']
```

Configuring the IBM: MQ Error Log Configuration Snippet

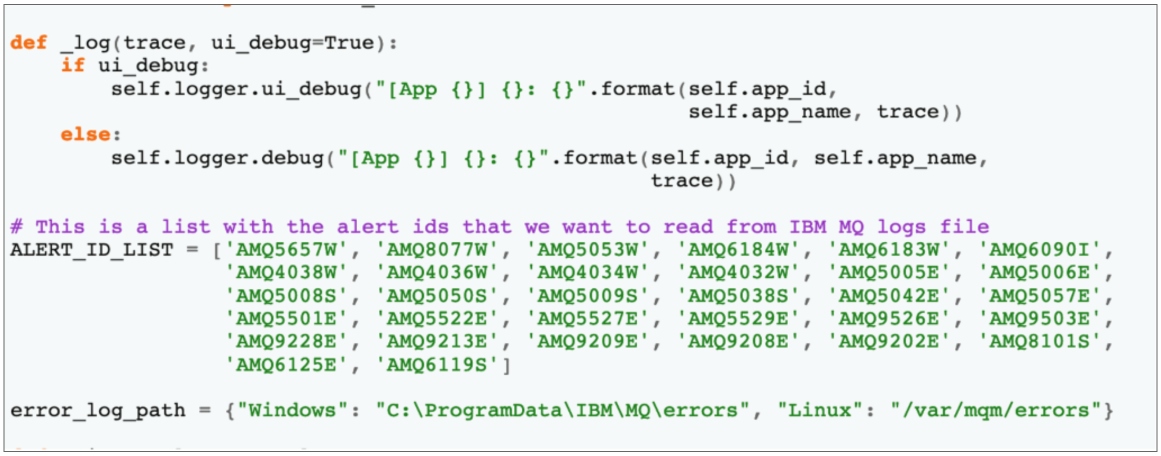
By default, only some errors are monitored and alerted in SL1. The IDs of the errors supported can be found in the snippet of the "IBM: MQ Error Log Configuration" Dynamic Application. You can add other error messages by adding the alert ID to the ALERT_ID_LIST list in the snippet.

To edit the snippet:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
2. Find the "IBM: MQ Error Log Configuration" Dynamic Application and click its wrench icon (🔧).
3. In the **Dynamic Applications Properties Editor**, click the **[Snippets]** tab.

4. In the **Dynamic Applications Snippet Editor & Registry** page, click the wrench icon (🔧) of the "Get-ErrorLogRecords" snippet.

5. The content of the snippet will appear. Add the alert IDs you want added to the `ALERT_ID_LIST` in the snippet:



```
def _log(trace, ui_debug=True):
    if ui_debug:
        self.logger.ui_debug("[App {}] {}: {}".format(self.app_id,
                                                       self.app_name, trace))
    else:
        self.logger.debug("[App {}] {}: {}".format(self.app_id, self.app_name,
                                                    trace))

# This is a list with the alert ids that we want to read from IBM MQ logs file
ALERT_ID_LIST = ['AMQ5657W', 'AMQ8077W', 'AMQ5053W', 'AMQ6184W', 'AMQ6183W', 'AMQ6090I',
                 'AMQ4038W', 'AMQ4036W', 'AMQ4034W', 'AMQ4032W', 'AMQ5005E', 'AMQ5006E',
                 'AMQ5008S', 'AMQ5050S', 'AMQ5009S', 'AMQ5038S', 'AMQ5042E', 'AMQ5057E',
                 'AMQ5501E', 'AMQ5522E', 'AMQ5527E', 'AMQ5529E', 'AMQ9526E', 'AMQ9503E',
                 'AMQ9228E', 'AMQ9213E', 'AMQ9209E', 'AMQ9208E', 'AMQ9202E', 'AMQ8101S',
                 'AMQ6125E', 'AMQ6119S']

error_log_path = {"Windows": "C:\ProgramData\IBM\MQ\errors", "Linux": "/var/mqm/errors"}
```

Chapter 44

IBM: SVC

Overview

The following sections describe how to configure and discover IBM SVC systems for monitoring by SL1 using the *IBM: SVC* PowerPack:

> **NOTE:** For more information about the *IBM: SVC* PowerPack, see the ***Monitoring IBM SVC*** manual.

Prerequisites for Monitoring IBM SVC

To configure the SL1 system to monitor IBM SVC systems using the *IBM: SVC* PowerPack, you must first have the following information about an IBM SMI-S Provider that has already been properly installed and configured:

- The username and password for a user with access to the SMI-S Provider
- IP address and port for the SMI-S Provider

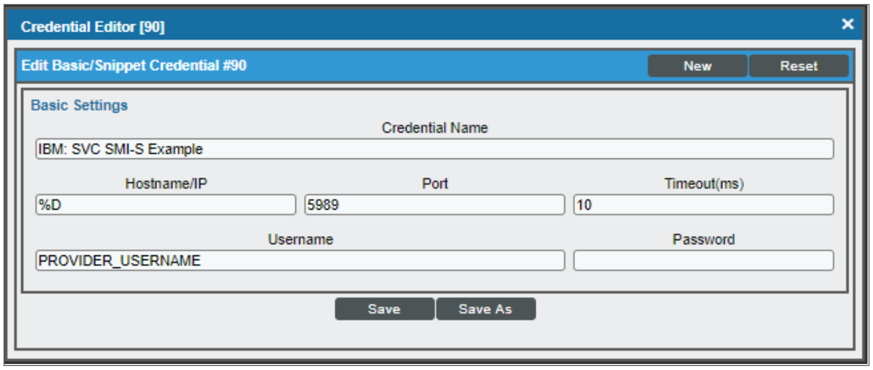
Creating a Basic/Snippet Credential for IBM SVC

To configure SL1 to monitor IBM SVC systems, you must first create a Basic/Snippet credential. This credential allows the Dynamic Applications in the *IBM: SVC* PowerPack to connect with an IBM SMI-S Provider.

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

To configure a Basic/Snippet credential to access an IBM SMI-S Provider:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **IBM: SVC SMI-S Example** credential, then click its wrench icon (🔧). The **Edit Basic/Snippet Credential** modal page appears:



Credential Name: IBM: SVC SMI-S Example

Hostname/IP: %D

Port: 5989

Timeout(ms): 10

Username: PROVIDER_USERNAME

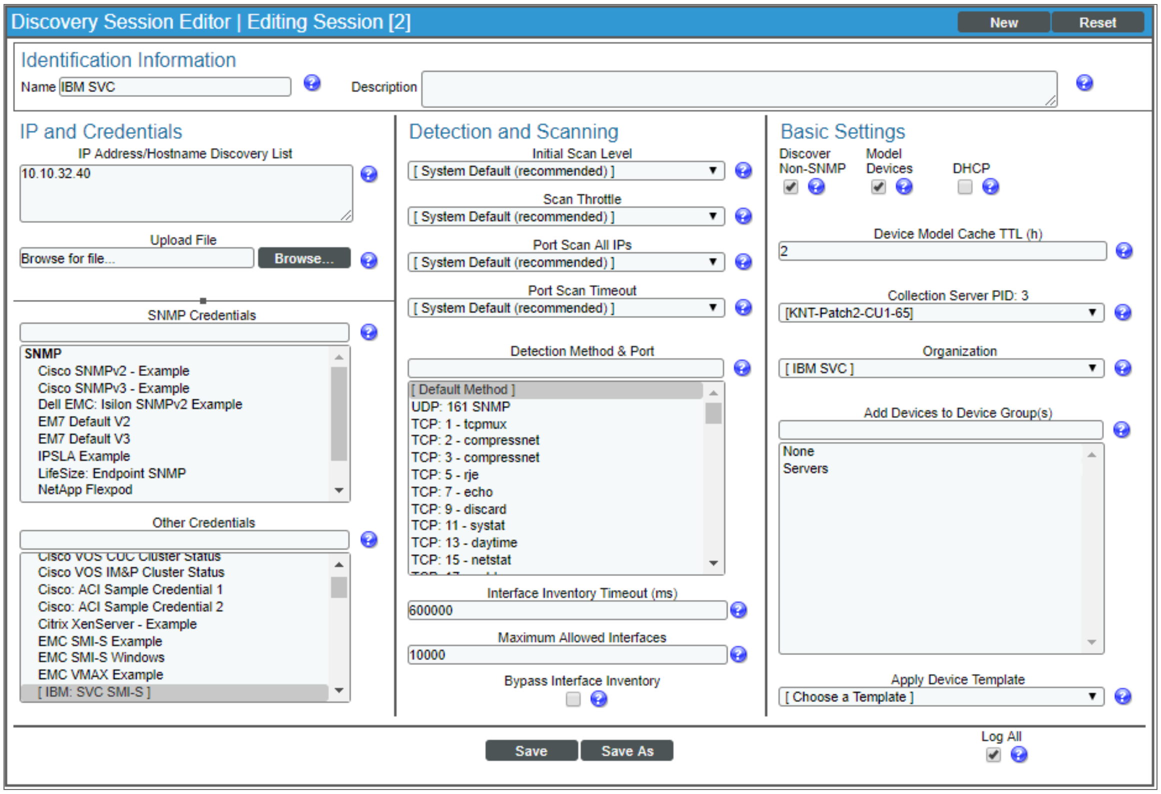
Password:

3. Complete the following fields:
   - ***Credential Name***. Type a name for the IBM SVC credential.
   - ***Username***. Type the username for a user with access to the SMI-S Provider.
   - ***Password***. Type the password for the SMI-S Provider account username.
4. Click the **[Save As]** button.

Discovering IBM SVC Component Devices

To discover an IBM SVC system:

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



Discovery Session Editor | Editing Session [2]

New | Reset

Identification Information

Name: IBM SVC

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.10.32.40

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

SNMP Credentials:

SNMP
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Dell EMC: Isilon SNMPv2 Example
EM7 Default V2
EM7 Default V3
IPSLA Example
LifeSize: Endpoint SNMP
NetApp Flexpod

Other Credentials:

Cisco VOS CUC Cluster Status
Cisco VOS IM&P Cluster Status
Cisco: ACI Sample Credential 1
Cisco: ACI Sample Credential 2
Citrix XenServer - Example
EMC SMI-S Example
EMC SMI-S Windows
EMC VMAX Example
[IBM: SVC SMI-S]

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: 3: [KNT-Patch2-CU1-65]

Organization: [IBM SVC]

Add Devices to Device Group(s):

None
Servers

Apply Device Template: [Choose a Template]

Log All: ☑

Save | Save As

3. In the **Discovery Session Editor** page, complete the following fields:

   - ***Name***. Type a name for the discovery session.
   - ***IP Address/Hostname Discovery List***. Type the IP address for the SMI-S Provider.
   - ***Other Credentials***. Select the Basic/Snippet credential you created for the SMI-S Provider.
   - ***Discover Non-SNMP***. Select this checkbox.
   - ***Model Devices***. Select this checkbox.

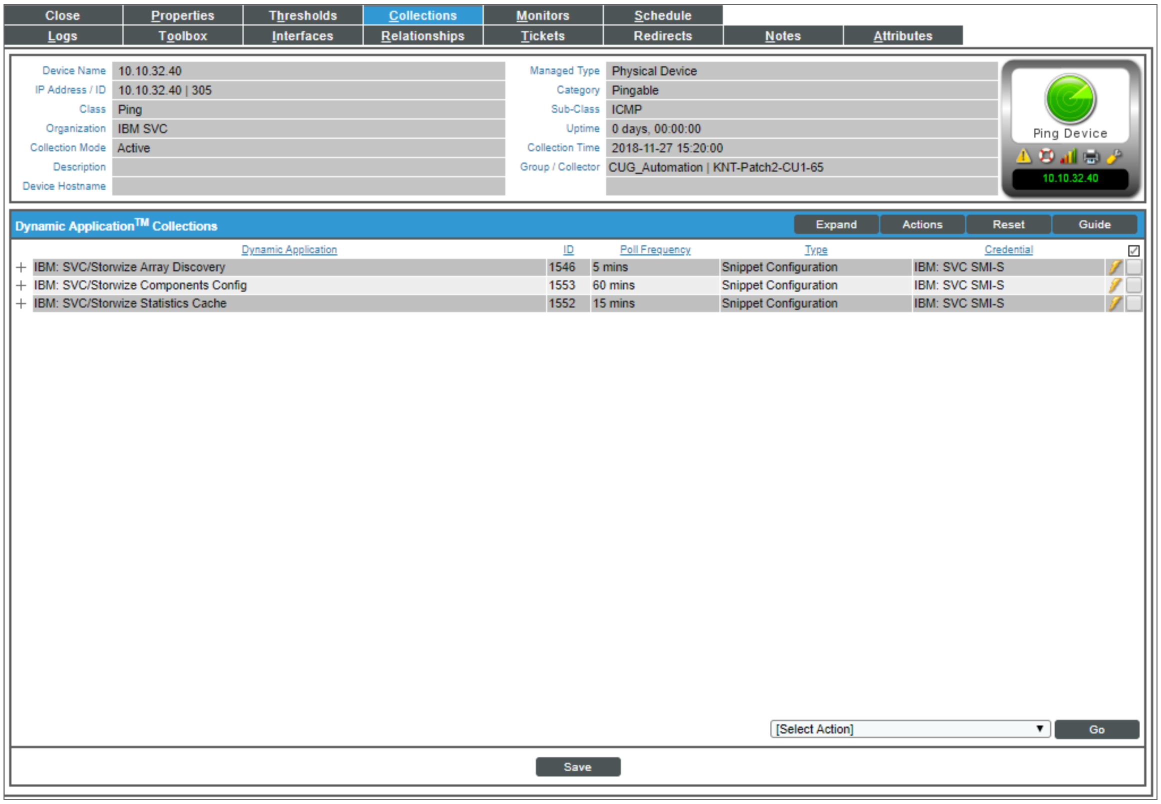
4. Optionally, you can enter values in the other fields on this page. For more information about the other fields on this page, see the ***Discovery & Credentials*** manual.
5. Click the **[Save]** button to save the discovery session and then close the **Discovery Session Editor** window.
6. The discovery 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.

Aligning the Dynamic Applications

To align the IBM SVC Dynamic Applications:

1. After discovery has completed, click the device icon for the IBM SVC device (). From the **Device Properties** page for the IBM SVC device, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.

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

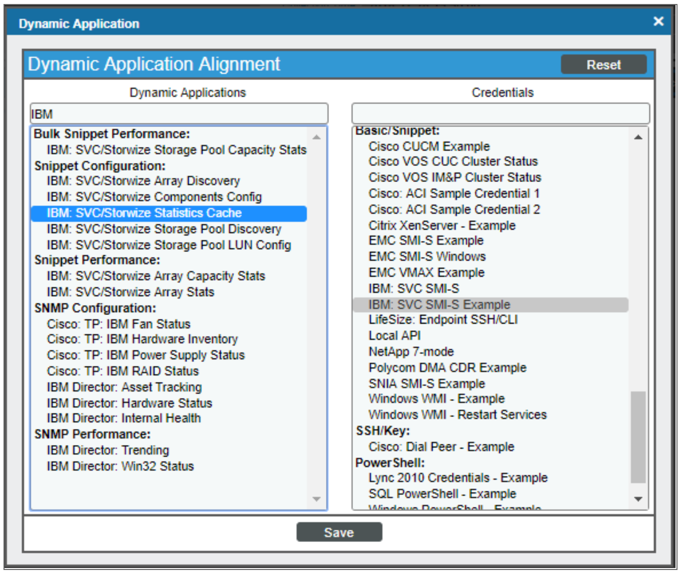


Device Name	10.10.32.40	Managed Type	Physical Device
IP Address / ID	10.10.32.40 | 305	Category	Pingable
Class	Ping	Sub-Class	ICMP
Organization	IBM SVC	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2018-11-27 15:20:00
Description		Group / Collector	CUG_Automation | KNT-Patch2-CU1-65
Device Hostname			

Dynamic Application^{TM} Collections

Dynamic Application	ID	Poll Frequency	Type	Credential
+ IBM: SVC/Storwize Array Discovery	1546	5 mins	Snippet Configuration	IBM: SVC SMI-S
+ IBM: SVC/Storwize Components Config	1553	60 mins	Snippet Configuration	IBM: SVC SMI-S
+ IBM: SVC/Storwize Statistics Cache	1552	15 mins	Snippet Configuration	IBM: SVC SMI-S

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



IBM

Bulk Snippet Performance:
- IBM: SVC/Storwize Storage Pool Capacity Stats

Snippet Configuration:
- IBM: SVC/Storwize Array Discovery
- IBM: SVC/Storwize Components Config
- IBM: SVC/Storwize Statistics Cache
- IBM: SVC/Storwize Storage Pool Discovery
- IBM: SVC/Storwize Storage Pool LUN Config

Snippet Performance:
- IBM: SVC/Storwize Array Capacity Stats
- IBM: SVC/Storwize Array Stats

SNMP Configuration:
- Cisco: TP: IBM Fan Status
- Cisco: TP: IBM Hardware Inventory
- Cisco: TP: IBM Power Supply Status
- Cisco: TP: IBM RAID Status
- IBM Director: Asset Tracking
- IBM Director: Hardware Status
- IBM Director: Internal Health

SNMP Performance:
- IBM Director: Trending
- IBM Director: Win32 Status

Basic/Snippet:
- Cisco CUCM Example
- Cisco VOS CUC Cluster Status
- Cisco VOS IM&P Cluster Status
- Cisco: ACI Sample Credential 1
- Cisco: ACI Sample Credential 2
- Citrix XenServer - Example
- EMC SMI-S Example
- EMC SMI-S Windows
- EMC VMAX Example
- IBM: SVC SMI-S
- IBM: SVC SMI-S Example
- LifeSize: Endpoint SSH/CLI
- Local API
- NetApp 7-mode
- Polycom DMA CDR Example
- SNIA SMI-S Example
- Windows WMI - Example
- Windows WMI - Restart Services

SSH/Key:
- Cisco: Dial Peer - Example

PowerShell:
- Lync 2010 Credentials - Example
- SQL PowerShell - Example
- Windows PowerShell - Example

3. In the ***Dynamic Applications*** field, select the "IBM: SVC/Storwize Statistics Cache" Dynamic Application.
4. In the ***Credentials*** field, select the credential you created.
5. Click the **[Save]** button.
6. Repeat steps 1-5 for the "IBM: SVC/Storwize Array Discovery" Dynamic Application, followed by the "IBM: SVC/Storwize Components Config" Dynamic Application.

NOTE: The "IBM: SVC/Storwize Array Stats" Dynamic Application requires that a few polling cycles of the "IBM: SVC/Storwize Statistics Cache" Dynamic Application complete before it begins the Array Stats collection. The "IBM: SVC/Storwize Array Stats" Dynamic Application is the cache consumer and the "IBM: SVC/Storwize Statistics Cache" Dynamic Application is the cache producer.

Chapter 45

IBM: Tivoli Storage Manager

Overview

The following sections describe how to configure and discover IBM Tivoli Storage Manager environments for monitoring by SL1 using the *IBM: Tivoli Storage Manager* PowerPack:

> NOTE: For more information about the *IBM: Tivoli Storage Manager* PowerPack, see the ***Monitoring IBM Tivoli Storage Manager*** manual.

Creating Credentials for IBM Tivoli Storage Manager

If you are connecting to your IBM Tivoli Storage Manager (TSM) environment using SSH with basic authentication, then you will need to create a ***SOAP/XML credential***.

If you connecting to your TSM environment using SSH with public-key authentication, you will need to create an ***SSH/Key credential*** in addition to the SOAP/XML credential.

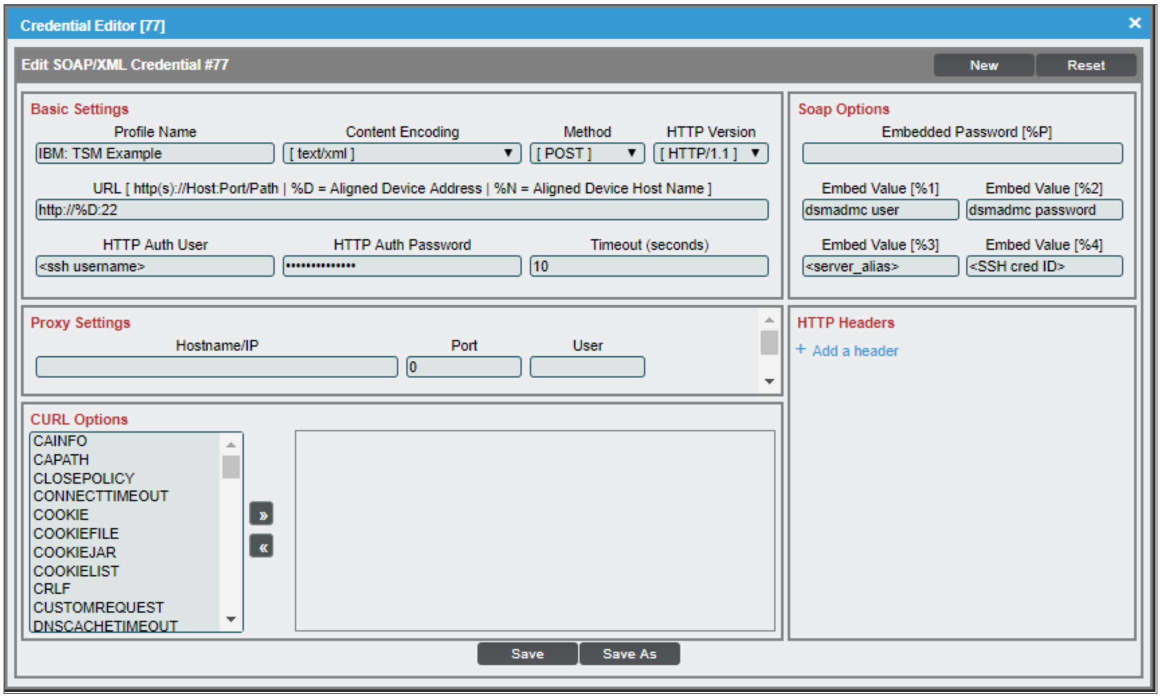
Creating a SOAP/XML Credential for IBM Tivoli Storage Manager

To use the Dynamic Applications in the *IBM: Tivoli Storage Manager* PowerPack, you must configure a SOAP/XML credential for your Tivoli Storage Manager (TSM) environment. The *IBM: Tivoli Storage Manager* PowerPack includes a template for SOAP/XML credentials that you can edit for use with your TSM environment.

To modify the template, perform the following steps:

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

2. Click the wrench icon (🔧) for the "IBM: TSM Example". The **Credential Editor** modal page appears:



Profile Name: IBM: TSM Example
Content Encoding: [text/xml]
Method: [POST]
HTTP Version: [HTTP/1.1]
URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: http://%D:22
HTTP Auth User: <ssh username>
HTTP Auth Password: •••••••••••••
Timeout (seconds): 10
Embedded Password [%P]:
Embed Value [%1]: dsmadmc user
Embed Value [%2]: dsmadmc password
Embed Value [%3]: <server_alias>
Embed Value [%4]: <SSH cred ID>
Hostname/IP:
Port: 0
User:

3. Supply values in the following fields:

   - ***Profile Name***. Enter a new name for the credential.
   - ***HTTP Auth User***. Enter the username for the TSM server, or the proxy server that you are connecting to via SSH.

> **NOTE:** The username you enter in the ***HTTP Auth User*** field must have the necessary permissions to successfully execute dsmadmc commands.

   - ***HTTP Auth Password***. Enter the password for the TSM server, or the proxy server you are connecting to via SSH. This field is required when not using a private RSA key to connect.

- ***Embed Value [%1]***. Enter the dsmadmc username. The dsmadmc login is configured separately by the TSM administrator, but the default login is admin/passw0rd. This field is required.
- ***Embed Value [%2]***. Enter the dsmadmc password. This field is required.
- ***Embed Value [%3]***. If you are using a proxy server, enter the TSM server name in this field as defined in your `dsm.sys` file. If this field is left unchanged, it's assumed that you're connecting directly to the TSM server instance.
- ***Embed Value [%4]***. If you are using an ***SSH/Key credential for public/private key access***, enter the credential ID of the SSH/Key credential in this field. Otherwise, leave this field blank.

4. Click the **[Save As]** button to save your changes as a new credential.

CAUTION: Do not click the **[Save]** button, as it will save over the example credential, which you may need for future use.

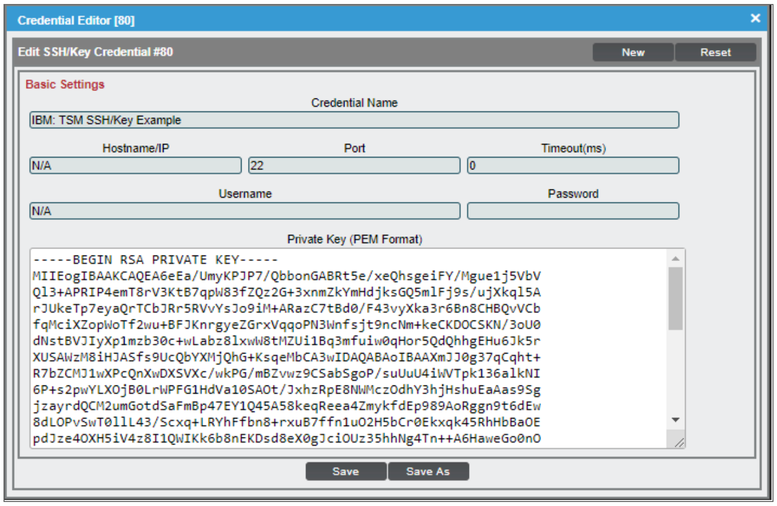
Creating an SSH/Key Credential for IBM Tivoli Storage Manager

When configuring monitoring for IBM Tivoli Storage Manager devices, if you want to use a public/private RSA key pair for the SSH connection rather than a username and password, you must also create an SSH/Key credential. This credential allows the Dynamic Applications in the *IBM: Tivoli Storage Manager* PowerPack to connect with an IBM Tivoli Storage Manager server or proxy client using an RSA key pair. After you create this credential, you must then enter its credential ID number in the ***SOAP/XML credential*** you created.

The *IBM: Tivoli Storage Manager* PowerPack includes a template for SSH/Key credentials that you can edit for use with your TSM environment, if needed.

To create an SSH/Key credential:

1. Generate an SSH RSA private/public key pair. This is commonly done using the "ssh-keygen" command-line utility.
2. Go to the **Credential Management** page (System > Manage > Credentials).
3. Click the wrench icon (🔧) for the "IBM: TSM SSH/Key Example" credential. The **Credential Editor** modal page appears:



Credential Name: IBM: TSM SSH/Key Example

Hostname/IP: N/A

Port: 22

Timeout(ms): 0

Username: N/A

Password:

Private Key (PEM Format):

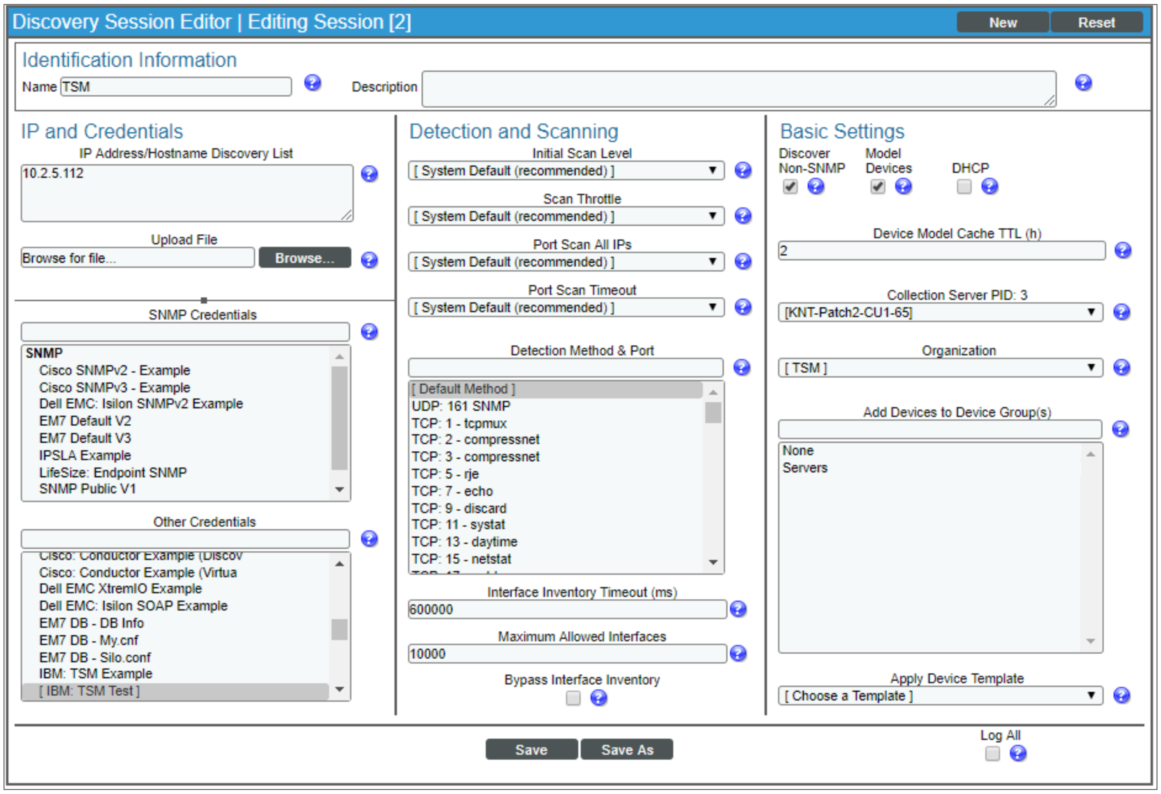
```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEA6eEa/UmyKPJP7/QbbonGABRt5e/xeQhsgeiFY/Mgue1j5VbV
Ql3+APRIP4emT8rV3KtB7qpW83fZQz2G+3xnmZkYmHdjksGQ5mlFj9s/ujXkql5A
rJUkeTp7eyaQrTCbJRr5RVvYsJo9iM+ARazC7tBd0/F43vyXka3r6Bn8CHBQvVCb
fqMciXZopWoTf2wu+BFJKnrgyeZGrxVqqoPN3Wnfsjt9ncNm+keCKDOCSKN/3oU0
dNstBVJIyXp1mzb30c+wLabz8lxwW8tMZUi1Bq3mfuiw0qHor5QdQhhgEHu6Jk5r
XUSAWzM8iHJASfs9UcQbYXMjQhG+KsqeMbCA3wIDAQABAoIBAAXmJJ0g37qCqht+
R7bZCMJ1wXPcQnXwDXSVXc/wkPG/mBZvwz9CSabSgoP/suUuU4iWVTpk136alkNI
6P+s2pwYLXOjB0LrWPFG1HdVa10SAOt/JxhzRpE8NWMczOdhY3hjHshuEaAas9Sg
jzayrdQCM2umGotdSaFmBp47EY1Q45A58keqReea4ZmykfdEp989AoRggn9t6dEw
8dLOPvSwT0llL43/Scxq+LRYhFfbn8+rxuB7ffn1uO2H5bCr0Ekxqk45RhHbBaOE
pdJze4OXH5iV4z8I1QWIKk6b8nEKDsd8eX0gJciOUz35hhNg4Tn++A6HaweGo0nO
```

4. Supply values in the following fields:
    - ***Credential Name***. Enter a new name for the credential.
    - ***Username***. Enter N/A. The credential cannot be saved if this field is empty.
    - ***Password***. Enter N/A. The credential cannot be saved if this field is empty.
    - ***Private Key (PEM Format)***. Paste the SSH private key that you copied from your collector into this field, in PEM format.
5. Click **[Save As]**. In the **Credential Management**, note the credential ID of the SSH/Key credential you just created.
6. Save the corresponding public key to the `authorized_keys` file on your SSH target (the TSM server or proxy client). This is typically found at `/root/.ssh/authorized_keys`
7. In the *SOAP/XML credential* you created, enter the credential ID of the SSH/Key credential in the ***Embed Value [%4]*** field.

Discovering IBM Tivoli Storage Manager Component Devices

To discover an IBM Tivoli Storage Manager (TSM) system:

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



Identification Information

Name: TSM

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.2.5.112

Upload File: Browse for file...

SNMP Credentials:
SNMP
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Dell EMC: Isilon SNMPv2 Example
EM7 Default V2
EM7 Default V3
IPSLA Example
LifeSize: Endpoint SNMP
SNMP Public V1

Other Credentials:
Cisco: Conductor Example (Discov
Cisco: Conductor Example (Virtua
Dell EMC XtremIO Example
Dell EMC: Isilon SOAP Example
EM7 DB - DB Info
EM7 DB - My.cnf
EM7 DB - Silo.conf
IBM: TSM Example
[IBM: TSM Test]

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: 3: [KNT-Patch2-CU1-65]

Organization: [TSM]

Add Devices to Device Group(s):
None
Servers

Apply Device Template: [Choose a Template]

Log All: □

3. In the **Discovery Session Editor** page, complete the following fields:

    - ***Name***. Type a name for the discovery session.
    - ***IP Address/Hostname Discovery List***. Type the IP address for the Tivoli Storage Manager server or proxy client.
    - ***Other Credentials***. Select the SOAP/XML credential you created for the Tivoli Storage Manager system.
    - ***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.

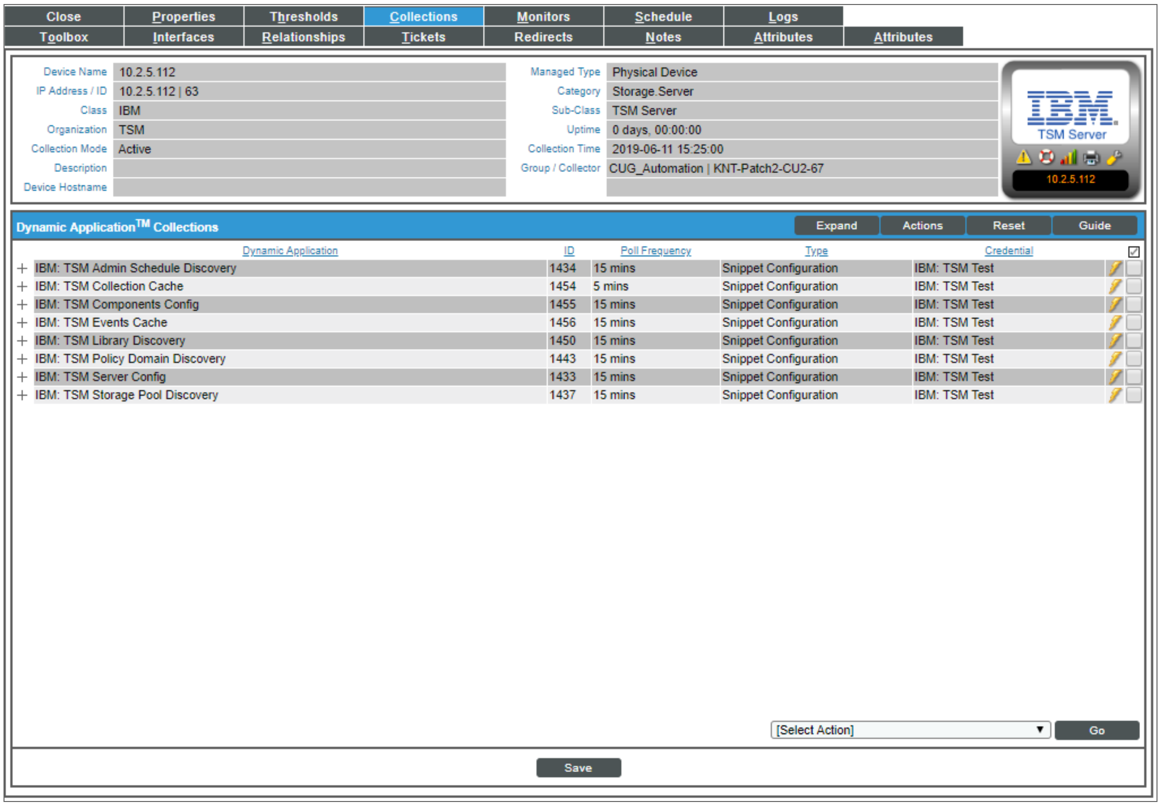
Verifying Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. After discovery has completed, click the device icon for the Tivoli Storage Manager (TSM) device (). From the **Device Properties** page for the TSM device, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. All applicable Dynamic Applications are automatically aligned to the root device during discovery.

> NOTE: It can take 10 to 15 minutes after the discovery session has completed for Dynamic Applications to appear in the **Dynamic Application Collections** page.

> NOTE: As data is collected and cached on the first polling interval and displayed on the second, you might not see any data until the second polling interval is completed. This could take as long as 30 minutes.



Device Name	10.2.5.112	Managed Type	Physical Device
IP Address / ID	10.2.5.112 | 63	Category	Storage.Server
Class	IBM	Sub-Class	TSM Server
Organization	TSM	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2019-06-11 15:25:00
Description		Group / Collector	CUG_Automation | KNT-Patch2-CU2-67
Device Hostname			

Dynamic Application^{TM} Collections

Dynamic Application	ID	Poll Frequency	Type	Credential	☑
+ IBM: TSM Admin Schedule Discovery	1434	15 mins	Snippet Configuration	IBM: TSM Test	□
+ IBM: TSM Collection Cache	1454	5 mins	Snippet Configuration	IBM: TSM Test	□
+ IBM: TSM Components Config	1455	15 mins	Snippet Configuration	IBM: TSM Test	□
+ IBM: TSM Events Cache	1456	15 mins	Snippet Configuration	IBM: TSM Test	□
+ IBM: TSM Library Discovery	1450	15 mins	Snippet Configuration	IBM: TSM Test	□
+ IBM: TSM Policy Domain Discovery	1443	15 mins	Snippet Configuration	IBM: TSM Test	□
+ IBM: TSM Server Config	1433	15 mins	Snippet Configuration	IBM: TSM Test	□
+ IBM: TSM Storage Pool Discovery	1437	15 mins	Snippet Configuration	IBM: TSM Test	□

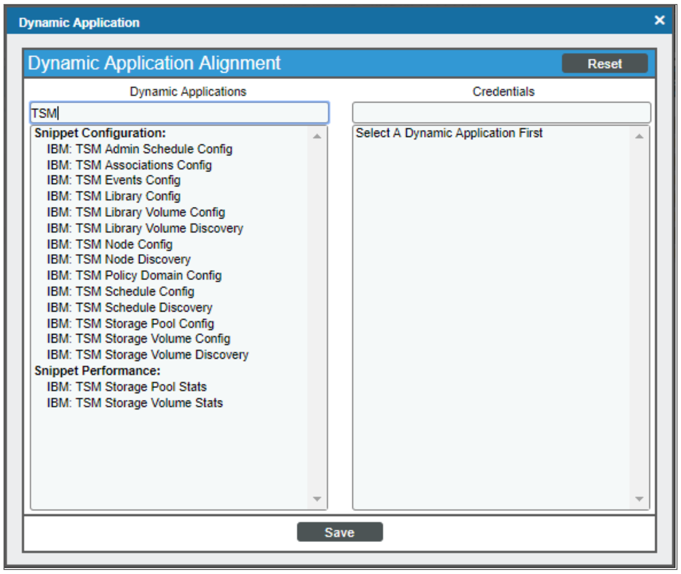
You should see the following Dynamic Applications aligned to the TSM device:

- IBM: TSM Admin Schedule Discovery
- IBM: TSM Collection Cache
- IBM: TSM Components Config
- IBM: TSM Events Cache

- IBM: TSM Library Discovery
- IBM: TSM Policy Domain Discovery
- IBM: TSM Server Config
- IBM: TSM Storage Pool Discovery

If the listed Dynamic Applications have not been automatically aligned during discovery, you can align them manually. To do so, perform the following steps:

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



TSM

Snippet Configuration:
IBM: TSM Admin Schedule Config
IBM: TSM Associations Config
IBM: TSM Events Config
IBM: TSM Library Config
IBM: TSM Library Volume Config
IBM: TSM Library Volume Discovery
IBM: TSM Node Config
IBM: TSM Node Discovery
IBM: TSM Policy Domain Config
IBM: TSM Schedule Config
IBM: TSM Schedule Discovery
IBM: TSM Storage Pool Config
IBM: TSM Storage Volume Config
IBM: TSM Storage Volume Discovery
Snippet Performance:
IBM: TSM Storage Pool Stats
IBM: TSM Storage Volume Stats

Select A Dynamic Application First

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

Chapter 46

IBM: WebSphere Application Server

Overview

The following sections describe how to configure and discover IBM WebSphere Application Servers for monitoring by SL1 using the *IBM: WebSphere Application Server* PowerPack:

NOTE: For more information about the *IBM: WebSphere Application Server* PowerPack, see the ***Monitoring IBM WebSphere Application Servers*** manual.

Prerequisites for Monitoring IBM WebSphere Application Servers

To configure the SL1 system to monitor IBM WebSphere Application Servers using the *IBM: WebSphere Application Server* PowerPack, you must first set up the following:

- ***Performance Monitoring Architecture (PMI)***. PMI is the monitoring structure for the WebSphere Application Server. The performance data provided by the WebSphere PMI helps to monitor and tune the application server performance. To set up PMI, follow the steps here: https://www.ibm.com/support/knowledgecenter/en/SSEQTP_8.5.5/com.ibm.websphere.base.doc/ae/tprf_pmi_encoll.html

NOTE: When configuring PMI, it is recommended that you set the status to "All" for each of the application servers you want to monitor.

NOTE: If PMI is disabled on any server, SL1 will continue to show statistics on that server. If the user does not want to see the statistics on the server on which PMI was disabled, they can recursively disable them. SL1 will eventually move that server to ***Vanished Devices*** and purge it based on the settings that the user has chosen.

- ***PerfServlet***. ScienceLogic will use the WebSphere credential that you create to access PMI output through the PerfServlet appication. To install PerfServlet, follow the steps here: https://www.ibm.com/support/knowledgecenter/en/SSEQTP_8.5.5/com.ibm.websphere.base.doc/ae/tprf_devprfservlet.html
    - After installing, ensure that PerfServlet is mapped to all the WebSphere application servers that you want to monitor
    - To configure the WebSphere credential and access the PerfServlet application, you will need the hostname, default http(s) transport port, and credentials.

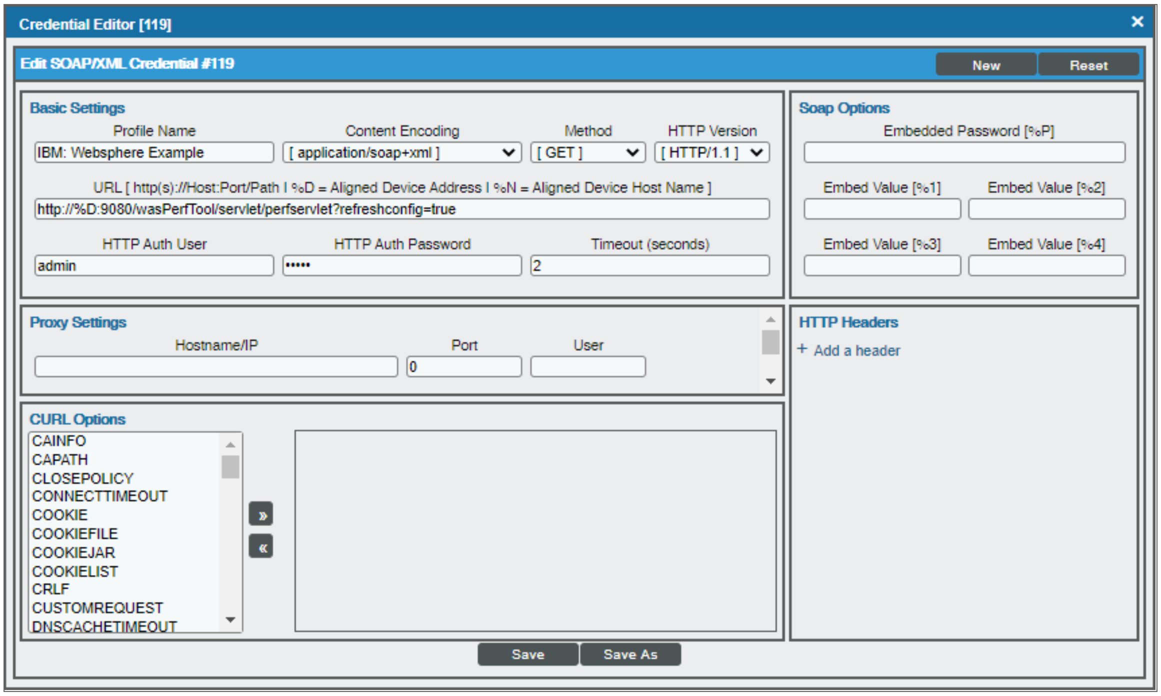
Creating a SOAP/XML Credential for IBM WebSphere Application Servers

To configure SL1 to monitor IBM WebSphere Application Servers, you must first create a SOAP/XML credential. This credential allows the Dynamic Applications in the *IBM: WebSphere Application Server* PowerPack to connect with an IBM WebSphere Application Server.

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

To configure a SOAP/XML credential to access an IBM WebSphere Application Server:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **IBM: WebSphere Example** credential, then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears:



Profile Name: IBM: Websphere Example

Content Encoding: [application/soap+xml]

Method: [GET]

HTTP Version: [HTTP/1.1]

URL: http://%D:9080/wasPerfTool/servlet/perfservlet?refreshconfig=true

HTTP Auth User: admin

HTTP Auth Password: •••••

Timeout (seconds): 2

Port: 0

3. Complete the following fields:

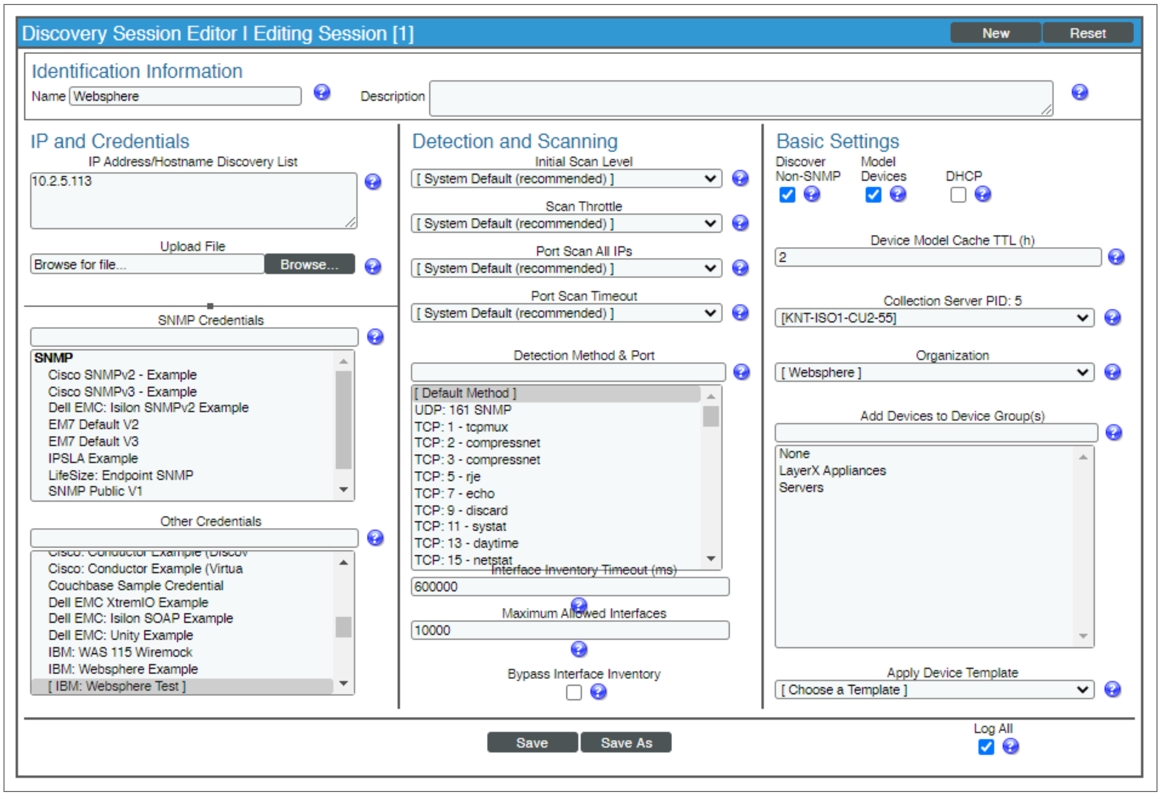
   - ***Profile Name***. Type a name for the IBM WebSphere credential.
   - ***URL***. The default value in this field is "http (s)://%D:<port>/wasPerfTool/servlet/perfservlet?refreshconfig=true" where %D is the hostname. The port number is determined from the information provided when setting up the PerfServlet.
   - ***HTTP Auth User***. Type the username for a user with access to the PerfServlet application.
   - ***HTTP Auth Password***. Type the password for the PerfServlet account username.

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

Discovering IBM WebSphere Component Devices

To discover an IBM WebSphere Application Server:

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



Discovery Session Editor | Editing Session [1]

Identification Information

Name: Websphere

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.2.5.113

Upload File: Browse for file...

SNMP Credentials

SNMP
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Dell EMC: Isilon SNMPv2 Example
EM7 Default V2
EM7 Default V3
IPSLA Example
LifeSize: Endpoint SNMP
SNMP Public V1

Other Credentials

Cisco: Conductor Example (Discov
Cisco: Conductor Example (Virtua
Couchbase Sample Credential
Dell EMC XtremIO Example
Dell EMC: Isilon SOAP Example
Dell EMC: Unity Example
IBM: WAS 115 Wiremock
IBM: Websphere Example
[IBM: Websphere Test]

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: 5: [KNT-ISO1-CU2-55]

Organization: [Websphere]

Add Devices to Device Group(s)

None
LayerX Appliances
Servers

Apply Device Template: [Choose a Template]

Log All: ☑

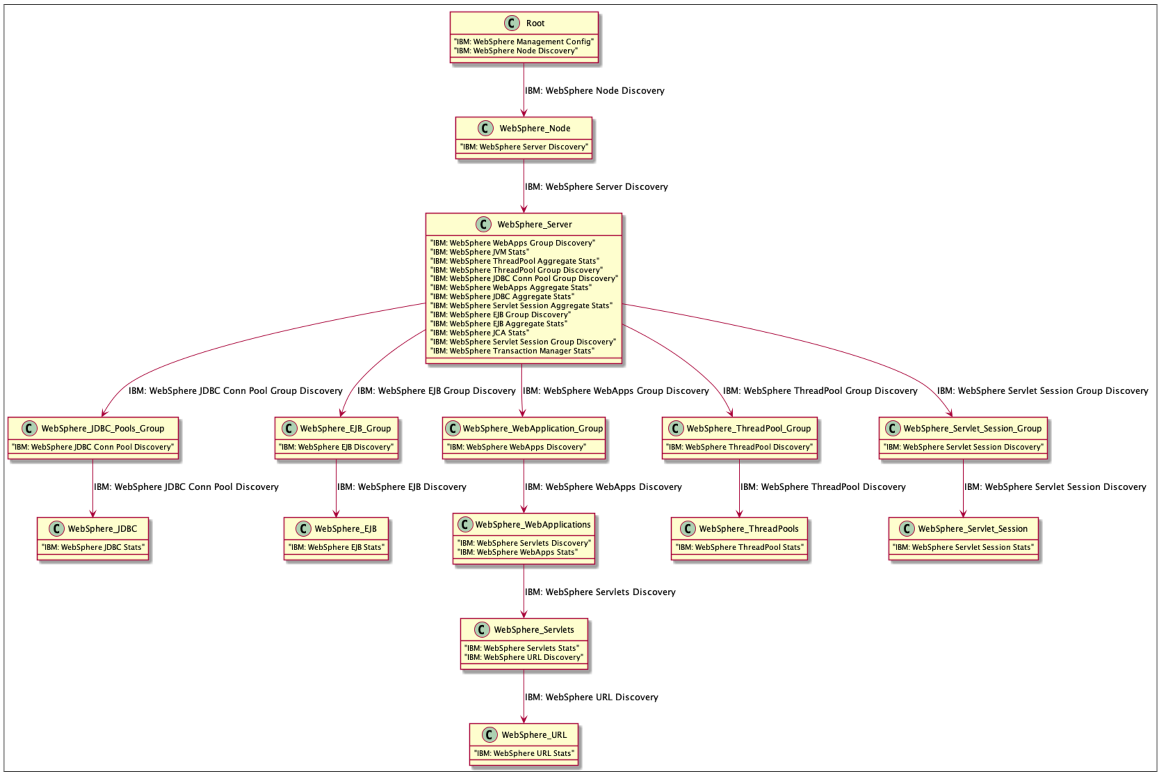
3. In the **Discovery Session Editor** page, complete the following fields:

    - ***Name***. Type a name for the discovery session.
    - ***IP Address/Hostname Discovery List***. Type the IP address for the WebSphere Application Server.
    - ***Other Credentials***. Select the SOAP/XML credential you created for the WebSphere Application Server.
    - ***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.

Verifying Discovery and Dynamic Application Alignment

During discovery, SL1 will discover the root device, then the WebSphere Node which will in turn discover the server. All applicable Dynamic Applications will be aligned to each component:



C Root
"IBM: WebSphere Management Config"
"IBM: WebSphere Node Discovery"
IBM: WebSphere Node Discovery
C WebSphere_Node
"IBM: WebSphere Server Discovery"
IBM: WebSphere Server Discovery
C WebSphere_Server
"IBM: WebSphere WebApps Group Discovery"
"IBM: WebSphere JVM Stats"
"IBM: WebSphere ThreadPool Aggregate Stats"
"IBM: WebSphere ThreadPool Group Discovery"
"IBM: WebSphere JDBC Conn Pool Group Discovery"
"IBM: WebSphere WebApps Aggregate Stats"
"IBM: WebSphere JDBC Aggregate Stats"
"IBM: WebSphere Servlet Session Aggregate Stats"
"IBM: WebSphere EJB Group Discovery"
"IBM: WebSphere EJB Aggregate Stats"
"IBM: WebSphere JCA Stats"
"IBM: WebSphere Servlet Session Group Discovery"
"IBM: WebSphere Transaction Manager Stats"
IBM: WebSphere JDBC Conn Pool Group Discovery
IBM: WebSphere EJB Group Discovery
IBM: WebSphere WebApps Group Discovery
IBM: WebSphere ThreadPool Group Discovery
IBM: WebSphere Servlet Session Group Discovery
C WebSphere_JDBC_Pools_Group
"IBM: WebSphere JDBC Conn Pool Discovery"
C WebSphere_EJB_Group
"IBM: WebSphere EJB Discovery"
C WebSphere_WebApplication_Group
"IBM: WebSphere WebApps Discovery"
C WebSphere_ThreadPool_Group
"IBM: WebSphere ThreadPool Discovery"
C WebSphere_Servlet_Session_Group
"IBM: WebSphere Servlet Session Discovery"
IBM: WebSphere JDBC Conn Pool Discovery
IBM: WebSphere EJB Discovery
IBM: WebSphere WebApps Discovery
IBM: WebSphere ThreadPool Discovery
IBM: WebSphere Servlet Session Discovery
C WebSphere_JDBC
"IBM: WebSphere JDBC Stats"
C WebSphere_EJB
"IBM: WebSphere EJB Stats"
C WebSphere_WebApplications
"IBM: WebSphere Servlets Discovery"
"IBM: WebSphere WebApps Stats"
C WebSphere_ThreadPools
"IBM: WebSphere ThreadPool Stats"
C WebSphere_Servlet_Session
"IBM: WebSphere Servlet Session Stats"
IBM: WebSphere Servlets Discovery
C WebSphere_Servlets
"IBM: WebSphere Servlets Stats"
"IBM: WebSphere URL Discovery"
IBM: WebSphere URL Discovery
C WebSphere_URL
"IBM: WebSphere URL Stats"

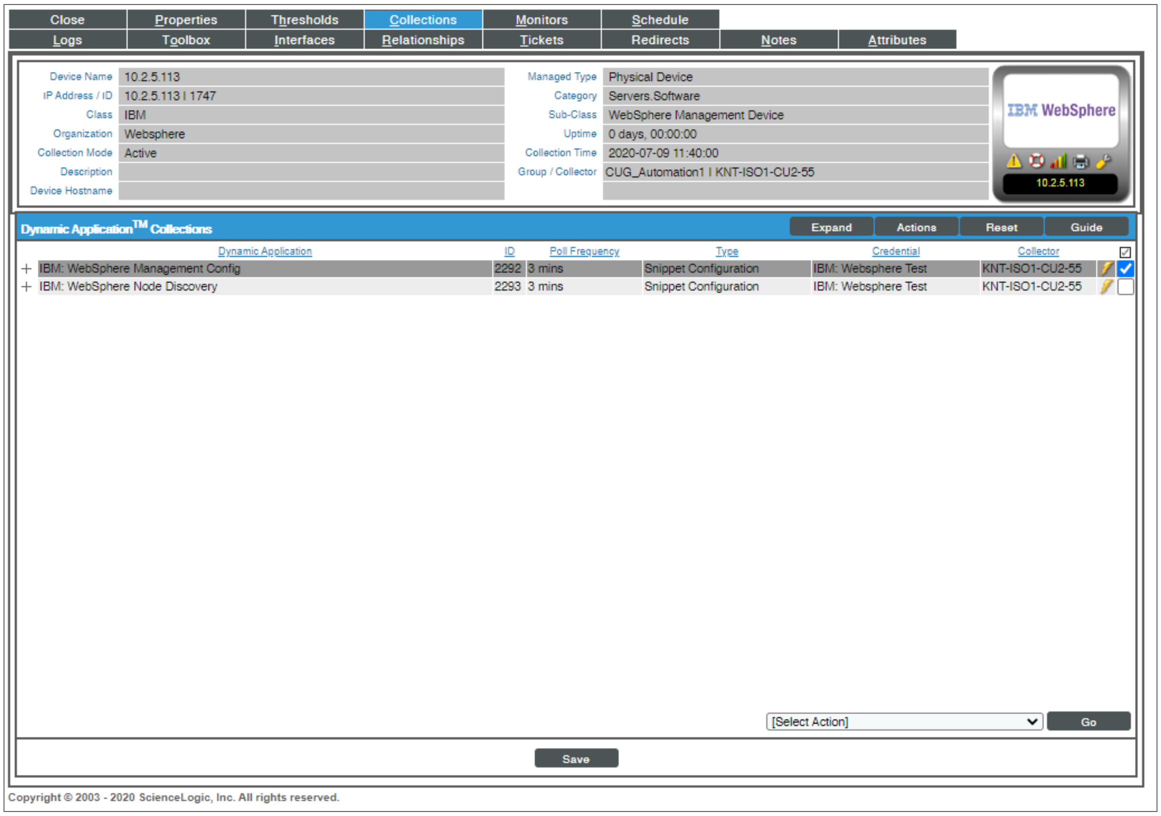
To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. After the discovery session has completed, go to the **Device Manager** (Registry > Devices > Device Manager) page and find the device(s) you discovered. When you have located the device in the **Device Manager**, click on its edit icon ( ).
2. In the **Device Properties** page, click the **[Collections]** tab.
3. All applicable Dynamic Applications for the WebSphere devices 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 WebSphere Management Device:

- IBM: WebSphere Management Config
- IBM: WebSphere Node Discovery



Device Name	10.2.5.113	Managed Type	Physical Device
IP Address / ID	10.2.5.113 I 1747	Category	Servers.Software
Class	IBM	Sub-Class	WebSphere Management Device
Organization	Websphere	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2020-07-09 11:40:00
Description		Group / Collector	CUG_Automation1 I KNT-ISO1-CU2-55
Device Hostname			

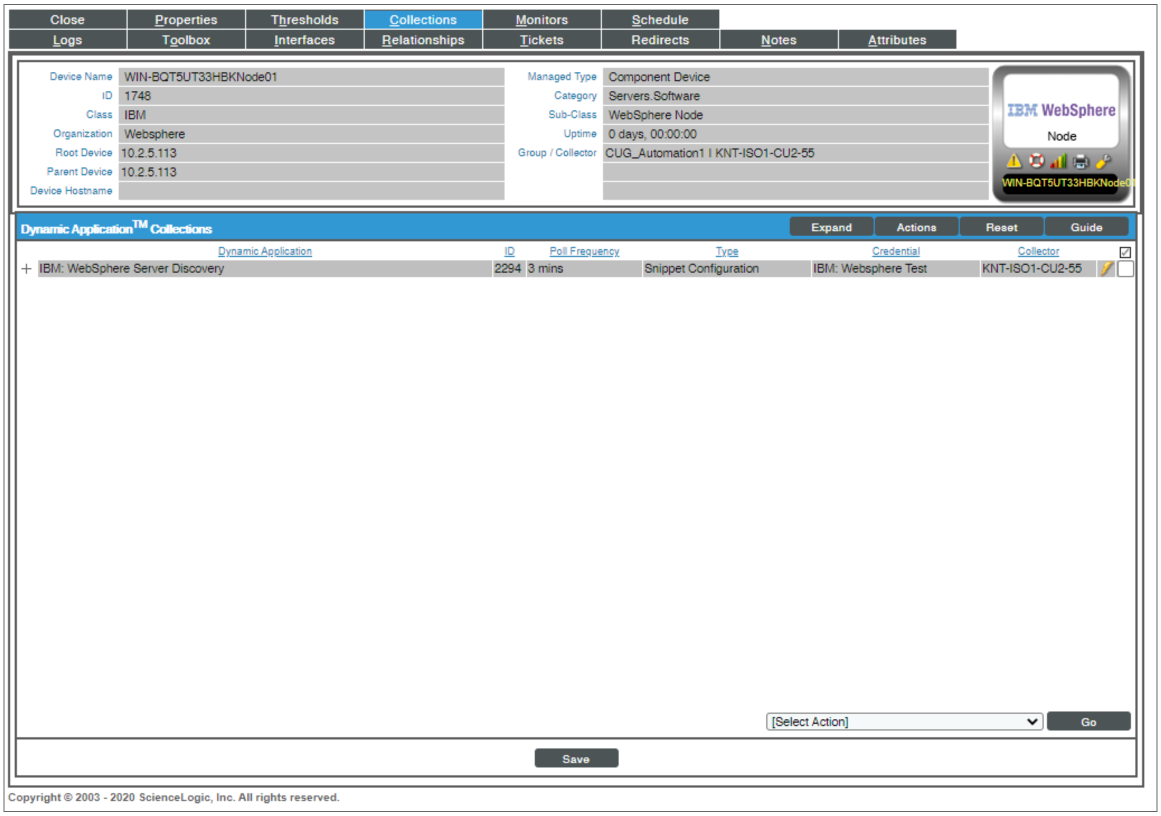
Dynamic Application™ Collections

	Dynamic Application	ID	Poll Frequency	Type	Credential	Collector	☑
+	IBM: WebSphere Management Config	2292	3 mins	Snippet Configuration	IBM: Websphere Test	KNT-ISO1-CU2-55	☑
+	IBM: WebSphere Node Discovery	2293	3 mins	Snippet Configuration	IBM: Websphere Test	KNT-ISO1-CU2-55	□

Copyright © 2003 - 2020 ScienceLogic, Inc. All rights reserved.

You should see the following Dynamic Application aligned to the WebSphere node:

- IBM: WebSphere Server Discovery



Device Name	WIN-BQT5UT33HBKNode01	Managed Type	Component Device
ID	1748	Category	Servers.Software
Class	IBM	Sub-Class	WebSphere Node
Organization	Websphere	Uptime	0 days, 00:00:00
Root Device	10.2.5.113	Group / Collector	CUG_Automation1 I KNT-ISO1-CU2-55
Parent Device	10.2.5.113		
Device Hostname			

Dynamic Application™ Collections

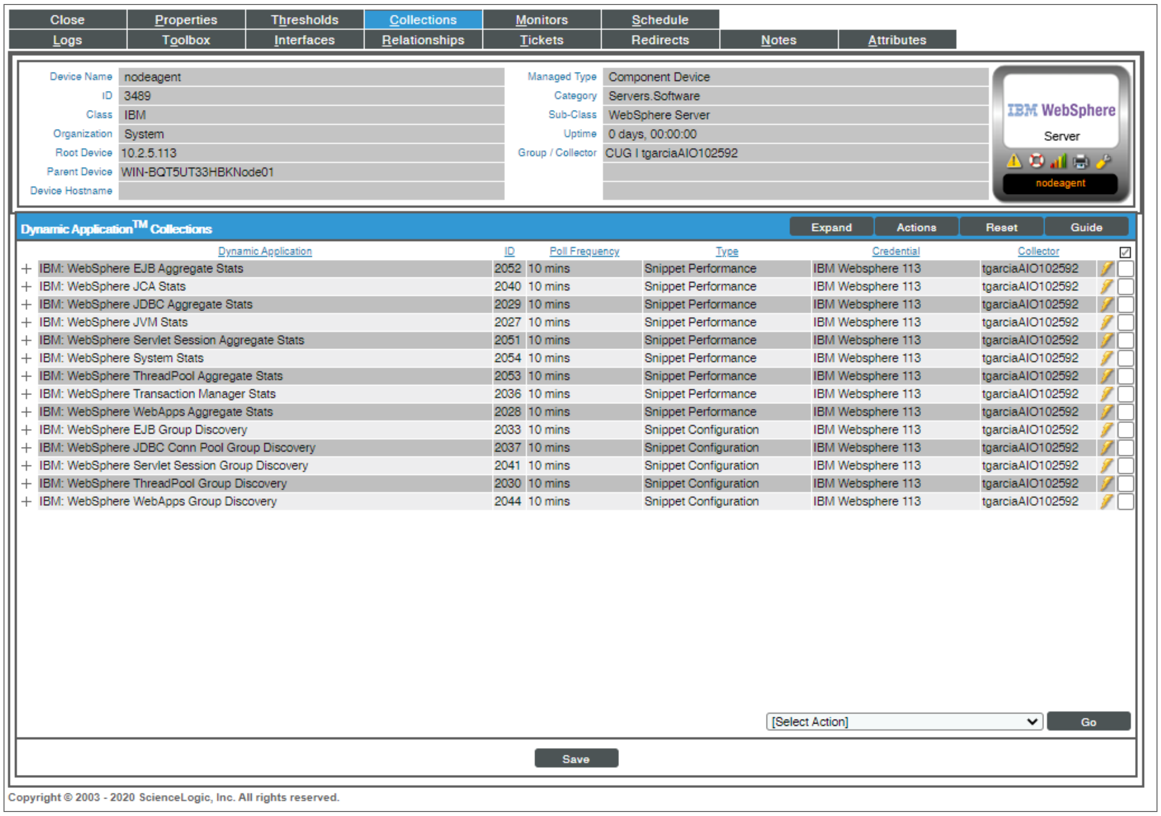
Dynamic Application	ID	Poll Frequency	Type	Credential	Collector	☑
+ IBM: WebSphere Server Discovery	2294	3 mins	Snippet Configuration	IBM: Websphere Test	KNT-ISO1-CU2-55	□

Copyright © 2003 - 2020 ScienceLogic, Inc. All rights reserved.

For all other server types, you should see the following Dynamic Application aligned to the WebSphere server:

- IBM: WebSphere EJB Aggregate Stats
- IBM: WebSphere EJB Group Discovery
- IBM: WebSphere JCA Stats
- IBM: WebSphere JDBC Aggregate Stats
- IBM: WebSphere JDBC Conn Pool Group Discovery
- IBM: WebSphere JVM Stats
- IBM: WebSphere Servlet Session Aggregate Stats
- IBM: WebSphere Servlet Session Group Discovery
- IBM: WebSphere System Stats
- IBM: WebSphere ThreadPool Aggregate Stats
- IBM: WebSphere ThreadPool Group Discovery
- IBM: WebSphere Transaction Manager Stats
- IBM: WebSphere WebApps Aggregate Stats
- IBM: WebSphere WebApps Group Discovery

NOTE: The "IBM: WebSphere System Stats" Dynamic Application will only align to servers of type "nodeagent" on managed nodes to collect data. If you have a system that does not have a "nodeagent" server, you will have to manually align the "IBM: WebSphere System Stats" Dynamic Application.



Device Name	nodeagent	Managed Type	Component Device
ID	3489	Category	Servers.Software
Class	IBM	Sub-Class	WebSphere Server
Organization	System	Uptime	0 days, 00:00:00
Root Device	10.2.5.113	Group / Collector	CUG I tgarciaAIO102592
Parent Device	WIN-BQT5UT33HBKNode01		
Device Hostname			

Dynamic Application™ Collections

Dynamic Application	ID	Poll Frequency	Type	Credential	Collector	☑
+ IBM: WebSphere EJB Aggregate Stats	2052	10 mins	Snippet Performance	IBM Websphere 113	tgarciaAIO102592	□
+ IBM: WebSphere JCA Stats	2040	10 mins	Snippet Performance	IBM Websphere 113	tgarciaAIO102592	□
+ IBM: WebSphere JDBC Aggregate Stats	2029	10 mins	Snippet Performance	IBM Websphere 113	tgarciaAIO102592	□
+ IBM: WebSphere JVM Stats	2027	10 mins	Snippet Performance	IBM Websphere 113	tgarciaAIO102592	□
+ IBM: WebSphere Servlet Session Aggregate Stats	2051	10 mins	Snippet Performance	IBM Websphere 113	tgarciaAIO102592	□
+ IBM: WebSphere System Stats	2054	10 mins	Snippet Performance	IBM Websphere 113	tgarciaAIO102592	□
+ IBM: WebSphere ThreadPool Aggregate Stats	2053	10 mins	Snippet Performance	IBM Websphere 113	tgarciaAIO102592	□
+ IBM: WebSphere Transaction Manager Stats	2036	10 mins	Snippet Performance	IBM Websphere 113	tgarciaAIO102592	□
+ IBM: WebSphere WebApps Aggregate Stats	2028	10 mins	Snippet Performance	IBM Websphere 113	tgarciaAIO102592	□
+ IBM: WebSphere EJB Group Discovery	2033	10 mins	Snippet Configuration	IBM Websphere 113	tgarciaAIO102592	□
+ IBM: WebSphere JDBC Conn Pool Group Discovery	2037	10 mins	Snippet Configuration	IBM Websphere 113	tgarciaAIO102592	□
+ IBM: WebSphere Servlet Session Group Discovery	2041	10 mins	Snippet Configuration	IBM Websphere 113	tgarciaAIO102592	□
+ IBM: WebSphere ThreadPool Group Discovery	2030	10 mins	Snippet Configuration	IBM Websphere 113	tgarciaAIO102592	□
+ IBM: WebSphere WebApps Group Discovery	2044	10 mins	Snippet Configuration	IBM Websphere 113	tgarciaAIO102592	□

[Select Action]

Copyright © 2003 - 2020 ScienceLogic, Inc. All rights reserved.

Chapter 47

JMX Base Pack *BETA*

Overview

The following sections describe how to configure and discover Java Management Extensions (JMX) resources for monitoring by SL1 using the *JMX Base Pack *BETA** PowerPack:

NOTE: For more information about the *JMX Base Pack *BETA** PowerPack, see the ***Monitoring Java Management Extensions (JMX)*** manual.

Prerequisites for Monitoring JMX Resources

Before you can monitor JMX resources in SL1 using the *JMX Base Pack *BETA** PowerPack, you must have the following information:

- The IP address of the HotSpot, JVM, or OpenJDK system that uses the JMX resources you want to monitor
- The username and password for the system that you want to monitor

- The specific port numbers that you want to monitor

Creating Credentials to Monitor JMX Resources

To configure SL1 to monitor JMX resources on a HotSpot, JVM, or OpenJDK system, you must first create a credential that enables SL1 to communicate with that system. There are two ways you can do this:

- If you are monitoring only a single port on the system, you can create a Basic/Snippet credential to monitor that specific port.
- If you are monitoring more than one port on the system, you must create a SOAP/XML credential to monitor those specific ports.

The processes for creating both types of credentials are described in this section.

Creating a Credential to Monitor a Single Port

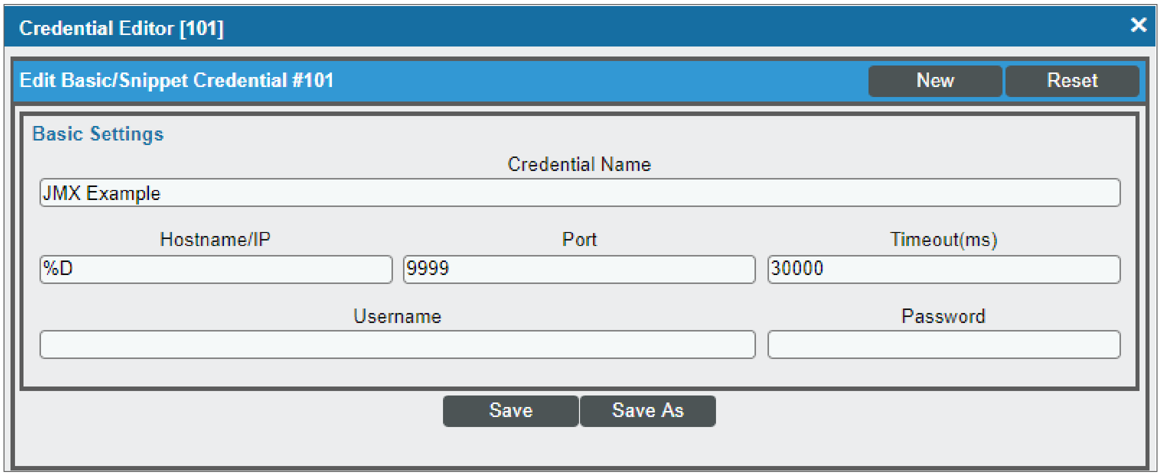
If you want to configure SL1 to monitor JMX resources on only a single port on a system, then you can create a Basic/Snippet credential to do so. This credential allows the Dynamic Applications in the *JMX Base Pack *BETA** PowerPack to connect with the server or virtual machine running JMX and access the port specified.

An example Basic/Snippet credential that you can edit for your own use is included in the PowerPack.

To create a Basic/Snippet credential:

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

2. Locate the **JMX Example** credential, and then click its wrench icon (🔧). The **Edit Basic/Snippet Credential** modal page appears:



Edit Basic/Snippet Credential #101

Basic Settings

Credential Name: JMX Example

Hostname/IP: %D

Port: 9999

Timeout(ms): 30000

Username:

Password:

3. Complete the following fields:

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

- ***Hostname/IP***. Type the IP address of the JMX system that you want to monitor, or type "%D".
- ***Port***. Type the port number that you want to monitor.
- ***Timeout(ms)***. Keep the default value.
- ***Username***. Type the username that is used to access the system that you want to monitor.
- ***Password***. Type the password that is used to access the system that you want to monitor.

4. Click the **[Save As]** button, and then click **[OK]**.

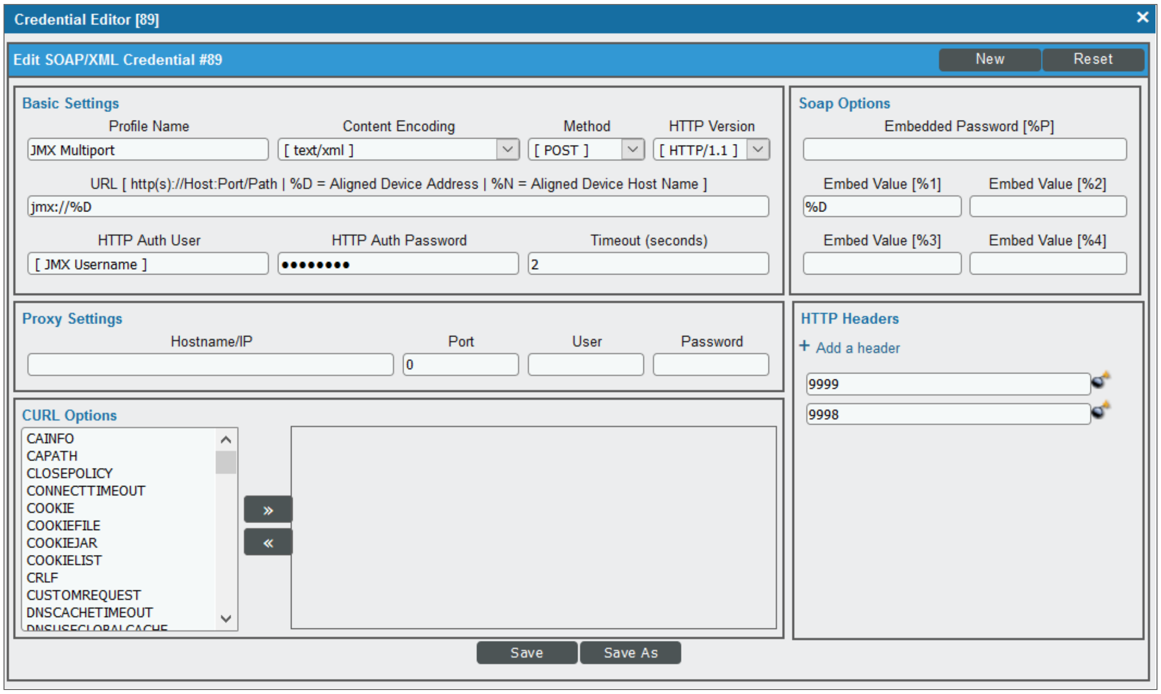
Creating a Credential to Monitor Multiple Ports

If you want to configure SL1 to monitor JMX resources on more than one port on a system, then you must create a SOAP/XML credential to do so. This credential allows the Dynamic Applications in the *JMX Base Pack *BETA** PowerPack to connect with the server or virtual machine running JMX and access all of the ports specified.

An example SOAP/XML credential that you can edit for your own use is included in the PowerPack.

To define a SOAP/XML credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **JMX Multiport** credential and click its wrench icon (🔧). The **Credential Editor** modal page appears:



Credential Editor [89]

Edit SOAP/XML Credential #89

Basic Settings

Profile Name	JMX Multiport
Content Encoding	[text/xml]
Method	[POST]
HTTP Version	[HTTP/1.1]
URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]	jmx://%D
HTTP Auth User	[JMX Username]
HTTP Auth Password	••••••••
Timeout (seconds)	2

Soap Options

Embedded Password [%P]	
Embed Value [%1]	%D
Embed Value [%2]	
Embed Value [%3]	
Embed Value [%4]	

Proxy Settings

Hostname/IP	
Port	0
User	
Password	

HTTP Headers

9999

9998

3. Enter values in the following fields:

Basic Settings

- ***Profile Name***. Type a new name for the credential.

- ***URL***. Keep the default value of "jmx://%D".
- ***HTTP Auth User***. Type the username that is used to access the system that you want to monitor.
- ***HTTP Auth Password***. Type the password that is used to access the system that you want to monitor.

SOAP Options

- ***Embed Value [%1]***. Type the IP address of the JMX system that you want to monitor, or type "%D".

HTTP Headers

- ***Add a header***. For each port that you want to monitor, click **[Add a header]** and then type the port number that you want to monitor in the blank field that appears.

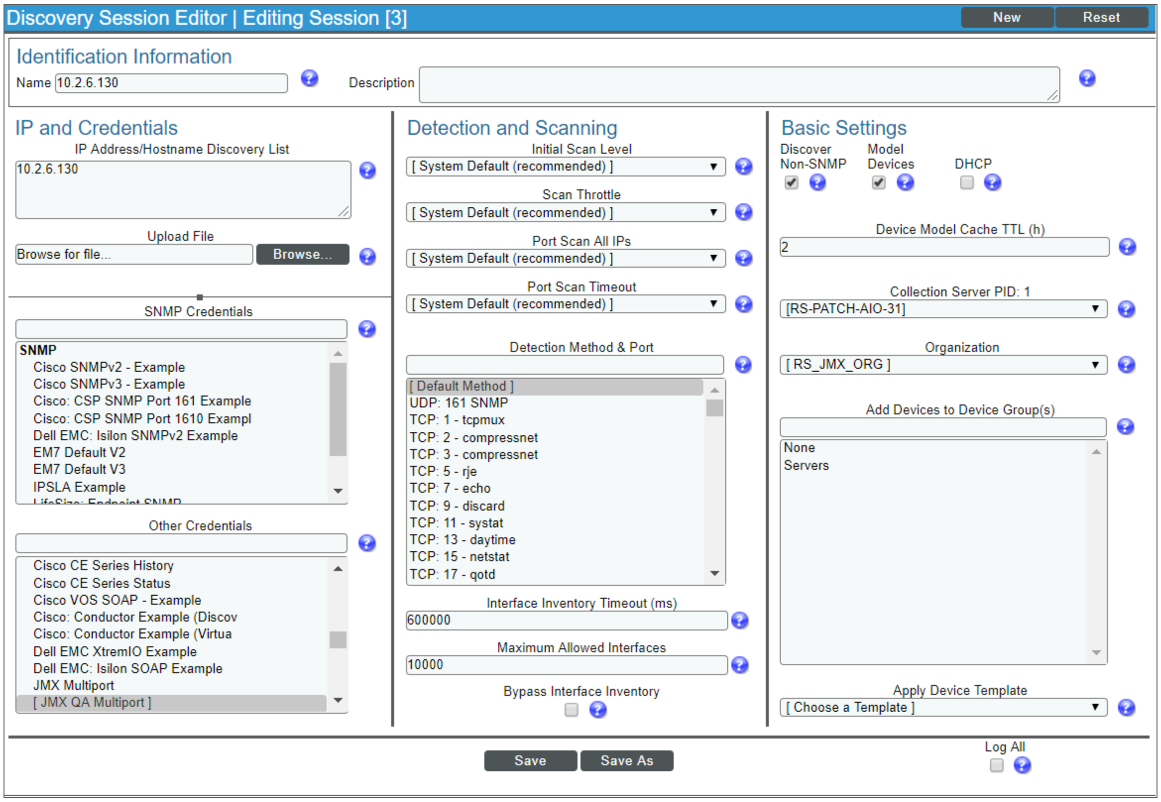
4. For all other fields, keep the default value.
5. Click the **[Save As]** button, and then click **[OK]**.

Discovering JMX Resources

To discover JMX resources:

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

3. On the **Discovery Session Editor** page, complete the following fields:



Discovery Session Editor | Editing Session [3]

Name: 10.2.6.130

IP Address/Hostname Discovery List: 10.2.6.130

Upload File: Browse for file...

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]

Interface Inventory Timeout (ms): 600000

Maximum Allowed Interfaces: 10000

Bypass Interface Inventory: □

Discover Non-SNMP: ☑

Model Devices: ☑

DHCP: □

Device Model Cache TTL (h): 2

Collection Server PID: 1: [RS-PATCH-AIO-31]

Organization: [RS_JMX_ORG]

Apply Device Template: [Choose a Template]

Log All: □

- ***Name***. Type a name for the discovery session.
- ***IP Address/Hostname Discovery List***. Type the hostname or IP address of the system that you want to monitor.
- ***Other Credentials***. Select the credential that you created for monitoring JMX resources.
- ***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 system is discovered, click the device icon (🖥) to view the **Device Properties** page for the system.

Understanding the Dynamic Applications in the JMX Base Pack *BETA* PowerPack

In most casesFor the most part, the Dynamic Applications in the *JMX Base Pack *BETA** PowerPack align to MBeans that are exposed in the server being monitored. A single MBean will generally have a performance Dynamic Application and a configuration Dynamic Application aligned to it. However, the "JMX: Base Configuration (Sample)" and "JMX: Base Performance (Sample)" Dynamic Applications provide an overview of the server metrics and thus span multiple MBeans.

If you collect the same data from different ports, then the configuration Dynamic Applications in the *JMX Base Pack *BETA** PowerPack will display the data for each port separately in the Configuration Report. Performance Dynamic Applications will display the metrics for all ports monitored by a particular Dynamic Application as different lines on its corresponding performance graph. If a performance collection is disabled on the server being monitored, the corresponding metric in SL1 will appear as a zero value.

Dynamic Applications with names appended by "(IBM)" are used to collect data from IBM servers, while those appended by "(HotSpot)" collect data from servers that are using HotSpot or OpenJDK. Dynamic Applications with names that are not appended by "(IBM)" or "(HotSpot)" are compatible with both. However, some of these Dynamic Applications, such as "JMX: Memory Configuration", might collect more or different data from one source over the other, depending on the detail of the server type being monitored. This behavior is expected.

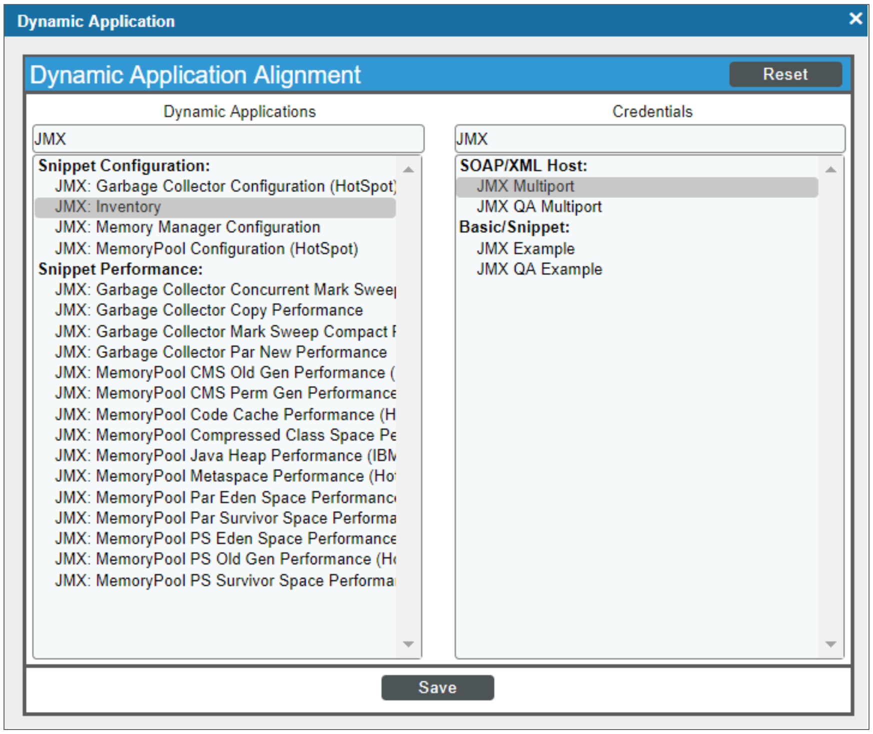
Manually Aligning the "JMX: Inventory" Dynamic Application

The "JMX: Inventory" Dynamic Application is not automatically aligned to your JMX system during discovery because of the possible load it can place on the Data Collector in some situations. This Dynamic Application provides a list of all JMX values that the system exports and their most recent values. You can then use that information to check that all necessary values are available for the system or create a new Dynamic Application to collect specific metrics that are not collected by other Dynamic Applications in the *JMX Base Pack *BETA** PowerPack. If you want to use the "JMX: Inventory" Dynamic Application, you must manually align it to your JMX system.

To manually align the "JMX: Inventory" Dynamic Application:

1. From the **Device Properties** page (Registry > Devices > wrench icon) for the JMX system, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. Click the **[Action]** button and then click *Add Dynamic Application*. The **Dynamic Application Alignment** page appears.
3. In the ***Dynamic Applications*** field, select the "JMX: Inventory" Dynamic Application.

4. In the ***Credentials*** field, select the credential you created for monitoring JMX resources.



JMX

Snippet Configuration:
JMX: Garbage Collector Configuration (HotSpot)
JMX: Inventory
JMX: Memory Manager Configuration
JMX: MemoryPool Configuration (HotSpot)
Snippet Performance:
JMX: Garbage Collector Concurrent Mark Sweep
JMX: Garbage Collector Copy Performance
JMX: Garbage Collector Mark Sweep Compact F
JMX: Garbage Collector Par New Performance
JMX: MemoryPool CMS Old Gen Performance (
JMX: MemoryPool CMS Perm Gen Performance
JMX: MemoryPool Code Cache Performance (H
JMX: MemoryPool Compressed Class Space Pe
JMX: MemoryPool Java Heap Performance (IBM
JMX: MemoryPool Metaspace Performance (Ho
JMX: MemoryPool Par Eden Space Performance
JMX: MemoryPool Par Survivor Space Performa
JMX: MemoryPool PS Eden Space Performance
JMX: MemoryPool PS Old Gen Performance (H
JMX: MemoryPool PS Survivor Space Performa

JMX

SOAP/XML Host:
JMX Multiport
JMX QA Multiport
Basic/Snippet:
JMX Example
JMX QA Example

5. Click the **[Save]** button.

Chapter 48

Kubernetes

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 and discover Kubernetes clusters for monitoring by SL1 using the *Kubernetes* PowerPack:

> NOTE: For more information about the *Kubernetes* PowerPack, see the ***Monitoring Kubernetes*** manual.

Prerequisites for Monitoring Kubernetes Clusters

Before you can monitor Kubernetes clusters using the *Kubernetes* PowerPack, you must first do the following:

1. If you will be using Dynamic Applications from the *Linux Base Pack* PowerPack, import and install version 103.
2. Create a Kubernetes service account that SL1 can use to communicate with the Kubernetes API. This service account must have the minimum permissions set in the ***Required Permissions for the Service Account Token*** section.
3. Extract the service account token.
4. Ensure that cURL 7.40 or greater is installed on all Kubernetes nodes that you want to monitor.
5. Configure SSH credentials on the Kubernetes nodes. These credentials must be the same on all nodes, and are used to retrieve data from the underlying Linux OS.

For more information about any of these steps, see https://kubernetes.io/docs/reference/access-authn-authz/rbac/.

Required Permissions for the Service Account Token

The minimum required permissions are required for the service account token:

~~~~
```

apiVersion: rbac.authorization.k8s.io/v1

kind: ClusterRole

metadata:
  name: cluster-limited

rules:

- apiGroups:

_ '*'

resources:

- nodes

- pods

- replicationcontrollers

- deployments

- statefulsets
~~~~

~~~
- replicasets
- daemonsets
- cronjobs
- jobs
- componentstatuses
- namespaces
- persistentvolumes
- persistentvolumeclaims
- services
- events
- ingresses
- horizontalpodautoscalers
verbs:
- get
- list
- watch
```
~~~

Creating Credentials for Kubernetes Clusters

Unlike other PowerPacks, you ***must not*** create a credential for Kubernetes using the **Credential Management** page (System > Manage > Credentials).

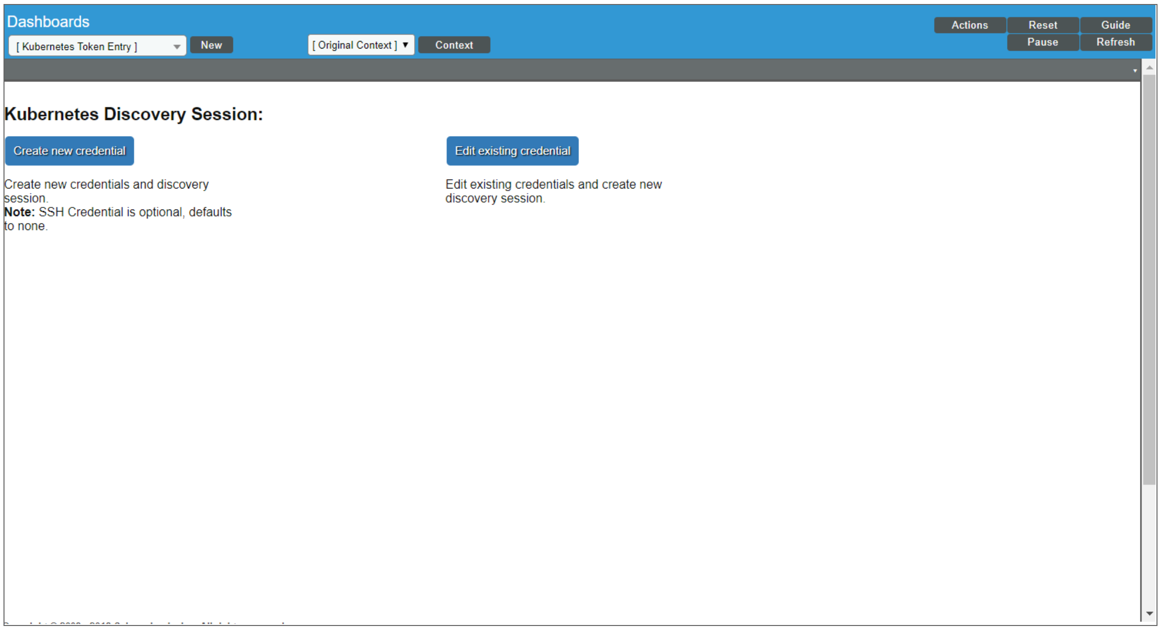
Instead, you must use the **Kubernetes Token Entry** dashboard that is included in the *Kubernetes* PowerPack. This dashboard automatically creates the following credentials based on your input:

- ***A master SSH/Key Credential***. This credential enables SL1 to communicate with the Kubernetes API so that it can monitor the Kubernetes master. It includes a host IP address, port number, and the service account token.
- ***A SOAP/XML Credential***. This credential includes HTTP headers that enable you to specify the Kubernetes topology that you want SL1 to discover.
- ***A node SSH/Key Credential***. This credential enables SL1 to monitor and run Dynamic Applications on Kubernetes nodes.

To create credentials for Kubernetes clusters:

1. Click the **Dashboards tab**. In the drop-down field in the upper-left corner of the page, select *Kubernetes Token Entry*.

2. On the **Kubernetes Token Entry** dashboard page, click **[Create new credential]**.



Kubernetes Discovery Session:

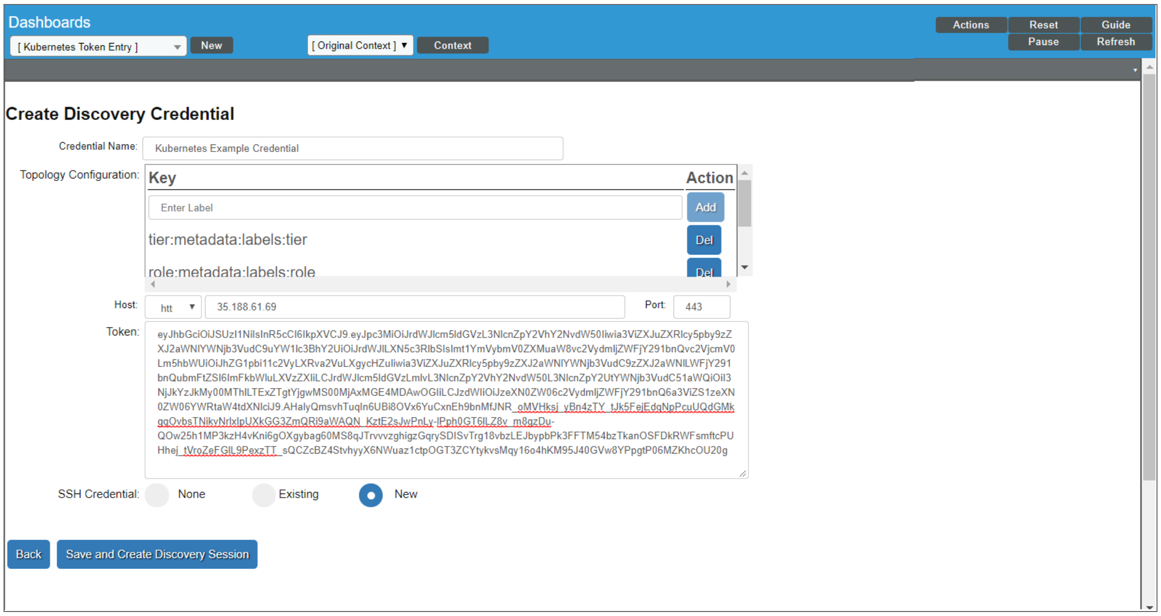
Create new credential

Create new credentials and discovery session.
Note: SSH Credential is optional, defaults to none.

Edit existing credential

Edit existing credentials and create new discovery session.

3. On the **Create Discovery Credential** dashboard page:



Create Discovery Credential

Credential Name: Kubernetes Example Credential

Topology Configuration:

Key	Action
Enter Label	Add
tier:metadata:labels:tier	Del
role:metadata:labels:role	Del

Host: htt ▼ 35.188.61.69 Port: 443

Token:

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJrdWJlcm5ldGVzL3NlcnZpY2VhY2NvdW50Iiwia3ViZXJuZXRlcy5pby9zZ
XJ2aWNlYWNjb3VudC9uYW1lc3BhY2UiOiJrdWJlLXN5c3RlbSIsImt1YmVybmV0ZXMuaW8vc2VydmljZWFjY291bnQvc2VjcmV0
Lm5hbWUiOiJhZG1pbi11c2VyLXRva2VuLXgycHZuIiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZXJ2aWNlLWFjY291
bnQubmFtZSI6ImFkbWluLXVzZXIiLCJrdWJlcm5ldGVzLmlvL3NlcnZpY2VhY2NvdW50L3NlcnZpY2UtYWNjb3VudC51aWQiOiI3
NjJkYzJkMy00MThlLTExZTgtYjgwMS00MjAxMGE4MDAwOGIiLCJzdWIiOiJzeXN0ZW06c2VydmljZWFjY291bnQ6a3ViZS1zeXN
0ZW06YWRtaW4tdXNlciJ9.AHalyQmsvhTuqln6UBi8OVx6YuCxnEh9bnMfJNR_oMVHksj_yBn4zTY_tJk5FejEdqNpPcuUQdGMk
gqOvbsTNikvNrlxlpUXkGG3ZmQRi9aWAQN_KztE2sJwPnLy-lPph0GT6lLZ8v_m8gzDu-
QOw25h1MP3kzH4vKni6gOXgybag60MS8qJTrvvvzghigzGqrySDISvTrg18vbzLEJbypbPk3FFTM54bzTkanOSFDkRWFsmftcPU
Hhej_tVroZeFGlL9PexzTT_sQCZcBZ4StvhyyX6NWuaz1ctpOGT3ZCYtykvsMqy16o4hKM95J40GVw8YPpgtP06MZKhcOU20g
```

SSH Credential: ○ None ○ Existing ● New

Back

Save and Create Discovery Session

- In the ***Credential Name*** field, type a name for the Kubernetes master SSH/Key credential.

- In the ***Topology Configuration*** field:
    - In the ***Enter Label*** field, type a topology definition that you want SL1 to use when discovering Kubernetes component devices. (For more information, see the ***Specifying the Kubernetes Topology for Discovery*** section.)
    - Click **[Add]**.
    - Repeat the previous two steps as needed until you have fully defined the discovery topology configuration.

NOTE: Specifying the discovery topology configuration creates a SOAP/XML credential that uses cURL commands for topology discovery.

- In the ***Host*** field, select *https://* if the IP address is secure or *http://* if it is not, and then type the IP address of the Kubernetes cluster.
- In the ***Port*** field, type the IP address port for the Kubernetes cluster.

NOTE: Ports 443 or 8443 are typically used for HTTPS.

NOTE: For steps on how to configure a customized IP port and to edit the snippet code in some Run Book Actions to use that IP port, see the ***Configuring Customized IP Ports*** section.

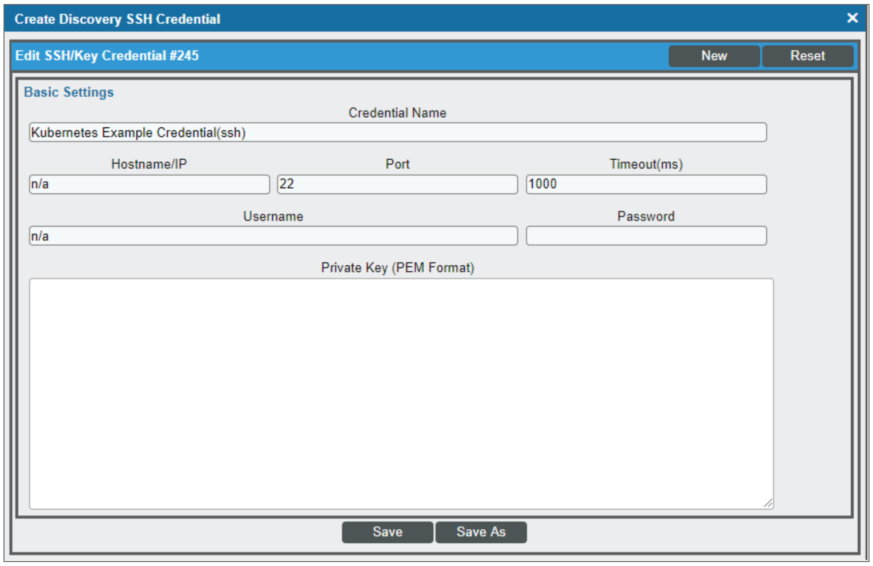
- In the ***Token*** field, paste your Kubernetes service account token.
- In the ***SSH Credential*** field:
    - Select *None* if you do not want to create or use an additional SSH/Key credential to monitor Kubernetes nodes.

NOTE: To fully monitor Kubernetes, a standard SSH/Key credential is required to communicate with the Kubernetes node.

    - Select *Existing* if you want to use an existing SSH/Key credential to monitor Kubernetes nodes, and then select that credential from the ***Existing SSH Key*** drop-down field.
    - Select *New* if you want to create a new SSH/Key credential to monitor Kubernetes nodes.

4. Click the **[Save and Create Discovery Session]** button.
    - If you selected *None* or *Existing* in the ***SSH Credential*** field, then SL1 saves your Kubernetes credentials and creates a new discovery session. Proceed to the ***Discovering a Kubernetes Cluster*** section.
    - If you selected *New* in the ***SSH Credential*** field, then the **Edit SSH/Key Credential** modal page appears. Proceed to step 5.

5. On the **Edit SSH/Key Credential** modal page, make entries in the following fields:



Create Discovery SSH Credential

Edit SSH/Key Credential #245

Basic Settings

Credential Name: Kubernetes Example Credential(ssh)

Hostname/IP: n/a

Port: 22

Timeout(ms): 1000

Username: n/a

Password:

Private Key (PEM Format):

- ***Credential Name***. Defaults to the same credential name as the Kubernetes master SSH/Key credential name that you entered in step 3, followed by "(ssh)".
- ***Hostname/IP***. Type "%D".
- ***Port***. Type the IP port of the Kubernetes nodes.

NOTE: Port 22 is typically used for SSH.

- ***Timeout (ms)***. Type the time, in milliseconds, after which SL1 will stop trying to communicate with the Kubernetes nodes. ScienceLogic recommends setting this field to a value of at least 1,000; however, you can increase the value if you experience high network latency.
- ***Username***. Type the SSH account username.

  If you want to monitor multiple EKS clusters, you must type the AWS EKS token account ID, the region name, and the cluster name in this field in the following format:

  ```
  AWS-EKS-token-account-id:region-name:cluster-name
  ```

  For example:

  ```
  1234567890121:us-east-1:ekscluster
  ```

- ***Password***. Type the password for the SSH account.
- ***Private Key (PEM Format)***. Type the SSH private key that you want SL1 to use to monitor the Kubernetes nodes.

NOTE: Most systems will require ***either*** a password or a private key for authentication.

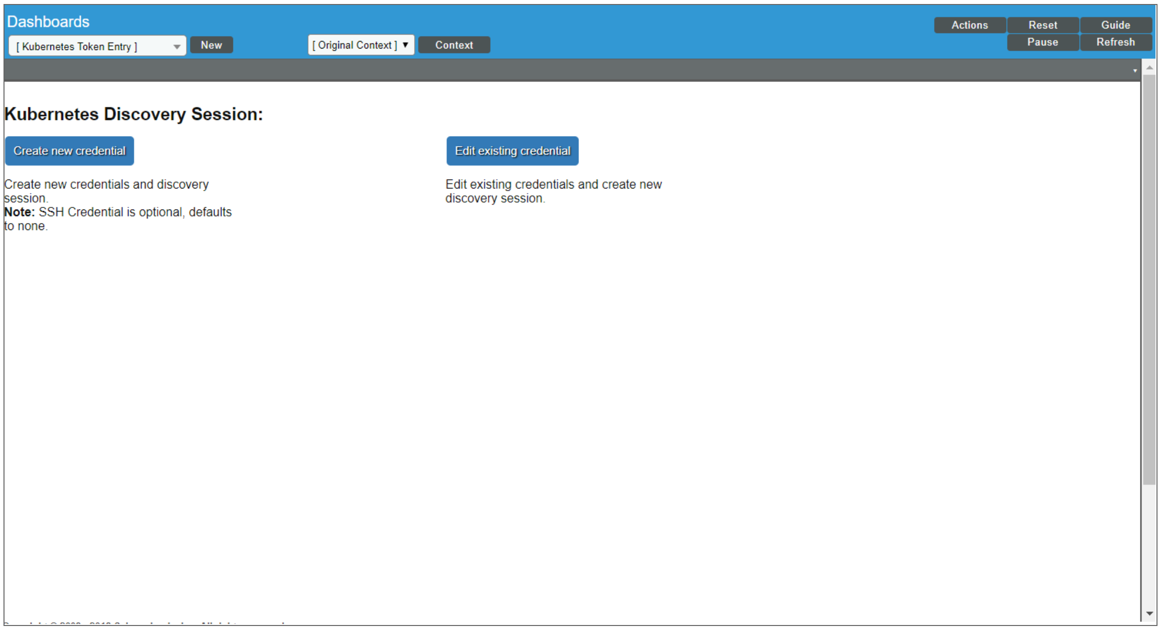
6. Click **[Save]** to save the SSH/Key credential for monitoring Kubernetes nodes. The **Create Discovery Credential** dashboard page appears again.
7. In the ***Existing SSH Key*** drop-down field, select the SSH/Key credential that you created in steps 5 and 6.
8. Click the **[Save and Create Discovery Session]** button.

WARNING: If you created an SSH/Key credential for Kubernetes nodes in steps 5 and 6, you must click the **[Save and Create Discovery Session]** button, as indicated in step 8, even though you already clicked the button once in step 4. Clicking the button the first time saved your Kubernetes master SSH/Key and SOAP/XML credentials; clicking it the second time will link the node SSH/Key credential to the master SSH/Key credential.

Configure the Discovery Session to Exclude Dynamic Applications from the Linux Base Pack

To configure the discovery session to exclude aligning *Linux Base Pack* Dynamic Applications:

1. On the **Kubernetes Token Entry** dashboard page, click **[Create new credential]**.

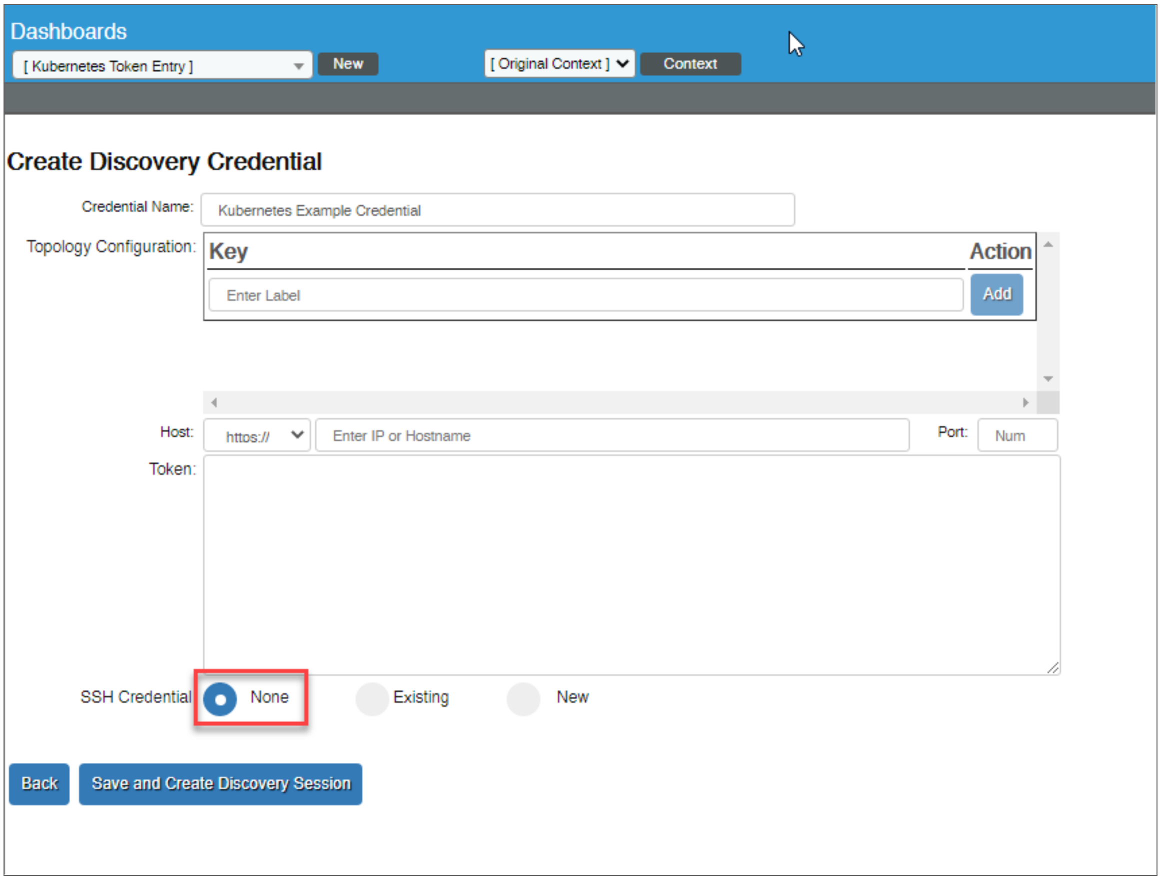


Kubernetes Discovery Session:

Create new credentials and discovery session.
Note: SSH Credential is optional, defaults to none.

Edit existing credentials and create new discovery session.

2. On the **Create Discovery Credential** dashboard page, fill out the fields as described in the *Creating Credentials for Kubernetes Clusters* section, then select **None** in the ***SSH Credential*** field.



Create Discovery Credential

Credential Name: Kubernetes Example Credential

Topology Configuration:

Key	Action
Enter Label	Add

Host: https:// Enter IP or Hostname Port: Num

Token:

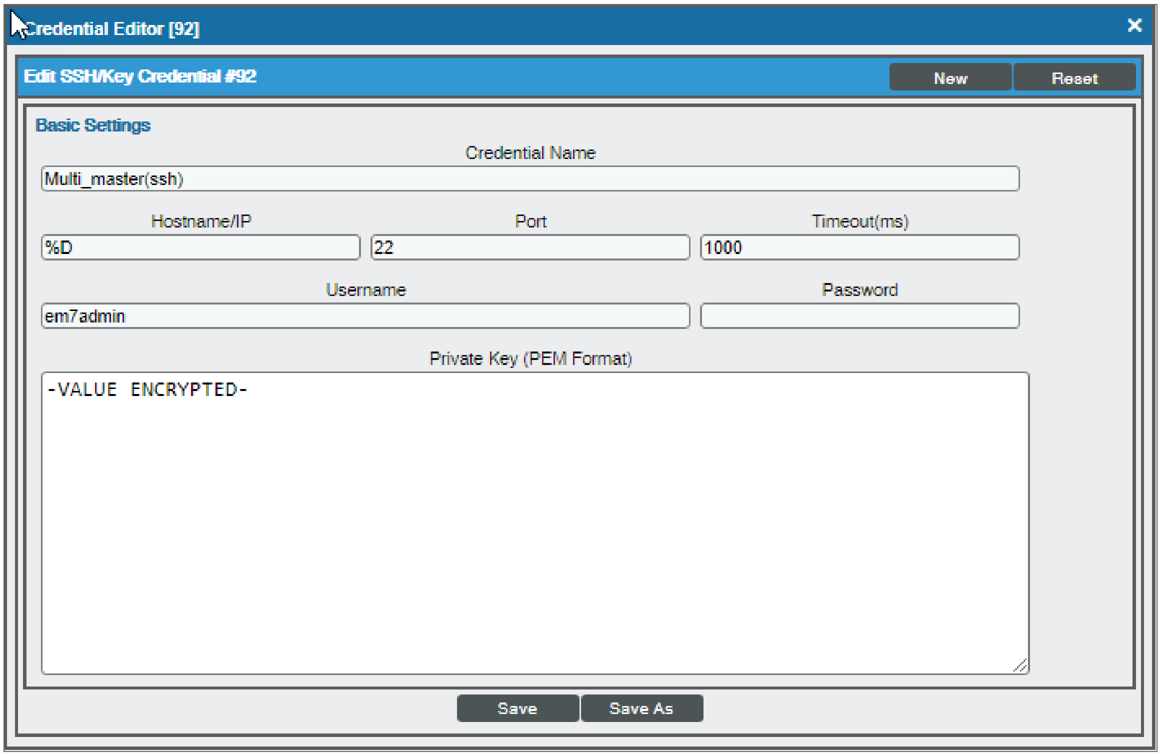
SSH Credential ● None ○ Existing ○ New

4. Click the **[Save and Create Discovery Session]** button.
5. Since you selected *None* in the ***SSH Credential*** field, SL1 saves your Kubernetes credentials and creates a new discovery session. Proceed to the ***Discovering a Kubernetes Cluster*** section to finish the process. The Kubernetes cluster will be discovered and there will not be any *Linux Base Pack* Dynamic Applications aligned.

Enabling Data Collection for Linux Base Pack Dynamic Applications

If you previously disabled auto-aligning the Linux Dynamic Applications and need to monitor a Linux machine that your nodes are deployed on, you can enable and align the *Linux Base Pack* Dynamic Applications by performing the following steps:

1. Create an SSH/Key credential. When naming the credential, use the name of the SSH/Key credential that you have already created for Kubernetes, but add "SSH" in the title. For example, if your credential name is "Multi_master", name it "Multi_master(ssh)":



Credential Editor [92]

Edit SSH/Key Credential #92

Basic Settings

Credential Name: Multi_master(ssh)

Hostname/IP: %D

Port: 22

Timeout(ms): 1000

Username: em7admin

Password:

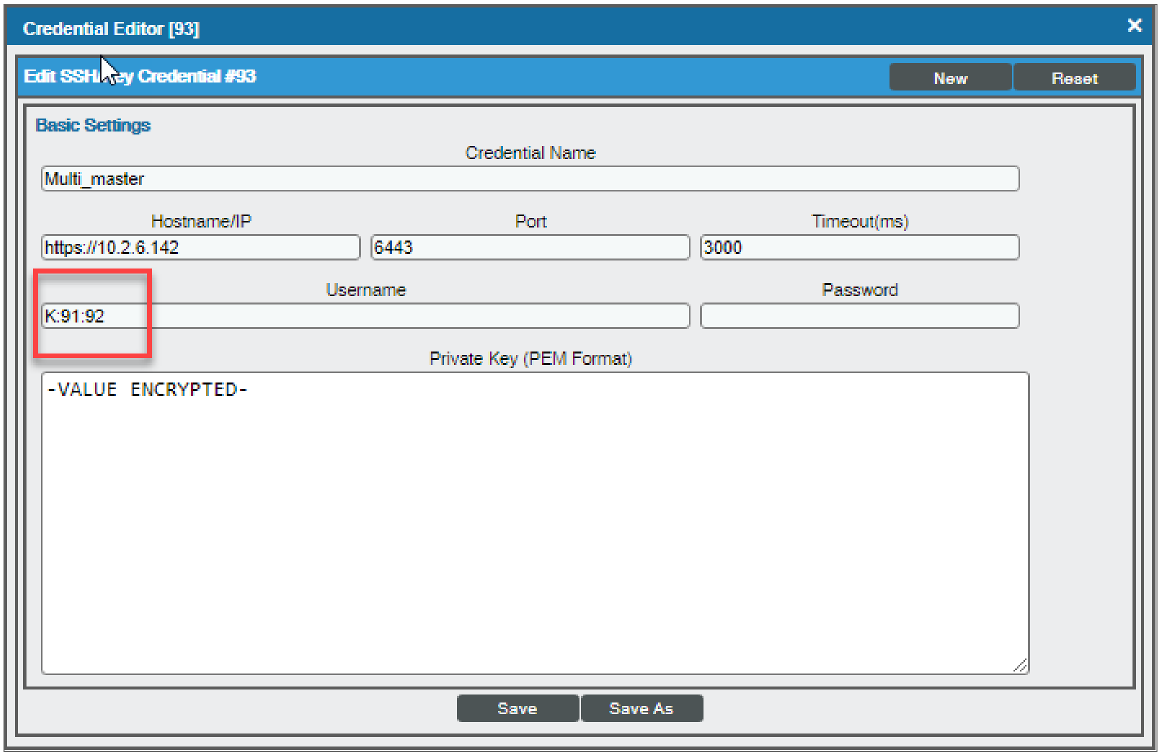
Private Key (PEM Format):

```
-VALUE ENCRYPTED-
```

2. Go to the **Kubernetes Token Entry** dashboard page, and click **[Edit existing credential]**.
3. Select the *original credential you created* (in our example, "Multi_master") in the ***Credential*** field.
4. In the ***SSH Credential*** field, select *Existing*.
5. In the ***Existing SSH Key*** field, select the SSH credential that you created in step 1 (in our example, "Multi_master(ssh)").
6. Click **[Save and Create Discovery Session]**.

NOTE: A copy of the original discovery session will appear in the **Discovery Control Panel**, but it will not automatically run. You may delete this discovery session.

7. Locate original Kubernetes credential in the **Credential Management** page (System > Manage > Credentials) and click its wrench icon (🔧).
8. Validate that the Kubernetes credential has been updated by confirming that the ***Username*** field now contains the ID of the new SSH credential:



Credential Name: Multi_master

Hostname/IP: https://10.2.6.142

Port: 6443

Timeout(ms): 3000

Username: K:91:92

Password:

Private Key (PEM Format):

```
-VALUE ENCRYPTED-
```

9. After about 15 minutes all the *Linux Base Pack* Dynamic Applications will align to the Kubernetes nodes.

If the Linux Base Pack Dynamic Applications are not aligning, you may need to clear the cache on the Data Collector that contains the cluster. To do this, execute the following query on the Data Collector:

```
DELETE

FROM cache.dynamic_app

WHERE 'key' LIKE 'KUBERNETES_NODE_APP_ALIGN_STATUS_%'
```

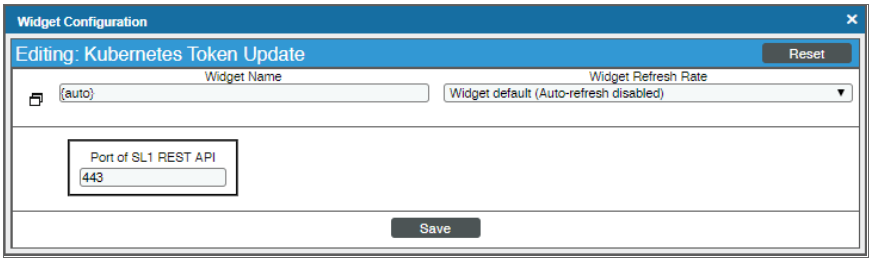
Configuring Customized IP Ports

To use a custom IP address port with your Kubernetes cluster, perform the following steps:

1. Go to the **Dashboards** page (System > Customize > Dashboards).

2. In the ***Dashboard Name*** column, type "Kubernetes Token Entry". Click the wrench icon (🔧) for the dashboard to open the **Dashboard Editor** page.

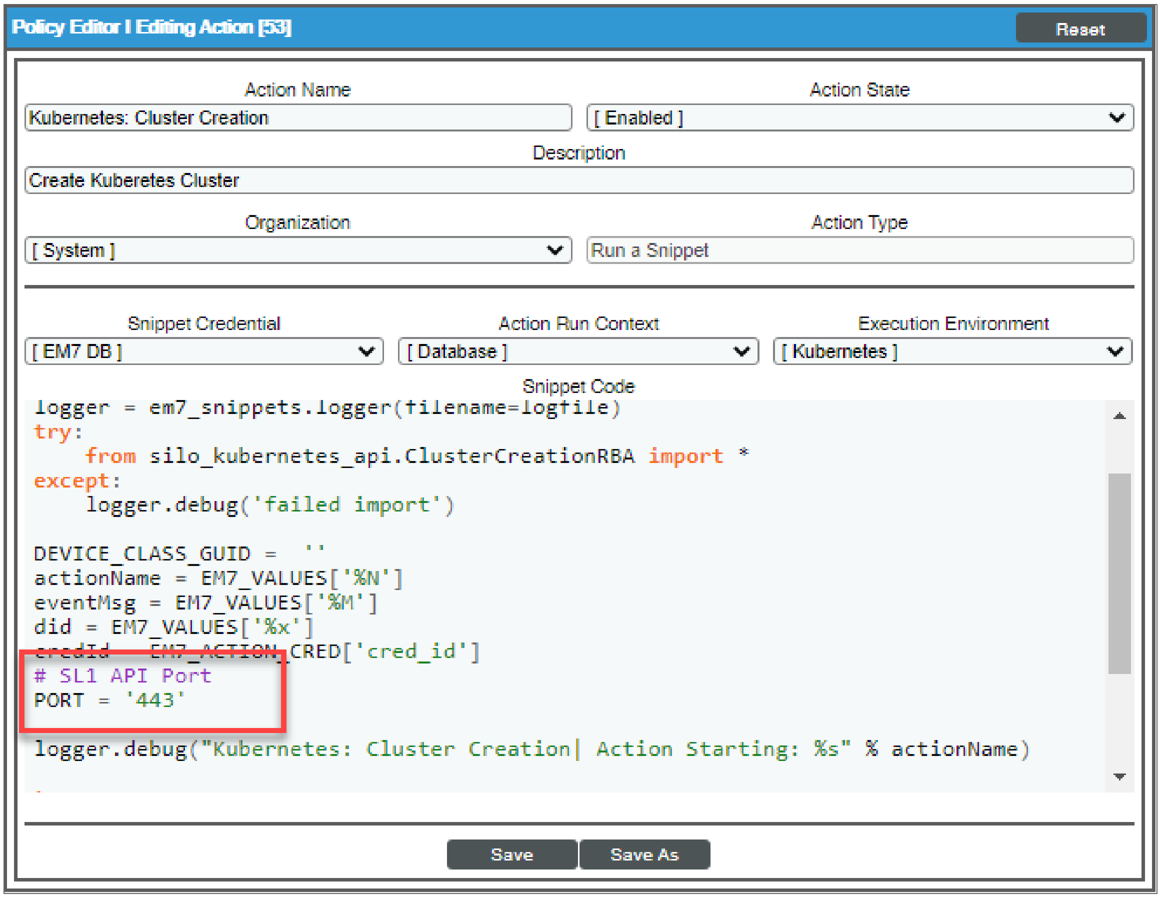
3. In the **Dashboard Editor** page, go to the top-right corner of the widget and click ***Options*** > ***Configure*** to open the **Widget Configuration** window. In the ***Widget Configuration*** window, type your custom port number into the ***Port of SL1 REST API*** field.



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

If you are using a customized IP port for your Kubernetes cluster, you will need to edit the snippet code in some of the PowerPack's run book actions for discovery to run successfully. To do so:

1. Go to the **Action Policy Manager** page (Registry > Run Book > Actions).
2. Locate the "Kubernetes: Cluster Creation" run book action and click its wrench icon (🔧).
3. In the **Action Policy Editor** window, find the entry for `PORT` in the ***Snippet Code*** field and update the entry to your customized port number.



Action Name: Kubernetes: Cluster Creation

Action State: [Enabled]

Description: Create Kuberetes Cluster

Organization: [System]

Action Type: Run a Snippet

Snippet Credential: [EM7 DB]

Action Run Context: [Database]

Execution Environment: [Kubernetes]

Snippet Code

```
logger = em7_snippets.logger(filename=logfile)
try:
    from silo_kubernetes_api.ClusterCreationRBA import *
except:
    logger.debug('failed import')

DEVICE_CLASS_GUID =  ''
actionName = EM7_VALUES['%N']
eventMsg = EM7_VALUES['%M']
did = EM7_VALUES['%x']
credId = EM7_ACTION_CRED['cred_id']
# SL1 API Port
PORT = '443'

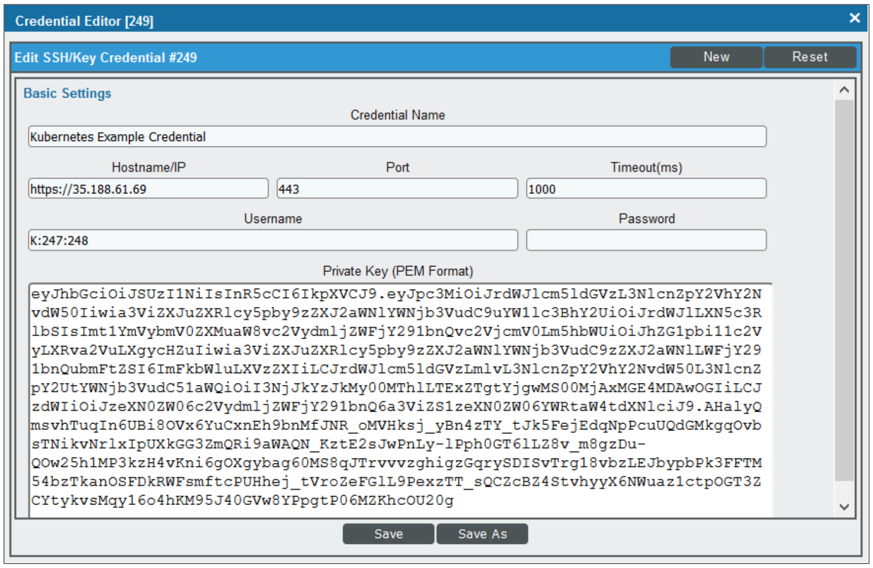
logger.debug("Kubernetes: Cluster Creation| Action Starting: %s" % actionName)
```

4. Click **[Save]**.
5. Repeat these steps for the following run book actions:
    - Kubernetes: GCP Cluster Update
    - Kubernetes: Node App Alignment
    - Kubernetes: Set Namespace Vanishing Timer

Viewing the Kubernetes Credentials

After you have created the Kubernetes credentials using the **Kubernetes Token Entry** dashboard, you can view the credentials on the **Credential Management** page (System > Manage > Credentials).

Master SSH/Key Credential



Credential Name: Kubernetes Example Credential

Hostname/IP: https://35.188.61.69

Port: 443

Timeout(ms): 1000

Username: K:247:248

Password:

Private Key (PEM Format)

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJrdWJlcm5ldGVzL3NlcnZpY2VhY2N
vdW50Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9uYW1lc3BhY2UiOiJrdWJlLXN5c3R
lbSIsImt1YmVybmV0ZXMuaW8vc2VydmljZWFjY291bnQvc2VjcmV0Lm5hbWUiOiJhZG1pbi11c2V
yLXRva2VuLXgycHZuIiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZXJ2aWNlLWFjY29
1bnQubmFtZSI6ImFkbWluLXVzZXIiLCJrdWJlcm5ldGVzLmlvL3NlcnZpY2VhY2NvdW50L3NlcnZ
pY2UtYWNjb3VudC51aWQiOiI3NjJkYzJkMy00MThlLTExZTgtYjgwMS00MjAxMGE4MDAwOGIiLCJ
zdWIiOiJzeXN0ZW06c2VydmljZWFjY291bnQ6a3ViZS1zeXN0ZW06YWRtaW4tdXNlciJ9.AHalyQ
msvhTuqIn6UBi8OVx6YuCxnEh9bnMfJNR_oMVHksj_yBn4zTY_tJk5FejEdqNpPcuUQdGMkgqOvb
sTNikvNrlxIpUXkGG3ZmQRi9aWAQN_KztE2sJwPnLy-lPph0GT6lLZ8v_m8gzDu-
QOw25h1MP3kzH4vKni6gOXgybag60MS8qJTrvvvzghigzGqrySDISvTrg18vbzLEJbypbPk3FFTM
54bzTkanOSFDkRWFsmftcPUHhej_tVroZeFGlL9PexzTT_sQCZcBZ4StvhyyX6NWuaz1ctpOGT3Z
CYtykvsMqy16o4hKM95J40GVw8YPpgtP06MZKhcOU20g
```

WARNING: You must not modify the master SSH/Key credential from this page. You must use the **Kubernetes Token Entry** dashboard to edit the master credential.

The master SSH/Key credential will include the ***Credential Name***, ***Hostname/IP***, ***Port***, and ***Private Key*** (service account token) values that you entered on the **Create Discovery Credential** dashboard page.

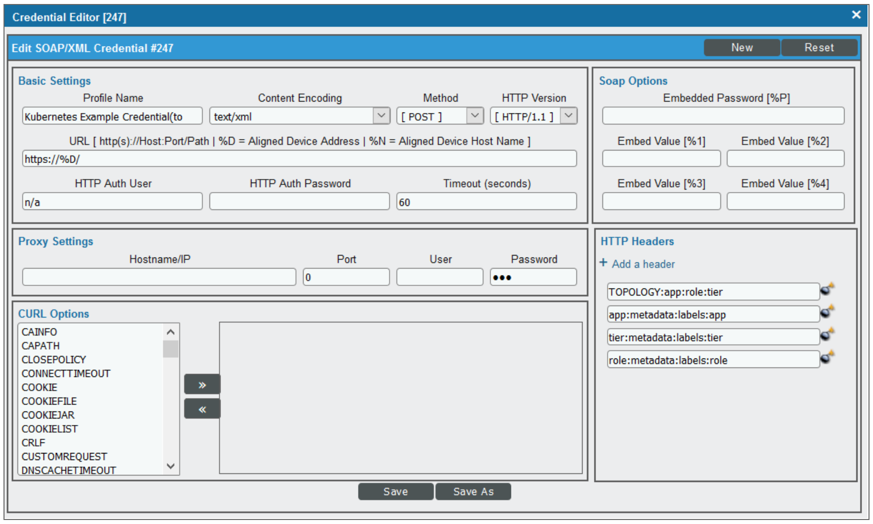
The ***Timeout(ms)*** field displays the default timeout value. You can edit this value if needed.

The ***Username*** field indicates the SOAP/XML credential and optional node SSH/Key credential that are associated with this master SSH/Key credential. The ***Username*** value is auto-generated in the following format:

```
K:SOAP/XML Credential ID #:Node SSH/Key Credential ID #
```

The ***Password*** field should remain blank.

SOAP/XML Credential



Profile Name: Kubernetes Example Credential(to

Content Encoding: text/xml

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://%D/

HTTP Auth User: n/a

HTTP Auth Password:

Timeout (seconds): 60

Embedded Password [%P]:

Embed Value [%1]:

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

Hostname/IP:

Port: 0

User:

Password: •••

HTTP Headers:
- TOPOLOGY:app:role:tier
- app:metadata:labels:app
- tier:metadata:labels:tier
- role:metadata:labels:role

CURL Options:
- CAINFO
- CAPATH
- CLOSEPOLICY
- CONNECTTIMEOUT
- COOKIE
- COOKIEFILE
- COOKIEJAR
- COOKIELIST
- CRLF
- CUSTOMREQUEST
- DNSCACHETIMEOUT

The SOAP/XML credential will include the ***HTTP Headers*** field values that you entered in the ***Topology Configuration*** field on the **Create Discovery Credential** dashboard page.

The ***Profile Name*** field defaults to the same credential name as the Kubernetes master SSH/Key credential name, followed by "(topo)".

All other fields in this credential use the default values needed for monitoring Kubernetes clusters.

Node SSH/Key Credential

The node SSH/Key credential will include the values that you defined on the **Edit SSH/Key Credential** modal page, as described in the *Creating Credentials for Kubernetes Clusters* section.

Specifying the Kubernetes Topology for Discovery

The *Kubernetes* PowerPack utilizes a ***flexible device topology***. This flexible topology enables you to specify the device component map hierarchy that you want SL1 to create when discovering and modeling your Kubernetes devices, rather than using a hierarchy that is pre-defined in the PowerPack.

When ***creating your Kubernetes credentials***, you can specify the device topology that you want to be modeled upon discovery. The topology is based on labels used in Kubernetes.

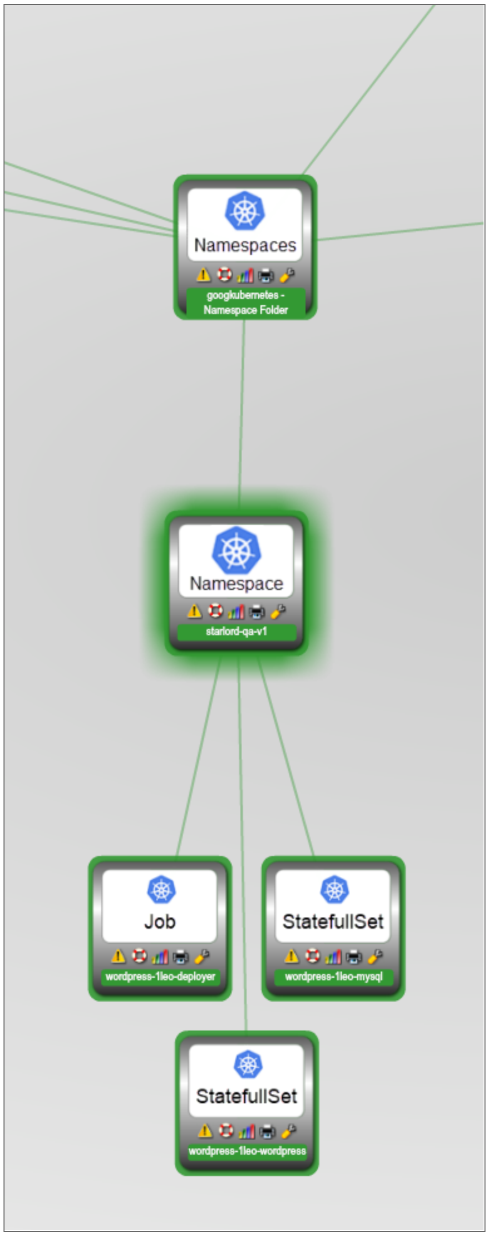
For example, if you want to separate your production and development environments, you could use labels such as "environment=prod" and "environment=dev" in Kubernetes. When discovering your Kubernetes system, SL1 could then use those labels to utilize the following features:

- ***Aggregation***. This enables SL1 to model the aggregation point and create a component device in the platform that represents grouping based on these labels. If just aggregation is required, then the device component map would display a component device for "dev" and another component device for "prod". All of the components with the "dev" and "prod" labels would then appear under those two component devices.
- ***Filtering***. This enables SL1 to create additional components that match a Kubernetes label. So in the case of the environment label, SL1 could selectively model only the production environment. (In this scenario, all of the controllers that do not match the production label would still appear in the device component map under the namespace.)

Example: Defining the Topology

The first step to utilizing the flexible topology is to define the topology and the components that you want to appear on the device component map.

The following example shows an application and its tiers modeled on a device component map ***without*** a defined topology:



To define the Kubernetes topology, you must first type a topology definition into the ***Topology Configuration*** field when *using the Kubernetes Token Entry dashboard to create your Kubernetes discovery credentials*. For example:

> TOPOLOGY:Application:Tier

This definition declares that additional components will be created in the device component map to reflect Applications and Application Tiers.

When defining the topology, keep the following important rules in mind:

- "TOPOLOGY" must be capitalized.
- The labels included in your topology definition are used to identify the component devices that will appear on the device component map. These labels ***must*** match a device class's ***Class Identifier 2*** component identifier. For more information about component identifiers and the ***Class Identifier 2*** identifier, see the ***Dynamic Application Development*** manual.
- The labels in your topology definition must be preceded by a colon, without a space.

Example: Defining the Application and Tier Labels

The next step is to define which Kubernetes labels will be used to identify the application and the tier. Once again, you will do so by adding entries to the ***Topology Configuration*** field in the ***Kubernetes Token Entry dashboard***. For example, you could enter the following to define the application:

```
Application:metadata:labels:app
```

This definition states that the Kubernetes label "app" will be used to create the application component.

Finally, the same is done for the Tier component, as follows:

```
Tier:metadata:labels:tier
```

This definition will use the label "tier" to create the application tier component.

You must define each of the components listed in your topology definition. Therefore, if the topology definition in the previous example included other components in addition to "Application" and "Tier", those would need to be defined similar to the application and tier definition examples in this section.

When defining these components, the first terms in the definitions must match the labels used in the topology definition. The middle terms in the definition represent the list of keys in the API response for a pod that identifies the members of that tier. The final term in the definition is the component's name.

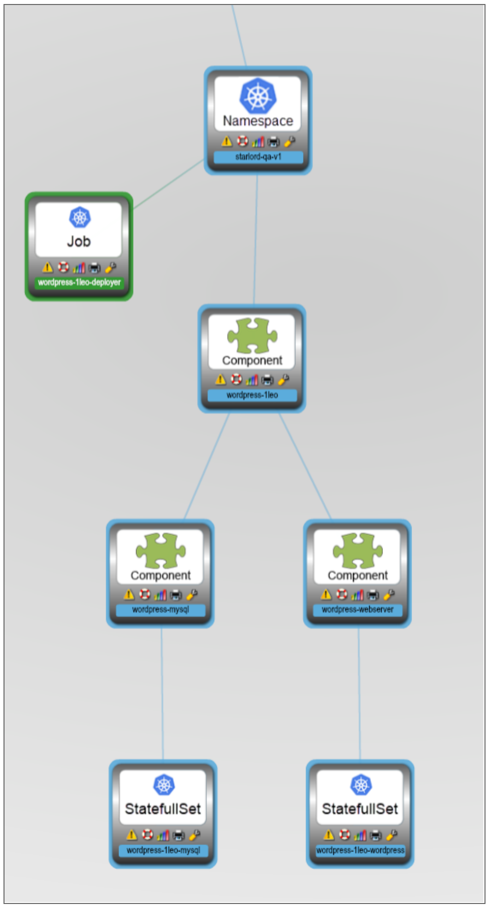
You can other API responses from the payload if they are meaningful to you. For example, if you wanted to have a component based on an application and another based on the field "dnsPolicy", then your topology definition would be "TOPOLOGY:Application:DNSPolicy", and your component definitions would be as follows:

```
Application:metadata:labels:app

DNSPolicy:dnsPolicy
```

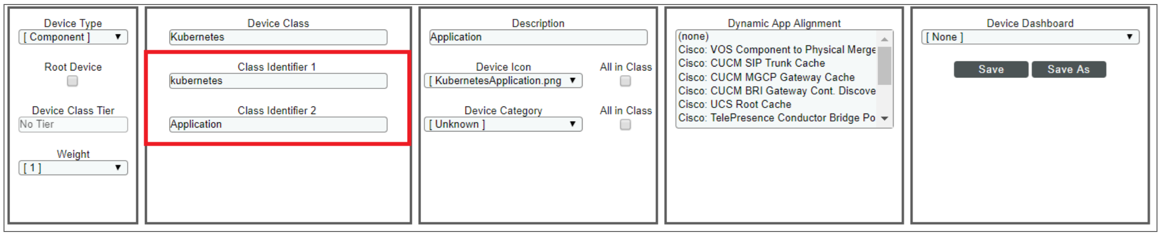
Example: Creating the Application and Tier Device Classes

The following example illustrates what the device component map might look like after the topology definitions are entered, as described in the previous two sections:



In this example, the generic "Component" device appears in the device component map. This is because no device classes match the names used in the topology definition and thus, SL1 uses a default device class.

For the purposes of this example, the following device classes are created:



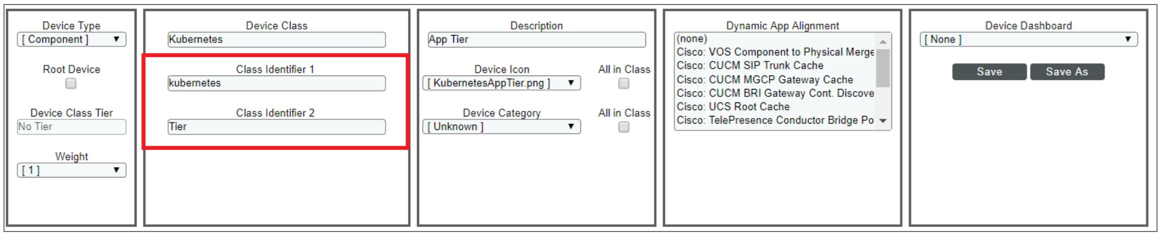
Device Type: [Component]
Root Device: ☐
Device Class Tier: No Tier
Weight: [1]

Device Class: Kubernetes
Class Identifier 1: kubernetes
Class Identifier 2: Application

Description: Application
Device Icon: [KubernetesApplication.png] All in Class ☐
Device Category: [Unknown] All in Class ☐

Dynamic App Alignment:
(none)
Cisco: VOS Component to Physical Merge
Cisco: CUCM SIP Trunk Cache
Cisco: CUCM MGCP Gateway Cache
Cisco: CUCM BRI Gateway Cont. Discove
Cisco: UCS Root Cache
Cisco: TelePresence Conductor Bridge Po

Device Dashboard: [None]



Device Type: [Component]
Root Device: ☐
Device Class Tier: No Tier
Weight: [1]

Device Class: Kubernetes
Class Identifier 1: kubernetes
Class Identifier 2: Tier

Description: App Tier
Device Icon: [KubernetesAppTier.png] All in Class ☐
Device Category: [Unknown] All in Class ☐

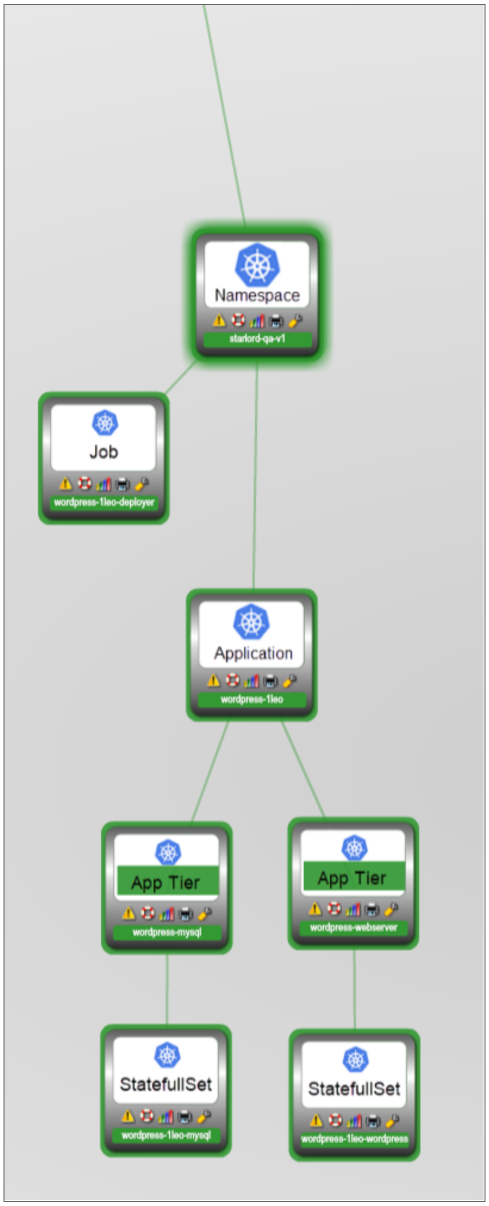
Dynamic App Alignment:
(none)
Cisco: VOS Component to Physical Merge
Cisco: CUCM SIP Trunk Cache
Cisco: CUCM MGCP Gateway Cache
Cisco: CUCM BRI Gateway Cont. Discove
Cisco: UCS Root Cache
Cisco: TelePresence Conductor Bridge Po

Device Dashboard: [None]

NOTE: For information on how to create device classes, see the ***Device Management*** manual.

For this example, when creating the device classes, the ***Class Identifier 1*** field must always be "Kubernetes" and the ***Class Identifier 2*** field value ***must*** match the fields in the credential's topology definition—in this case, "Application" and "Tier".

After you have created these device classes, the device component map tree will appear as follows:



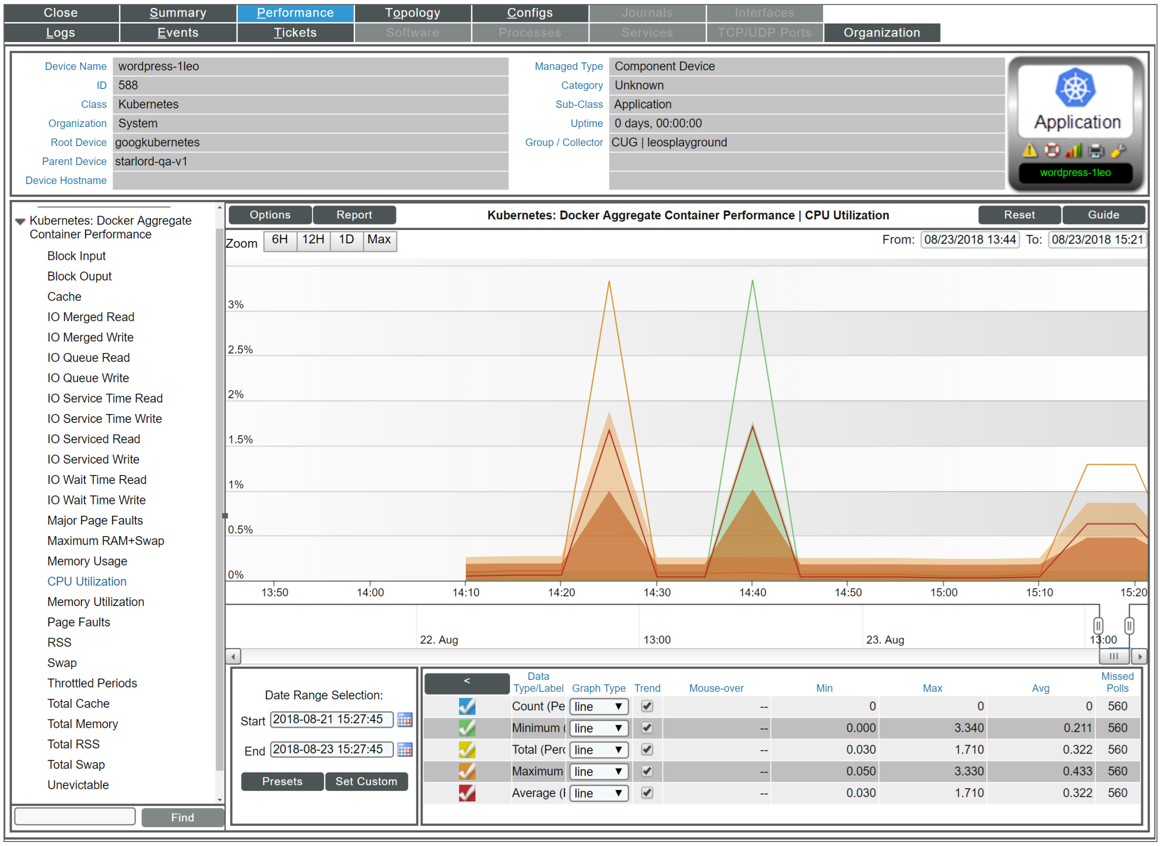
NOTE: If you previously discovered your Kubernetes system prior to defining device classes that were specific to your topology definition, then after you have defined the device classes, you must delete any of the generic devices that were used in lieu of those device classes in order for SL1 to rebuild the device component map with the new device classes. For instance, in our example above, the devices that were initially discovered with the generic "Component" device class had to be deleted from the **Device Manager** page (Registry > Devices > Device Manager) so that they could be automatically rediscovered with the newly defined device classes.

Metric Aggregation

The *Kubernetes* PowerPack also enables you to aggregate Docker Container metrics on any of the Aggregation components. To enable Docker Container aggregation, simply add the "@" symbol to the component definition. For example:

Application@:metadata:labels:app.kubernetes.io/name

The following screenshot illustrates the metrics that will be collected after you have added the "@" symbol to the definition:



Device Name	wordpress-1leo	Managed Type	Component Device
ID	588	Category	Unknown
Class	Kubernetes	Sub-Class	Application
Organization	System	Uptime	0 days, 00:00:00
Root Device	googkubernetes	Group / Collector	CUG | leosplayground
Parent Device	starlord-qa-v1		
Device Hostname			

Kubernetes: Docker Aggregate Container Performance | CPU Utilization

From: 08/23/2018 13:44 To: 08/23/2018 15:21

Date Range Selection:

Start 2018-08-21 15:27:45

End 2018-08-23 15:27:45

	Data Type/Label	Graph Type	Trend	Mouse-over	Min	Max	Avg	Missed Polls
☑	Count (Pe	line ▼	☑	--	0	0	0	560
☑	Minimum (	line ▼	☑	--	0.000	3.340	0.211	560
☑	Total (Perc	line ▼	☑	--	0.030	1.710	0.322	560
☑	Maximum	line ▼	☑	--	0.050	3.330	0.433	560
☑	Average (I	line ▼	☑	--	0.030	1.710	0.322	560

NOTE: These Dynamic Applications are always aligned to the component device; however, they do not collect data unless you include the "@" symbol in the component definition.

Filtering

Filtering enables the creation of specific aggregation components. In the preceding examples, application components would be created for ***all*** applications with that label. If you wanted to model only a set of applications or one specific application, you can do so using filtering.

For example, to create only a single "example-1" application component for the example application in the previous sections, you could modify the ***Topology Configuration*** as follows:

```
TOPOLOGY:Application:Tier

Application:metadata:labels:app.kubernetes.io/name=example-1

Tier:metadata:labels:app.kubernetes.io/component
```

> **TIP:** You can include lists when filtering. For example, you could include multiple application names, separated by comma.

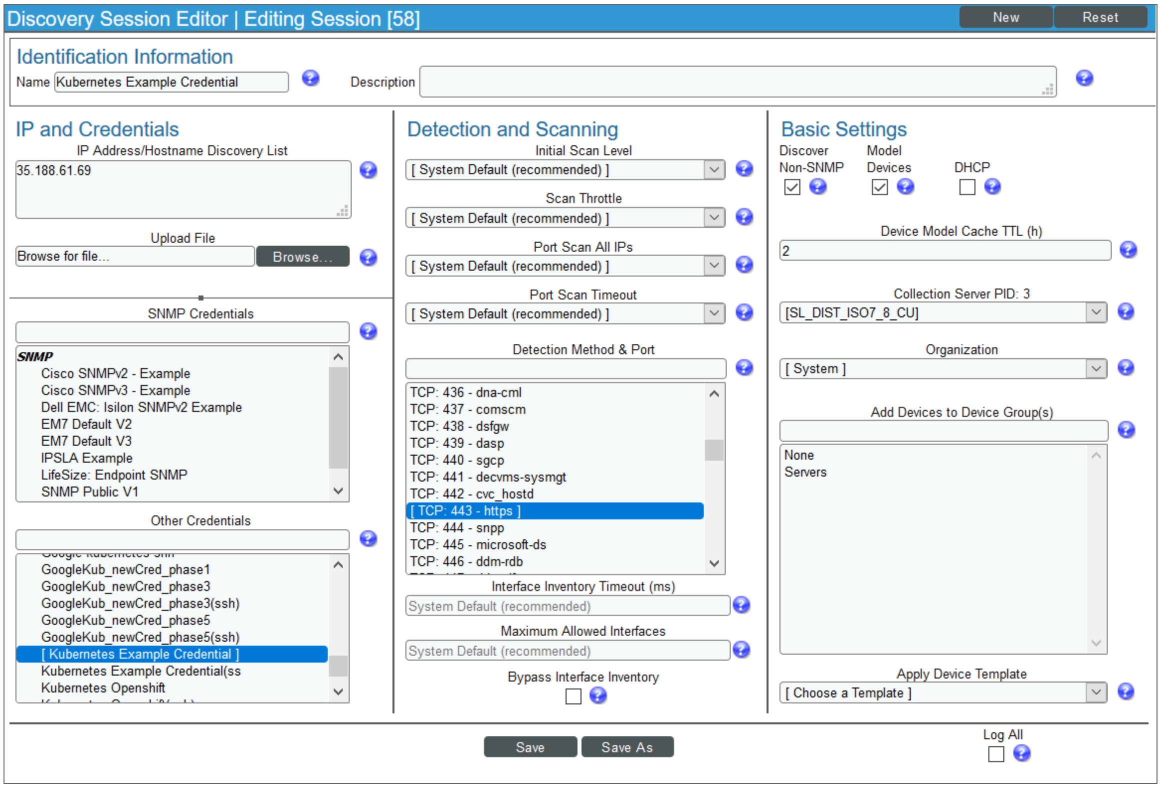
Discovering a Kubernetes Cluster

When you use the **Kubernetes Token Entry** dashboard to create credentials for the Kubernetes cluster that you want to monitor, SL1 automatically creates a discovery session that will discover your Kubernetes cluster and component devices.

To discover your Kubernetes cluster:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. Locate the discovery session with the ***Session Name*** that matches the name of the Kubernetes master SSH/Key credential that you created. (For example, if your SSH/Key credential is called "Kubernetes Example Credential", then the discovery ***Session Name*** will also be "Kubernetes Example Credential".)
3. If you want to run the discovery session immediately, proceed to step 6. Otherwise, to view the discovery session, click its wrench icon (🔧) and continue to step 4.

4. The **Discovery Session Editor** window appears. It includes the following information:



Discovery Session Editor | Editing Session [58]

New Reset

Identification Information

Name: Kubernetes Example Credential

Description:

IP and Credentials

IP Address/Hostname Discovery List: 35.188.61.69

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

SNMP Credentials

SNMP
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Dell EMC: Isilon SNMPv2 Example
EM7 Default V2
EM7 Default V3
IPSLA Example
LifeSize: Endpoint SNMP
SNMP Public V1

Other Credentials

GoogleKub_newCred_phase1
GoogleKub_newCred_phase3
GoogleKub_newCred_phase3(ssh)
GoogleKub_newCred_phase5
GoogleKub_newCred_phase5(ssh)
[Kubernetes Example Credential]
Kubernetes Example Credential(ss
Kubernetes Openshift

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

TCP: 436 - dna-cml
TCP: 437 - comscm
TCP: 438 - dsfgw
TCP: 439 - dasp
TCP: 440 - sgcp
TCP: 441 - decvms-sysmgt
TCP: 442 - cvc_hostd
[TCP: 443 - https]
TCP: 444 - snpp
TCP: 445 - microsoft-ds
TCP: 446 - ddm-rdb

Interface Inventory Timeout (ms): System Default (recommended)

Maximum Allowed Interfaces: System Default (recommended)

Bypass Interface Inventory: □

Basic Settings

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

Device Model Cache TTL (h): 2

Collection Server PID: 3: [SL_DIST_ISO7_8_CU]

Organization: [System]

Add Devices to Device Group(s)

None
Servers

Apply Device Template: [Choose a Template]

Save Save As

Log All: □

- *Name*. Displays the name of the discovery session, which matches the name of the Kubernetes master SSH/Key credential that you created. If you want to edit this discovery session, you should type a new name in this field.
- *IP Address/Hostname Discovery List*. Displays the IP address from the Kubernetes master SSH/Key credential that you created.
- *Other Credentials*. The Kubernetes master SSH/Key credential that you created is selected.
- *Detection Method & Port*. The port from the Kubernetes master SSH/Key credential that you created is selected.
- *Discover Non-SNMP*. This checkbox is selected.

NOTE: For more information about the other fields on this page, see the ***Discovery & Credentials*** manual.

5. If you did not make any changes to the discovery session, you can close the window without saving and then proceed to the next step. If you did make changes, click **[Save As]** and then close the **Discovery Session Editor** window. The discovery session you created will appear at the top of the **Discovery Control Panel** page.

6. Click the discovery session's lightning-bolt icon (⚡) to run discovery. The **Discovery Session** window appears.
7. When you run the discovery session, a Run Book Action in the *Kubernetes* PowerPack creates a virtual device that acts as the root device in your Kubernetes cluster. When the Kubernetes root device is discovered, you can click its device icon (🖥) to view the cluster's device properties.

NOTE: SL1 might take several minutes to discover the component devices for your cluster.

Relationships Between Component Devices

In addition to the parent/child relationships between component devices, relationships are automatically created by the Dynamic Applications in the *Kubernetes* PowerPack between each controller device and its underlying Docker container.

Chapter 49

LayerX

Overview

The following sections describe how to configure and discover LayerX appliances for monitoring by SL1 using the *LayerX Appliance Monitoring* PowerPack:

NOTE: For more information about the *LayerX Appliance Monitoring* PowerPack, see the ***Monitoring LayerX Appliances*** manual.

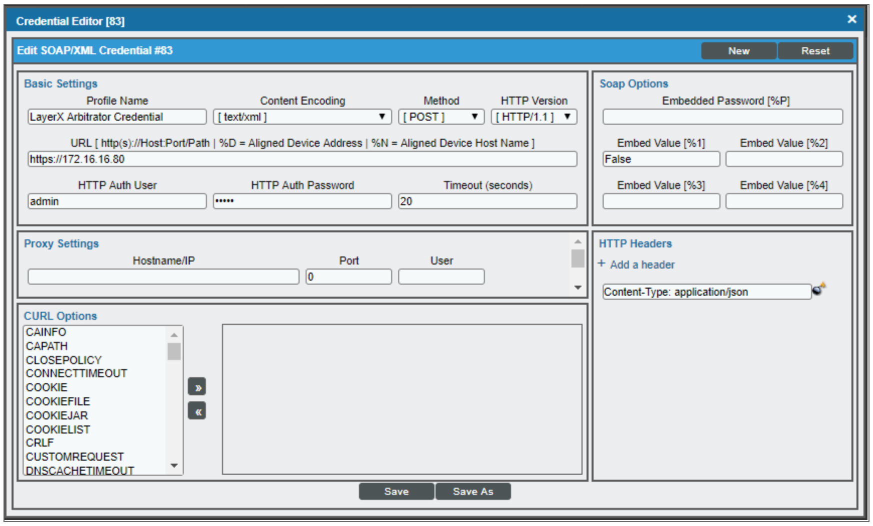
Creating a SOAP/XML Credential for LayerX Appliances

To configure SL1 to monitor LayerX appliances, you must first create a SOAP/XML credential. This credential allows the Dynamic Applications in the *LayerX Appliance Monitoring* PowerPack to connect with the LayerX appliance.

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

To configure the SOAP/XML credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **LayerX: Appliance Sample** credential, then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears:



Credential Editor [83]

Edit SOAP/XML Credential #83

Basic Settings

Profile Name: LayerX Arbitrator Credential

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://172.16.16.80

HTTP Auth User: admin

HTTP Auth Password: •••••

Timeout (seconds): 20

Soap Options

Embedded Password [%P]:

Embed Value [%1]: False

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

Proxy Settings

Hostname/IP:

Port: 0

User:

HTTP Headers

Content-Type: application/json

CURL Options

3. Complete the following fields:

   - ***Profile Name***. Enter a name for the LayerX credential.
   - ***URL***. Enter the IP address of the LayerX appliance you want to monitor.
   - ***HTTP Auth User***. Enter the username for a user with access to the LayerX appliance.
   - ***Password***. Enter the password for the LayerX account username.

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

Testing the LayerX Credential

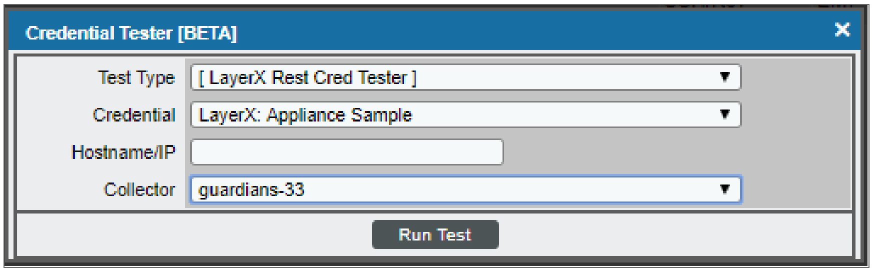
SL1 includes a Credential Test for LayerX. Credential Tests define a series of steps that SL1 can execute on demand to validate whether a credential works as expected.

The **LayerX Rest Cred Tester** can be used to test a SOAP/XML credential for monitoring LayerX using the Dynamic Applications in the *LayerX Appliance Monitoring* PowerPack. The LayerX Rest Cred Tester performs the following steps:

- ***Test Reachability***. Checks to see if the LayerX device is reachable using ICMP.
- ***Test Port Availability***. Checks to see if the appropriate port is open.
- ***Test Silo Rest Pack***. Attempts to collect data using the REST protocol collector using the given snippet argument.

To test the LayerX credential:

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



Credential Tester [BETA]

Test Type: [LayerX Rest Cred Tester]

Credential: LayerX: Appliance Sample

Hostname/IP:

Collector: guardians-33

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

4. Click the **[Run Test]** button. The **Test Credential** window appears, displaying 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:

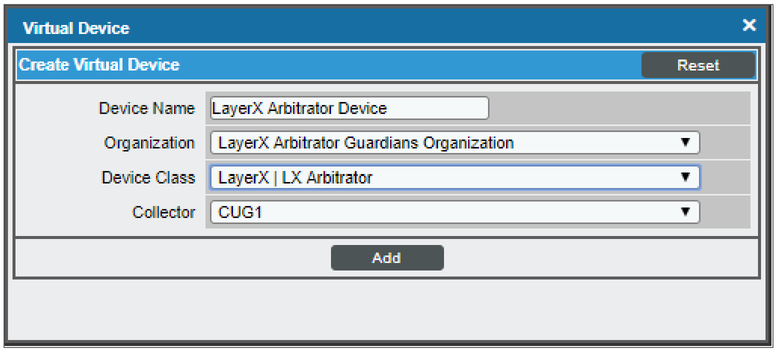
   - ***Step***. The name of the step.
   - ***Description***. A description of the action performed during the step.
   - ***Log Message***. The result of the step for this credential test.
   - ***Status***. The result of this step indicates whether the credential or the network environment is configured 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".

Creating the LayerX Virtual Device (MUD Systems Only)

If you are on a Military Unique Deployment (MUD) system, the Run Book Action will not create your device for you. Instead, you must create a ***virtual device*** that represents the LayerX appliance. A virtual device is a user-defined container that represents a device or service that cannot be discovered by SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications. If you are not on a MUD system, you can go directly to the ***Discovering LayerX Appliances*** section.

To create a virtual device that represents your LayerX appliance:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Click **[Actions]** and select *Create Virtual Device* from the menu. The **Virtual Device** modal page appears.
3. Enter values in the following fields:



Device Name: LayerX Arbitrator Device
Organization: LayerX Arbitrator Guardians Organization
Device Class: LayerX | LX Arbitrator
Collector: CUG1

- ***Device Name***. Enter a name for the device.
- ***Organization***. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.
- ***Device Class***. Select *LayerX | LX Arbitrator* or *Layer X| LX Reporter* depending on the LayerX appliance you are discovering.
- ***Collector***. Select the collector group that will monitor the device.

4. Click **[Add]** to create the virtual device.

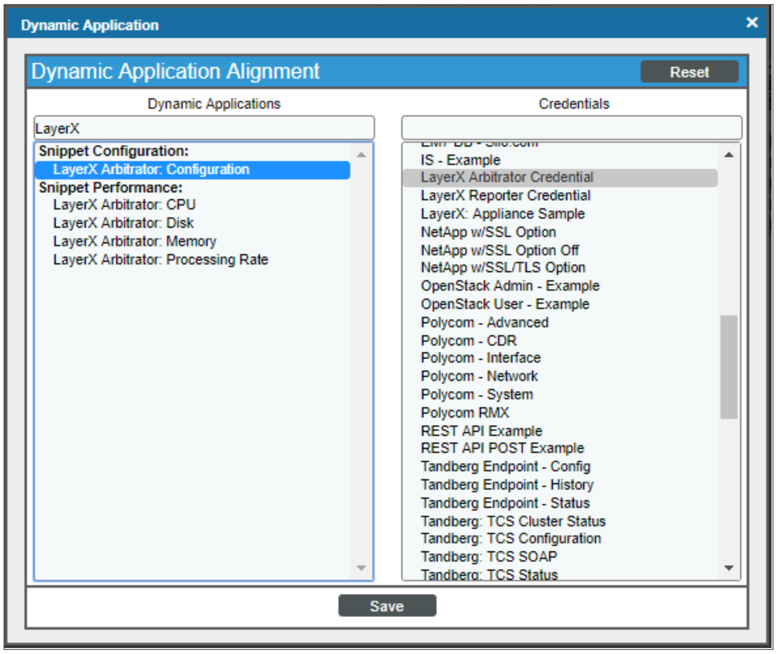
Manually Aligning LayerX Dynamic Applications (MUD Systems Only)

In you are on a Military Unique Deployment (MUD) system, you must manually align the LayerX Dynamic Applications to the LayerX virtual device. If you are on a non-MUD system, you can go directly to the ***Discovering LayerX Appliances*** section.

To manually align the LayerX Dynamic Applications:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Click the wrench icon (🔧) for your LayerX virtual device.
3. In the ***Device Administration*** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
4. Click the **[Actions]** button and select *Add Dynamic Application* from the menu.

5. In the **Dynamic Application Alignment** modal:



- In the ***Dynamic Applications*** field, select a Dynamic Application to align. Depending on the type of LayerX appliance, align Dynamic Applications according to the tables below.

Align the following Dynamic Applications to a **LayerX Reporter** appliance:

Dynamic Application	Credential Type
LayerX Reporter: Configuration	Snippet Configuration
LayerX Reporter: CPU	Snippet Performance
LayerX Reporter: Memory	Snippet Performance
LayerX: Service Status	Snippet Configuration
REST: Performance Metrics Monitor	Snippet Performance

Align the following Dynamic Applications to a **LayerX Arbitrator** appliance:

Dynamic Application	Credential Type
LayerX Arbitrator: Configuration	Snippet Configuration
LayerX Arbitrator: CPU	Snippet Performance
LayerX Arbitrator: Disk	Snippet Performance
LayerX Arbitrator: Memory	Snippet Performance
LayerX Arbitrator: Processing Rate	Snippet Performance

Dynamic Application	Credential Type
LayerX: Service Status	Snippet Configuration
REST: Performance Metrics Monitor	Snippet Performance

- In the ***Credentials*** field, select the credential you created for your LayerX appliance.

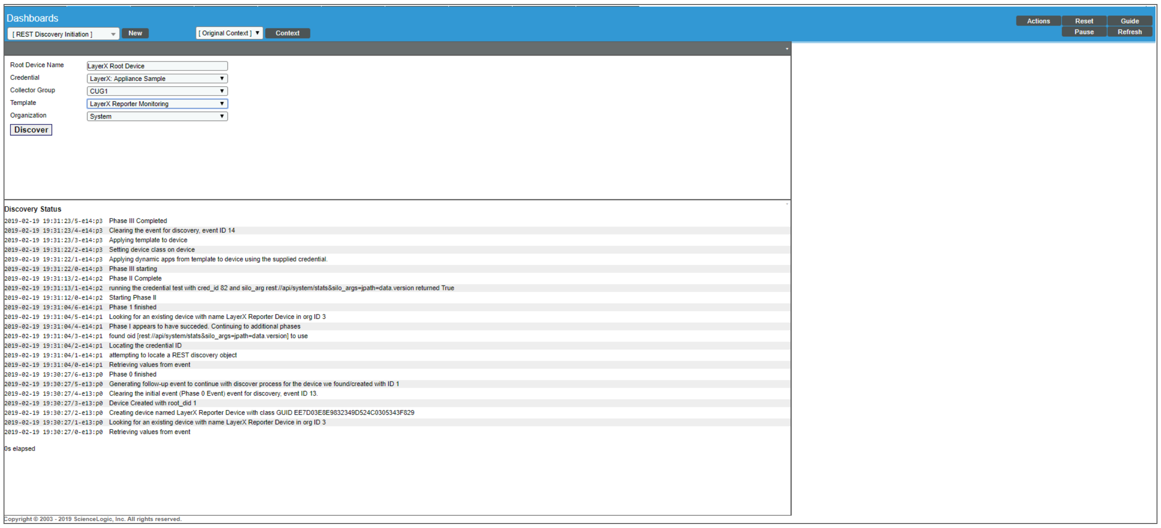
6. Click **[Save]** to align the Dynamic Application with the LayerX virtual device.

Discovering LayerX Appliances (Non-MUD Systems)

Because the *LayerX Appliance Monitoring* PowerPack is a REST-based PowerPack, you can use the **REST Discovery Initiation** dashboard to discover LayerX appliances.

To create a discovery session with the dashboard:

1. Click the **Dashboards tab**. In the drop-down field in the upper-left corner of the page, select *REST Discovery Initiation*.
2. On the **REST Discovery Initiation** dashboard page:



Root Device Name: LayerX Root Device
Credential: LayerX: Appliance Sample
Collector Group: CUG1
Template: LayerX Reporter Monitoring
Organization: System

Discovery Status

```
2019-02-19 19:31:23/5-e14:p3  Phase III Completed
2019-02-19 19:31:23/4-e14:p3  Clearing the event for discovery, event ID 14
2019-02-19 19:31:23/3-e14:p3  Applying template to device
2019-02-19 19:31:22/2-e14:p3  Setting device class on device
2019-02-19 19:31:22/1-e14:p3  Applying dynamic apps from template to device using the supplied credential.
2019-02-19 19:31:22/0-e14:p3  Phase III starting
2019-02-19 19:31:13/2-e14:p2  Phase II Complete
2019-02-19 19:31:13/1-e14:p2  running the credential test with cred_id 82 and silo_arg rest://api/system/stats&silo_args=jpath=data.version returned True
2019-02-19 19:31:12/0-e14:p2  Starting Phase II
2019-02-19 19:31:04/6-e14:p1  Phase 1 finished
2019-02-19 19:31:04/5-e14:p1  Looking for an existing device with name LayerX Reporter Device in org ID 3
2019-02-19 19:31:04/4-e14:p1  Phase I appears to have succeded. Continuing to additional phases
2019-02-19 19:31:04/3-e14:p1  found oid [rest://api/system/stats&silo_args=jpath=data.version] to use
2019-02-19 19:31:04/2-e14:p1  Locating the credential ID
2019-02-19 19:31:04/1-e14:p1  attempting to locate a REST discovery object
2019-02-19 19:31:04/0-e14:p1  Retrieving values from event
2019-02-19 19:30:27/6-e13:p0  Phase 0 finished
2019-02-19 19:30:27/5-e13:p0  Generating follow-up event to continue with discover process for the device we found/created with ID 1
2019-02-19 19:30:27/4-e13:p0  Clearing the initial event (Phase 0 Event) event for discovery, event ID 13.
2019-02-19 19:30:27/3-e13:p0  Device Created with root_did 1
2019-02-19 19:30:27/2-e13:p0  Creating device named LayerX Reporter Device with class GUID EE7D03E8E9832349D524C0305343F829
2019-02-19 19:30:27/1-e13:p0  Looking for an existing device with name LayerX Reporter Device in org ID 3
2019-02-19 19:30:27/0-e13:p0  Retrieving values from event

0s elapsed
```

Copyright © 2003 - 2019 ScienceLogic, Inc. All rights reserved.

- In the ***Root Device Name*** field, type a name for the LayerX root device.
- In the ***Credential*** field, select the SOAP/XML credential that you created.
- In the ***Collector Group*** field, select the collector group.
- In the ***Template*** field, select the appropriate LayerX device template.
- In the ***Organization*** field, select your organization.

NOTE: In the device template, if a credential is set for the Dynamic Application, it will be used. If a credential is not set for the Dynamic Application, the credential selected in the dashboard will be used. In most cases, the template will have Dynamic Applications with no credentials set.

4. Click the **[Discover]** button. The progress of the discovery session will be displayed in the **Discovery Status** pane.

NOTE: The LayerX Appliance Monitoring PowerPack has two device templates, one for Arbitrator and one for Reporter devices. If you need to discover both types of devices, you will need to run the **REST Discovery Initiation** once for each device type.

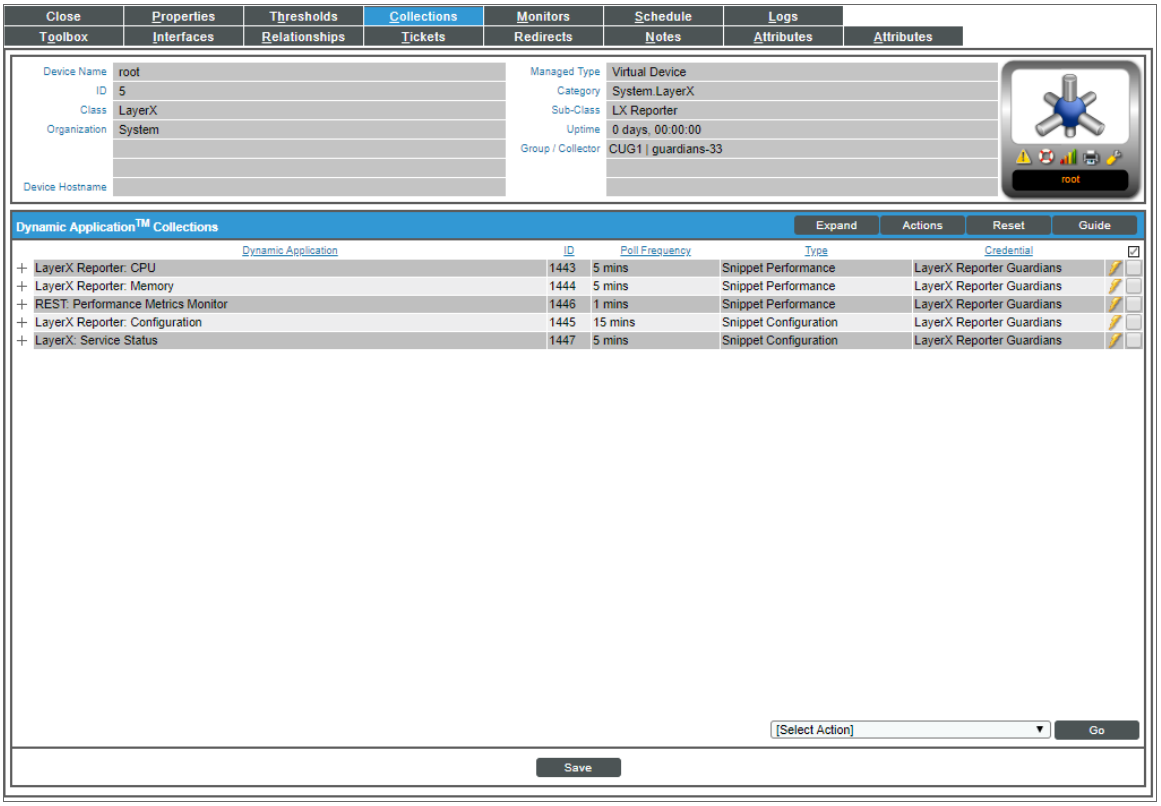
After the discovery session has completed, find the device ID in the logs in the **Discovery Status** pane. Then go to the **Device Manager** page (Registry > Devices > Device Manager) and search for the device ID. When you have located the device, click on its edit icon (✏) or its graph (📊) icon to view details about the device.

Verifying Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. After the discovery session has completed, go to the **Device Manager** (Registry > Devices > Device Manager) page and find the device you discovered in the **REST Discovery Initiation** dashboard. You can find the device ID in the logs in the **Discovery Status** pane when your discovery session is complete. When you have located the device in the **Device Manager**, click on its edit icon (✏).
2. In the **Device Properties** page, click the **[Collections]** tab.
3. All applicable Dynamic Applications for the LayerX appliance are automatically aligned during discovery. The Dynamic Applications aligned depend on the device template you selected 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 root
ID 5
Class LayerX
Organization System
Device Hostname

Managed Type Virtual Device
Category System.LayerX
Sub-Class LX Reporter
Uptime 0 days, 00:00:00
Group / Collector CUG1 | guardians-33

Dynamic Application^{TM} Collections

	Dynamic Application	ID	Poll Frequency	Type	Credential		☑
+	LayerX Reporter: CPU	1443	5 mins	Snippet Performance	LayerX Reporter Guardians		□
+	LayerX Reporter: Memory	1444	5 mins	Snippet Performance	LayerX Reporter Guardians		□
+	REST: Performance Metrics Monitor	1446	1 mins	Snippet Performance	LayerX Reporter Guardians		□
+	LayerX Reporter: Configuration	1445	15 mins	Snippet Configuration	LayerX Reporter Guardians		□
+	LayerX: Service Status	1447	5 mins	Snippet Configuration	LayerX Reporter Guardians		□

You should see the following Dynamic Applications aligned to the LayerX Reporter appliance:

Dynamic Application	Credential Type
LayerX Reporter: Configuration	Snippet Configuration
LayerX Reporter: CPU	Snippet Performance
LayerX Reporter: Memory	Snippet Performance
LayerX: Service Status	Snippet Configuration
REST: Performance Metrics Monitor	Snippet Performance

You should see the following Dynamic Applications aligned to the LayerX Arbitrator appliance:

Dynamic Application	Credential Type
LayerX Arbitrator: Configuration	Snippet Configuration
LayerX Arbitrator: CPU	Snippet Performance
LayerX Arbitrator: Disk	Snippet Performance
LayerX Arbitrator: Memory	Snippet Performance
LayerX Arbitrator: Processing Rate	Snippet Performance

Dynamic Application	Credential Type
LayerX: Service Status	Snippet Configuration
REST: Performance Metrics Monitor	Snippet Performance

Chapter 50

Linux Base Pack

Overview

The following sections describe how to configure and discover Linux devices for monitoring by SL1 using SSH and the *Linux Base Pack* PowerPack:

NOTE: For more information about the *Linux Base Pack* PowerPack, see the ***Monitoring Linux and Solaris*** manual.

Prerequisites for Monitoring Linux Devices with SSH

Before you can monitor Linux devices using the *Linux Base Pack* PowerPack, you must have the following information about the devices that have already been properly configured:

- IP addresses of the devices you want to monitor
- SSH private keys for the devices you want to monitor

Additionally, if you want to collect interface information about your Linux devices, you must install *ifconfig* on those devices.

Configuring Linux Devices to Collect Data

The following tables list the Collection Objects included in those Dynamic Applications and the Linux commands used by each of those objects. You can use these commands to grant or restrict access to certain data types on the user account you will use to monitor your Linux devices.

The following table is a list of configuration and performance Dynamic Applications in the PowerPack:

Dynamic Application	Collection Object	Linux Command
Linux: Configuration Discovery		Determines if a device is a Linux system before discovery in SL1. If the device is not a Linux system, it will not be discovered.

Linux: CPU Configuration	All	`cat /proc/cpuinfo/`
		`lscpu`

Linux: CPU Cores Performance	All	`cat /proc/stat`
Linux: CPU Performance	All	`cat /proc/stat`
Linux: Disk IOPs Performance	All	`cat /proc/diskstats`
Linux: File System Performance	All	`df -kPT`
Linux: Hardware Configuration	All	`sudo dmidecode -qt 1,2,3`
Linux: ICMP Performance	All	`cat /proc/net/snmp`
Linux: Interface Performance	All	`/sbin/ifconfig`
Linux: Memory Performance	All	`cat /proc/meminfo`
Linux: Network Configuration	All	`/sbin/ifconfig`
Linux: Route Table Configuration	All	`netstat -rn`
Linux: System Configuration	Kernel Version	`cat /proc/sys/kernel/osrelease`
	Distribution Genus	`cat /etc/os-release`
	Host Name	`cat /proc/sys/kernel/hostname`
	Distribution Release	`cat /etc/os-release | grep PRETTY_NAME`
	AppDynamics Host Name | IP Address	`hostname=$(cat /proc/sys/kernel/hostname) && echo $hostname"|"<silo:ip>`
	AppDynamics Namespace	`echo "appdynamics/ns"`
	Architecture Type	`uname -a`

Dynamic Application	Collection Object	Linux Command
	Compiler	`cat /proc/version`
	Domain Name	`cat /proc/sys/kernel/domainname`
	Dynatrace Hostname	`cat /proc/sys/kernel/hostname`
	Dynatrace Namespace	`echo "dynatrace/physical/ns"`
	New Relic Hostname	`cat /proc/sys/kernel/hostname`
	New Relic Namespace	`echo "newrelic/server/ns"`
	Release Date	`cat /proc/sys/kernel/version`
	SMP Support	`cat /proc/sys/kernel/version`
	Time Zone	`date`
	Total Physical Memory (MBytes)	`cat /proc/meminfo`
	Total Swap Memory (MBytes)	`cat /proc/meminfo`
Linux: System Load Performance	All	`cat /proc/loadavg`
Linux: TCP Performance	All	`cat /proc/net/snmp`
	TCP Ports Listening Cache	`netstat -ltn`
Linux: TCP Services Configuration	All	`netstat -ltn | grep tcp`
Linux: UDP Performance	All	`cat /proc/net/snmp`
Linux: UDP Services Configuration	All	`netstat -lun | grep udp`
Linux: Zombie Process	All	`ps aux | grep Z`

The following table is a list of internal collection inventory and performance Dynamic Applications in the PowerPack:

Dynamic Application	Collection Object	Linux Command
Linux: IC Availability	All	Internal Collection that consumes data stored by

Dynamic Application	Collection Object	Linux Command
		the "Linux: ICDA Cache" Dynamic Application.
Linux: IC Detail	All	Internal Collection that consumes data stored by the "Linux: ICDA Cache" Dynamic Application.
Linux: IC Filesystem Inventory	All	Internal Collection that consumes data stored by the "Linux: ICDA Cache" Dynamic Application.
Linux: IC Filesystem Performance	All	Internal Collection that consumes data stored by the "Linux: ICDA Cache" Dynamic Application.
Linux: IC Interface Inventory	All	Internal Collection that consumes data stored by the "Linux: ICDA Cache" Dynamic Application.
Linux: IC Interface Performance	All	Internal Collection that consumes data stored by the "Linux: ICDA Cache" Dynamic Application.
Linux: IC Port Performance	All	Internal Collection that consumes data stored by the "Linux: ICDA Cache" Dynamic Application.
Linux: IC Process Inventory	All	Internal Collection that consumes data stored by the "Linux: ICDA Cache" Dynamic Application.
Linux: IC Process Performance	All	Internal Collection that consumes data stored by the "Linux: ICDA Cache" Dynamic Application.
Linux: ICDA Cache	Filesystem	`df -kPT`
	Hardware Config Product Name	`cat /sys/devices/virtual/dmi/id/product_name`
	Interface	`/sbin/ifconfig`
	Latency	`ping -c1 -W 1 <silo:ip>`
	Process	`ps aux`
	Processes CPU Usage	`cat /proc/stat`
	Processes Memory Usage	`free -b`
	Software Distribution Release	`grep "PRETTY_NAME" /etc/os-release`
	Uptime	`cat /proc/uptime`

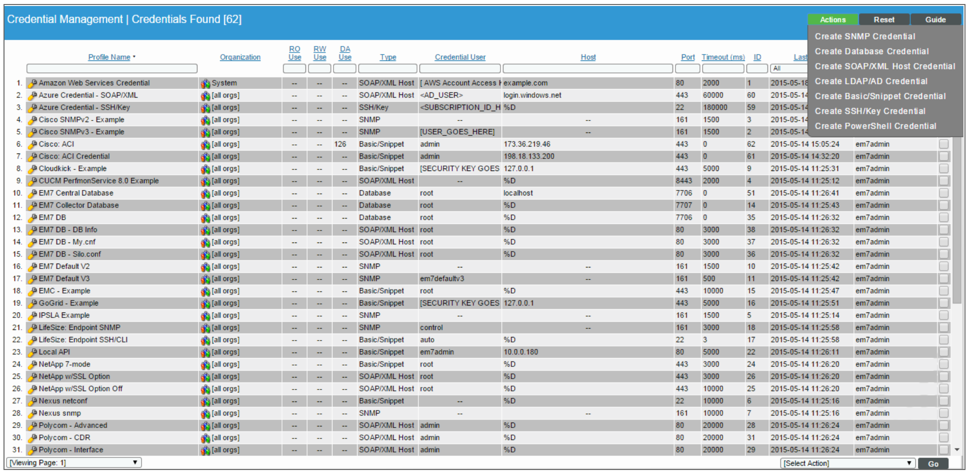
NOTE: Linux Base Pack v103 uses a number of standard Linux commands to collect information about a particular device. Most of these commands do not require any specific or elevated permissions to be executed. The PowerPack includes one single command (`dmidecode`) in the "Linux: Hardware Configuration" Dynamic Application which requires root permissions to execute. ScienceLogic recommends configuring a password-less sudo for the user for `dmidecode` as the PowerPack does not support sudo with a password prompt. If the user is not configured correctly the "Linux: Hardware Configuration" Dynamic Application will fail with the following error: `sudo: no tty present and no askpass program specified` You can validate if your configuration is correct by clicking the lightning bolt icon (⚡) on the Dynamic Application for the device in question.

Creating an SSH/Key Credential

To configure SL1 to monitor Linux devices using SSH, you must first create an SSH/Key credential. This credential allows the Dynamic Applications in the *Linux Base Pack* PowerPack) to connect with a Linux device.

To create an SSH/Key credential:

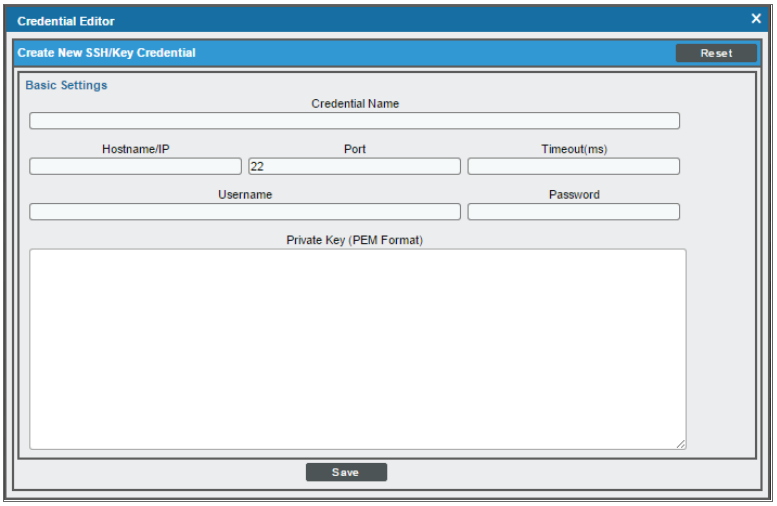
1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the **[Actions]** menu, and then select ***Create SSH/Key Credential***. The **Create New SSH/Key Credential** modal page appears.


Actions
Reset
Guide
Create SNMP Credential
Create Database Credential
Create SOAP/XML Host Credential
Create LDAP/AD Credential
Create Basic/Snippet Credential
Create SSH/Key Credential
Create PowerShell Credential
[Viewing Page: 1]
[Select Action]
Go

Credential Management | Credentials Found [62]

	Profile Name	Organization	RO Use	RW Use	DA Use	Type	Credential User	Host	Port	Timeout (ms)	ID	Last		
												All		
1.	Amazon Web Services Credential	System	--	--	--	SOAP/XML Host	[AWS Account Access I	example.com	80	2000	1	2015-05-18		
2.	Azure Credential - SOAP/XML	[all orgs]	--	--	--	SOAP/XML Host	<AD_USER>	login.windows.net	443	60000	60	2015-05-14		
3.	Azure Credential - SSH/Key	[all orgs]	--	--	--	SSH/Key	<SUBSCRIPTION_ID_H	%D	22	180000	59	2015-05-14		
4.	Cisco SNMPv2 - Example	[all orgs]	--	--	--	SNMP	--	--	161	1500	3	2015-05-14		
5.	Cisco SNMPv3 - Example	[all orgs]	--	--	--	SNMP	[USER_GOES_HERE]	--	161	1500	2	2015-05-14		
6.	Cisco: ACI	[all orgs]	--	--	126	Basic/Snippet	admin	173.36.219.46	443	0	62	2015-05-14 15:05:24	em7admin	□
7.	Cisco: ACI Credential	[all orgs]	--	--	--	Basic/Snippet	admin	198.18.133.200	443	0	61	2015-05-14 14:32:20	em7admin	□
8.	Cloudkick - Example	[all orgs]	--	--	--	Basic/Snippet	[SECURITY KEY GOES	127.0.0.1	443	5000	9	2015-05-14 11:25:31	em7admin	□
9.	CUCM PerfmonService 8.0 Example	[all orgs]	--	--	--	SOAP/XML Host	--	%D	8443	2000	4	2015-05-14 11:25:12	em7admin	□
10.	EM7 Central Database	[all orgs]	--	--	--	Database	root	localhost	7706	0	51	2015-05-14 11:26:41	em7admin	□
11.	EM7 Collector Database	[all orgs]	--	--	--	Database	root	%D	7707	0	14	2015-05-14 11:25:43	em7admin	□
12.	EM7 DB	[all orgs]	--	--	--	Database	root	%D	7706	0	35	2015-05-14 11:26:32	em7admin	□
13.	EM7 DB - DB Info	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	38	2015-05-14 11:26:32	em7admin	□
14.	EM7 DB - My.cnf	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	37	2015-05-14 11:26:32	em7admin	□
15.	EM7 DB - Silo.conf	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	36	2015-05-14 11:26:32	em7admin	□
16.	EM7 Default V2	[all orgs]	--	--	--	SNMP	--	--	161	1500	10	2015-05-14 11:25:42	em7admin	□
17.	EM7 Default V3	[all orgs]	--	--	--	SNMP	em7defaultv3	--	161	500	11	2015-05-14 11:25:42	em7admin	□
18.	EMC - Example	[all orgs]	--	--	--	Basic/Snippet	root	%D	443	10000	15	2015-05-14 11:25:47	em7admin	□
19.	GoGrid - Example	[all orgs]	--	--	--	Basic/Snippet	[SECURITY KEY GOES	127.0.0.1	443	5000	16	2015-05-14 11:25:51	em7admin	□
20.	IPSLA Example	[all orgs]	--	--	--	SNMP	--	--	161	1500	5	2015-05-14 11:25:14	em7admin	□
21.	LifeSize: Endpoint SNMP	[all orgs]	--	--	--	SNMP	control	--	161	3000	18	2015-05-14 11:25:58	em7admin	□
22.	LifeSize: Endpoint SSH/CLI	[all orgs]	--	--	--	Basic/Snippet	auto	%D	22	3	17	2015-05-14 11:25:58	em7admin	□
23.	Local API	[all orgs]	--	--	--	Basic/Snippet	em7admin	10.0.0.180	80	5000	22	2015-05-14 11:26:11	em7admin	□
24.	NetApp 7-mode	[all orgs]	--	--	--	Basic/Snippet	root	%D	443	3000	24	2015-05-14 11:26:20	em7admin	□
25.	NetApp w/SSL Option	[all orgs]	--	--	--	SOAP/XML Host	root	%D	443	3000	26	2015-05-14 11:26:20	em7admin	□
26.	NetApp w/SSL Option Off	[all orgs]	--	--	--	SOAP/XML Host	root	%D	443	10000	25	2015-05-14 11:26:20	em7admin	□
27.	Nexus netconf	[all orgs]	--	--	--	Basic/Snippet	--	%D	22	10000	6	2015-05-14 11:25:16	em7admin	□
28.	Nexus snmp	[all orgs]	--	--	--	SNMP	--	--	161	10000	7	2015-05-14 11:25:16	em7admin	□
29.	Polycom - Advanced	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	28	2015-05-14 11:26:24	em7admin	□
30.	Polycom - CDR	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	31	2015-05-14 11:26:24	em7admin	□
31.	Polycom - Interface	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	29	2015-05-14 11:26:24	em7admin	□

3. On the **Create New SSH/Key Credential** modal page, supply values in the following fields:



- ***Credential Name***. Type a name for the credential.
- ***Hostname/IP***. Type the hostname or IP address of the Linux device you want to monitor.
  - You can include the variable **%D** in this field. SL1 will replace the variable with the IP address of the device that is currently using the credential.
  - You can include the variable **%N** in this field. SL1 will replace the variable with hostname of the device that is currently using the credential. If SL1 cannot determine the hostname, SL1 will replace the variable with the primary management IP address for the device.
- ***Port***. Type the port number associated with the data you want to retrieve.

NOTE: The default TCP port for SSH servers is 22.

- ***Timeout (ms)***. Type the time, in milliseconds, after which SL1 will stop trying to communicate with the authenticating server.
- ***Username***. Type the username for an SSH or user account on the device to be monitored.
- ***Password***. Type the password for an SSH user account on the device to be monitored.
- ***Private Key (PEM Format)***. Type or paste the SSH private key that you want SL1 to use, in PEM format.

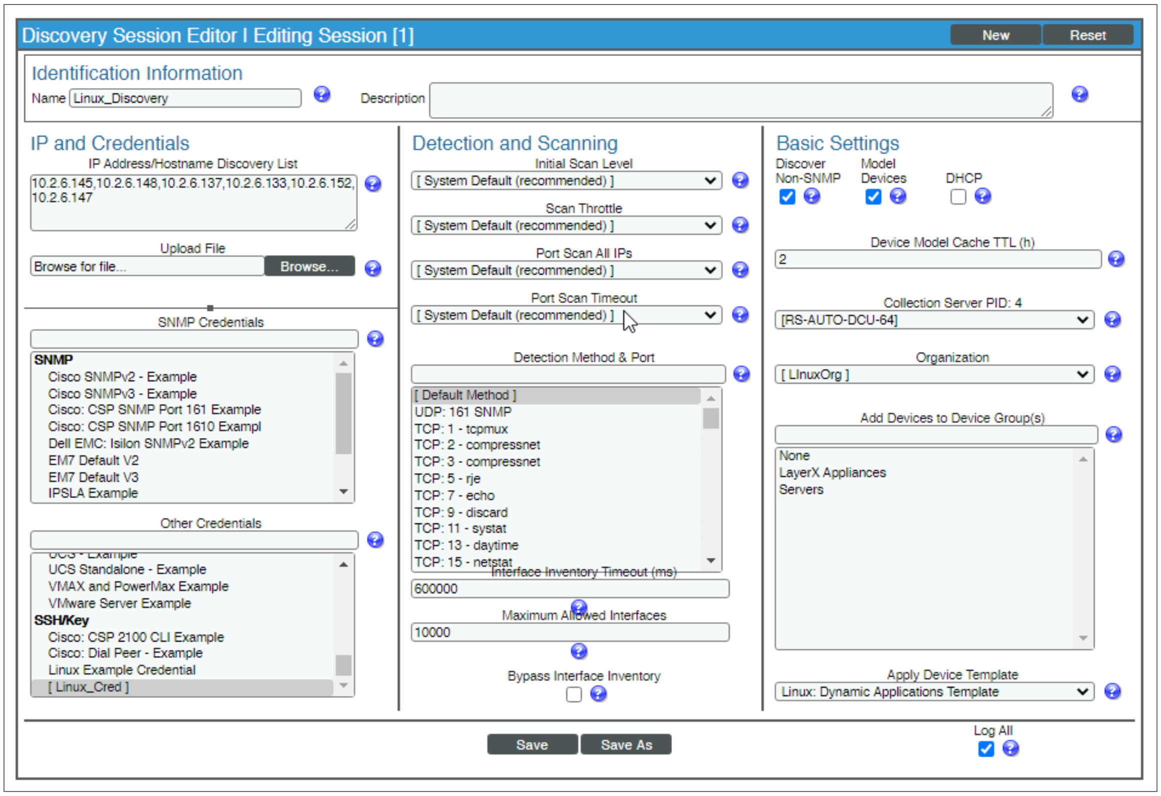
NOTE: To monitor Amazon Web Services Linux instances, the private key must include the lines "BEGIN RSA PRIVATE KEY" and "END RSA PRIVATE KEY", as well as all preceding and following dashes on those lines.

4. Click **[Save]**.

Discovering Linux Devices

To discover Linux devices using a discovery session, 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. On this page, define values in the following fields:



Identification Information

Name: Linux_Discovery

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.2.6.145,10.2.6.148,10.2.6.137,10.2.6.133,10.2.6.152, 10.2.6.147

Upload File: Browse for file...

SNMP Credentials

SNMP
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Cisco: CSP SNMP Port 161 Example
Cisco: CSP SNMP Port 1610 Exampl
Dell EMC: Isilon SNMPv2 Example
EM7 Default V2
EM7 Default V3
IPSLA Example

Other Credentials

UCS - Example
UCS Standalone - Example
VMAX and PowerMax Example
VMware Server Example
SSH/Key
Cisco: CSP 2100 CLI Example
Cisco: Dial Peer - Example
Linux Example Credential
[Linux_Cred]

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: 4: [RS-AUTO-DCU-64]

Organization: [LinuxOrg]

Add Devices to Device Group(s)

None
LayerX Appliances
Servers

Apply Device Template: Linux: Dynamic Applications Template

Log All: ☑

- ***IP Address Discovery List***. Type the IP addresses for the Linux devices you want to monitor, separated by a comma.
- ***Other Credentials***. Select the SSH/Key credentials you created for the Linux devices.
- ***Discover Non-SNMP***. Select this checkbox.
- ***Model Devices***. Select this checkbox.
- ***Apply Device Template***. Select the device template that you configured.

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 Linux devices are discovered, click their device icons (🖥) to view the **Device Properties** pages for the Linux devices.

> **NOTE:** The "Linux: IC Interface Inventory" Dynamic Application runs during nightly discovery. If you want to force discovery of interfaces at a time outside of nightly discovery, run the following command on the collector: `sudo -u s-em7-core /opt/em7/bin/python /opt/em7/backend/discover_update.py`

Relationships Between Component Devices

The Dynamic Applications in the *Linux Base Pack* PowerPack can automatically build relationships between Linux servers and other associated devices:

- If you discover AppDynamics applications using the Dynamic Applications in the *Cisco: AppDynamics* PowerPack, SL1 will automatically create relationships between Linux Servers and AppDynamics Nodes.
- If you discover Dynatrace environments using the Dynamic Applications in the *Dynatrace* PowerPack, SL1 will automatically create relationships between Linux Servers and Dynatrace Hosts.
- If you discover New Relic devices using the Dynamic Applications in the *New Relic* PowerPack, SL1 will automatically create relationships between Linux Servers and New Relic Servers.

Chapter 51

Microsoft: Azure

Overview

The following sections describe how to configure and discover Microsoft Azure resources for monitoring by SL1 using the *Microsoft: Azure* PowerPack:

NOTE: The *Microsoft: Azure* PowerPack can monitor Microsoft Azure resources, Microsoft Azure Government resources, and Microsoft Azure resources in Germany and China regions.

NOTE: For more information about the *Microsoft: Azure* PowerPack, see the ***Monitoring Microsoft Azure*** manual.

Configuring an Azure Active Directory Application

To create a SOAP/XML credential that allows SL1 to access Microsoft Azure, you must provide the following information about an Azure application that is already registered with an Azure AD tenant:

- Application ID
- Subscription ID (if monitoring a single subscription)
- Tenant ID
- Secret key

To capture the above information, you must first create (or already have) an application that is registered with Azure Active Directory. The registered application must have Reader access in the subscription. You can then enter the required information about the application when configuring the SOAP/XML credential in SL1. The registered application and the ScienceLogic credential allow SL1 to retrieve information from Microsoft Azure.

TIP: For details on registering an Azure application, see https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app.

Creating an Active Directory Application in the Azure Portal

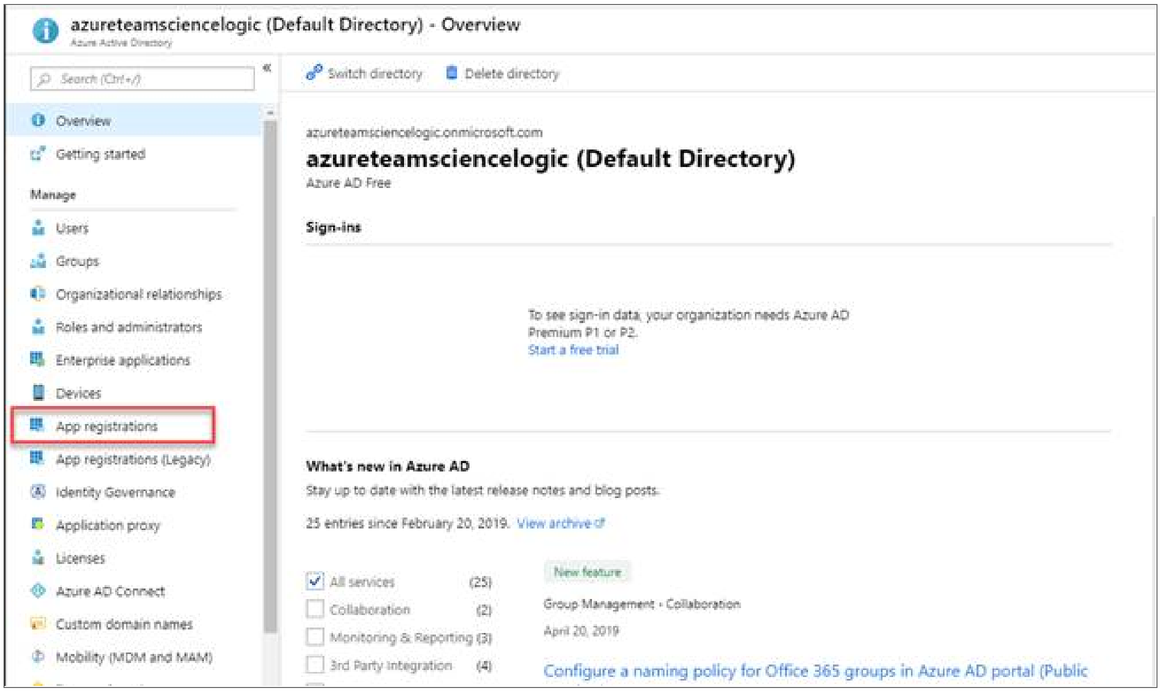
When configuring a SOAP/XML credential in SL1, you must provide the application ID, subscription ID, tenant ID, and secret key of an application that is registered with Azure Active Directory. You will use this registered application to authenticate your Azure account.

NOTE: You must have Service Administrator rights to create an Azure Active Directory application.

To create an application in Azure and register it with Azure Active Directory:

1. Log in to the Azure portal and type "active directory" in the **Search** field at the top of the window.

2. From the search results, select *Azure Active Directory*, and then click **App registrations**. The **App registrations** page appears:



azureteamsciencelogic.onmicrosoft.com

azureteamsciencelogic (Default Directory)

Azure AD Free

Sign-ins

To see sign-in data, your organization needs Azure AD Premium P1 or P2.
Start a free trial

What's new in Azure AD

Stay up to date with the latest release notes and blog posts.

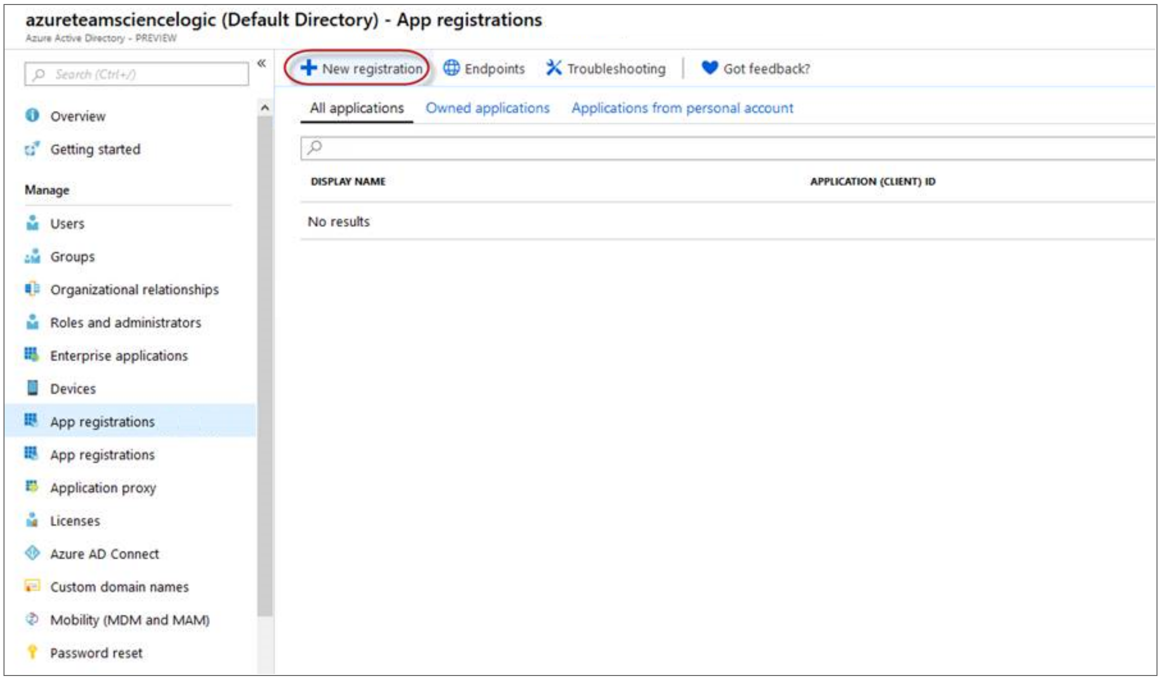
25 entries since February 20, 2019. View archive

Group Management › Collaboration

April 20, 2019

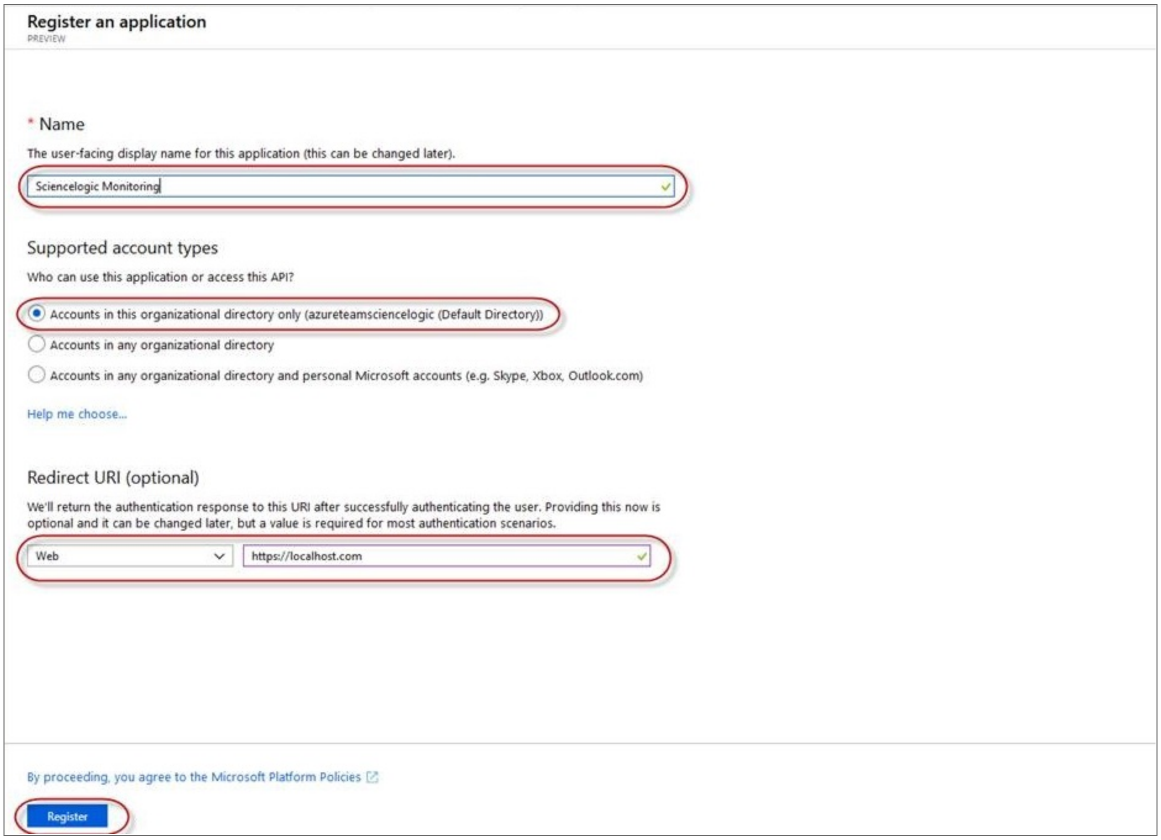
Configure a naming policy for Office 365 groups in Azure AD portal (Public

3. Click the **[New registration]** button.



DISPLAY NAME	APPLICATION (CLIENT) ID
No results	

4. When the **Register an application page** appears, enter your application's registration information:
   - ***Name***. Type a name for the application.
   - ***Supported account types***. Select *Accounts in this organizational directory only*.
   - ***Redirect URI (optional)***. Select *Web* in the drop-down menu and type a valid URL.



Register an application
PREVIEW

* Name
The user-facing display name for this application (this can be changed later).
Sciencelogic Monitoring ✓

Supported account types
Who can use this application or access this API?
● Accounts in this organizational directory only (azureteamsciencelogic (Default Directory))
○ Accounts in any organizational directory
○ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)
Help me choose...

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
Web | https://localhost.com ✓

By proceeding, you agree to the Microsoft Platform Policies

Register

5. Click the **[Register]**button. A message appears confirming that your application was added.

Adding Microsoft Graph APIs Permissions to the Application

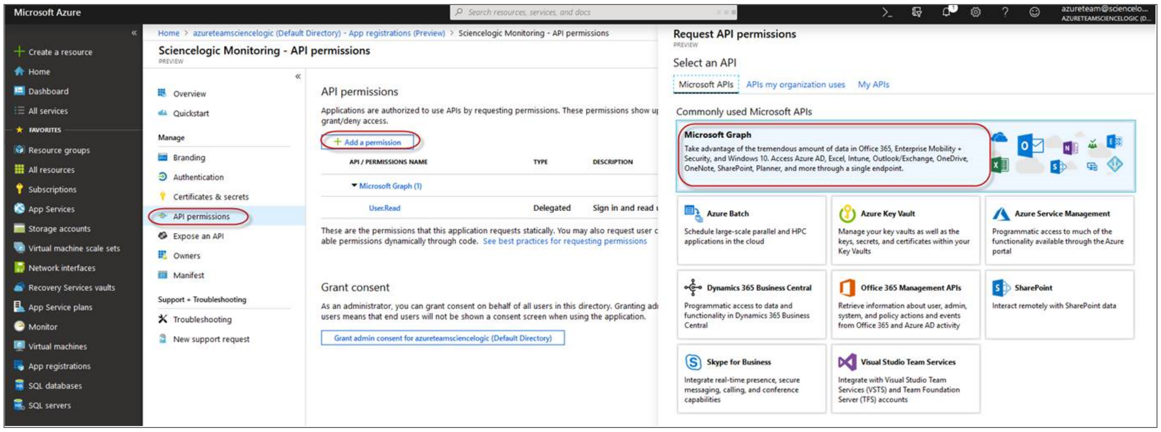
By default, any new Application has Microsoft Graph API permission. At a minimum, the Microsoft Graph APIs must have permission to directly read data.

To add the Microsoft Graph APIs:

1. In the **Search** field of the Azure portal (https://portal.azure.com), type "active directory".

2. Click **[App registrations]**, and then click on the name of the Azure Active Directory application you will use to authenticate your Azure account.

3. Click ***API Permissions***, and then click **[Add a permission]**. Next, select the **Microsoft Graph** option.



Applications are authorized to use APIs by requesting permissions. These permissions show u grant/deny access.

These are the permissions that this application requests statically. You may also request user c able permissions dynamically through code.

As an administrator, you can grant consent on behalf of all users in this directory. Granting ad users means that end users will not be shown a consent screen when using the application.

Microsoft Graph: Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Batch: Schedule large-scale parallel and HPC applications in the cloud

Azure Key Vault: Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Service Management: Programmatic access to much of the functionality available through the Azure portal

Dynamics 365 Business Central: Programmatic access to data and functionality in Dynamics 365 Business Central

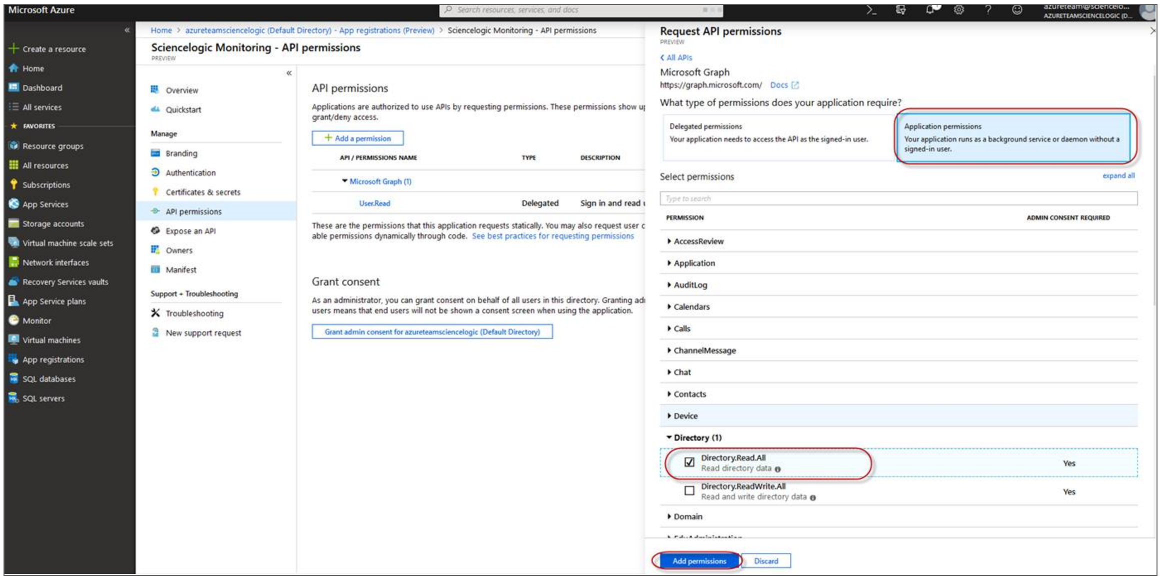
Office 365 Management APIs: Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

SharePoint: Interact remotely with SharePoint data

Skype for Business: Integrate real-time presence, secure messaging, calling, and conference capabilities

Visual Studio Team Services: Integrate with Visual Studio Team Services (VSTS) and Team Foundation Server (TFS) accounts

4. In the **Request API permissions** pane, under Select permissions, click the arrow next to **Directory** to open the submenu and select the checkbox for ***Directory.Read.all*** permission.



What type of permissions does your application require?

Delegated permissions: Your application needs to access the API as the signed-in user.

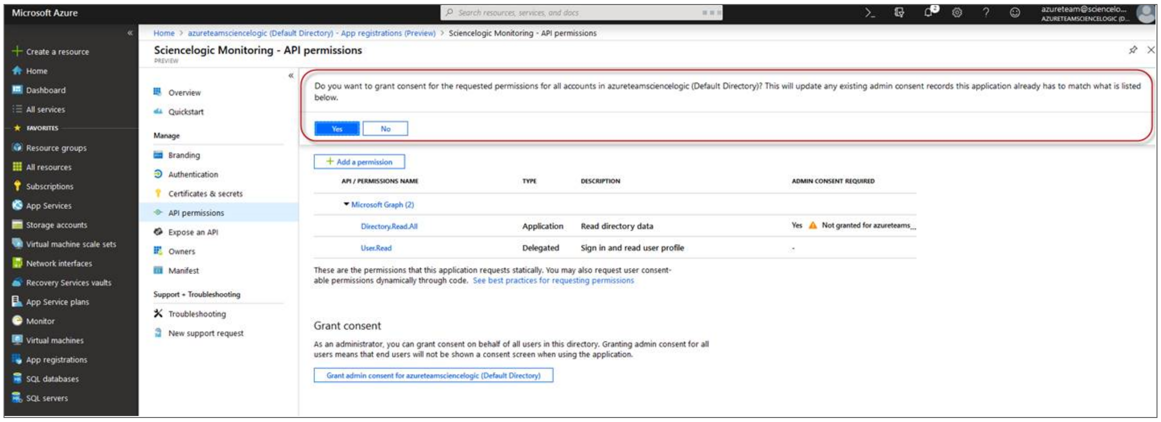
Application permissions: Your application runs as a background service or daemon without a signed-in user.

PERMISSION	ADMIN CONSENT REQUIRED
▸ AccessReview	
▸ Application	
▸ AuditLog	
▸ Calendars	
▸ Calls	
▸ ChannelMessage	
▸ Chat	
▸ Contacts	
▸ Device	
▾ Directory (1)	
☑ Directory.Read.All Read directory data	Yes
□ Directory.ReadWrite.All Read and write directory data	Yes
▸ Domain	

5. After you have added the Read directory data, in the **API permissions** page, click the **[Add Permissions]** button.

6. Click **[Grant admin consent for [Directory Name]]**.

7. A pop-up window appears asking if you grant consent for the required permissions for all accounts in your directory. Click **[Yes]**.



Do you want to grant consent for the requested permissions for all accounts in azureteamsciencelogic (Default Directory)? This will update any existing admin consent records this application already has to match what is listed below.

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
Microsoft Graph (2)			
Directory.Read.All	Application	Read directory data	Yes ⚠ Not granted for azureteams...
User.Read	Delegated	Sign in and read user profile	-

These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. See best practices for requesting permissions

Grant consent

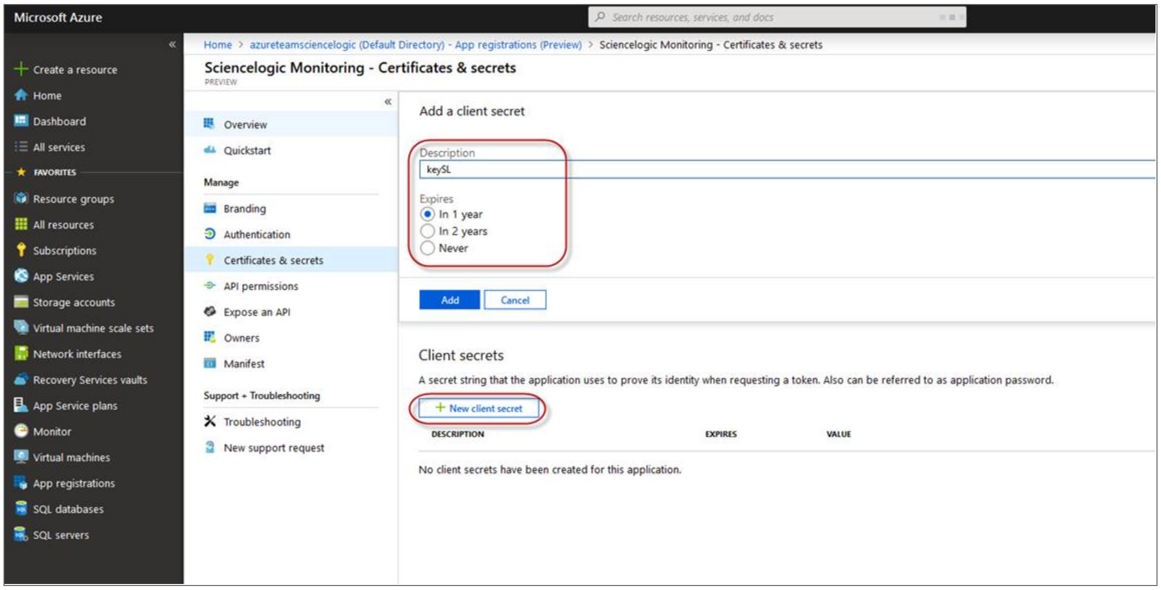
As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end users will not be shown a consent screen when using the application.

Generating the Secret Key

When configuring a SOAP/XML credential for Azure in SL1, you need to provide a secret key for the Azure Active Directory application that you will use to authenticate your account.

To generate a secret key:

1. Log in to the Azure portal at https://portal.azure.com, and type "active directory" in the **Search** field at the top of the window.
2. From the search results, select *Azure Active Directory*, and then click **App registrations**.
3. Select the app and then click **[Certificates & secrets]**.
4. In the **Client secrets** pane, click **[+ New client secret]**.



Add a client secret

Description: keySL

Expires
● In 1 year
○ In 2 years
○ Never

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

DESCRIPTION	EXPIRES	VALUE

No client secrets have been created for this application.

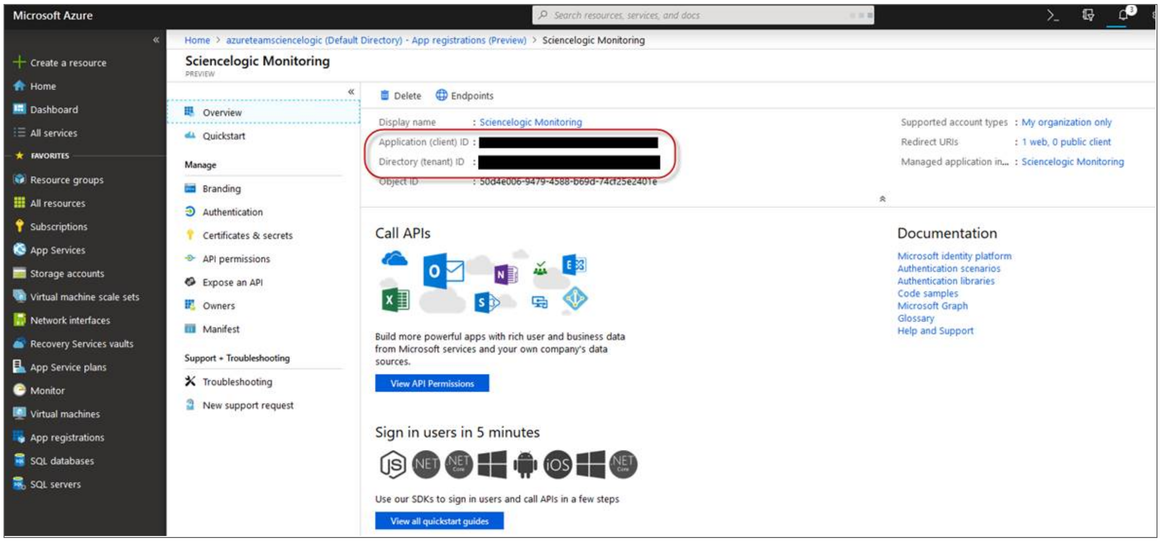
5. In the **Add a client secret** pane, type a name in the ***Description*** field and select a duration in the ***Expires*** field.
6. Click **[Add]** to generate the secret key. A new key value displays in the **Client secrets** pane.
7. Copy and save the key value.

Locating the Application ID and Tenant ID

When configuring a SOAP/XML credential for Azure in SL1, you need to provide the Application ID of the Azure Active Directory application you will use to authenticate your Azure account.

To locate the Application ID:

1. Log in to the Azure portal at https://portal.azure.com, and type "active directory" in the **Search** field at the top of the window.
2. From the search results, select *Azure Active Directory*, and then click **App registrations**.
3. Click the name of the Active Directory application you will use to authenticate your Azure account. The Application ID and Tenant ID appear in the **Overview** section.



Display name : Sciencelogic Monitoring

Application (client) ID : [redacted]

Directory (tenant) ID : [redacted]

Object ID : 50d4e006-9479-4588-b69d-74cf25e2401e

Supported account types : My organization only

Redirect URIs : 1 web, 0 public client

Managed application in... : Sciencelogic Monitoring

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Use our SDKs to sign in users and call APIs in a few steps

4. Copy and save the values in the corresponding credential fields.

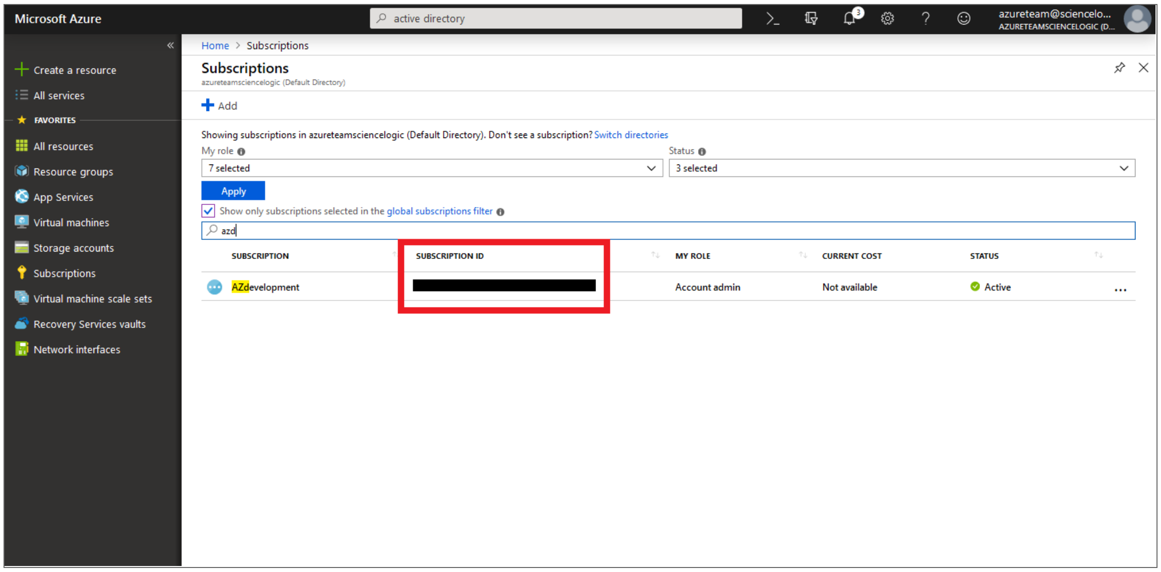
Locating the Subscription ID

If you are monitoring only a single Azure subscription, you must provide the Subscription ID of the Azure Active Directory application you will use to authenticate your account when you configure your SOAP/XML credential for Azure in SL1.

NOTE: If you are monitoring an account with multiple child subscriptions, you can skip this section.

To locate the Subscription ID:

1. In the left pane of the Azure portal (https://portal.azure.com), click **[Subscriptions]**.
2. Copy and save the ***Subscription ID*** of the subscription where you created the Azure Active Directory application you will use to authenticate your account.



Showing subscriptions in azureteamsciencelogic (Default Directory). Don't see a subscription? Switch directories

My role: 7 selected

Status: 3 selected

☑ Show only subscriptions selected in the global subscriptions filter

azd

SUBSCRIPTION	SUBSCRIPTION ID	MY ROLE	CURRENT COST	STATUS
AZdevelopment	[redacted]	Account admin	Not available	✓ Active

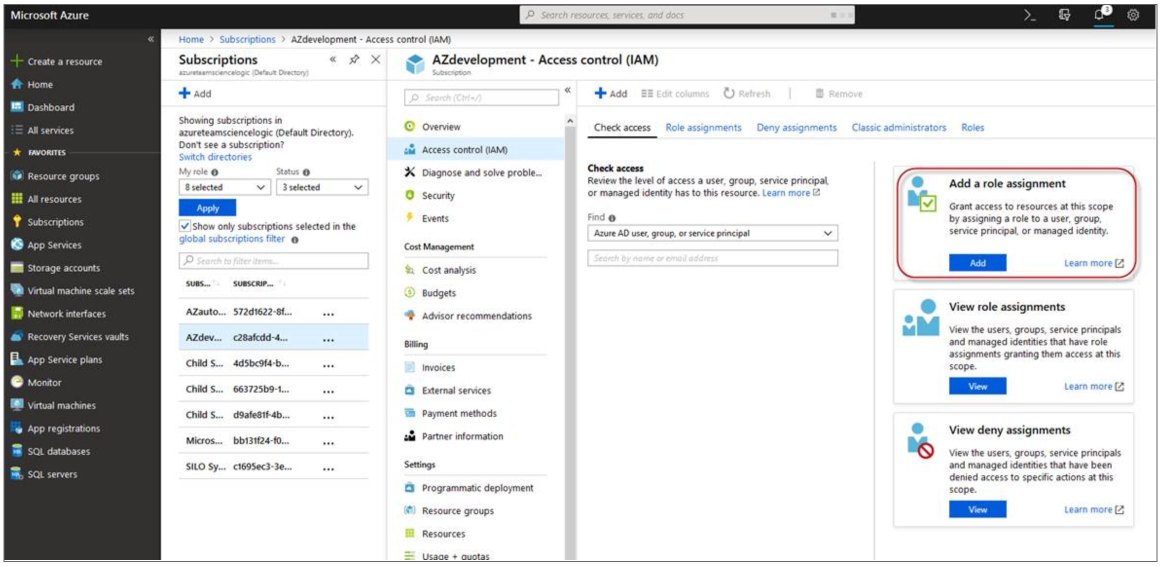
Adding Reader Access to the Active Directory Application

To allow ScienceLogic to access your Azure account, you must specify the type of access the user whose information you will use in your SOAP/XML credential has to the Active Directory application used to authenticate your account. Use the ***Reader*** access role, which is a read-only user that can view everything but cannot make changes.

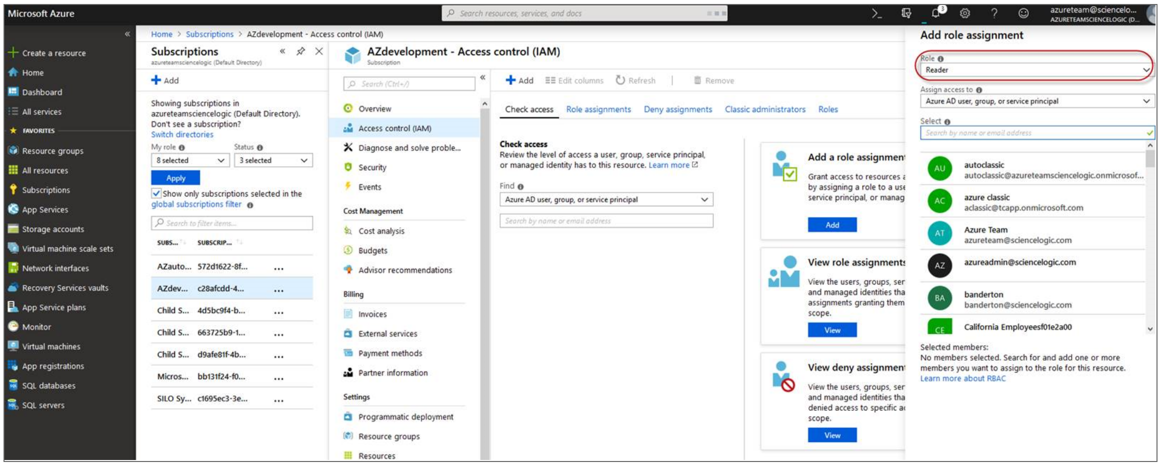
To specify the access role to the Azure Active Directory application:

1. In the left pane of the Azure Portal (https://portal.azure.com), click **[Subscriptions]**.
2. Click the name of your subscription, and then click **[Access control (IAM)]**.

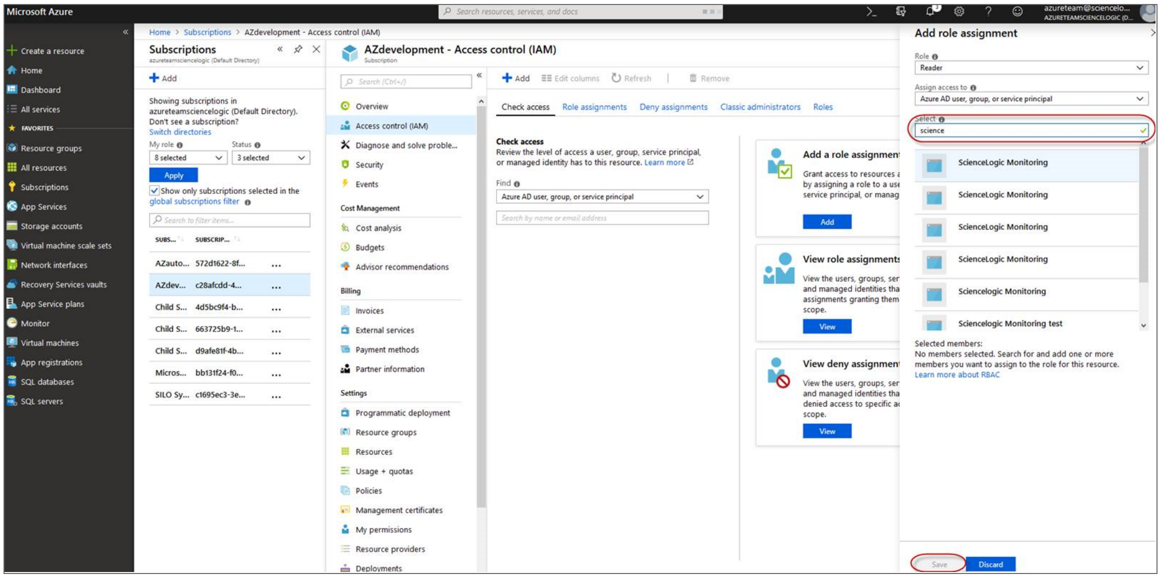
3. In the **Access Control (IAM)** pane, click the **[Add]** button in the **Add a role assignment** section.


Microsoft Azure
Search resources, services, and docs
Create a resource
Home
Dashboard
All services
FAVORITES
Resource groups
All resources
Subscriptions
App Services
Storage accounts
Virtual machine scale sets
Network interfaces
Recovery Services vaults
App Service plans
Monitor
Virtual machines
App registrations
SQL databases
SQL servers
Home > Subscriptions > AZdevelopment - Access control (IAM)
Subscriptions
azureteamsciencelogic (Default Directory)
Add
Showing subscriptions in azureteamsciencelogic (Default Directory). Don't see a subscription?
Switch directories
My role
Status
8 selected
3 selected
Apply
Show only subscriptions selected in the global subscriptions filter
Search to filter items...
SUBS...
SUBSCRIP...
AZauto... 572d1622-8f...
AZdev... c28afcdd-4...
Child S... 4d5bc9f4-b...
Child S... 663725b9-1...
Child S... d9afe81f-4b...
Micros... bb131f24-f0...
SILO Sy... c1695ec3-3e...
AZdevelopment - Access control (IAM)
Subscription
Search (Ctrl+/)
Overview
Access control (IAM)
Diagnose and solve proble...
Security
Events
Cost Management
Cost analysis
Budgets
Advisor recommendations
Billing
Invoices
External services
Payment methods
Partner information
Settings
Programmatic deployment
Resource groups
Resources
Usage + quotas
Add
Edit columns
Refresh
Remove
Check access
Role assignments
Deny assignments
Classic administrators
Roles
Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more
Find
Azure AD user, group, or service principal
Search by name or email address
Add a role assignment
Grant access to resources at this scope by assigning a role to a user, group, service principal, or managed identity.
Add
Learn more
View role assignments
View the users, groups, service principals and managed identities that have role assignments granting them access at this scope.
View
Learn more
View deny assignments
View the users, groups, service principals and managed identities that have been denied access to specific actions at this scope.
View
Learn more

4. In the **Add a role assignment** pane, select *Reader* in the ***Role*** field.


Microsoft Azure
Search resources, services, and docs
azureteam@sciencelo...
AZURE
TEAMSCIENCELOGIC (D...
Create a resource
Home
Dashboard
All services
FAVORITES
Resource groups
All resources
Subscriptions
App Services
Storage accounts
Virtual machine scale sets
Network interfaces
Recovery Services vaults
App Service plans
Monitor
Virtual machines
App registrations
SQL databases
SQL servers
Home > Subscriptions > AZdevelopment - Access control (IAM)
Subscriptions
AZdevelopment - Access control (IAM)
Check access
Role assignments
Deny assignments
Classic administrators
Roles
Add a role assignment
View role assignments
View deny assignments
Add
View
Add role assignment
Role
Reader
Assign access to
Azure AD user, group, or service principal
Select
Search by name or email address
AU autoclassic autoclassic@azureteamsciencelogic.onmicrosof...
AC azure classic aclassic@tcapp.onmicrosoft.com
AT Azure Team azureteam@sciencelogic.com
AZ azureadmin@sciencelogic.com
BA banderton banderton@sciencelogic.com
CE California Employeesf01e2a00
Selected members:
No members selected. Search for and add one or more members you want to assign to the role for this resource.
Learn more about RBAC

5. In the ***Select*** field, type the name of the Azure Active Directory application you will use to authenticate your account.



Add role assignment

Role: Reader

Assign access to: Azure AD user, group, or service principal

Select: science

Selected members:
No members selected. Search for and add one or more members you want to assign to the role for this resource.

6. Select the application from the search results and click **[Save]**.

Setting Up a Proxy Server

Depending on your needs, you can optionally enable SL1 to connect to Azure through a third-party proxy server such as SQUID. With this configuration, SL1 connects to the proxy server, which then connects to Azure. Azure relays information to the proxy server and SL1 then retrieves that information from the proxy.

NOTE: You can connect to Azure via a proxy server regardless of whether you are monitoring a single subscription or an account with multiple child subscriptions. You can connect to Microsoft Azure, Microsoft Azure Government, and Microsoft Azure Germany and China regions via a proxy server.

NOTE: The *Microsoft: Azure* PowerPack is certified to work with SQUID version 3.5.12 proxy servers.

If you choose to use a proxy server, configure the third-party proxy server based on the third-party documentation. Depending on the type of authentication you require, you might need to specify a user name and password for the proxy server configuration. Also, make a note of the port you opened for the configuration, as this information is needed when creating the SOAP/XML credential.

Creating a SOAP/XML Credential for Azure

After you note the application ID, subscription ID, tenant ID, and secret key of the application (that is registered with Azure Active Directory) that you will use to authenticate your Azure account, you can create a SOAP/XML credential for Azure in SL1. This credential allows the Dynamic Applications in the *Microsoft: Azure* PowerPack to communicate with your Azure subscriptions.

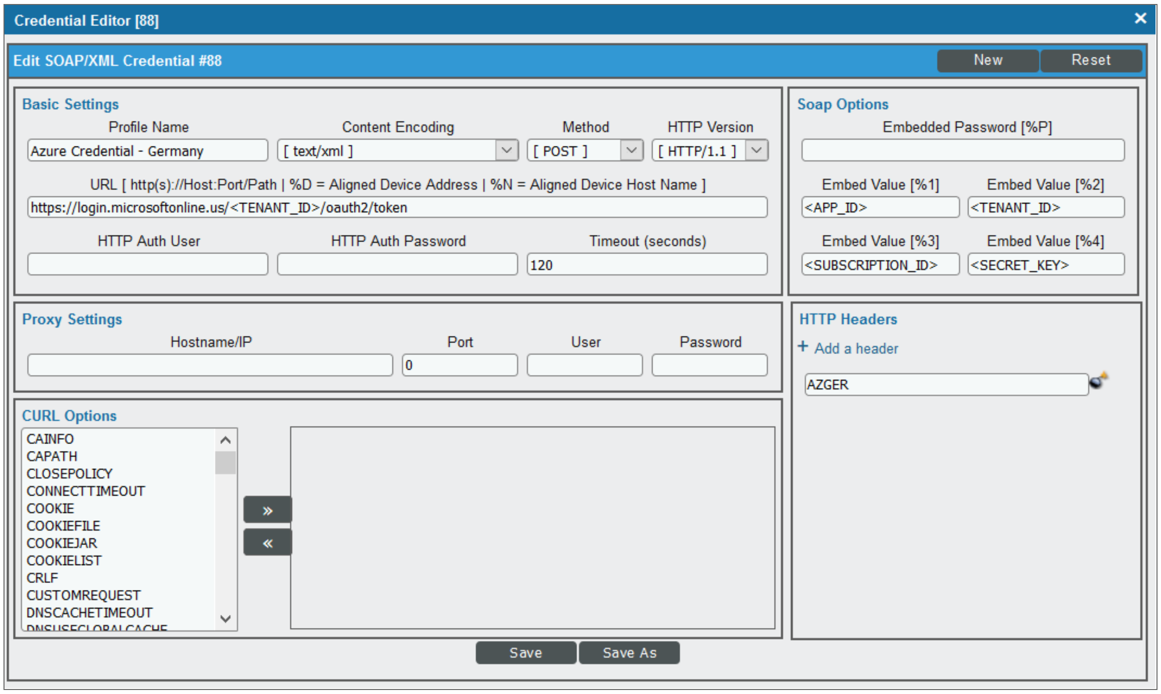
If you want to connect to your Azure account through a third-party proxy server, you must also add the proxy information in the credential. This applies to Microsoft Azure, Microsoft Azure Government, and the Microsoft Azure German and Chinese regions.

The *Microsoft: Azure* PowerPack includes multiple sample credentials you can use as templates for creating SOAP/XML credentials for Azure. They are:

- **Azure Credential - China**, for users who connect to an Azure data center in a Chinese region
- **Azure Credential - Germany**, for users who connect to an Azure data center in a German region (requires a subscription in Germany or Europe)
- **Azure Credential Gov Example**, for users who subscribe to Microsoft Azure Government
- **Azure Credential Proxy Example**, for users who connect to Azure through a third-party proxy server
- **Azure Credential Example**, for all other users.

To create a SOAP/XML credential for Azure:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the sample credential you want to use and then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears:



Credential Editor [88]

Edit SOAP/XML Credential #88

Basic Settings

Profile Name: Azure Credential - Germany
Content Encoding: [text/xml]
Method: [POST]
HTTP Version: [HTTP/1.1]
URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://login.microsoftonline.us/<TENANT_ID>/oauth2/token
HTTP Auth User:
HTTP Auth Password:
Timeout (seconds): 120

Soap Options

Embedded Password [%P]:
Embed Value [%1]: <APP_ID>
Embed Value [%2]: <TENANT_ID>
Embed Value [%3]: <SUBSCRIPTION_ID>
Embed Value [%4]: <SECRET_KEY>

Proxy Settings

Hostname/IP:
Port: 0
User:
Password:

HTTP Headers

+ Add a header
AZGER

CURL Options

CAINFO
CAPATH
CLOSEPOLICY
CONNECTTIMEOUT
COOKIE
COOKIEFILE
COOKIEJAR
COOKIELIST
CRLF
CUSTOMREQUEST
DNSCACHETIMEOUT
DNSUSEGLOBALCACHE

3. Enter values in the following fields:

Basic Settings

- ***Profile Name***. Type a new name for the Azure credential.

- ***Content Encoding***. Select *text/xml*.
- ***Method***. Select *POST*.
- ***HTTP Version***. Select *HTTP/1.1*.
- ***URL***. Type the tenant ID in the appropriate place in the URL provided in the sample credential.
- ***HTTP Auth User***. Leave this field blank.
- ***HTTP Auth Password***. Leave this field blank.
- ***Timeout (seconds)***. Type "120".

Proxy Settings

- ***Hostname/IP***. If you are connecting to Azure via a proxy server, type the server's hostname or IP address. Otherwise, leave this field blank.
- ***Port***. If you are connecting to Azure via a proxy server, type the port number you opened when *setting up the proxy server*. Otherwise, leave this field blank.
- ***User***. If you are connecting to Azure via a proxy server using basic authentication, type the server's administrator username. Otherwise, leave this field blank.
- ***Password***. If you are connecting to Azure via a proxy server using basic authentication, type the server's administrator password. Otherwise, leave this field blank.

CURL Options

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

SOAP Options

- ***Embedded Password [%P]***. Type the secret key for the Azure Active Directory application.
- ***Embed Value [%1]***. Type the Application ID for the Azure Active Directory application.
- ***Embed Value [%2]***. Type the Tenant ID for the Azure Active Directory application.
- ***Embed Value [%3]***. If you are monitoring only a single Azure subscription, type the Subscription ID for the Azure Active Directory application. If you are monitoring multiple subscriptions, leave this field blank.
- ***Embed Value [%4]***. Leave this field blank. Optionally, you can use this field to add the secret key for the Azure Active Directory application.

HTTP Headers

- ***HTTP Headers***. Leave this field blank, unless one of the following scenarios applies to you:
  - If you are using Microsoft Azure Government, this field contains the text "AZGOV".
  - If you are monitoring Microsoft Azure resources in Germany, this field contains the text "AZGER".
  - If you are monitoring Microsoft Azure resources in China, this field contains the text "AZCHINA".
  - If you would like to enable extended logging, enter "LOGGING" in to a header field. The log file is located at `/tmp/azure.log`
  - SSL certification verification is enabled by default, but you can disable it in a header field by entering "VERIFY:FALSE".

4. Click **[Save As]**.
5. In the confirmation message, click **[OK]**.

Load-Balancing an Account with Multiple Subscriptions

When monitoring an account with multiple child subscriptions, instead of discovering all child subscriptions in a single dynamic component map under their parent account, you can load-balance subscriptions and their components across multiple Data Collectors.

To do this:

- The Collector Group that discovers a group of subscriptions can contain only one Data Collector. You cannot use multiple Data Collectors to discover the Azure components in a single dynamic component map or discover the same device in multiple dynamic component maps.
- To group multiple Azure subscriptions into a single dynamic component map, you need to create a shared credential for that group of subscriptions.
- To create the credential:
  - Perform all of the steps in the section on ***Configuring an Azure Active Directory Application***.
  - Align each subscription in the group with the same application that you registered with Azure AD.
  - In the credential, enter the application ID in the ***Embed Value [%1]*** field.
  - In the credential, leave the ***Embed Value [%3]*** field blank.
- During discovery, use this credential to discover the group of subscriptions.
- During discovery, specify the Data Collector you want to use for the group of subscriptions.
- The discovered subscriptions will reside in a common dynamic component map.
- Repeat these steps for each group of subscriptions.

Testing the Azure Credential

The *Microsoft: Azure* PowerPack includes a Credential Test for Microsoft Azure. Credential Tests define a series of steps that SL1 can execute on demand to validate whether a credential works as expected.

The "Azure Credential Test - ARM" can be used to test a SOAP/XML credential for monitoring Azure using the Dynamic Applications in the *Microsoft: Azure* PowerPack.

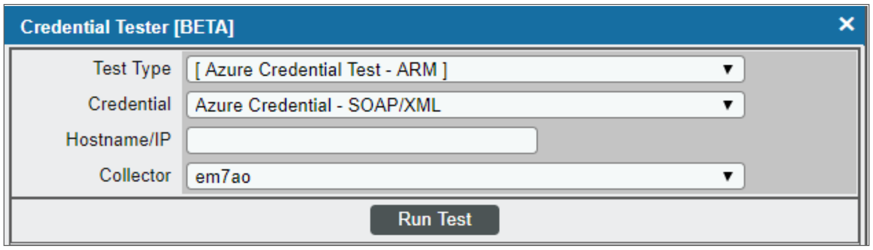
CAUTION: When testing Azure credentials for version 110 or greater of the *Microsoft: Azure* PowerPack, you should use the "Azure Credential Test - ARM" that is included in the PowerPack rather than the "Azure Credential Test" that is included by default in SL1. The "Azure Credential Test - ARM" supports proxy server entries in the credential being tested and can test that your Azure credential has the latest required permissions in Azure, whereas the older "Azure Credential Test" cannot do these things.

The "Azure Credential Test - ARM" performs the following steps:

- ***Test Port Availability***. Performs an NMAP request to test the availability of the Azure endpoint HTTPS port.
- ***Test Name Resolution***. Performs an nslookup request on the Azure endpoint.
- ***Make connection to Azure account***. Attempts to connect to the Azure service using the account specified in the credential.
- ***Validate Azure Microsoft Graph Permission***. Verifies that the Azure Active Directory application has Microsoft Graph API permissions.
- ***Validate Azure subscription assignments***. Verifies that the Azure Active Directory application is assigned to the subscription.

To test the Azure credential:

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



Credential Tester [BETA]

Test Type	[Azure Credential Test - ARM]
Credential	Azure Credential - SOAP/XML
Hostname/IP	
Collector	em7ao

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

4. Click the **[Run Test]** button. The **Test Credential** window appears, displaying 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".

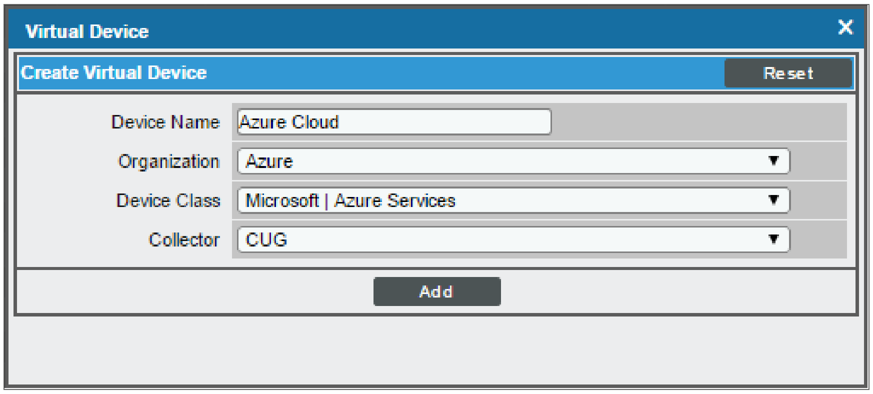
Creating an Azure Virtual Device

Because the Azure service does not have a static IP address, you cannot discover an Azure device using discovery. Instead, you must create a ***virtual device*** that represents the Azure service. A virtual device is a user-defined container that represents a device or service that cannot be discovered by SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications.

To create a virtual device that represents your Azure service:

1. Go to the **Device Manager** page (Devices > Device Manager, or Registry > Devices > Device Manager in the classic SL1 user interface).
2. Click the **[Actions]** button and select *Create Virtual Device* from the menu. The **Virtual Device** modal page appears.

3. Enter values in the following fields:



Device Name: Azure Cloud
Organization: Azure
Device Class: Microsoft | Azure Services
Collector: CUG

- ***Device Name***. Enter a name for the device. For example, "Azure Cloud".
- ***Organization***. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.
- ***Device Class***. Select *Microsoft | Azure Services*.
- ***Collector***. Select the collector group that will monitor the device.

TIP: When monitoring an account with multiple child subscriptions, you can load-balance how SL1 monitors your Azure components by discovering groups of subscriptions and their components across multiple collectors. For details, see the section on ***Load-Balancing an Account with Multiple Subscriptions***.

4. Click **[Add]** to create the virtual device.

Aligning the Azure Dynamic Applications

The Dynamic Applications in the *Microsoft: Azure* PowerPack are divided into the following types:

- ***Discovery***. These Dynamic Applications poll Azure for new instances of services or changes to existing instances of services.
- ***Configuration***. These Dynamic Applications retrieve configuration information about each service instance and retrieve any changes to that configuration information.
- ***Performance***. These Dynamic Applications poll Azure for performance metrics.

When configuring SL1 to monitor Azure services, you can manually align Dynamic Applications to discover Azure component devices.

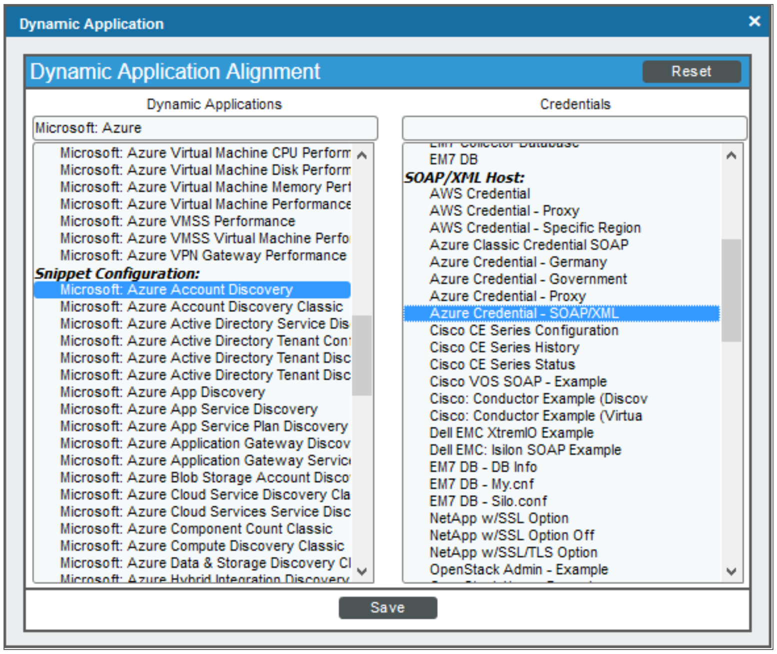
Discovering Azure Component Devices

To discover all the components of your Azure platform, you must manually align the "Microsoft: Azure Account Discovery" Dynamic Application with the Azure virtual device.

> **TIP:** When monitoring an account with multiple child subscriptions, ScienceLogic recommends that you first review your device capacity and load limits to determine the best method for implementation prior to discovery. For details, see the section on *Load-Balancing an Account with Multiple Subscriptions*.

To manually align the "Microsoft: Azure Account Discovery" Dynamic Application:

1. Go to the **Device Manager** page (Devices > Device Manager, or Registry > Devices > Device Manager in the classic SL1 user interface).
2. Click the wrench icon (🔧) for your Azure virtual device.
3. In the ***Device Administration*** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
4. Click the **[Actions]** button and select *Add Dynamic Application* from the menu.
5. In the **Dynamic Application Alignment** modal:


Dynamic Application
×
Dynamic Application Alignment
Reset
Dynamic Applications
Credentials
Microsoft: Azure
Microsoft: Azure Virtual Machine CPU Perform
Microsoft: Azure Virtual Machine Disk Perform
Microsoft: Azure Virtual Machine Memory Perf
Microsoft: Azure Virtual Machine Performance
Microsoft: Azure VMSS Performance
Microsoft: Azure VMSS Virtual Machine Perfo
Microsoft: Azure VPN Gateway Performance
Snippet Configuration:
Microsoft: Azure Account Discovery
Microsoft: Azure Account Discovery Classic
Microsoft: Azure Active Directory Service Dis
Microsoft: Azure Active Directory Tenant Con
Microsoft: Azure Active Directory Tenant Disc
Microsoft: Azure Active Directory Tenant Disc
Microsoft: Azure App Discovery
Microsoft: Azure App Service Discovery
Microsoft: Azure App Service Plan Discovery
Microsoft: Azure Application Gateway Discov
Microsoft: Azure Application Gateway Servic
Microsoft: Azure Blob Storage Account Disco
Microsoft: Azure Cloud Service Discovery Cla
Microsoft: Azure Cloud Services Service Disc
Microsoft: Azure Component Count Classic
Microsoft: Azure Compute Discovery Classic
Microsoft: Azure Data & Storage Discovery Cl
Microsoft: Azure Hybrid Integration Discovery
EM7 DB
SOAP/XML Host:
AWS Credential
AWS Credential - Proxy
AWS Credential - Specific Region
Azure Classic Credential SOAP
Azure Credential - Germany
Azure Credential - Government
Azure Credential - Proxy
Azure Credential - SOAP/XML
Cisco CE Series Configuration
Cisco CE Series History
Cisco CE Series Status
Cisco VOS SOAP - Example
Cisco: Conductor Example (Discov
Cisco: Conductor Example (Virtua
Dell EMC XtremIO Example
Dell EMC: Isilon SOAP Example
EM7 DB - DB Info
EM7 DB - My.cnf
EM7 DB - Silo.conf
NetApp w/SSL Option
NetApp w/SSL Option Off
NetApp w/SSL/TLS Option
OpenStack Admin - Example
Save

   - In the ***Dynamic Applications*** field, select *Microsoft: Azure Account Discovery*.
   - In the ***Credentials*** field, select the credential you created for your Azure service.

6. Click **[Save]** to align the Dynamic Application with the Azure virtual device.

When you align the "Microsoft: Azure Account Discovery" Dynamic Application with the Azure virtual device, SL1 does one of the following, depending on your subscription model:

- If you are monitoring an account with multiple child subscriptions, SL1 creates a root component device representing the Azure account and one or more child component devices representing all of your Azure subscriptions.
- If you are monitoring a single subscription, SL1 creates a root component device representing your Azure subscription.

TIP: When monitoring an account with multiple child subscriptions, you can load-balance how SL1 monitors your Azure components by discovering groups of subscriptions and their components across multiple collectors. For details, see the section on ***Load-Balancing an Account with Multiple Subscriptions***.

SL1 then automatically aligns several other Dynamic Applications to the subscription component devices. These additional Dynamic Applications discover and create component devices for Active Directory tenants, Traffic Manager profiles, and each location used by the Azure account.

Under each location, SL1 then discovers the following component devices:

- Application Gateway Services
  - Application Gateways
- App Services
  - App Service Plan
    - Function App
    - Web App

- Azure Cache for Redis
- Azure Database for MySQL Services
    - Azure Database for MySQL Servers
- Azure Database for PostgreSQL Services
    - Azure Database for PostgreSQL Servers
- Azure Functions
- Azure Kubernetes Services (AKS)
    - Azure Kubernetes Clusters
- Azure Service Buses (Relay)
- Batch Accounts
- Content Delivery Networks
    - CDN Profiles
        - CDN Endpoints
- Cosmos DB Accounts
- DNS Services
    - DNS Zones
- ExpressRoute Services
    - ExpressRoute Circuits
        - ExpressRoute Peering
            - ExpressRoute Circuit Connections
- Key Vaults
- Load Balancer Services
    - Load Balancers
- Network Security Group Services
    - Network Security Groups
- Recovery Service Vaults Services
    - Recovery Service Vaults
- Resource Groups Services
    - Resource Groups
- SQL Server Services
    - SQL Servers
    - SQL Databases
- Storage Manage Disks
    - Manage Disk Service
        - Manage Disk

- Storage Services
    - Storage Accounts
- Virtual Machines Services
    - Virtual Machines
- Virtual Network Services
    - Virtual Networks
        - ExpressRoute Gateways
        - Virtual Network Gateways
        - Virtual Network Subnets
- VM Scale Set Services
    - VM Scale Sets
        - Virtual Machines
- Web Application Firewalls (WAF)
    - WAF on CDN Policies
    - WAF on Application Gateway Policies

NOTE: SL1 might take several minutes to align these Dynamic Applications and create the component devices in your Azure service.

NOTE: When discovering a large number of component devices, such as when discovering an account with multiple child subscriptions, the discovery process can cause the appearance of numerous critical events with the message, "`Large backlog of asynchronous jobs detected`". This will occur only during the initial discovery session.

Relationships Between Component Devices

In addition to parent/child relationships between component devices, SL1 also creates relationships between the following component devices:

- Apps and Resource Groups
- Application Gateways and Resource Groups
- Application Gateways and Virtual Network Subnets
- Azure CosmosDB and Resource Groups
- Azure CosmosDB and Virtual Networks
- Azure CosmosDB and Virtual Network Subnets
- Azure Traffic Managers and Traffic Managers
- Batch Accounts and Key Vaults

- Batch Accounts and Resource Groups
- Batch Accounts and Storage Groups
- CDN Profiles and Resource Groups
- Key Vaults and Resource Groups
- Key Vaults and Virtual Networks
- Key Vault Rules and Subnets
- Kubernetes Agent Pools and Subnets
- Load Balancers and Resource Groups
- Managed Disks and Resource Groups
- Managed Disks and Virtual Machines
- Network Security Groups and Resource Groups
- Network Security Groups and Virtual Network Subnets
- PostgreSQL Servers and Resource Groups
- PostgreSQL Servers and Subnets
- PostgreSQL Servers and PostgreSQL Server Replicas
- PostgreSQL Servers and Virtual Networks
- Recovery Service Vaults and Resource Groups
- Redis Cache Servers and Redis Cache Servers
- Redis Caches and Resource Groups
- Redis Caches and Subnets
- Redis Caches and Virtual Networks
- Service Bus Namespaces and Resource Groups
- Service Bus Namespaces and Service Bus Namespaces
- Service Bus Namespaces and Subnets
- Service Bus Namespaces and Virtual Networks
- SQL Databases and Resource Groups
- SQL Servers and Resource Groups
- SQL Servers and Server Replicas
- SQL Servers and Subnets
- SQL Servers and Virtual Networks
- SQL Servers and Virtual Network Subnets
- Storage Accounts and Resource Groups
- Traffic Manager Profiles and Resource Groups
- Virtual Machines and Network Security Groups
- Virtual Machines and Resource Groups

- Virtual Machines and Storage Accounts
- Virtual Machines and Virtual Networks
- Virtual Machines and Virtual Network Subnets
- Virtual Machine Scale Sets and Load Balancers
- Virtual Machine Scale Sets and Resource Groups
- Virtual Machine Scale Sets and Virtual Network Subnets
- Virtual Machine Scale Set Virtual Machines and Resource Groups
- Virtual Networks and Resource Groups
- VPN Gateways and Resource Groups
- VPN Gateways and Virtual Network Subnets
- WAF CDN Policies and Endpoints
- WAF CDN Policies and Resource Groups
- WAF Gateway Policies and Application Gateways
- WAF Gateway Policies and Resource Groups

Additionally, the platform can automatically build relationships between Azure component devices and other associated devices:

- If you discover Cisco Cloud Center devices using the Dynamic Applications in the *Cisco: CloudCenter* PowerPack version 103 or later, SL1 will automatically create relationships between Azure Virtual Machines and Cisco Cloud Center applications.
- If you discover Dynatrace environments using the Dynamic Applications in the *Dynatrace* PowerPack, SL1 will automatically create relationships between the following device types:
    - Azure Virtual Machines and Dynatrace Hosts
    - Azure Virtual Machine Scale Sets and Dynatrace Hosts
- If you discover Office 365 services using the Dynamic Applications in the *Microsoft: Office 365* PowerPack version 101 or later, SL1 will automatically create relationships between Azure Active Directory tenants and Office 365 Active Directory tenants.

Chapter

51

Microsoft: Azure

Overview

The following sections describe how to configure and discover Microsoft Azure resources for monitoring by SL1 using the *Microsoft: Azure* PowerPack:

> **NOTE**: The *Microsoft: Azure* PowerPack can monitor Microsoft Azure resources, Microsoft Azure Government resources, and Microsoft Azure resources in Germany and China regions.

NOTE: For more information about the *Microsoft: Azure* PowerPack, see the ***Monitoring Microsoft Azure*** manual.

Configuring an Azure Active Directory Application

To create a SOAP/XML credential that allows SL1 to access Microsoft Azure, you must provide the following information about an Azure application that is already registered with an Azure AD tenant:

- Application ID
- Subscription ID (if monitoring a single subscription)
- Tenant ID
- Secret key

To capture the above information, you must first create (or already have) an application that is registered with Azure Active Directory. The registered application must have Reader access in the subscription. You can then enter the required information about the application when configuring the SOAP/XML credential in SL1. The registered application and the ScienceLogic credential allow SL1 to retrieve information from Microsoft Azure.

TIP: For details on registering an Azure application, see https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app.

Creating an Active Directory Application in the Azure Portal

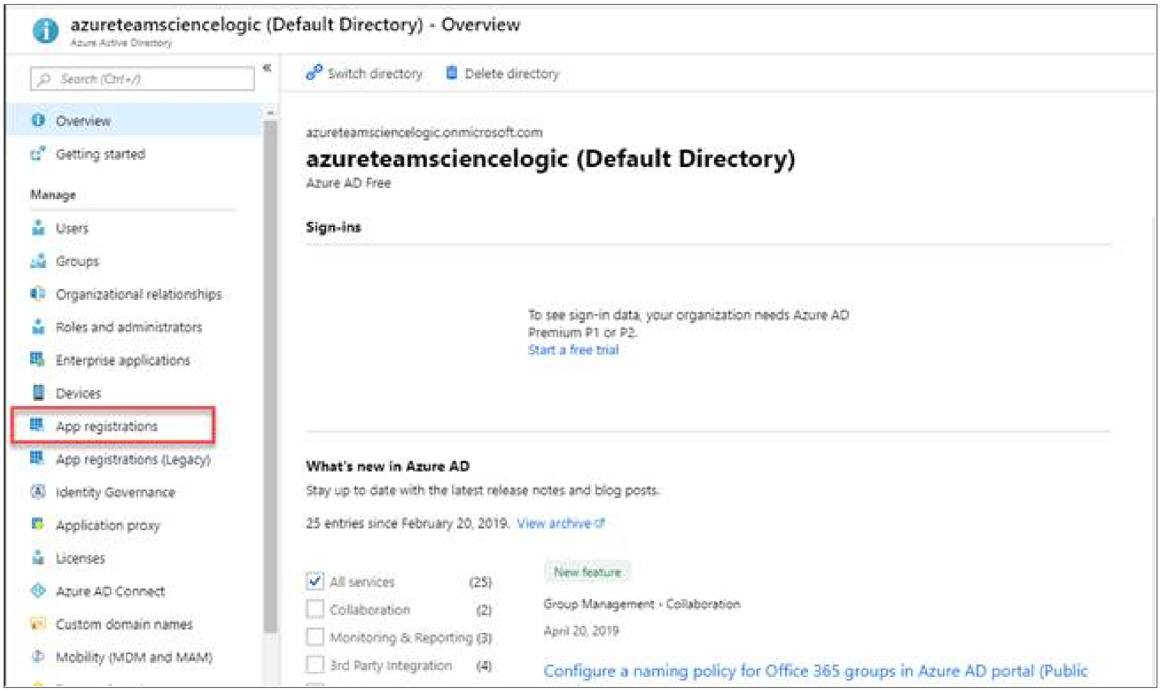
When configuring a SOAP/XML credential in SL1, you must provide the application ID, subscription ID, tenant ID, and secret key of an application that is registered with Azure Active Directory. You will use this registered application to authenticate your Azure account.

NOTE: You must have Service Administrator rights to create an Azure Active Directory application.

To create an application in Azure and register it with Azure Active Directory:

1. Log in to the Azure portal and type "active directory" in the **Search** field at the top of the window.

2. From the search results, select *Azure Active Directory*, and then click **App registrations**. The **App registrations** page appears:



azureteamsciencelogic (Default Directory) - Overview

Azure Active Directory

azureteamsciencelogic.onmicrosoft.com

azureteamsciencelogic (Default Directory)

Azure AD Free

Sign-ins

To see sign-in data, your organization needs Azure AD Premium P1 or P2.

Start a free trial

What's new in Azure AD

Stay up to date with the latest release notes and blog posts.

25 entries since February 20, 2019. View archive

☑ All services (25)

□ Collaboration (2)

□ Monitoring & Reporting (3)

□ 3rd Party Integration (4)

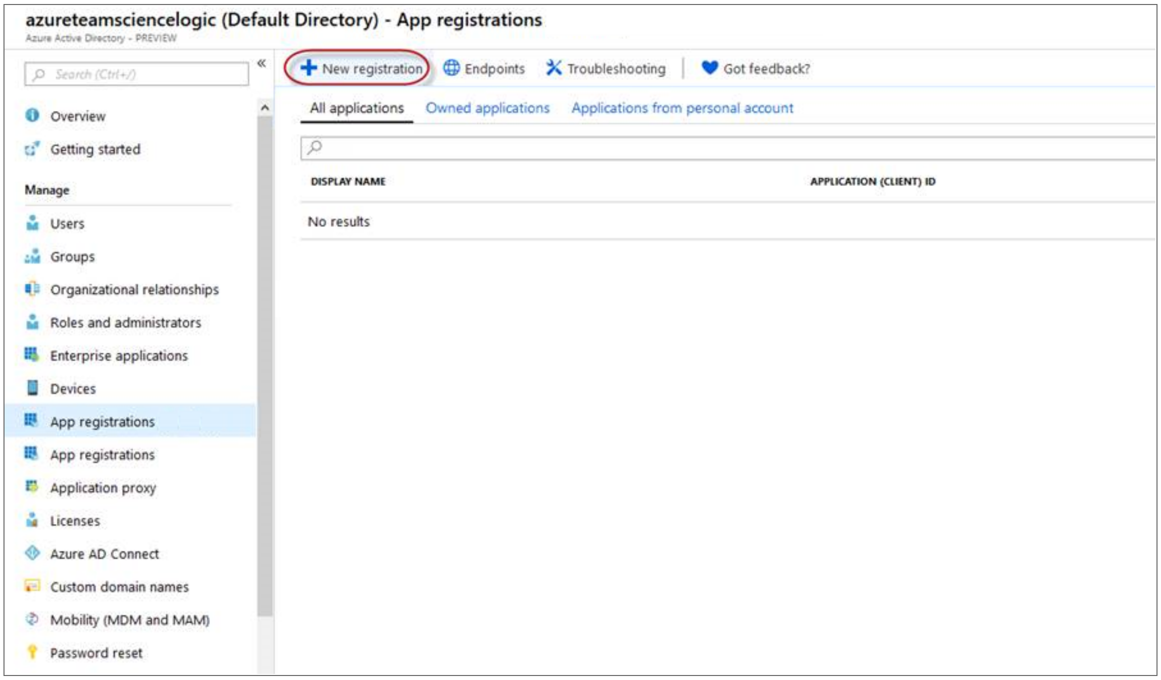
New feature

Group Management › Collaboration

April 20, 2019

Configure a naming policy for Office 365 groups in Azure AD portal (Public

3. Click the **[New registration]** button.

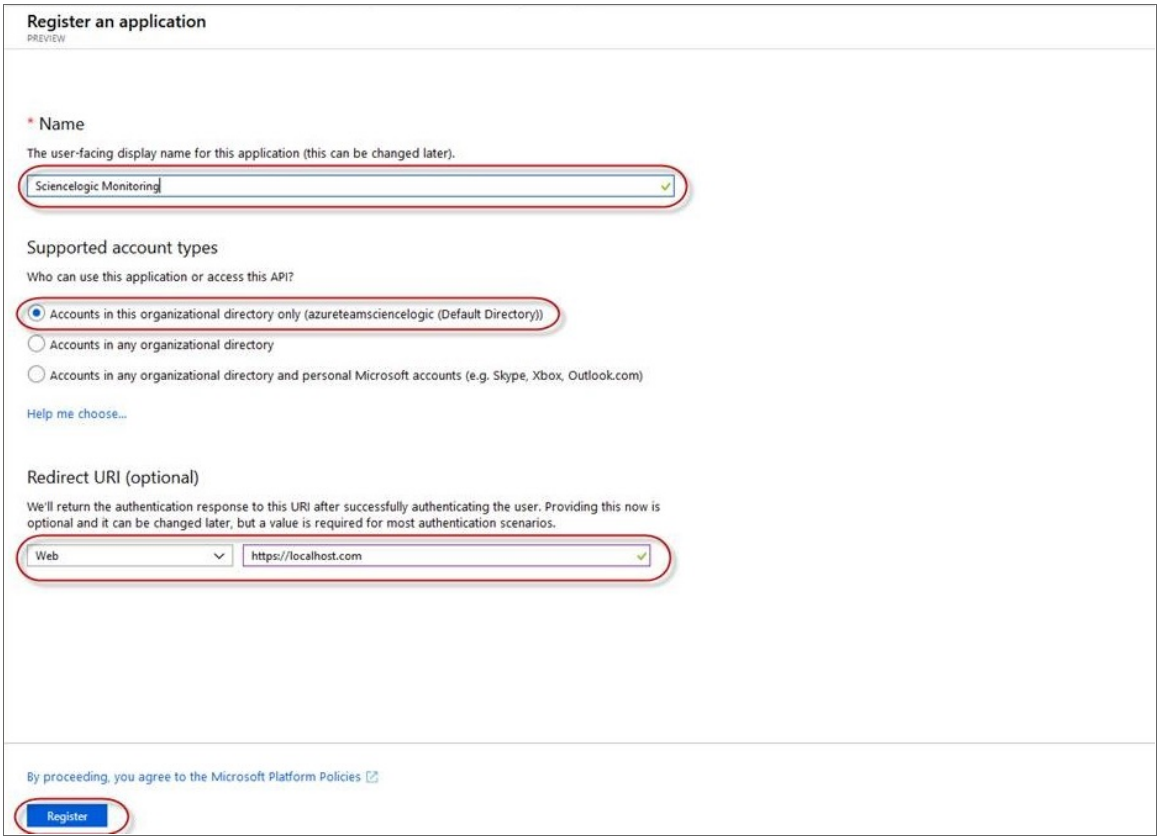


azureteamsciencelogic (Default Directory) - App registrations

Azure Active Directory - PREVIEW

DISPLAY NAME	APPLICATION (CLIENT) ID
No results	

4. When the **Register an application page** appears, enter your application's registration information:
    - ***Name***. Type a name for the application.
    - ***Supported account types***. Select *Accounts in this organizational directory only*.
    - ***Redirect URI (optional)***. Select *Web* in the drop-down menu and type a valid URL.



Register an application
PREVIEW

* Name
The user-facing display name for this application (this can be changed later).
Sciencelogic Monitoring

Supported account types
Who can use this application or access this API?
● Accounts in this organizational directory only (azureteamsciencelogic (Default Directory))
○ Accounts in any organizational directory
○ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

Help me choose...

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
Web
https://localhost.com

By proceeding, you agree to the Microsoft Platform Policies

5. Click the **[Register]**button. A message appears confirming that your application was added.

Adding Microsoft Graph APIs Permissions to the Application

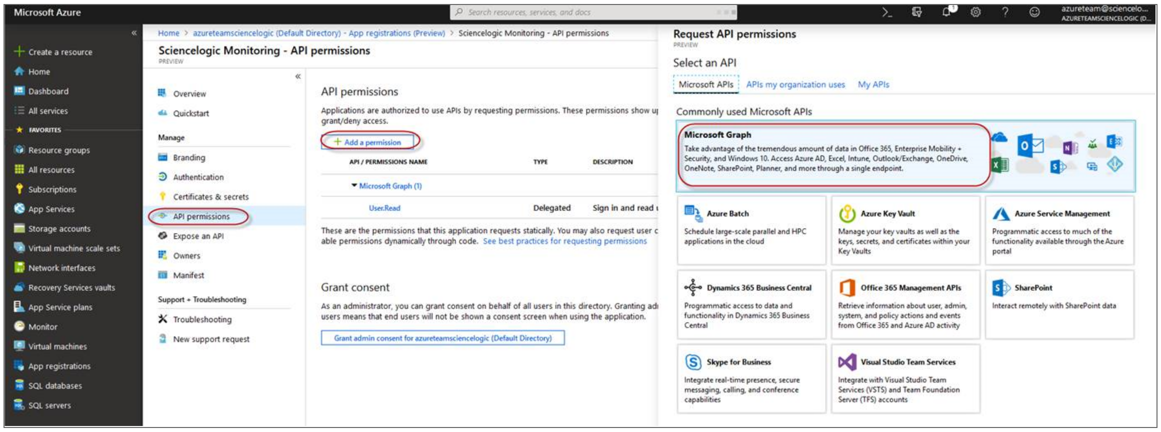
By default, any new Application has Microsoft Graph API permission. At a minimum, the Microsoft Graph APIs must have permission to directly read data.

To add the Microsoft Graph APIs:

1. In the **Search** field of the Azure portal (https://portal.azure.com), type "active directory".

2. Click **[App registrations]**, and then click on the name of the Azure Active Directory application you will use to authenticate your Azure account.

3. Click ***API Permissions***, and then click **[Add a permission]**. Next, select the **Microsoft Graph** option.



Applications are authorized to use APIs by requesting permissions. These permissions show u grant/deny access.

These are the permissions that this application requests statically. You may also request user c able permissions dynamically through code. See best practices for requesting permissions

As an administrator, you can grant consent on behalf of all users in this directory. Granting adı users means that end users will not be shown a consent screen when using the application.

Microsoft Graph: Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Batch: Schedule large-scale parallel and HPC applications in the cloud

Azure Key Vault: Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Service Management: Programmatic access to much of the functionality available through the Azure portal

Dynamics 365 Business Central: Programmatic access to data and functionality in Dynamics 365 Business Central

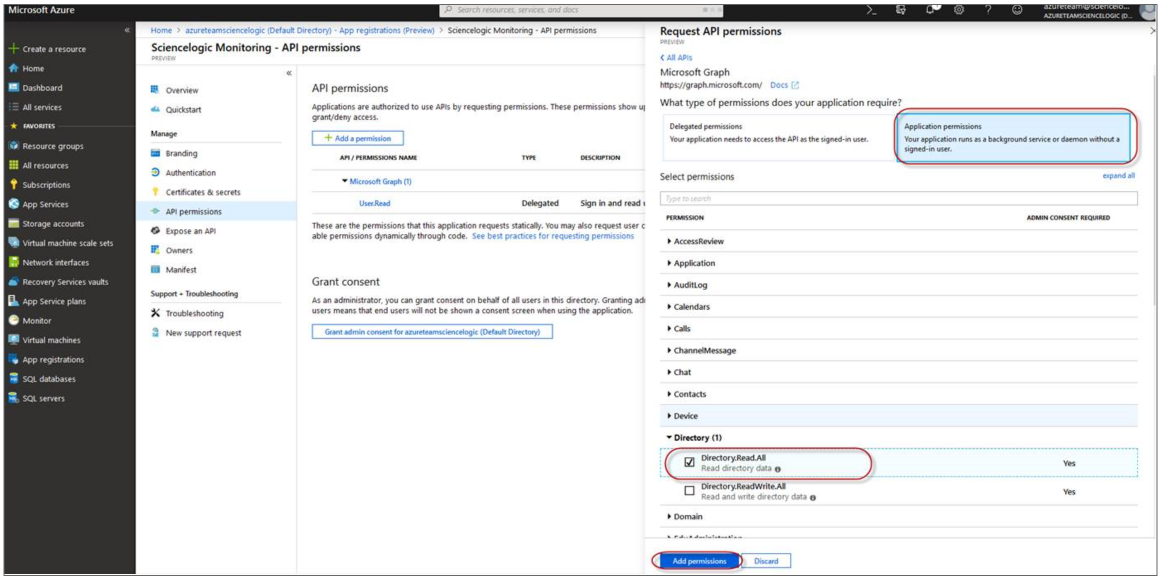
Office 365 Management APIs: Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

SharePoint: Interact remotely with SharePoint data

Skype for Business: Integrate real-time presence, secure messaging, calling, and conference capabilities

Visual Studio Team Services: Integrate with Visual Studio Team Services (VSTS) and Team Foundation Server (TFS) accounts

4. In the **Request API permissions** pane, under Select permissions, click the arrow next to **Directory** to open the submenu and select the checkbox for ***Directory.Read.all*** permission.



Applications are authorized to use APIs by requesting permissions. These permissions show u grant/deny access.

These are the permissions that this application requests statically. You may also request user c able permissions dynamically through code. See best practices for requesting permissions

As an administrator, you can grant consent on behalf of all users in this directory. Granting adı users means that end users will not be shown a consent screen when using the application.

What type of permissions does your application require?

Delegated permissions: Your application needs to access the API as the signed-in user.

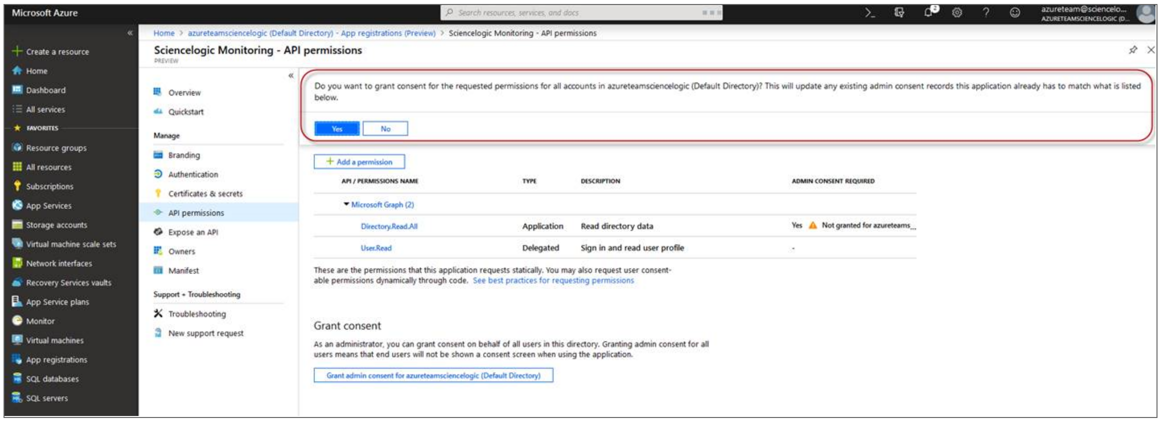
Application permissions: Your application runs as a background service or daemon without a signed-in user.

PERMISSION	ADMIN CONSENT REQUIRED
▸ AccessReview	
▸ Application	
▸ AuditLog	
▸ Calendars	
▸ Calls	
▸ ChannelMessage	
▸ Chat	
▸ Contacts	
▸ Device	
▾ Directory (1)	
☑ Directory.Read.All Read directory data	Yes
□ Directory.ReadWrite.All Read and write directory data	Yes
▸ Domain	

5. After you have added the Read directory data, in the **API permissions** page, click the **[Add Permissions]** button.

6. Click **[Grant admin consent for [Directory Name]]**.

7. A pop-up window appears asking if you grant consent for the required permissions for all accounts in your directory. Click **[Yes]**.



Do you want to grant consent for the requested permissions for all accounts in azureteamsciencelogic (Default Directory)? This will update any existing admin consent records this application already has to match what is listed below.

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
▾ Microsoft Graph (2)			
Directory.Read.All	Application	Read directory data	Yes ⚠ Not granted for azureteams...
User.Read	Delegated	Sign in and read user profile	-

These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. See best practices for requesting permissions

Grant consent

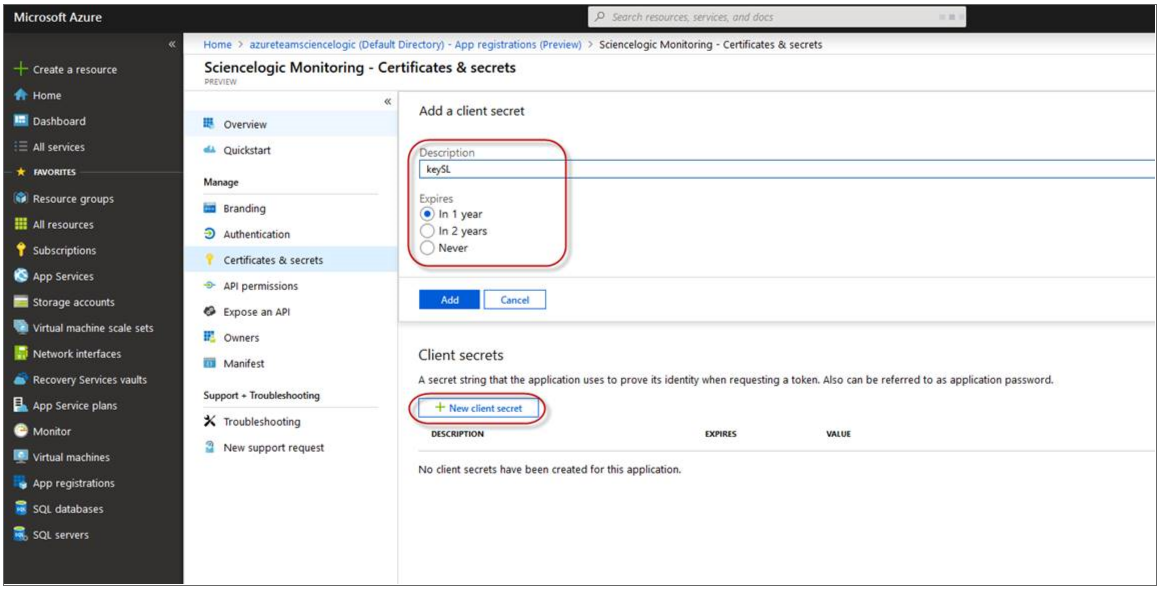
As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end users will not be shown a consent screen when using the application.

Generating the Secret Key

When configuring a SOAP/XML credential for Azure in SL1, you need to provide a secret key for the Azure Active Directory application that you will use to authenticate your account.

To generate a secret key:

1. Log in to the Azure portal at https://portal.azure.com, and type "active directory" in the **Search** field at the top of the window.
2. From the search results, select *Azure Active Directory*, and then click **App registrations**.
3. Select the app and then click **[Certificates & secrets]**.
4. In the **Client secrets** pane, click **[+ New client secret]**.



Add a client secret

Description: keySL

Expires
● In 1 year
○ In 2 years
○ Never

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

DESCRIPTION	EXPIRES	VALUE

No client secrets have been created for this application.

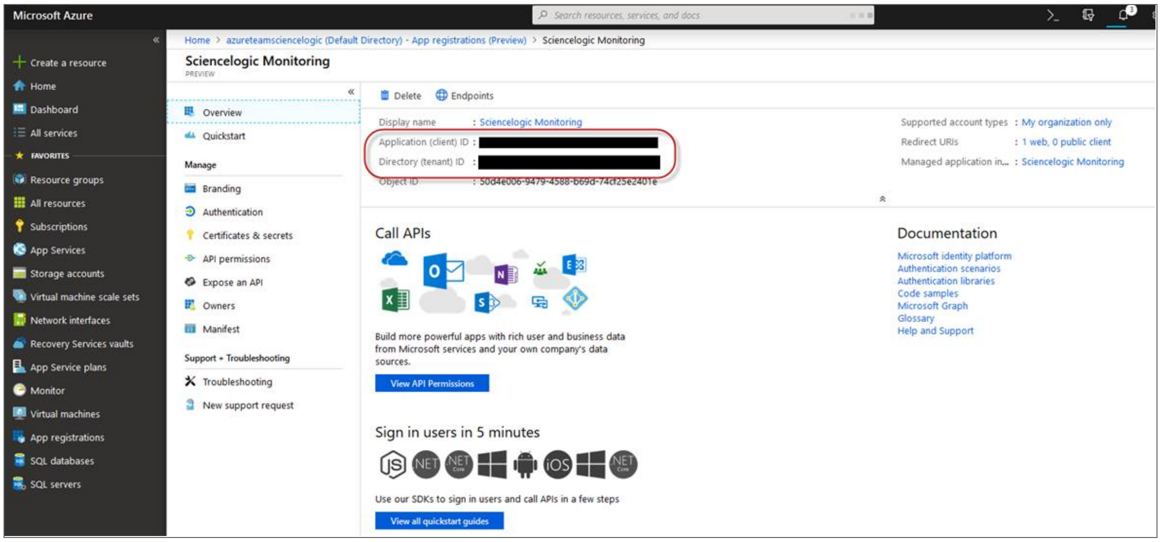
5. In the **Add a client secret** pane, type a name in the ***Description*** field and select a duration in the ***Expires*** field.
6. Click **[Add]** to generate the secret key. A new key value displays in the **Client secrets** pane.
7. Copy and save the key value.

Locating the Application ID and Tenant ID

When configuring a SOAP/XML credential for Azure in SL1, you need to provide the Application ID of the Azure Active Directory application you will use to authenticate your Azure account.

To locate the Application ID:

1. Log in to the Azure portal at https://portal.azure.com, and type "active directory" in the **Search** field at the top of the window.
2. From the search results, select *Azure Active Directory*, and then click **App registrations**.
3. Click the name of the Active Directory application you will use to authenticate your Azure account. The Application ID and Tenant ID appear in the **Overview** section.



Display name : Sciencelogic Monitoring
Application (client) ID : [redacted]
Directory (tenant) ID : [redacted]
Object ID : 50d4e006-9479-4588-b69d-74cf25e2401e

Supported account types : My organization only
Redirect URIs : 1 web, 0 public client
Managed application in... : Sciencelogic Monitoring

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Use our SDKs to sign in users and call APIs in a few steps

4. Copy and save the values in the corresponding credential fields.

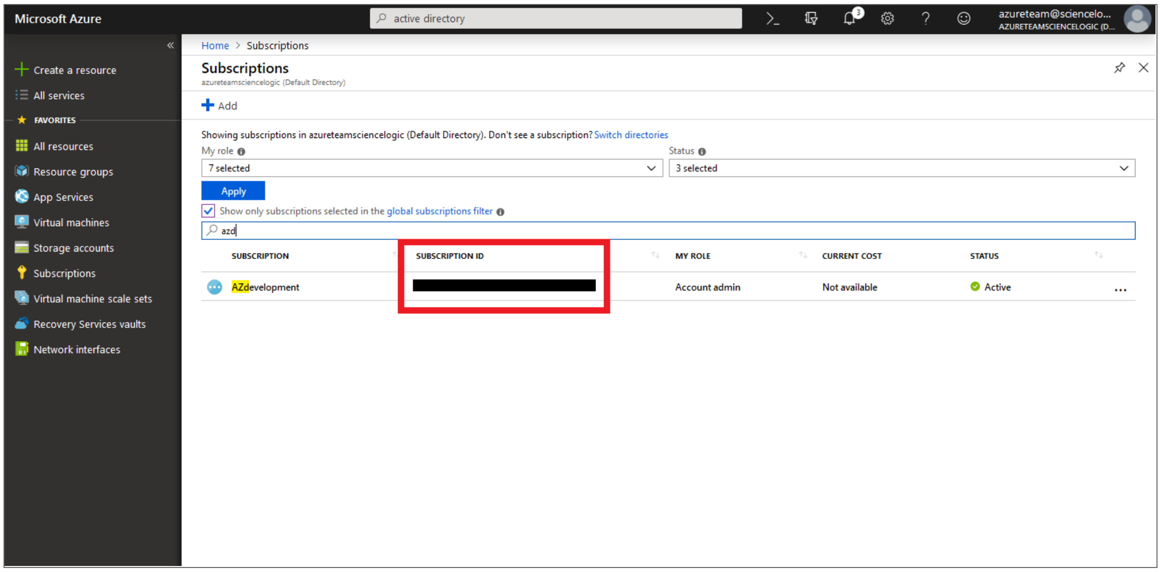
Locating the Subscription ID

If you are monitoring only a single Azure subscription, you must provide the Subscription ID of the Azure Active Directory application you will use to authenticate your account when you configure your SOAP/XML credential for Azure in SL1.

NOTE: If you are monitoring an account with multiple child subscriptions, you can skip this section.

To locate the Subscription ID:

1. In the left pane of the Azure portal (https://portal.azure.com), click **[Subscriptions]**.
2. Copy and save the ***Subscription ID*** of the subscription where you created the Azure Active Directory application you will use to authenticate your account.



Subscriptions
azureteamsciencelogic (Default Directory)

Showing subscriptions in azureteamsciencelogic (Default Directory). Don't see a subscription? Switch directories

My role: 7 selected

Status: 3 selected

☑ Show only subscriptions selected in the global subscriptions filter

azd

SUBSCRIPTION	SUBSCRIPTION ID	MY ROLE	CURRENT COST	STATUS
AZdevelopment	[redacted]	Account admin	Not available	Active

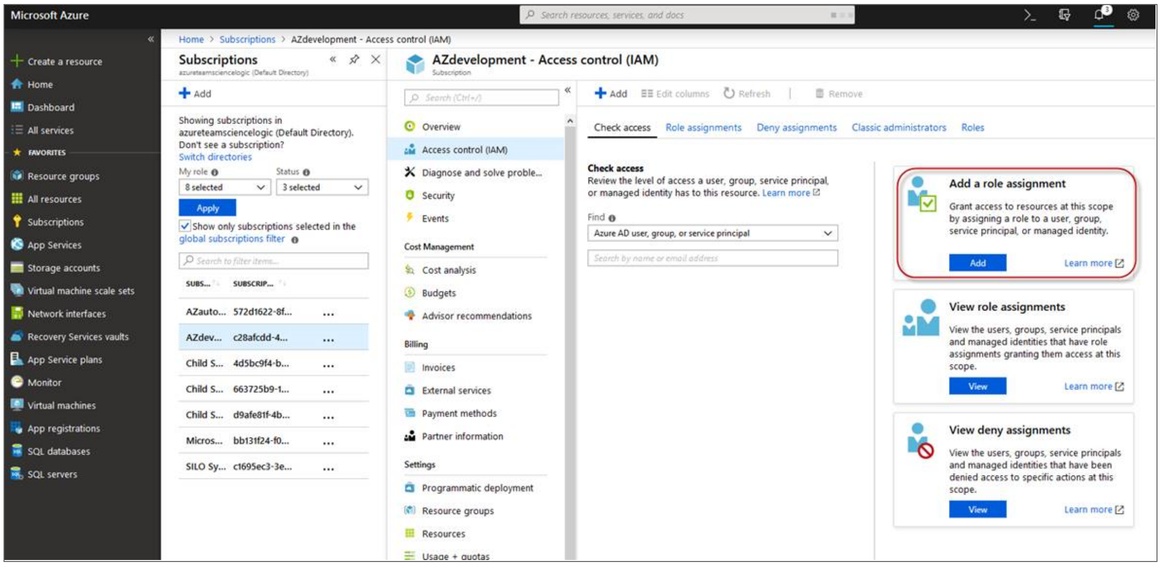
Adding Reader Access to the Active Directory Application

To allow ScienceLogic to access your Azure account, you must specify the type of access the user whose information you will use in your SOAP/XML credential has to the Active Directory application used to authenticate your account. Use the ***Reader*** access role, which is a read-only user that can view everything but cannot make changes.

To specify the access role to the Azure Active Directory application:

1. In the left pane of the Azure Portal (https://portal.azure.com), click **[Subscriptions]**.
2. Click the name of your subscription, and then click **[Access control (IAM)]**.

3. In the **Access Control (IAM)** pane, click the **[Add]** button in the **Add a role assignment** section.



Showing subscriptions in azureteamsciencelogic (Default Directory). Don't see a subscription? Switch directories

☑ Show only subscriptions selected in the global subscriptions filter

Check access

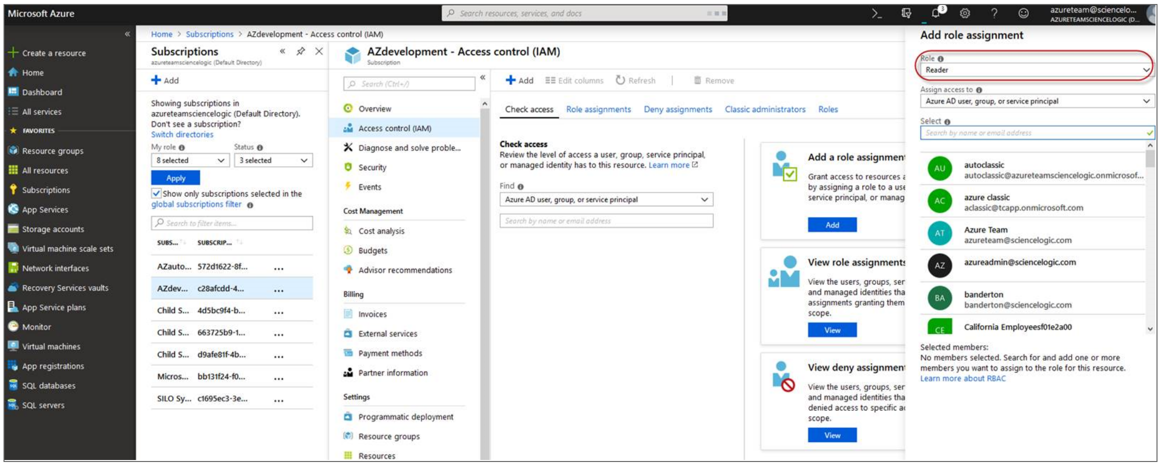
Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Add a role assignment: Grant access to resources at this scope by assigning a role to a user, group, service principal, or managed identity.

View role assignments: View the users, groups, service principals and managed identities that have role assignments granting them access at this scope.

View deny assignments: View the users, groups, service principals and managed identities that have been denied access to specific actions at this scope.

4. In the **Add a role assignment** pane, select *Reader* in the ***Role*** field.



Role: Reader

Assign access to: Azure AD user, group, or service principal

Select: Search by name or email address

autoclassic — autoclassic@azureteamsciencelogic.onmicrosof...

azure classic — aclassic@tcapp.onmicrosoft.com

Azure Team — azureteam@sciencelogic.com

azureadmin@sciencelogic.com

banderton — banderton@sciencelogic.com

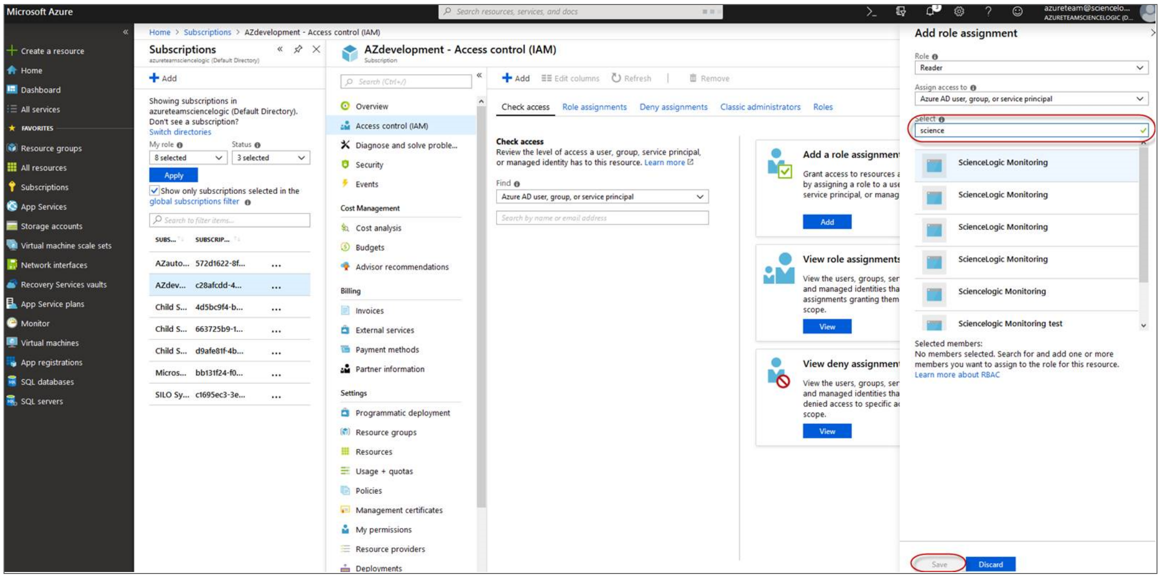
California Employeesf01e2a00

Selected members:

No members selected. Search for and add one or more members you want to assign to the role for this resource.

Learn more about RBAC

5. In the ***Select*** field, type the name of the Azure Active Directory application you will use to authenticate your account.



Showing subscriptions in azureteamsciencelogic (Default Directory). Don't see a subscription? Switch directories

My role: 8 selected

Status: 3 selected

☑ Show only subscriptions selected in the global subscriptions filter

SUBS...	SUBSCRIP...
AZauto...	572d1622-8f...
AZdev...	c28afcdd-4...
Child S...	4d5bc9f4-b...
Child S...	663725b9-1...
Child S...	d9afe81f-4b...
Micros...	bb131f24-f0...
SILO Sy...	c1695ec3-3e...

Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Find: Azure AD user, group, or service principal

Role: Reader

Assign access to: Azure AD user, group, or service principal

Select: science

ScienceLogic Monitoring

ScienceLogic Monitoring

ScienceLogic Monitoring

ScienceLogic Monitoring

Sciencelogic Monitoring

Sciencelogic Monitoring test

Selected members:

No members selected. Search for and add one or more members you want to assign to the role for this resource.

Learn more about RBAC

6. Select the application from the search results and click **[Save]**.

Setting Up a Proxy Server

Depending on your needs, you can optionally enable SL1 to connect to Azure through a third-party proxy server such as SQUID. With this configuration, SL1 connects to the proxy server, which then connects to Azure. Azure relays information to the proxy server and SL1 then retrieves that information from the proxy.

NOTE: You can connect to Azure via a proxy server regardless of whether you are monitoring a single subscription or an account with multiple child subscriptions. You can connect to Microsoft Azure, Microsoft Azure Government, and Microsoft Azure Germany and China regions via a proxy server.

NOTE: The *Microsoft: Azure* PowerPack is certified to work with SQUID version 3.5.12 proxy servers.

If you choose to use a proxy server, configure the third-party proxy server based on the third-party documentation. Depending on the type of authentication you require, you might need to specify a user name and password for the proxy server configuration. Also, make a note of the port you opened for the configuration, as this information is needed when creating the SOAP/XML credential.

Creating a SOAP/XML Credential for Azure

After you note the application ID, subscription ID, tenant ID, and secret key of the application (that is registered with Azure Active Directory) that you will use to authenticate your Azure account, you can create a SOAP/XML credential for Azure in SL1. This credential allows the Dynamic Applications in the *Microsoft: Azure* PowerPack to communicate with your Azure subscriptions.

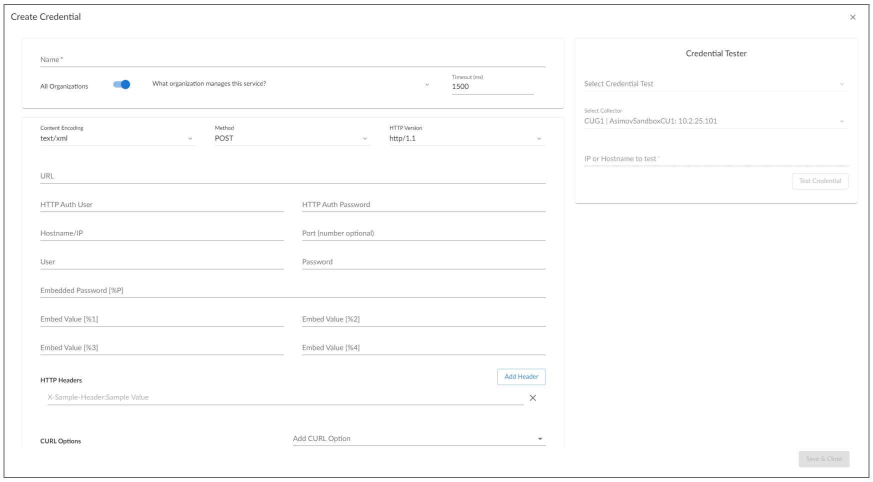
If you want to connect to your Azure account through a third-party proxy server, you must also add the proxy information in the credential. This applies to Microsoft Azure, Microsoft Azure Government, and the Microsoft Azure German and Chinese regions.

The *Microsoft: Azure* PowerPack includes multiple sample credentials you can use as templates for creating SOAP/XML credentials for Azure. They are:

- **Azure Credential - China**, for users who connect to an Azure data center in a Chinese region
- **Azure Credential - Germany**, for users who connect to an Azure data center in a German region (requires a subscription in Germany or Europe)
- **Azure Credential Gov Example**, for users who subscribe to Microsoft Azure Government
- **Azure Credential Proxy Example**, for users who connect to Azure through a third-party proxy server
- **Azure Credential Example**, for all other users.

To create a SOAP/XML credential for Azure:

1. Go to the **Credentials** page (Manage > Credentials).
2. Locate the sample credential you want to use and then click its **[Actions]** icon (⋯) and select ***Edit***. The **Edit Credential** modal page appears.



Create Credential

Timeout (ms): 1500

Content Encoding: text/xml

Method: POST

HTTP Version: http/1.1

Select Collector: CUG1 | AsimovSandboxCU1: 10.2.25.101

HTTP Headers: X-Sample-Header:Sample Value

3. Supply values in the following fields:

   - ***Name***. Type a new name for the Azure credential.
   - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***What organization manages this service?*** drop-down field to align the credential with those specific organizations.
   - ***Timeout (ms)***. Type "120".
   - ***Content Encoding***. Select *text/xml*.
   - ***Method***. Select *POST*.

- ***HTTP Version***. Select *HTTP/1.1*.
- ***URL***. Type the tenant ID in the appropriate place in the URL provided in the sample credential.
- ***HTTP Auth User***. Leave this field blank.
- ***HTTP Auth Password***. Leave this field blank.

Proxy Settings

- ***Hostname/IP***. If you are connecting to Azure via a proxy server, type the server's hostname or IP address. Otherwise, leave this field blank.
- ***Port***. If you are connecting to Azure via a proxy server, type the port number you opened when *setting up the proxy server*. Otherwise, leave this field blank.
- ***User***. If you are connecting to Azure via a proxy server using basic authentication, type the server's administrator username. Otherwise, leave this field blank.
- ***Password***. If you are connecting to Azure via a proxy server using basic authentication, type the server's administrator password. Otherwise, leave this field blank.

SOAP Options

- ***Embedded Password [%P]***. Type the secret key for the Azure Active Directory application.
- ***Embed Value [%1]***. Type the Application ID for the Azure Active Directory application.
- ***Embed Value [%2]***. Type the Tenant ID for the Azure Active Directory application.
- ***Embed Value [%3]***. If you are monitoring only a single Azure subscription, type the Subscription ID for the Azure Active Directory application. If you are monitoring multiple subscriptions, leave this field blank.
- ***Embed Value [%4]***. Leave this field blank. Optionally, you can use this field to add the secret key for the Azure Active Directory application.

HTTP Headers

- ***HTTP Headers***. Leave this field blank, unless one of the following scenarios applies to you:
  - If you are using Microsoft Azure Government, this field contains the text "AZGOV".
  - If you are monitoring Microsoft Azure resources in Germany, this field contains the text "AZGER".
  - If you are monitoring Microsoft Azure resources in China, this field contains the text "AZCHINA".
  - If you would like to enable extended logging, enter "LOGGING" in to a header field. The log file is located at `/tmp/azure.log`
  - SSL certification verification is enabled by default, but you can disable it in a header field by entering "VERIFY:FALSE".

cURL Options

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

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

> **NOTE:** If you would like to test your credential using the Credential Tester panel, click **[Save & Test]**. For detailed instructions on using the Credential Tester panel, see the *Using the Credential Tester Panel* section.

Load-Balancing an Account with Multiple Subscriptions

When monitoring an account with multiple child subscriptions, instead of discovering all child subscriptions in a single dynamic component map under their parent account, you can load-balance subscriptions and their components across multiple Data Collectors.

To do this:

- The Collector Group that discovers a group of subscriptions can contain only one Data Collector. You cannot use multiple Data Collectors to discover the Azure components in a single dynamic component map or discover the same device in multiple dynamic component maps.
- To group multiple Azure subscriptions into a single dynamic component map, you need to create a shared credential for that group of subscriptions.
- To create the credential:
    - Perform all of the steps in the section on *Configuring an Azure Active Directory Application*.
    - Align each subscription in the group with the same application that you registered with Azure AD.
    - In the credential, enter the application ID in the ***Embed Value [%1]*** field.
    - In the credential, leave the ***Embed Value [%3]*** field blank.
- During discovery, use this credential to discover the group of subscriptions.
- During discovery, specify the Data Collector you want to use for the group of subscriptions.
- The discovered subscriptions will reside in a common dynamic component map.
- Repeat these steps for each group of subscriptions.

Creating an Azure Credential

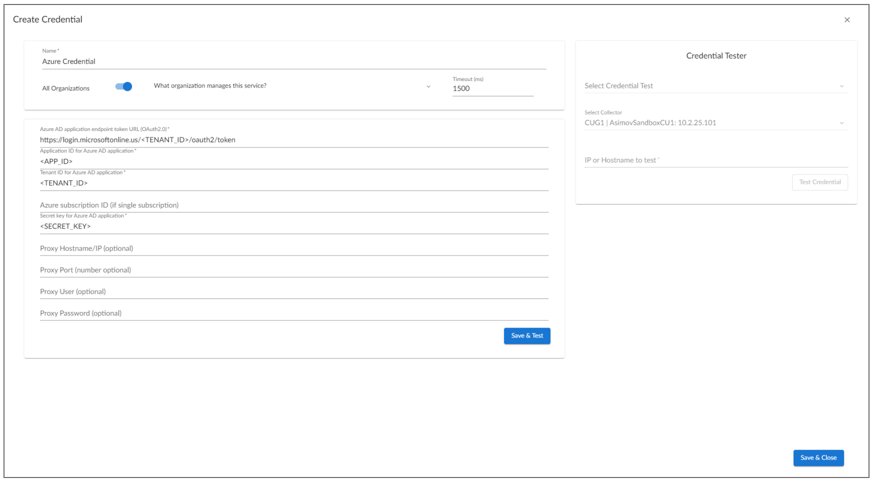
To configure SL1 to monitor Microsoft Azure, you must first create an Azure credential. This credential allows the Dynamic Applications in the *Microsoft: Azure*PowerPack to connect with the Azure Active Directory Application.

SL1 includes an Azure credential type that you can use to connect with the Azure service during guided discovery. This credential type uses field names and terminology that are specific to the Azure service.

> **NOTE:** Alternatively, you could monitor Azure using a generic SOAP/XML credential that does not include Azure-specific fields. For more information, see the ***Monitoring Microsoft Azure*** manual.

To define an Azure-specific credential:

1. Go to the **Credentials** page (System > Manage > Credentials).
2. Click the **[Create New]** button and then select *Create Azure Credential*. The **Create Credential** modal page appears:



Create Credential

Name*
Azure Credential

All Organizations

Timeout (ms)
1500

Azure AD application endpoint token URL (OAuth2.0)*
https://login.microsoftonline.us/<TENANT_ID>/oauth2/token

Application ID for Azure AD application*
<APP_ID>

Tenant ID for Azure AD application*
<TENANT_ID>

Secret key for Azure AD application*
<SECRET_KEY>

Select Collector
CUG1 | AsimovSandboxCU1: 10.2.25.101

×
What organization manages this service?
Azure subscription ID (if single subscription)
Proxy Hostname/IP (optional)
Proxy Port (number optional)
Proxy User (optional)
Proxy Password (optional)
Save & Test
Credential Tester
Select Credential Test
IP or Hostname to test*
Test Credential
Save & Close

3. Supply values in the following fields:

   - ***Name***. Name of the credential. Can be any combination of alphanumeric characters.
   - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***What organization manages this service?*** drop-down field to align the credential with those specific organizations.
   - ***Timeout (ms)***. Time, in milliseconds, after which SL1 will stop trying to communicate with the device from which you want to retrieve data.
   - ***Azure AD application endpoint token URL (OAuth2.0)***. The AD application endpoint token URL for the Azure Active Directory application.
   - ***Application ID for Azure AD application***. The Application ID for the Azure Active Directory application.
   - ***Tenant ID for Azure AD application***. The Tenant ID for the Azure Active Directory application.
   - ***Azure subscription ID (if single subscription)***. The subscription ID for the Azure Active Directory application. This field is required only if you are monitoring a single Azure subscription.
   - ***Secret key for Azure AD application***. The secret key for the Azure Active Directory application.

   ## Proxy Settings

   If you use a proxy server in front of the Azure Active Directory applications you want to communicate with, enter values in these fields. Otherwise, you can skip these fields.

   - ***Proxy Hostname/IP***. The host name or IP address of the proxy server.
   - ***Proxy Port***. Port on the proxy server to which you will connect.

- ***Proxy User***. Username to use to access the proxy server.
- ***Proxy Password***. Password to use to access the proxy server.

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

> **NOTE:** If you would like to test your credential using the Credential Tester panel, click **[Save & Test]**. For detailed instructions on using the Credential Tester panel, see the ***Testing the Azure Credential*** section.

Testing the Azure Credential Using the Credential Tester Panel

The *Microsoft: Azure* PowerPack includes a Credential Test for Microsoft Azure. Credential Tests define a series of steps that SL1 can execute on demand to validate whether a credential works as expected.

To test the Azure credential using the Credential Tester panel:

1. After ***defining an Azure credential***, click the **[Save & Test]** button. This activates the Credential Tester fields.
2. In the Credential Tester panel, supply values in the following fields:

    - ***Select Credential Test***. Select a credential test to run. This drop-down list includes the ***ScienceLogic Default Credential Tests***, credential tests included in any PowerPacks that have been optionally installed on your system, and credential tests that users have created on your system.
    - ***Select Collector***. Select the All-In-One Appliance or Data Collector that will run the test.
    - ***IP or Hostname to test***. Type a hostname or IP address that will be used during the test. For example, if you are testing an SNMP credential, the hostname/IP address you supply will be used to perform a test SNMP request.

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

    The **Testing 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 execution of the credential test.
    - ***Status***. Whether the result of this step indicates the credential and/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 and/or the network environment if the step has a status of "Failed".

Creating a SOAP/XML Credential for Azure

After you note the application ID, subscription ID, tenant ID, and secret key of the application (that is registered with Azure Active Directory) that you will use to authenticate your Azure account, you can create a SOAP/XML credential for Azure in SL1. This credential allows the Dynamic Applications in the *Microsoft: Azure* PowerPack to communicate with your Azure subscriptions.

If you want to connect to your Azure account through a third-party proxy server, you must also add the proxy information in the credential. This applies to Microsoft Azure, Microsoft Azure Government, and the Microsoft Azure German and Chinese regions.

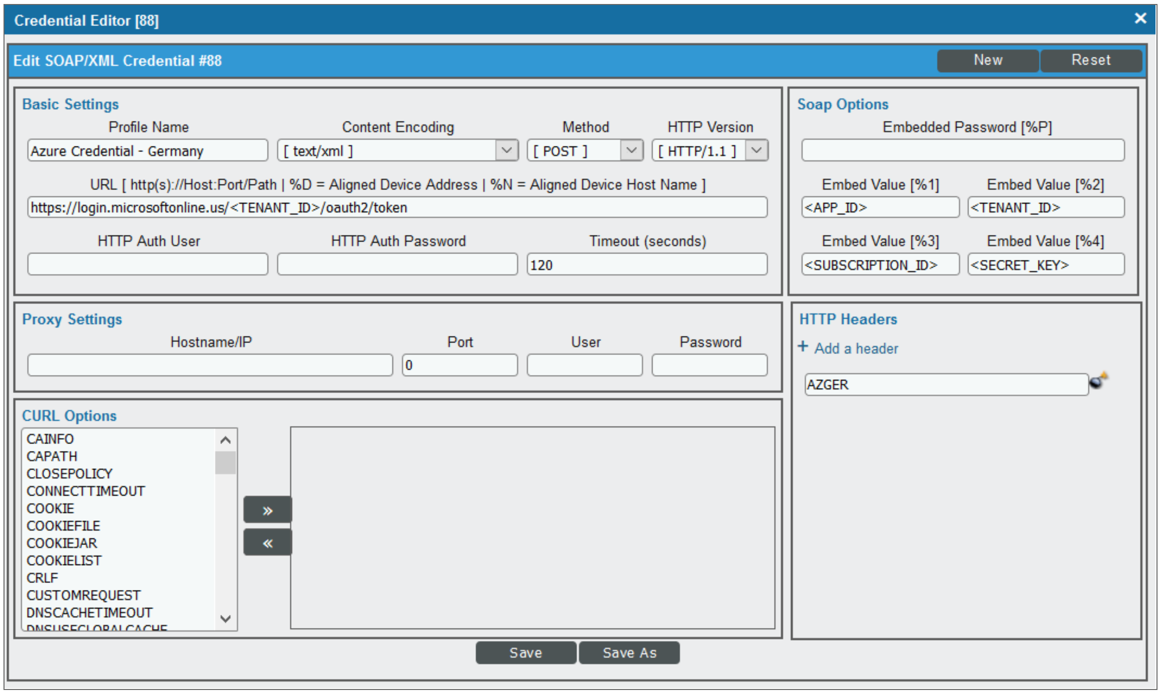
The *Microsoft: Azure* PowerPack includes multiple sample credentials you can use as templates for creating SOAP/XML credentials for Azure. They are:

- **Azure Credential - China**, for users who connect to an Azure data center in a Chinese region
- **Azure Credential - Germany**, for users who connect to an Azure data center in a German region (requires a subscription in Germany or Europe)
- **Azure Credential Gov Example**, for users who subscribe to Microsoft Azure Government
- **Azure Credential Proxy Example**, for users who connect to Azure through a third-party proxy server
- **Azure Credential Example**, for all other users.

To create a SOAP/XML credential for Azure:

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

2. Locate the sample credential you want to use and then click its wrench icon ( ). The **Edit SOAP/XML Credential** modal page appears:



Credential Editor [88]

Edit SOAP/XML Credential #88

Basic Settings

Profile Name: Azure Credential - Germany

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://login.microsoftonline.us/<TENANT_ID>/oauth2/token

HTTP Auth User:

HTTP Auth Password:

Timeout (seconds): 120

Soap Options

Embedded Password [%P]:

Embed Value [%1]: <APP_ID>

Embed Value [%2]: <TENANT_ID>

Embed Value [%3]: <SUBSCRIPTION_ID>

Embed Value [%4]: <SECRET_KEY>

Proxy Settings

Hostname/IP:

Port: 0

User:

Password:

HTTP Headers

+ Add a header

AZGER

CURL Options

CAINFO
CAPATH
CLOSEPOLICY
CONNECTTIMEOUT
COOKIE
COOKIEFILE
COOKIEJAR
COOKIELIST
CRLF
CUSTOMREQUEST
DNSCACHETIMEOUT
DNSUSEGLOBALCACHE

3. Enter values in the following fields:

Basic Settings

- ***Profile Name***. Type a new name for the Azure credential.
- ***Content Encoding***. Select *text/xml*.
- ***Method***. Select *POST*.
- ***HTTP Version***. Select *HTTP/1.1*.
- ***URL***. Type the tenant ID in the appropriate place in the URL provided in the sample credential.
- ***HTTP Auth User***. Leave this field blank.
- ***HTTP Auth Password***. Leave this field blank.
- ***Timeout (seconds)***. Type "120".

Proxy Settings

- ***Hostname/IP***. If you are connecting to Azure via a proxy server, type the server's hostname or IP address. Otherwise, leave this field blank.
- ***Port***. If you are connecting to Azure via a proxy server, type the port number you opened when *setting up the proxy server*. Otherwise, leave this field blank.

- ***User***. If you are connecting to Azure via a proxy server using basic authentication, type the server's administrator username. Otherwise, leave this field blank.
- ***Password***. If you are connecting to Azure via a proxy server using basic authentication, type the server's administrator password. Otherwise, leave this field blank.

CURL Options

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

SOAP Options

- ***Embedded Password [%P]***. Type the secret key for the Azure Active Directory application.
- ***Embed Value [%1]***. Type the Application ID for the Azure Active Directory application.
- ***Embed Value [%2]***. Type the Tenant ID for the Azure Active Directory application.
- ***Embed Value [%3]***. If you are monitoring only a single Azure subscription, type the Subscription ID for the Azure Active Directory application. If you are monitoring multiple subscriptions, leave this field blank.
- ***Embed Value [%4]***. Leave this field blank. Optionally, you can use this field to add the secret key for the Azure Active Directory application.

HTTP Headers

- ***HTTP Headers***. Leave this field blank, unless one of the following scenarios applies to you:
  - If you are using Microsoft Azure Government, this field contains the text "AZGOV".
  - If you are monitoring Microsoft Azure resources in Germany, this field contains the text "AZGER".
  - If you are monitoring Microsoft Azure resources in China, this field contains the text "AZCHINA".
  - If you would like to enable extended logging, enter "LOGGING" in to a header field. The log file is located at `/tmp/azure.log`
  - SSL certification verification is enabled by default, but you can disable it in a header field by entering "VERIFY:FALSE".

4. Click **[Save As]**.
5. In the confirmation message, click **[OK]**.

Load-Balancing an Account with Multiple Subscriptions

When monitoring an account with multiple child subscriptions, instead of discovering all child subscriptions in a single dynamic component map under their parent account, you can load-balance subscriptions and their components across multiple Data Collectors.

To do this:

- The Collector Group that discovers a group of subscriptions can contain only one Data Collector. You cannot use multiple Data Collectors to discover the Azure components in a single dynamic component map or discover the same device in multiple dynamic component maps.

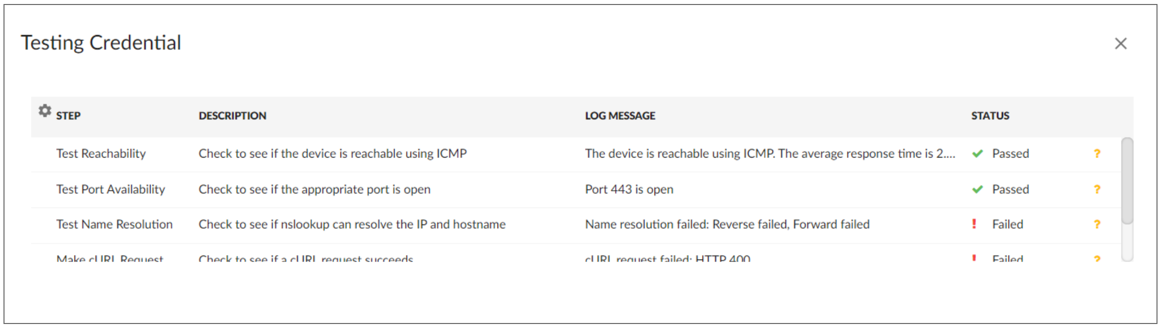
- To group multiple Azure subscriptions into a single dynamic component map, you need to create a shared credential for that group of subscriptions.
- To create the credential:
  - Perform all of the steps in the section on ***Configuring an Azure Active Directory Application***.
  - Align each subscription in the group with the same application that you registered with Azure AD.
  - In the credential, enter the application ID in the ***Embed Value [%1]*** field.
  - In the credential, leave the ***Embed Value [%3]*** field blank.
- During discovery, use this credential to discover the group of subscriptions.
- During discovery, specify the Data Collector you want to use for the group of subscriptions.
- The discovered subscriptions will reside in a common dynamic component map.
- Repeat these steps for each group of subscriptions.

Testing the Azure Credential

You can test a credential from the **Credentials** page using a predefined credential test.

To run a credential test from the **Credentials** page:

1. Go to the **Credentials** page (Manage > Credentials).
2. Click the **Actions** button (⋯) of the credential that you want to test, and then select *Test*.
3. The **Credential Test Form** modal page appears. Fill out the following fields on this page:
   - ***Credential***. Select the credential to test. This drop-down list includes only credentials that you have access to. (If you clicked the **Actions** button (⋯) and then selected *Test* for a specific credential, then this field is read-only.)
   - ***Select Credential Test***. Select a credential test to run. This drop-down list includes the ***ScienceLogic Default Credential Tests***, credential tests included in any PowerPacks that have been optionally installed on your system, and credential tests that users have created on your system.
   - ***Collector***. Select the All-In-One Appliance or Data Collector that will run the test.
   - ***IP or Hostname to Test***. Type a hostname or IP address that will be used during the test. For example, if you are testing an SNMP credential, the hostname/IP address you supply will be used to perform a test SNMP request.
4. Click **[Run Test]** button to run the credential test. The **Testing Credential** window appears:



Testing Credential

STEP	DESCRIPTION	LOG MESSAGE	STATUS	
Test Reachability	Check to see if the device is reachable using ICMP	The device is reachable using ICMP. The average response time is 2....	✓ Passed	?
Test Port Availability	Check to see if the appropriate port is open	Port 443 is open	✓ Passed	?
Test Name Resolution	Check to see if nslookup can resolve the IP and hostname	Name resolution failed: Reverse failed, Forward failed	! Failed	?
Make cURL Request	Check to see if a cURL request succeeds	cURL request failed: HTTP 400	! Failed	?

The **Testing 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 execution of the credential test.
- ***Status***. Whether the result of this step indicates the credential and/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 and/or the network environment if the step has a status of "Failed".

Testing the Azure Credential in the SL1 Classic User Interface

The *Microsoft: Azure* PowerPack includes a Credential Test for Microsoft Azure. Credential Tests define a series of steps that SL1 can execute on demand to validate whether a credential works as expected.

The "Azure Credential Test - ARM" can be used to test a SOAP/XML credential for monitoring Azure using the Dynamic Applications in the *Microsoft: Azure* PowerPack.

CAUTION: When testing Azure credentials for version 110 or greater of the *Microsoft: Azure* PowerPack, you should use the "Azure Credential Test - ARM" that is included in the PowerPack rather than the "Azure Credential Test" that is included by default in SL1. The "Azure Credential Test - ARM" supports proxy server entries in the credential being tested and can test that your Azure credential has the latest required permissions in Azure, whereas the older "Azure Credential Test" cannot do these things.

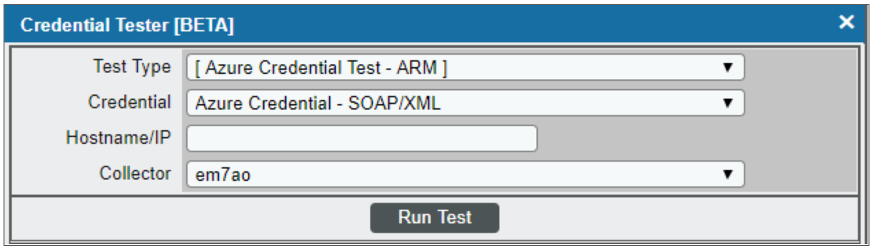
The "Azure Credential Test - ARM" performs the following steps:

- ***Test Port Availability***. Performs an NMAP request to test the availability of the Azure endpoint HTTPS port.
- ***Test Name Resolution***. Performs an nslookup request on the Azure endpoint.
- ***Make connection to Azure account***. Attempts to connect to the Azure service using the account specified in the credential.

- ***Validate Azure Microsoft Graph Permission***. Verifies that the Azure Active Directory application has Microsoft Graph API permissions.
- ***Validate Azure subscription assignments***. Verifies that the Azure Active Directory application is assigned to the subscription.

To test the Azure credential:

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



Credential Tester [BETA]

Test Type: [Azure Credential Test - ARM]

Credential: Azure Credential - SOAP/XML

Hostname/IP:

Collector: em7ao

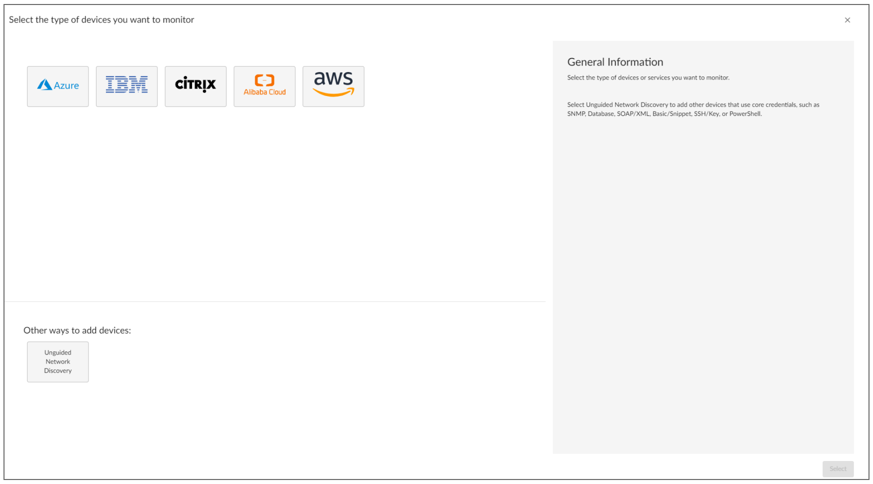
3. Supply values in the following fields:
   - ***Test Type***. This field is pre-populated with the credential test you selected.
   - ***Credential***. Select the credential to test. This drop-down list includes only credentials that you have access to that can be tested using the selected credential test.
   - ***Hostname/IP***. Leave this field blank.
   - ***Collector***. Select the All-In-One Appliance or Data Collector that will run the test.
4. Click the **[Run Test]** button. The **Test Credential** window appears, displaying 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".

Microsoft Azure Guided Discovery

You can use the Universal Discovery Framework process in SL1 that guides you through a variety of existing discovery types in addition to traditional SNMP discovery. This process, which is also called "guided discovery", lets you pick a discovery type based on the type of devices you want to monitor. The Universal Discovery workflow includes a button for Microsoft Azure.

To run a guided or Universal Discovery:

1. On the **Devices** page (🖥) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears.



Select the type of devices you want to monitor

General Information

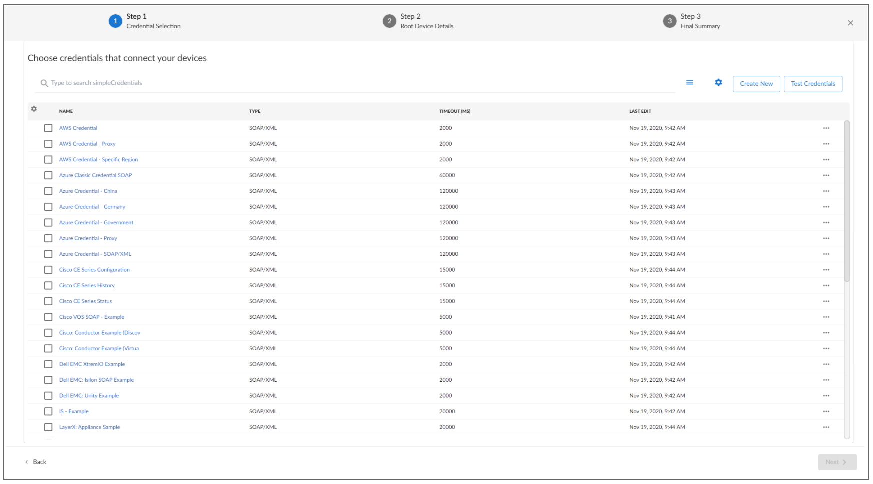
Select the type of devices or services you want to monitor.

Select Unguided Network Discovery to add other devices that use core credentials, such as SNMP, Database, SOAP/XML, Basic/Snippet, SSH/Key, or PowerShell.

Other ways to add devices:

2. Select the **Microsoft Azure** button. Additional information about the requirements for device discovery appears in the **General Information** pane to the right.

3. Click **[Select]**. The **Credential Selection** page appears.



Step 1 Credential Selection

Step 2 Root Device Details

Step 3 Final Summary

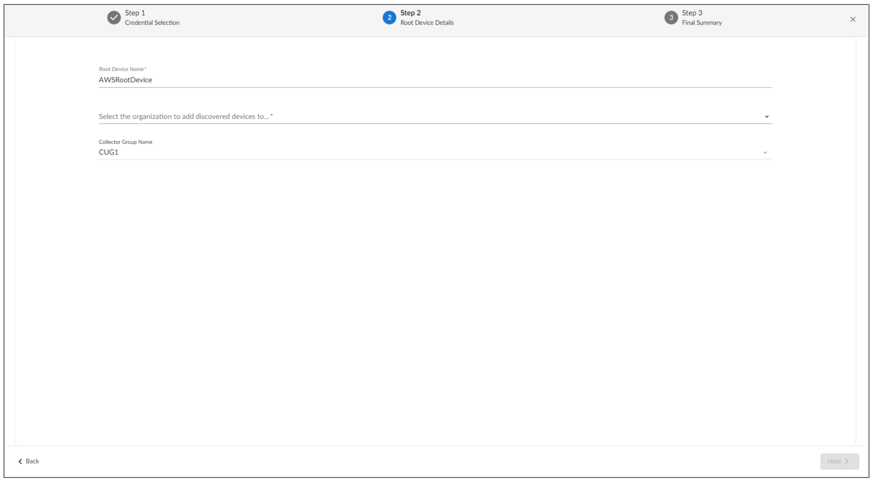
Choose credentials that connect your devices

Type to search simpleCredentials

	NAME	TYPE	TIMEOUT (MS)	LAST EDIT	
□	AWS Credential	SOAP/XML	2000	Nov 19, 2020, 9:42 AM	•••
□	AWS Credential - Proxy	SOAP/XML	2000	Nov 19, 2020, 9:42 AM	•••
□	AWS Credential - Specific Region	SOAP/XML	2000	Nov 19, 2020, 9:42 AM	•••
□	Azure Classic Credential SOAP	SOAP/XML	60000	Nov 19, 2020, 9:42 AM	•••
□	Azure Credential - China	SOAP/XML	120000	Nov 19, 2020, 9:43 AM	•••
□	Azure Credential - Germany	SOAP/XML	120000	Nov 19, 2020, 9:43 AM	•••
□	Azure Credential - Government	SOAP/XML	120000	Nov 19, 2020, 9:43 AM	•••
□	Azure Credential - Proxy	SOAP/XML	120000	Nov 19, 2020, 9:43 AM	•••
□	Azure Credential - SOAP/XML	SOAP/XML	120000	Nov 19, 2020, 9:43 AM	•••
□	Cisco CE Series Configuration	SOAP/XML	15000	Nov 19, 2020, 9:44 AM	•••
□	Cisco CE Series History	SOAP/XML	15000	Nov 19, 2020, 9:44 AM	•••
□	Cisco CE Series Status	SOAP/XML	15000	Nov 19, 2020, 9:44 AM	•••
□	Cisco VOS SOAP - Example	SOAP/XML	5000	Nov 19, 2020, 9:41 AM	•••
□	Cisco: Conductor Example (Discov	SOAP/XML	5000	Nov 19, 2020, 9:44 AM	•••
□	Cisco: Conductor Example (Virtua	SOAP/XML	5000	Nov 19, 2020, 9:44 AM	•••
□	Dell EMC XtremIO Example	SOAP/XML	2000	Nov 19, 2020, 9:42 AM	•••
□	Dell EMC: Isilon SOAP Example	SOAP/XML	2000	Nov 19, 2020, 9:42 AM	•••
□	Dell EMC: Unity Example	SOAP/XML	2000	Nov 19, 2020, 9:42 AM	•••
□	IS - Example	SOAP/XML	20000	Nov 19, 2020, 9:42 AM	•••
□	LayerX: Appliance Sample	SOAP/XML	20000	Nov 19, 2020, 9:44 AM	•••

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

4. On the **Credential Selection** page of the guided discovery process, select the Azure credential that you configured, and then click **[Next]**. The **Root Device Details** page appears.



Root Device Name*
AWSRootDevice

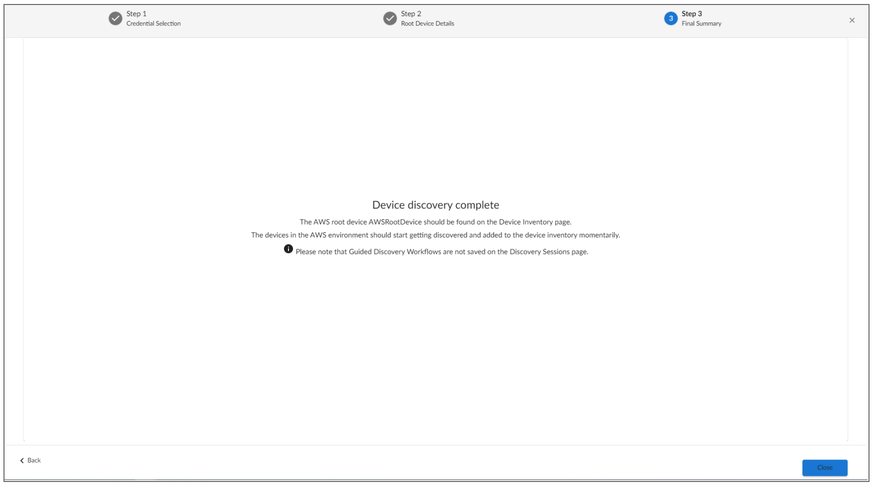
Select the organization to add discovered devices to...*

Collector Group Name
CUG1

5. Complete the following fields:

   - ***Root Device Name***. Type the name of the root device for the Microsoft Azure root device you want to monitor.
   - ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered device.
   - ***Collector Group Name***. Select an existing collector group to communicate with the discovered device. This field is required.

6. Click **[Next]**. SL1 creates the Microsoft Azure root device with the appropriate Device Class assigned to it and aligns the relevant Dynamic Applications. The **Final Summary** page appears.



Device discovery complete

The AWS root device AWSRootDevice should be found on the Device Inventory page.

The devices in the AWS environment should start getting discovered and added to the device inventory momentarily.

Please note that Guided Discovery Workflows are not saved on the Discovery Sessions page.

8. Click **[Close]**.

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

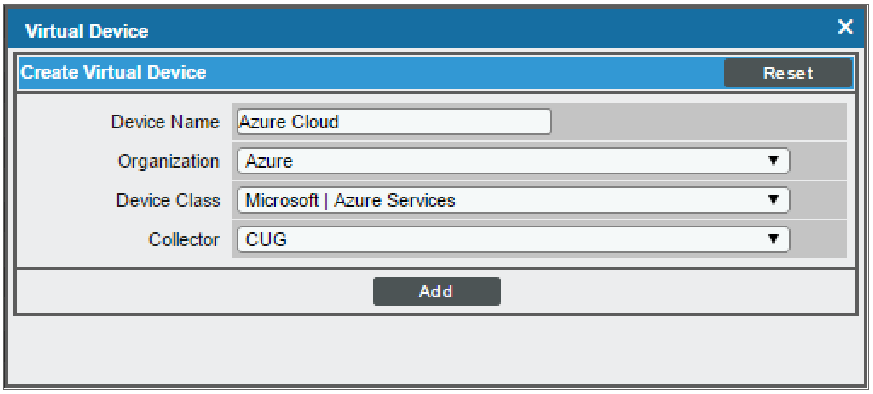
Creating an Azure Virtual Device for Discovery in the SL1 Classic User Interface

Because the Azure service does not have a static IP address, you cannot discover an Azure device using discovery. Instead, you must create a ***virtual device*** that represents the Azure service. A virtual device is a user-defined container that represents a device or service that cannot be discovered by SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications.

To create a virtual device that represents your Azure service:

1. Go to the **Device Manager** page (Devices > Device Manager, or Registry > Devices > Device Manager in the classic SL1 user interface).
2. Click the **[Actions]** button and select *Create Virtual Device* from the menu. The **Virtual Device** modal page appears.

3. Enter values in the following fields:



Device Name	Azure Cloud
Organization	Azure
Device Class	Microsoft | Azure Services
Collector	CUG

- ***Device Name***. Enter a name for the device. For example, "Azure Cloud".
- ***Organization***. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.
- ***Device Class***. Select *Microsoft | Azure Services*.
- ***Collector***. Select the collector group that will monitor the device.

TIP: When monitoring an account with multiple child subscriptions, you can load-balance how SL1 monitors your Azure components by discovering groups of subscriptions and their components across multiple collectors. For details, see the section on ***Load-Balancing an Account with Multiple Subscriptions***.

4. Click **[Add]** to create the virtual device.

Aligning the Azure Dynamic Applications

The Dynamic Applications in the *Microsoft: Azure* PowerPack are divided into the following types:

- ***Discovery***. These Dynamic Applications poll Azure for new instances of services or changes to existing instances of services.
- ***Configuration***. These Dynamic Applications retrieve configuration information about each service instance and retrieve any changes to that configuration information.
- ***Performance***. These Dynamic Applications poll Azure for performance metrics.

When configuring SL1 to monitor Azure services, you can manually align Dynamic Applications to discover Azure component devices.

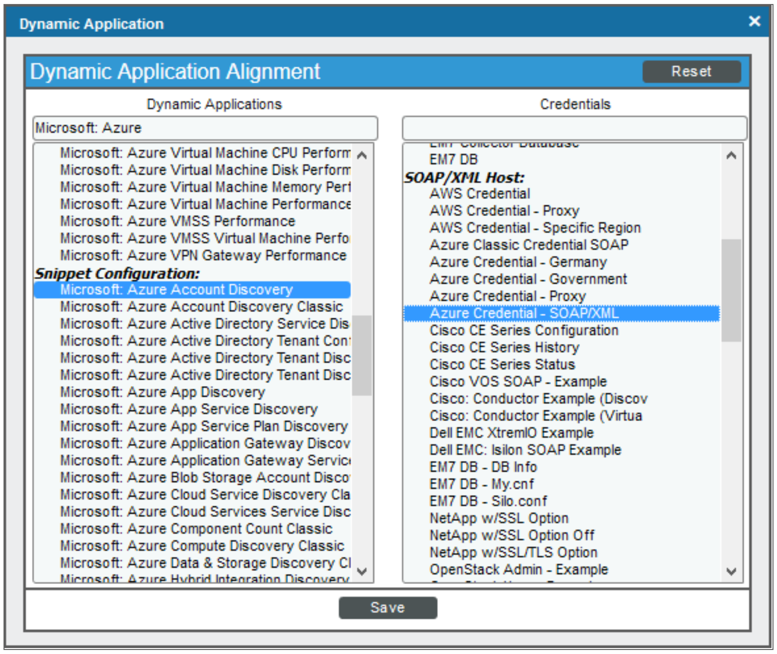
Discovering Azure Component Devices

To discover all the components of your Azure platform, you must manually align the "Microsoft: Azure Account Discovery" Dynamic Application with the Azure virtual device.

TIP: When monitoring an account with multiple child subscriptions, ScienceLogic recommends that you first review your device capacity and load limits to determine the best method for implementation prior to discovery. For details, see the section on ***Load-Balancing an Account with Multiple Subscriptions***.

To manually align the "Microsoft: Azure Account Discovery" Dynamic Application:

1. Go to the **Device Manager** page (Devices > Device Manager, or Registry > Devices > Device Manager in the classic SL1 user interface).
2. Click the wrench icon (🔧) for your Azure virtual device.
3. In the ***Device Administration*** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
4. Click the **[Actions]** button and select *Add Dynamic Application* from the menu.
5. In the **Dynamic Application Alignment** modal:


Dynamic Application
×
Dynamic Application Alignment
Reset
Dynamic Applications
Credentials
Microsoft: Azure
Microsoft: Azure Virtual Machine CPU Perform
Microsoft: Azure Virtual Machine Disk Perform
Microsoft: Azure Virtual Machine Memory Perf
Microsoft: Azure Virtual Machine Performance
Microsoft: Azure VMSS Performance
Microsoft: Azure VMSS Virtual Machine Perfo
Microsoft: Azure VPN Gateway Performance
Snippet Configuration:
Microsoft: Azure Account Discovery
Microsoft: Azure Account Discovery Classic
Microsoft: Azure Active Directory Service Dis
Microsoft: Azure Active Directory Tenant Con
Microsoft: Azure Active Directory Tenant Disc
Microsoft: Azure Active Directory Tenant Disc
Microsoft: Azure App Discovery
Microsoft: Azure App Service Discovery
Microsoft: Azure App Service Plan Discovery
Microsoft: Azure Application Gateway Discov
Microsoft: Azure Application Gateway Servic
Microsoft: Azure Blob Storage Account Disco
Microsoft: Azure Cloud Service Discovery Cla
Microsoft: Azure Cloud Services Service Disc
Microsoft: Azure Component Count Classic
Microsoft: Azure Compute Discovery Classic
Microsoft: Azure Data & Storage Discovery Cl
Microsoft: Azure Hybrid Integration Discovery
EM7 DB
SOAP/XML Host:
AWS Credential
AWS Credential - Proxy
AWS Credential - Specific Region
Azure Classic Credential SOAP
Azure Credential - Germany
Azure Credential - Government
Azure Credential - Proxy
Azure Credential - SOAP/XML
Cisco CE Series Configuration
Cisco CE Series History
Cisco CE Series Status
Cisco VOS SOAP - Example
Cisco: Conductor Example (Discov
Cisco: Conductor Example (Virtua
Dell EMC XtremIO Example
Dell EMC: Isilon SOAP Example
EM7 DB - DB Info
EM7 DB - My.cnf
EM7 DB - Silo.conf
NetApp w/SSL Option
NetApp w/SSL Option Off
NetApp w/SSL/TLS Option
OpenStack Admin - Example
Save

- In the ***Dynamic Applications*** field, select *Microsoft: Azure Account Discovery*.
- In the ***Credentials*** field, select the credential you created for your Azure service.

6. Click **[Save]** to align the Dynamic Application with the Azure virtual device.

When you align the "Microsoft: Azure Account Discovery" Dynamic Application with the Azure virtual device, SL1 does one of the following, depending on your subscription model:

- If you are monitoring an account with multiple child subscriptions, SL1 creates a root component device representing the Azure account and one or more child component devices representing all of your Azure subscriptions.
- If you are monitoring a single subscription, SL1 creates a root component device representing your Azure subscription.

TIP: When monitoring an account with multiple child subscriptions, you can load-balance how SL1 monitors your Azure components by discovering groups of subscriptions and their components across multiple collectors. For details, see the section on ***Load-Balancing an Account with Multiple Subscriptions***.

SL1 then automatically aligns several other Dynamic Applications to the subscription component devices. These additional Dynamic Applications discover and create component devices for Active Directory tenants, Traffic Manager profiles, and each location used by the Azure account.

Under each location, SL1 then discovers the following component devices:

- Application Gateway Services
    - Application Gateways
- App Services
    - App Service Plan
        - Function App
        - Web App

- Azure Cache for Redis
- Azure Database for MySQL Services
    - Azure Database for MySQL Servers
- Azure Database for PostgreSQL Services
    - Azure Database for PostgreSQL Servers
- Azure Functions
- Azure Kubernetes Services (AKS)
    - Azure Kubernetes Clusters
- Azure Service Buses (Relay)
- Batch Accounts
- Content Delivery Networks
    - CDN Profiles
        - CDN Endpoints
- Cosmos DB Accounts
- DNS Services
    - DNS Zones
- ExpressRoute Services
    - ExpressRoute Circuits
        - ExpressRoute Peering
            - ExpressRoute Circuit Connections
- Key Vaults
- Load Balancer Services
    - Load Balancers
- Network Security Group Services
    - Network Security Groups
- Recovery Service Vaults Services
    - Recovery Service Vaults
- Resource Groups Services
    - Resource Groups
- SQL Server Services
    - SQL Servers
    - SQL Databases
- Storage Manage Disks
    - Manage Disk Service
        - Manage Disk

- Storage Services
    - Storage Accounts
- Virtual Machines Services
    - Virtual Machines
- Virtual Network Services
    - Virtual Networks
        - ExpressRoute Gateways
        - Virtual Network Gateways
        - Virtual Network Subnets
- VM Scale Set Services
    - VM Scale Sets
        - Virtual Machines
- Web Application Firewalls (WAF)
    - WAF on CDN Policies
    - WAF on Application Gateway Policies

NOTE: SL1 might take several minutes to align these Dynamic Applications and create the component devices in your Azure service.

NOTE: When discovering a large number of component devices, such as when discovering an account with multiple child subscriptions, the discovery process can cause the appearance of numerous critical events with the message, "`Large backlog of asynchronous jobs detected`". This will occur only during the initial discovery session.

Relationships Between Component Devices

In addition to parent/child relationships between component devices, SL1 also creates relationships between the following component devices:

- Apps and Resource Groups
- Application Gateways and Resource Groups
- Application Gateways and Virtual Network Subnets
- Azure CosmosDB and Resource Groups
- Azure CosmosDB and Virtual Networks
- Azure CosmosDB and Virtual Network Subnets
- Azure Traffic Managers and Traffic Managers
- Batch Accounts and Key Vaults

- Batch Accounts and Resource Groups
- Batch Accounts and Storage Groups
- CDN Profiles and Resource Groups
- Key Vaults and Resource Groups
- Key Vaults and Virtual Networks
- Key Vault Rules and Subnets
- Kubernetes Agent Pools and Subnets
- Load Balancers and Resource Groups
- Managed Disks and Resource Groups
- Managed Disks and Virtual Machines
- Network Security Groups and Resource Groups
- Network Security Groups and Virtual Network Subnets
- PostgreSQL Servers and Resource Groups
- PostgreSQL Servers and Subnets
- PostgreSQL Servers and PostgreSQL Server Replicas
- PostgreSQL Servers and Virtual Networks
- Recovery Service Vaults and Resource Groups
- Redis Cache Servers and Redis Cache Servers
- Redis Caches and Resource Groups
- Redis Caches and Subnets
- Redis Caches and Virtual Networks
- Service Bus Namespaces and Resource Groups
- Service Bus Namespaces and Service Bus Namespaces
- Service Bus Namespaces and Subnets
- Service Bus Namespaces and Virtual Networks
- SQL Databases and Resource Groups
- SQL Servers and Resource Groups
- SQL Servers and Server Replicas
- SQL Servers and Subnets
- SQL Servers and Virtual Networks
- SQL Servers and Virtual Network Subnets
- Storage Accounts and Resource Groups
- Traffic Manager Profiles and Resource Groups
- Virtual Machines and Network Security Groups
- Virtual Machines and Resource Groups

- Virtual Machines and Storage Accounts
- Virtual Machines and Virtual Networks
- Virtual Machines and Virtual Network Subnets
- Virtual Machine Scale Sets and Load Balancers
- Virtual Machine Scale Sets and Resource Groups
- Virtual Machine Scale Sets and Virtual Network Subnets
- Virtual Machine Scale Set Virtual Machines and Resource Groups
- Virtual Networks and Resource Groups
- VPN Gateways and Resource Groups
- VPN Gateways and Virtual Network Subnets
- WAF CDN Policies and Endpoints
- WAF CDN Policies and Resource Groups
- WAF Gateway Policies and Application Gateways
- WAF Gateway Policies and Resource Groups

Additionally, the platform can automatically build relationships between Azure component devices and other associated devices:

- If you discover Cisco Cloud Center devices using the Dynamic Applications in the *Cisco: CloudCenter* PowerPack version 103 or later, SL1 will automatically create relationships between Azure Virtual Machines and Cisco Cloud Center applications.
- If you discover Dynatrace environments using the Dynamic Applications in the *Dynatrace* PowerPack, SL1 will automatically create relationships between the following device types:
    - Azure Virtual Machines and Dynatrace Hosts
    - Azure Virtual Machine Scale Sets and Dynatrace Hosts
- If you discover Office 365 services using the Dynamic Applications in the *Microsoft: Office 365* PowerPack version 101 or later, SL1 will automatically create relationships between Azure Active Directory tenants and Office 365 Active Directory tenants.

Chapter 52

Microsoft: Office 365

Overview

The following sections describe how to configure and discover Microsoft Office 365 services for monitoring by SL1 using the *Microsoft: Office 365* PowerPack:

NOTE: For more information about the *Microsoft: Office 365* PowerPack, see the ***Monitoring Microsoft Office 365*** manual.

Configuring Office 365 Monitoring

To create a SOAP/XML credential that allows SL1 to access Microsoft Office 365, you must provide the following information about an Office 365 application that is already registered with an Active Directory tenant in Microsoft Azure:

- Application ID
- Tenant ID
- Secret Key

To capture the above information, you must first create or use an existing an Office 365 application that is registered with Azure Active Directory. The application must have access permissions for Office 365 Management APIs and Microsoft Graph APIs. You can then enter the required information about the application when configuring the SOAP/XML credential in SL1. The registered application and the ScienceLogic credential allow SL1 to retrieve information from Office 365.

The following sections describe how to create a registered application, add the appropriate API permissions, and capture the application ID, tenant ID, and secret key.

Creating an Office 365 Active Directory Application in the Azure Portal

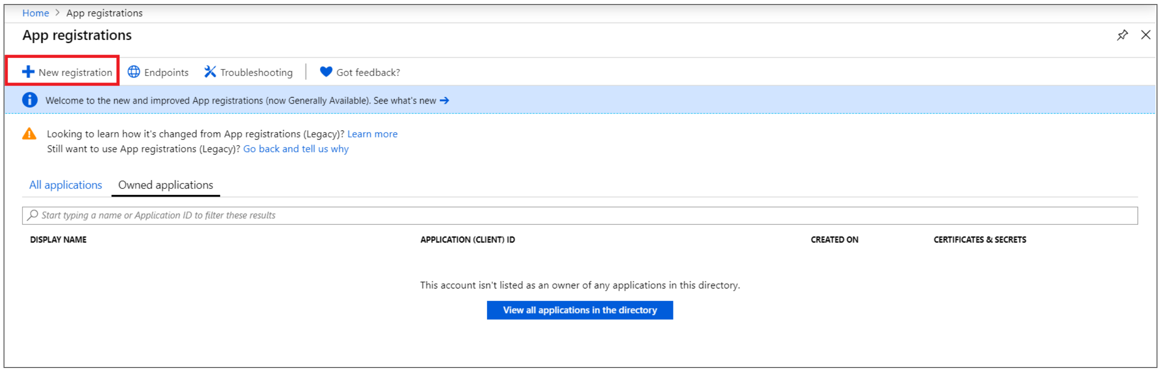
When configuring a SOAP/XML credential in SL1, you must provide the application ID, tenant ID, and secret key of an Office 365 application that is registered with Azure Active Directory. You use this registered application to authenticate your Office 365 account.

NOTE: You must have Service Administrator rights to create an Active Directory application.

To create an Office 365 application on the Azure portal and register it with Azure Active Directory:

1. Log in to the Azure portal at https://portal.azure.com and type "App registrations" in the **Search** field at the top of the window.
2. From the search results, select *App registrations*. The **App registrations** page appears.

3. Click the **[New registration]** button.

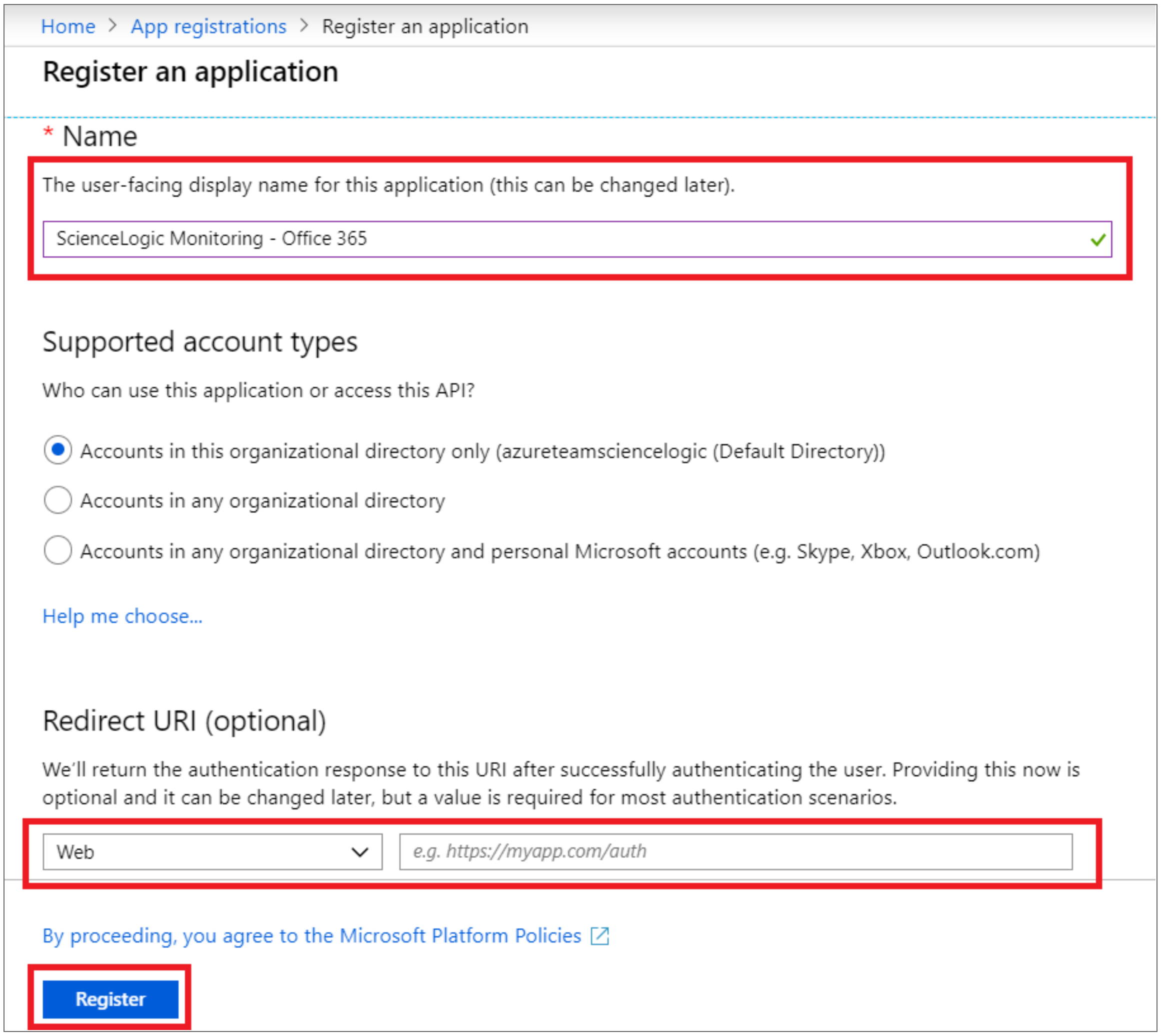


Welcome to the new and improved App registrations (now Generally Available). See what's new →

Looking to learn how it's changed from App registrations (Legacy)? Learn more
Still want to use App registrations (Legacy)? Go back and tell us why

This account isn't listed as an owner of any applications in this directory.

4. When the **Register an application page** appears, enter your application's registration information:
   - ***Name***. Type a name for the application.
   - ***Supported account types***. Select the account types that you want to be supported in your application.
   - ***Redirect URI (optional)***. Select *Web* in the drop-down menu and type a valid URL. For example: https://localhost.com.



Home > App registrations > Register an application

Register an application

* Name

The user-facing display name for this application (this can be changed later).

ScienceLogic Monitoring - Office 365

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (azureteamsciencelogic (Default Directory))

○ Accounts in any organizational directory

○ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

Help me choose...

Redirect URI (optional)

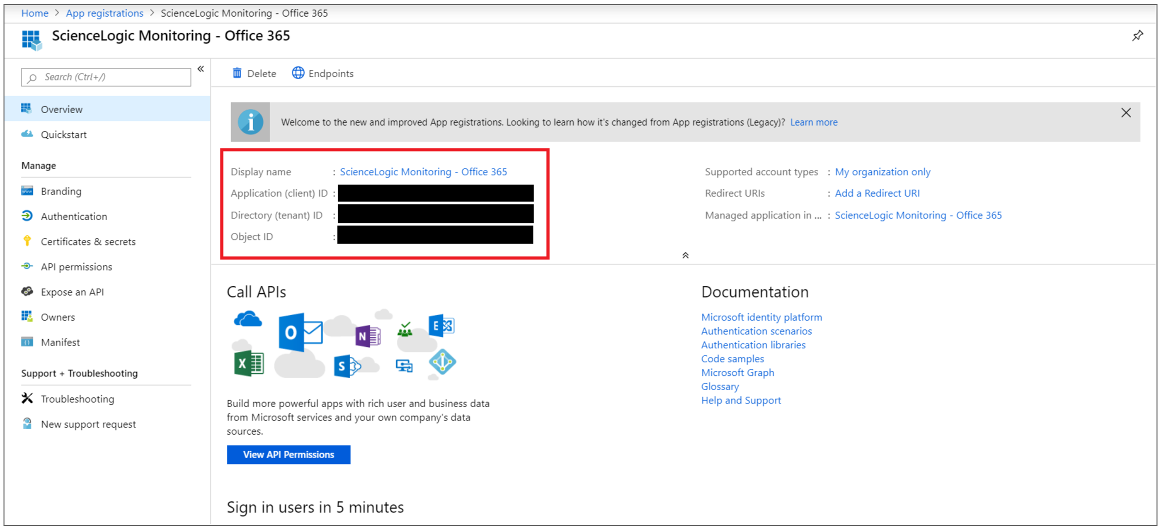
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | e.g. https://myapp.com/auth

By proceeding, you agree to the Microsoft Platform Policies

5. Click the **[Register]** button. The **Overview** page for your new application appears.

6. On the **Overview** page for your new application, copy and save the values in the *Application (client) ID* and *Directory (tenant) ID* fields. You will need these values when creating your Office 365 credential in SL1.



Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Display name : ScienceLogic Monitoring - Office 365
Application (client) ID : [redacted]
Directory (tenant) ID : [redacted]
Object ID : [redacted]

Supported account types : My organization only
Redirect URIs : Add a Redirect URI
Managed application in ... : ScienceLogic Monitoring - Office 365

Call APIs

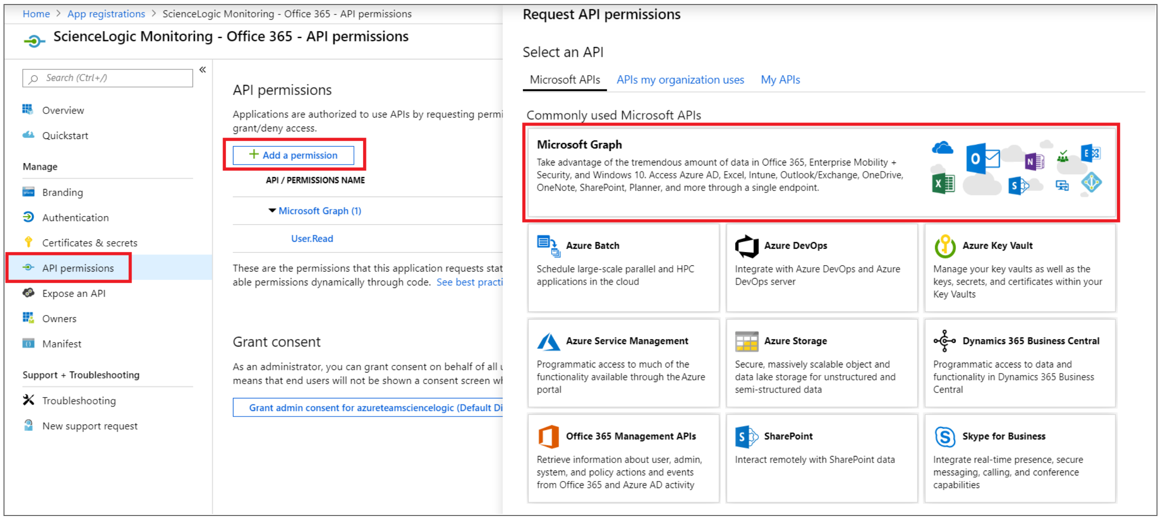
Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Adding API Permissions to the Application

Your Office 365 application must have access permissions for Microsoft Graph APIs and Office 365 Management APIs to be monitored in SL1.

To add API permissions to application:

1. From the page for your new application, click **[View API Permissions]**.
2. Click **[Add a permission]**, then click the **Microsoft Graph** option.



Applications are authorized to use APIs by requesting permi grant/deny access.

These are the permissions that this application requests stat able permissions dynamically through code. See best practi

As an administrator, you can grant consent on behalf of all u means that end users will not be shown a consent screen wh

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Batch
Schedule large-scale parallel and HPC applications in the cloud

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Key Vault
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

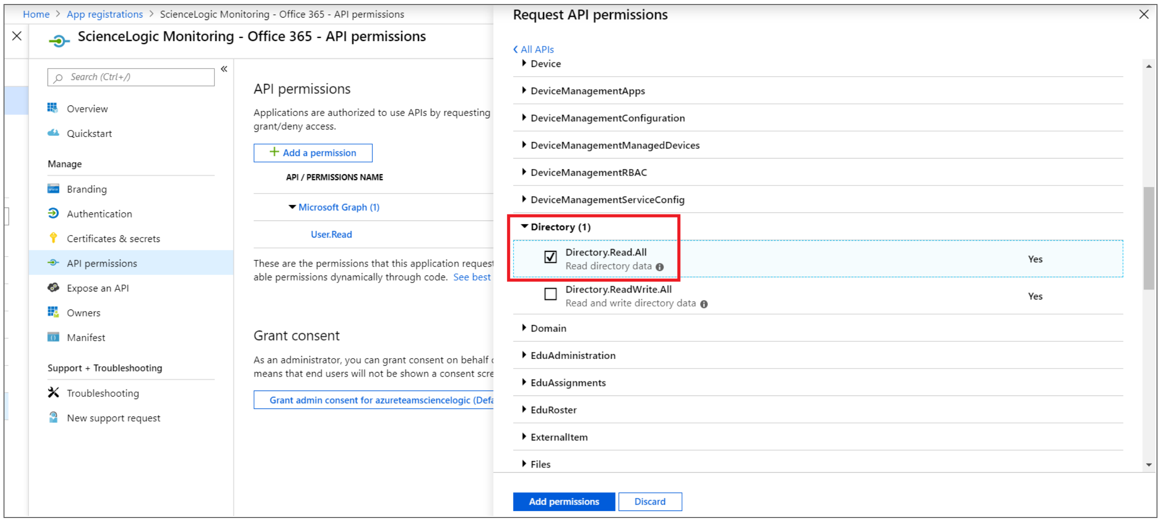
Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

SharePoint
Interact remotely with SharePoint data

Skype for Business
Integrate real-time presence, secure messaging, calling, and conference capabilities

3. In the **Request API permissions** pane, click **Application permissions**.

4. Click the arrow next to **Directory** to open the sub-menu, and then select the checkbox for the *Directory.Read.All* permission.



Applications are authorized to use APIs by requesting grant/deny access.

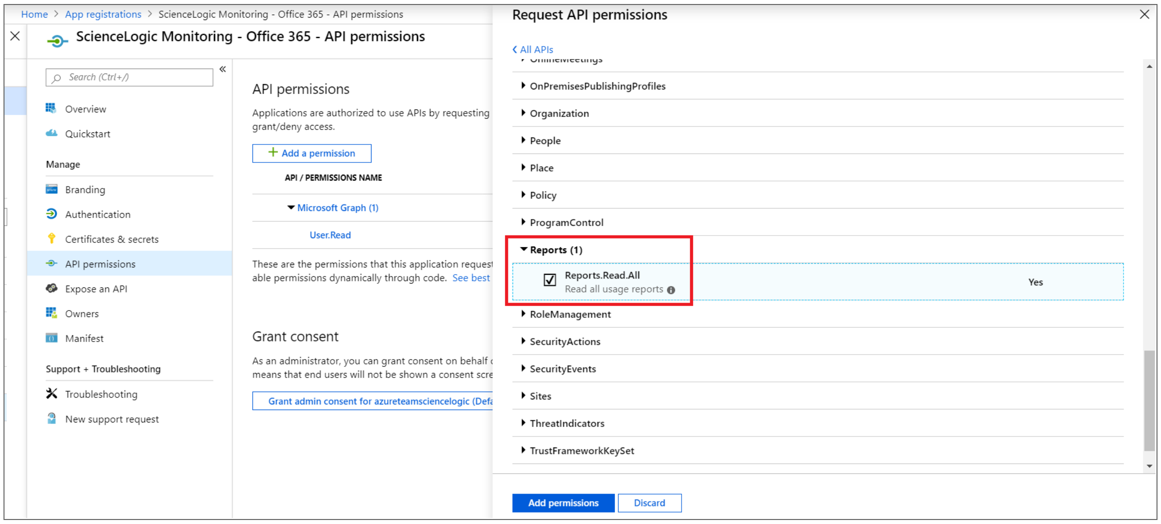
These are the permissions that this application request able permissions dynamically through code. See best

As an administrator, you can grant consent on behalf means that end users will not be shown a consent scre

☑ Directory.Read.All Read directory data — Yes

□ Directory.ReadWrite.All Read and write directory data — Yes

5. Click the arrow next to **Reports** to open the sub-menu, and then select the checkbox for the *Reports.Read.All* permission.



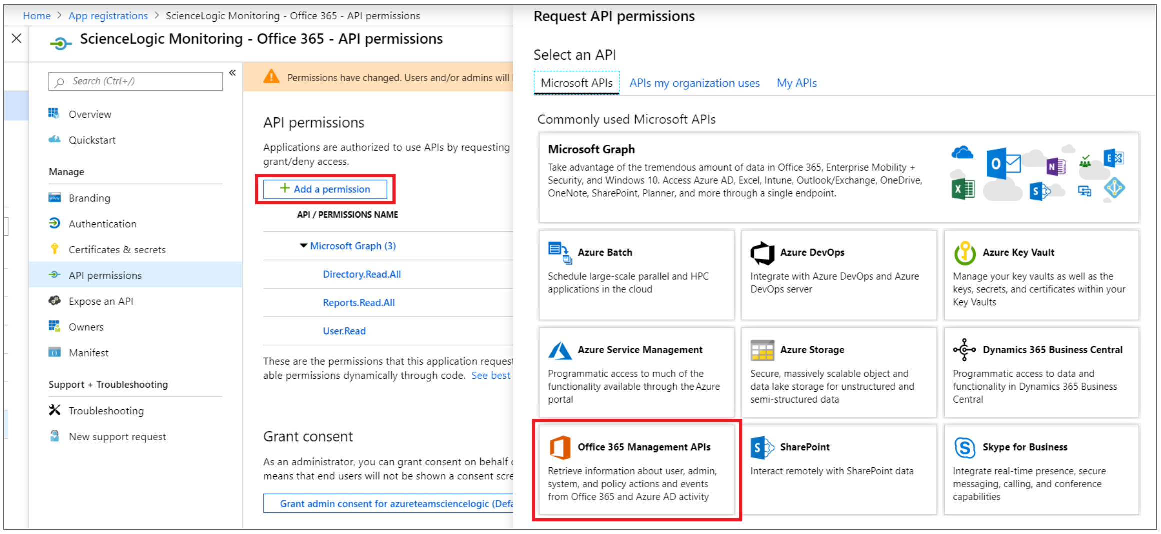
Applications are authorized to use APIs by requesting grant/deny access.

These are the permissions that this application request able permissions dynamically through code. See best

As an administrator, you can grant consent on behalf means that end users will not be shown a consent scre

☑ Reports.Read.All Read all usage reports — Yes

6. Click the **[Add permissions]** button.
7. On the **API permissions** page, click **[Add a permission]**, and then click the *Office 365 Management APIs* option.



Home > App registrations > ScienceLogic Monitoring - Office 365 - API permissions
ScienceLogic Monitoring - Office 365 - API permissions
Search (Ctrl+/)
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
API permissions
Expose an API
Owners
Manifest
Support + Troubleshooting
Troubleshooting
New support request
+ Add a permission
Grant admin consent for azureteamsciencelogic (Defa
Microsoft APIs
APIs my organization uses
My APIs

Permissions have changed. Users and/or admins will

API permissions

Applications are authorized to use APIs by requesting grant/deny access.

API / PERMISSIONS NAME
Microsoft Graph (3)
Directory.Read.All
Reports.Read.All
User.Read

These are the permissions that this application request able permissions dynamically through code. See best

Grant consent

As an administrator, you can grant consent on behalf means that end users will not be shown a consent scre

Request API permissions

Select an API

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Batch
Schedule large-scale parallel and HPC applications in the cloud

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Key Vault
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

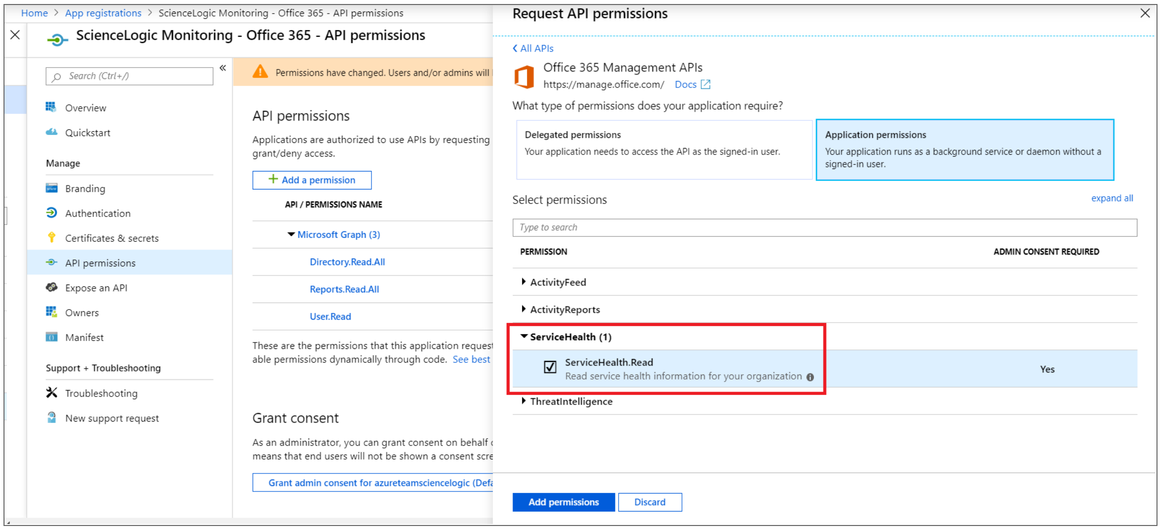
Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

SharePoint
Interact remotely with SharePoint data

Skype for Business
Integrate real-time presence, secure messaging, calling, and conference capabilities

8. In the **Request API permissions** pane, click **Application permissions**.
9. Click the arrow next to **ServiceHealth** to open the sub-menu, and then select the checkbox for the *ServiceHealth.Read* permission.



Permissions have changed. Users and/or admins will

API permissions

Applications are authorized to use APIs by requesting grant/deny access.

API / PERMISSIONS NAME
Microsoft Graph (3)
Directory.Read.All
Reports.Read.All
User.Read

These are the permissions that this application request able permissions dynamically through code. See best

Grant consent

As an administrator, you can grant consent on behalf means that end users will not be shown a consent scre

Request API permissions

Office 365 Management APIs
https://manage.office.com/

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

PERMISSION	ADMIN CONSENT REQUIRED
ActivityFeed	
ActivityReports	
ServiceHealth (1)	
☑ ServiceHealth.Read Read service health information for your organization	Yes
ThreatIntelligence	

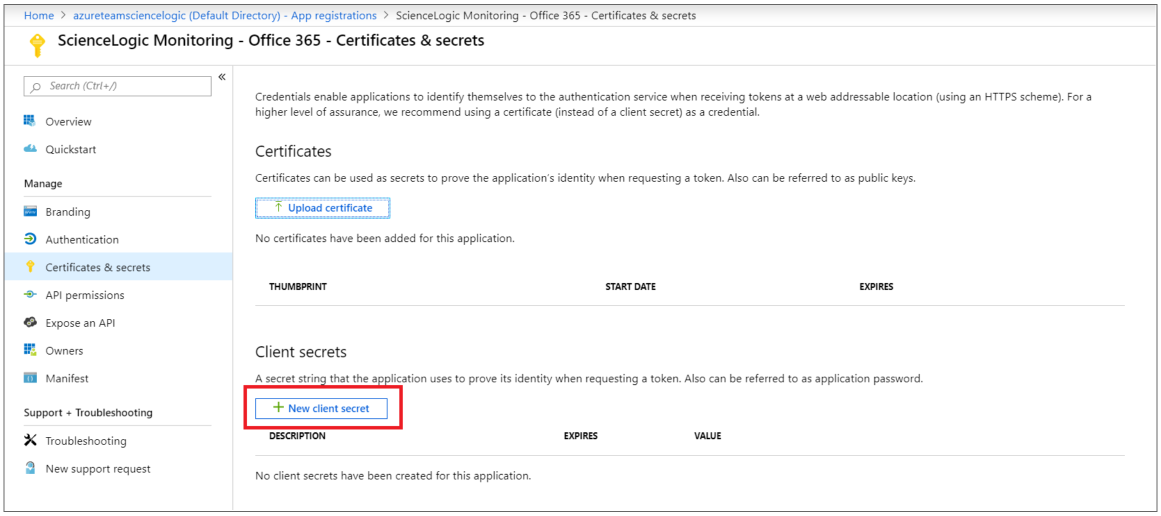
10. Click the **[Add permissions]** button.
11. On the **API permissions** page, click **[Grant admin consent for [Directory Name]]**.
12. A pop-up window appears asking if you grant consent for the required permissions for all accounts in your directory. Click **[Yes]**.

Generating the Secret Key

When configuring a SOAP/XML credential for Office 365 in SL1, you need to provide a secret key for the Office 365 Active Directory application that you will use to authenticate your account.

To generate a secret key:

1. From the Azure portal, type "Active Directory" in the **Search** field at the top of the window.
2. From the search results, select *Azure Active Directory*, and then click **App registrations** on the left pane.
3. Select your Office 365 app from the list.
4. Click **[Certificates & secrets]** on the left pane.
5. In the **Client secrets** pane, click **[+ New client secret]**.



Home > azureteamsciencelogic (Default Directory) - App registrations > ScienceLogic Monitoring - Office 365 - Certificates & secrets

ScienceLogic Monitoring - Office 365 - Certificates & secrets

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

No certificates have been added for this application.

THUMBPRINT	START DATE	EXPIRES

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

DESCRIPTION	EXPIRES	VALUE

No client secrets have been created for this application.

6. In the **Add a client secret** pane, type a name in the ***Description*** field and select a duration in the ***Expires*** field.
7. Click **[Add]** to generate the secret key. A new key value displays in the **Client secrets** pane.
8. Copy and save the key value.

Creating a SOAP/XML Credential for Microsoft Office 365

To configure SL1 to monitor Microsoft Office 365, you must create a SOAP/XML credential. This credential allows the Dynamic Applications in the *Microsoft: Office 365* PowerPack to communicate with your Office 365 account.

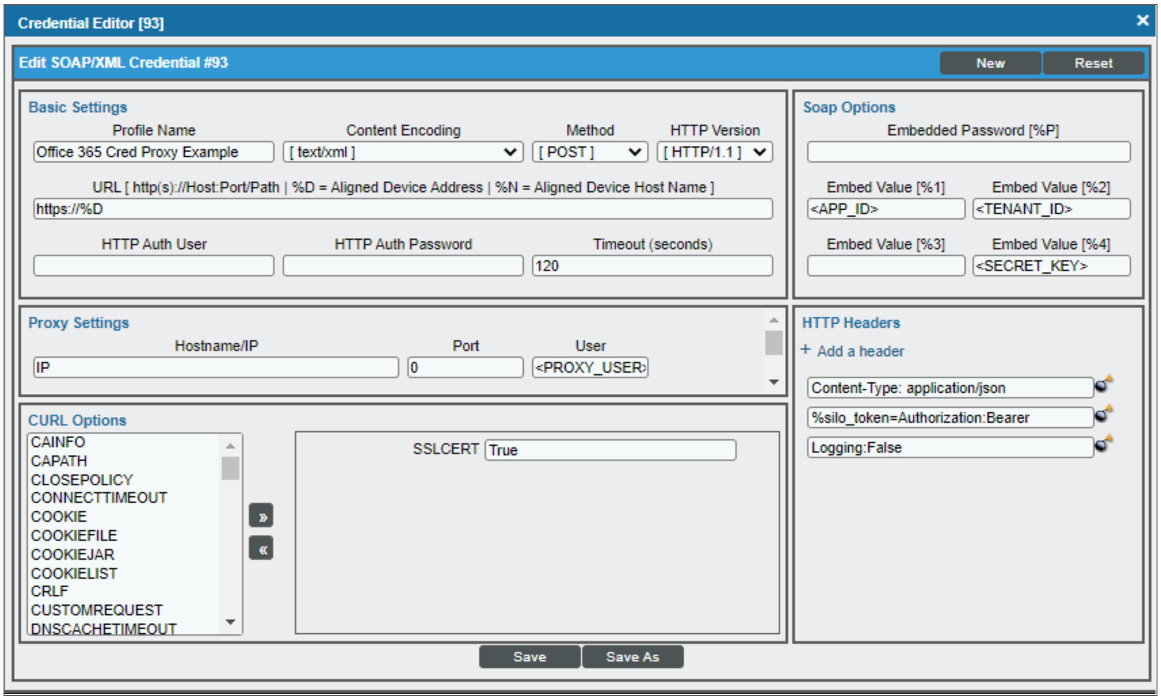
If you want to connect to your Office 365 account through a third-party proxy server, you must also add the proxy information in the credential.

The *Microsoft: Office 365* PowerPack includes two example SOAP/XML credentials that you can use as templates for creating SOAP/XML credentials for Office 365. They are:

- **Office 365 Cred Proxy Example**, for users who connect to Office 365 through a third-party proxy server
- **Office 365 Credential Example**, for all other users

To configure a SOAP/XML credential to access Microsoft Office 365:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the sample credential you want to use and then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears.
3. Enter values in the following fields:



Credential Editor [93]

Edit SOAP/XML Credential #93

Basic Settings

Profile Name: Office 365 Cred Proxy Example
Content Encoding: [text/xml]
Method: [POST]
HTTP Version: [HTTP/1.1]
URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://%D
HTTP Auth User:
HTTP Auth Password:
Timeout (seconds): 120

Soap Options

Embedded Password [%P]:
Embed Value [%1]: <APP_ID>
Embed Value [%2]: <TENANT_ID>
Embed Value [%3]:
Embed Value [%4]: <SECRET_KEY>

Proxy Settings

Hostname/IP: IP
Port: 0
User: <PROXY_USER>

HTTP Headers

Content-Type: application/json
%silo_token=Authorization:Bearer
Logging:False

CURL Options

CAINFO
CAPATH
CLOSEPOLICY
CONNECTTIMEOUT
COOKIE
COOKIEFILE
COOKIEJAR
COOKIELIST
CRLF
CUSTOMREQUEST
DNSCACHETIMEOUT

SSLCERT: True

Basic Settings

- ***Profile Name***. Type a new name for the Microsoft Office 365 credential.
- ***URL***. Type "https://%D".
- ***HTTP Auth User***. Leave this field blank.
- ***HTTP Auth Password***. Leave this field blank.

Proxy Settings

- ***Hostname/IP***. If you are connecting to Office 365 via a proxy server, type the server's hostname or IP address. Otherwise, leave this field blank.
- ***Port***. If you are connecting to Office 365 via a proxy server, type the port number you opened when setting up the proxy server. Otherwise, leave this field blank.

- ***User***. If you are connecting to Office 365 via a proxy server using basic authentication, type the server's administrator username. Otherwise, leave this field blank.
- ***Password***. If you are connecting to Office 365 via a proxy server using basic authentication, type the server's administrator password. Otherwise, leave this field blank.

CURL Options

- ***SSL Cert***. The default value of this field is "True". You can also replace this value with your SSL certificate path. If your SSL certificate is expired or if you do not want extra security, set the value of this field to "False".

SOAP Options

- ***Embedded Password [%P]***. Leave this field blank.
- ***Embed Value [%1]***. Type the Application ID for the Office 365 Active Directory application.
- ***Embed Value [%2]***. Type the Tenant ID for the Office 365 Active Directory application.
- ***Embed Value [%3]***. Leave this field blank.
- ***Embed Value [%4]***. Type the secret key for the Office 365 Active Directory application.

HTTP Headers

- ***HTTP Headers***. The following headers are added by default:
    - ***Content-Type: application/son***. Leave the default value that appears in this field.
    - ***%silo_token-Authorization:Bearer***. Leave the default value that appears in this field.
    - ***Logging:False/True***. The default value of this field is "Logging:False". If you would like your credential to gather event information and errors to display in the **/tmp/0365_error.log** log file, set the value of this field to "Logging:True".

4. For all other fields, use the default values.
5. Click the **[Save As]** button.

Testing Your Office 365 Credential

The *Microsoft: Office 365* PowerPack includes a Credential Test for Office 365. Credential Tests define a series of steps that SL1 can execute on demand to validate whether a credential works as expected.

The "Office 365 Credential Test" can be used to test a SOAP/XML credential for monitoring Office 365 using the Dynamic Applications in the *Microsoft: Office 365* PowerPack.

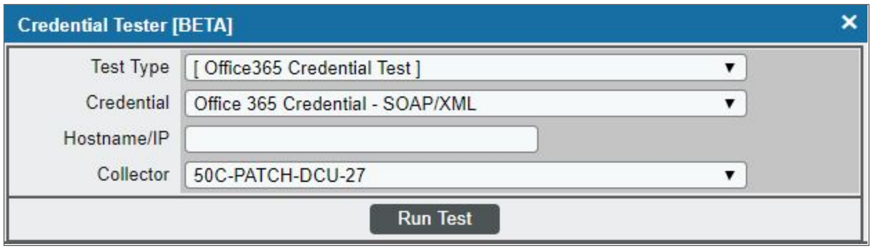
The "Office 365 Credential Test" performs the following steps:

- ***Test Port Availability***. Performs an NMAP request to test the availability of the Office 365 endpoint HTTPS port.
- ***Test Name Resolution***. Performs an nslookup request on the Office 365 endpoint.

- ***Make connection to Office 365 Management API***. Attempts to connect to the Office 365 Management API using the account information specified in the credential.
- ***Make connection to Office 365 Graph API***. Attempts to connect to the Office 365 Graph API using the account information specified in the credential.

To test the Office 365 credential:

1. Go to the **Credential Test Management** page (System > Customize > Credential Tests).
2. Locate the **Office 365 Credential Test** and click its lightning bolt icon ( ). The **Credential Tester** modal page appears:



Test Type: [Office365 Credential Test]
Credential: Office 365 Credential - SOAP/XML
Hostname/IP:
Collector: 50C-PATCH-DCU-27

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***. Leave this field blank.
   - ***Collector***. Select the All-In-One Appliance or Data Collector that will run the test.
4. Click the **[Run Test]** button. The **Test Credential** window appears, displaying 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".

Discovering Office 365 Devices

To discover and monitor your Office 365 devices, you must do the following:

- Create a virtual device representing the Office 365 service
- Configure the device template that is included in the *Microsoft: Office 365* PowerPack
- Align the device template to the Office 365 virtual device

Each of these steps is documented in the following sections.

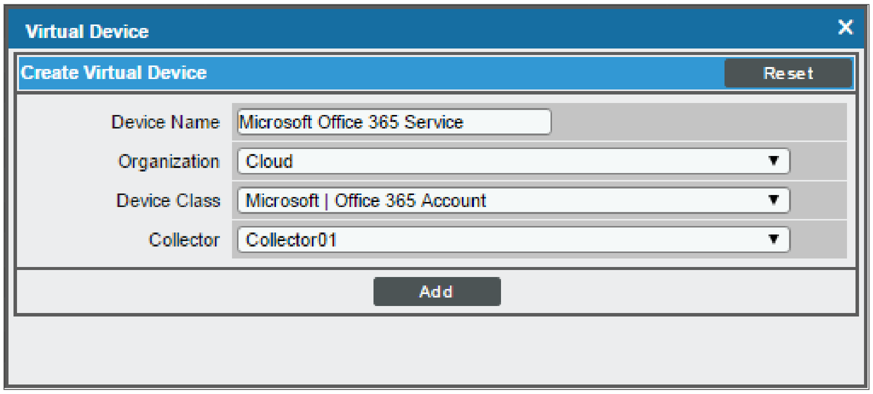
> **TIP:** If you have multiple Office 365 subscriptions you want to monitor, you should create a separate virtual device, credential, and device template for each root device. You can also create different organizations for each Office 365 subscription.

Creating a Microsoft Office 365 Virtual Device

Because the Microsoft Office 365 service does not have an IP address, you cannot discover an Office 365 device using discovery. Instead, you must create a ***virtual device*** that represents the root device for the Office 365 service. A virtual device is a user-defined container that represents a device or service that cannot be discovered by SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications.

To create a virtual device that represents your Office 365 service:

1. Go to the **Device Manager** page (Devices > Device Manager, or Registry > Devices > Device Manager in the SL1 classic user interface).
2. Click the **[Actions]** button and select *Create Virtual Device* from the menu. The **Virtual Device** modal page appears.
3. Enter values in the following fields:



Device Name: Microsoft Office 365 Service
Organization: Cloud
Device Class: Microsoft | Office 365 Account
Collector: Collector01

- ***Device Name***. Enter a name for the device. For example, you could enter "Microsoft Office 365 Service" in this field.
- ***Organization***. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.

- ***Device Class***. Select *Microsoft | Office 365 Account*.
- ***Collector***. Select the collector group that will monitor the device.

4. Click the **[Add]** button to create the virtual device.

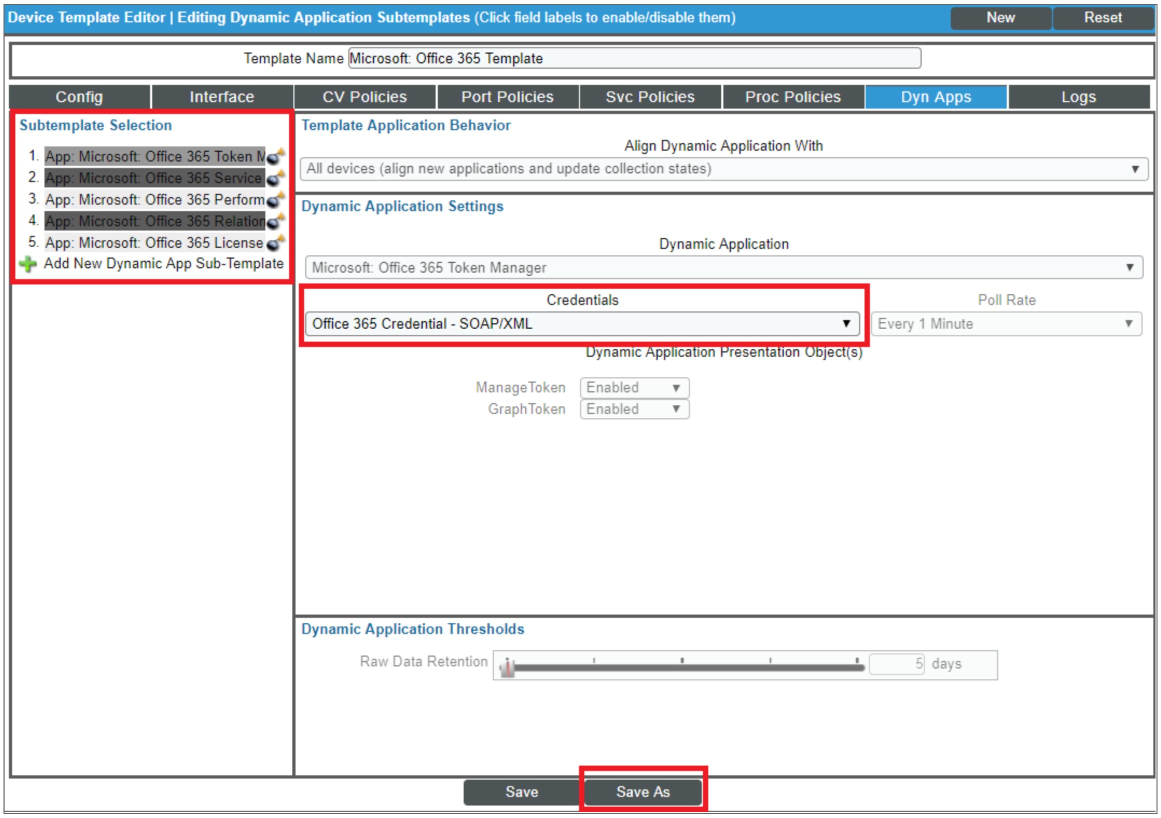
Configuring the Office 365 Device Template

The *Microsoft: Office 365* PowerPack includes the "Microsoft: Office 365 Template", which you can use to create a device template for your own Office 365 account. This device template enables SL1 to align all of the necessary Dynamic Applications to the Office 365 root component device.

Before you can use the "Microsoft: Office 365 Template", you must give the template a new name and configure it so that each Dynamic Application in the template aligns with the credential you created earlier.

To configure the Office 365 device template:

1. Go to the **Configuration Templates** page (Devices > Templates, or Registry > Devices > Templates in the SL1 classic user interface).
2. Locate the "Microsoft: Office 365 Template" and click its wrench icon (🔧). The **Device Template Editor** modal page appears.
3. In the ***Template Name*** field, type a new name for the device template.
4. Click the **[Dyn Apps]** tab. The **Editing Dynamic Application Subtemplates** page appears.
5. In the **Subtemplate Selection** pane, click the first Dynamic Application name, then select your Office 365 credential in the *Credentials* field in the Dynamic Application Settings pane.
6. Repeat step 5 for each of the Dynamic Applications listed in the **Subtemplate Selection** pane.


Device Template Editor | Editing Dynamic Application Subtemplates (Click field labels to enable/disable them)
New
Reset
Config
Interface
CV Policies
Port Policies
Svc Policies
Proc Policies
Dyn Apps
Logs
Save
Save As

Template Name: Microsoft: Office 365 Template

Subtemplate Selection

1. App: Microsoft: Office 365 Token M
2. App: Microsoft: Office 365 Service
3. App: Microsoft: Office 365 Perform
4. App: Microsoft: Office 365 Relation
5. App: Microsoft: Office 365 License

Add New Dynamic App Sub-Template

Template Application Behavior

Align Dynamic Application With: All devices (align new applications and update collection states)

Dynamic Application Settings

Dynamic Application: Microsoft: Office 365 Token Manager

Credentials: Office 365 Credential - SOAP/XML

Poll Rate: Every 1 Minute

Dynamic Application Presentation Object(s)

ManageToken: Enabled

GraphToken: Enabled

Dynamic Application Thresholds

Raw Data Retention: 5 days

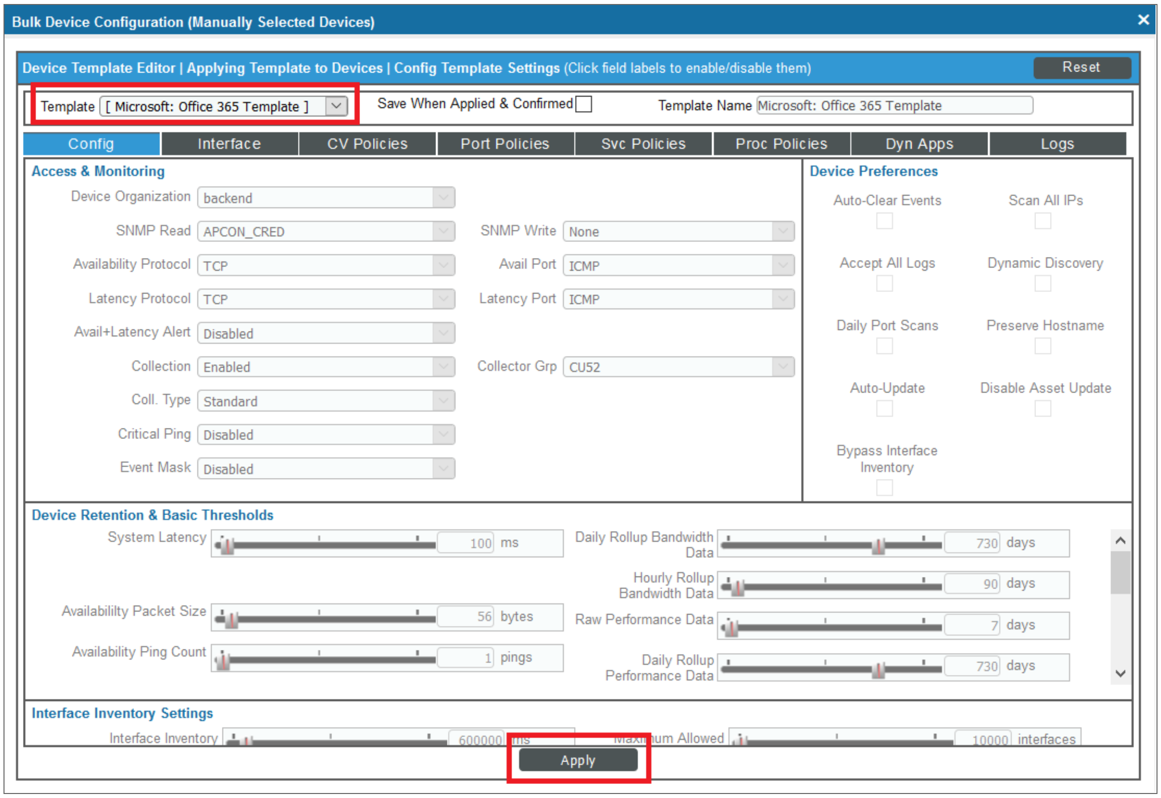
7. When you are finished, click **[Save As]**.

Aligning the Device Template to Your Office 365 Virtual Device

After you have configured the Office 365 device template so that each Dynamic Application in the template aligns with your Office 365 credential, you can use that template to align the Dynamic Applications to the virtual device that you created to act as the root device for your Office 365 environment. When you do so, SL1 discovers and models all of the components in your Office 365 service.

To align the Office 365 device template to the Office 365 virtual device:

1. Go to the **Device Manager** page (Devices > Device Manager, or Registry > Devices > Device Manager in the SL1 classic user interface).
2. On the **Device Manager** page, select the checkbox for the Office 365 virtual device.
3. In the ***Select Actions*** field, in the lower right corner of the page, select the option *MODIFY by Template* and then click the **[Go]** button. The **Device Template Editor** page appears.
4. In the ***Template*** drop-down list, select your Office 365 device template.
5. Click the **[Apply]** button, and then click **[Confirm]** to align the Dynamic Applications to the root component device.



Bulk Device Configuration (Manually Selected Devices)

Device Template Editor | Applying Template to Devices | Config Template Settings (Click field labels to enable/disable them)

Template: [Microsoft: Office 365 Template]

Save When Applied & Confirmed □

Template Name: Microsoft: Office 365 Template

Access & Monitoring

- Device Organization: backend
- SNMP Read: APCON_CRED
- SNMP Write: None
- Availability Protocol: TCP
- Avail Port: ICMP
- Latency Protocol: TCP
- Latency Port: ICMP
- Avail+Latency Alert: Disabled
- Collection: Enabled
- Collector Grp: CU52
- Coll. Type: Standard
- Critical Ping: Disabled
- Event Mask: Disabled

Device Preferences

- Auto-Clear Events □
- Scan All IPs □
- Accept All Logs □
- Dynamic Discovery □
- Daily Port Scans □
- Preserve Hostname □
- Auto-Update □
- Disable Asset Update □
- Bypass Interface Inventory □

Device Retention & Basic Thresholds

- System Latency: 100 ms
- Availabililty Packet Size: 56 bytes
- Availability Ping Count: 1 pings
- Daily Rollup Bandwidth Data: 730 days
- Hourly Rollup Bandwidth Data: 90 days
- Raw Performance Data: 7 days
- Daily Rollup Performance Data: 730 days

Interface Inventory Settings

- Interface Inventory: 600000 ms
- Maximum Allowed: 10000 interfaces

Relationships Between Component Devices

In addition to parent/child relationships between component devices, SL1 also creates relationships between Office 365 component devices and other associated devices:

- If you discover Azure devices using the Dynamic Applications in the *Microsoft: Azure* PowerPack version 110 or later, SL1 will automatically create relationships between Office 365 Active Directory tenants and Azure Active Directory tenants.

Chapter 53

Microsoft: SQL Server Enhanced

Overview

The following sections describe how to configure and discover Microsoft SQL Servers for monitoring in SL1 using the *Microsoft: SQL Server Enhanced* PowerPack:

NOTE: If you already have Windows Server discovered, you might not need to create a new SQL Server credential or run a separate discovery session for SQL Servers if the PowerShell credential information is the same as that used for the Windows Server credential. In this scenario, you need only to install the *Microsoft: SQL Server Enhanced* PowerPack and ensure that the Windows user account used in the credential has the appropriate permissions, as outlined in the **Prerequisites** section.

NOTE: For more information about the *Microsoft: SQL Server Enhanced* PowerPack, see the ***Monitoring SQL Servers*** manual.

Prerequisites for Monitoring SQL Servers

To configure the SL1 system to monitor SQL servers using the *Microsoft: SQL Server Enhanced* PowerPack, you must first have the following information about the SQL Servers that you want to monitor:

- IP addresses and ports for the SQL Servers
- Username and password for a Windows user account with access to the SQL Servers

The SQL Servers that you monitor must be running PowerShell version 3.0 or later and need to have the SQL Server PowerShell (SQLPS) module installed. This SQLPS module is installed by SQL Server Management Studio. You can also install the SqlServer PowerShell module found here: https://www.powershellgallery.com/packages/Sqlserver/21.1.18218

To determine if the proper cmdlets are available for this PowerPack to collect, run `Get-Command Invoke-SqlCmd` to see if the Invoke-SqlCmd cmdlet is installed.

In addition, the *Microsoft: SQL Server Enhanced* PowerPack requires the following permissions for the user account used for monitoring:

- SQL 2014 and newer versions require one of the following configurations:
  - The user account has an enabled login on every instance and database to be monitored, with CONNECT SQL, VIEW SERVER STATE, and CONNECT ANY DATABASE permission granted to the login on each instance. The login should have VIEW DATABASE STATE permission and DB_DATAREADER role granted on the 'master' database, and the DB_DATAREADER role granted on the 'msdb' database.
  - The user account has an enabled login on every instance and has the SYSADMIN role.
- SQL 2008 to SQL 2012 versions require one of the following configurations:
  - The user account has an enabled login on every instance and database to be monitored, with CONNECT SQL and VIEW SERVER STATE granted to the login on each instance. The login should also have VIEW DATABASE STATE permission and the DB_DATAREADER role granted on the 'master' database, and the DB_DATAREADER role granted on the 'msdb' database. In addition, every database in the instance should have CONNECT access granted to the login.
  - The user account has an enabled login on every instance and has the SYSADMIN role.

ScienceLogic provides a PowerShell script on the ScienceLogic Support Site that automates the permissions-granting that is required as stated above. The script can be downloaded here: https://portal-cdn.sciencelogic.com/powerpackextras/5819/19047/winrm_configuration_wizardv3.0.zip

After downloading the script, perform the following steps:

1. Copy the winrm_configuration_scriptv3.0.zip file to the Windows server where Microsoft SQL Server is installed and from which you will be collecting data. Unzip the file.
2. Using the credentials for an account that is a member of the Administrator's group, log in to the Windows server you want to monitor. You can log in directly or use Remote Desktop to log in.
3. Right-click on the Windows PowerShell icon and select ***Run As Administrator***.

4. At the Windows PowerShell prompt, navigate to the directory where you unzipped the PowerShell script named winrm_configuration_wizard.ps1.
5. At the PowerShell prompt, enter the following to enable execution of the script:

```
Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope Process -Force
```

> **NOTE:** The execution policy setting persists only during the current PowerShell session.

6. After the warning text, select Y.
7. To set the required, least-privileged permissions for the user account SL1 will use to monitor all SQL Server instances and databases on the server, run the following script:

```
.\winrm_configuration_wizard.ps1 -user <domain>\<username> -sql_only
```

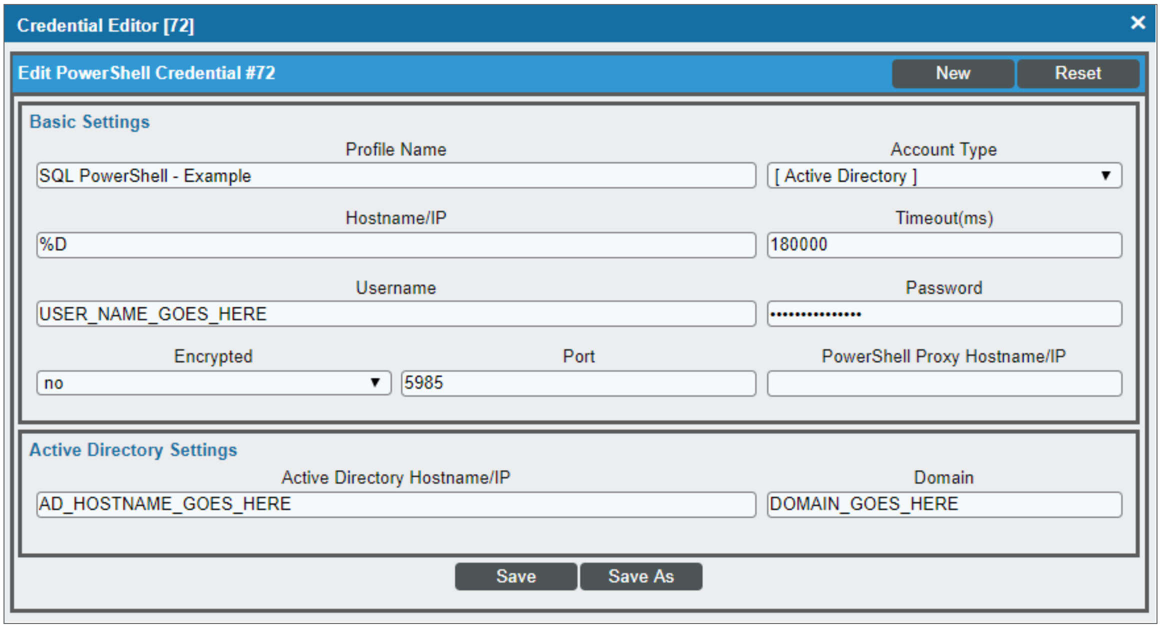
Creating a PowerShell SQL Server Credential

To configure SL1 to monitor SQL Servers, you must first create a PowerShell credential. This credential allows the Dynamic Applications in the *Microsoft: SQL Server Enhanced* PowerPack to connect with an SQL Server. An example PowerShell credential that you can edit for your own use is included in the PowerPack.

To create a PowerShell credential for an SQL Server:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **SQL PowerShell - Example** credential, and then click its wrench icon (🔧). The **Edit PowerShell Credential** modal page appears.

3. Complete the following fields:



Credential Editor [72]

Edit PowerShell Credential #72

Basic Settings

Profile Name: SQL PowerShell - Example

Account Type: [Active Directory]

Hostname/IP: %D

Timeout(ms): 180000

Username: USER_NAME_GOES_HERE

Password: ••••••••••••••

Encrypted: no

Port: 5985

PowerShell Proxy Hostname/IP:

Active Directory Settings

Active Directory Hostname/IP: AD_HOSTNAME_GOES_HERE

Domain: DOMAIN_GOES_HERE

- ***Profile Name***. Type a new name for your SQL Server credential.
- ***Account Type***. Select *Active Directory*.
- ***Hostname/IP***. Type "%D".
- ***Timeout***. Type "18000".
- ***Username***. Type the username for a Windows user with access to the SQL Server.
- ***Password***. Type the password for the Windows account username.

NOTE: The user account whose username and password are provided in the credential must have certain permissions in all SQL Server instances that SL1 will monitor. For a list of these permissions, see the *Prerequisites* section.

- ***Encrypted***. Select *no*.
- ***Port***. Type "5985".
- ***PowerShell Proxy Hostname/IP***. Leave this field blank.
- ***Active Directory Hostname/IP***. Specify the hostname or IP address of the Active Directory server that will authenticate the credential.
- ***Domain***. Specify the domain where the monitored SQL Server resides.

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

5. When the confirmation message appears, click **[OK]**.

SQL Cluster Monitoring

For SQL Clusters that only include SQL Instances in an Active/Active configuration, follow the steps in the ***Discovering SQL Servers*** section.

For SQL Clusters that include an SQL Instance in an Active/Passive configuration, additional discovery steps are required and listed below.

> **NOTE:**SL1's Active/Passive SQL Instance monitoring leverages the SL1 GUID Component Identifier to allow the SQL Instance component and its child database components to move between SQL Servers during a failover. Adding this GUID Component Identifier on SL1 versions prior to 8.12.1 will create a duplicate SQL Instance component on any already discovered SQL Servers. To prevent this, the GUID Component Identifier is not used by default. The "Enable Active Passive Cluster Failover" threshold in the "Microsoft: SQL Server Discovery" Dynamic Application provides the option to use the GUID Component Identifier when enabled. A value of "0" in the ***Threshold Value*** disables Active/Passive cluster failover; a value of "1" enables it.

Monitoring SQL Clusters on SL1 8.12.1 or greater.

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
2. Click the wrench icon (🔧) for the "Microsoft: SQL Server Discovery" Dynamic Application to open the **Dynamic Applications Properties Editor**page.
3. In the **[Thresholds]** tab, click the wrench icon (🔧) for the "Enable Active Passive Cluster Failover" threshold and change the ***Threshold Value*** to *1*.
4. Click **[Save]**.
5. Follow the steps in the ***Discovering SQL Servers*** section on each Windows Server in the cluster.

Monitoring SQL CLusters on SL1 8.8.1 to 8.12.0

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
2. Click the wrench icon (🔧) for the "Microsoft: SQL Server Discovery" Dynamic Application to open the **Dynamic Applications Properties Editor**page.
3. In the **[Properties]** tab, change the ***Operational State*** field to *Disabled*.
4. Click **[Save]**.
5. Follow the steps in the ***Discovering SQL Servers*** section on each Windows Server in the cluster.
6. Go to the **Device Components** page (Registry > Devices > Device Components).
7. Click the wrench icon (🔧) for one of the Windows Servers that make up the SQL Cluster to open its **Device Properties** page.

8. In the **[Thresholds]** tab, under **Dynamic App Thresholds | Microsoft: SQL Server Discovery**, change ***Enable Active Passive Cluster*** to *1*.
9. Repeat steps 7 and 8 for each of the Windows Servers that make up the SQL Cluster.
10. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
11. Click the wrench icon (🔧) for the "Microsoft: SQL Server Discovery" Dynamic Application to open the **Dynamic Applications Properties Editor**page.
12. In the **[Properties]** tab, change the ***Operational State*** field to *Enabled*.
13. Click **[Save]**.

Discovering SQL Servers

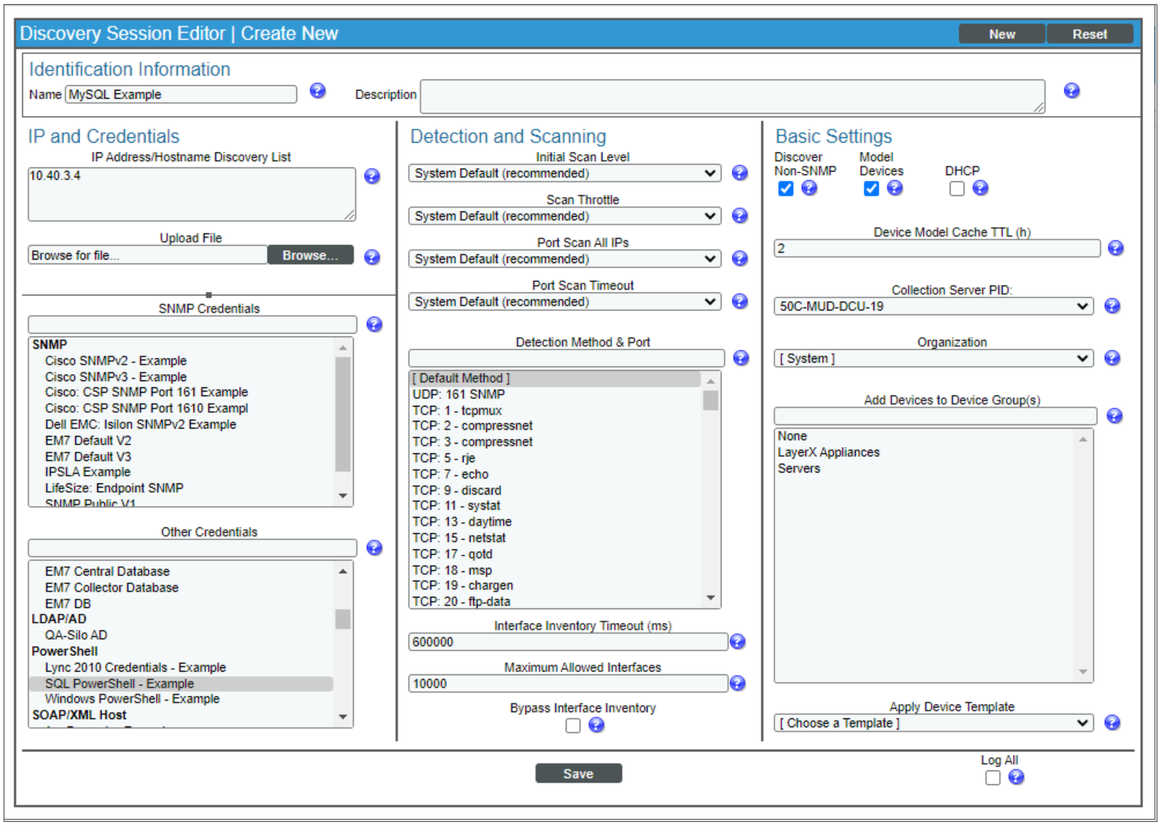
When you discover SQL Servers in SL1, SL1 auto-aligns a series of Dynamic Applications to discover, configure, and monitor the following SQL Server component devices:

- SQL Servers
    - SQL Server instances
        - SQL Server databases

To discover SQL Servers and their component devices, perform the following steps:

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

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



Discovery Session Editor | Create New

Identification Information

Name: MySQL Example

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.40.3.4

Upload File: Browse for file...

Initial Scan Level: System Default (recommended)

Scan Throttle: System Default (recommended)

Port Scan All IPs: System Default (recommended)

Port Scan Timeout: System Default (recommended)

Discover Non-SNMP: ☑

Model Devices: ☑

DHCP: □

Device Model Cache TTL (h): 2

Collection Server PID: 50C-MUD-DCU-19

Organization: [System]

Interface Inventory Timeout (ms): 600000

Maximum Allowed Interfaces: 10000

Bypass Interface Inventory: □

Apply Device Template: [Choose a Template]

Log All: □

3. Supply values in the following fields:

- ***IP Address/Hostname Discovery List***. Type the IP addresses or the range of IP addresses for the SQL Servers you want to discover.
- ***Other Credentials***. Select the *PowerShell credential you created*.
- ***Discover Non-SNMP***. Because the discovery session is not using an SNMP credential, select this checkbox.

4. Optionally, supply values in the other fields in this page. For a description of the fields in this page, see the ***Discovery & Credentials*** manual.

5. Click the **[Save]** button.

6. The **Discovery Control Panel** page will refresh. Click the lightning bolt icon (⚡) for the discovery session you created.

7. In the pop-up window that appears, click the **[OK]** button. The **Discovery Session** page displays the progress of the discovery session.

Relationships Between Component Devices

SL1 can automatically build relationships between SQL servers and other associated devices:

- If you discover Windows server clusters using the Dynamic Applications in the *Microsoft: Windows Server Cluster* PowerPack version 100 or later, SL1 will automatically create relationships between SQL servers and Windows server clusters.

Chapter 54

MySQL

Overview

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

NOTE: For more information about the *MySQL*PowerPack, see the ***Monitoring MySQL*** manual.

Prerequisites for Monitoring MySQL

To configure the SL1 system to monitor MySQL servers and instances using the *MySQL* PowerPack, you must first create a read-only MySQL user for each instance to be monitored. For discovery of multiple instances on the same IP address, ScienceLogic recommends creating the same user and password on each instance. The user must have the minimum following privileges:

Privilege	Definition	Level(s)
SELECT	Enables the use of SELECT.	Global, database, table, column.
EXECUTE	Enable the use of statements that execute stored routines (stored procedures and functions). This is necessary for queries on the system database.	

Creating a SOAP/XML Credential for MySQL

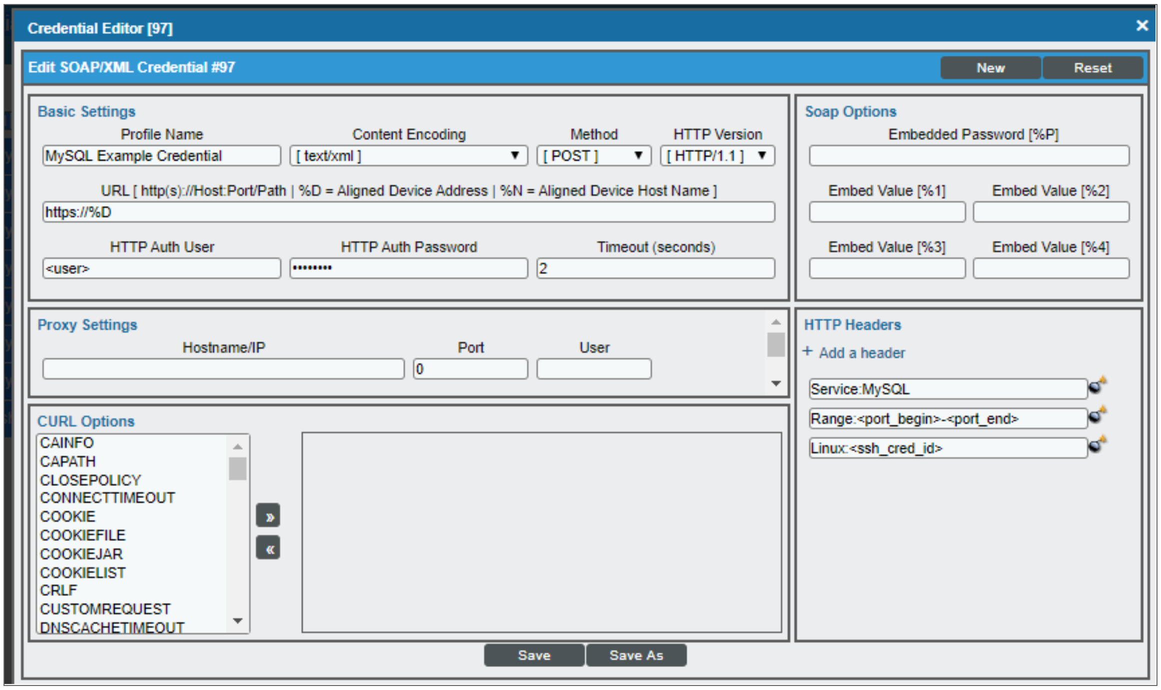
To configure SL1 to monitor MySQL, you must create a SOAP/XML credential. This credential allows the Dynamic Applications in the *MySQL* PowerPack to communicate with your MySQL server and instances.

The *MySQL*PowerPack includes an example SOAP/XML credential that you can use as a template for creating SOAP/XML credentials for MySQL.

To configure a SOAP/XML credential to access your MySQL server:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **MySQL Example Credential** and click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears.

3. Enter values in the following fields:


Credential Editor [97]

Edit SOAP/XML Credential #97

Basic Settings

Profile Name: MySQL Example Credential

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://%D

HTTP Auth User: <user>

HTTP Auth Password: ••••••••

Timeout (seconds): 2

Proxy Settings

Hostname/IP:

Port: 0

User:

CURL Options

CAINFO
CAPATH
CLOSEPOLICY
CONNECTTIMEOUT
COOKIE
COOKIEFILE
COOKIEJAR
COOKIELIST
CRLF
CUSTOMREQUEST
DNSCACHETIMEOUT

Soap Options

Embedded Password [%P]:

Embed Value [%1]:

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

HTTP Headers

Service:MySQL
Range:<port_begin>-<port_end>
Linux:<ssh_cred_id>

Basic Settings

- ***Profile Name***. Type a new name for the MySQL credential.
- ***URL***. Type "%D".
- ***HTTP Auth User***. Type the username for your MySQL server.
- ***HTTP Auth Password***. Type the password for your MySQL server.

NOTE: To discover multiple MySQL instances on the same IP address, ScienceLogic recommends creating the same user and password on each instance, so the user will need to create only one credential.

HTTP Headers

- ***HTTP Headers***. The following headers are in the example credential and are required:
    - Service:MySQL
    - Range:<port_begin>-<port_end>. Specify the range of ports on which your MySQL server is running. For example, "Range:3305-3310".
    - Linux:<ssh_cred_id>. If you have ***configured credentials to read the error log***, enter the credential ID for the SSH credential for a Linux server. For Windows servers, update the field to "Windows:<powershell_cred_id>".

4. For all other fields, use the default values.
5. Click the **[Save As]** button.

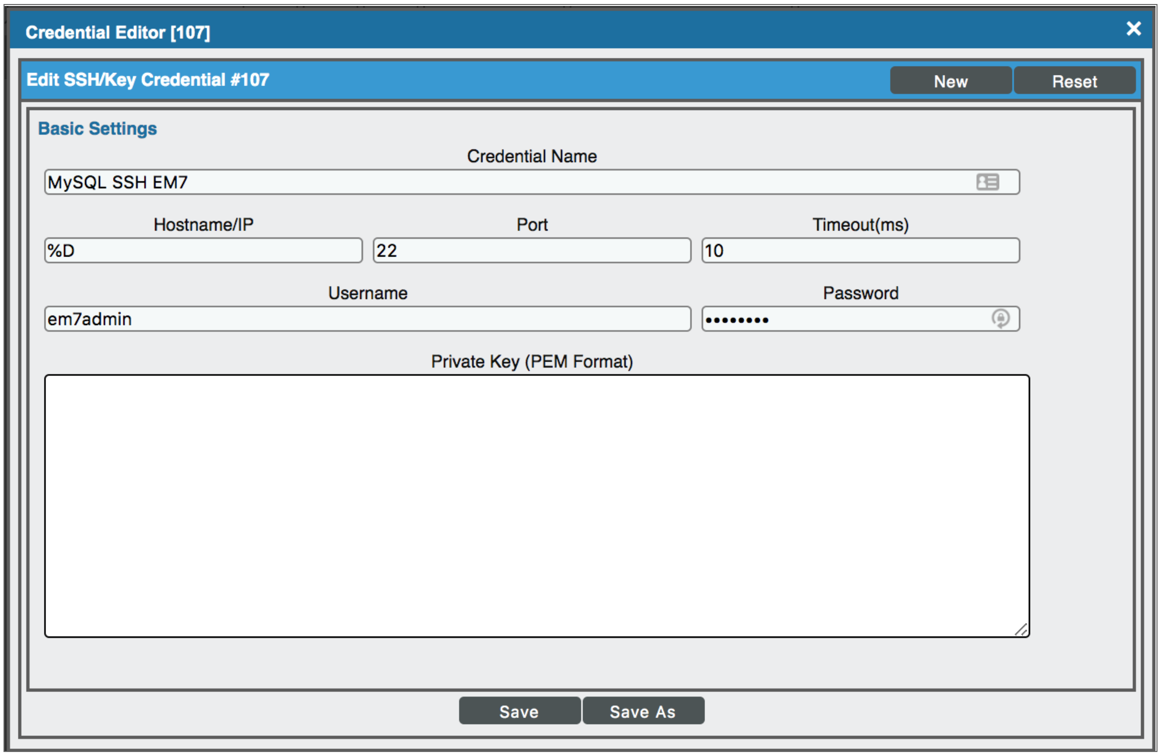
Configuring the Credential to Read the MySQL Error Log

In addition to the *SOAP/XML credential created to monitor MySQL*, another credential must be created to read the MySQL Error Log. The credentials are configured differently for Linux and Windows servers.

For Linux servers, you must create an SSH/Key credential. To create the credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the **[Action]**s button and select the option *Create SSH/Key Credential* for Linux servers or *Create PowerShell Credential* for Windows Servers.
3. Enter values in the following fields:

For Linux Servers:



Credential Editor [107]

Edit SSH/Key Credential #107

Basic Settings

Credential Name: MySQL SSH EM7

Hostname/IP: %D

Port: 22

Timeout(ms): 10

Username: em7admin

Password: ••••••••

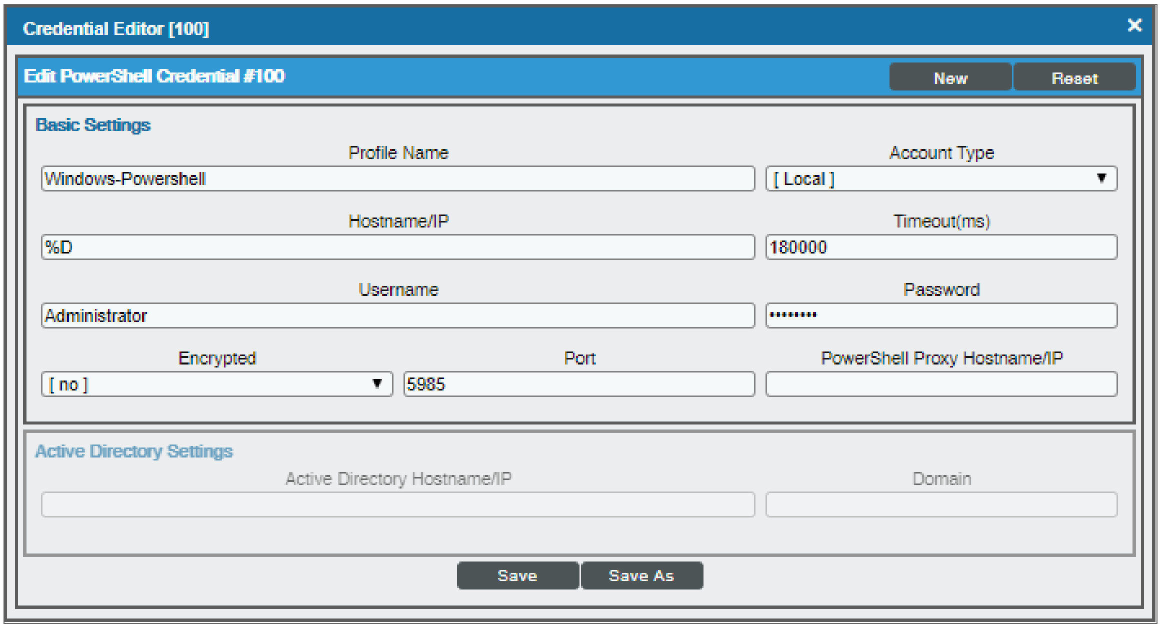
Private Key (PEM Format):

- ***Credential Name***. Type a new name for the credential.
- ***Hostname/IP***. Type "%D".
- ***Username***. Type the username for your Linux server.
- ***Password***. Type the password for your Linux server.

4. For all other fields, use the default values.
5. Click the **[Save]** button.

For Windows servers, you must create a PowerShell credential. To create the credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the **[Action]**s button and select *Create PowerShell Credential*.
3. Enter values in the following fields:



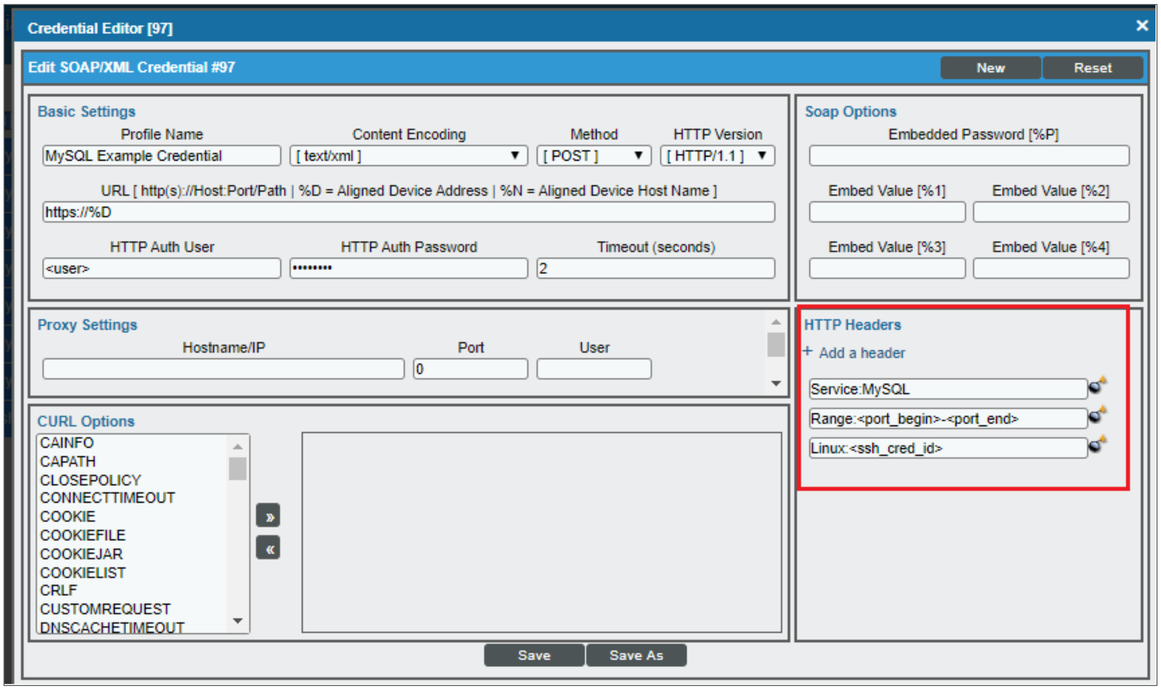
Profile Name: Windows-Powershell
Account Type: [Local]
Hostname/IP: %D
Timeout(ms): 180000
Username: Administrator
Password: ••••••••
Encrypted: [no]
Port: 5985
PowerShell Proxy Hostname/IP:
Active Directory Hostname/IP:
Domain:

- ***Profile Name***. Type a new name for the credential.
- ***Hostname/IP***. Type "%D".
- ***Username***. Type your username for the Windows server.
- ***Password***. Type your password for the Windows server.

4. For all other fields, use the default values.
5. Click the **[Save]** button.

To configure the existing SOAP credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the *MySQL credential you created* and click its wrench icon (). The **Edit SOAP/XML Credential** modal page appears.
3. In the **HTTP Headers** pane, enter the credential ID for the SSH credential for a Linux server. For Windows servers, update the field to "Windows:<powershell_cred_id>".



Profile Name: MySQL Example Credential

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://%D

HTTP Auth User: <user>

HTTP Auth Password: ••••••••

Timeout (seconds): 2

Embedded Password [%P]:

Embed Value [%1]:

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

Hostname/IP:

Port: 0

User:

Service:MySQL

Range:<port_begin>-<port_end>

Linux:<ssh_cred_id>

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

Discovering MySQL Servers

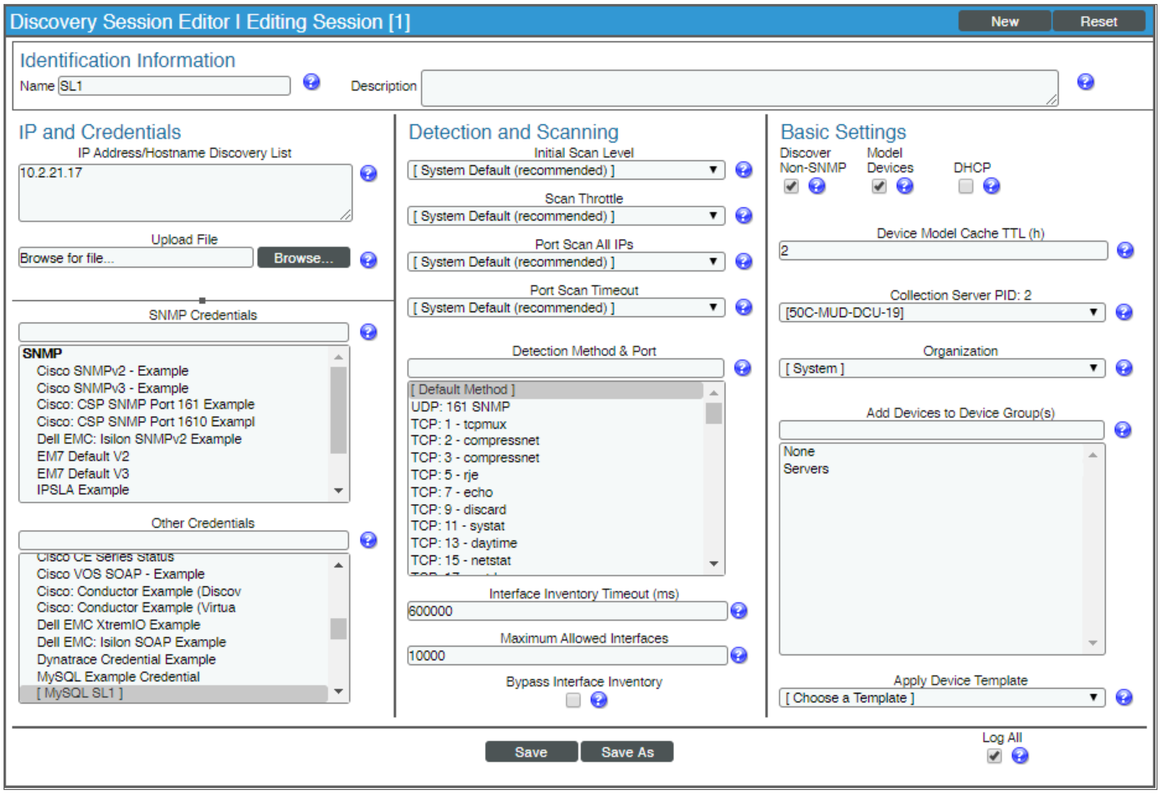
To model and monitor your MySQL servers and instances, you must run a discovery session to discover the MySQL server that SL1 will use as the root device for monitoring the MySQL instances.

Several minutes after the discovery session has completed, the "MySQL: Discovery" Dynamic Application in the *MySQL* PowerPack should automatically align to the MySQL server, creating the MySQL server container. The remaining Dynamic Applications in the PowerPack will then discover, model, and monitor the remaining MySQL instances.

To discover the MySQL server 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:



Discovery Session Editor | Editing Session [1]

Identification Information

Name: SL1

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.2.21.17

Upload File: Browse for file...

SNMP Credentials:

SNMP
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Cisco: CSP SNMP Port 161 Example
Cisco: CSP SNMP Port 1610 Exampl
Dell EMC: Isilon SNMPv2 Example
EM7 Default V2
EM7 Default V3
IPSLA Example

Other Credentials:

Cisco CE Series Status
Cisco VOS SOAP - Example
Cisco: Conductor Example (Discov
Cisco: Conductor Example (Virtua
Dell EMC XtremIO Example
Dell EMC: Isilon SOAP Example
Dynatrace Credential Example
MySQL Example Credential
[MySQL SL1]

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: [50C-MUD-DCU-19]

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(es) of the MySQL server you want to discover.
- ***Other Credentials***. Select the SOAP/XML credential(s) you created for the MySQL server.
- ***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.

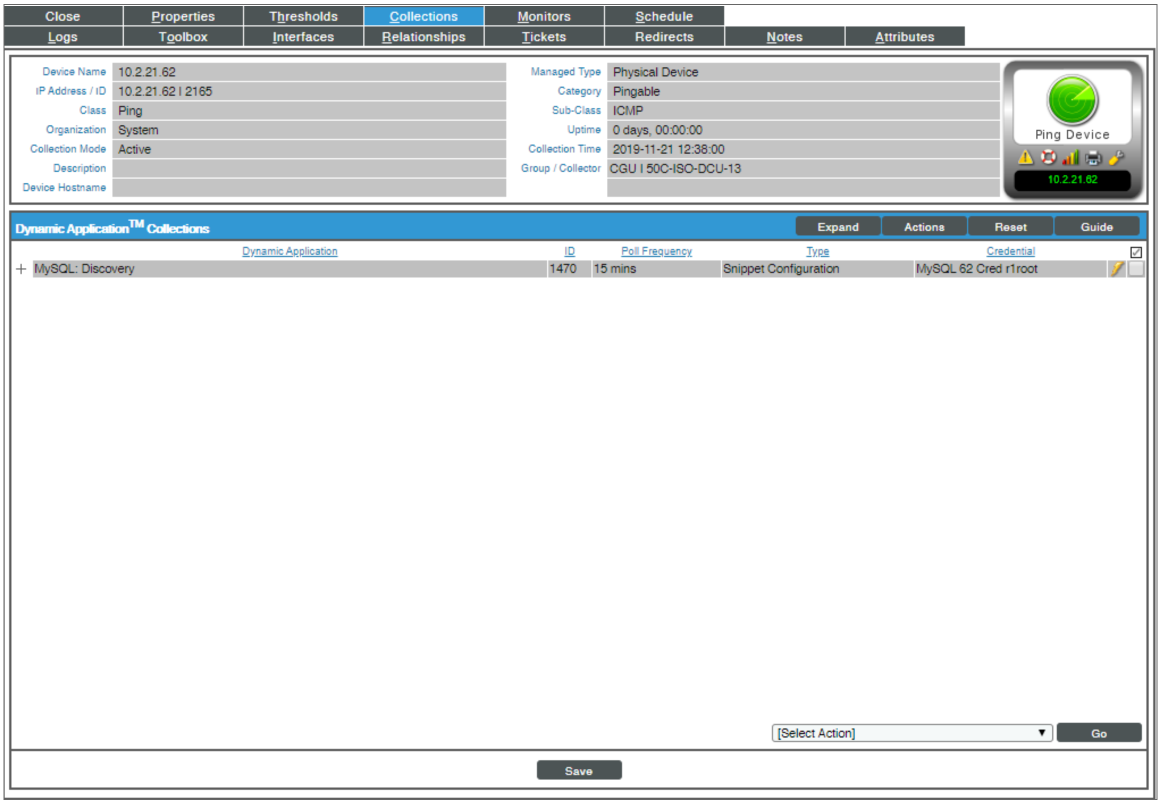
7. The **Discovery Session** window appears. When the cluster root device(s) are discovered, click the device icon ( ) to view the **Device Properties** page for each device.

Verifying Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery, perform the following steps:

1. After discovery has completed, click the device icon for the MySQL server (🖨).
2. From the **Device Properties** page for the MySQL server, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
3. The "MySQL: Discovery" Dynamic Application for the server is 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	10.2.21.62	Managed Type	Physical Device
IP Address / ID	10.2.21.62 I 2165	Category	Pingable
Class	Ping	Sub-Class	ICMP
Organization	System	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2019-11-21 12:38:00
Description		Group / Collector	CGU I 50C-ISO-DCU-13
Device Hostname			

Dynamic Application™ Collections

Dynamic Application	ID	Poll Frequency	Type	Credential	☑
+ MySQL: Discovery	1470	15 mins	Snippet Configuration	MySQL 62 Cred r1root	□

The MySQL server container will then be created and the "MySQL: Instance Discovery" Dynamic Application will auto-align to the server container. The MySQL server container will then discover, model, and monitor the remaining MySQL instances.

The following Dynamic Applications will auto-align to the MySQL instances:

- MySQL: Instance Commands Performance
- MySQL: Instance Handler Performance

- MySQL: Instance InnoDB Buffer Pool Performance
- MySQL: Instance InnoDB Data Performance
- MySQL: Instance InnoDB Row Performance
- MySQL: Instance Overall Performance
- MySQL: Instance Sort and Select Performance
- MySQL: Instance Table Locking Performance
- MySQL: Instance Threads and Connections Performance
- MySQL: Instance Configuration
- MySQL: Instance InnoDB Configuration

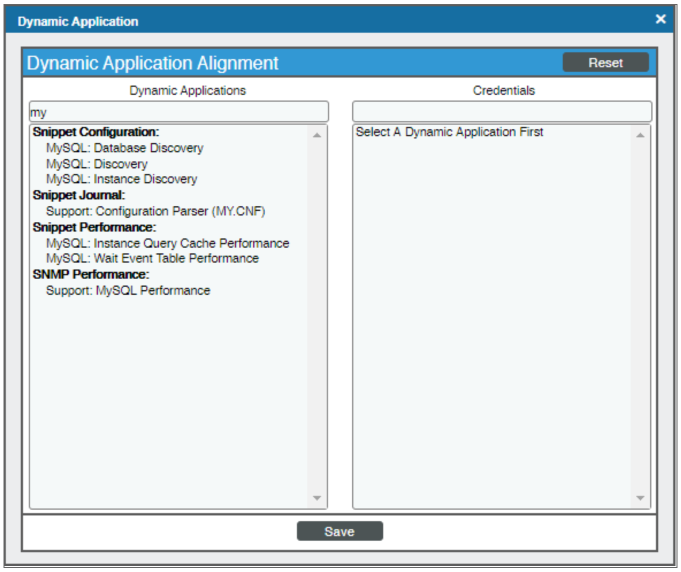
The following Dynamic Applications will not automatically align during discovery and will need to be manually aligned:

- MySQL: Events Errors Summary Configuration
- MySQL: Performance Schema Statements Configuration
- MySQL: Performance Schema Summary Statement Configuration
- MySQL: Process List Configuration
- MySQL: Statements With Error/Warning Configuration

NOTE: To collect data for the manually-aligned Dynamic Applications, you will need to enable the system database and performance_schema in the MySQL instance.

To manually align Dynamic Applications, perform the following steps:

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



my

Snippet Configuration:
MySQL: Database Discovery
MySQL: Discovery
MySQL: Instance Discovery
Snippet Journal:
Support: Configuration Parser (MY.CNF)
Snippet Performance:
MySQL: Instance Query Cache Performance
MySQL: Wait Event Table Performance
SNMP Performance:
Support: MySQL Performance

Select A Dynamic Application First

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.

Chapter 55

NetApp Base Pack

Overview

The following sections describe how to configure and discover NetApp appliances for monitoring in SL1 using the *NetApp Base Pack* PowerPack:

NOTE: For more information about the *NetApp Base Pack* PowerPack, see the ***Monitoring NetApp Appliances*** manual.

Prerequisites for Monitoring NetApp

Before you discover your NetApp appliances in your SL1 system, you must perform the following configuration tasks on each NetApp Appliance you want to discover:

- Configure a user account on the NetApp device that SL1 will use to connect to the NetApp API. The user account must be assigned a role that includes the following allowed capabilities:
  - login-http-admin
  - api-system-get-*
  - api-aggr-list-info
  - api-lun-list-info
  - api-volume-list-info
  - api-perf-object-get-instances
  - api-storage-shelf-environment-list-info
  - api-net-config-get-active
  - api-vfiler-list-info
  - api-disk-list-info
  - api-snapshot-list-info

> **NOTE**: For Clustered Data ONTAP 8.3 or later, the documentation for customizing the role of a user account is located in the *Clustered Data ONTAP 8.3 System Administration Guide for Cluster Administrators* in the section titled “Customizing an access-control role to restrict user access to specific commands”. To view the guide, go to https://library.netapp.com/ecm/ecm_get_file/ECMP1636037. You can download additional NetApp documentation from the NetApp Support Portal at http://mysupport.netapp.com.
>
> If you are discovering a Clustered Data ONTAP system, the user account you use for the ScienceLogic credential should be given the built-in "readonly" role and access to the "ontapi" application. For example:
>
> ```
> security login create [username] -application ontapi -role readonly -vserver
> [clustername]
> ```

- Determine whether connections to the API on your NetApp device require SSL.
- If you are discovering a NetApp v8 system, you must enable the NetApp multistore license. To do this, execute the following command on your NetApp appliance:

  ```
  options licensed_feature.multistore.enable on
  ```

Configuring NetApp Credentials

To use the Dynamic Applications in the *NetApp Base Pack* PowerPack, you must first define two or more NetApp credentials in SL1. These credentials allow SL1 to communicate with the NetApp appliances. The *NetApp Base Pack* PowerPack includes templates for the NetApp credentials.

The *NetApp Base Pack* PowerPack includes the following example credentials:

- ***NetApp 7-mode***. This Basic/Snippet type credential allows you to retrieve data from a NetApp 7-Mode appliance.
- ***NetApp w/SSL Option***. This SOAP/XML type credential allows you to retrieve data from a NetApp C-Mode device that uses SSL. In production, most NetApp C-Mode devices use SSL.
- ***NetApp w/SSL Option Off***. This SOAP/XML type credential allows you to retrieve data from a NetApp C-Mode device that does not use SSL.
- ***NetApp w/SSL/TLS Option***. This SOAP/XML type credential allows you to retrieve data from a NetApp C-Mode device that uses TLS.

NOTE: The user account configured for the credential must be assigned a role that includes "login-http-admin" and "api-system-get-*" as allowed capabilities.

In addition, during discovery you will use an SNMP credential to retrieve basic device data from the NetApp devices. You must determine the SNMP Community String for your NetApp devices and then decide whether you need to create a new SNMP credential or can use an existing SNMP credential.

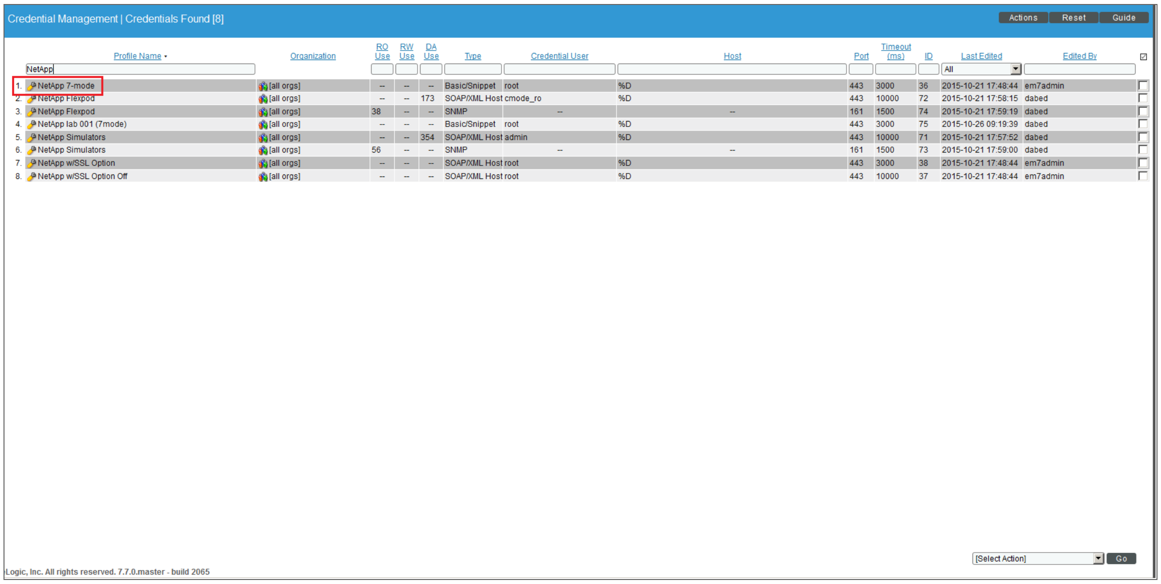
- If your NetApp devices use the same community string as other SNMP devices in your network, you can use an existing SNMP credential during discovery.
- If your NetApp devices use a different SNMP community string that the other SNMP devices in your network, you must create a new SNMP credential for the NetApp devices.

Creating a Credential for 7-Mode

> **NOTE:** If TLS is required for the discovery of a 7-mode NetApp system, the example credential provided will need to be replaced by a SOAP/XML credential, as described in the *Creating a Credential for C-Mode* section. In that case, the ***Embed Value [%1]*** field should be set to *True* and the TLS version should be entered in ***Embed Value [%2]***.

To modify the example credentials for use with your NetApp 7-Mode appliances, perform the following steps:

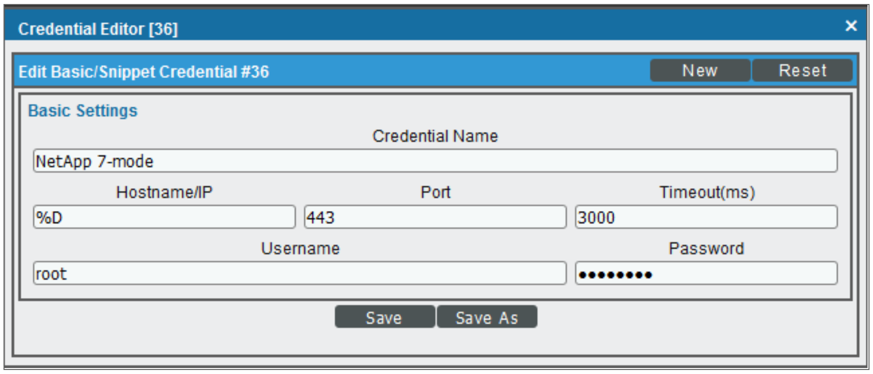
1. Go to the **Credential Management** page (System > Manage > Credentials).



Credential Management | Credentials Found [8]

	Profile Name	Organization	RO Use	RW Use	DA Use	Type	Credential User	Host	Port	Timeout (ms)	ID	Last Edited	Edited By	☑
	NetApp											All		
1.	NetApp 7-mode	[all orgs]	--	--	--	Basic/Snippet	root	%D	443	3000	36	2015-10-21 17:48:44	em7admin	□
2.	NetApp Flexpod	[all orgs]	--	--	173	SOAP/XML Host	cmode_ro	%D	443	10000	72	2015-10-21 17:58:15	dabed	□
3.	NetApp Flexpod	[all orgs]	38	--	--	SNMP	--	--	161	1500	74	2015-10-21 17:59:19	dabed	□
4.	NetApp lab 001 (7mode)	[all orgs]	--	--	--	Basic/Snippet	root	%D	443	3000	75	2015-10-26 09:19:39	dabed	□
5.	NetApp Simulators	[all orgs]	--	--	354	SOAP/XML Host	admin	%D	443	10000	71	2015-10-21 17:57:52	dabed	□
6.	NetApp Simulators	[all orgs]	56	--	--	SNMP	--	--	161	1500	73	2015-10-21 17:59:00	dabed	□
7.	NetApp w/SSL Option	[all orgs]	--	--	--	SOAP/XML Host	root	%D	443	3000	38	2015-10-21 17:48:44	em7admin	□
8.	NetApp w/SSL Option Off	[all orgs]	--	--	--	SOAP/XML Host	root	%D	443	10000	37	2015-10-21 17:48:44	em7admin	□

2. Click the wrench icon (🔧) for the ***NetApp 7-mode***. The **Credential Editor** modal window appears:



Credential Editor [36]

Edit Basic/Snippet Credential #36

Basic Settings

Credential Name: NetApp 7-mode		
Hostname/IP: %D	Port: 443	Timeout(ms): 3000
Username: root		Password: ••••••••

3. Supply values in the following fields:

   - ***Credential Name***. Enter a new name for the credential.

- ***Username***. Enter the username that SL1 will use to connect to the NetApp appliance.
- ***Password***. Enter the password for the username you entered in the ***HTTP Auth User*** field.

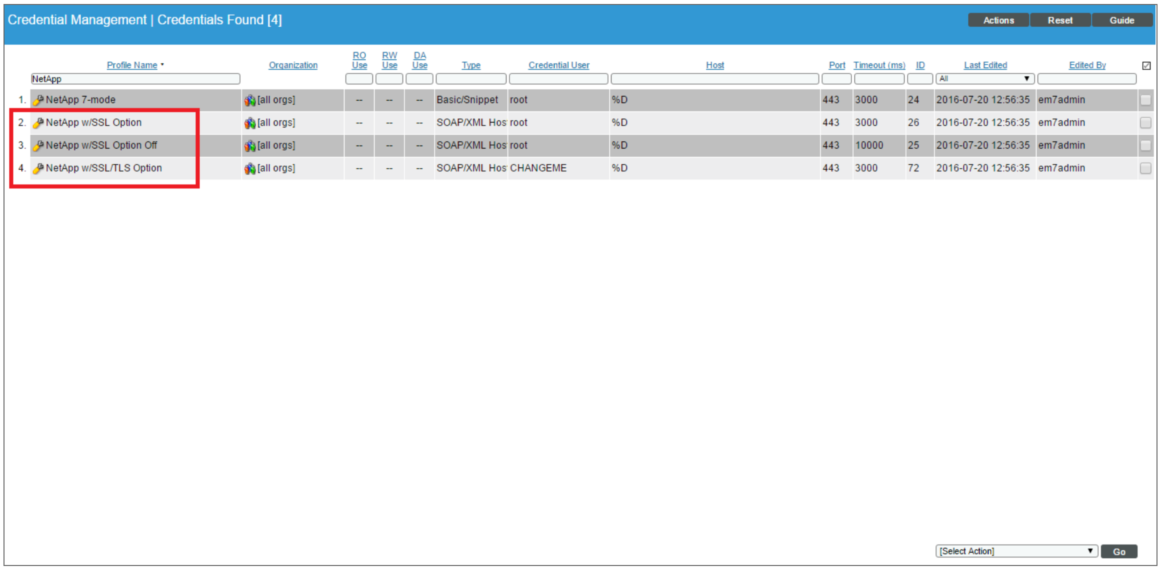
> **NOTE**: The user account configured for the credential must be assigned a role that includes "login-http-admin" and "api-system-get-*" as allowed capabilities.

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

Creating a Credential for C-Mode

To modify the example credentials for use with your NetApp C-Mode appliances, perform the following steps:

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

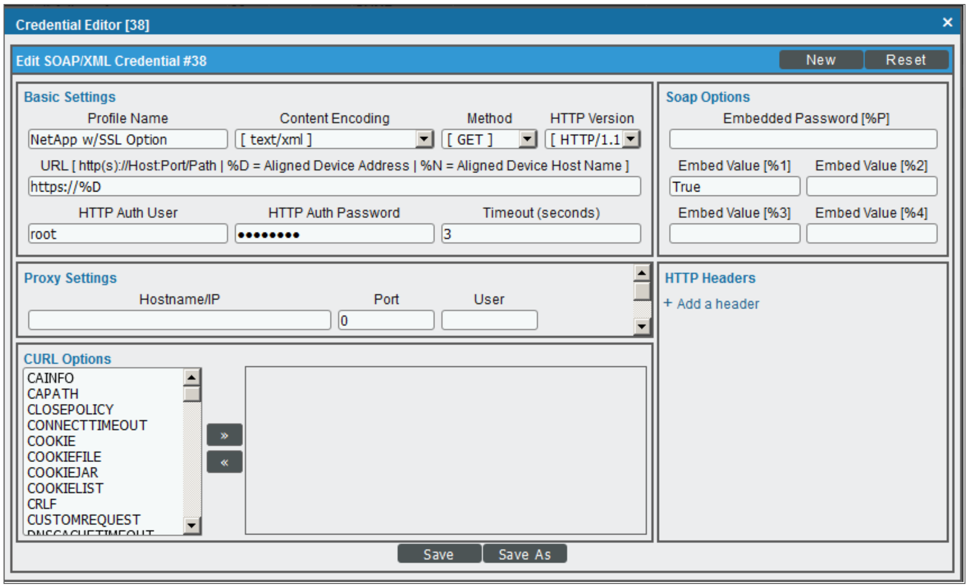


Credential Management | Credentials Found [4]

	Profile Name	Organization	RO Use	RW Use	DA Use	Type	Credential User	Host	Port	Timeout (ms)	ID	Last Edited	Edited By	☑
	NetApp											All		
1.	NetApp 7-mode	[all orgs]	--	--	--	Basic/Snippet	root	%D	443	3000	24	2016-07-20 12:56:35	em7admin	□
2.	NetApp w/SSL Option	[all orgs]	--	--	--	SOAP/XML Hos	root	%D	443	3000	26	2016-07-20 12:56:35	em7admin	□
3.	NetApp w/SSL Option Off	[all orgs]	--	--	--	SOAP/XML Hos	root	%D	443	10000	25	2016-07-20 12:56:35	em7admin	□
4.	NetApp w/SSL/TLS Option	[all orgs]	--	--	--	SOAP/XML Hos	CHANGEME	%D	443	3000	72	2016-07-20 12:56:35	em7admin	□

- If you want SL1 to use SSL when connecting to the NetApp device, click the wrench icon (🔧) for the ***NetApp w/SSL Option*** credential.
- If you do not want SL1 to use SSL or TLS when connecting to the NetApp device, click the wrench icon (🔧) for the ***NetApp w/SSL Option Off*** credential.
- If you want SL1 to use TLS when connecting to the NetApp device, click the wrench icon (🔧) for the ***NetApp w/SSL/TLS Option*** credential.

The **Credential Editor** modal window appears:


Credential Editor [38]

Edit SOAP/XML Credential #38

Basic Settings

Profile Name: NetApp w/SSL Option

Content Encoding: [text/xml]

Method: [GET]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://%D

HTTP Auth User: root

HTTP Auth Password: ●●●●●●●●

Timeout (seconds): 3

Soap Options

Embedded Password [%P]:

Embed Value [%1]: True

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

Proxy Settings

Hostname/IP:

Port: 0

User:

HTTP Headers

CURL Options

3. Supply values in the following fields:

    - ***Profile Name***. Type a new name for the credential.
    - ***URL***. Use the provided value of "https://%D".
    - ***HTTP Auth User***. Type the username that SL1 will use to connect to the NetApp appliance.
    - ***HTTP Auth Password***. Type the password for the username you entered in the ***HTTP Auth User*** field.
    - ***Embed Value [%1]***. Type "True" if you want SL1 to use SSL or TLS when connecting to the NetApp device, or if you are discovering a 7-mode NetApp system in which TLS is required. Type "False" if you do not want SL1 to use SSL or TLS when connecting to the NetApp device.
    - ***Embed Value [%2]***. Type one of the following, depending on the version of TLS you use, if you want SL1 to use TLS when connecting to the NetApp device: "TLSv1.0", "TLSv1.1", or "TLSv1.2". Otherwise, keep this field blank.
    - ***Port***. If SL1 is running in FIPS-compliant mode, set the port to 80.

NOTE: The user account configured for the credential must be assigned a role that includes "login-http-admin" and "api-system-get-*" as allowed capabilities.

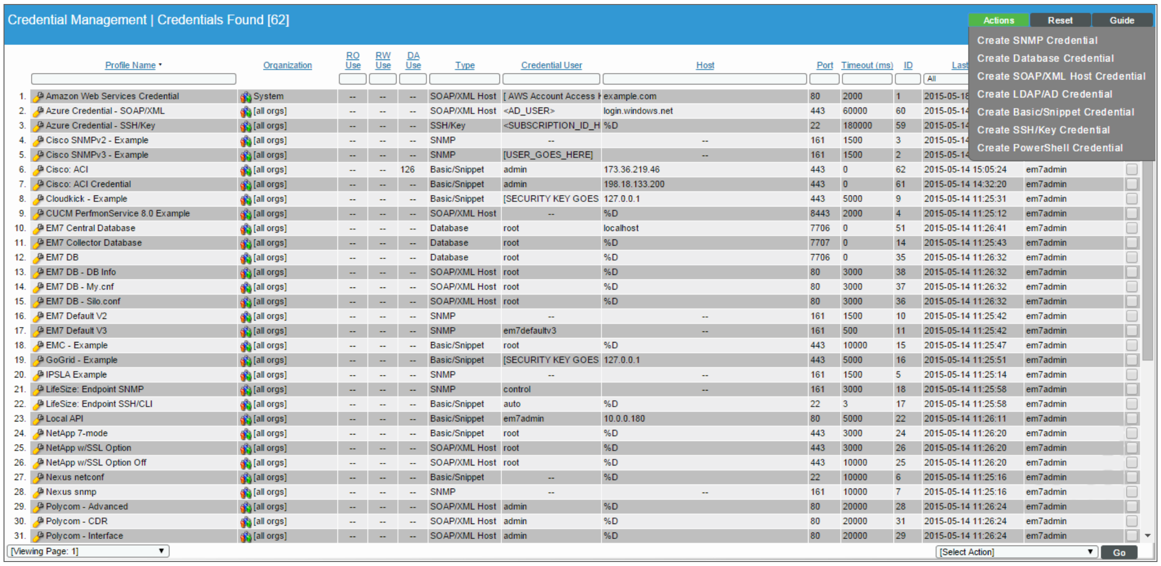
4. Click the **[Save As]** button.

Creating an SNMP Credential

SNMP Credentials allow SL1 to access SNMP data on a managed device. SL1 uses SNMP credentials to perform discovery, run auto-discovery, and gather information from SNMP Dynamic Applications.

To create an SNMP credential:

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



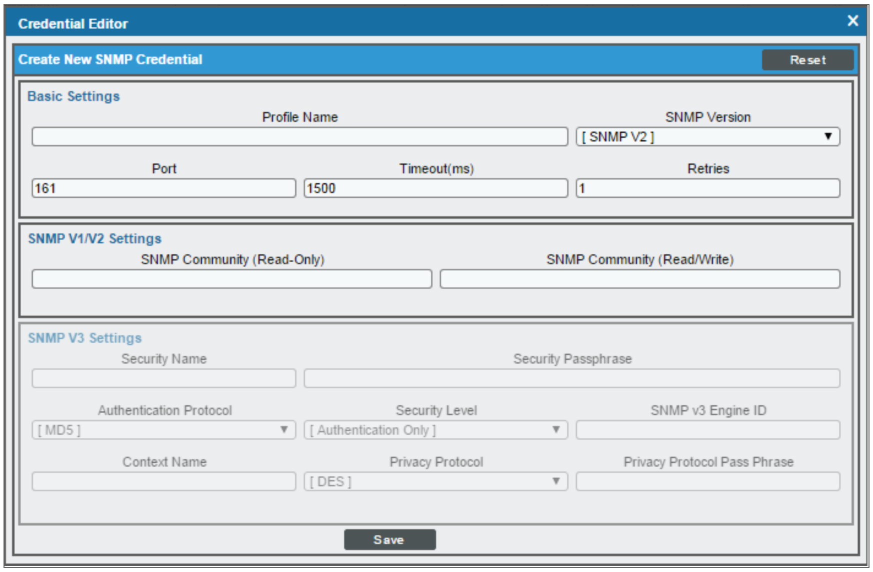
Credential Management | Credentials Found [62]

Actions
Reset
Guide
Create SNMP Credential
Create Database Credential
Create SOAP/XML Host Credential
Create LDAP/AD Credential
Create Basic/Snippet Credential
Create SSH/Key Credential
Create PowerShell Credential

	Profile Name ▾	Organization	RO Use	RW Use	DA Use	Type	Credential User	Host	Port	Timeout (ms)	ID	Last		
												All		
1.	Amazon Web Services Credential	System	--	--	--	SOAP/XML Host	[AWS Account Access I	example.com	80	2000	1	2015-05-18		
2.	Azure Credential - SOAP/XML	[all orgs]	--	--	--	SOAP/XML Host	<AD_USER>	login.windows.net	443	60000	60	2015-05-14		
3.	Azure Credential - SSH/Key	[all orgs]	--	--	--	SSH/Key	<SUBSCRIPTION_ID_H	%D	22	180000	59	2015-05-14		
4.	Cisco SNMPv2 - Example	[all orgs]	--	--	--	SNMP	--	--	161	1500	3	2015-05-14		
5.	Cisco SNMPv3 - Example	[all orgs]	--	--	--	SNMP	[USER_GOES_HERE]	--	161	1500	2	2015-05-14		
6.	Cisco: ACI	[all orgs]	--	--	126	Basic/Snippet	admin	173.36.219.46	443	0	62	2015-05-14 15:05:24	em7admin	☐
7.	Cisco: ACI Credential	[all orgs]	--	--	--	Basic/Snippet	admin	198.18.133.200	443	0	61	2015-05-14 14:32:20	em7admin	☐
8.	Cloudkick - Example	[all orgs]	--	--	--	Basic/Snippet	[SECURITY KEY GOES	127.0.0.1	443	5000	9	2015-05-14 11:25:31	em7admin	☐
9.	CUCM PerfmonService 8.0 Example	[all orgs]	--	--	--	SOAP/XML Host	--	%D	8443	2000	4	2015-05-14 11:25:12	em7admin	☐
10.	EM7 Central Database	[all orgs]	--	--	--	Database	root	localhost	7706	0	51	2015-05-14 11:26:41	em7admin	☐
11.	EM7 Collector Database	[all orgs]	--	--	--	Database	root	%D	7707	0	14	2015-05-14 11:25:43	em7admin	☐
12.	EM7 DB	[all orgs]	--	--	--	Database	root	%D	7706	0	35	2015-05-14 11:26:32	em7admin	☐
13.	EM7 DB - DB Info	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	38	2015-05-14 11:26:32	em7admin	☐
14.	EM7 DB - My.cnf	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	37	2015-05-14 11:26:32	em7admin	☐
15.	EM7 DB - Silo.conf	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	36	2015-05-14 11:26:32	em7admin	☐
16.	EM7 Default V2	[all orgs]	--	--	--	SNMP	--	--	161	1500	10	2015-05-14 11:25:42	em7admin	☐
17.	EM7 Default V3	[all orgs]	--	--	--	SNMP	em7defaultv3	--	161	500	11	2015-05-14 11:25:42	em7admin	☐
18.	EMC - Example	[all orgs]	--	--	--	Basic/Snippet	root	%D	443	10000	15	2015-05-14 11:25:47	em7admin	☐
19.	GoGrid - Example	[all orgs]	--	--	--	Basic/Snippet	[SECURITY KEY GOES	127.0.0.1	443	5000	16	2015-05-14 11:25:51	em7admin	☐
20.	IPSLA Example	[all orgs]	--	--	--	SNMP	--	--	161	1500	5	2015-05-14 11:25:14	em7admin	☐
21.	LifeSize: Endpoint SNMP	[all orgs]	--	--	--	SNMP	control	--	161	3000	18	2015-05-14 11:25:58	em7admin	☐
22.	LifeSize: Endpoint SSH/CLI	[all orgs]	--	--	--	Basic/Snippet	auto	%D	22	3	17	2015-05-14 11:25:58	em7admin	☐
23.	Local API	[all orgs]	--	--	--	Basic/Snippet	em7admin	10.0.0.180	80	5000	22	2015-05-14 11:26:11	em7admin	☐
24.	NetApp 7-mode	[all orgs]	--	--	--	Basic/Snippet	root	%D	443	3000	24	2015-05-14 11:26:20	em7admin	☐
25.	NetApp w/SSL Option	[all orgs]	--	--	--	SOAP/XML Host	root	%D	443	3000	26	2015-05-14 11:26:20	em7admin	☐
26.	NetApp w/SSL Option Off	[all orgs]	--	--	--	SOAP/XML Host	root	%D	443	10000	25	2015-05-14 11:26:20	em7admin	☐
27.	Nexus netconf	[all orgs]	--	--	--	Basic/Snippet	--	%D	22	10000	6	2015-05-14 11:25:16	em7admin	☐
28.	Nexus snmp	[all orgs]	--	--	--	SNMP	--	--	161	10000	7	2015-05-14 11:25:16	em7admin	☐
29.	Polycom - Advanced	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	28	2015-05-14 11:26:24	em7admin	☐
30.	Polycom - CDR	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	31	2015-05-14 11:26:24	em7admin	☐
31.	Polycom - Interface	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	29	2015-05-14 11:26:24	em7admin	☐

[Viewing Page: 1] ▾ [Select Action] ▾ Go

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



Credential Editor ×

Create New SNMP Credential — Reset

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:

Save

3. Supply values in the following fields:
   - ***Profile Name***. Name of the credential. Can be any combination of alphanumeric characters.
   - ***SNMP Version***. SNMP version. Choices are *SNMP V1*, *SNMP V2*, and *SNMP V3*. The default value is *SNMP V2*.
   - ***Port***. The port SL1 will use to communicate with the external device or application. The default value is *161*.

- ***Timeout (ms)***. Time, in milliseconds, after which SL1 will stop trying to communicate with the SNMP device. The default value is *1500*.
- ***Retries***. Number of times SL1 will try to authenticate and communicate with the external device. The default value is *1*.

SNMP V1/V2 Settings

These fields appear if you selected *SNMP V1* or *SNMP V2* in the ***SNMP Version*** field. The fields are inactive if you selected SNMP V3.

- ***SNMP Community (Read-Only)***. The SNMP community string (password) required for read-only access of SNMP data on the remote device or application. For SNMP V1 and SNMP V2 credentials, you must supply a community string, either in this field or in the ***SNMP Community (Read/Write)*** field.
- ***SNMP Community (Read/Write)***. The SNMP community string (password) required for read and write access of SNMP data on the remote device or application. For SNMP V1 and SNMP V2 credentials, you must supply a community string, either in this field or in the ***SNMP Community (Read Only)*** field.

SNMP V3 Settings

These fields appear if you selected *SNMP V3* in the ***SNMP Version*** field. These fields are inactive if you selected SNMP V1 or SNMP V2.

- ***Security Name***. Name for SNMP authentication. This field is required.
- ***Security Passphrase***. Password to authenticate the credential. This value must contain at least 8 characters. This value is required if you use a ***Security Level*** that includes authentication.
- ***Authentication Protocol***. Select an authentication algorithm for the credential. This field is required. Choices are:
  - *MD5*. This is the default value.
  - *SHA*
  - *SHA-224*
  - *SHA-256*
  - *SHA-384*
  - *SHA-512*

NOTE: The *SHA* option is SHA-128.

- ***Security Level***. Specifies the combination of security features for the credentials. This field is required. Choices are:
  - *No Authentication / No Encryption*.
  - *Authentication Only*. This is the default value.
  - *Authentication and Encryption*.
- ***SNMP v3 Engine ID***. The unique engine ID for the SNMP agent you want to communicate with. (SNMPv3 authentication and encryption keys are generated based on the associated passwords and the engine ID.) This field is optional.
- ***Context Name***. A context is a mechanism within SNMPv3 (and AgentX) that allows you to use parallel versions of the same MIB objects. For example, one version of a MIB might be associated with SNMP Version 2 and another version of the same MIB might be associated with SNMP Version 3. For SNMP Version 3, specify the context name in this field. This field is optional.
- ***Privacy Protocol***. The privacy service encryption and decryption algorithm. This field is required. Choices are:
  - *DES*. This is the default value.
  - *AES-128*
  - *AES-192*
  - *AES-256*
- ***Privacy Protocol Passphrase***. Privacy password for the credential. This field is optional.

4. Click the **[Save]** button to save the new SNMP credential.
5. Repeat steps 1-4 for each SNMP-enabled device in your network that you want to monitor with SL1.

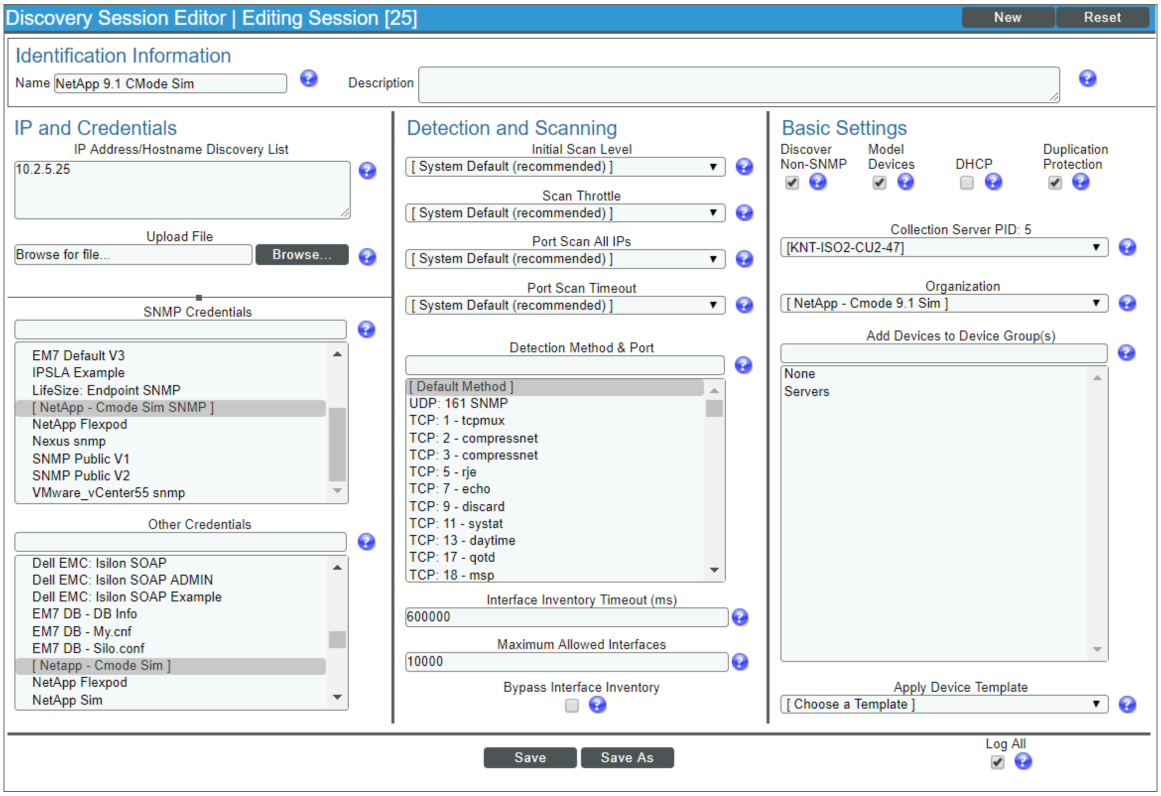
NOTE: When you define an SNMP Credential, SL1 automatically aligns the credential with all organizations of which you are a member.

Discovering a NetApp Appliance

To create and run a discovery session that will discover a NetApp appliance, perform the following steps:

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

2. Click the **[Create]** button to create a new discovery session. The **Discovery Session Editor** window appears:



Discovery Session Editor | Editing Session [25]

New Reset

Identification Information

Name: NetApp 9.1 CMode Sim

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.2.5.25

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

SNMP Credentials:

- EM7 Default V3
- IPSLA Example
- LifeSize: Endpoint SNMP
- [NetApp - Cmode Sim SNMP]
- NetApp Flexpod
- Nexus snmp
- SNMP Public V1
- SNMP Public V2
- VMware_vCenter55 snmp

Other Credentials:

- Dell EMC: Isilon SOAP
- Dell EMC: Isilon SOAP ADMIN
- Dell EMC: Isilon SOAP Example
- EM7 DB - DB Info
- EM7 DB - My.cnf
- EM7 DB - Silo.conf
- [Netapp - Cmode Sim]
- NetApp Flexpod
- NetApp Sim

Detection and Scanning

Initial Scan Level: [System Default (recommended)]

Scan Throttle: [System Default (recommended)]

Port Scan All IPs: [System Default (recommended)]

Port Scan Timeout: [System Default (recommended)]

Detection Method & Port:

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

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: [KNT-ISO2-CU2-47]

Organization: [NetApp - Cmode 9.1 Sim]

Add Devices to Device Group(s):

- None
- Servers

Apply Device Template: [Choose a Template]

Save Save As

Log All: ☑

3. Enter values in the following fields:

   - ***IP Address Discovery List***. Enter the IP address for the NetApp appliance. This can be the address for a single filer (in the case of 7-mode) or the IP address for a cluster (in the case of clustered Data ONTAP).
   - ***SNMP Credential***. Select an SNMP credential to use with the NetApp appliance.
   - ***Other Credentials***. Select the credential that you configured in the previous section.

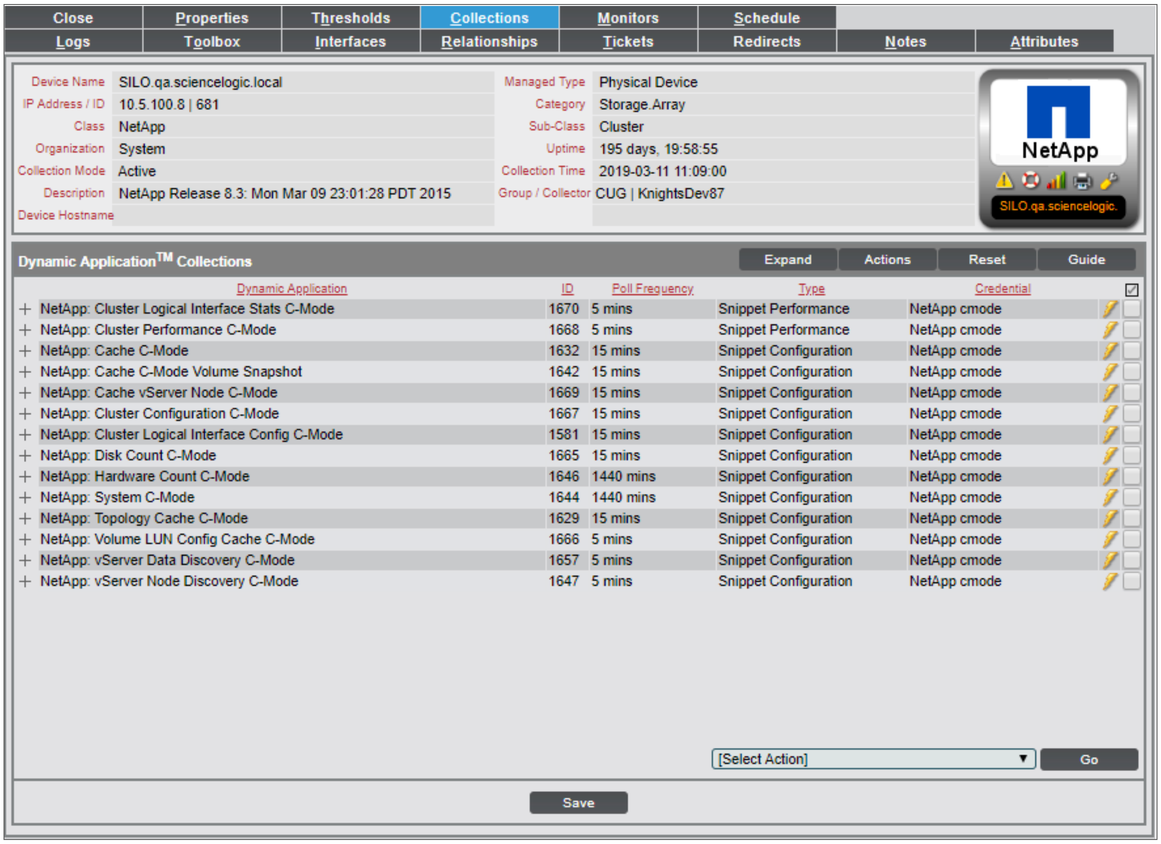
4. You can enter values in the other fields on this page, but are not required to and can simply accept the default values. For more information about the other fields on this page, see the ***Discovery & Credentials*** manual.
5. Click the **[Save]** button and then close the **Discovery Session Editor** window.
6. The discovery session you created will appear at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon ( ) to run the discovery session.
7. The **Discovery Session** window will be displayed.
8. When the NetApp appliance is discovered, click its device icon ( ) to view the **Device Properties** page for the NetApp appliance.

Verifying Discovery and Dynamic Applications

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

NOTE: It can take several minutes after discovery for Dynamic Applications to appear on the **Dynamic Application Collections** page. If the specified Dynamic Applications do not appear on this page, try clicking the **[Reset]** button.

1. From the **Device Properties** page for the NetApp appliance, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. If the NetApp appliance is a C-Mode device, the following Dynamic Applications should be displayed in the list of Dynamic Applications aligned to the NetApp appliance:



Device Name	SILO.qa.sciencelogic.local	Managed Type	Physical Device
IP Address / ID	10.5.100.8 | 681	Category	Storage.Array
Class	NetApp	Sub-Class	Cluster
Organization	System	Uptime	195 days, 19:58:55
Collection Mode	Active	Collection Time	2019-03-11 11:09:00
Description	NetApp Release 8.3: Mon Mar 09 23:01:28 PDT 2015	Group / Collector	CUG | KnightsDev87
Device Hostname			

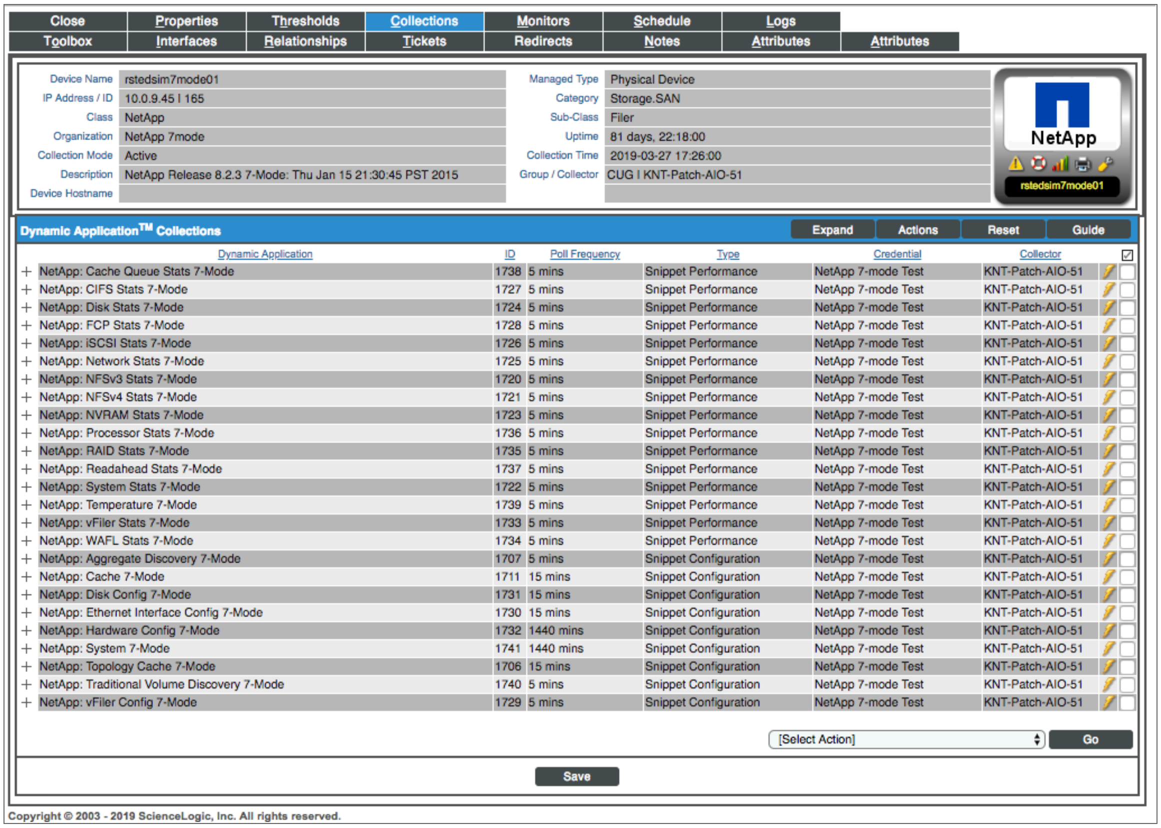
Dynamic Application™ Collections

Dynamic Application	ID	Poll Frequency	Type	Credential
NetApp: Cluster Logical Interface Stats C-Mode	1670	5 mins	Snippet Performance	NetApp cmode
NetApp: Cluster Performance C-Mode	1668	5 mins	Snippet Performance	NetApp cmode
NetApp: Cache C-Mode	1632	15 mins	Snippet Configuration	NetApp cmode
NetApp: Cache C-Mode Volume Snapshot	1642	15 mins	Snippet Configuration	NetApp cmode
NetApp: Cache vServer Node C-Mode	1669	15 mins	Snippet Configuration	NetApp cmode
NetApp: Cluster Configuration C-Mode	1667	15 mins	Snippet Configuration	NetApp cmode
NetApp: Cluster Logical Interface Config C-Mode	1581	15 mins	Snippet Configuration	NetApp cmode
NetApp: Disk Count C-Mode	1665	15 mins	Snippet Configuration	NetApp cmode
NetApp: Hardware Count C-Mode	1646	1440 mins	Snippet Configuration	NetApp cmode
NetApp: System C-Mode	1644	1440 mins	Snippet Configuration	NetApp cmode
NetApp: Topology Cache C-Mode	1629	15 mins	Snippet Configuration	NetApp cmode
NetApp: Volume LUN Config Cache C-Mode	1666	5 mins	Snippet Configuration	NetApp cmode
NetApp: vServer Data Discovery C-Mode	1657	5 mins	Snippet Configuration	NetApp cmode
NetApp: vServer Node Discovery C-Mode	1647	5 mins	Snippet Configuration	NetApp cmode

- NetApp: Cache C-Mode
- NetApp: Cache C-Mode Volume Snapshot
- NetApp: Cache vServer Node C-Mode
- NetApp: Cluster Configuration C-Mode
- NetApp: Cluster Logical Interface Config C-Mode

- NetApp: Cluster Logical Interface Stats C-Mode
- NetApp: Cluster Performance C-Mode
- NetApp: Disk Count C-Mode
- NetApp: Hardware Count C-Mode
- NetApp: System C-Mode
- NetApp: Topology Cache C-Mode
- NetApp: Volume LUN Config Cache C-Mode
- NetApp: vServer Data Discovery C-Mode
- NetApp: vServer Node Discovery C-Mode

3. If the NetApp appliance is a 7-Mode device, the following Dynamic Applications should be displayed in the list of Dynamic Applications aligned to the NetApp appliance:



Device Name	rstedsim7mode01	Managed Type	Physical Device
IP Address / ID	10.0.9.45 I 165	Category	Storage.SAN
Class	NetApp	Sub-Class	Filer
Organization	NetApp 7mode	Uptime	81 days, 22:18:00
Collection Mode	Active	Collection Time	2019-03-27 17:26:00
Description	NetApp Release 8.2.3 7-Mode: Thu Jan 15 21:30:45 PST 2015	Group / Collector	CUG I KNT-Patch-AIO-51
Device Hostname			

Dynamic Application™ Collections

Dynamic Application	ID	Poll Frequency	Type	Credential	Collector	☑
NetApp: Cache Queue Stats 7-Mode	1738	5 mins	Snippet Performance	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: CIFS Stats 7-Mode	1727	5 mins	Snippet Performance	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: Disk Stats 7-Mode	1724	5 mins	Snippet Performance	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: FCP Stats 7-Mode	1728	5 mins	Snippet Performance	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: iSCSI Stats 7-Mode	1726	5 mins	Snippet Performance	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: Network Stats 7-Mode	1725	5 mins	Snippet Performance	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: NFSv3 Stats 7-Mode	1720	5 mins	Snippet Performance	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: NFSv4 Stats 7-Mode	1721	5 mins	Snippet Performance	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: NVRAM Stats 7-Mode	1723	5 mins	Snippet Performance	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: Processor Stats 7-Mode	1736	5 mins	Snippet Performance	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: RAID Stats 7-Mode	1735	5 mins	Snippet Performance	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: Readahead Stats 7-Mode	1737	5 mins	Snippet Performance	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: System Stats 7-Mode	1722	5 mins	Snippet Performance	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: Temperature 7-Mode	1739	5 mins	Snippet Performance	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: vFiler Stats 7-Mode	1733	5 mins	Snippet Performance	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: WAFL Stats 7-Mode	1734	5 mins	Snippet Performance	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: Aggregate Discovery 7-Mode	1707	5 mins	Snippet Configuration	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: Cache 7-Mode	1711	15 mins	Snippet Configuration	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: Disk Config 7-Mode	1731	15 mins	Snippet Configuration	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: Ethernet Interface Config 7-Mode	1730	15 mins	Snippet Configuration	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: Hardware Config 7-Mode	1732	1440 mins	Snippet Configuration	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: System 7-Mode	1741	1440 mins	Snippet Configuration	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: Topology Cache 7-Mode	1706	15 mins	Snippet Configuration	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: Traditional Volume Discovery 7-Mode	1740	5 mins	Snippet Configuration	NetApp 7-mode Test	KNT-Patch-AIO-51	□
NetApp: vFiler Config 7-Mode	1729	5 mins	Snippet Configuration	NetApp 7-mode Test	KNT-Patch-AIO-51	□

- NetApp: Aggregate Discovery 7-Mode
- NetApp: Cache 7-Mode
- NetApp: Cache Queue Stats 7-Mode
- NetApp: CIFS Stats 7-Mode
- NetApp: Disk Config 7-Mode

- NetApp: Disk Stats 7-Mode
- NetApp: Ethernet Interface Config 7-Mode
- NetApp: FCP Stats 7-Mode
- NetApp: Hardware Config 7-Mode
- NetApp: iSCSI Stats 7-Mode
- NetApp: Network Stats 7-Mode
- NetApp: NFSv3 Stats 7-Mode
- NetApp: NFSv4 Stats 7-Mode
- NetApp: NVRAM Stats 7-Mode
- NetApp: Processor Stats 7-Mode
- NetApp: RAID Stats 7-Mode
- NetApp: Readahead Stats 7-Mode
- NetApp: System 7-Mode
- NetApp: System Stats 7-Mode
- NetApp: Temperature 7-Mode
- NetApp: Topology Cache 7-Mode
- NetApp: Traditional Volume Discovery 7-Mode
- NetApp: vFiler Config 7-Mode
- NetApp: vFiler Stats 7-Mode
- NetApp: WAFL Stats 7-Mode

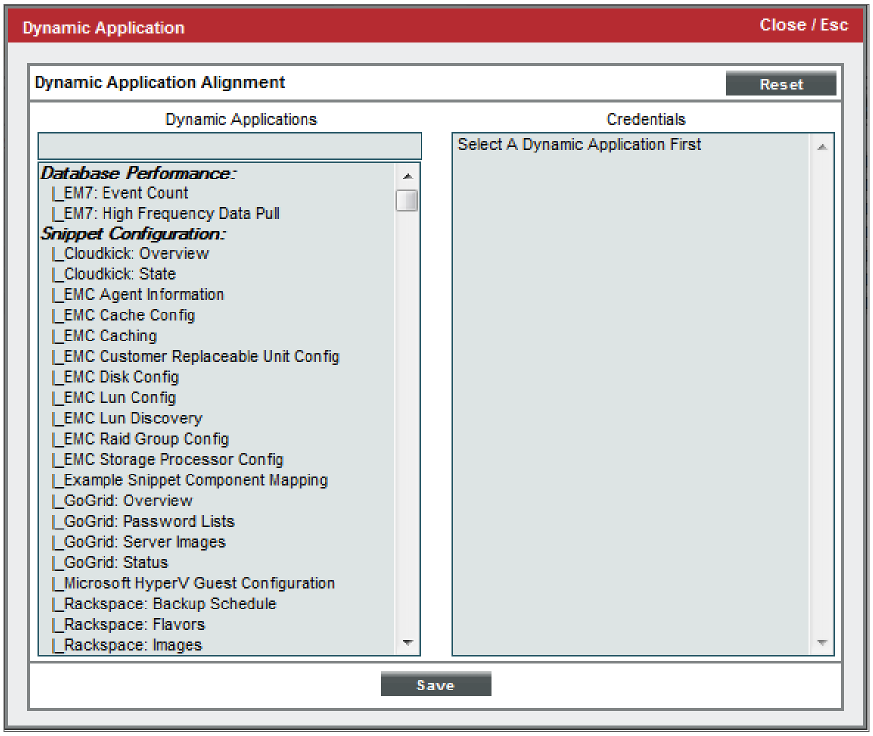
4. If one or more of these Dynamic Applications are not automatically aligned with each NetApp device, follow the instructions in the section on ***Manually Aligning the Dynamic Applications***.

Manually Aligning the Dynamic Applications

If the Dynamic Applications have not been automatically aligned, you can align them manually:

1. From the **Device Properties** page for the NetApp appliance, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.

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



Select A Dynamic Application First

Database Performance:
- |_EM7: Event Count
- |_EM7: High Frequency Data Pull

Snippet Configuration:
- |_Cloudkick: Overview
- |_Cloudkick: State
- |_EMC Agent Information
- |_EMC Cache Config
- |_EMC Caching
- |_EMC Customer Replaceable Unit Config
- |_EMC Disk Config
- |_EMC Lun Config
- |_EMC Lun Discovery
- |_EMC Raid Group Config
- |_EMC Storage Processor Config
- |_Example Snippet Component Mapping
- |_GoGrid: Overview
- |_GoGrid: Password Lists
- |_GoGrid: Server Images
- |_GoGrid: Status
- |_Microsoft HyperV Guest Configuration
- |_Rackspace: Backup Schedule
- |_Rackspace: Flavors
- |_Rackspace: Images

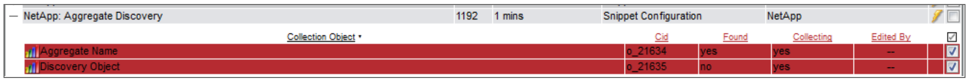
3. In the ***Dynamic Applications*** field, select the Dynamic Application you want to align.

4. In the ***Credentials*** field, select the credential *you created for this NetApp appliance*.

5. Click the **[Save]** button.

6. Repeat steps 2-5 for the remaining Dynamic Applications to align with the C-mode or 7-Mode NetApp appliance.

7. After aligning the Dynamic Applications, click the **[Reset]** button and then click the plus icon (+) for the Dynamic Application. If collection for the Dynamic Application was successful, the graph icons (📊) for the Dynamic Application are enabled:



— NetApp: Aggregate Discovery		1192	1 mins	Snippet Configuration	NetApp		□
Collection Object ▾	Cid	Found	Collecting	Edited By			☑
📊 Aggregate Name	o_21634	yes	yes	--			☑
📊 Discovery Object	o_21635	no	yes	--			☑

8. Click a graph icon (📊) to view the collected data. The **Configuration Report** page will display the number of components of each type and the total number of components managed by the NetApp appliance.

Relationships with Other Types of Component Devices

SL1 can automatically build relationships between NetApp component devices and other associated devices. If you discover a vCenter device using the Dynamic Applications in the *VMware: vSphere Base Pack* PowerPack, SL1 will automatically create relationships between NetApp LUNs and VMware Datastores, where appropriate.

Chapter 56

New Relic: APM

Overview

The following sections describe how to configure and discover New Relic services for monitoring by SL1 using the *New Relic: APM* PowerPack:

NOTE: For more information about the *New Relic: APM* PowerPack, see the ***Monitoring New Relic*** manual.

Prerequisites for Monitoring New Relic Services

To configure the SL1 system to monitor New Relic services using the *New Relic: APM* PowerPack, you must first have the following information about the New Relic services that you want to monitor *for each account and sub-account*:

- A New Relic REST API key. To generate the REST API key, go to the Account Settings page for your New Relic account.
- The username and password for your New Relic service.
- Insights Query Key. This is optional. Add this to the credential if you want to discover infrastructure groups used for server monitoring. You can generate this from your Insights account.

> **NOTE:** Ensure that you do not have the *New Relic: APM Pro* PowerPack installed before installing the *New Relic: APM* PowerPack. These PowerPacks are not compatible. If you have the *New Relic: APM Pro* PowerPack installed, it will need to be uninstalled prior to installing the *New Relic: APM* PowerPack. The historical data from the *New Relic: APM Pro* PowerPack will be deleted when it is uninstalled.

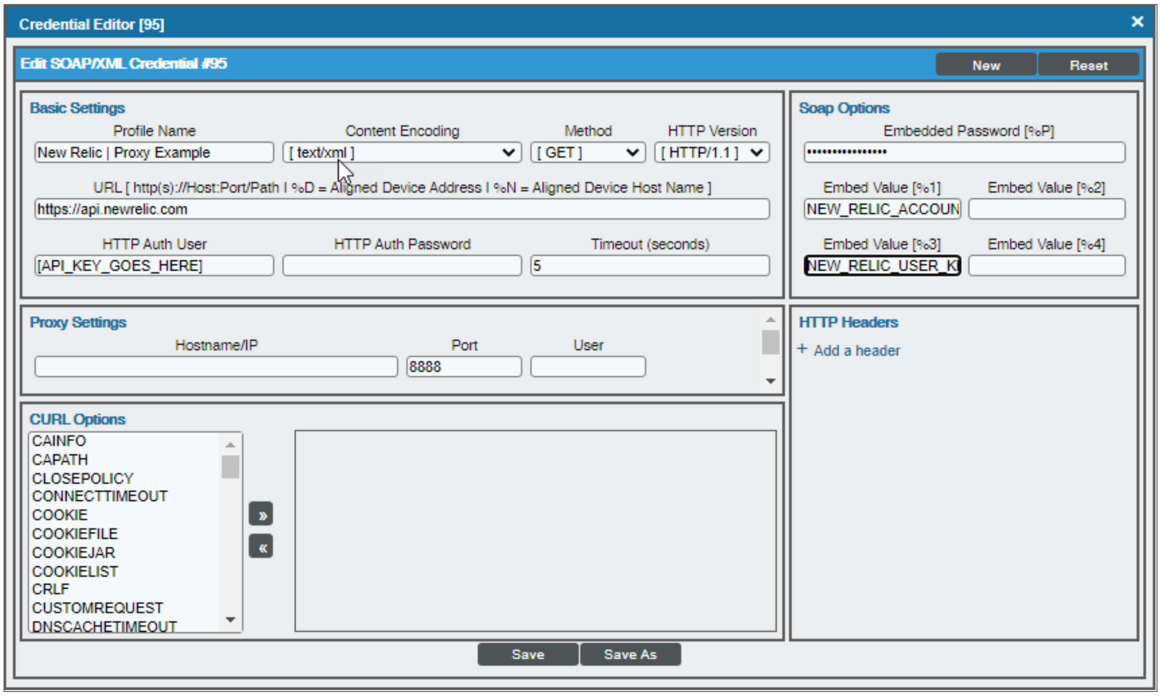
Creating a SOAP/XML Credential for New Relic

To configure SL1 to monitor New Relic services, you must create a SOAP/XML credential. This credential allows the Dynamic Applications in the *New Relic: APM* PowerPack to communicate with your New Relic service.

To configure a SOAP/XML credential to access New Relic:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **New Relic | Proxy Example** credential, and then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears.

3. Enter values in the following fields:



Credential Editor [95]

Edit SOAP/XML Credential #95

Basic Settings

Profile Name: New Relic | Proxy Example

Content Encoding: [text/xml]

Method: [GET]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://api.newrelic.com

HTTP Auth User: [API_KEY_GOES_HERE]

HTTP Auth Password:

Timeout (seconds): 5

Soap Options

Embedded Password [%P]: ••••••••••••••••

Embed Value [%1]: NEW_RELIC_ACCOUN

Embed Value [%2]:

Embed Value [%3]: NEW_RELIC_USER_K

Embed Value [%4]:

Proxy Settings

Hostname/IP:

Port: 8888

User:

HTTP Headers

+ Add a header

CURL Options

CAINFO
CAPATH
CLOSEPOLICY
CONNECTTIMEOUT
COOKIE
COOKIEFILE
COOKIEJAR
COOKIELIST
CRLF
CUSTOMREQUEST
DNSCACHETIMEOUT

Basic Settings

- ***Profile Name***. Type a new name for the credential.
- ***URL***. Leave this field as the default ("https://api.newrelic.com").
- ***HTTP Auth User***. Type your New Relic API key in this field.
- ***HTTP Auth Password***. Leave this field blank.

SOAP Options

- ***Embedded Password [%P]***. Type the Insights Query Key in this field if you want to discover infrastructure groups for server monitoring. If you do not have an Insights account, leave this field blank.
- ***Embed Value [%1]***. Type the ID number for your New Relic account.
- ***Embed Value [%3]***. To collect data with New Relic object tags, you must enter a New Relic user key into this field. New Relic user keys begin with "NRAK-" followed by an alpha-numeric value. Leave this field blank if you do not wish to collect tags.

NOTE: There are several system-defined tags that are automatically applied by New Relic. To avoid duplicate data, SL1 does not collect these tags and will collect only user-defined tags.

4. For all other fields, use the default values.
5. Click the **[Save As]** button.

Discovering New Relic Component Devices

To model and monitor your New Relic devices, you must run a discovery session to discover your New Relic services.

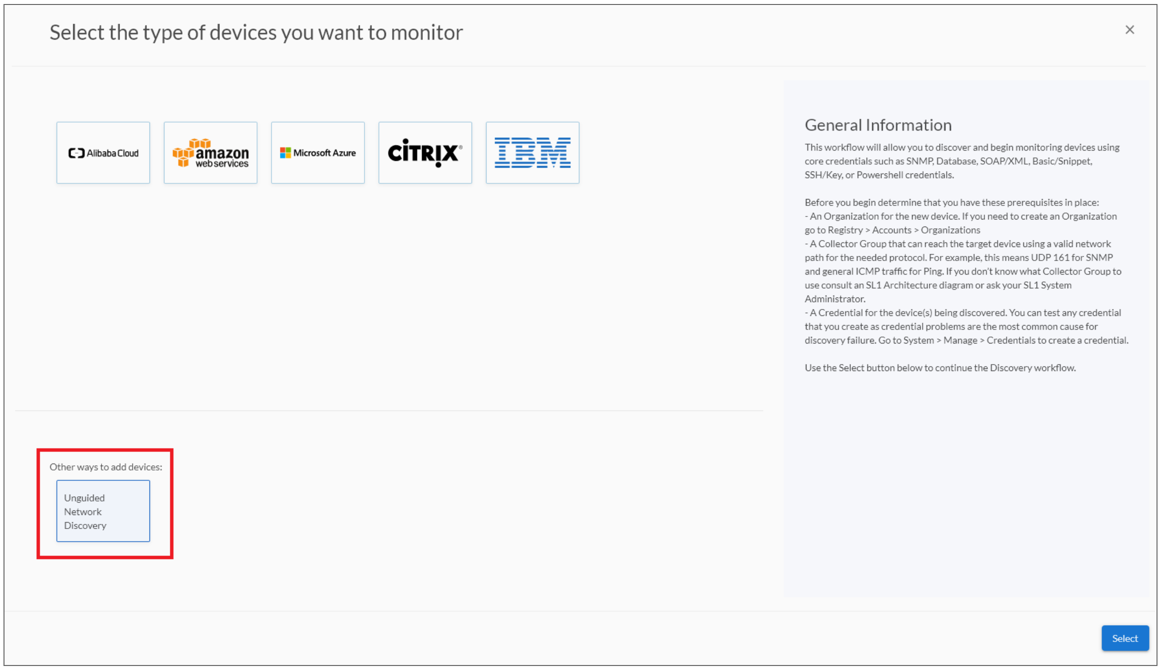
WARNING: If you have multiple New Relic accounts and sub-accounts to discover, follow the steps in the *Discovering Additional New Relic Accounts* section.

NOTE: The PowerPack does not model applications with "reporting: false" statuses.

Several minutes after the discovery session has completed, the Dynamic Applications in the *New Relic: APM* PowerPack should automatically align to the services and then discover, model, and monitor the remaining New Relic component devices.

To discover the New Relic service that you want to monitor, perform the following steps:

1. On the **Devices** page (🖥) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears:


Select the type of devices you want to monitor
×
Alibaba Cloud
amazon web services
Microsoft Azure
CITRIX
IBM
Other ways to add devices:
Unguided Network Discovery
Select

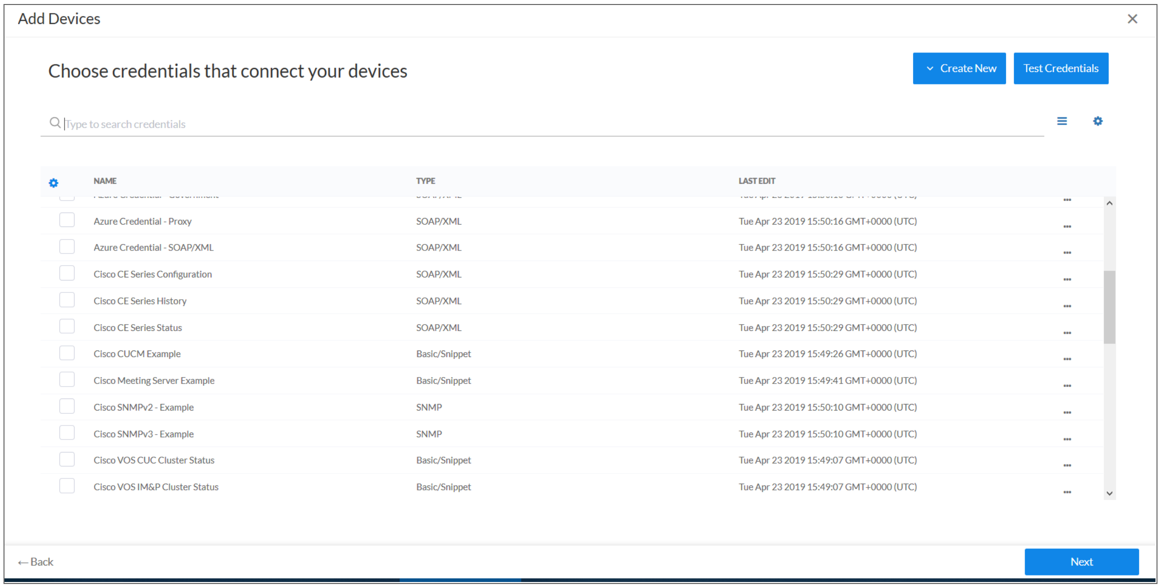
General Information

This workflow will allow you to discover and begin monitoring devices using core credentials such as SNMP, Database, SOAP/XML, Basic/Snippet, SSH/Key, or Powershell credentials.

Before you begin determine that you have these prerequisites in place:
- An Organization for the new device. If you need to create an Organization go to Registry > Accounts > Organizations
- A Collector Group that can reach the target device using a valid network path for the needed protocol. For example, this means UDP 161 for SNMP and general ICMP traffic for Ping. If you don't know what Collector Group to use consult an SL1 Architecture diagram or ask your SL1 System Administrator.
- A Credential for the device(s) being discovered. You can test any credential that you create as credential problems are the most common cause for discovery failure. Go to System > Manage > Credentials to create a credential.

Use the Select button below to continue the Discovery workflow.

2. Click the **[Unguided Network Discovery]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.
3. Click **[Select]**. The **Add Devices** page appears:
4. Complete the following fields:
    - ***Name***. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.
    - ***Description***. Optional. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **[Discovery Sessions]** tab.
    - ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered devices.
5. Click **[Next]**. The **Credentials** page of the **Add Devices** wizard appears:

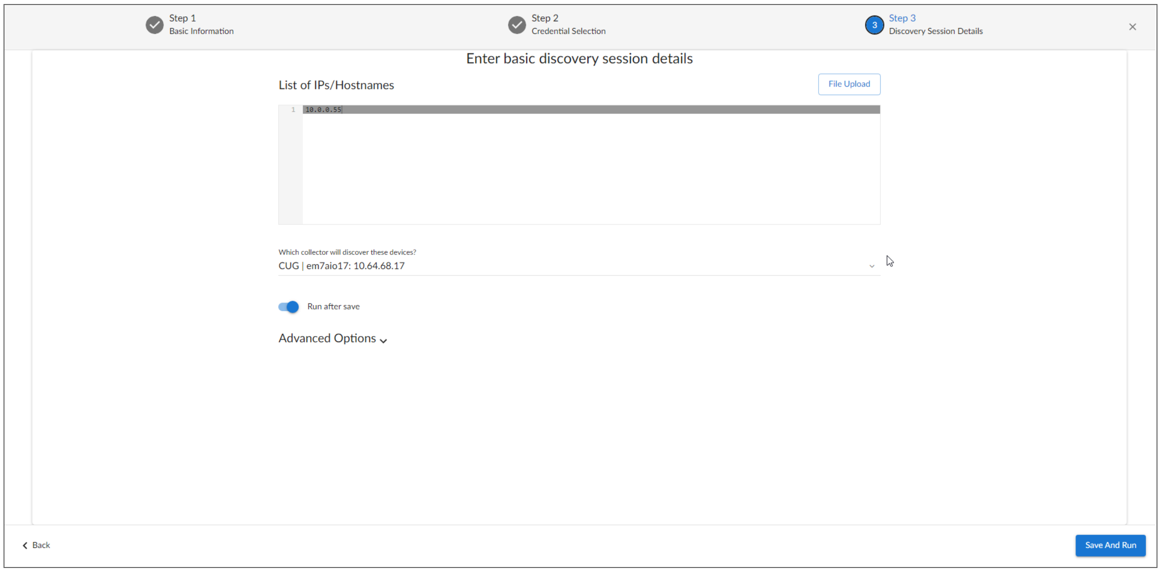


Add Devices

Choose credentials that connect your devices

	NAME	TYPE	LAST EDIT
□	Azure Credential - Proxy	SOAP/XML	Tue Apr 23 2019 15:50:16 GMT+0000 (UTC)
□	Azure Credential - SOAP/XML	SOAP/XML	Tue Apr 23 2019 15:50:16 GMT+0000 (UTC)
□	Cisco CE Series Configuration	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)
□	Cisco CE Series History	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)
□	Cisco CE Series Status	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)
□	Cisco CUCM Example	Basic/Snippet	Tue Apr 23 2019 15:49:26 GMT+0000 (UTC)
□	Cisco Meeting Server Example	Basic/Snippet	Tue Apr 23 2019 15:49:41 GMT+0000 (UTC)
□	Cisco SNMPv2 - Example	SNMP	Tue Apr 23 2019 15:50:10 GMT+0000 (UTC)
□	Cisco SNMPv3 - Example	SNMP	Tue Apr 23 2019 15:50:10 GMT+0000 (UTC)
□	Cisco VOS CUC Cluster Status	Basic/Snippet	Tue Apr 23 2019 15:49:07 GMT+0000 (UTC)
□	Cisco VOS IM&P Cluster Status	Basic/Snippet	Tue Apr 23 2019 15:49:07 GMT+0000 (UTC)

6. On the **Credentials** page, locate and select the SOAP/XML credentials you created for the New Relic service.
7. Click **[Next]**. The **Discovery Session Details** page of the **Add Devices** wizard appears:



Enter basic discovery session details

List of IPs/Hostnames

```
10.0.0.55
```

Which collector will discover these devices?
CUG | em7aio17: 10.64.68.17

● Run after save

8. Complete the following fields:

    - ***List of IPs/Hostnames***. Type "api.newrelic.com".
    - ***Which collector will monitor these devices?***. Select an existing collector to monitor the discovered devices. Required.
    - ***Run after save***. Select this option to run this discovery session as soon as you click **[Save and Close]**.

      In the **Advanced options** section, click the down arrow icon (⌄) to complete the following fields:

        - ***Discover Non-SNMP***. Enable this setting.
        - ***Model Devices***. Enable this setting.

9. Click **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.
10. If you selected the **Run after save** option on this page, the discovery session runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page includes a link to the **Device Investigator** page for the discovered device.

Discovering New Relic Component Devices in the SL1 Classic User Interface

To model and monitor your New Relic devices, you must run a discovery session to discover your New Relic services.

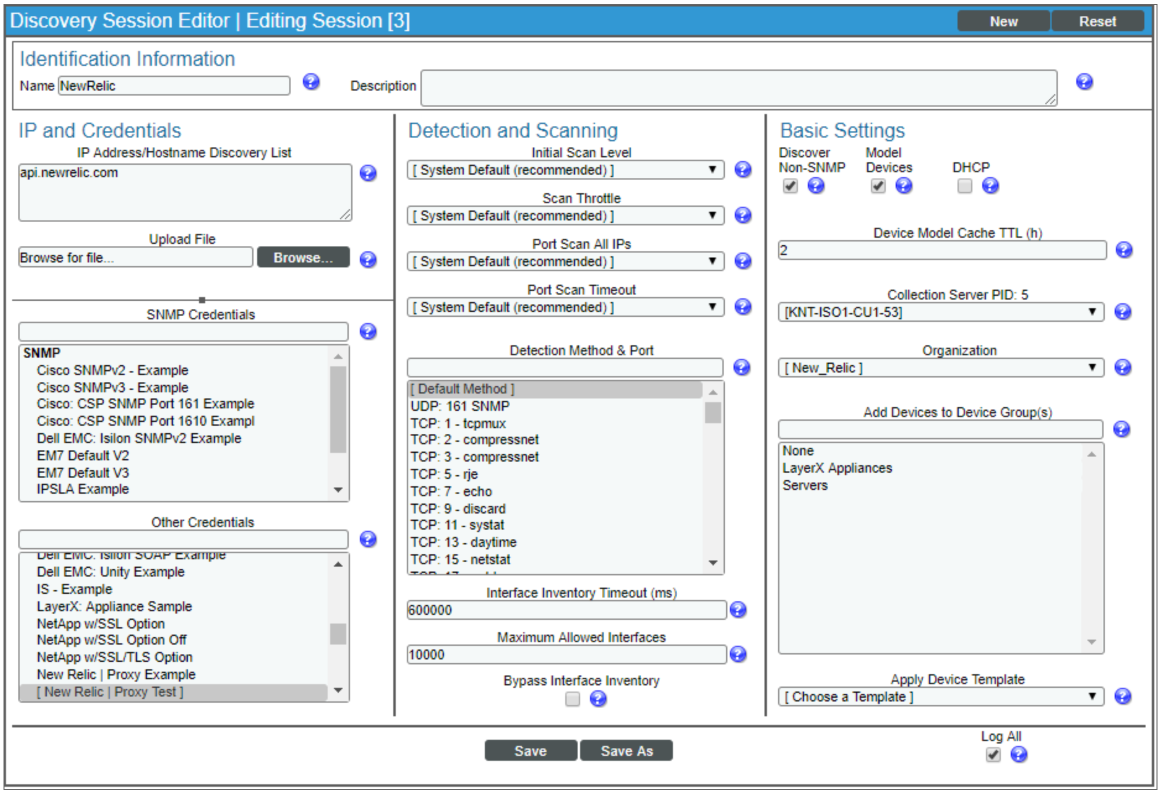
WARNING: If you have multiple New Relic accounts and sub-accounts to discover, follow the steps in the *Discovering Additional New Relic Accounts* section.

NOTE: The PowerPack does not model applications with "reporting: false" statuses.

Several minutes after the discovery session has completed, the Dynamic Applications in the *New Relic: APM* PowerPack should automatically align to the services and then discover, model, and monitor the remaining New Relic component devices.

To discover the New Relic service 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:


Discovery Session Editor | Editing Session [3]

Identification Information

Name: NewRelic

Description:

IP and Credentials

IP Address/Hostname Discovery List: api.newrelic.com

Upload File: Browse for file...

SNMP Credentials:
SNMP
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Cisco: CSP SNMP Port 161 Example
Cisco: CSP SNMP Port 1610 Exampl
Dell EMC: Isilon SNMPv2 Example
EM7 Default V2
EM7 Default V3
IPSLA Example

Other Credentials:
Dell EMC: Isilon SOAP Example
Dell EMC: Unity Example
IS - Example
LayerX: Appliance Sample
NetApp w/SSL Option
NetApp w/SSL Option Off
NetApp w/SSL/TLS Option
New Relic | Proxy Example
[New Relic | Proxy Test]

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: 5: [KNT-ISO1-CU1-53]

Organization: [New_Relic]

Add Devices to Device Group(s):
None
LayerX Appliances
Servers

Apply Device Template: [Choose a Template]

Log All: ☑

- ***Name***. Type a name for the discovery session.
- ***IP Address/Hostname Discovery List***. Type "api.newrelic.com".
- ***Other Credentials***. Select the SOAP/XML credentials you created for the New Relic service.
- ***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 device is discovered, click the device icon (🖥) to view the **Device Properties** page for each device.

Discovering Additional New Relic Accounts

If you have already discovered a New Relic account and want to discover additional New Relic accounts, you must create a credential for each account you want to discover, edit the New Relic device template for each new account, and then create a virtual device to which you will align the template.

Create Credentials

Using the steps outlined in the ***Creating a SOAP/XML Credential for New Relic*** section, create a credential for each additional New Relic account you want to discover.

Edit the Device Template

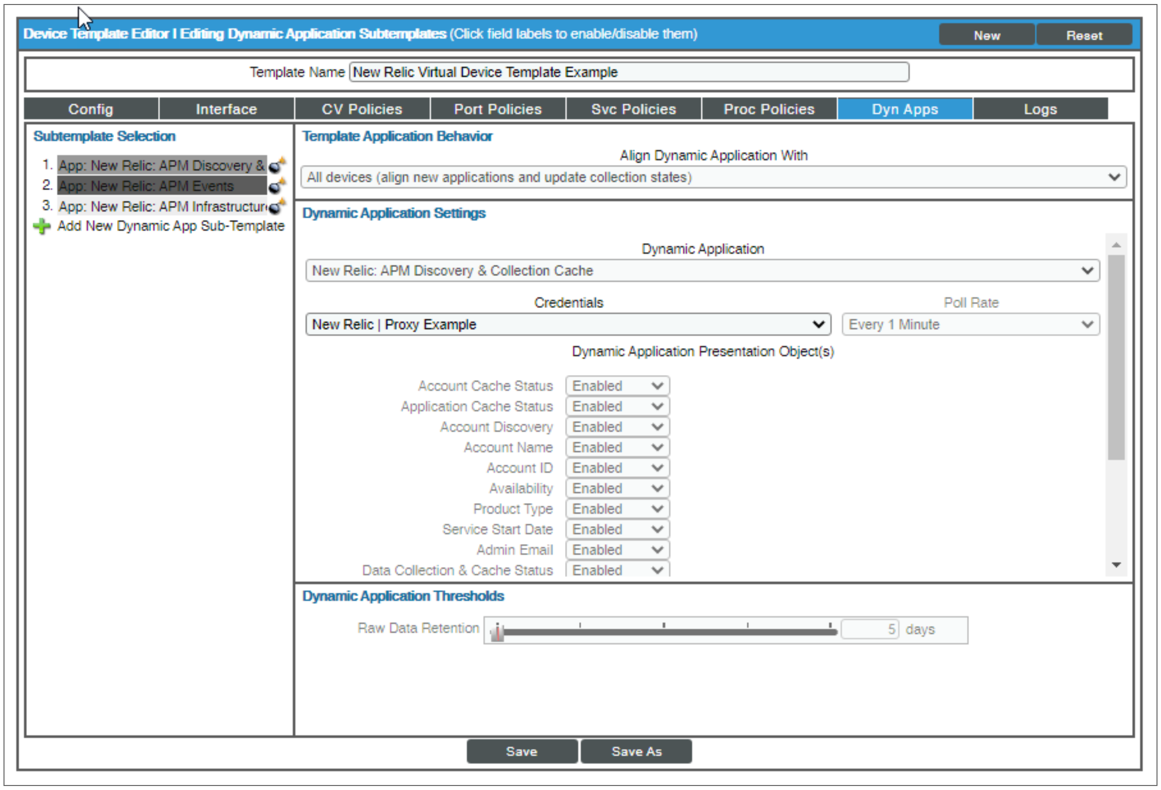
A ***device template*** allows you to save a device configuration and apply it to multiple devices. The *New Relic: APM*PowerPack includes the "New Relic Virtual Device Template Example". You must configure a device template for each additional New Relic account you want to discover.

If you configure this device template correctly, once you align the template to the New Relic virtual device, SL1 will use the device template to automatically align the New Relic discovery Dynamic Applications and start collecting data.

To configure the New Relic device template:

1. Go to the **Configuration Templates** page (Devices > Templates, or Registry > Devices > Templates in the SL1 classic user interface).
2. Locate the "New Relic Virtual Device Template Example" and click its wrench icon (🔧). The **Device Template Editor** page appears.
3. Click the **[Dyn Apps]** tab. The **Editing Dynamic Application Subtemplates** page appears.

4. Complete the following fields:



Device Template Editor | Editing Dynamic Application Subtemplates (Click field labels to enable/disable them)

Template Name: New Relic Virtual Device Template Example

Subtemplate Selection

1. App: New Relic: APM Discovery &
2. App: New Relic: APM Events
3. App: New Relic: APM Infrastructur

Add New Dynamic App Sub-Template

Template Application Behavior

Align Dynamic Application With: All devices (align new applications and update collection states)

Dynamic Application Settings

Dynamic Application: New Relic: APM Discovery & Collection Cache

Credentials: New Relic | Proxy Example

Poll Rate: Every 1 Minute

Dynamic Application Presentation Object(s)

Account Cache Status	Enabled
Application Cache Status	Enabled
Account Discovery	Enabled
Account Name	Enabled
Account ID	Enabled
Availability	Enabled
Product Type	Enabled
Service Start Date	Enabled
Admin Email	Enabled
Data Collection & Cache Status	Enabled

Dynamic Application Thresholds

Raw Data Retention: 5 days

- **Template Name**. Type a new name for the device template.
- **Credentials**. Select the SOAP/XML credential that you created for the New Relic account.

5. Click the next Dynamic Application listed in the **Subtemplate Selection** section on the left side of the page and then select the New Relic SOAP/XML credential in the ***Credentials*** field.
6. Repeat step 5 until the you have selected the New Relic SOAP/XML credential in the ***Credentials*** field for all of the Dynamic Applications listed in the **Subtemplate Selection** section.
7. Click **[Save As]**.

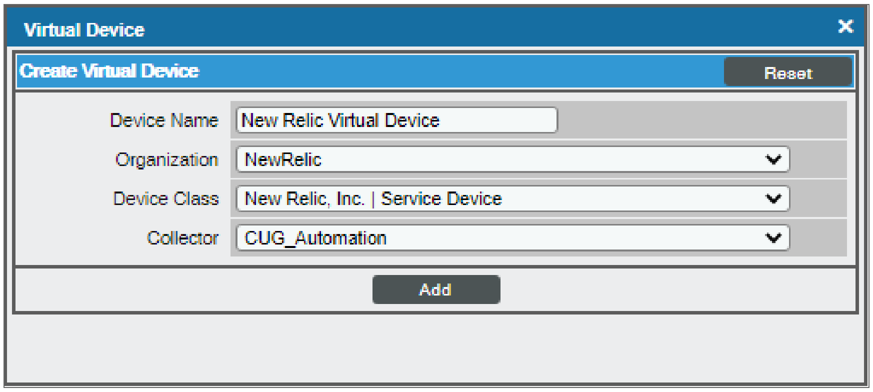
NOTE: You must rename the sample **New Relic Virtual Device Template Example** and click **[Save As]** to save it. If you do not rename the device template, then your device template will be overwritten the next time you upgrade the *New Relic: APM*PowerPack.

Create a Virtual Device

To discover an additional New Relic account, you must create a ***virtual device*** that represents the New Relic account. A virtual device is a user-defined container that represents a device or service that cannot be discovered by SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications.

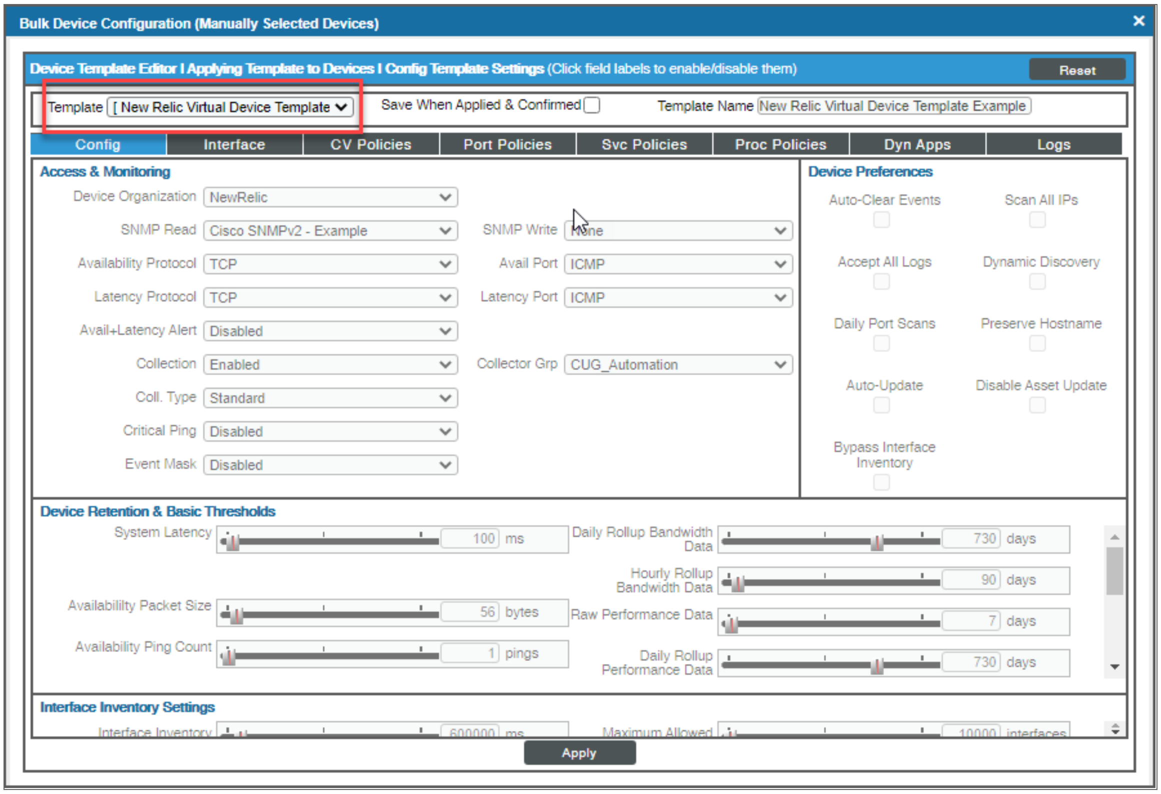
To create a virtual device that represents your New Relic account:

1. Go to the **Device Manager** page (Devices > Device Manager, or Registry > Devices > Device Manager in the SL1 classic user interface).
2. Click the **[Actions]** button and select *Create Virtual Device* from the menu. The **Virtual Device** modal page appears:



Device Name: New Relic Virtual Device
Organization: NewRelic
Device Class: New Relic, Inc. | Service Device
Collector: CUG_Automation

3. Complete the following fields:
   - ***Device Name***. Type a name for the virtual device.
   - ***Organization***. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.
   - ***Device Class***. Select *New Relic, Inc. | Service Device*.
   - ***Collector***. Select the collector group that will monitor the device.
4. Click **[Add]** to create the virtual device.
5. In the **Device Manager** page (Devices > Device Manager, or Registry > Devices > Device Manager in the SL1 classic user interface), select the checkbox (☑) for the virtual device that you just created.
6. Click the ***Select Actions*** drop-down and select *MODIFY By Template* from the menu and click **[Go]**.
7. In the **Device Template Editor**, use the ***Template*** drop-down to select the device template that you created for the New Relic account and click the **[Apply]** button.
8. Click the **[Confirm]** button to save your changes.



Device Template Editor | Applying Template to Devices | Config Template Settings (Click field labels to enable/disable them)

Template [New Relic Virtual Device Template

Save When Applied & Confirmed □

Template Name New Relic Virtual Device Template Example

Access & Monitoring

Device Organization NewRelic

SNMP Read Cisco SNMPv2 - Example

SNMP Write None

Availability Protocol TCP

Avail Port ICMP

Latency Protocol TCP

Latency Port ICMP

Avail+Latency Alert Disabled

Collection Enabled

Collector Grp CUG_Automation

Coll. Type Standard

Critical Ping Disabled

Event Mask Disabled

Device Preferences

Auto-Clear Events □

Scan All IPs □

Accept All Logs □

Dynamic Discovery □

Daily Port Scans □

Preserve Hostname □

Auto-Update □

Disable Asset Update □

Bypass Interface Inventory □

Device Retention & Basic Thresholds

System Latency 100 ms

Daily Rollup Bandwidth Data 730 days

Hourly Rollup Bandwidth Data 90 days

Availability Packet Size 56 bytes

Raw Performance Data 7 days

Availability Ping Count 1 pings

Daily Rollup Performance Data 730 days

Interface Inventory Settings

Interface Inventory 600000 ms

Maximum Allowed 10000 interfaces

Verifying Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. After discovery has completed, go to the **Devices** page and click the device for the New Relic service. From the **Device Investigator** page for the New Relic service, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. All applicable Dynamic Applications for the service 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 New Relic service:

- New Relic: APM Discovery & Collection Cache
- New Relic: APM Events
- New Relic: APM Infrastructure Group Discovery

If the listed Dynamic Applications have not been automatically aligned during discovery, or you want to align more Dynamic Applications, you can align them manually. To do so, perform the following steps:

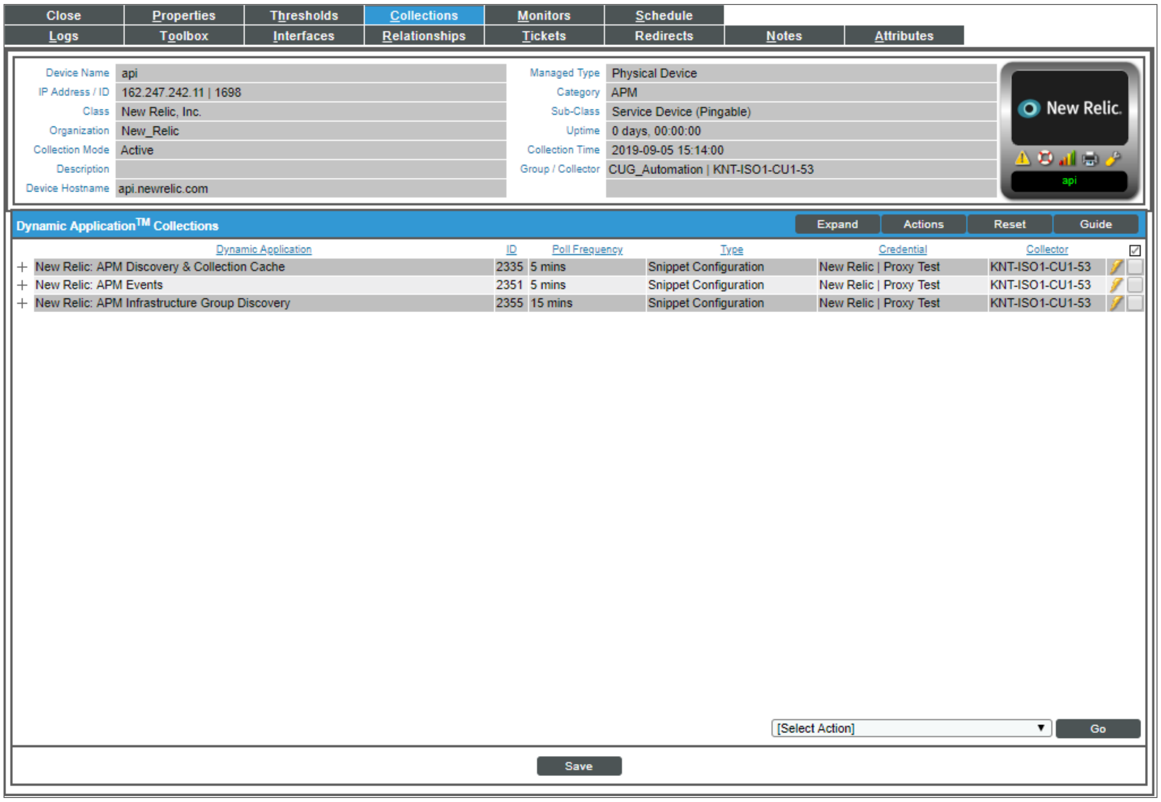
1. Click the **[Edit]** button, and then select **[Align Dynamic App]**. The **Align Dynamic Application** window appears.
2. Click *Choose Dynamic Application*. The **Choose Dynamic Application** window appears.
3. Select the Dynamic Application you want to align and click **[Select]**. The name of the selected Dynamic Application appears in the **Align Dynamic Application** window.
4. If a default credential is listed below the Dynamic Application and you want to use that credential, skip ahead to step 7. Otherwise, uncheck the box next to the credential name.
5. Click *Choose Credential*. The **Choose Credential** window appears.
6. Select the credential for the Dynamic Application and click the **[Select]** button. The name of the selected credential appears in the **Align Dynamic Application** window.
7. Click the **[Align Dynamic App]** button. When the Dynamic Application is successfully aligned, it is added to the **[Collections]** tab, and a confirmation message appears at the bottom of the tab.
8. Repeat steps 1-7 for any other unaligned Dynamic Applications.

Verifying Discovery and Dynamic Application Alignment in the SL1 Classic User Interface

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. After discovery has completed, click the device icon for the New Relic service (). From the **Device Properties** page for the New Relic service, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. All applicable Dynamic Applications for the service 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	api	Managed Type	Physical Device
IP Address / ID	162.247.242.11 | 1698	Category	APM
Class	New Relic, Inc.	Sub-Class	Service Device (Pingable)
Organization	New_Relic	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2019-09-05 15:14:00
Description		Group / Collector	CUG_Automation | KNT-ISO1-CU1-53
Device Hostname	api.newrelic.com		

Dynamic Application^{TM} Collections

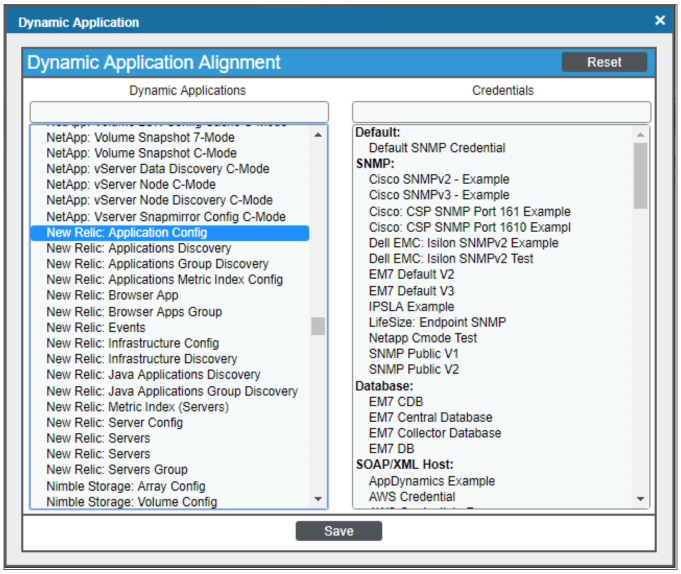
	Dynamic Application	ID	Poll Frequency	Type	Credential	Collector	☑
+	New Relic: APM Discovery & Collection Cache	2335	5 mins	Snippet Configuration	New Relic | Proxy Test	KNT-ISO1-CU1-53	□
+	New Relic: APM Events	2351	5 mins	Snippet Configuration	New Relic | Proxy Test	KNT-ISO1-CU1-53	□
+	New Relic: APM Infrastructure Group Discovery	2355	15 mins	Snippet Configuration	New Relic | Proxy Test	KNT-ISO1-CU1-53	□

You should see the following Dynamic Applications aligned to the New Relic service:

- New Relic: APM Discovery & Collection Cache
- New Relic: APM Events
- New Relic: APM Infrastructure Group Discovery

If the listed Dynamic Applications have not been automatically aligned during discovery, or you want to align more Dynamic Applications, you can align them manually. To do so, perform the following steps:

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



NetApp: Volume Snapshot 7-Mode
NetApp: Volume Snapshot C-Mode
NetApp: vServer Data Discovery C-Mode
NetApp: vServer Node C-Mode
NetApp: vServer Node Discovery C-Mode
NetApp: Vserver Snapmirror Config C-Mode
New Relic: Application Config
New Relic: Applications Discovery
New Relic: Applications Group Discovery
New Relic: Applications Metric Index Config
New Relic: Browser App
New Relic: Browser Apps Group
New Relic: Events
New Relic: Infrastructure Config
New Relic: Infrastructure Discovery
New Relic: Java Applications Discovery
New Relic: Java Applications Group Discovery
New Relic: Metric Index (Servers)
New Relic: Server Config
New Relic: Servers
New Relic: Servers
New Relic: Servers Group
Nimble Storage: Array Config
Nimble Storage: Volume Config

Default:
Default SNMP Credential
SNMP:
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Cisco: CSP SNMP Port 161 Example
Cisco: CSP SNMP Port 1610 Exampl
Dell EMC: Isilon SNMPv2 Example
Dell EMC: Isilon SNMPv2 Test
EM7 Default V2
EM7 Default V3
IPSLA Example
LifeSize: Endpoint SNMP
Netapp Cmode Test
SNMP Public V1
SNMP Public V2
Database:
EM7 CDB
EM7 Central Database
EM7 Collector Database
EM7 DB
SOAP/XML Host:
AppDynamics Example
AWS Credential

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 any other unaligned Dynamic Applications.

Relationships with Other Types of Component Devices

Additionally, the Dynamic Applications in the *New Relic: APM* PowerPack can automatically build relationships between New Relic devices and other associated devices:

- If you discover Linux devices using the Dynamic Applications in the *Linux Base Pack* PowerPack version 102 or later, SL1 will automatically create relationships between New Relic devices and Linux servers.
- If you discover Windows servers using the Dynamic Applications in the *Microsoft Base Pack* PowerPack version 107 or later, SL1 will automatically create relationships between New Relic devices and Windows servers.
- If you discover Windows servers using the Dynamic Applications in the *Microsoft: Windows Server* PowerPack version 108 or later, SL1 will automatically create relationships between New Relic devices and Windows servers.

Chapter 57

NGINX: Open Source and Plus

Overview

The following sections describe how to configure and discover NGINX services for monitoring by SL1 using the *NGINX: Open Source and Plus* PowerPack:

NOTE: For more information about the *NGINX: Open Source and Plus* PowerPack, see the ***Monitoring NGINX: Open Source and Plus*** manual.

Prerequisites for Monitoring NGINX Services

To configure the SL1 system to monitor NGINX services using the *NGINX: Open Source and Plus* PowerPack, note the following for monitoring the NGINX Open Source Software (OSS):

- The status module must be included when NGINX is instantiated.
- The status stub must be configured in the NGINX configuration.

NOTE: Restart NGINX after editing the configuration.

To learn more about the setup of the status module, see the following NGINX resources:

- Monitoring NGINX (https://www.nginx.com/blog/monitoring-nginx)
- Module ngx_http_stub_status_module (http://nginx.org/en/docs/http/ngx_http_stub_status_module.html)

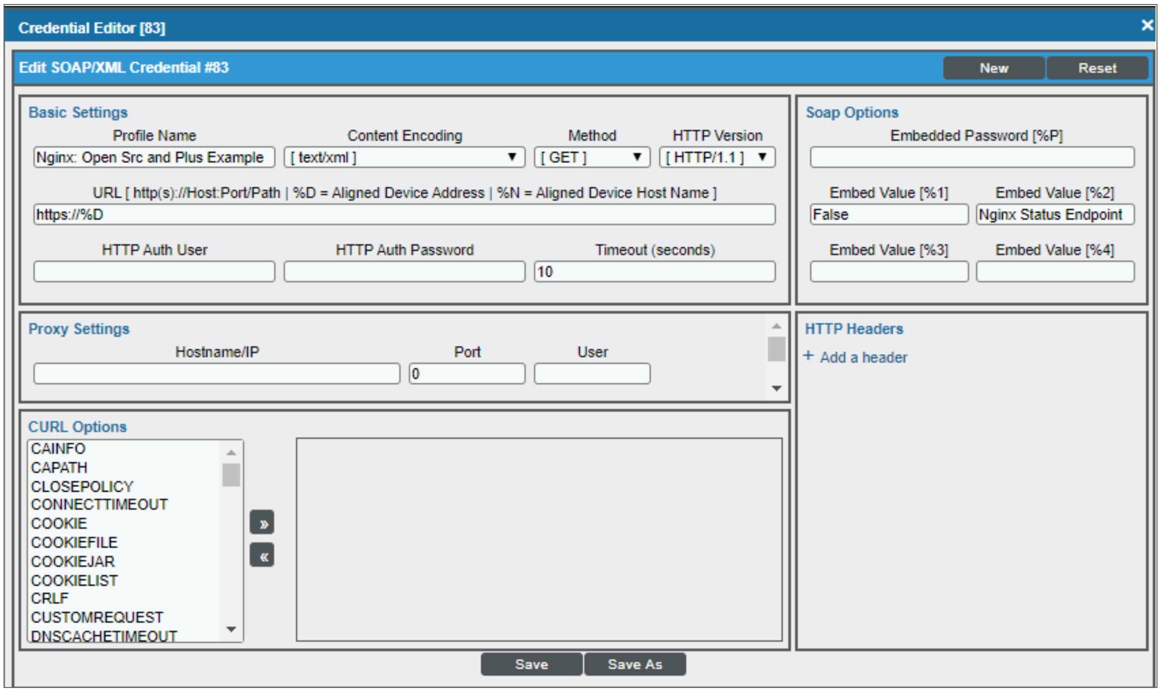
Creating a SOAP/XML Credential for NGINX

To configure SL1 to monitor NGINX web services, you must create a SOAP/XML credential. This credential allows the Dynamic Applications in the *NGINX: Open Source and Plus* PowerPack to communicate with your NGINX web server.

To configure a SOAP/XML credential to access NGINX:

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

2. Locate the **NGINX: Open Src and Plus Example** credential, and then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears.



Profile Name: Nginx: Open Src and Plus Example
Content Encoding: [text/xml]
Method: [GET]
HTTP Version: [HTTP/1.1]
URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://%D
HTTP Auth User:
HTTP Auth Password:
Timeout (seconds): 10
Embedded Password [%P]:
Embed Value [%1]: False
Embed Value [%2]: Nginx Status Endpoint
Embed Value [%3]:
Embed Value [%4]:
Hostname/IP:
Port: 0
User:

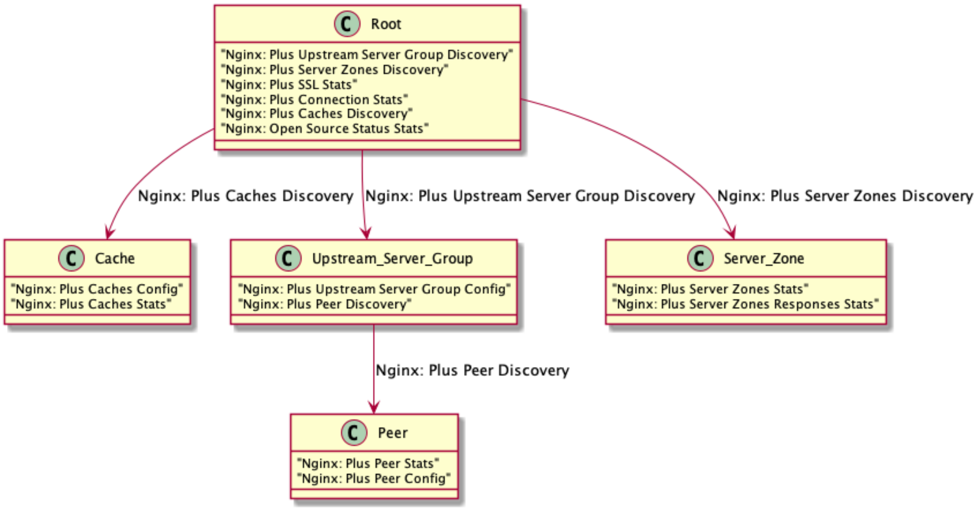
3. Enter values in the following fields:

   - ***Profile Name***. Type a new name for the credential.
   - ***URL***. Leave this field as the default.
   - ***Embed Value [%1]***. Used by the REST libraries for SSL certificate validation. Do one of the following:
     - Type "True" to enable SSL certificate validation.
     - Type "False" or leave this field blank to disable SSL certificate verification.
   - ***Embed Value [%2]***. Type a specific API endpoint name to connect to if you want to override the default /nginx_status endpoint for the Nginx: Open Source Status Stats Dynamic Application.

4. For all other fields, use the default values.
5. Click the **[Save As]** button.

Discovering NGINX Component Devices

To model and monitor your NGINX services, you must run a discovery session to discover your NGINX services. The following diagram illustrates the way the discovery process works for NGINX.



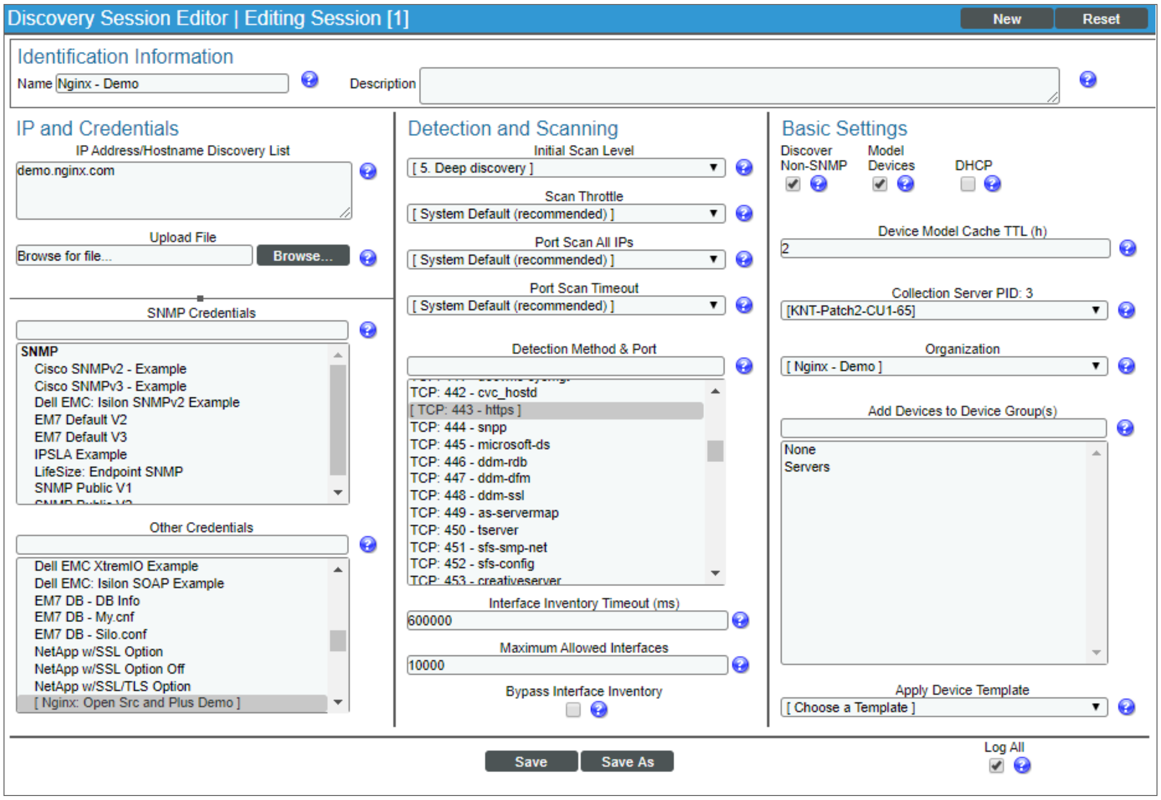
C Root
"Nginx: Plus Upstream Server Group Discovery"
"Nginx: Plus Server Zones Discovery"
"Nginx: Plus SSL Stats"
"Nginx: Plus Connection Stats"
"Nginx: Plus Caches Discovery"
"Nginx: Open Source Status Stats"
Nginx: Plus Caches Discovery
Nginx: Plus Upstream Server Group Discovery
Nginx: Plus Server Zones Discovery
C Cache
"Nginx: Plus Caches Config"
"Nginx: Plus Caches Stats"
C Upstream_Server_Group
"Nginx: Plus Upstream Server Group Config"
"Nginx: Plus Peer Discovery"
C Server_Zone
"Nginx: Plus Server Zones Stats"
"Nginx: Plus Server Zones Responses Stats"
Nginx: Plus Peer Discovery
C Peer
"Nginx: Plus Peer Stats"
"Nginx: Plus Peer Config"

Several minutes after the discovery session has completed, the Dynamic Applications in the *NGINX: Open Source and Plus* PowerPack should automatically align to the services and then discover, model, and monitor the remaining NGINX component devices.

To discover the NGINX service 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:



Discovery Session Editor | Editing Session [1]

Identification Information

Name: Nginx - Demo

Description:

IP and Credentials

IP Address/Hostname Discovery List: demo.nginx.com

Upload File: Browse for file...

SNMP Credentials

SNMP
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Dell EMC: Isilon SNMPv2 Example
EM7 Default V2
EM7 Default V3
IPSLA Example
LifeSize: Endpoint SNMP
SNMP Public V1

Other Credentials

Dell EMC XtremIO Example
Dell EMC: Isilon SOAP Example
EM7 DB - DB Info
EM7 DB - My.cnf
EM7 DB - Silo.conf
NetApp w/SSL Option
NetApp w/SSL Option Off
NetApp w/SSL/TLS Option
[Nginx: Open Src and Plus Demo]

Detection and Scanning

Initial Scan Level: [5. Deep discovery]

Scan Throttle: [System Default (recommended)]

Port Scan All IPs: [System Default (recommended)]

Port Scan Timeout: [System Default (recommended)]

Detection Method & Port

TCP: 442 - cvc_hostd
[TCP: 443 - https]
TCP: 444 - snpp
TCP: 445 - microsoft-ds
TCP: 446 - ddm-rdb
TCP: 447 - ddm-dfm
TCP: 448 - ddm-ssl
TCP: 449 - as-servermap
TCP: 450 - tserver
TCP: 451 - sfs-smp-net
TCP: 452 - sfs-config
TCP: 453 - creativeserver

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: 3: [KNT-Patch2-CU1-65]

Organization: [Nginx - Demo]

Add Devices to Device Group(s)

None
Servers

Apply Device Template: [Choose a Template]

Log All: ☑

- ***Name***. Type a name for the discovery session.
- ***IP Address/Hostname Discovery List***. Type the IP address or hostname of your NGINX server.
- ***Other Credentials***. Select the SOAP/XML credentials you created for the NGINX service.
- ***Initial Scan Level***. Select *5. Deep discovery*.
- **Detection Method & Port**. Select *TCP 80 - http* and *TCP 443 - https*.
- ***Discover Non-SNMP***. Select this checkbox.
- ***Model Devices***. Select this checkbox.
- ***Log All***. 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.

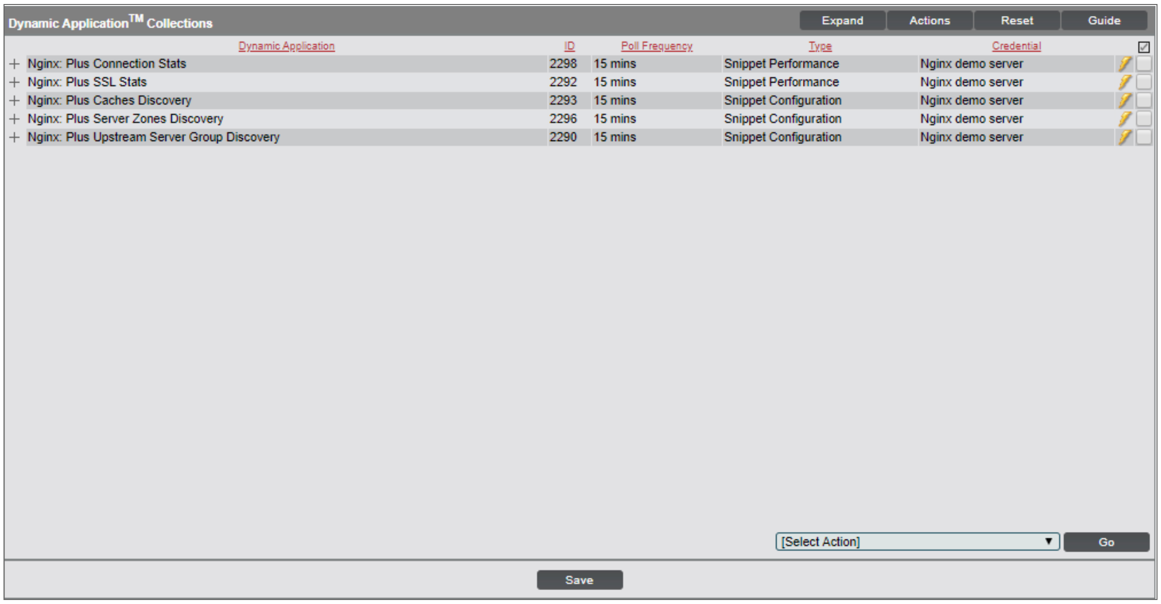
7. The **Discovery Session** window appears. When the device is discovered, click the device icon (🖥) to view the **Device Properties** page for each device.

Verifying Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. After discovery has completed, click the device icon for the NGINX service (). From the **Device Properties** page for the NGINX service, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. All applicable Dynamic Applications for the service 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.



Dynamic Application™ Collections

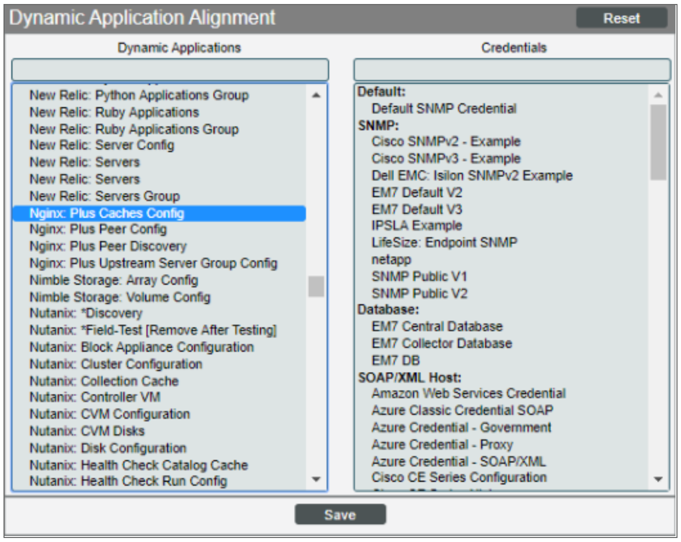
	Dynamic Application	ID	Poll Frequency	Type	Credential	☑
+	Nginx: Plus Connection Stats	2298	15 mins	Snippet Performance	Nginx demo server	□
+	Nginx: Plus SSL Stats	2292	15 mins	Snippet Performance	Nginx demo server	□
+	Nginx: Plus Caches Discovery	2293	15 mins	Snippet Configuration	Nginx demo server	□
+	Nginx: Plus Server Zones Discovery	2296	15 mins	Snippet Configuration	Nginx demo server	□
+	Nginx: Plus Upstream Server Group Discovery	2290	15 mins	Snippet Configuration	Nginx demo server	□

You should see the following Dynamic Applications aligned to the NGINX service:

- Nginx: Plus Connection Stats
- Nginx: Plus SSL Stats
- Nginx: Plus Caches Discovery
- Nginx: Plus Server Zones Discovery
- Nginx: Plus Upstream Server Group Discovery

If the listed Dynamic Applications have not been automatically aligned during discovery, or you want to align more Dynamic Applications, you can align them manually. To do so, perform the following steps:

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


Dynamic Application Alignment
Reset
Dynamic Applications
Credentials
New Relic: Python Applications Group
New Relic: Ruby Applications
New Relic: Ruby Applications Group
New Relic: Server Config
New Relic: Servers
New Relic: Servers
New Relic: Servers Group
Nginx: Plus Caches Config
Nginx: Plus Peer Config
Nginx: Plus Peer Discovery
Nginx: Plus Upstream Server Group Config
Nimble Storage: Array Config
Nimble Storage: Volume Config
Nutanix: *Discovery
Nutanix: *Field-Test [Remove After Testing]
Nutanix: Block Appliance Configuration
Nutanix: Cluster Configuration
Nutanix: Collection Cache
Nutanix: Controller VM
Nutanix: CVM Configuration
Nutanix: CVM Disks
Nutanix: Disk Configuration
Nutanix: Health Check Catalog Cache
Nutanix: Health Check Run Config
Default:
Default SNMP Credential
SNMP:
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Dell EMC: Isilon SNMPv2 Example
EM7 Default V2
EM7 Default V3
IPSLA Example
LifeSize: Endpoint SNMP
netapp
SNMP Public V1
SNMP Public V2
Database:
EM7 Central Database
EM7 Collector Database
EM7 DB
SOAP/XML Host:
Amazon Web Services Credential
Azure Classic Credential SOAP
Azure Credential - Government
Azure Credential - Proxy
Azure Credential - SOAP/XML
Cisco CE Series Configuration
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 any other unaligned Dynamic Applications.

Chapter 58

Nimble Storage

Overview

The following sections describe how to configure and discover Nimble Storage Arrays for monitoring in SL1 using the *Nimble Storage (2.3)* PowerPack:

NOTE: For more information about the *Nimble Storage (2.3)* PowerPack, see the ***Monitoring Nimble Storage Arrays*** manual.

Prerequisites for Monitoring Nimble Storage Arrays

Before you can monitor Nimble Storage Arrays in SL1 using the Nimble Storage (2.3) PowerPack, you must have the following:

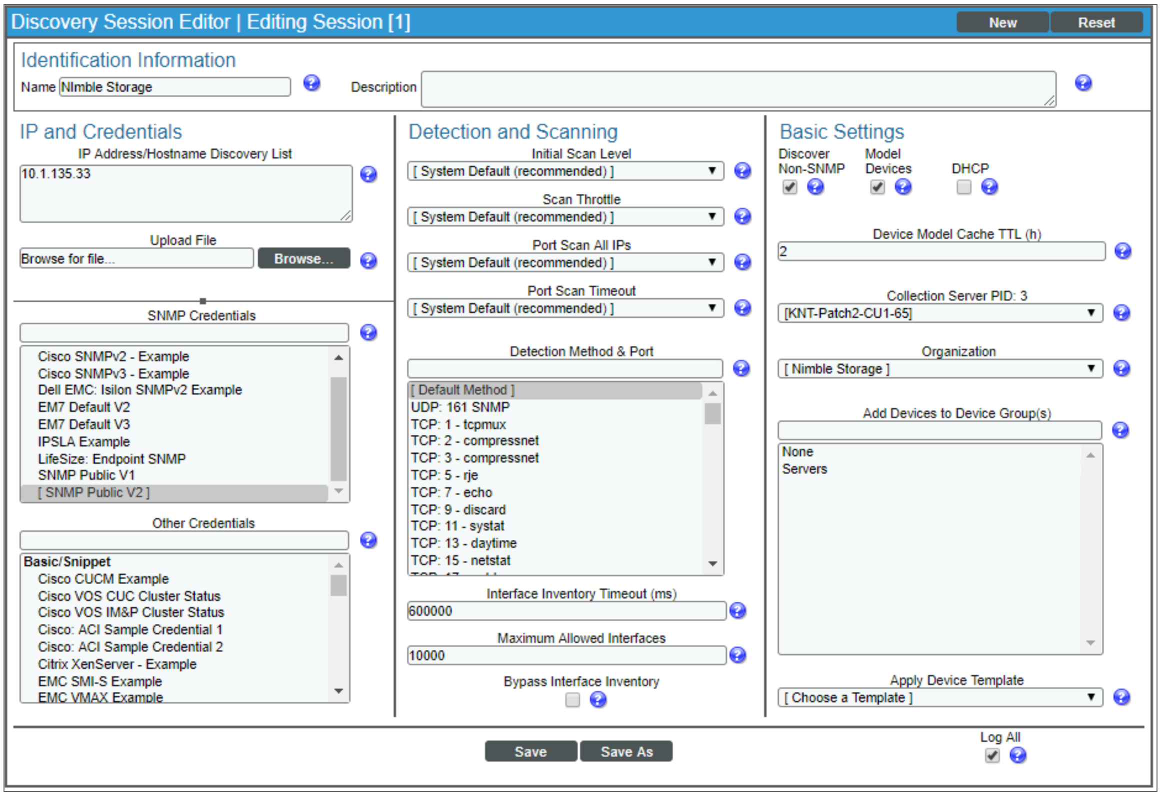
- Access to TCP port 161 from the SL1 Collector or SL1 All-In-One server
- Nimble Insight SNMP version 2.3 or later

Discovering Nimble Storage Arrays

The *Nimble Storage (2.3)* PowerPack uses SNMP to align to arrays. In order to discover a Nimble Storage Array, the array must be able to support Nimble Insight SNMP version 2.3 or later.

To discover Nimble Storage Arrays, perform the following steps:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. Click the **[Create]** button. The **Discovery Session Editor** page appears:



Name: NImble Storage

IP Address/Hostname Discovery List: 10.1.135.33

Initial Scan Level: [System Default (recommended)]

Scan Throttle: [System Default (recommended)]

Port Scan All IPs: [System Default (recommended)]

Port Scan Timeout: [System Default (recommended)]

Interface Inventory Timeout (ms): 600000

Maximum Allowed Interfaces: 10000

Bypass Interface Inventory: □

Discover Non-SNMP: ☑

Model Devices: ☑

DHCP: □

Device Model Cache TTL (h): 2

Collection Server PID: 3: [KNT-Patch2-CU1-65]

Organization: [Nimble Storage]

Apply Device Template: [Choose a Template]

Log All: ☑

3. Supply values in the following fields:
   - ***Name***. Type a unique name for the discovery session.
   - ***IP Address/Hostname Discovery List***. Type the IP address of the Nimble Storage Array.
   - ***SNMP Credentials***. Select the *SNMP Public V1* or *SNMP Public V2* credential.
   - ***Discover Non-SNMP***. Select this checkbox.
4. Optionally, supply values in the other fields in this page. For a description of the fields in this page, see the ***Discovery & Credentials*** manual.
5. Click the **[Save]** button.
6. The **Discovery Control Panel** page will refresh. Click the lightning bolt icon (⚡) for the discovery session you created.
7. In the pop-up window that appears, click the **[OK]** button. The **Discovery Session** page displays the progress of the discovery session.

> **NOTE:** The PowerPack uses the Volume Name to uniquely identify volume components. It's important that volume names on the Nimble Storage arrays are uniquely named and never reused to avoid any duplicate device creation on SL1.

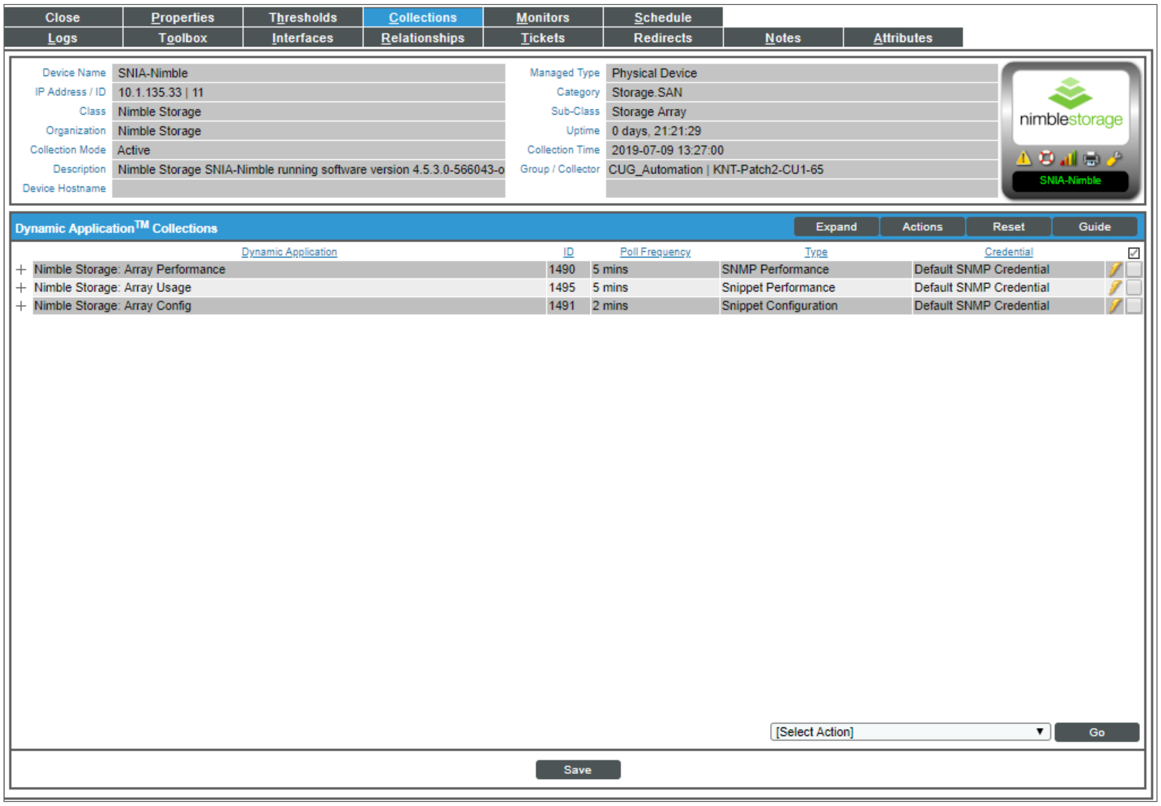
Verifying Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

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

You should see the following Dynamic Applications aligned to the Nimble Storage Array:

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



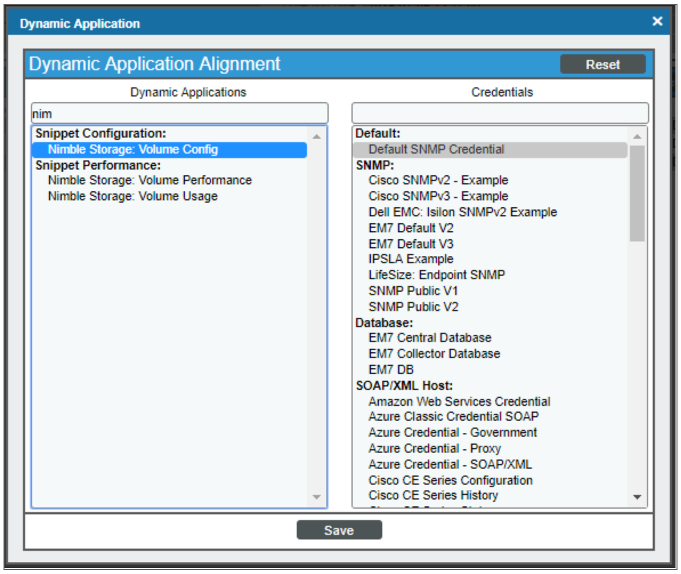
Device Name	SNIA-Nimble	Managed Type	Physical Device
IP Address / ID	10.1.135.33 | 11	Category	Storage.SAN
Class	Nimble Storage	Sub-Class	Storage Array
Organization	Nimble Storage	Uptime	0 days, 21:21:29
Collection Mode	Active	Collection Time	2019-07-09 13:27:00
Description	Nimble Storage SNIA-Nimble running software version 4.5.3.0-566043-o	Group / Collector	CUG_Automation | KNT-Patch2-CU1-65
Device Hostname			

Dynamic Application^{TM} Collections

	Dynamic Application	ID	Poll Frequency	Type	Credential	☑
+	Nimble Storage: Array Performance	1490	5 mins	SNMP Performance	Default SNMP Credential	□
+	Nimble Storage: Array Usage	1495	5 mins	Snippet Performance	Default SNMP Credential	□
+	Nimble Storage: Array Config	1491	2 mins	Snippet Configuration	Default SNMP Credential	□

If the listed Dynamic Applications have not been automatically aligned during discovery, you can align them manually. To do so, perform the following steps:

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



Dynamic Applications

nim

Snippet Configuration:
- Nimble Storage: Volume Config

Snippet Performance:
- Nimble Storage: Volume Performance
- Nimble Storage: Volume Usage

Credentials

Default:
- Default SNMP Credential

SNMP:
- Cisco SNMPv2 - Example
- Cisco SNMPv3 - Example
- Dell EMC: Isilon SNMPv2 Example
- EM7 Default V2
- EM7 Default V3
- IPSLA Example
- LifeSize: Endpoint SNMP
- SNMP Public V1
- SNMP Public V2

Database:
- EM7 Central Database
- EM7 Collector Database
- EM7 DB

SOAP/XML Host:
- Amazon Web Services Credential
- Azure Classic Credential SOAP
- Azure Credential - Government
- Azure Credential - Proxy
- Azure Credential - SOAP/XML
- Cisco CE Series Configuration
- Cisco CE Series History

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.

Chapter 59

Nutanix: Base Pack

Overview

The following sections describe how to configure and discover your Nutanix system for monitoring by SL1 using the *Nutanix Base Pack* PowerPack:

WARNING: You can monitor Prism Elements **or** Prism Central. You must choose between monitoring Prism Elements or Prism Central as the root device, and then run discovery accordingly. It is recommended that you monitor Prism Central in all cases, unless you have only Prism Elements instances with **no** Prism Central instances.

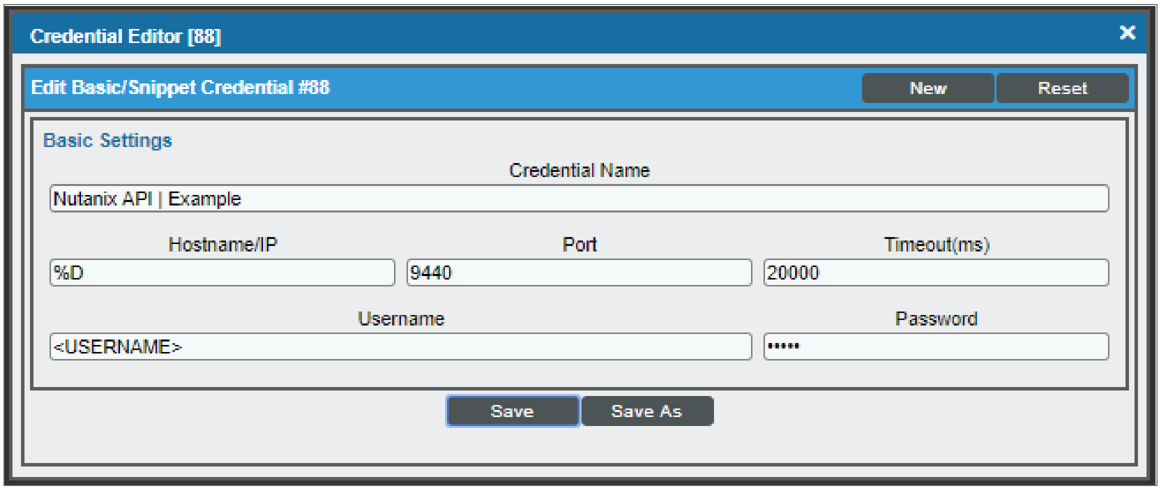
NOTE: For more information about the *Nutanix: Base Pack* PowerPack, see the ***Monitoring Nutanix*** manual.

Configuring the Nutanix Credentials

To use the Dynamic Applications in the *Nutanix Base Pack* PowerPack, you must first configure the credential in SL1. This credential allows SL1 to communicate with the Nutanix API. The PowerPack includes the "Nutanix API | Example" credential that you can use as a template.

To configure the Nutanix credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **Nutanix API | Example** credential and click its wrench icon (🔧). The **Credential Editor** modal page appears:



Credential Name: Nutanix API | Example

Hostname/IP: %D

Port: 9440

Timeout(ms): 20000

Username: <USERNAME>

Password: •••••

3. Enter values in the following fields:

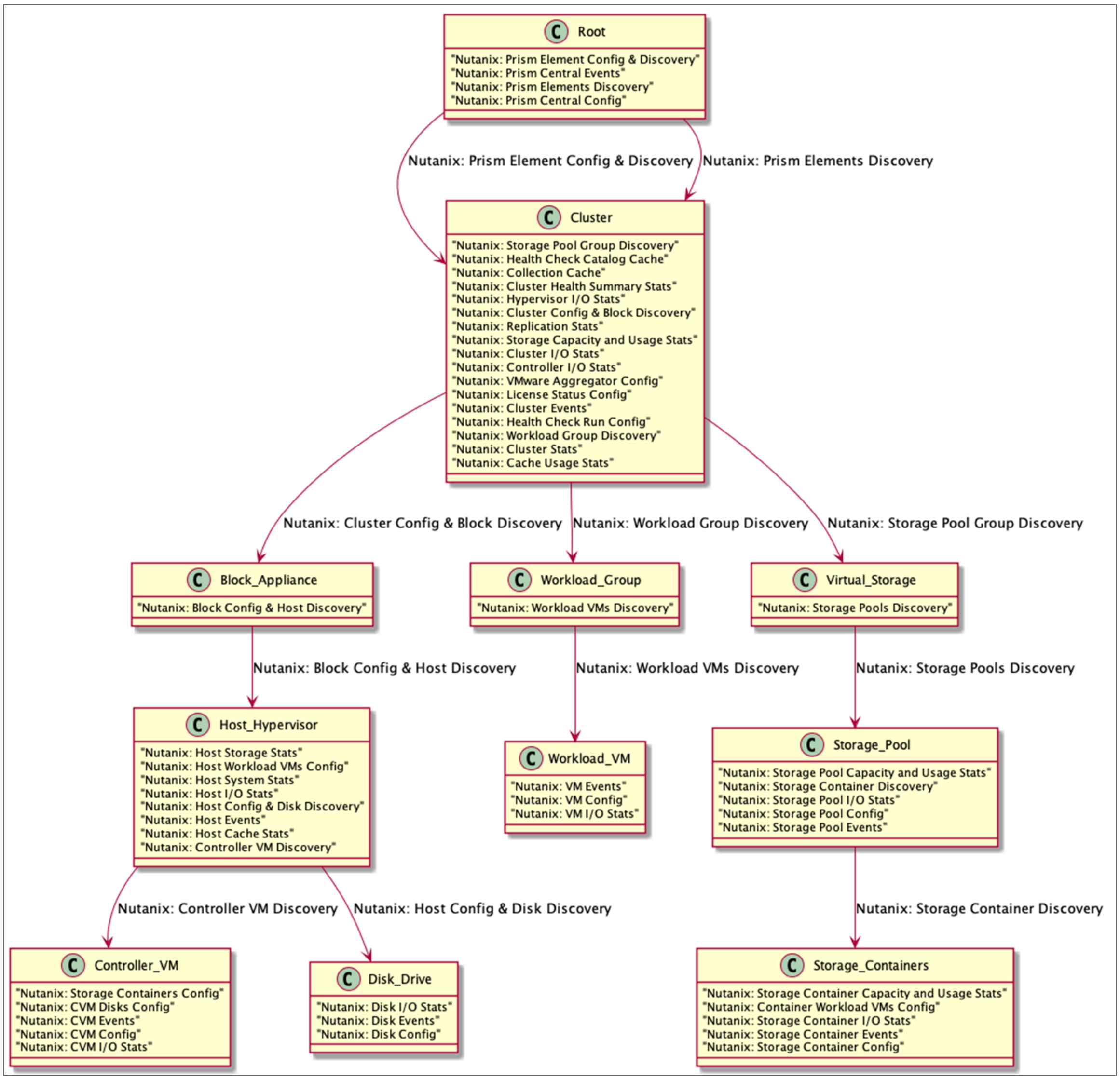
   - ***Credential Name***. Type a new name for your Nutanix credential.
   - ***Hostname/IP***. Type %D.
   - ***Username***. Type the username that SL1 will use to connect to the Nutanix system.
   - ***Password***. Type the password for the username you entered.

NOTE: You can use the default values for the remaining fields.

4. Click the **[Save As]** button, and then click **[OK]**.

Discovering Nutanix Systems

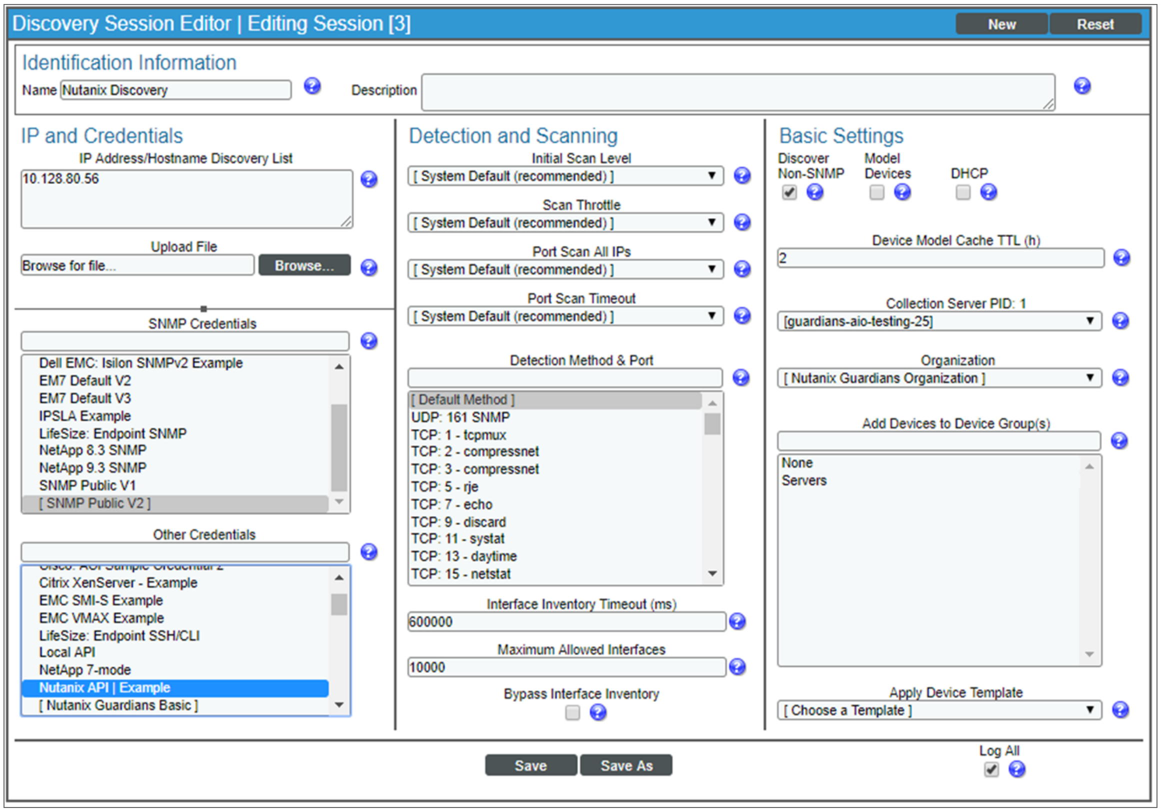
To model and monitor your Nutanix systems, you must run a discovery session to discover your Nutanix systems. The following diagram illustrates the way the discovery process works for Nutanix:


C Root
"Nutanix: Prism Element Config & Discovery"
"Nutanix: Prism Central Events"
"Nutanix: Prism Elements Discovery"
"Nutanix: Prism Central Config"
Nutanix: Prism Element Config & Discovery
Nutanix: Prism Elements Discovery
C Cluster
"Nutanix: Storage Pool Group Discovery"
"Nutanix: Health Check Catalog Cache"
"Nutanix: Collection Cache"
"Nutanix: Cluster Health Summary Stats"
"Nutanix: Hypervisor I/O Stats"
"Nutanix: Cluster Config & Block Discovery"
"Nutanix: Replication Stats"
"Nutanix: Storage Capacity and Usage Stats"
"Nutanix: Cluster I/O Stats"
"Nutanix: Controller I/O Stats"
"Nutanix: VMware Aggregator Config"
"Nutanix: License Status Config"
"Nutanix: Cluster Events"
"Nutanix: Health Check Run Config"
"Nutanix: Workload Group Discovery"
"Nutanix: Cluster Stats"
"Nutanix: Cache Usage Stats"
Nutanix: Cluster Config & Block Discovery
Nutanix: Workload Group Discovery
Nutanix: Storage Pool Group Discovery
C Block_Appliance
"Nutanix: Block Config & Host Discovery"
C Workload_Group
"Nutanix: Workload VMs Discovery"
C Virtual_Storage
"Nutanix: Storage Pools Discovery"
Nutanix: Block Config & Host Discovery
Nutanix: Workload VMs Discovery
Nutanix: Storage Pools Discovery
C Host_Hypervisor
"Nutanix: Host Storage Stats"
"Nutanix: Host Workload VMs Config"
"Nutanix: Host System Stats"
"Nutanix: Host I/O Stats"
"Nutanix: Host Config & Disk Discovery"
"Nutanix: Host Events"
"Nutanix: Host Cache Stats"
"Nutanix: Controller VM Discovery"
C Workload_VM
"Nutanix: VM Events"
"Nutanix: VM Config"
"Nutanix: VM I/O Stats"
C Storage_Pool
"Nutanix: Storage Pool Capacity and Usage Stats"
"Nutanix: Storage Container Discovery"
"Nutanix: Storage Pool I/O Stats"
"Nutanix: Storage Pool Config"
"Nutanix: Storage Pool Events"
Nutanix: Controller VM Discovery
Nutanix: Host Config & Disk Discovery
Nutanix: Storage Container Discovery
C Controller_VM
"Nutanix: Storage Containers Config"
"Nutanix: CVM Disks Config"
"Nutanix: CVM Events"
"Nutanix: CVM Config"
"Nutanix: CVM I/O Stats"
C Disk_Drive
"Nutanix: Disk I/O Stats"
"Nutanix: Disk Events"
"Nutanix: Disk Config"
C Storage_Containers
"Nutanix: Storage Container Capacity and Usage Stats"
"Nutanix: Container Workload VMs Config"
"Nutanix: Storage Container I/O Stats"
"Nutanix: Storage Container Events"
"Nutanix: Storage Container Config"

To create and run a discovery session that will discover your Nutanix system, perform the following steps:

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

2. Click the **[Create]** button to create a new discovery session. The **Discovery Session Editor** window appears:



Discovery Session Editor | Editing Session [3]

Identification Information

Name: Nutanix Discovery

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.128.80.56

Upload File: Browse for file...

SNMP Credentials: [SNMP Public V2]

Other Credentials: Nutanix API | Example

Detection and Scanning

Initial Scan Level: [System Default (recommended)]

Scan Throttle: [System Default (recommended)]

Port Scan All IPs: [System Default (recommended)]

Port Scan Timeout: [System Default (recommended)]

Detection Method & Port: [Default Method]

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: 1: [guardians-aio-testing-25]

Organization: [Nutanix Guardians Organization]

Add Devices to Device Group(s):

Apply Device Template: [Choose a Template]

Log All: ☑

3. Enter values in the following fields:

- ***IP Address Discovery List***. Type the IP addresses for the Nutanix systems you want to discover.

NOTE: Do not include both Prism Element and Prism Central devices in the ***IP Address Discovery List*** field. The *Nutanix: Base Pack* PowerPack supports discovery of individual Prism Element clusters OR a Prism Central device with multiple Prism Element clusters. It is recommended that customers use only one of these options.

- ***SNMP Credentials***. Select *SNMP Public V2* if applicable.
- ***Other Credentials***. Select the credential that you configured in the previous section.
- ***Discover Non-SNMP***. If you are not using an SNMP credential, ensure that this checkbox is selected.
- ***Organization***. Select your organization.

4. You can enter values in the other fields on this page, but are not required to and can simply accept the default values. 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 will appear at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon (⚡) to run the discovery session.
7. The **Discovery Session** window will be displayed.
8. When the Nutanix system is discovered, click its device icon (🖥) to view the **Device Properties** page for the Nutanix system.
9. After the Nutanix system is discovered, the child components and devices associated with that system will also appear in the **Device Manager** page.

NOTE: It can take up to 30 minutes for the Dynamic Applications and device class to align.

Verifying Discovery and Dynamic Application Alignment

Verifying Prism Elements Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Prism Elements Dynamic Applications during discovery:

1. From the **Device Properties** page for the Nutanix system, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. The "Nutanix: Prism Element Config & Discovery" Dynamic Application should be displayed in the list of Dynamic Applications aligned to the Nutanix system.

In addition, the "Nutanix: Prism Element Classify Root Device Class" Run Book Action will be triggered to automatically align the correct device class to the discovered root device.

Verifying Prism Central Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Prism Central Dynamic Applications during discovery:

1. From the **Device Properties** page for the Nutanix system, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. The following Dynamic Applications should be displayed in the list of Dynamic Applications aligned to the Nutanix system:
    - Nutanix: Prism Central Config
    - Nutanix: Prism Central Events
    - Nutanix: Prism Elements Discovery

In addition, the "Nutanix: Prism Central Classify Root Device Class" Run Book Action will be triggered to automatically align the correct device class to the discovered root device.

Configuring Virtual Device Alerts for Prism Central Devices

If you have chosen not to model virtual devices, but want to see alerts for those devices, you can configure virtual device alerts to appear on Prism Central devices.

To configure your Prism Central devices to display alerts for virtual devices:

1. Go to the **Dynamic Applications Manager** (System > Manage > Dynamic Applications) page.
2. Find the "Nutanix: Prism Central Events" Dynamic Application and click its wrench icon (🔧).
3. Click the **[Thresholds]** tab, and click the wrench icon (🔧) for the "Display Workload VM Alerts" Threshold Object.
4. In the ***Threshold Value*** field, type 1 and then click **[Save]**. Alerts for virtual devices will now appear on your Prism Central devices. By default, the Threshold Value is set to 0, and alerts will appear on the VM.

Chapter

60

OpenStack

Overview

The following sections describe how to configure OpenStack resources for monitoring by SL1 using the *OpenStack* PowerPack:

NOTE: For more information about the *OpenStack* PowerPack, see the ***Monitoring OpenStack*** manual.

Configuring OpenStack for Monitoring

To discover OpenStack resources for monitoring by SL1, you must create a SOAP/XML credential that includes authentication information for an OpenStack user.

The user whose information is used in this credential can be either an administrator or a regular (non-administrator) user. Administrator credentials enable SL1 to discover an OpenStack domain and resource pool; regular user credentials enable SL1 to discover only a single project within a specified domain and those components that the user has permissions for in the policy files. The recommended policy edits described in the ***Adding the User Role to API Policy Endpoints*** section will enable non-administrator users to discover resource pools.

The following sections describe how to assign a role to an OpenStack user and then add that user role to the appropriate API policy endpoints.

Prerequisites for Monitoring OpenStack

Before completing the following sections, you must have already created the OpenStack domain and projects you want to monitor, the user whose information you will include in the SOAP/XML credential, and the role you want to assign to that user.

TIP: ScienceLogic recommends that you create a new user role that will be used only for ScienceLogic monitoring and then add this ScienceLogic-specific user role to the policy endpoints described in the ***Adding the User Role to API Policy Endpoints*** section. Having a ScienceLogic-specific user role makes it easier to manage the role's policy permissions without having to change any of your existing user roles.

Assigning a Role to a User

After you have created the user whose information you will include in the SOAP/XML credential, you must assign that user a role in a specific project. This can be done either in the OpenStack portal or using the OpenStackClient command line interface. Both methods are described in this section.

Method 1: OpenStack Portal

To assign the user a role using the OpenStack portal:

1. Log in to the OpenStack portal and navigate to the **Projects** page (Identity > Projects).
2. Locate the project you want to monitor. In the **Actions** column, click **[Manage Members]**.
3. If the user whose information you will include in the SOAP/XML credential does not already appear in the **Project Members** list, locate the user in the **All Users** list and click the plus (+) icon for that user.
4. Locate the user in the **Project Members** list and use the drop-down menu next to the user's name to select the user's role.
5. Click **[Save]**.

Method 2: Command Line Interface

To add a role to the user in a project using the OpenStackClient (OSC) command line interface, SSH into OSC and then use the following command format:

```
openstack role add <role name> --project <project name> user <username>
```

Adding the User Role to API Policy Endpoints

After you have assigned the user a role, you must add the user's assigned role to endpoints in the following OpenStack API policies:

- Keystone (identity services)
- Nova (compute services)
- Neutron (networking services)
- Cinder (block storage services)

For example, to allow a user to list OpenStack projects, Keystone's policy.json file needs to include the following rule:

```
 "identity:list_projects" : "role: <user-role>"
```

A rule can also contain multiple roles by using the "or" syntax. For example:

```
 "identity:list_projects" : "role: <user-role-1> or role: <user-role-2>"
```

By default, a role can be any of the following:

- admin
- user
- member

Policy Permissions for Administrators

For administrator users, you must update the following policies:

Keystone Policy

An administrator user defined in the SOAP/XML credential needs permissions to the following endpoints defined in /etc/keystone/policy.json:

- identity:get_region
- identity:list_regions
- identity:get_endpoint
- identity:list_endpoints
- identity:get_domain
- identity:list_domains
- identity:get_project
- identity:list_projects

Nova Policy

An administrator user defined in the SOAP/XML credential needs permissions to the following endpoints defined in /etc/nova/policy.json:

- os_compute_api:os-aggregates:index
- os_compute_api:os-aggregates:show
- os_compute_api:os-extended-server-attributes
- os_compute_api:flavors
- os_compute_api:os-hosts
- os_compute_api:os-hypervisors
- os_compute_api:limits
- os_compute_api:os-networks
- os_compute_api:os-networks:view
- os_compute_api:os-networks-associate
- os_compute_api:os-security-group-default-rules
- os_compute_api:os-security-groups
- os_compute_api:os-server-diagnostics
- os_compute_api:os-server-groups
- os_compute_api:os-server-usage
- os_compute_api:servers:detail
- os_compute_api:servers:index:get_all_tenants
- os_compute_api:servers:detail:get_all_tenants
- os_compute_api:servers:show
- os_compute_api:servers:show:host_status
- os_compute_api:os-services
- os_compute_api:os-simple-tenant-usage:show
- os_compute_api:os-simple-tenant-usage:list
- os_compute_api:os-tenant-networks
- os_compute_api:os-virtual-interfaces
- os_compute_api:os-volumes
- os_compute_api:os-volumes-attachments:show

Neutron Policy

An administrator user defined in the SOAP/XML credential needs permissions to the following endpoints defined in /etc/neutron/policy.json:

- get_subnet

- get_subnet:segment_id
- get_subnetpool
- get_address_scope
- get_network
- get_network:router:external
- get_network:segments
- get_network:provider:network_type
- get_network:provider:physical_network
- get_network:provider:segmentation_id
- get_network:queue_id
- get_network_ip_availabilities
- get_network_ip_availability
- get_segment
- get_port
- get_port:queue_id
- get_router
- get_router:distributed
- get_router:ha
- get_dhcp-networks
- get_l3-routers
- get_network_profiles
- get_network_profile
- get_flavors
- get_flavor

Cinder Policy

An administrator user defined in the SOAP/XML credential needs permission to the following endpoint defined in /etc/cinder/policy.json:

- volume_extension:services:index

Policy Permissions for Non-Administrator Users

For regular (non-administrator) users, you must update the following policies:

Keystone Policy

A regular user defined in the SOAP/XML credential needs permissions to the following endpoints defined in /etc/keystone/policy.json:

- identity:get_region
- identity:list_regions
- identity:get_endpoint
- identity:list_endpoints
- identity:get_domain
- identity:list_domains
- identity:get_project
- identity:list_projects

Nova Policy

A regular user defined in the SOAP/XML credential needs permissions to the following endpoints defined in /etc/nova/policy.json:

- os_compute_api:os-aggregates:index
- os_compute_api:os-aggregates:show
- os_compute_api:os-extended-server-attributes
- os_compute_api:flavors
- os_compute_api:os-hosts
- os_compute_api:os-hypervisors
- os_compute_api:limits
- os_compute_api:os-networks
- os_compute_api:os-networks:view
- os_compute_api:os-networks-associate
- os_compute_api:os-security-group-default-rules
- os_compute_api:os-security-groups
- os_compute_api:os-server-diagnostics
- os_compute_api:os-server-groups
- os_compute_api:os-server-usage
- os_compute_api:servers:detail
- os_compute_api:servers:index:get_all_tenants

- os_compute_api:servers:detail:get_all_tenants
- os_compute_api:servers:show
- os_compute_api:servers:show:host_status
- os_compute_api:os-services
- os_compute_api:os-simple-tenant-usage:show
- os_compute_api:os-simple-tenant-usage:list
- os_compute_api:os-tenant-networks
- os_compute_api:os-virtual-interfaces
- os_compute_api:os-volumes
- os_compute_api:os-volumes-attachments:show

Neutron Policy

A regular user defined in the SOAP/XML credential needs permissions to the following endpoints defined in /etc/neutron/policy.json:

- get_subnet
- get_subnet:segment_id
- get_subnetpool
- get_address_scope
- get_network
- get_network:router:external
- get_network:segments
- get_network:provider:network_type
- get_network:provider:physical_network
- get_network:provider:segmentation_id
- get_network:queue_id
- get_network_ip_availabilities
- get_network_ip_availability
- get_segment
- get_port
- get_port:queue_id
- get_router
- get_router:distributed
- get_router:ha
- get_dhcp-networks
- get_l3-routers

- get_network_profiles
- get_network_profile
- get_flavors
- get_flavor

Creating a SOAP/XML Credential for OpenStack

To configure SL1 to monitor OpenStack, you must first create a SOAP/XML credential. This credential allows the Dynamic Applications in the *OpenStack* PowerPack to communicate with your OpenStack domain.

The PowerPack includes two example SOAP/XML credentials that you can edit for your own use:

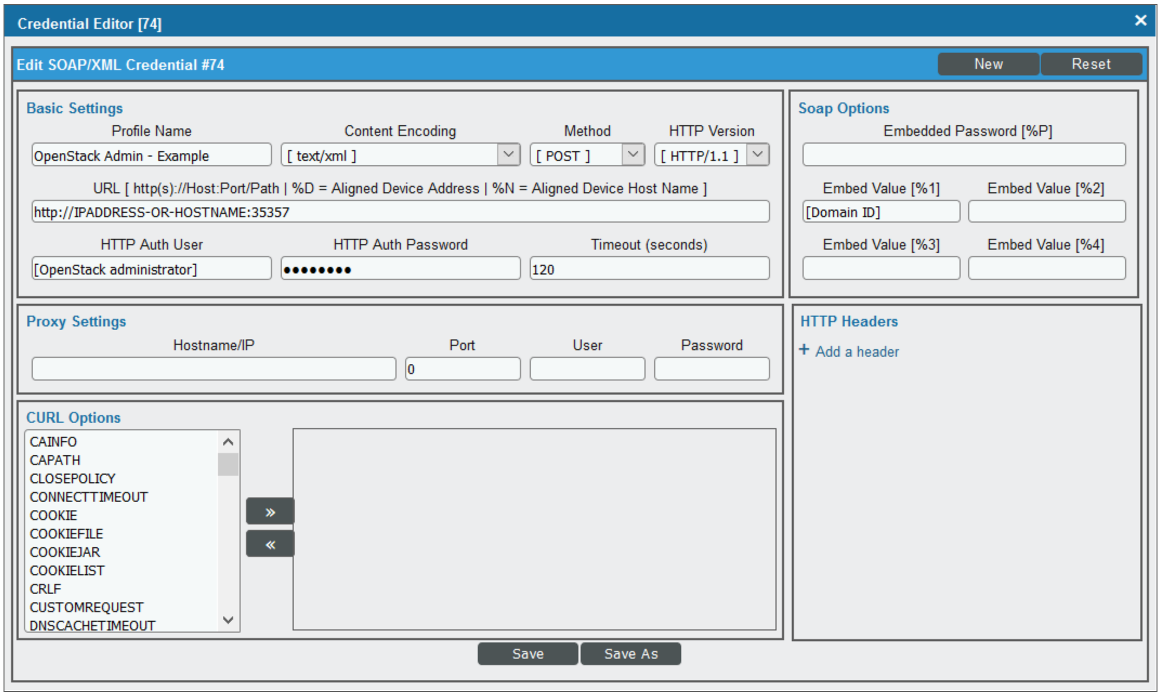
- **OpenStack Admin - Example**. This credential is for administrators and will discover all projects contained within the specified domain.
- **OpenStack User - Example**. This credential is for regular (non-administrator) users and will discover a single project within a specified domain and those components that the user has permissions for in the policy files.

> NOTE: During discovery, SL1 discovers only those OpenStack components within the single domain that is specified in the SOAP/XML credential, regardless of whether the credential is for an administrator or a regular user. To discover multiple domains, you must create a separate credential for each domain, which results in each domain being discovered with its own separate dynamic component map. To load-balance multiple domains, ScienceLogic recommends discovering different domains on different Data Collectors or All-In-One Appliances.

To configure a SOAP/XML credential to access OpenStack:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **OpenStack Admin - Example** or **OpenStack User - Example** credential, then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears.

3. Complete the following fields:



Credential Editor [74]

Edit SOAP/XML Credential #74

Basic Settings

Profile Name: OpenStack Admin - Example

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: http://IPADDRESS-OR-HOSTNAME:35357

HTTP Auth User: [OpenStack administrator]

HTTP Auth Password: ••••••••

Timeout (seconds): 120

Soap Options

Embedded Password [%P]:

Embed Value [%1]: [Domain ID]

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

Proxy Settings

Hostname/IP:

Port: 0

User:

Password:

HTTP Headers

CURL Options

Basic Settings

- *Profile Name*. Type a name for the OpenStack credential.
- *Content Encoding*. Select *text/xml*.
- *Method*. Select POST.
- *HTTP Version*. Select HTTP/1.1.
- *URL*. Type "http://<IP Address>:<Port>", replacing <IP address> with the IP address or hostname of the OpenStack domain and replacing <Port> with the appropriate port number.
- *HTTP Auth User*. Type the OpenStack username.
- *HTTP Auth Password*. Type the OpenStack user's password.
- *Timeout (seconds)*. Type "120".

Proxy Settings

- *Hostname/IP*. Leave this field blank.
- *Port*. Type "0".
- *User*. Leave this field blank.
- *Password*. 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 the OpenStack domain ID.
- ***Embed Value [%2]***. If you are creating a credential for a regular (non-administrator) user, type the OpenStack project name. Otherwise, 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.

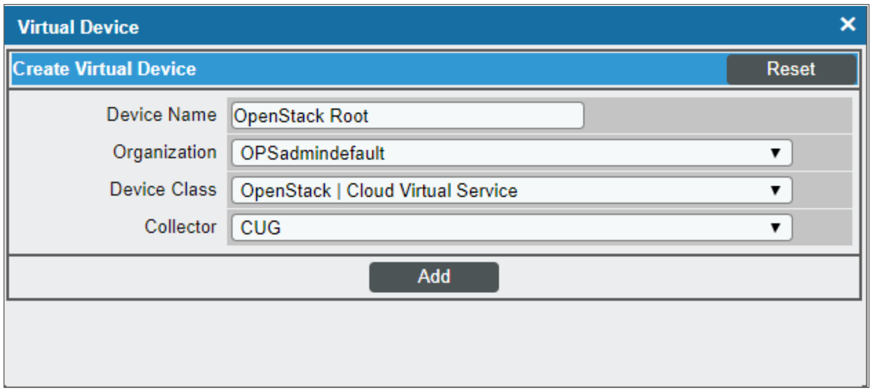
4. Click the **[Save As]** button.

Creating an OpenStack Virtual Device

To discover OpenStack resources, you must first create a ***virtual device*** that represents the root device for the OpenStack domain. A virtual device is a user-defined container that represents a device or service that cannot be discovered by SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications.

To create a virtual device that represents your OpenStack root device:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Click the **[Actions]** button and select *Create Virtual Device* from the menu. The **Virtual Device** modal page appears.
3. Complete the following fields:



Virtual Device

Create Virtual Device

Device Name	OpenStack Root
Organization	OPSadmindefault
Device Class	OpenStack | Cloud Virtual Service
Collector	CUG

- ***Device Name***. Type a name for the device.

- ***Organization***. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.
- ***Device Class***. Select *OpenStack | Cloud Virtual Service*.
- ***Collector***. Select the collector group that will monitor the device.

4. Click the **[Add]** button to create the virtual device.

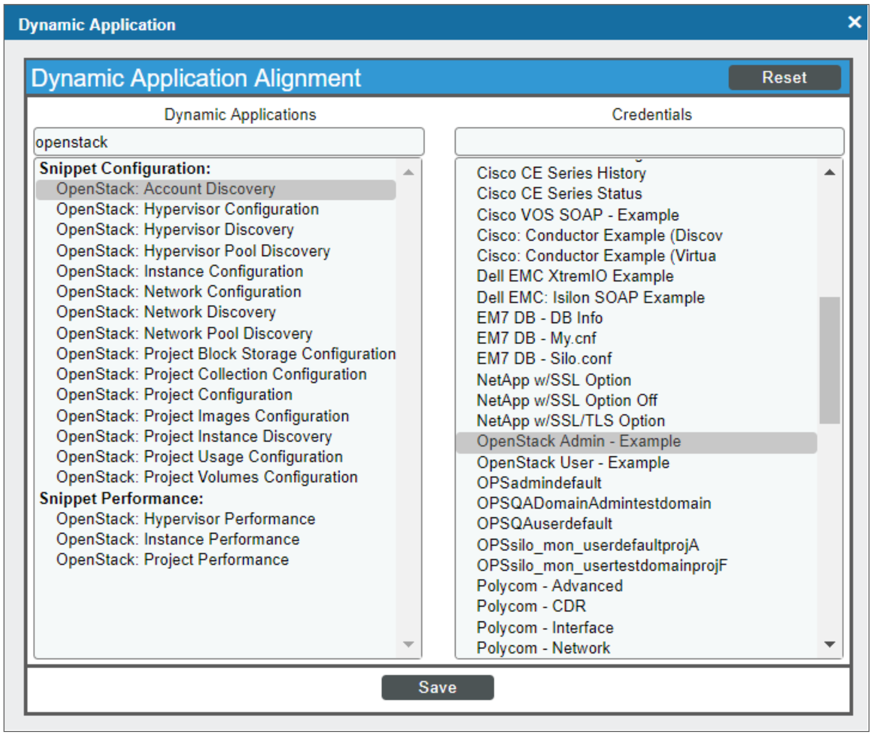
Discovering OpenStack Component Devices

To discover and model the components of your OpenStack domain, you must manually align the "OpenStack: Account Discovery" Dynamic Application with the OpenStack virtual device. When you do so, the "OpenStack: Account Discovery" Dynamic Application uses the virtual device as the root component device representing the OpenStack account and creates child component devices for all of the resources used by that account.

To align the "OpenStack: Account Discovery" Dynamic Application to your OpenStack virtual device:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Click the wrench icon (🔧) for your OpenStack virtual device.
3. In the **Device Administration** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
4. Click the **[Action]** button and select *Add Dynamic Application* from the menu.

5. On the **Dynamic Application Alignment** modal page:


Dynamic Application
×
Dynamic Application Alignment
Reset
Dynamic Applications
Credentials
openstack
Snippet Configuration:
OpenStack: Account Discovery
OpenStack: Hypervisor Configuration
OpenStack: Hypervisor Discovery
OpenStack: Hypervisor Pool Discovery
OpenStack: Instance Configuration
OpenStack: Network Configuration
OpenStack: Network Discovery
OpenStack: Network Pool Discovery
OpenStack: Project Block Storage Configuration
OpenStack: Project Collection Configuration
OpenStack: Project Configuration
OpenStack: Project Images Configuration
OpenStack: Project Instance Discovery
OpenStack: Project Usage Configuration
OpenStack: Project Volumes Configuration
Snippet Performance:
OpenStack: Hypervisor Performance
OpenStack: Instance Performance
OpenStack: Project Performance
Cisco CE Series History
Cisco CE Series Status
Cisco VOS SOAP - Example
Cisco: Conductor Example (Discov
Cisco: Conductor Example (Virtua
Dell EMC XtremIO Example
Dell EMC: Isilon SOAP Example
EM7 DB - DB Info
EM7 DB - My.cnf
EM7 DB - Silo.conf
NetApp w/SSL Option
NetApp w/SSL Option Off
NetApp w/SSL/TLS Option
OpenStack Admin - Example
OpenStack User - Example
OPSadmindefault
OPSQADomainAdmintestdomain
OPSQAuserdefault
OPSsilo_mon_userdefaultprojA
OPSsilo_mon_usertestdomainprojF
Polycom - Advanced
Polycom - CDR
Polycom - Interface
Polycom - Network
Save

- In the ***Dynamic Applications*** field, select *OpenStack: Account Discovery*.
- In the ***Credentials*** field, select the credential you created for OpenStack.

6. Click the **[Save]** button to align the Dynamic Application with the OpenStack virtual device and discover the OpenStack domain and resources.

Relationships Between Component Devices

In addition to parent/child relationships between component devices, SL1 also creates relationships between the following component devices:

- Virtual machines and hypervisors
- Virtual machines and networks

Chapter

61

Oracle: Database

Overview

The following sections describe how to configure and discover your Oracle Database instances for monitoring by SL1 using the *Oracle: Database* PowerPack:

NOTE: For more information about the *Oracle: Database* PowerPack, see the ***Monitoring Oracle*** manual.

Prerequisites for Monitoring Oracle Database Instances

To configure the SL1 system to monitor Oracle Database instances using the *Oracle: Database* PowerPack, you must first have the following prerequisites and permissions:

- The Oracle database user must have access the following privileges:
  - sys_privileges: GRANT CREATE SESSION
  - role_privileges: GRANT SELECT_CATALOG_ROLE
  - tan_privileges: GRANT SELECT ON SYS.V_$DIAG_ALERT_EXT, GRANT SELECT ON SYS.TS$
- The Oracle database user must have access to the following tables:
  - all_tables
  - dba_data_files
  - dba_free_space
  - dba_registry
  - dba_scheduler_jobs_broken
  - dba_scheduler_jobs_failed
  - dba_tablespaces
  - dba_temp_files
  - gv$sort_segment
  - sessions_info
  - sys.dba_ind_partitions
  - sys.dba_ind_subpartitions
  - sys.dba_indexes
  - sys.dba_objects
  - sys.v_$database_block_corruption
  - v$archive_dest
  - v$archived_log
  - v$block_change_tracking
  - v$controlfile
  - v$database
  - v$datafile
  - v$datafile_header
  - v$diag_alert_ext
  - v$dispatcher
  - v$latch
  - v$librarycache
  - v$log
  - v$log_history
  - v$logfile
  - v$open_cursor
  - v$parameter

- v$resource_limit
- v$rollstat
- v$rowcache
- v$session
- v$sesstat
- v$statname
- v$sysstat
- v$tablespace
- v$tempfile
- v$version

- If you are monitoring an RAC system, the user must have access to the following:
  - v$asm_diskgroup
  - v$recovery_file_dest
- The Oracle database user must have permission to alter sessions.

Configuring Oracle Credentials

To monitor Oracle Database instances using SL1, you must create two credentials. The types of credentials that are required for monitoring depend on the type of server that is hosting the Oracle Database:

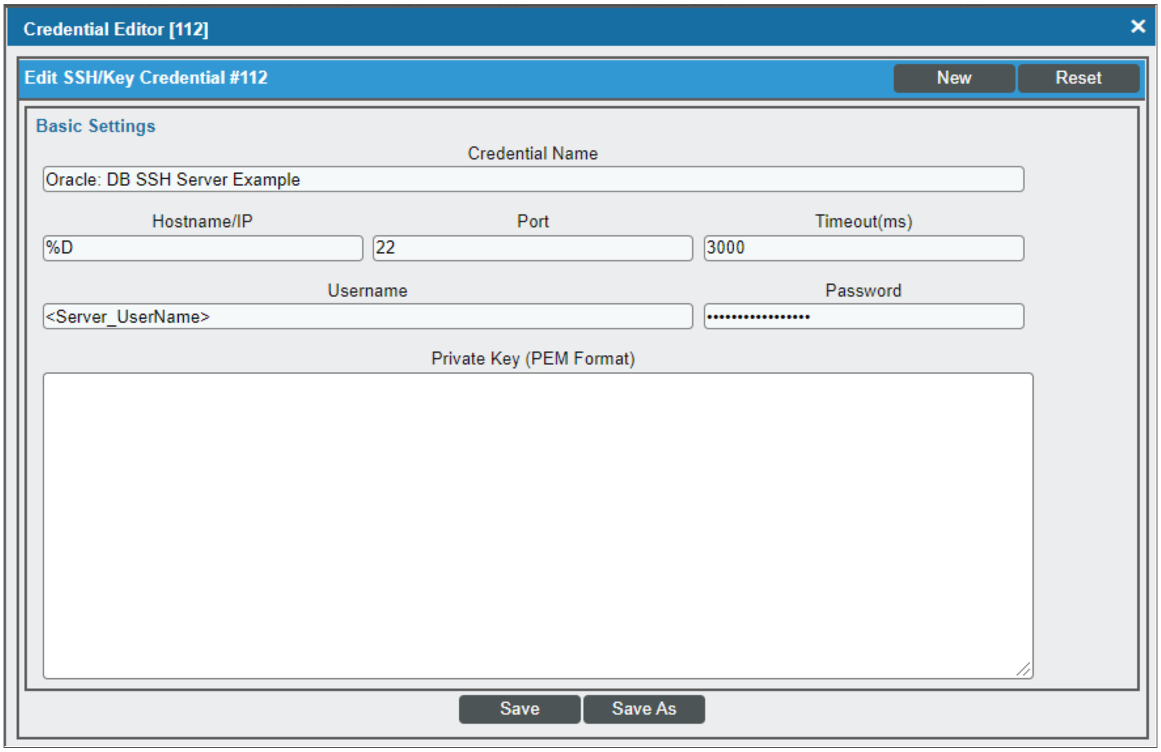
- Linux and Unix users must use an *SSH/Key credential* and a *SOAP/XML credential*
- Windows users must use a *PowerShell credential* and a *SOAP/XML credential*

Creating an SSH/Key Credential (Linux Users)

Linux and Unix users must create an SSH/Key credential.

To create an SSH/Key credential :

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the wrench icon (🔧) for the "Oracle: DB SSH Server Example" credential. The **Credential Editor** modal page appears:



Credential Editor [112]

Edit SSH/Key Credential #112

Basic Settings

Credential Name: Oracle: DB SSH Server Example

Hostname/IP: %D

Port: 22

Timeout(ms): 3000

Username: <Server_UserName>

Password: •••••••••••••••••

Private Key (PEM Format):

3. Supply values in the following fields:

    - ***Credential Name***. Type a new name for the credential.
    - ***Hostname/IP.*** Type "%D" or the IP address of the server that is hosting the Oracle Database.
    - ***Port***. Type 22.
    - ***Username***. Type the username for the Linux server that is hosting the Oracle Database.
    - ***Password***. Type the password for the Linux server that is hosting the Oracle Database.
    - ***Private Key (PEM Format)***. Optional. Use if required for SSH authentication. For information on gathering a private key, see the section on ***Enabling PEM on a Linux Machine***.

4. Click the **[Save As]** button.
5. When the confirmation message appears, click **[OK]**.

NOTE: The credential ID will appear at the top of the window after it has been saved. Take note of the ID as you will need it when creating the SOAP/XML credential.

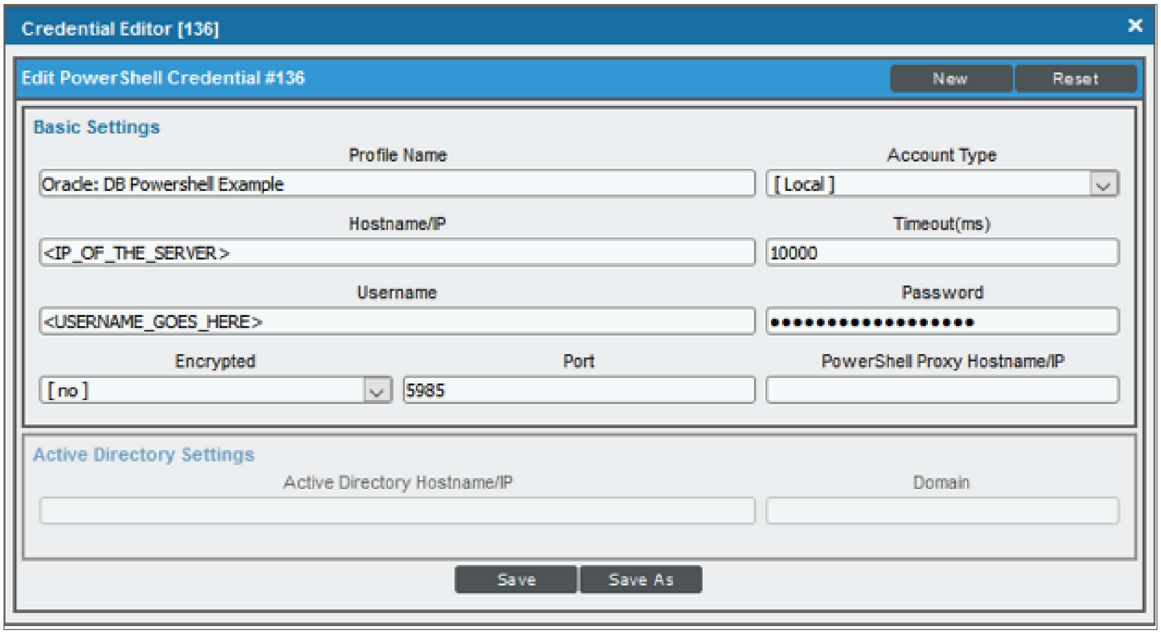
Creating a PowerShell Credential (Windows Users)

Windows users must create a PowerShell credential.

To create a PowerShell credential:

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

2. Click the wrench icon (🔧) for the "Oracle: DB Powershell Example" credential. The **Credential Editor** modal page appears:



Credential Editor [136]

Edit PowerShell Credential #136

Basic Settings

Profile Name	Oracle: DB Powershell Example
Account Type	[Local]
Hostname/IP	<IP_OF_THE_SERVER>
Timeout(ms)	10000
Username	<USERNAME_GOES_HERE>
Password	●●●●●●●●●●●●●●●●●●
Encrypted	[no]
Port	5985
PowerShell Proxy Hostname/IP	

Active Directory Settings

Active Directory Hostname/IP	
Domain	

3. Supply values in the following fields:

   - ***Profile Name***. Type a new name for the credential.
   - ***Account Type***. Select *Local*. Servers that are part of an Active Directory are not supported.
   - ***Hostname/IP***. Type "%D" or the IP address of the server that is hosting the Oracle Database.
   - ***Timeout (ms)***. Type the time, in milliseconds, after which SL1 will stop trying to collect data from the authenticating server. For collection to be successful, SL1 must connect to the authenticating server, execute the PowerShell command, and receive a response within the amount of time specified in this field.
   - ***Username***. Type the username for the Windows server that is hosting the Oracle Database.
   - ***Password***. Type the password for the Windows server that is hosting the Oracle Database.
   - ***Encrypted***. Select whether SL1 will communicate with the device using an encrypted connection. Choices are:
     - *yes*. When communicating with the Windows server, SL1 will use a local user account with authentication of type "Basic Auth". You must then use HTTPS and can use a Microsoft Certificate or a self-signed certificate.
     - *no*. When communicating with the Windows server, SL1 will not encrypt the connection.
   - ***Port***. Type 5985 (http) or 5986 (https).
   - ***PowerShell Proxy Hostname/IP***. Leave this field blank.

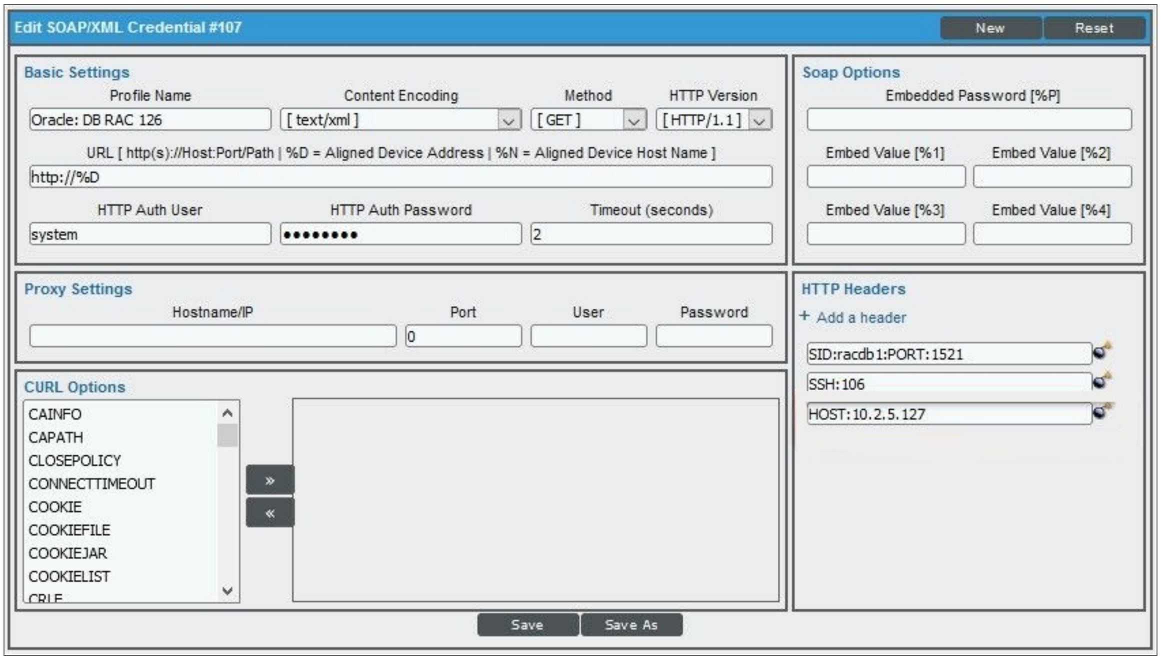
4. Click the **[Save As]** button.

> **NOTE:** The credential ID will appear at the top of the window after it has been saved. Take note of the ID as you will need it when creating the SOAP/XML credential.

Creating a SOAP/XML Credential

To create the SOAP/XML credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the wrench icon (🔧) for either the "Oracle: DB Example" credential for Windows users. The **Credential Editor** modal page appears:



Edit SOAP/XML Credential #107

Basic Settings

Profile Name: Oracle: DB RAC 126

Content Encoding: [text/xml]

Method: [GET]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: http://%D

HTTP Auth User: system

HTTP Auth Password: ••••••••

Timeout (seconds): 2

Proxy Settings

Hostname/IP:

Port: 0

User:

Password:

Soap Options

Embedded Password [%P]:

Embed Value [%1]:

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

HTTP Headers

SID:racdb1:PORT:1521

SSH:106

HOST:10.2.5.127

3. Update the values in the following fields:

Basic Settings

- ***Profile Name***. Type a new name for the credential.
- ***URL***. Leave the default value of https://%D.
- ***HTTP Auth User***. Type the username for the Oracle Database account.
- ***HTTP Auth Password***. Type the password for the Oracle Database account.

NOTE: Discovering multiple instances on a single database server is supported, but all instances must share the same credentials entered in the SOAP/XML credential's ***HTTP Auth User*** and ***HTTP Auth Password*** fields.

HTTP Headers

- ***HTTP Headers***. Add the following headers by clicking ***+ Add a header***. A header should be added for each Oracle Database instance you are monitoring:
  - `SID: <Oracle Instance SID>:PORT<Oracle Instance Port that is listening for DB requests>`. For example:

    ```
    SID:SL121:PORT:22
    ```

    For ASM instances, add "ASM" as the SID value. The entire ASM name must be added as the SID value. For example, if +ASM1 is the name, the header will be:

    ```
    SID:+ASM:PORT:1521
    ```

    If a host, or IP address, for the Oracle: Database is assigned to a different IP address from the server, you must add an additional header to the SOAP credential. For example:

    ```
    HOST:<host_address> (i.e. HOST:10.2.5.95)
    OR
    HOST:FROM_LISTENER
    ```

NOTE: Only the SIDs listed in the credential will be discovered.

NOTE: For ASM instances, all Dynamic Applications (except the RAC Dynamic Applications) will be aligned to the instance but will show "NO DATA".

  - `<OS_TYPE>:<CRED_ID>`. The OS type and ID of the SSH/Key credential or PowerShell credential you created. For OS type, enter SSH for Linux or PSH for Windows. For example:

    ```
    SSH:152

    or

    PSH:153
    ```

NOTE: Only one OS type per credential is supported.

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

Enabling PEM on a Linux Machine

Linux and Unix users can create an SSH/Key credential in order to monitor Oracle Database instances in SL1. The ***Private Key (PEM Format)*** field may be filled when *creating an SSH/Key credential*. To enable PEM on a Linux machine, perform the following steps:

1. Create a PEM folder to place the identity keys.

> **NOTE:** ScienceLogic suggests that you create a PEM folder inside the .ssh folder of the user that will use the PEM authentication.

2. Run the following command on your Linux machine to create the SSH key. This command will create public and private keys:

```
ssh-keygen -b 2048 -f identity - t rsa
```

> **NOTE:** The value "identity" in the command above will be the name of the file that is generated. This value can be replaced with any file name.

3. The private key generated from this command is the .pem file needed for the SSH/Key credential. Copy the contents of the file to input into the SL1 credential.
4. Add the generated public key to the `authorized_keys` file that is found in `~/.ssh/authorized_keys` manually or by using the following command:

```
cat identity.pub >> ~/.ssh/authorized_keys
```

5. Restart the SSH service by running the following command:

```
sudo service ssh restart
```

Following the steps above, you can create an SSH/Key credential in SL1 by supplying your Linux server username, Linux server password, and private key. If you would like to create an SSH/Key credential by supplying only your Linux server username and private key, perform the following steps on your Linux machine:

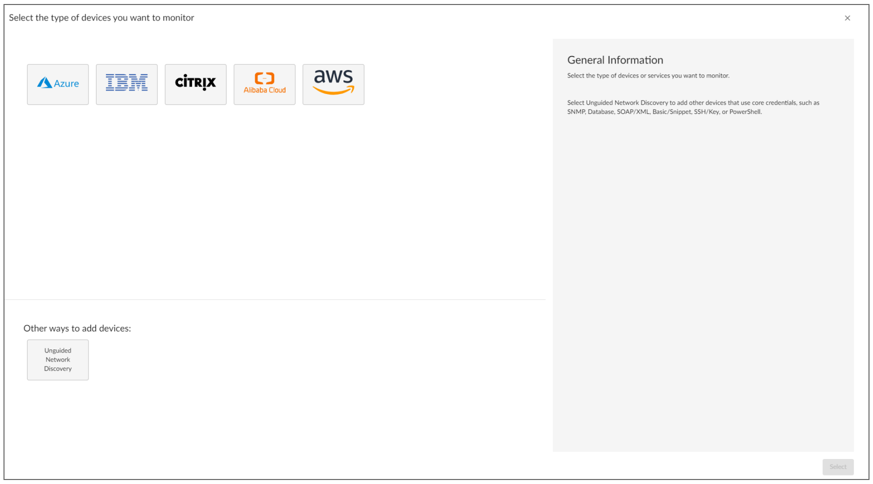
1. Find the `sshd_config` file.
2. Find the `PasswordAuthentication` command line, delete `yes`, and input `no`.
3. Restart the SSH service by running the following command:

```
sudo service ssh restart
```

Discovering Oracle Database Instances

To create and run a discovery session that will discover an Oracle instance, perform the following steps:

1. On the **Devices** page (🖳) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears:



Select the type of devices you want to monitor

General Information

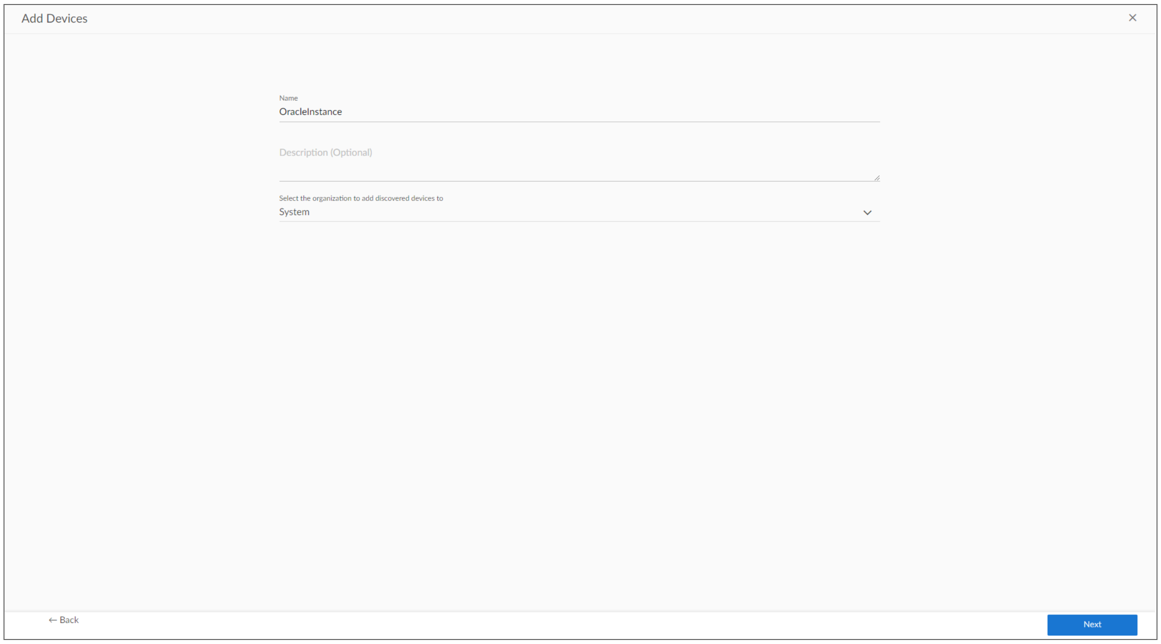
Select the type of devices or services you want to monitor.

Select Unguided Network Discovery to add other devices that use core credentials, such as SNMP, Database, SOAP/XML, Basic/Snippet, SSH/Key, or PowerShell.

Other ways to add devices:

2. Click the **[Unguided Network Discovery]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.

3. Click **[Select]**. The **Add Devices** page appears:



Add Devices

Name: OracleInstance

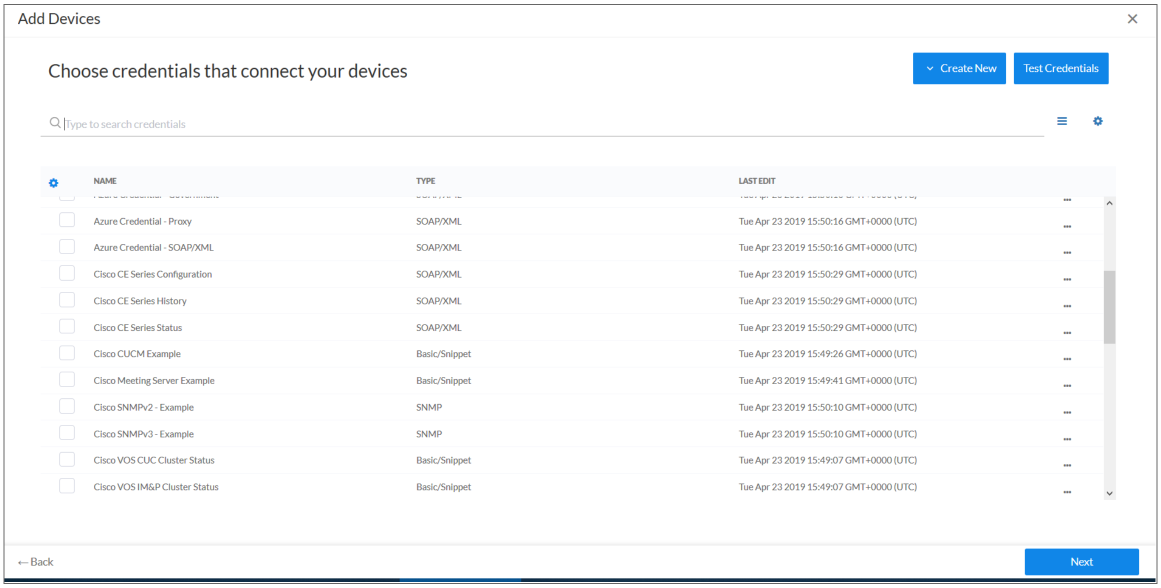
Description (Optional)

Select the organization to add discovered devices to: System

4. Complete the following fields:

   - ***Name***. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.
   - ***Description***. Optional. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **[Discovery Sessions]** tab.
   - ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered devices.

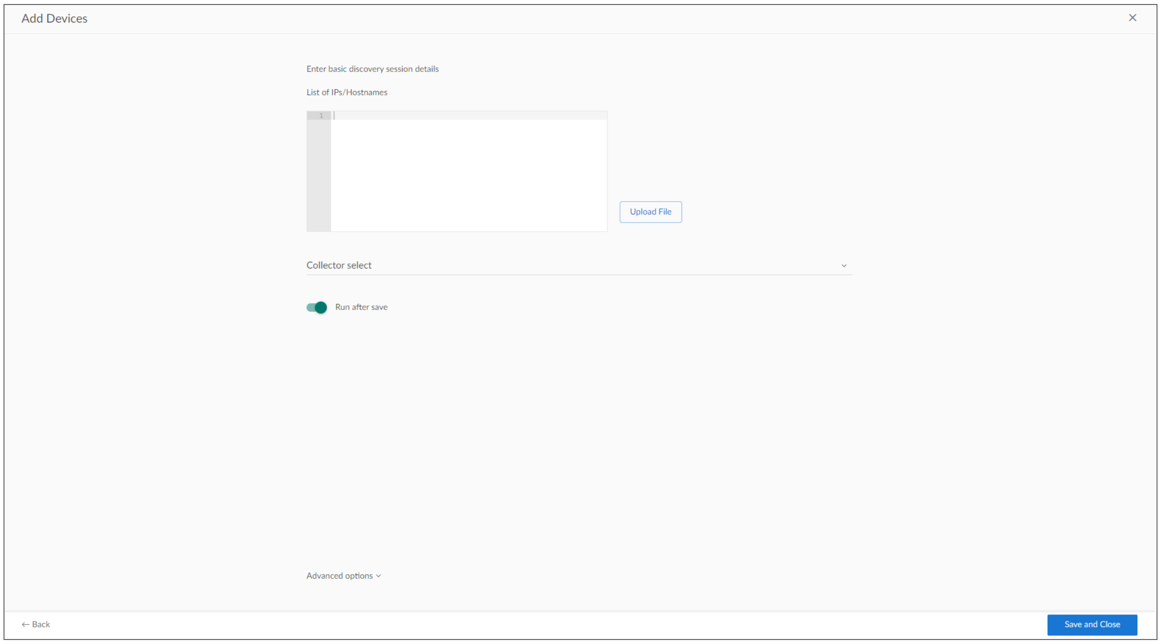
5. Click **[Next]**. The **Credentials** page of the **Add Devices** wizard appears:


Add Devices
×
Choose credentials that connect your devices
Create New
Test Credentials
Type to search credentials
← Back
Next

	NAME	TYPE	LAST EDIT	
□	Azure Credential - Government	SOAP/XML	[illegible]	...
□	Azure Credential - Proxy	SOAP/XML	Tue Apr 23 2019 15:50:16 GMT+0000 (UTC)	...
□	Azure Credential - SOAP/XML	SOAP/XML	Tue Apr 23 2019 15:50:16 GMT+0000 (UTC)	...
□	Cisco CE Series Configuration	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)	...
□	Cisco CE Series History	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)	...
□	Cisco CE Series Status	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)	...
□	Cisco CUCM Example	Basic/Snippet	Tue Apr 23 2019 15:49:26 GMT+0000 (UTC)	...
□	Cisco Meeting Server Example	Basic/Snippet	Tue Apr 23 2019 15:49:41 GMT+0000 (UTC)	...
□	Cisco SNMPv2 - Example	SNMP	Tue Apr 23 2019 15:50:10 GMT+0000 (UTC)	...
□	Cisco SNMPv3 - Example	SNMP	Tue Apr 23 2019 15:50:10 GMT+0000 (UTC)	...
□	Cisco VOS CUC Cluster Status	Basic/Snippet	Tue Apr 23 2019 15:49:07 GMT+0000 (UTC)	...
□	Cisco VOS IM&P Cluster Status	Basic/Snippet	Tue Apr 23 2019 15:49:07 GMT+0000 (UTC)	...

6. On the **Credentials** page, select the *SOAP/XML credential* you created.

7. Click **[Next]**. The **Discovery Session Details** page of the **Add Devices** wizard appears:



8. Complete the following fields:

    - ***List of IPs/Hostnames***. Type the IP address for the server that is hosting your Oracle Database.

    - ***Which collector will monitor these devices?***. Select an existing collector to monitor the discovered devices. Required.

    - ***Run after save***. Select this option to run this discovery session as soon as you click **[Save and Close]**.

      In the **Advanced options** section, click the down arrow icon (⌄) to complete the following fields:

      - ***Discover Non-SNMP***. Enable this setting.

      - ***Model Devices***. Enable this setting.

9. Click **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.

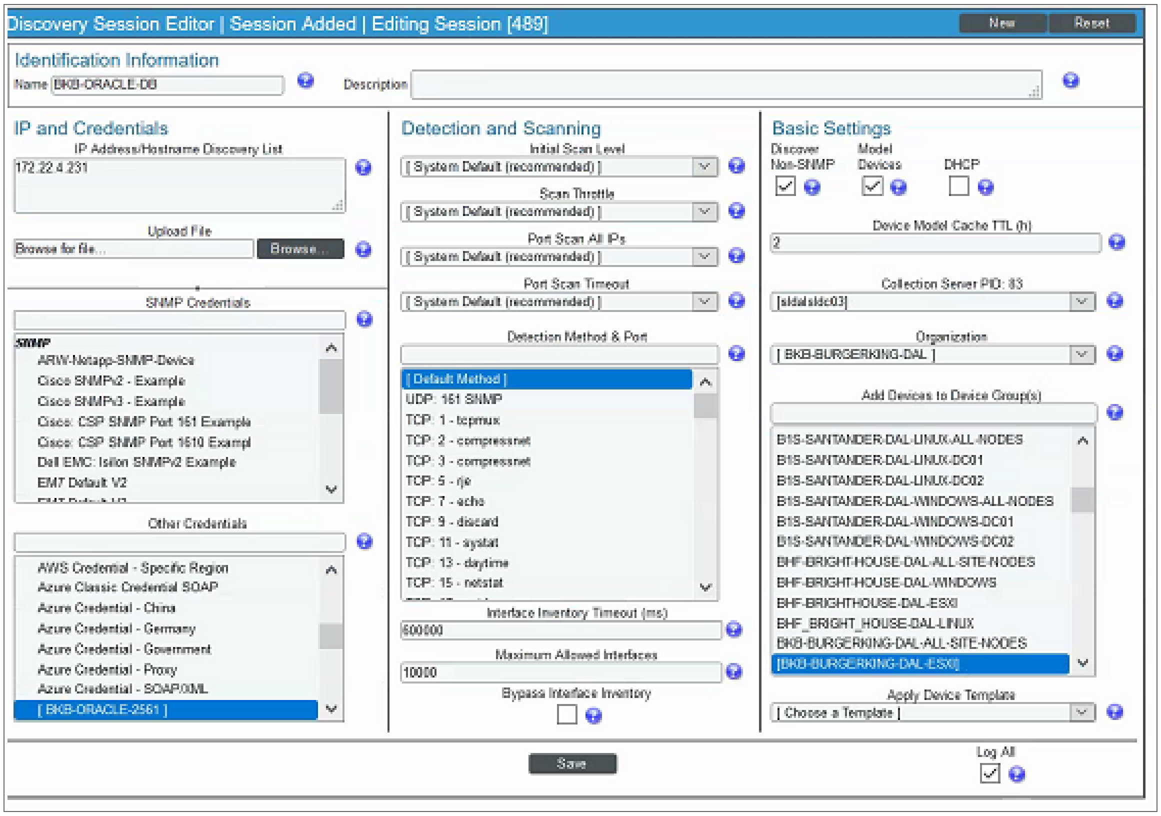
10. If you selected the **Run after save** option on this page, the discovery session runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page includes a link to the **Device Investigator** page for the discovered device.

Discovering Oracle Database Instances in the SL1 Classic User Interface

To model and monitor your Oracle Database instances, you must run a discovery session. To create and run a discovery session that will discover your Oracle Database instances, perform the following steps:

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

2. Click the **[Create]** button to create a new discovery session. The **Discovery Session Editor** window appears:



Discovery Session Editor | Session Added | Editing Session [489]

Identification Information

Name: BKB-ORACLE-DB

Description:

IP and Credentials

IP Address/Hostname Discovery List: 172.22.4.231

Upload File: Browse for file...

SNMP Credentials

Other Credentials: [BKB-ORACLE-2561]

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]

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: 83: [sldalsldc03]

Organization: [BKB-BURGERKING-DAL]

Add Devices to Device Group(s): [BKB-BURGERKING-DAL-ESXI]

Apply Device Template: [Choose a Template]

Log All: ☑

New
Reset
Browse...
SNMP
ARW-Netapp-SNMP-Device
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Cisco: CSP SNMP Port 161 Example
Cisco: CSP SNMP Port 1610 Exampl
Dell EMC: Isilon SNMPv2 Example
EM7 Default V2
AWS Credential - Specific Region
Azure Classic Credential SOAP
Azure Credential - China
Azure Credential - Germany
Azure Credential - Government
Azure Credential - Proxy
Azure Credential - SOAP/XML
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
B1S-SANTANDER-DAL-LINUX-ALL-NODES
B1S-SANTANDER-DAL-LINUX-DC01
B1S-SANTANDER-DAL-LINUX-DC02
B1S-SANTANDER-DAL-WINDOWS-ALL-NODES
B1S-SANTANDER-DAL-WINDOWS-DC01
B1S-SANTANDER-DAL-WINDOWS-DC02
BHF-BRIGHT-HOUSE-DAL-ALL-SITE-NODES
BHF-BRIGHT-HOUSE-DAL-WINDOWS
BHF-BRIGHTHOUSE-DAL-ESXI
BHF_BRIGHT_HOUSE-DAL-LINUX
BKB-BURGERKING-DAL-ALL-SITE-NODES
Save

3. Enter values in the following fields:

    - ***IP Address Discovery List***. Type the IP address for the server that is hosting your Oracle Database. One discovery session per server is supported. The IP address can be assigned to a different IP address than the server.
    - ***Other Credentials***. Select the SOAP/XML credential that you configured in the previous section.
    - ***Discover Non-SNMP***. Select this checkbox.
    - ***Model Devices***. Select this checkbox.

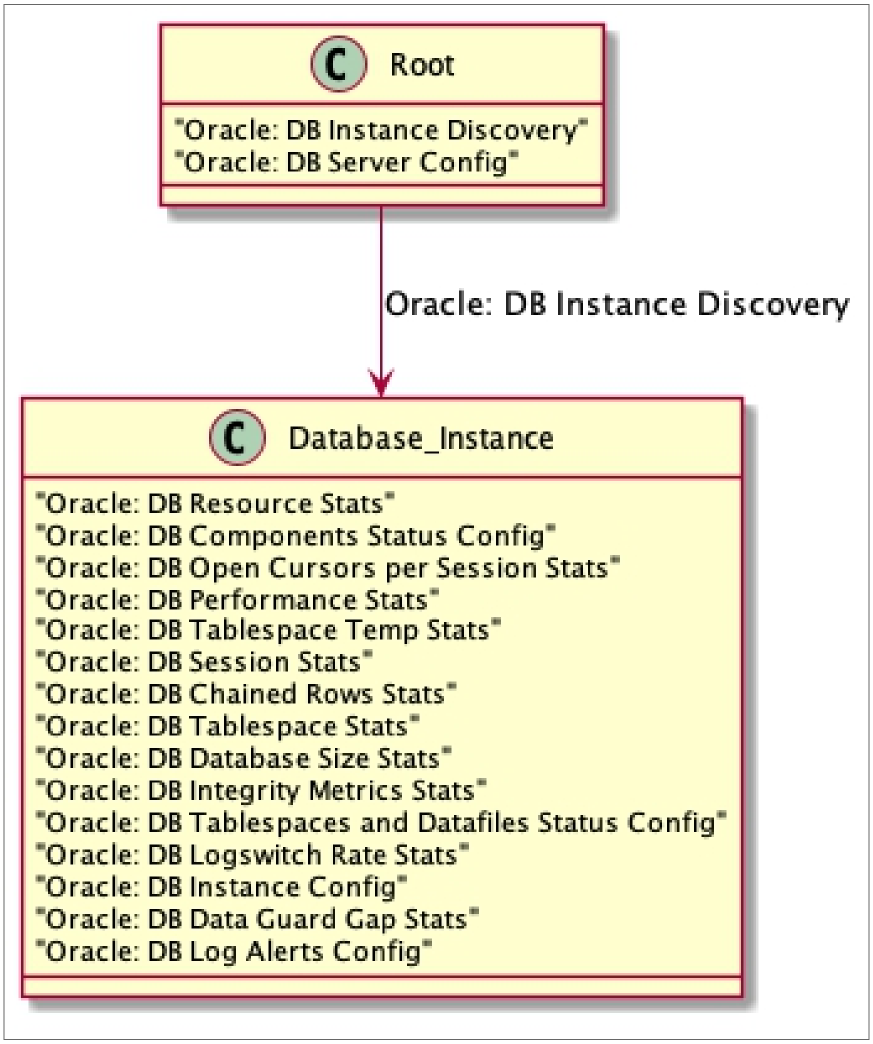
4. You can enter values in the other fields on this page, but are not required to and can simply accept the default values. For more information about the other fields on this page, see the ***Discovery & Credentials*** manual.
5. Click the **[Save]** button and then close the **Discovery Session Editor** window.
6. The discovery session you created will appear at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon (⚡) to run the discovery session.
7. The **Discovery Session** window will be displayed.

8. When the server that is hosting the Oracle Database is discovered, click its device icon () to view the **Device Properties** page for that device.
9. After the server hosting the Oracle Database is discovered, the "Oracle: DB Instance Discovery" Dynamic Application will automatically be aligned. This Dynamic Application will discover the Oracle Database instances which will appear in the **Device Manager** page.

> **NOTE:** If you are on a Windows system and are having issues with discovery, please see the ***Monitoring Windows Systems with PowerShell*** manual section.

Verifying Discovery and Dynamic Application Alignment

During discovery, SL1 will discover the root device then the Database instance. All applicable Dynamic Applications will be aligned to the component as follows:


C Root
"Oracle: DB Instance Discovery"
"Oracle: DB Server Config"
Oracle: DB Instance Discovery
C Database_Instance
"Oracle: DB Resource Stats"
"Oracle: DB Components Status Config"
"Oracle: DB Open Cursors per Session Stats"
"Oracle: DB Performance Stats"
"Oracle: DB Tablespace Temp Stats"
"Oracle: DB Session Stats"
"Oracle: DB Chained Rows Stats"
"Oracle: DB Tablespace Stats"
"Oracle: DB Database Size Stats"
"Oracle: DB Integrity Metrics Stats"
"Oracle: DB Tablespaces and Datafiles Status Config"
"Oracle: DB Logswitch Rate Stats"
"Oracle: DB Instance Config"
"Oracle: DB Data Guard Gap Stats"
"Oracle: DB Log Alerts Config"

To verify alignment of the Oracle Database Dynamic Applications:

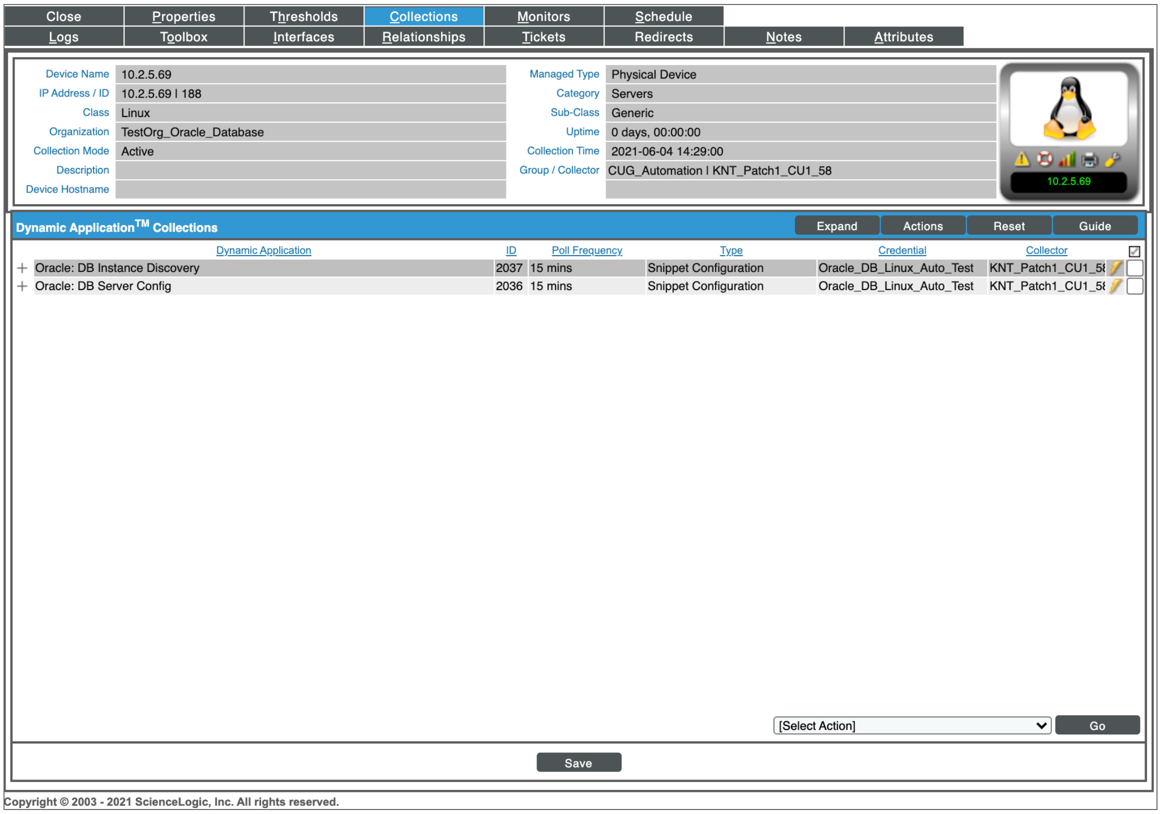
1. After discovery has completed, click the device icon for the Oracle device (🖥). From the **Device Properties** page for the Oracle device, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.

   > **NOTE:** It can take two to three polling cycles after the discovery session has completed for Dynamic Applications to appear in the **Dynamic Application Collections** page.

2. All applicable Dynamic Applications are automatically aligned to the root device and component devices during discovery:

You should see the following Dynamic Applications aligned to the root device:

- Oracle: DB Instance Discovery
- Oracle: DB Server Config



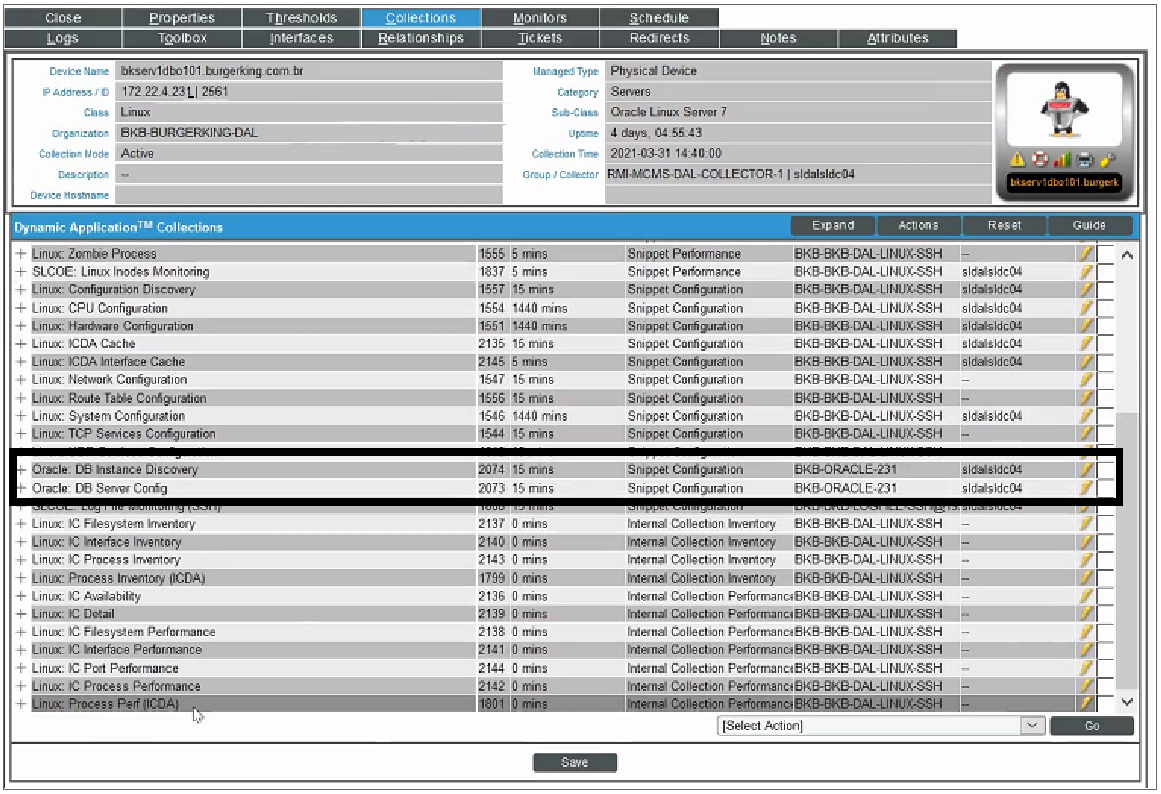
Device Name	10.2.5.69	Managed Type	Physical Device
IP Address / ID	10.2.5.69 | 188	Category	Servers
Class	Linux	Sub-Class	Generic
Organization	TestOrg_Oracle_Database	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2021-06-04 14:29:00
Description		Group / Collector	CUG_Automation | KNT_Patch1_CU1_58
Device Hostname			

Dynamic Application™ Collections

Dynamic Application	ID	Poll Frequency	Type	Credential	Collector	☑
+ Oracle: DB Instance Discovery	2037	15 mins	Snippet Configuration	Oracle_DB_Linux_Auto_Test	KNT_Patch1_CU1_5ε	□
+ Oracle: DB Server Config	2036	15 mins	Snippet Configuration	Oracle_DB_Linux_Auto_Test	KNT_Patch1_CU1_5ε	□

Copyright © 2003 - 2021 ScienceLogic, Inc. All rights reserved.

Using an Oracle PP on an existing Linux device will not interfere with the historical data on the device. Instead, the Oracle will align at the root with the other Linux Dynamic Applications.



Device Name	bkserv1dbo101.burgerking.com.br	Managed Type	Physical Device
IP Address / ID	172.22.4.231 | 2561	Category	Servers
Class	Linux	Sub-Class	Oracle Linux Server 7
Organization	BKB-BURGERKING-DAL	Uptime	4 days, 04:55:43
Collection Mode	Active	Collection Time	2021-03-31 14:40:00
Description	--	Group / Collector	RMI-MCMS-DAL-COLLECTOR-1 | sldalsldc04
Device Hostname			

Dynamic Application™ Collections

Linux: Zombie Process	1555	5 mins	Snippet Performance	BKB-BKB-DAL-LINUX-SSH	--
SLCOE: Linux Inodes Monitoring	1837	5 mins	Snippet Performance	BKB-BKB-DAL-LINUX-SSH	sldalsldc04
Linux: Configuration Discovery	1557	15 mins	Snippet Configuration	BKB-BKB-DAL-LINUX-SSH	sldalsldc04
Linux: CPU Configuration	1554	1440 mins	Snippet Configuration	BKB-BKB-DAL-LINUX-SSH	sldalsldc04
Linux: Hardware Configuration	1551	1440 mins	Snippet Configuration	BKB-BKB-DAL-LINUX-SSH	sldalsldc04
Linux: ICDA Cache	2135	15 mins	Snippet Configuration	BKB-BKB-DAL-LINUX-SSH	sldalsldc04
Linux: ICDA Interface Cache	2145	5 mins	Snippet Configuration	BKB-BKB-DAL-LINUX-SSH	sldalsldc04
Linux: Network Configuration	1547	15 mins	Snippet Configuration	BKB-BKB-DAL-LINUX-SSH	--
Linux: Route Table Configuration	1556	15 mins	Snippet Configuration	BKB-BKB-DAL-LINUX-SSH	--
Linux: System Configuration	1546	1440 mins	Snippet Configuration	BKB-BKB-DAL-LINUX-SSH	sldalsldc04
Linux: TCP Services Configuration	1544	15 mins	Snippet Configuration	BKB-BKB-DAL-LINUX-SSH	--
Oracle: DB Instance Discovery	2074	15 mins	Snippet Configuration	BKB-ORACLE-231	sldalsldc04
Oracle: DB Server Config	2073	15 mins	Snippet Configuration	BKB-ORACLE-231	sldalsldc04
Linux: IC Filesystem Inventory	2137	0 mins	Internal Collection Inventory	BKB-BKB-DAL-LINUX-SSH	--
Linux: IC Interface Inventory	2140	0 mins	Internal Collection Inventory	BKB-BKB-DAL-LINUX-SSH	--
Linux: IC Process Inventory	2143	0 mins	Internal Collection Inventory	BKB-BKB-DAL-LINUX-SSH	--
Linux: Process Inventory (ICDA)	1799	0 mins	Internal Collection Inventory	BKB-BKB-DAL-LINUX-SSH	--
Linux: IC Availability	2136	0 mins	Internal Collection Performance	BKB-BKB-DAL-LINUX-SSH	--
Linux: IC Detail	2139	0 mins	Internal Collection Performance	BKB-BKB-DAL-LINUX-SSH	--
Linux: IC Filesystem Performance	2138	0 mins	Internal Collection Performance	BKB-BKB-DAL-LINUX-SSH	--
Linux: IC Interface Performance	2141	0 mins	Internal Collection Performance	BKB-BKB-DAL-LINUX-SSH	--
Linux: IC Port Performance	2144	0 mins	Internal Collection Performance	BKB-BKB-DAL-LINUX-SSH	--
Linux: IC Process Performance	2142	0 mins	Internal Collection Performance	BKB-BKB-DAL-LINUX-SSH	--
Linux: Process Perf (ICDA)	1801	0 mins	Internal Collection Performance	BKB-BKB-DAL-LINUX-SSH	--

You should see the following Dynamic Applications aligned to **non-RAC Oracle Database instances on Linux Systems**:

- Oracle: DB Archived File System Stats
- Oracle: DB Chained Rows Stats
- Oracle: DB Components Status Config
- Oracle: DB Data Guard Gap Stats
- Oracle: DB Database Size Stats
- Oracle: DB Instance Config
- Oracle: DB Integrity Metrics Stats

NOTE: The Oracle: DB Integrity Metrics Stats Dynamic Application uses the prior() function which requires SL1 version 8.14.2 or newer.

- Oracle: DB Log Alerts Config

NOTE: The Oracle: DB Log Alerts Config Dynamic Application requires that the database administrator grant SELECT privileges in the v$diag_alert_text to the monitoring user.

- Oracle: DB Logswitch Rate Stats
- Oracle: DB Non-Archived File System Stats
- Oracle: DB Open Cursors per Session Stats
- Oracle: DB Performance Stats
- Oracle: DB Resource Stats
- Oracle: DB Session Stats
- Oracle: DB Tablespace Stats
- Oracle: DB Tablespace Temp Stats
- Oracle: DB Tablespaces and Datafiles Status Config

You should see the following Dynamic Applications aligned to **non-RAC Oracle Database instances on Windows and Solaris Systems**:

- Oracle: DB Chained Rows Stats
- Oracle: DB Components Status Config
- Oracle: DB Data Guard Gap Stats
- Oracle: DB Database Size Stats
- Oracle: DB Instance Config
- Oracle: DB Integrity Metrics Stats

NOTE: The Oracle: DB Integrity Metrics Stats Dynamic Application uses the prior() function which requires SL1 version 8.14.2 or newer.

- Oracle: DB Log Alerts Config

NOTE: The Oracle: DB Log Alerts Config Dynamic Application requires that the database administrator grant SELECT privileges in the v$diag_alert_text to the monitoring user.

- Oracle: DB Logswitch Rate Stats
- Oracle: DB Open Cursors per Session Stats
- Oracle: DB Performance Stats
- Oracle: DB Resource Stats
- Oracle: DB Session Stats
- Oracle: DB Tablespace Stats
- Oracle: DB Tablespace Temp Stats
- Oracle: DB Tablespaces and Datafiles Status Config

You should see the following Dynamic Applications aligned to **RAC Oracle Database instances on Linux Systems**:

- Oracle: DB Archived File System Stats
- Oracle: DB Chained Rows Stats
- Oracle: DB Components Status Config
- Oracle: DB Data Guard Gap Stats
- Oracle: DB Database Size Stats
- Oracle: DB Instance Config
- Oracle: DB Integrity Metrics Stats

NOTE: The Oracle: DB Integrity Metrics Stats Dynamic Application uses the prior() function which requires SL1 version 8.14.2 or newer.

- Oracle: DB Log Alerts Config

NOTE: The Oracle: DB Log Alerts Config Dynamic Application requires that the database administrator grant SELECT privileges in the v$diag_alert_text to the monitoring user.

- Oracle: DB Logswitch Rate Stats
- Oracle: DB Non-Archived File System Stats
- Oracle: DB Open Cursors per Session Stats
- Oracle: DB Performance Stats
- Oracle: DB RAC Disk Group Space Stats
- Oracle: DB RAC Flash Recovery Stats
- Oracle: DB RAC Global Cache Stats

NOTE: The Oracle RAC Dynamic Applications will only be aligned on RAC systems.

- Oracle: DB Resource Stats
- Oracle: DB Session Stats
- Oracle: DB Tablespace Stats
- Oracle: DB Tablespace Temp Stats
- Oracle: DB Tablespaces and Datafiles Status Config

You should see the following Dynamic Applications aligned to **RAC Oracle Database instances on Windows and Solaris Systems**:

- Oracle: DB Chained Rows Stats
- Oracle: DB Components Status Config
- Oracle: DB Data Guard Gap Stats
- Oracle: DB Database Size Stats
- Oracle: DB Instance Config
- Oracle: DB Integrity Metrics Stats

NOTE: The Oracle: DB Integrity Metrics Stats Dynamic Application uses the prior() function which requires SL1 version 8.14.2 or newer.

- Oracle: DB Log Alerts Config

NOTE: The Oracle: DB Log Alerts Config Dynamic Application requires that the database administrator grant SELECT privileges in the v$diag_alert_text to the monitoring user.

- Oracle: DB Logswitch Rate Stats
- Oracle: DB Open Cursors per Session Stats
- Oracle: DB Performance Stats
- Oracle: DB RAC Disk Group Space Stats
- Oracle: DB RAC Flash Recovery Stats
- Oracle: DB RAC Global Cache Stats

NOTE: The Oracle RAC Dynamic Applications will only be aligned on RAC systems.

- Oracle: DB Resource Stats
- Oracle: DB Session Stats
- Oracle: DB Tablespace Stats
- Oracle: DB Tablespace Temp Stats
- Oracle: DB Tablespaces and Datafiles Status Config

Troubleshooting Discovery Issues

Oracle: Database v102 includes a check_oracle script for Discovery troubleshooting purposes. The script details information about any Discovery/Alignment issues that appear once a Support Escalation is opened.
To run the included check_oracle script for the PowerPack:

1. Ensure the script has executable permissions:
   ```
   >sudo chmod 744
   /opt/em7/envs/2BF4A4FD8DC2BA5EDDD565F9CF373156/lib/python2.7/site-
   packages/silo/oracle_db/check_oracle.py
   ```
2. Execute the script as user s-em7-core:
   ```
   >sudo -u s-em7-core
   /opt/em7/envs/2BF4A4FD8DC2BA5EDDD565F9CF373156/lib/python2.7/site-
   packages/silo/oracle_db/check_oracle.py
   ```
3. When the script has finished, provide the results file:
   ```
   /tmp/Oracle_results_10.1.2.3_1622740963
   ```

Chapter

62

Palo Alto

Overview

The following sections describe how to configure and discover Palo Alto firewalls for monitoring by SL1 using the *Palo Alto* PowerPack:

> NOTE: For more information about the *Palo Alto* PowerPack, see the ***Monitoring Palo Alto*** manual.

Prerequisites for Monitoring Palo Alto Firewalls

Before you can monitor Palo Alto firewalls in SL1 using the *Palo Alto* PowerPack, you must have the following information:

- SNMP community strings for the devices you want to monitor
- IP addresses for each device you want to monitor
- Username and password for a user with access to the devices you want to monitor

> **NOTE:** The monitored firewalls must be running PAN-OS version 8.0 or later to ensure the proper collection of tunnel performance data.

Creating Credentials for Palo Alto

To configure SL1 to monitor Palo Alto firewalls, you must create the SNMP and Basic/Snippet credentials that enable SL1 to connect with those firewalls.

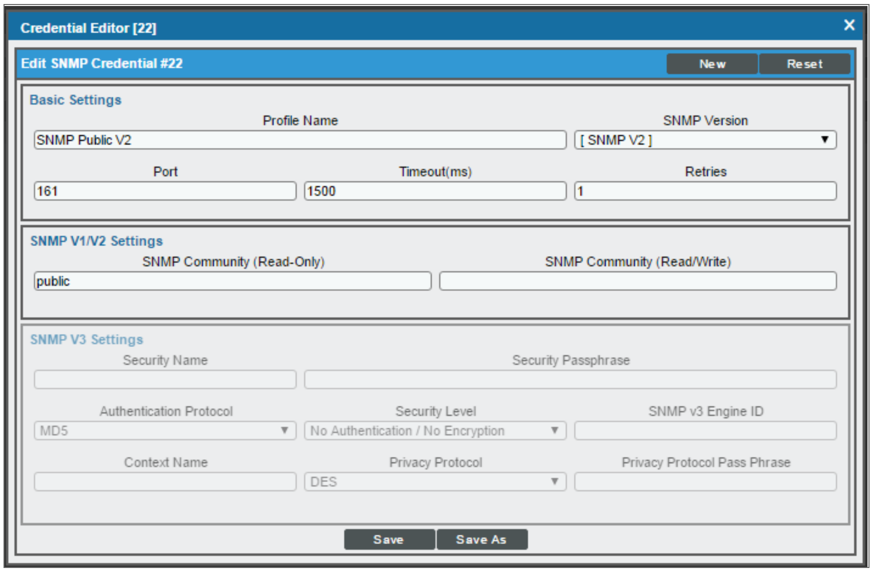
> **NOTE:** The *Palo Alto* PowerPack currently supports only basic authentication for discovery; it does not support the use of an API key.

Creating an SNMP Credential

Some of the Dynamic Applications in the *Palo Alto* PowerPack use SNMP to collect information about Palo Alto firewalls. To use these Dynamic Applications, you must first define an SNMP credential that enables SL1 to communicate with the firewalls.

To configure an SNMP credential:

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



Basic Settings
Profile Name: SNMP Public V2
SNMP Version: [SNMP V2]
Port: 161
Timeout(ms): 1500
Retries: 1

SNMP V1/V2 Settings
SNMP Community (Read-Only): public
SNMP Community (Read/Write):

SNMP V3 Settings
Security Name:
Security Passphrase:
Authentication Protocol: MD5
Security Level: No Authentication / No Encryption
SNMP v3 Engine ID:
Context Name:
Privacy Protocol: DES
Privacy Protocol Pass Phrase:

- ***Profile Name***. Type a name for the credential.

- ***SNMP Version***. Select *SNMP V2*.
- ***SNMP Community (Read Only)***. Type the community string for the Palo Alto firewalls you want to monitor.

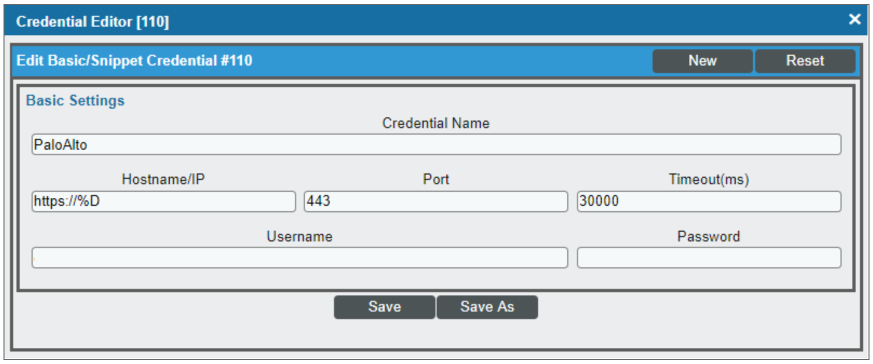
4. Supply values in the other fields on this page as needed. In most cases, you can accept the default values for the other fields.
5. Click the **[Save]** button.

Creating a Basic/Snippet Credential

To configure SL1 to monitor Palo Alto devices, you must also create a Basic/Snippet credential. This credential enables some of the Dynamic Applications in the *Palo Alto* PowerPack to connect with those devices.

To create a Basic/Snippet credential for Palo Alto devices:

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



Credential Name: PaloAlto

Hostname/IP: https://%D

Port: 443

Timeout(ms): 30000

Username:

Password:

- ***Credential Name***. Type a name for the credential.
- ***Hostname/IP***. Type "https://%D".
- ***Port***. Type "443".
- ***Timeout***. Type "30000".
- ***Username***. Type the username for a user account with access to the Palo Alto firewalls.
- ***Password***. Type the password for the Palo Alto user account.

4. Click the **[Save As]** button.
5. When the confirmation message appears, click **[OK]**.

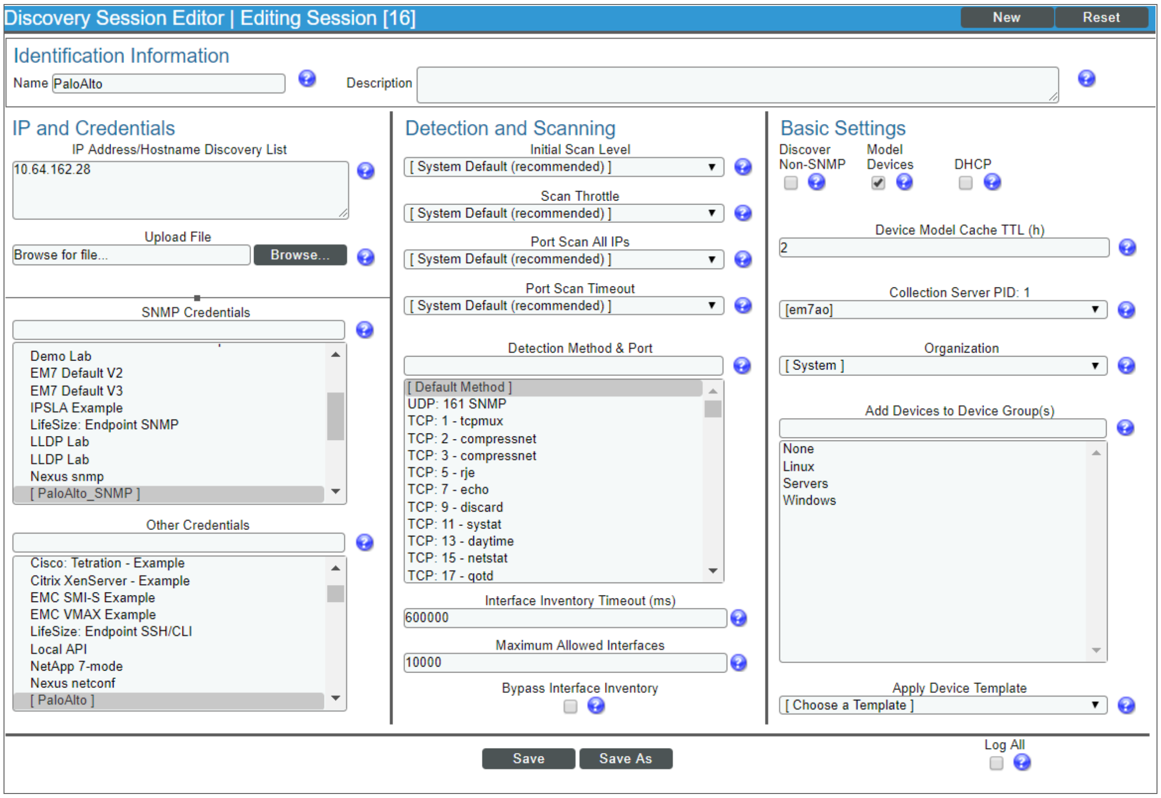
Discovering Palo Alto Devices

After you have created the necessary credentials, you can discover the Palo Alto devices that you want to monitor. Several minutes after the discovery session has completed, the Dynamic Applications in the *Palo Alto* PowerPack will automatically align to the devices, enabling you to view configuration and performance data about the devices.

> **NOTE:** This PowerPack discovers virtual Palo Alto devices that respond to SNMP. However, if they are provisioned, SL1 will not model them. SL1 will model the devices if they exist when the next discovery session is run.

To discover the Palo Alto devices that you want to monitor:

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, complete the following fields:



Discovery Session Editor | Editing Session [16]

Identification Information

Name: PaloAlto

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.64.162.28

Upload File: Browse for file...

SNMP Credentials: [PaloAlto_SNMP]

Other Credentials: [PaloAlto]

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]

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: 1: [em7ao]

Organization: [System]

Add Devices to Device Group(s):

Apply Device Template: [Choose a Template]

Log All: □

- ***IP Address/Hostname Discovery List***. Type the IP address or addresses for the Palo Alto devices that you want to discover.

- ***SNMP Credentials***. Select the SNMP credential you created for the Palo Alto devices.
- ***Other Credentials***. Select the Basic/Snippet credentials you created for the Palo Alto devices.
- ***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 device(s) are discovered, click the device icon (🖥) to view the **Device Properties** page for each device.

Chapter

63

Pure Storage

Overview

The following sections describe how to configure and discover Pure Storage FlashArrays and their component devices for monitoring by SL1 using the *Pure Storage* PowerPack:

NOTE: For more information about the *Pure Storage* PowerPack, see the ***Monitoring Pure Storage*** manual.

Generating a Pure Storage API Token

The *Pure Storage* PowerPack uses the Pure Storage REST API for collecting configuration and performance data. The Pure API uses port 443; therefore, you must have access to that port. You must also use an API Token, which you can create on the Pure FlashArray and then copy into the ***Basic/Snippet credential*** you create that enables SL1 to discover and monitor the FlashArray.

There are two ways to create the API Token:

- Generate the API token through the Purity user interface (System > Users > Create API Token)
- Generate the API token through the Purity command line interface (`pureadmin create --api-token`)

You can also view existing API tokens in the Purity user interface by navigating to System > Users > API Tokens, clicking the gear icon next to the username, and then selecting *Show API Token*.

After the API Token has been generated, copy and save it for use in the credential.

Testing TCP Port Connectivity

The Pure Storage REST API service runs on TCP port 443 from the primary IP address assigned to the Pure FlashArray. This IP address should be the same one used to access the Purity user interface. To enable SL1 to communicate with the Pure API, your ScienceLogic Data Collector or All-In-One Appliance must have access to TCP port 443.

To test TCP port connectivity, log in to the command line interface of your Data Collector or All-In-One Appliance as the root user and type the following command:

```
nmap -p 443 10.1.1.10
```

If TCP port 443 is open, the following message displays:

```
Starting Nmap 5.51 ( http://nmap.org ) at 2015-10-01 18:42 UTC
Nmap scan report for purestorage-001.mydomain.net (204.110.219.37)
Host is up (0.027s latency).
PORT    STATE SERVICE
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

If the port does not appear, or it appears with the state of "filtered", check your firewall settings. If there is a firewall between the ScienceLogic Data Collector or All-In-One Appliance and the Pure Storage REST API, ensure that it can communicate over TCP port 443.

Configuring a Pure Storage Credential

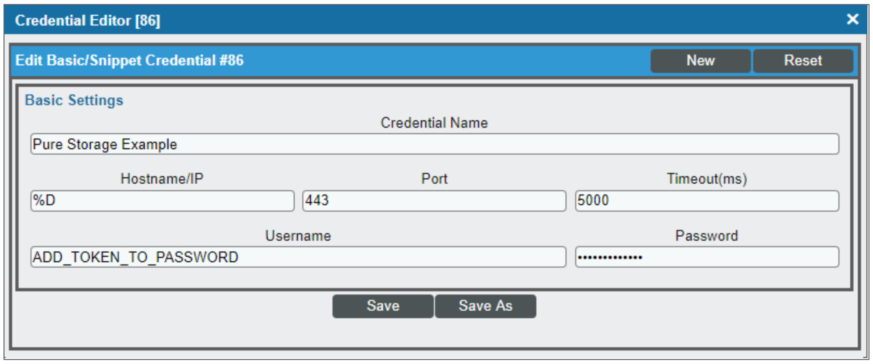
To configure SL1 to monitor Pure Storage, you must first create a Basic/Snippet credential that allows the Dynamic Applications in the *Pure Storage* PowerPack to connect with the Pure Storage FlashArray. An example Basic/Snippet credential that you can edit for your own use is included in the *Pure Storage* PowerPack.

To create a Basic/Snippet credential to access Docker hosts and swarms:

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

2. Locate the example **Pure Storage Example** credential, and then click its wrench icon (🔧). The **Edit Basic/Snippet Credential** modal page appears.

3. Complete the following fields:



Edit Basic/Snippet Credential #86

Basic Settings

Credential Name: Pure Storage Example

Hostname/IP: %D

Port: 443

Timeout(ms): 5000

Username: ADD_TOKEN_TO_PASSWORD

Password: ••••••••••••••

- ***Credential Name***. Type a new name for the Pure Storage credential.
- ***Hostname/IP***. Type "%D".
- ***Port***. Type "443".
- ***Timeout(ms)***. Type a value greater than or equal to "5000".
- ***Username***. Type your Pure Storage username.
- ***Password***. Type or paste the Pure Storage API token.

4. Click the **[Save As]** button.
5. When the confirmation message appears, click **[OK]**.

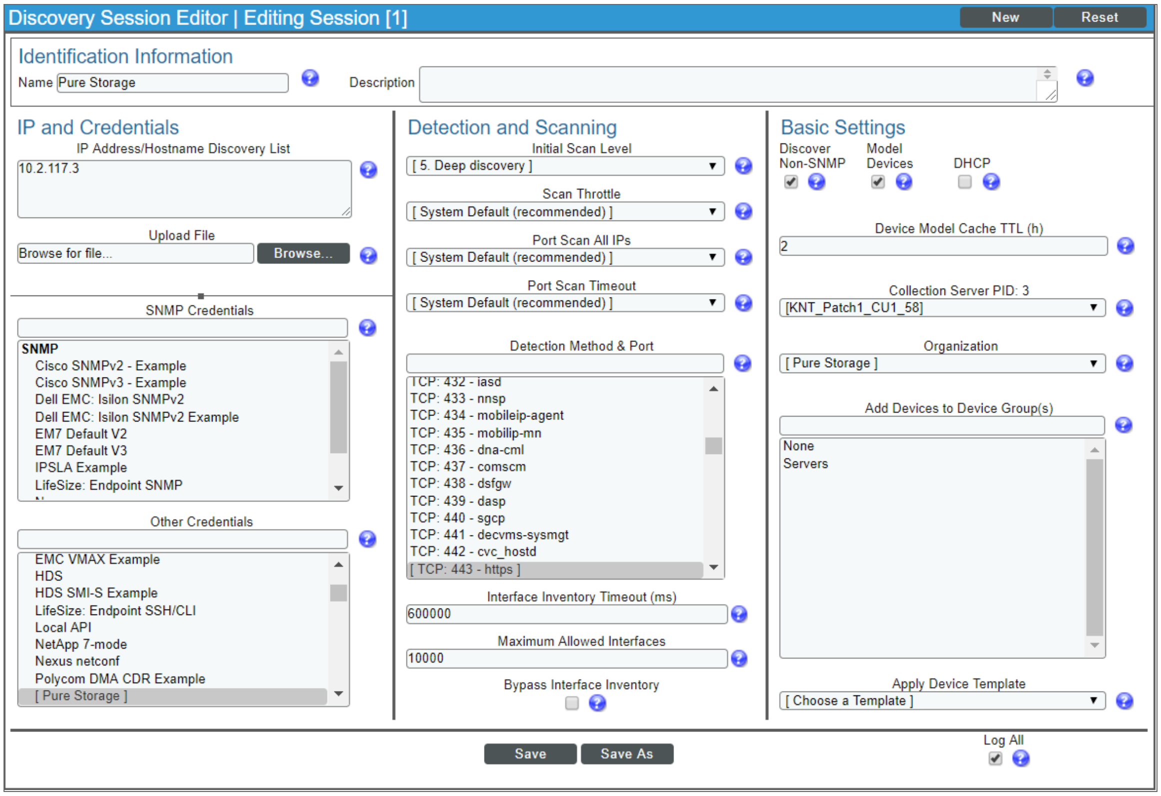
Discovering Pure Storage Components

To discover and model your Pure Storage FlashArray and component devices for monitoring, you must run a discovery session. Several minutes after the discovery session has completed, the Dynamic Applications in the *Pure Storage* PowerPack will automatically align to the FlashArray root device. These Dynamic Applications will discover, model, and monitor the remaining Pure Storage components.

To discover Pure Storage components:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery), and then click the **[Create]** button. The **Discovery Session Editor** page appears.

2. In the **Discovery Session Editor** page, complete the following fields:



Discovery Session Editor | Editing Session [1]

Identification Information

Name: Pure Storage

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.2.117.3

Upload File: Browse for file...

SNMP Credentials:

SNMP
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Dell EMC: Isilon SNMPv2
Dell EMC: Isilon SNMPv2 Example
EM7 Default V2
EM7 Default V3
IPSLA Example
LifeSize: Endpoint SNMP

Other Credentials:

EMC VMAX Example
HDS
HDS SMI-S Example
LifeSize: Endpoint SSH/CLI
Local API
NetApp 7-mode
Nexus netconf
Polycom DMA CDR Example
[Pure Storage]

Detection and Scanning

Initial Scan Level: [5. Deep discovery]

Scan Throttle: [System Default (recommended)]

Port Scan All IPs: [System Default (recommended)]

Port Scan Timeout: [System Default (recommended)]

Detection Method & Port:

TCP: 432 - iasd
TCP: 433 - nnsp
TCP: 434 - mobileip-agent
TCP: 435 - mobilip-mn
TCP: 436 - dna-cml
TCP: 437 - comscm
TCP: 438 - dsfgw
TCP: 439 - dasp
TCP: 440 - sgcp
TCP: 441 - decvms-sysmgt
TCP: 442 - cvc_hostd
[TCP: 443 - https]

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: 3 [KNT_Patch1_CU1_58]

Organization: [Pure Storage]

Add Devices to Device Group(s):

None
Servers

Apply Device Template: [Choose a Template]

Log All: ☑

- ***Name***. Type a name for your discovery session.
- ***IP Address/Hostname Discovery List***. Type the IP address for the Pure Storage FlashArray that you want to discover.
- ***Other Credentials***. Select the *Basic/Snippet credential* you created for Docker.
- ***Initial Scan Level***. Select *5. Deep discovery*.
- ***Detection Method & Port***. Select *TCP 443 - https*.
- ***Discover Non-SNMP***. Select this checkbox.
- ***Model Devices***. Select this checkbox.

3. 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.

4. Click the **[Save]** button to save the discovery session, and then close the **Discovery Session Editor** window.

5. The discovery session you created displays at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon ( ) to run the discovery session.

6. The **Discovery Session** window appears. When a root device is discovered, click its device icon ( ) to view the **Device Properties** page for that device.

Manually Aligning Dynamic Applications

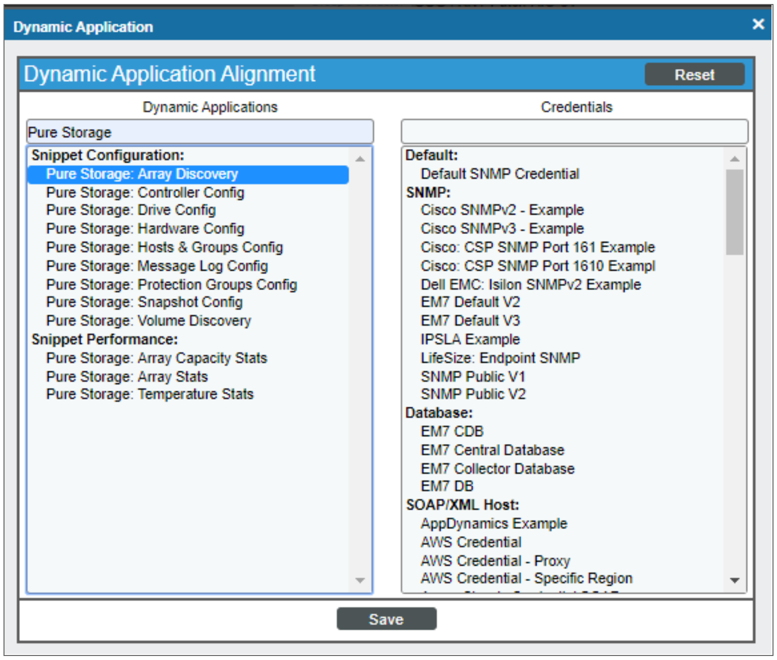
To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. From the **Device Properties** page (Registry > Devices > wrench icon (🔧)) for the Pure Storage FlashArray, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. The following Dynamic Applications should appear in the list of aligned Dynamic Applications:
    - Pure Storage: Array Capacity Stats
    - Pure Storage: Array Discovery
    - Pure Storage: Array Stats
    - Pure Storage: Controller Config
    - Pure Storage: Drive Config
    - Pure Storage: Hardware Config
    - Pure Storage: Hosts & Groups Config
    - Pure Storage: Message Log Config
    - Pure Storage: Protection Groups Config
    - Pure Storage: Temperature Stats
    - Pure Storage: Volume Discovery

NOTE: It can take several minutes after discovery for Dynamic Applications to display on the **Dynamic Application Collections** page. If the listed Dynamic Applications do not display on this page, try clicking the **[Reset]** button.

If the Dynamic Applications have not been automatically aligned, you can align them manually. To do so, perform the following steps:

1. Go to the **Device Properties** page (Registry > Devices > wrench icon(🔧)) for the Pure Storage FlashArray and click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. On the **Dynamic Application Collections** page, click the **[Action]** button and then select *Add Dynamic Application* from the menu. The **Dynamic Application Alignment** page appears.



Pure Storage

Snippet Configuration:
Pure Storage: Array Discovery
Pure Storage: Controller Config
Pure Storage: Drive Config
Pure Storage: Hardware Config
Pure Storage: Hosts & Groups Config
Pure Storage: Message Log Config
Pure Storage: Protection Groups Config
Pure Storage: Snapshot Config
Pure Storage: Volume Discovery
Snippet Performance:
Pure Storage: Array Capacity Stats
Pure Storage: Array Stats
Pure Storage: Temperature Stats

Default:
Default SNMP Credential
SNMP:
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Cisco: CSP SNMP Port 161 Example
Cisco: CSP SNMP Port 1610 Exampl
Dell EMC: Isilon SNMPv2 Example
EM7 Default V2
EM7 Default V3
IPSLA Example
LifeSize: Endpoint SNMP
SNMP Public V1
SNMP Public V2
Database:
EM7 CDB
EM7 Central Database
EM7 Collector Database
EM7 DB
SOAP/XML Host:
AppDynamics Example
AWS Credential
AWS Credential - Proxy
AWS Credential - Specific Region

3. In the ***Dynamic Applications*** field, select a Dynamic Application to align.
4. In the ***Credentials*** field, select the *Basic/Snippet credential* you created for Pure Storage.
5. Click the **[Save]** button.
6. Repeat steps 2-5 as needed to align any additional Dynamic Applications.

Chapter 64

Silver Peak

Overview

The following sections describe how to configure and discover New Relic services for monitoring by SL1 using the *Silver Peak* PowerPack:

NOTE: For more information about the *Silver Peak* PowerPack, see the ***Monitoring Silver Peak*** manual.

Prerequisites for Monitoring Silver Peak

To configure the SL1 system to monitor Silver Peak Unity Orchestrator and edge devices using the *Silver Peak* PowerPack, you must have the following information about the Unity Orchestrator that you want to monitor:

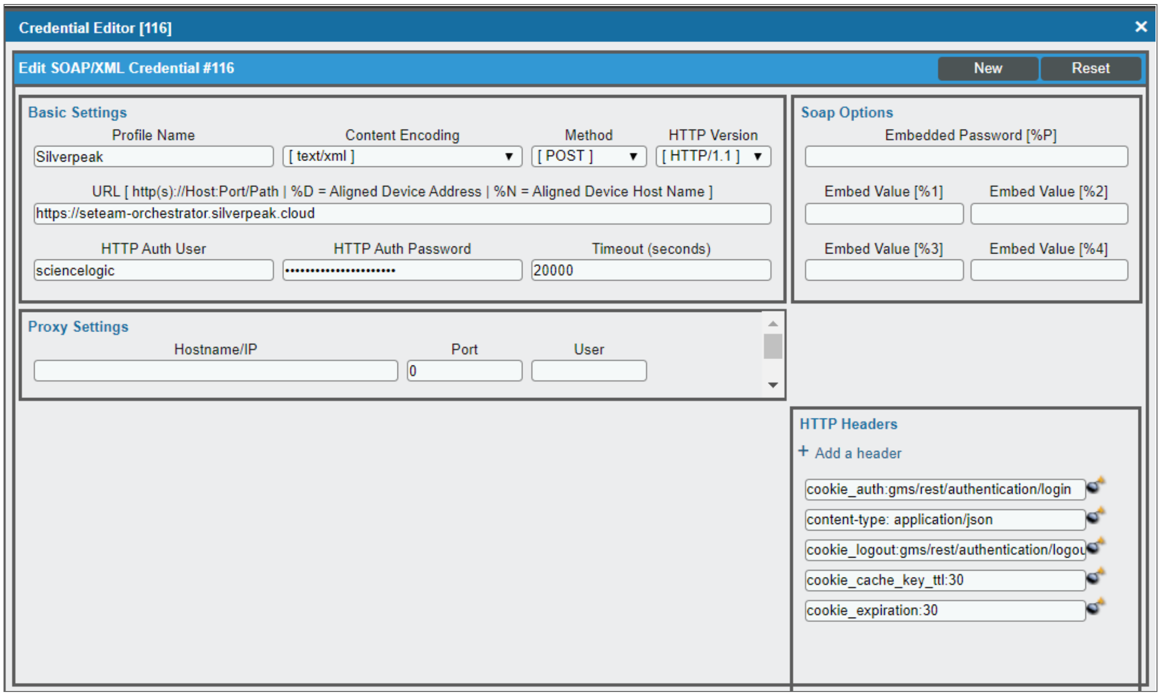
- The IP address or URL of your Orchestrator
- The username and password for the administrator account on your Orchestrator

Creating a SOAP/XML Credential for Silver Peak

To configure SL1 to monitor Silver Peak, you must create a SOAP/XML credential. This credential allows the Dynamic Applications in the *Silver Peak* PowerPack to communicate with your Silver Peak Unity Orchestrator.

To configure a SOAP/XML credential to access the Orchestrator:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **Silver Peak Cookie Example** credential, and then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal appears.
3. Enter values in the following fields:



Credential Editor [116]

Edit SOAP/XML Credential #116

Basic Settings

Profile Name: Silverpeak

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://seteam-orchestrator.silverpeak.cloud

HTTP Auth User: sciencelogic

HTTP Auth Password: ••••••••••••••••••••••

Timeout (seconds): 20000

Soap Options

Embedded Password [%P]:

Embed Value [%1]:

Embed Value [%2]:

Embed Value [%3]:

Embed Value [%4]:

Proxy Settings

Hostname/IP:

Port: 0

User:

HTTP Headers

+ Add a header

cookie_auth:gms/rest/authentication/login

content-type: application/json

cookie_logout:gms/rest/authentication/logou

cookie_cache_key_ttl:30

cookie_expiration:30

Basic Settings

- ***Profile Name***. Enter a new name for the credential.
- ***URL***. Enter the URL or IP address for the Orchestrator
- ***HTTP Auth User***. Enter the username for the administrator account on your Orchestrator.
- ***HTTP Auth Password***. Enter the password for the administrator account on your Orchestrator.

4. Add the following **HTTP Headers**:
   - cookie_auth:gms/rest/authentication/login
   - content-type: application/json

- cookie_logout:gms/rest/authentication/logout

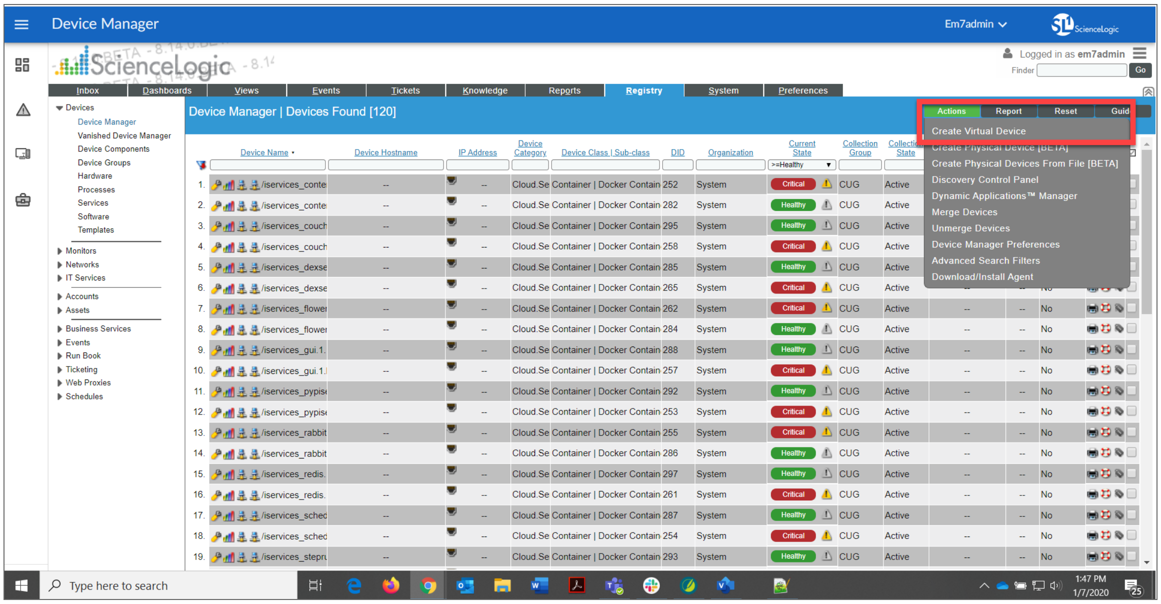
5. For all other fields, use the default values.
6. Click the **[Save As]** button.

Creating a Virtual Device for the Orchestrator

To configure SL1 to monitor Silver Peak, you must create a virtual device to represent your Orchestrator. The PowerPack includes a Device Class ("Silver Peak | Unity Orchestrator") for the Orchestrator.

To create a virtual device, you must complete the following tasks:

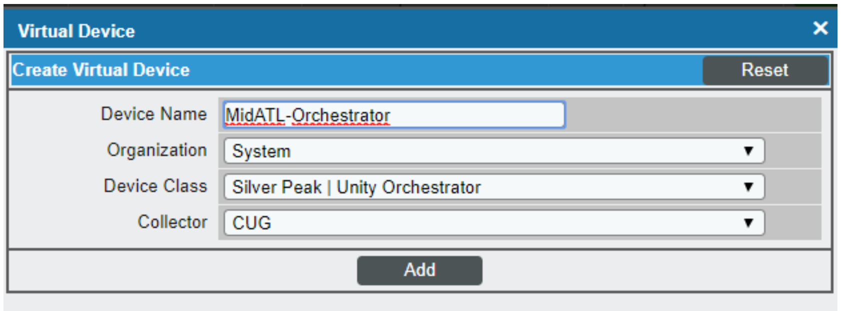
1. Go to the **Device Manager** page (Registry > Devices > Device Manager).



Device Manager | Devices Found [120]

	Device Name	Device Hostname	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State	Collection Group	Collection State			
								>=Healthy					
1.	/iservices_conte	--	--	Cloud.Se	Container | Docker Contain	252	System	Critical	CUG	Active			
2.	/iservices_conte	--	--	Cloud.Se	Container | Docker Contain	282	System	Healthy	CUG	Active			
3.	/iservices_couch	--	--	Cloud.Se	Container | Docker Contain	295	System	Healthy	CUG	Active			
4.	/iservices_couch	--	--	Cloud.Se	Container | Docker Contain	258	System	Critical	CUG	Active			
5.	/iservices_dexse	--	--	Cloud.Se	Container | Docker Contain	285	System	Healthy	CUG	Active			
6.	/iservices_dexse	--	--	Cloud.Se	Container | Docker Contain	265	System	Critical	CUG	Active			
7.	/iservices_flowe	--	--	Cloud.Se	Container | Docker Contain	262	System	Critical	CUG	Active	--	--	No
8.	/iservices_flowe	--	--	Cloud.Se	Container | Docker Contain	284	System	Healthy	CUG	Active	--	--	No
9.	/iservices_gui.1.	--	--	Cloud.Se	Container | Docker Contain	288	System	Healthy	CUG	Active	--	--	No
10.	/iservices_gui.1.	--	--	Cloud.Se	Container | Docker Contain	257	System	Critical	CUG	Active	--	--	No
11.	/iservices_pypis	--	--	Cloud.Se	Container | Docker Contain	292	System	Healthy	CUG	Active	--	--	No
12.	/iservices_pypis	--	--	Cloud.Se	Container | Docker Contain	253	System	Critical	CUG	Active	--	--	No
13.	/iservices_rabbit	--	--	Cloud.Se	Container | Docker Contain	255	System	Critical	CUG	Active	--	--	No
14.	/iservices_rabbit	--	--	Cloud.Se	Container | Docker Contain	286	System	Healthy	CUG	Active	--	--	No
15.	/iservices_redis.	--	--	Cloud.Se	Container | Docker Contain	297	System	Healthy	CUG	Active	--	--	No
16.	/iservices_redis.	--	--	Cloud.Se	Container | Docker Contain	261	System	Critical	CUG	Active	--	--	No
17.	/iservices_sched	--	--	Cloud.Se	Container | Docker Contain	287	System	Healthy	CUG	Active	--	--	No
18.	/iservices_sched	--	--	Cloud.Se	Container | Docker Contain	254	System	Critical	CUG	Active	--	--	No
19.	/iservices_stepr	--	--	Cloud.Se	Container | Docker Contain	293	System	Healthy	CUG	Active	--	--	No

2. From the **[Actions]** menu, select *Create Virtual Device*.
3. The **Create Virtual Device** modal appears.



Device Name	MidATL-Orchestrator
Organization	System
Device Class	Silver Peak | Unity Orchestrator
Collector	CUG

4. Supply a value in each of the following fields:

   - ***Device Name***. Name of the virtual device. Can be any combination of alphanumeric characters, up to 32 characters in length.
   - ***Organization***. Organization to associate with the virtual device. Select from the drop-down list of all organizations in SL1.
   - ***Device Class***. The device class to associate with the virtual device. Select *Silver Peak | Unity Orchestrator* from the drop-down list of device classes.
   - ***Collector***. Specifies which instance of SL1 will perform auto-discovery and gather data from the device. Can also specify a "virtual" poller. Select from the drop-down list of all collectors in SL1.

5. Select the **[Add]** button to save the new virtual device.

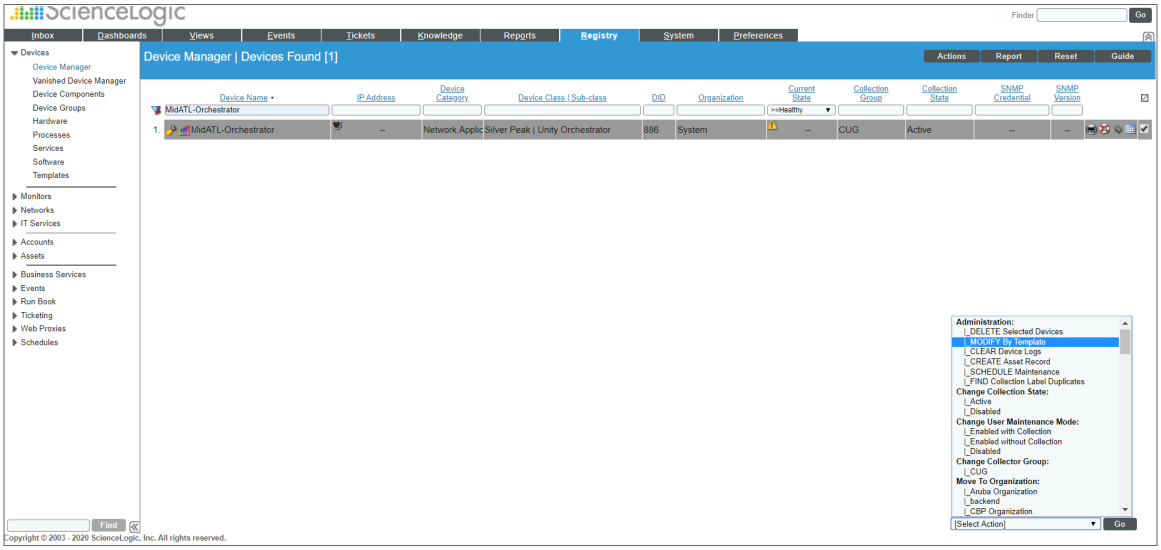
> NOTE: For more information about virtual devices, see ***Virtual Devices*** in the Device Management manual.

Aligning the Virtual Device with the Device Template

When SL1 discovers a device, SL1 applies some default configuration settings to that device. You can edit these settings or use a device template to edit the settings for one or more devices. In this step, you will use the "Silver Peak: Orchestrator Template" to apply a configuration to your Silver Peak Unity Orchestrator.

To use a device template to change the configuration of one or more devices:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. In the **Device Manager** page, select the checkbox for your Orchestrator virtual device.

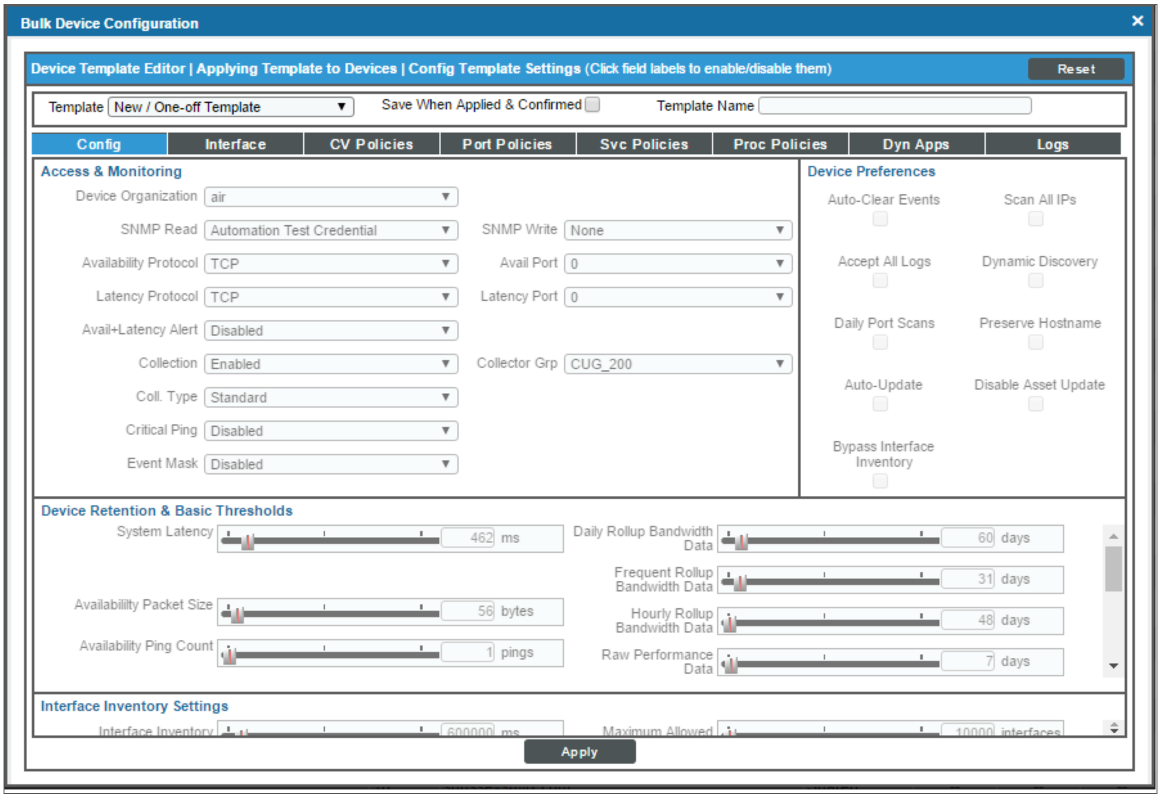


Device Manager | Devices Found [1]

	Device Name	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State	Collection Group	Collection State	SNMP Credential	SNMP Version	☑
	MidATL-Orchestrator						>=Healthy					
1.	MidATL-Orchestrator	--	Network.Applic	Silver Peak | Unity Orchestrator	886	System	--	CUG	Active	--	--	☑

3. In the ***Select Actions*** field, in the lower right, select the option *Modify by Template*. Click the **[Go]** button.

4. The **Bulk Device Configuration** page appears.



Bulk Device Configuration

Device Template Editor | Applying Template to Devices | Config Template Settings (Click field labels to enable/disable them)

Template: New / One-off Template
Save When Applied & Confirmed □
Template Name:

Access & Monitoring

Device Organization: air
SNMP Read: Automation Test Credential
SNMP Write: None
Availability Protocol: TCP
Avail Port: 0
Latency Protocol: TCP
Latency Port: 0
Avail+Latency Alert: Disabled
Collection: Enabled
Collector Grp: CUG_200
Coll. Type: Standard
Critical Ping: Disabled
Event Mask: Disabled

Device Preferences

Auto-Clear Events □
Scan All IPs □
Accept All Logs □
Dynamic Discovery □
Daily Port Scans □
Preserve Hostname □
Auto-Update □
Disable Asset Update □
Bypass Interface Inventory □

Device Retention & Basic Thresholds

System Latency: 462 ms
Daily Rollup Bandwidth Data: 60 days
Frequent Rollup Bandwidth Data: 31 days
Availability Packet Size: 56 bytes
Hourly Rollup Bandwidth Data: 48 days
Availability Ping Count: 1 pings
Raw Performance Data: 7 days

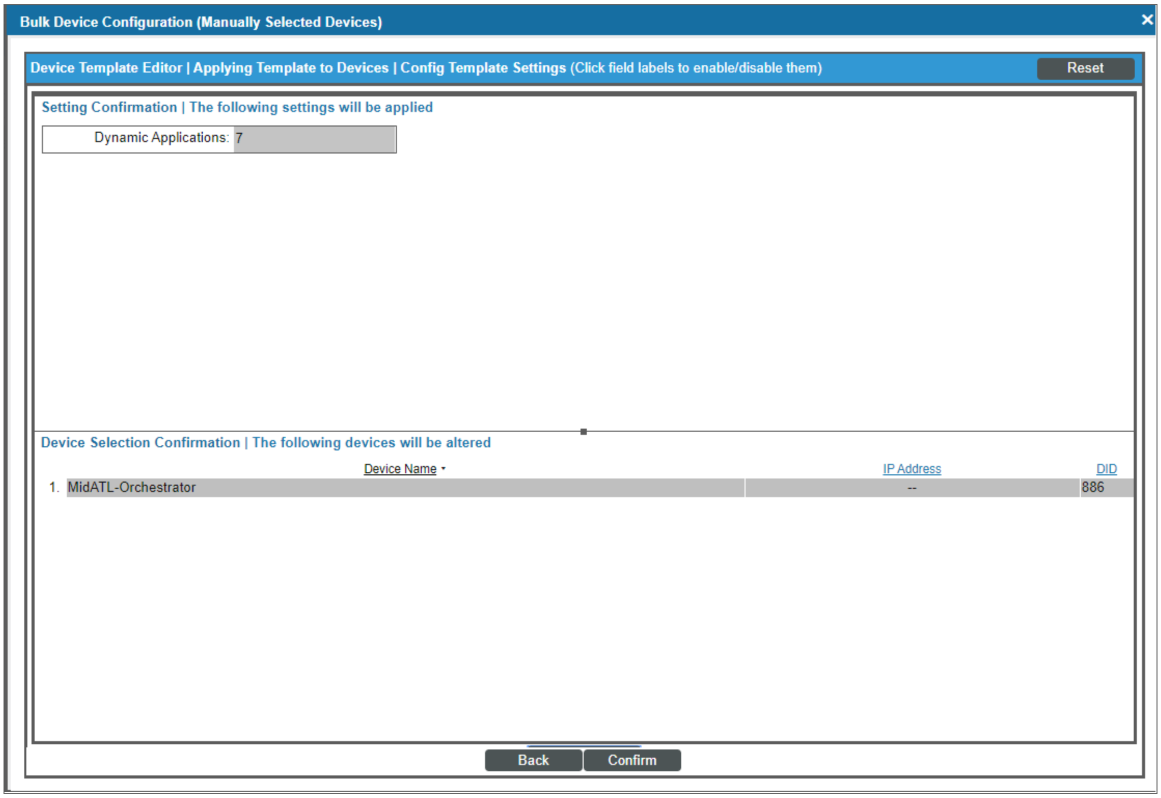
Interface Inventory Settings

Interface Inventory: 600000 ms
Maximum Allowed: 10000 interfaces

- In the ***Template*** field, select "Silver Peak: Orchestrator Template".
- ***Save When Applied & Confirmed***. From the **Bulk Device Configuration** page, you can edit the value in any of the fields in any of the tabs of the device template.
    - *If you select this field*, any changes you make to fields in the **Bulk Device Configuration** page will be saved to the template.
    - *If you don't select this field*, you can edit the values in any of the fields, and the edited values won't be saved in the device template, but will be applied to the device group.

5. Click the **[Apply]** button to apply the device template and any changed field values to the selected device.

6. The **Device Setting Confirmation** page appears.



Bulk Device Configuration (Manually Selected Devices)
Device Template Editor | Applying Template to Devices | Config Template Settings (Click field labels to enable/disable them)
Reset
Setting Confirmation | The following settings will be applied
Device Selection Confirmation | The following devices will be altered
Back
Confirm

Dynamic Applications: 7

	Device Name	IP Address	DID
1.	MidATL-Orchestrator	--	886

- In this page, you can view any settings in the device template that are different from SL1 default settings.
- You can click a field to disable it. When you disabled a field, its value will not be applied to the selected device group or selected devices.
- You can also view a list of devices to which the device template will be applied.

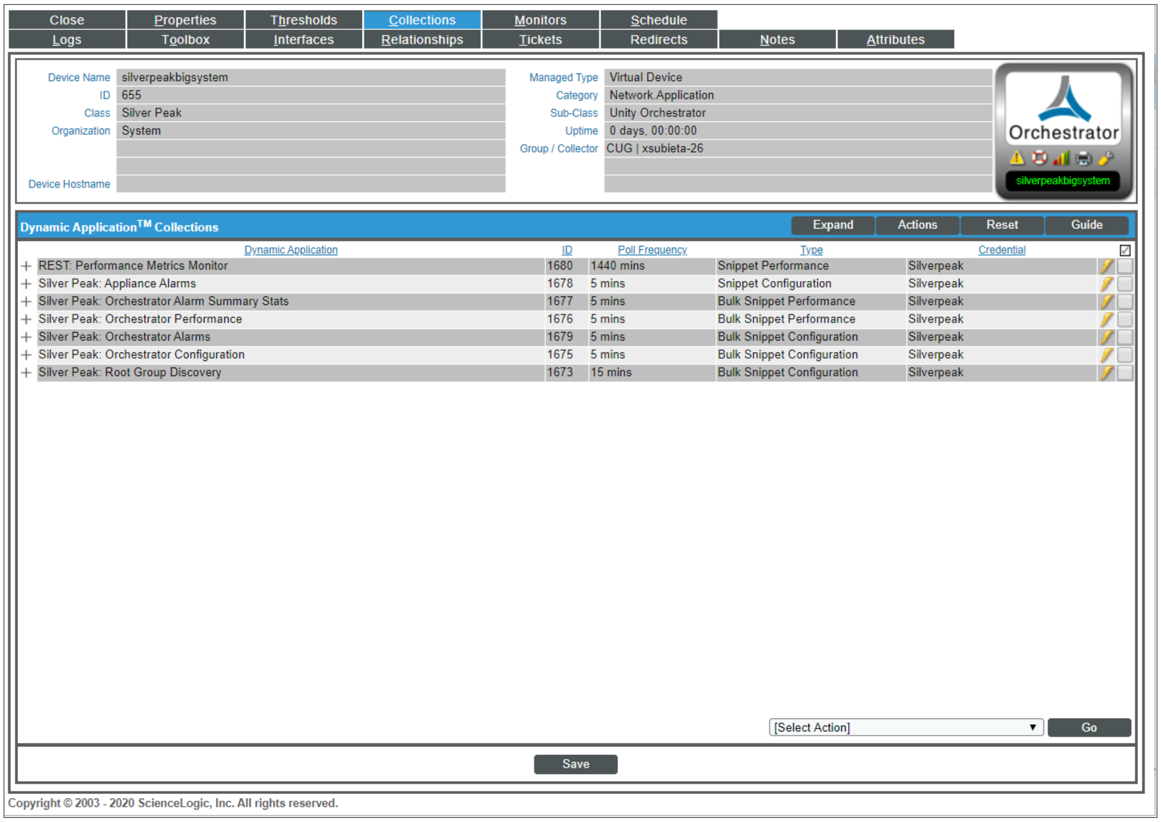
7. To approve the changes and the device list, click the **[Confirm]** button in the **Device Setting Confirmation** page.
8. The device template will be applied to the selected device.

Verifying Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. After discovery has completed, click the device icon for the Silver Peak Unity Orchestrator. From the **Device Properties** page for the Orchestrator, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. All applicable Dynamic Applications for the service 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	silverpeakbigsystem	Managed Type	Virtual Device
ID	655	Category	Network.Application
Class	Silver Peak	Sub-Class	Unity Orchestrator
Organization	System	Uptime	0 days, 00:00:00
		Group / Collector	CUG | xsubieta-26
Device Hostname			

Dynamic Application™ Collections

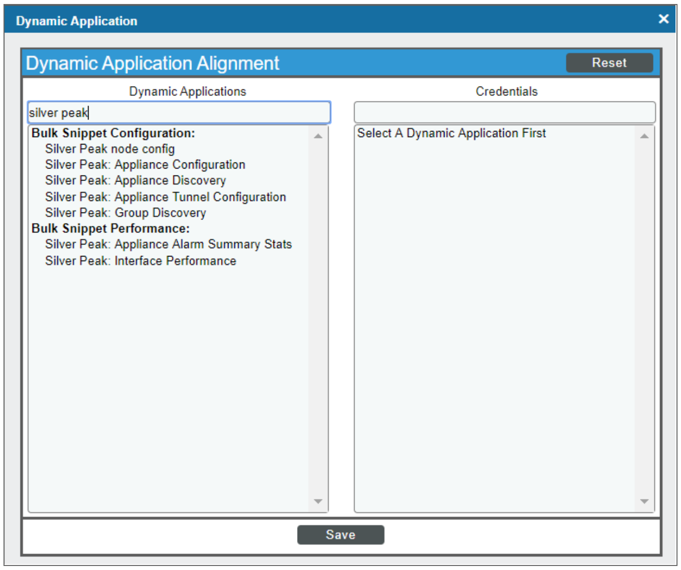
Dynamic Application	ID	Poll Frequency	Type	Credential	☑
+ REST: Performance Metrics Monitor	1680	1440 mins	Snippet Performance	Silverpeak	□
+ Silver Peak: Appliance Alarms	1678	5 mins	Snippet Configuration	Silverpeak	□
+ Silver Peak: Orchestrator Alarm Summary Stats	1677	5 mins	Bulk Snippet Performance	Silverpeak	□
+ Silver Peak: Orchestrator Performance	1676	5 mins	Bulk Snippet Performance	Silverpeak	□
+ Silver Peak: Orchestrator Alarms	1679	5 mins	Bulk Snippet Configuration	Silverpeak	□
+ Silver Peak: Orchestrator Configuration	1675	5 mins	Bulk Snippet Configuration	Silverpeak	□
+ Silver Peak: Root Group Discovery	1673	15 mins	Bulk Snippet Configuration	Silverpeak	□

You should see the following Dynamic Applications aligned to the New Relic service:

- REST: Performance Metrics Monitor
- Silver Peak: Appliance Alarms
- Silver Peak: Orchestrator Alarm Summary Stats
- Silver Peak: Orchestrator Performance
- Silver Peak: Orchestrator Alarms
- Silver Peak: Orchestrator Configuration
- Silver Peak: Root Group Discovery

If the listed Dynamic Applications have not been automatically aligned during discovery, or you want to align more Dynamic Applications, you can align them manually. To do so, perform the following steps:

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



silver peak

Bulk Snippet Configuration:
Silver Peak node config
Silver Peak: Appliance Configuration
Silver Peak: Appliance Discovery
Silver Peak: Appliance Tunnel Configuration
Silver Peak: Group Discovery
Bulk Snippet Performance:
Silver Peak: Appliance Alarm Summary Stats
Silver Peak: Interface Performance

Select A Dynamic Application First

2. In the ***Dynamic Applications*** field, select the Dynamic Application you want to align. You can narrow the search, as shown in the example above.
3. In the ***Credentials*** field, select the credential specified in the table.
4. Click the **[Save]** button.
5. Repeat steps 1-4 for any other unaligned Dynamic Applications.

Chapter 65

SMI-S: Array

Overview

The following sections describe how to configure SMI-S storage arrays for monitoring by SL1 using the *SMI-S: Array* PowerPack:

NOTE: For more information about the *SMI-S: Array* PowerPack, see the ***Monitoring SMI-S Storage Devices*** manual.

Prerequisites for Monitoring SMI-S Providers

To configure the SL1 system to monitor an SMI-S Provider using the *SMI-S: Array* PowerPack, you must have the following information about the SMI-S Provider that you want to monitor:

- IP address and port for the SMI-S Provider
- Username and password for a user with access to the SMI-S Provider

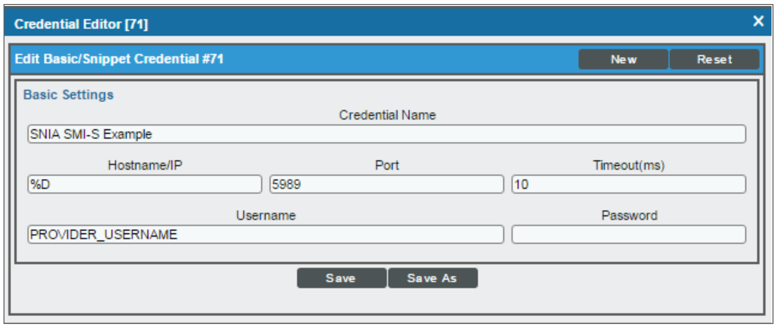
The SMI-S Provider will act as the root device during discovery by SL1.

Creating a Credential to Monitor Storage Arrays

To configure SL1 to monitor storage arrays, you must first create a Basic/Snippet credential. This credential allows the Dynamic Applications in the *SMI-S: Array* PowerPack to connect with an SMI-S Provider. An example Basic/Snippet credential that you can edit for your own use is included in the *SMI-S: Array* PowerPack.

To create a Basic/Snippet credential to access an SMI-S Provider:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **SNIA SMI-S Example** credential and then click its wrench icon (🔧). The **Edit Basic/Snippet Credential** modal page appears.
3. Enter values in the following fields:



Credential Editor [71]

Edit Basic/Snippet Credential #71

Basic Settings

Credential Name: SNIA SMI-S Example

Hostname/IP: %D

Port: 5989

Timeout(ms): 10

Username: PROVIDER_USERNAME

Password:

- ***Credential Name***. Enter a new name for the credential.
- ***Hostname/IP***. Enter "%D".
- ***Port***. Enter "5989" for an HTTPS connection.
- ***Username***. Enter the username for a user with access to the SMI-S Provider.
- ***Password***. Enter the password for the SMI-S Provider account username.

4. Click the **[Save As]** button.
5. When the confirmation message appears, click **[OK]**.

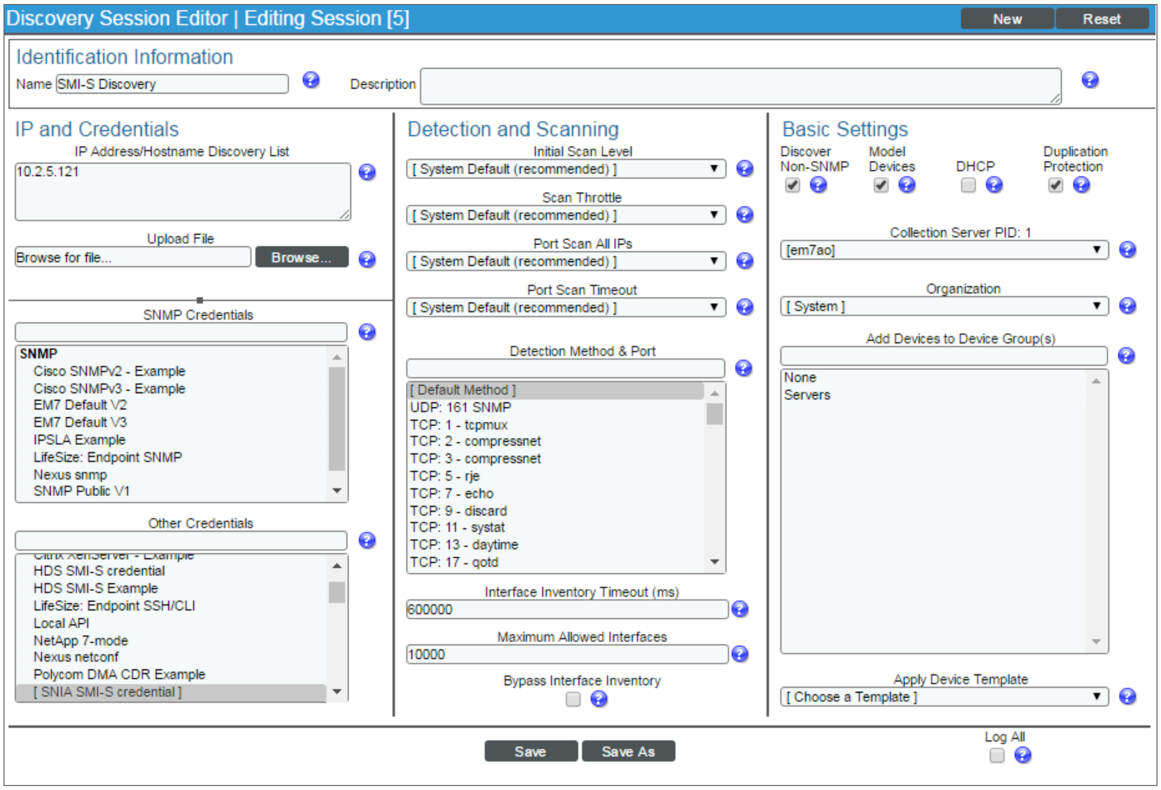
Discovering Storage Arrays

To model and monitor your storage system, you must first run a discovery session to discover the SMI-S Provider that SL1 will use as the root device for monitoring the storage system.

The discovery session will discover the SMI-S Provider as a pingable device using ***the Basic/Snippet credential that you created***. You must then manually align the "SMI-S: Array Discovery" Dynamic Application to the SMI-S Provider pingable device. When you do so, SL1 will discover, model, and monitor the remaining component devices in your storage system.

To discover the storage system 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. On this page, define values in the following fields:



Discovery Session Editor | Editing Session [5]

Identification Information

Name: SMI-S Discovery

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.2.5.121

Upload File: Browse for file...

SNMP Credentials: SNMP — Cisco SNMPv2 - Example, Cisco SNMPv3 - Example, EM7 Default V2, EM7 Default V3, IPSLA Example, LifeSize: Endpoint SNMP, Nexus snmp, SNMP Public V1

Other Credentials: Citrix XenServer - Example, HDS SMI-S credential, HDS SMI-S Example, LifeSize: Endpoint SSH/CLI, Local API, NetApp 7-mode, Nexus netconf, Polycom DMA CDR Example, [SNIA SMI-S credential]

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: 1: [em7ao]

Organization: [System]

Add Devices to Device Group(s): None, Servers

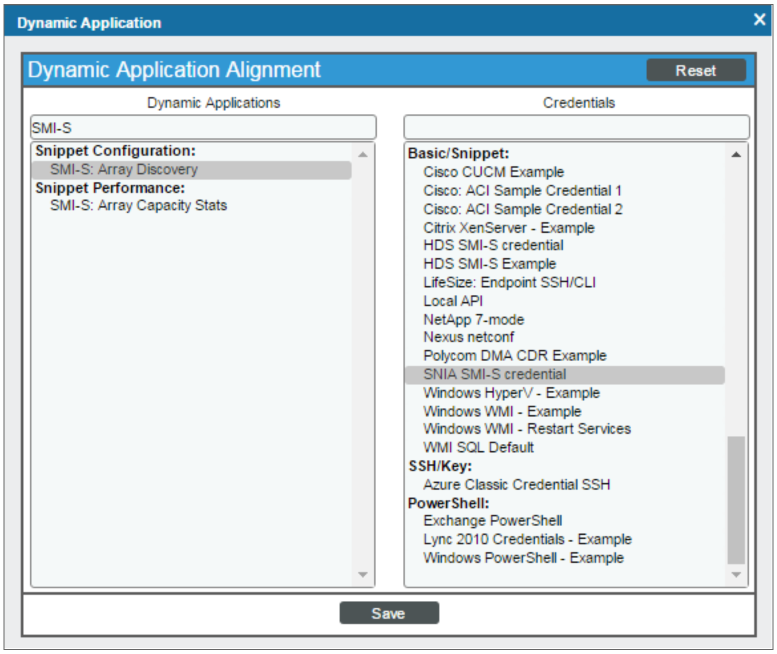
Apply Device Template: [Choose a Template]

Log All: □

- ***IP Address Discovery List***. Enter the IP address for the SMI-S Provider.
- ***Other Credentials***. Select the Basic/Snippet credential you created for the SMI-S Provider.
- ***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 SMI-S Provider is discovered, click its device icon ( ) to view the **Device Properties** page for the SMI-S Provider.
8. From the **Device Properties** page for the SMI-S Provider, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.

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



Dynamic Application

Dynamic Application Alignment

Dynamic Applications

SMI-S

Snippet Configuration:
SMI-S: Array Discovery
Snippet Performance:
SMI-S: Array Capacity Stats

Credentials

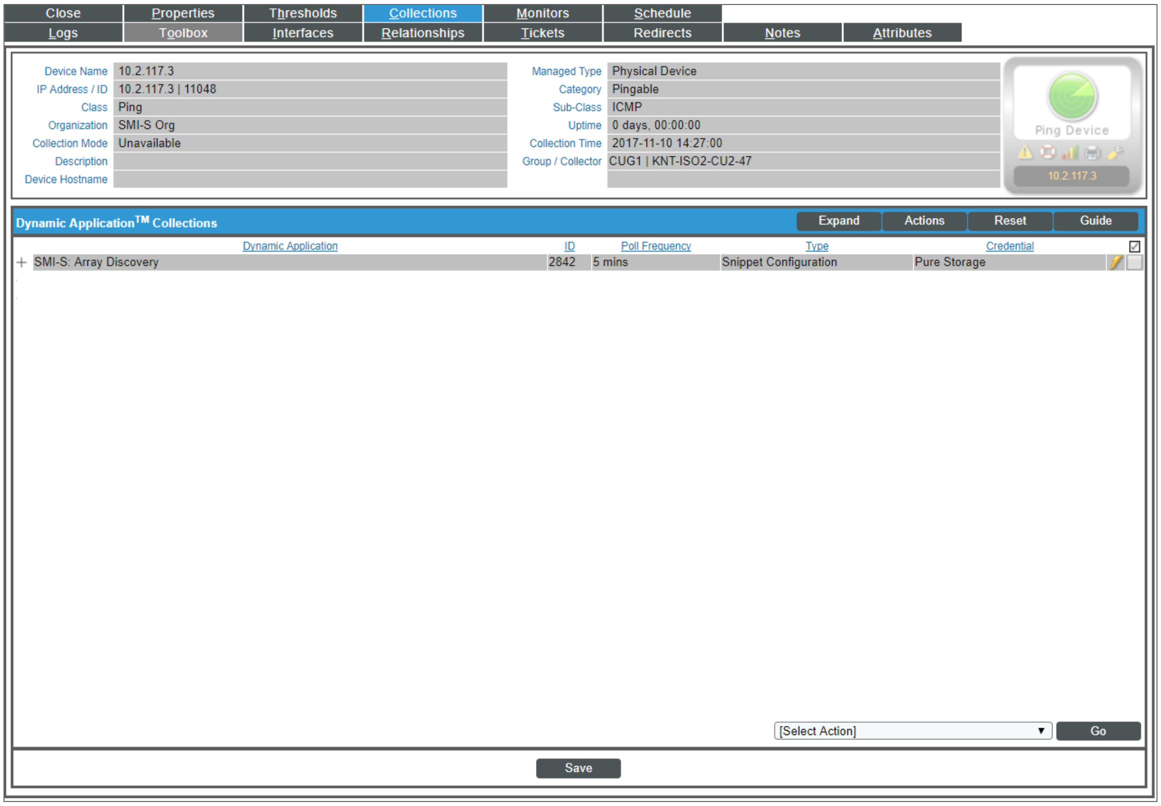
Basic/Snippet:
Cisco CUCM Example
Cisco: ACI Sample Credential 1
Cisco: ACI Sample Credential 2
Citrix XenServer - Example
HDS SMI-S credential
HDS SMI-S Example
LifeSize: Endpoint SSH/CLI
Local API
NetApp 7-mode
Nexus netconf
Polycom DMA CDR Example
SNIA SMI-S credential
Windows HyperV - Example
Windows WMI - Example
Windows WMI - Restart Services
WMI SQL Default
SSH/Key:
Azure Classic Credential SSH
PowerShell:
Exchange PowerShell
Lync 2010 Credentials - Example
Windows PowerShell - Example

10. In the ***Dynamic Applications*** field, select *SMI-S: Array Discovery*.

11. In the ***Credentials*** field, select the Basic/Snippet credential you configured for the SMI-S Provider.

12. Click the **[Save]** button.

13. The "SMI-S: Array Discovery" Dynamic Application appears on the **Dynamic Application Collections** page and begins auto-aligning the other Dynamic Applications in the *SMI-S: Array* PowerPack to the SMI-S Provider and discovering the other component devices in the storage system.



Device Name	10.2.117.3	Managed Type	Physical Device
IP Address / ID	10.2.117.3 | 11048	Category	Pingable
Class	Ping	Sub-Class	ICMP
Organization	SMI-S Org	Uptime	0 days, 00:00:00
Collection Mode	Unavailable	Collection Time	2017-11-10 14:27:00
Description		Group / Collector	CUG1 | KNT-ISO2-CU2-47
Device Hostname			

Dynamic Application^{TM} Collections

Dynamic Application	ID	Poll Frequency	Type	Credential	☑
+ SMI-S: Array Discovery	2842	5 mins	Snippet Configuration	Pure Storage	□

NOTE: It might take several minutes after manually aligning the discovery Dynamic Application for SL1 to discover and model the remaining component devices in the storage system.

Chapter

66

SoftLayer: Cloud

Overview

The following sections describe how to configure SoftLayer resources for monitoring by SL1 using the *SoftLayer: Cloud* PowerPack:

NOTE: For more information about the *SoftLayer: Cloud* PowerPack, see the ***Monitoring SoftLayer*** manual.

Copying Your SoftLayer API Key

Before you can monitor your SoftLayer account in SL1, you must first generate or retrieve the user-specific API key for your SoftLayer account. SL1 requires this unique API key to communicate with your SoftLayer account.

To generate your SoftLayer API key:

1. Log in to the SoftLayer customer portal and go to the **Users** page (Account > Users).
2. Click the **Generate** link in the ***API Key*** column for your SoftLayer user. The **Generate** link changes to a **Show** link.

3. Click the **Show** link. Your API key appears.
4. Copy the API key.

To retrieve your SoftLayer API key:

1. Log in to the SoftLayer customer portal.
2. Click your username on the Navigation Pane. The **Edit User Profile** page appears.
3. Locate and copy the API Key.

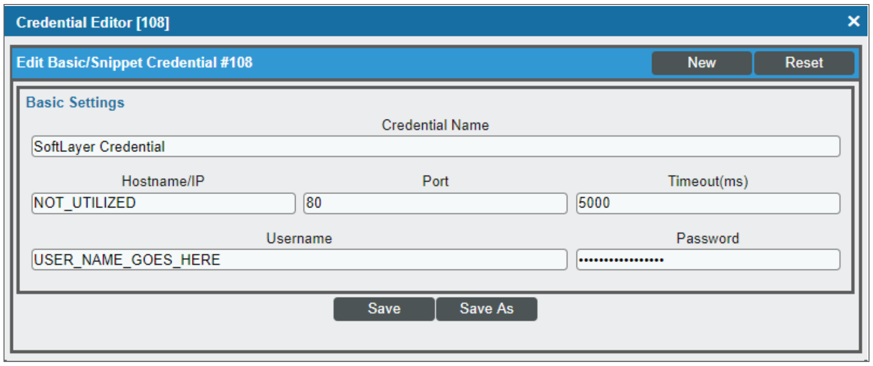
Configuring a SoftLayer Credential

To configure SL1 to monitor a SoftLayer account, you must create a Basic/Snippet credential. This credential allows the Dynamic Applications in the *SoftLayer: Cloud* PowerPack to communicate with your SoftLayer account.

An example Basic/Snippet credential that you can edit for your own use is included in the *SoftLayer: Cloud* PowerPack.

To configure a Basic/Snippet credential to access your SoftLayer account:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **SoftLayer Credential** and click its wrench icon (🔧). The **Edit Basic/Snippet Credential** page appears.
3. Complete the following fields:



Credential Editor [108]

Edit Basic/Snippet Credential #108

Basic Settings

Credential Name: SoftLayer Credential

Hostname/IP: NOT_UTILIZED

Port: 80

Timeout(ms): 5000

Username: USER_NAME_GOES_HERE

Password: ••••••••••••••••••

- ***Credential Name***. Type a new name for the SoftLayer credential.
- ***Hostname/IP***. Type a value, such as "%D".

NOTE: The credential requires a value in the ***Hostname/IP*** field, but the value itself does not matter.

- ***Port***. Type "80".
- ***Timeout***. Type "5000".

- ***Username***. Type your SoftLayer account username.
- ***Password***. Type the ***API key for the SoftLayer account***.

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

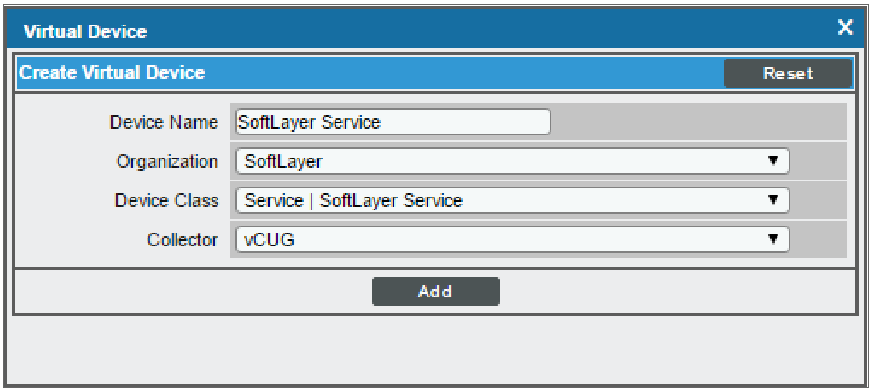
Creating a SoftLayer Virtual Device

Because the SoftLayer service does not have an IP address, you cannot discover a SoftLayer device using discovery. Instead, you must create a ***virtual device*** that represents the root device for the SoftLayer service. A virtual device is a user-defined container that represents a device or service that cannot be discovered by SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications.

TIP: If you have multiple SoftLayer subscriptions you want to monitor, you should create a separate virtual root device for each.

To create a virtual device that represents your SoftLayer service:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Click the **[Actions]** button and select *Create Virtual Device* from the menu. The **Virtual Device** modal page appears.
3. Enter values in the following fields:



Device Name: SoftLayer Service
Organization: SoftLayer
Device Class: Service | SoftLayer Service
Collector: vCUG

- ***Device Name***. Enter a name for the device. For example, you could enter "SoftLayer Service" in this field.
- ***Organization***. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.
- ***Device Class***. Select *Service | SoftLayer Service*.
- ***Collector***. Select the collector group that will monitor the device.

4. Click the **[Add]** button to create the virtual device.

Aligning the SoftLayer Dynamic Applications

There are three types of Dynamic Applications included in the *SoftLayer: Cloud* PowerPack:

- ***Discovery***. These Dynamic Applications poll SoftLayer for new instances of services or changes to existing instances of services.
- ***Configuration***. These Dynamic Applications retrieve configuration information about each service instance and retrieve any changes to that configuration information.
- ***Performance***. These Dynamic Applications poll SoftLayer for performance metrics.

To discover all of the components of your SoftLayer account, you must manually align the "SoftLayer: Account Discovery" Dynamic Application with the SoftLayer virtual device.

When you align the "SoftLayer: Account Discovery" Dynamic Application with the SoftLayer virtual device, the Dynamic Application creates a component device representing the SoftLayer account. Under the SoftLayer account component device, SL1 automatically aligns additional Dynamic Applications that:

- Discover and create child component devices for each region used by the SoftLayer account
- Discover and create child component devices for the SoftLayer CDN service and any CDN accounts associated with the SoftLayer account
- Retrieve SoftLayer account invoice information

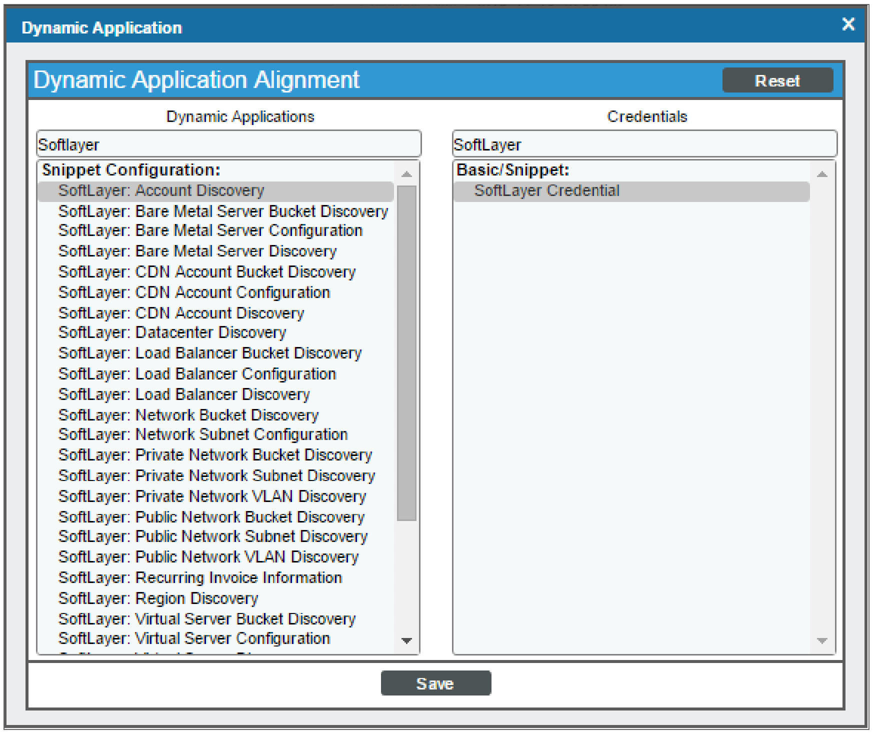
Under each region, SL1 then discovers "bucket" component devices that act as parents for each of the following component devices, which SL1 also discovers:

- Virtual Servers
- Bare Metal Servers
- Network Services
    - Private Networks
        - Subnets
        - VLANs
    - Public Networks
        - Subnets
        - VLANs
- Local Load Balancers

To align the "SoftLayer: Account Discovery" Dynamic Application to your SoftLayer virtual device, perform the following steps:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).

2. Click the wrench icon (🔧) for your SoftLayer virtual device.
3. In the **Device Administration** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
4. Click the **[Action]** button and select *Add Dynamic Application* from the menu.
5. In the **Dynamic Application Alignment** modal page:


Dynamic Application
Dynamic Application Alignment
Reset
Dynamic Applications
Credentials
Softlayer
SoftLayer
Snippet Configuration:
SoftLayer: Account Discovery
SoftLayer: Bare Metal Server Bucket Discovery
SoftLayer: Bare Metal Server Configuration
SoftLayer: Bare Metal Server Discovery
SoftLayer: CDN Account Bucket Discovery
SoftLayer: CDN Account Configuration
SoftLayer: CDN Account Discovery
SoftLayer: Datacenter Discovery
SoftLayer: Load Balancer Bucket Discovery
SoftLayer: Load Balancer Configuration
SoftLayer: Load Balancer Discovery
SoftLayer: Network Bucket Discovery
SoftLayer: Network Subnet Configuration
SoftLayer: Private Network Bucket Discovery
SoftLayer: Private Network Subnet Discovery
SoftLayer: Private Network VLAN Discovery
SoftLayer: Public Network Bucket Discovery
SoftLayer: Public Network Subnet Discovery
SoftLayer: Public Network VLAN Discovery
SoftLayer: Recurring Invoice Information
SoftLayer: Region Discovery
SoftLayer: Virtual Server Bucket Discovery
SoftLayer: Virtual Server Configuration
Basic/Snippet:
SoftLayer Credential
Save

- In the ***Dynamic Applications*** field, select *SoftLayer: Account Discovery*.
- In the ***Credentials*** field, select the ***credential you created for your SoftLayer service***.

6. Click the **[Save]** button to align the Dynamic Application with the SoftLayer virtual device.

Adding Collection Objects to the SoftLayer Dynamic Applications

If you want SL1 to collect information about your SoftLayer account that is not already collected by the Dynamic Applications in the *SoftLayer: Cloud* PowerPack, you can add a Collection Object to the appropriate Dynamic Application to enable SL1 to do so.

The following SoftLayer reference documents describe the possible properties that can be collected:

- For bare metal servers: http://sldn.softlayer.com/reference/datatypes/SoftLayer_Hardware_Server

- For virtual servers: http://sldn.softlayer.com/reference/datatypes/SoftLayer_Virtual_Guest
- For load balancers: http://sldn.softlayer.com/reference/datatypes/SoftLayer_Billing_Item_Network_Application_Delivery_Controller_LoadBalancer_VirtualIpAddress

To add a SoftLayer property as a collection object, you must translate the property hierarchy to a string. To format the property hierarchy as a string, separate each group in the hierarchy with a dash character followed by a dash and the property name. For example, the property for hard drive capacity (named "capacity") on a bare metal server is under the hardDrives group, then the hardwareComponentModel group. The string format for this hierarchy is:

```
hardDrives-hardwareComponentModel-capacity
```

To add a Collection Object to a SoftLayer Dynamic Application:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
2. Find the Dynamic Application to which you want to add a collection object, then click its wrench icon (🔧). The **Dynamic Applications Properties Editor** page appears. You can add collection objects to the following Dynamic Applications:
    - SoftLayer: Bare Metal Server Configuration
    - SoftLayer: Bare Metal Server Private Network Performance
    - SoftLayer: Bare Metal Server Public Network Performance
    - SoftLayer: Virtual Server Configuration
    - SoftLayer: Virtual Server CPU Performance
    - SoftLayer: Virtual Server Memory Performance
    - SoftLayer: Virtual Server Private Network Performance
    - SoftLayer: Virtual Server Public Network Performance
    - SoftLayer: Load Balancer Configuration
3. Click the **[Collections]** tab. The **Dynamic Applications | Collections Objects** page appears.
4. Enter values in the fields on this page. Enter the string that represents the property hierarchy in the ***Snippet Arguments*** field. For information about the other fields in this page, see the see the ***Dynamic Application Development manual***.
5. Click the **[Save]** button to save the collection object.
6. If you added a collection object to a performance Dynamic Application, a presentation object is automatically created for the collection object. If you want to edit the presentation object, click the **[Presentations]** tab and click the wrench icon (🔧) for the presentation object.
7. If you added a collection object for a property that is in a group from which no other properties are collected, you must repeat steps 1 - 6 to add the unique ID of that group as a collection object.

Chapter 67

VMware: NSX

Overview

The following sections describe how to configure VMware NSX resources for monitoring by SL1 using the *VMware: NSX* PowerPack:

> NOTE: For more information about the *VMware: NSX* PowerPack, see the ***Monitoring VMware NSX*** manual.

Prerequisites for Monitoring VMware NSX

To configure SL1 to monitor VMware NSX using the *VMware: NSX* PowerPack, you must first configure an NSX Manager user account to handle RESTful API requests. You will need this account's username and password when *creating the Basic/Snippet credential* to communicate with the NSX Manager for monitoring.

This API-only user account must be configured in the NSX Manager configuration terminal and have web interface privileges. After you create the user account, perform an API request to give the user account the appropriate role.

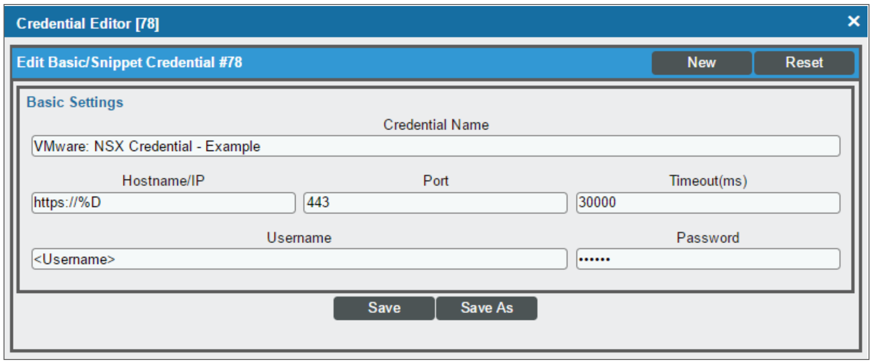
Creating a Basic/Snippet Credential

To use the Dynamic Applications in the *VMware: NSX* PowerPack, you must create a Basic/Snippet credential for the NSX Manager. The *VMware: NSX* PowerPack includes an example Basic/Snippet credential that you can edit for use with NSX Manager.

To modify the template credential, perform the following steps:

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

2. Click the wrench icon (🔧) for the "VMware: NSX Credential - Example" credential. The **Credential Editor** modal page appears:



Credential Editor [78]

Edit Basic/Snippet Credential #78

Basic Settings

Credential Name: VMware: NSX Credential - Example

Hostname/IP: https://%D

Port: 443

Timeout(ms): 30000

Username: <Username>

Password: ••••••

3. Supply values in the following fields:

   - ***Credential Name***. Type a new name for the credential.
   - ***Hostname/IP***. Type "https://%D".
   - ***Port***. Type "443".
   - ***Timeout(ms)***. Keep the default value.
   - ***Username***. Type the username of the NSX API-only administrative user.
   - ***Password***. Type the NSX API-only user's password.

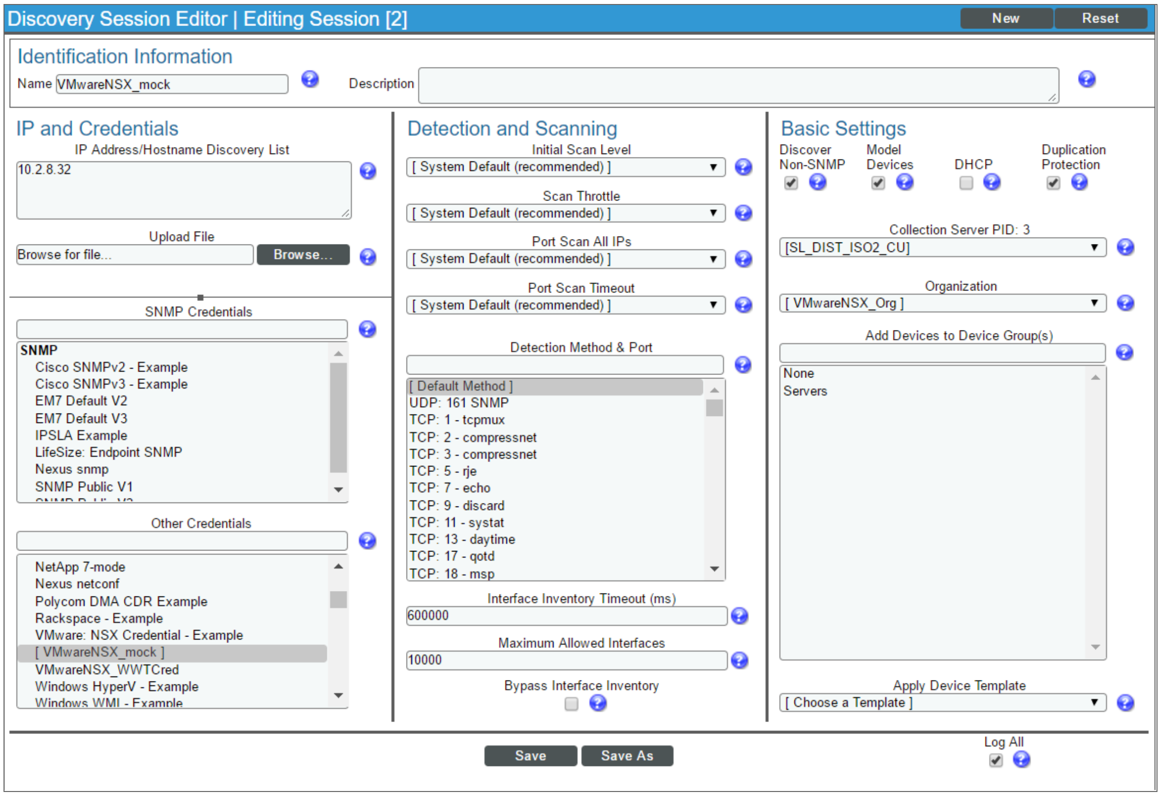
4. Click the **[Save As]** button to save your changes as a new credential.

Discovering a VMware NSX Manager

To create and run a discovery session that will discover an NSX Manager, perform the following steps:

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

2. Click the **[Create]** button to create a new discovery session. The **Discovery Session Editor** modal page appears:



Discovery Session Editor | Editing Session [2]

Identification Information

Name: VMwareNSX_mock

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.2.8.32

Upload File: Browse for file...

SNMP Credentials:
SNMP
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
EM7 Default V2
EM7 Default V3
IPSLA Example
LifeSize: Endpoint SNMP
Nexus snmp
SNMP Public V1

Other Credentials:
NetApp 7-mode
Nexus netconf
Polycom DMA CDR Example
Rackspace - Example
VMware: NSX Credential - Example
[VMwareNSX_mock]
VMwareNSX_WWTCred
Windows HyperV - Example
Windows WMI - Example

Detection and Scanning

Initial Scan Level: [System Default (recommended)]

Scan Throttle: [System Default (recommended)]

Port Scan All IPs: [System Default (recommended)]

Port Scan Timeout: [System Default (recommended)]

Detection Method & Port:
[Default Method]
UDP: 161 SNMP
TCP: 1 - tcpmux
TCP: 2 - compressnet
TCP: 3 - compressnet
TCP: 5 - rje
TCP: 7 - echo
TCP: 9 - discard
TCP: 11 - systat
TCP: 13 - daytime
TCP: 17 - qotd
TCP: 18 - msp

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: 3 [SL_DIST_ISO2_CU]

Organization: [VMwareNSX_Org]

Add Devices to Device Group(s):
None
Servers

Apply Device Template: [Choose a Template]

Log All: ☑

3. Enter values in the following fields:

- ***IP Address Discovery List***. Type the IP address for the NSX Manager.
- ***Other Credentials***. Select the *Basic/Snippet credential* you created.
- ***Discover Non-SNMP***. 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** modal page.

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. After SL1 discovers the NSX Manager, click its device icon ( ) to view the **Device Properties** page for the NSX Manager.

Chapter 68

VMware: vSphere Base Pack

Overview

The following sections describe how to configure VMware vCenter resources for monitoring by SL1 using the *VMware: vSphere Base Pack* PowerPack:

NOTE: For more information about the *VMware: vSphere Base Pack* PowerPack, see the ***Monitoring VMware Systems*** manual.

Prerequisites for Monitoring VMware vCenter Servers

Before performing the steps for configuring a vCenter server, you must:

- Have access to a VMware vCenter server that monitors your ESXi and ESX servers.
- Have access to the vCenter server using the vSphere web client.

If the Windows Server that hosts the vCenter server is SNMP-enabled, you must also configure your ESXi or ESX servers for communication using SNMP. To do so, you must:

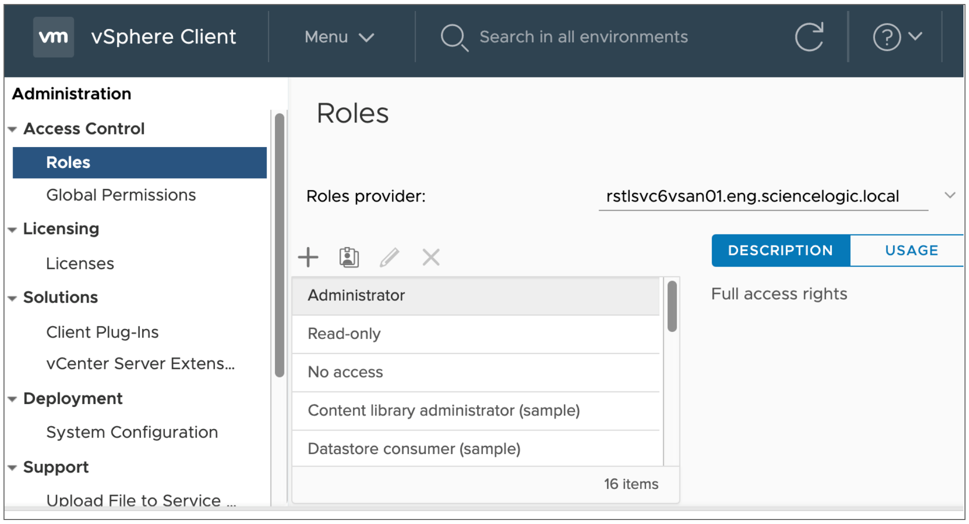
- Configure SNMP community strings, traps, and polling on the ESXi or ESX server. Assign the server at least one SNMP community string. For more information, see VMware's documentation for Configuring SNMP for ESXi 6.5 or Configuring SNMP for ESXi 6.7.

Creating a Read-Only User Account for Monitoring

Administrative users are the only default user type that have the level of access SL1 requires to collect data from the VMware vCenter web service. If you do not want to use the username and password of an administrative user in the SOAP/XML credential, you can set up a custom user role with the specific read-only access SL1 requires to the VMware vCenter web service.

To create a custom user role that grants the read-only access SL1 requires, perform the following steps:

1. Open your vCenter client at `https://<vcenterservername>/ui`
2. Select Menu > Administration from the drop-down.
3. In the menu at the left of the page, click Access Control > Roles. The **Roles** page appears:



Roles provider: rstlsvc6vsan01.eng.sciencelogic.local

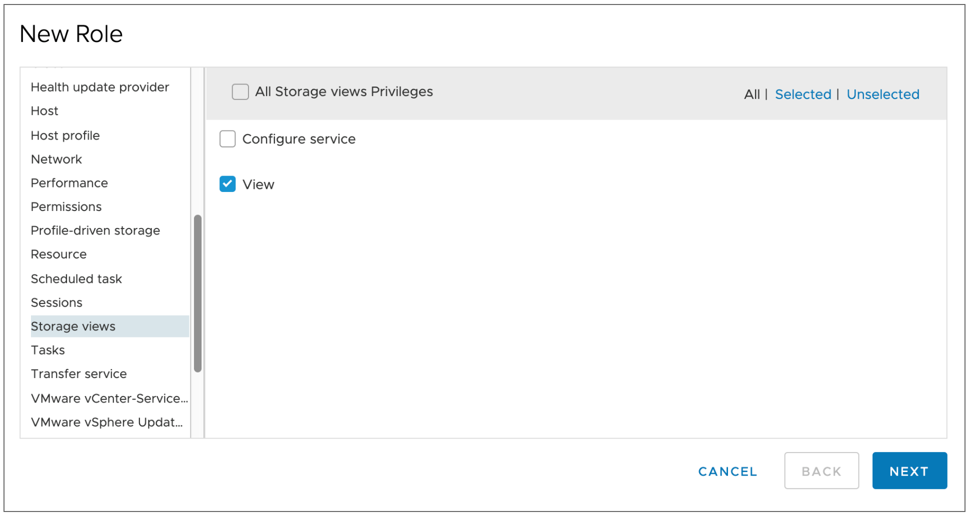
Administrator
Read-only
No access
Content library administrator (sample)
Datastore consumer (sample)

16 items

Full access rights

4. Click the plus sign (+) to add a new Role. The **New Role** page appears:

5. In the pane on the left, select **Storage views** and select the ***View*** checkbox. Click **[Next]**.

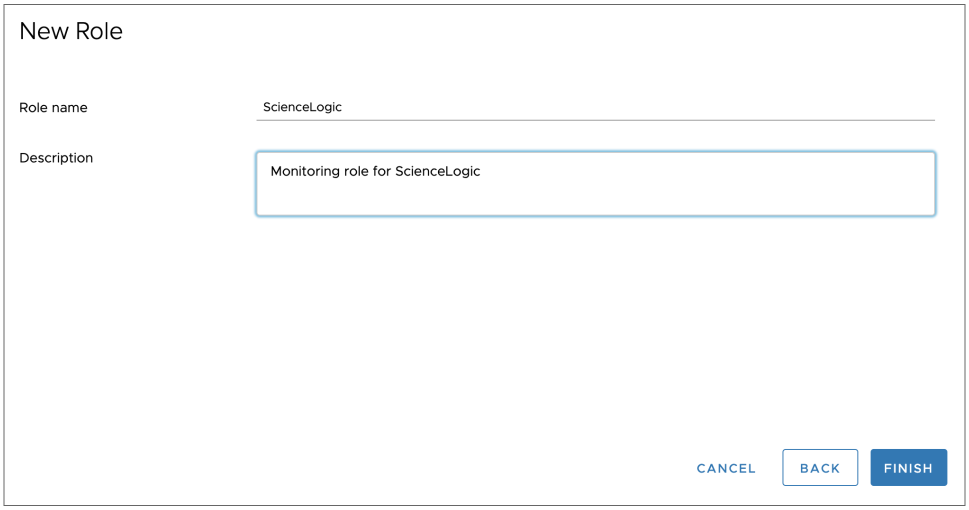

New Role

☐ All Storage views Privileges

☐ Configure service

☑ View

6. In the next screen, enter a name for the role in the ***Role name*** field. Optionally, you can enter a description in the ***Description*** field.


New Role

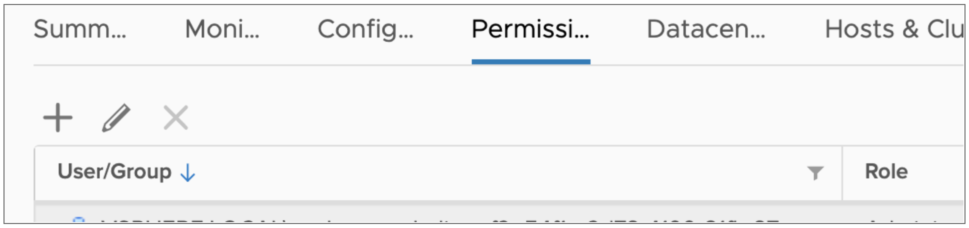
Role name: ScienceLogic

Description: Monitoring role for ScienceLogic

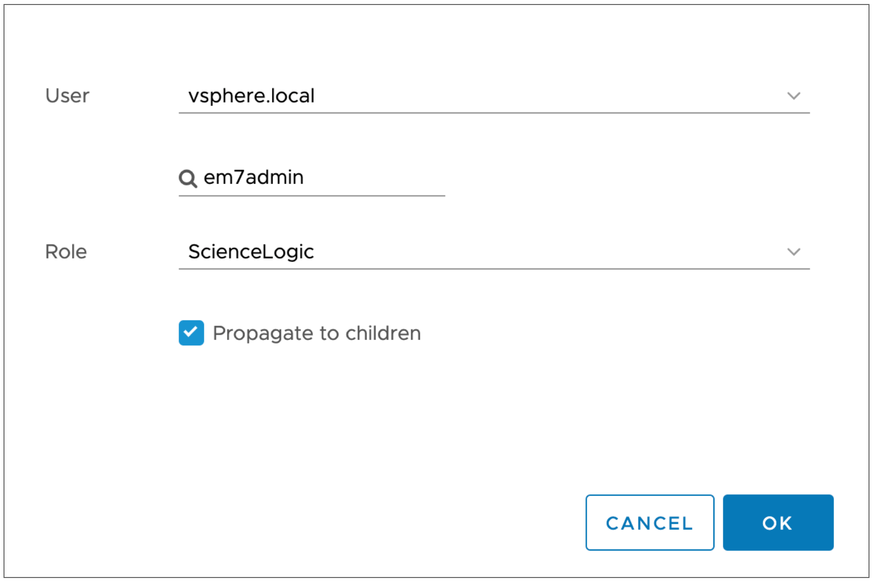
7. Click the **[Finish]** button.

To assign the custom role to a user account, perform the following steps:

1. In the vCenter client, select your vCenter server containing the hosts and clusters you are monitoring and click the **[Permissions]** tab.



2. Click the plus sign (+) to add permissions.
3. Enter values in the following fields:
    - ***User***. Select your domain and add the user in the field below.
    - ***Role***. Select the role that you just created.
    - ***Propagate to children***. Select this checkbox.



User vsphere.local

em7admin

Role ScienceLogic

☑ Propagate to children

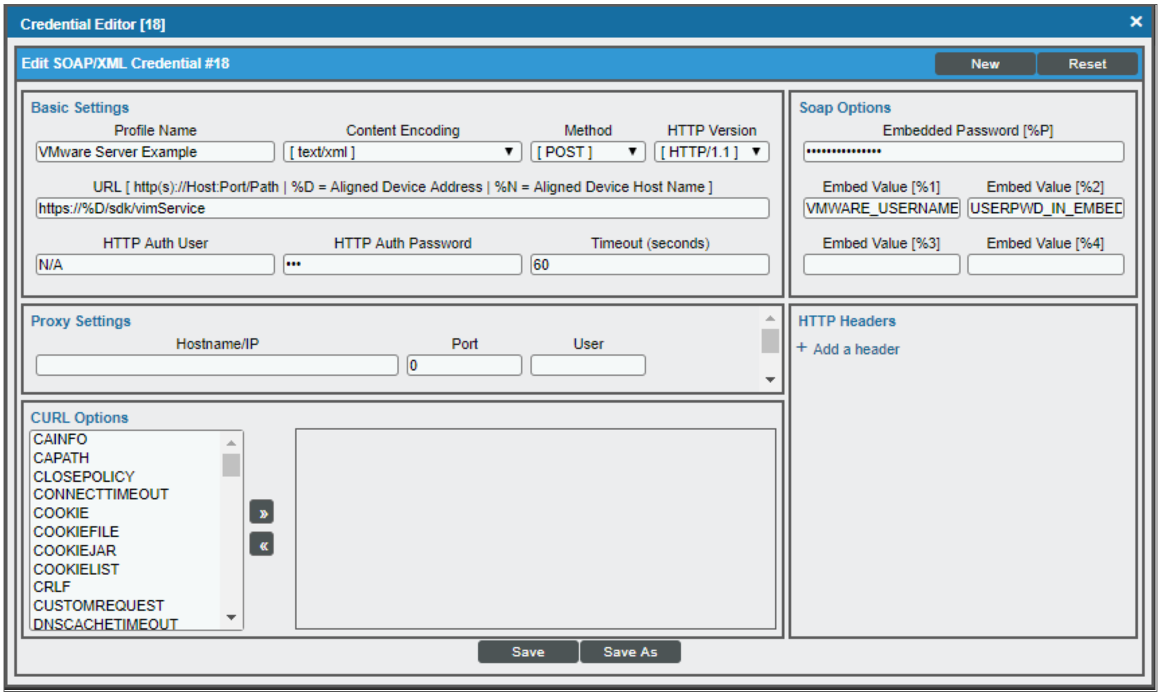
4. Click the **[OK]** button.

Configuring a SOAP/XML Credential

To modify either of the VMware credential templates in the SL1 classic user interface, perform the following steps:

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

2. Click the wrench icon ( ) for the "VMware Server Example" credential. The **Credential Editor** modal page appears:



Profile Name: VMware Server Example

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://%D/sdk/vimService

HTTP Auth User: N/A

HTTP Auth Password: •••

Timeout (seconds): 60

Embedded Password [%P]: •••••••••••••••

Embed Value [%1]: VMWARE_USERNAME

Embed Value [%2]: USERPWD_IN_EMBED

Embed Value [%3]:

Embed Value [%4]:

Hostname/IP:

Port: 0

User:

3. Supply values in the following fields:

   - ***Profile Name***. Enter a new name for the credential.
   - ***URL***. In most cases, you can use the default setting.
   - ***Embed Value [%1]***. Enter the username SL1 will use to connect to the VMware web service in the format `<domain>/<username>`. For example, `silo_domain\john_user`
   - ***Embedded Password [%P]***. Enter the password SL1 will use to connect to the VMware web service.

4. Click the **[Save As]** button to save your changes as a new credential.

CAUTION: Do not click the **[Save]** button, as it will save over the example credential, which you may need for future use.

Testing the VMware Credential

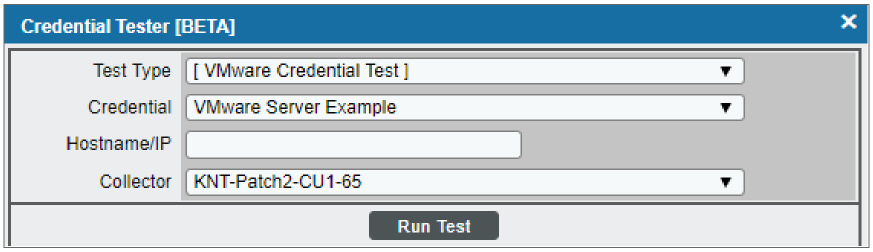
SL1 includes a Credential Test for VMware. Credential Tests define a series of steps that SL1 can execute on demand to validate whether a credential works as expected.

The VMware Credential Test can be used to test a SOAP/XML credential for monitoring VMware using the Dynamic Applications in the *VMware: vSphere Base Pack* PowerPack. The VMware Credential Test performs the following steps:

- ***Test Reachability***. Attempts to reach the vCenter server using ICMP.
- ***Attempt VMware Connection***. Attempts to connect to the VMware service using the account specified in the credential.

To test the VMware credential:

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



Credential Tester [BETA] ✕

Test Type: [VMware Credential Test] ▼
Credential: VMware Server Example ▼
Hostname/IP:
Collector: KNT-Patch2-CU1-65 ▼

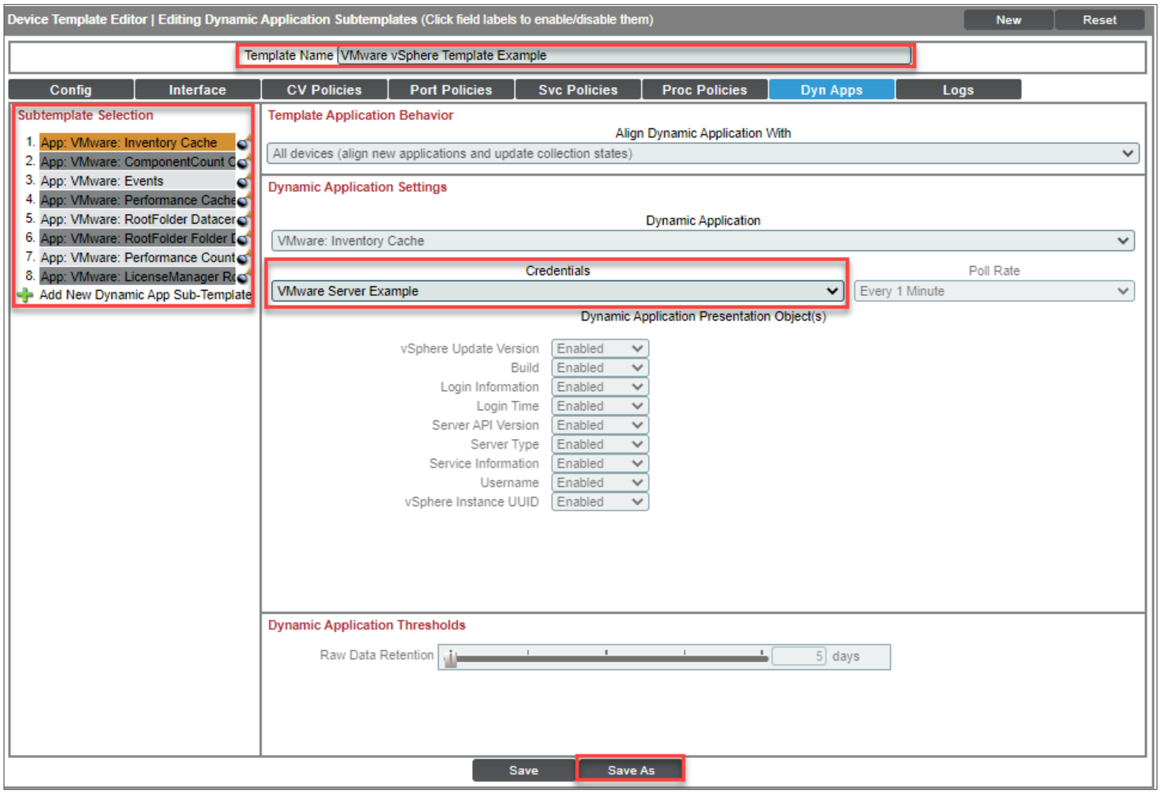
3. Supply values in the following fields:
   - ***Test Type***. This field is pre-populated with the credential test you selected.
   - ***Credential***. Select the credential to test. This drop-down list includes only credentials that you have access to that can be tested using the selected credential test.
   - ***Hostname/IP***. Type the IP address for the vCenter server.
   - ***Collector***. Select the All-In-One Appliance or Data Collector that will run the test.
4. Click the **[Run Test]** button. The **Test Credential** window appears, displaying 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***. Hover over the question mark icon (❓) with your mouse 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".

Configuring a VMware Device Template

A ***device template*** allows you to save a device configuration and apply it to multiple devices. The *VMware: vSphere Base Pack* PowerPack includes the "VMware vSphere Template." If you configure and apply this device template when you discover your vCenter server, SL1 aligns the appropriate Dynamic Applications to the discovered vCenter server device.

To configure the VMware device template:

1. Go to the **Configuration Templates** page (Devices > Templates or Registry > Devices > Templates in the SL1 classic user interface).
2. Locate the "VMware vSphere Template" and click its wrench icon (🔧). The **Device Template Editor** page appears.
3. Click the **[Dyn Apps]** tab. The **Editing Dynamic Application Subtemplates** page appears.
4. Complete the following fields:



Device Template Editor | Editing Dynamic Application Subtemplates (Click field labels to enable/disable them)

Template Name: VMware vSphere Template Example

Subtemplate Selection

1. App: VMware: Inventory Cache
2. App: VMware: ComponentCount C
3. App: VMware: Events
4. App: VMware: Performance Cache
5. App: VMware: RootFolder Datacer
6. App: VMware: RootFolder Folder D
7. App: VMware: Performance Count
8. App: VMware: LicenseManager Ro

Add New Dynamic App Sub-Template

Template Application Behavior

Align Dynamic Application With: All devices (align new applications and update collection states)

Dynamic Application Settings

Dynamic Application: VMware: Inventory Cache

Credentials: VMware Server Example

Poll Rate: Every 1 Minute

Dynamic Application Presentation Object(s)

vSphere Update Version: Enabled
Build: Enabled
Login Information: Enabled
Login Time: Enabled
Server API Version: Enabled
Server Type: Enabled
Service Information: Enabled
Username: Enabled
vSphere Instance UUID: Enabled

Dynamic Application Thresholds

Raw Data Retention: 5 days

- **Template Name**. Type a new name for the device template.
- **Credentials**. Select the SOAP/XML credential that you created for VMware.

5. Click the next Dynamic Application listed in the **Subtemplate Selection** section on the left side of the page and then select the VMware SOAP/XML credential in the ***Credentials*** field.

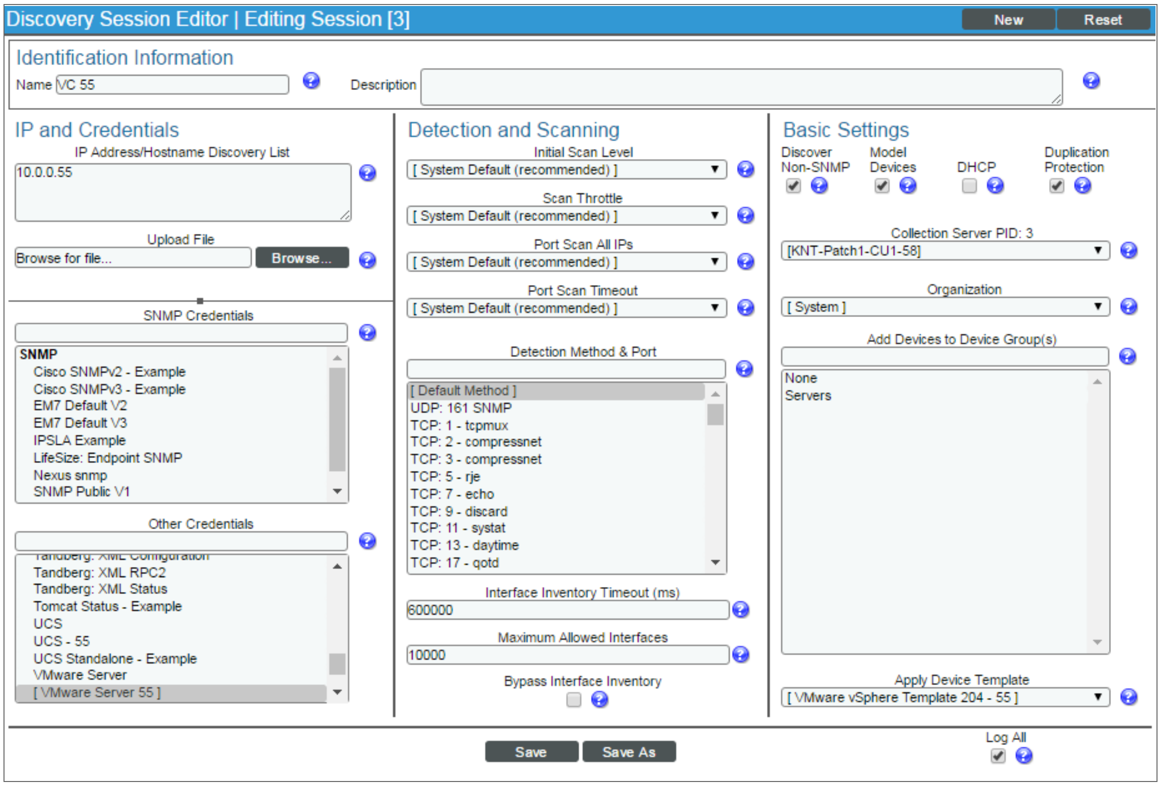
6. Repeat step 5 until the you have selected the VMware SOAP/XML credential in the ***Credentials*** field for all of the Dynamic Applications listed in the **Subtemplate Selection** section.
7. Click **[Save As]**.

> CAUTION: Do not click the **[Save]** button, as it will save over the "VMware vSphere Template", which you may need for future use.

Discovering a vCenter Server

To create and run a discovery session that will discover a vCenter server, perform the following steps:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. Click the **[Create]** button to create a new discovery session. The **Discovery Session Editor** modal page appears:



Discovery Session Editor | Editing Session [3]

Identification Information

Name: VC 55

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.0.0.55

Upload File: Browse for file...

SNMP Credentials:
SNMP
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
EM7 Default V2
EM7 Default V3
IPSLA Example
LifeSize: Endpoint SNMP
Nexus snmp
SNMP Public V1

Other Credentials:
Tandberg: XML Configuration
Tandberg: XML RPC2
Tandberg: XML Status
Tomcat Status - Example
UCS
UCS - 55
UCS Standalone - Example
VMware Server
[VMware Server 55]

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: 3: [KNT-Patch1-CU1-58]

Organization: [System]

Add Devices to Device Group(s):
None
Servers

Apply Device Template: [VMware vSphere Template 204 - 55]

Log All: ☑

3. Enter values in the following fields:

- ***IP Address Discovery List***. Type the IP address for the vCenter server.

- ***SNMP Credentials***. If the Windows server that hosts the vCenter server is SNMP-enabled, then select the SNMP credential for the vCenter server in this field. If you do not select an SNMP credential in this field, then you must select the ***Discover Non-SNMP*** checkbox.

> **NOTE:** For integration between SL1 and ServiceNow, it is recommended that you discover your VMware environment using SNMP, so that the root device is classified as a vCenter device rather than as a Ping device. If you discover as non-SNMP, you will need to manually reclassify the root device as a vCenter device class.

- ***Other Credentials***. Select the SOAP/XML credential that you created for VMware.
- ***Discover Non-SNMP***. If the Windows server that hosts the vCenter server is not SNMP-enabled, then you must select this checkbox.
- ***Apply Device Template***. Select the device template that you created for VMware.

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** modal page.
6. The discovery session you created will appear 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 vCenter server is discovered, click its device icon (🖥) to view the **Device Properties** page for the vCenter server.

Configuring the VMware Dynamic Applications

The following sections describe how to configure some of the Dynamic Applications in the *VMware: vSphere Base Pack*PowerPack.

Configuring the "VMware: Events" Dynamic Application

The "VMware: Events" Dynamic Application is designed to collect events from VMware devices using the VMware API and insert those events into the device log of the aligned vCenter server.

For SL1 to insert VMware events into the device log, the Data Collector that monitors the vCenter server must be configured to process API events. For instructions on how to configure a Data Collector to process API events, see the ***Global Settings*** chapter in the ***System Administration*** manual.

You can specify which types of events the "VMware: Events" Dynamic Application collects by editing the event dictionary Python script located in the "VMware Event Collection" snippet of the "VMware: Events" Dynamic Application. This event dictionary includes a series of rows that look like this:

```
"ClusterStatusChangedEvent": {"count": 0, "countAll": 0, "collect": True},
```

Each row begins with an event type. This event type value must match the "eventTypeId" value the VMware API uses in its "EventFilterSpec" data object to indicate which events should be collected. For more information, see VMware's documentation on the "EventFilterSpec" data object.

To specify which events the "VMware: Events" Dynamic Application collects:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
2. Click the wrench icon (🔧) for the "VMware: Events" Dynamic Application. The **Dynamic Applications Properties Editor** page appears.
3. Click the **[Snippets]** tab. The **Dynamic Applications Snippet Editor & Registry** page appears.
4. Click the wrench icon (🔧) for the "VMware Event Collection" snippet.
5. Locate the section that looks like this:

```
event_dict = {
  "AlarmStatusChangedEvent": {"count": 0, "countAll": 0, "collect": True},
  "ClusterStatusChangedEvent": {"count": 0, "countAll": 0, "collect": True},
  "HostStatusChangedEvent": {"count": 0, "countAll": 0, "collect": True},
  "UserLoginSessionEvent": {"count": 0, "countAll": 0, "collect": True},
  "UserLogoutSessionEvent": {"count": 0, "countAll": 0, "collect": True},
  "VmEvent": {"count": 0, "countAll": 0, "collect": True},
  "VmMigratedEvent": {"count": 0, "countAll": 0, "collect": True},
  "other": {"count": 0, "countAll": 0, "collect": True},
}
```

6. Following the format shown above, add new rows for any additional event types you want to include in the event dictionary or delete the rows of any event types you want to remove from the event dictionary.
7. For each event type listed in the event dictionary:

   - If you want the Dynamic Application to collect that event type, change the `"collect"` value to "`True`". For example:

     ```
     "AlarmStatusChangedEvent": {"count": 0, "countAll": 0, "collect": True},
     ```

   - If you do not want the Dynamic Application to collect that event type, change the `"collect"` value to "`False`". For example:

     ```
     "UserLoginSessionEvent": {"count": 0, "countAll": 0, "collect": False},
     ```

   - If you want the Dynamic Application to collect all event types, locate the `"other"` line and change the `"collect"` value to "`True`". For example:

     ```
     "other": {"count": 0, "countAll": 0, "collect": True},
     ```

NOTE: Changing the `"other"` `"collect"` value to "`True`" overrides any event types with a `"collect"` value of "`False`". If you do not want to collect all event types, then you must either remove the `"other"` row or change its `"collect"` value to "`False`".

8. Click the **[Save]** button.

TIP: If you have edited the "VMware Event Collection" snippet and want to maintain your `event_dict` settings the next time the PowerPack is upgraded, you must copy the event dictionary Python script, install the new version of the PowerPack, and then follow the steps in this section to paste the settings into the "VMware Event Collection" snippet in the upgraded version of the "VMware: Events" Dynamic Application.

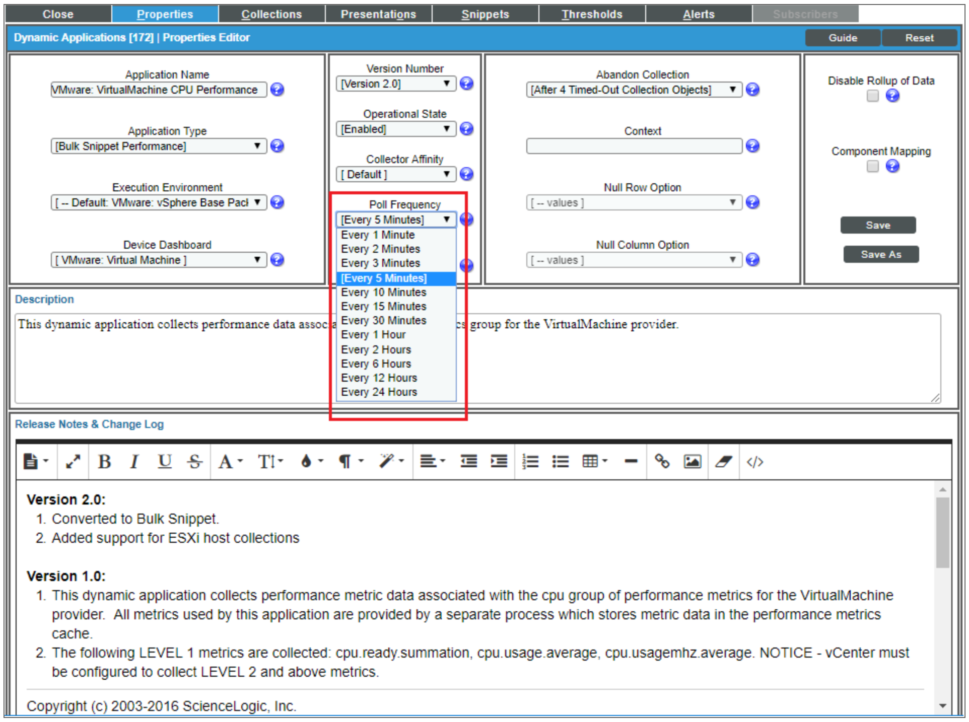
Configuring the Polling Frequency for VMware Performance Dynamic Applications

In the *VMware: vSphere Base Pack* PowerPack, some of the Dynamic Applications require that their ***Poll Frequency*** be set to a specific time to ensure the accuracy of the data they collect.

CAUTION: If there is a need to change the polling from the shipped values, vCenter performance is likely to be affected. Other configurations of the values are not recommended and/or guaranteed to work correctly.

To set the polling frequency:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
2. Search for the Dynamic Application whose polling frequency you want to update and click on its wrench icon (🔧).
3. In the **Dynamic Applications Properties Editor**, use the drop-down in the ***Poll Frequency*** field to select the polling frequency.



Dynamic Applications [172] | Properties Editor

Application Name: VMware: VirtualMachine CPU Performance

Application Type: [Bulk Snippet Performance]

Execution Environment: [-- Default: VMware: vSphere Base Pacl

Device Dashboard: [VMware: Virtual Machine]

Version Number: [Version 2.0]

Operational State: [Enabled]

Collector Affinity: [Default]

Poll Frequency: [Every 5 Minutes]

- Every 1 Minute
- Every 2 Minutes
- Every 3 Minutes
- [Every 5 Minutes]
- Every 10 Minutes
- Every 15 Minutes
- Every 30 Minutes
- Every 1 Hour
- Every 2 Hours
- Every 6 Hours
- Every 12 Hours
- Every 24 Hours

Abandon Collection: [After 4 Timed-Out Collection Objects]

Context:

Null Row Option: [-- values]

Null Column Option: [-- values]

Disable Rollup of Data ☐

Component Mapping ☐

Description

This dynamic application collects performance data assoc ... cs group for the VirtualMachine provider.

Release Notes & Change Log

Version 2.0:

1. Converted to Bulk Snippet.
2. Added support for ESXi host collections

Version 1.0:

1. This dynamic application collects performance metric data associated with the cpu group of performance metrics for the VirtualMachine provider. All metrics used by this application are provided by a separate process which stores metric data in the performance metrics cache.
2. The following LEVEL 1 metrics are collected: cpu.ready.summation, cpu.usage.average, cpu.usagemhz.average. NOTICE - vCenter must be configured to collect LEVEL 2 and above metrics.

Copyright (c) 2003-2016 ScienceLogic, Inc.

4. Set the polling frequencies for the following Dynamic Applications using the guidelines listed:

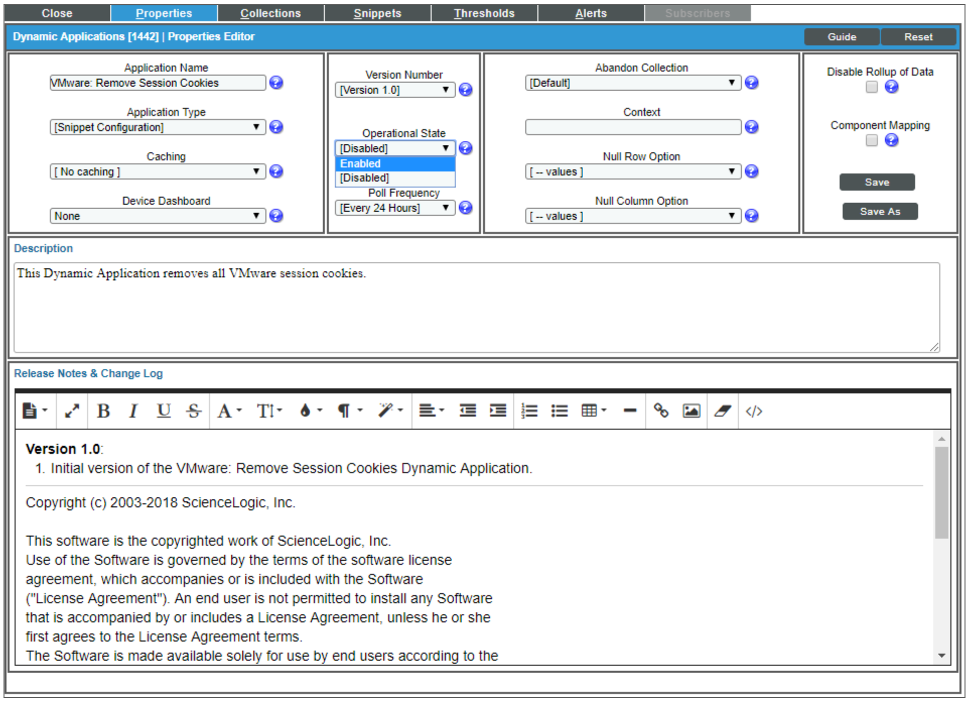
   - ***VMware: VirtualMachine CPU Performance***. No more than 5 minutes.
   - ***VMware: VirtualMachine Datastore Performance***. No more than 5 minutes.
   - ***VMware: VirtualMachine Disk Performance***. No more than 5 minutes.
   - ***VMware: Inventory Cache***. Exactly 1 minute.
   - ***VMware: Datastore Space Performance***. No less than 15 minutes.

Configuring the "VMware: Remove Session Cookies" Dynamic Application

The "VMware: Remove Session Cookies" Dynamic Application allows users to force a new API session to collect new objects.

To execute the Dynamic Application:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
2. Find the "VMware: Remove Session Cookies" Dynamic Application and click on its wrench icon (🔧).
3. In the **Dynamic Applications Properties Editor** page, click the ***Operational State*** drop-down and select *Enabled*.



Dynamic Applications [1442] | Properties Editor

Application Name: VMware: Remove Session Cookies

Application Type: [Snippet Configuration]

Caching: [No caching]

Device Dashboard: None

Version Number: [Version 1.0]

Operational State: [Disabled]
- Enabled
- [Disabled]

Poll Frequency: [Every 24 Hours]

Abandon Collection: [Default]

Context:

Null Row Option: [-- values]

Null Column Option: [-- values]

Disable Rollup of Data ☐

Component Mapping ☐

Description

This Dynamic Application removes all VMware session cookies.

Release Notes & Change Log

Version 1.0:
1. Initial version of the VMware: Remove Session Cookies Dynamic Application.

Copyright (c) 2003-2018 ScienceLogic, Inc.

This software is the copyrighted work of ScienceLogic, Inc.
Use of the Software is governed by the terms of the software license
agreement, which accompanies or is included with the Software
("License Agreement"). An end user is not permitted to install any Software
that is accompanied by or includes a License Agreement, unless he or she
first agrees to the License Agreement terms.
The Software is made available solely for use by end users according to the

4. Align the "VMware: Remove Session Cookies" Dynamic Application to any VMware root device.
5. On the root device, go to the **[Collections]** tab on the **Device Properties** page and run the "VMware: Remove Session Cookies" Dynamic Application you just aligned by clicking the lightning bolt icon (⚡).
6. After running the Dynamic Application, check the session logs. If you get an "Failed to retrieve security token from vSphere SSO server" error, run the Dynamic Application again.
7. When the "VMware: Remove Session Cookies" Dynamic Application has successfully run, change its ***Operational State*** back to *Disabled*.

Relationships with Other Types of Component Devices

In addition to the parent/child relationships between component devices, the following relationships are automatically created by the Dynamic Applications in the *VMware: vSphere Base Pack* PowerPack:

- VMware Virtual Machines and VMware Datastores
- VMware Virtual Machines and VMware Networks
- VMware Virtual Machines and Cisco Cloud Center
- VMware VirtualApps and VMware Networks
- VMware Hosts and VMware Datastores
- VMware Hosts and VMware Networks
- VMware Hosts and VMware Virtual Machines
- VMware Datastore Clusters and VMware Virtual Machines

- VMware Datastore Clusters and VMware Host Clusters
- VMware Datastore Clusters and VMware Hosts

SL1 can also automatically build relationships between VMware component devices and other associated devices. If you discover one or more of the following:

- A Dynatrace host using the Dynamic Applications in the *Dynatrace* PowerPack
- A Cisco UC VOS application using the Dynamic Applications in the *Cisco: UC VOS* PowerPack
- A Cisco CUCM cluster using the Dynamic Applications in the *Cisco: CUCM* PowerPack
- An EMC VNX device using the Dynamic Applications in the *EMC: VNX* PowerPack
- A NetApp device using the Dynamic Applications in the *NetApp Base Pack* PowerPack
- A UCS device using the Dynamic Applications in the *Cisco: UCS* PowerPack

SL1 automatically creates relationships between the following types of component devices, where appropriate:

- Dynatrace hosts and VMware Datastores
- Cisco UC VOS applications and VMware Datastores
- Cisco CUCM clusters and VMware Datastores
- EMC VNX LUNs and VMware Datastores
- NetApp LUNs and VMware Datastores
- VMware Hosts and UCS Service Profiles

Determining Availability for Component Devices

The Dynamic Applications that discover the component devices managed by a vCenter server include collection objects that define the availability status of those component devices.

The following types of component devices are considered unavailable if a vCenter server reports that the power state is off:

- Compute Resource
- Host Server (i.e., ESX and ESXi Servers)
- Virtual Machine

The following types of component devices are considered unavailable if a vCenter server loses its connection to an ESXi hypervisor host server:

- Host Server
- Virtual Machine

The following types of component devices are considered unavailable if a vCenter server does not include information about those components in the appropriate response:

- Distributed Virtual Switch

- Distributed Virtual Portgroup
- Folder
- Network
- Resource Pool

The following types of component devices are considered unavailable based on other conditions:

- ***Datastore***. A datastore is considered unavailable if it is not accessible. A datastore is not accessible if no hosts have successfully mounted the datastore volume.
- ***Cluster***. A cluster is considered unavailable if no hosts are associated with the cluster or all hosts associated with the cluster are powered off.

When a VMware device is shut down, an event is created to alert the user that the device is unavailable. If you turn off VMware devices intentionally, you can suppress these availability events.

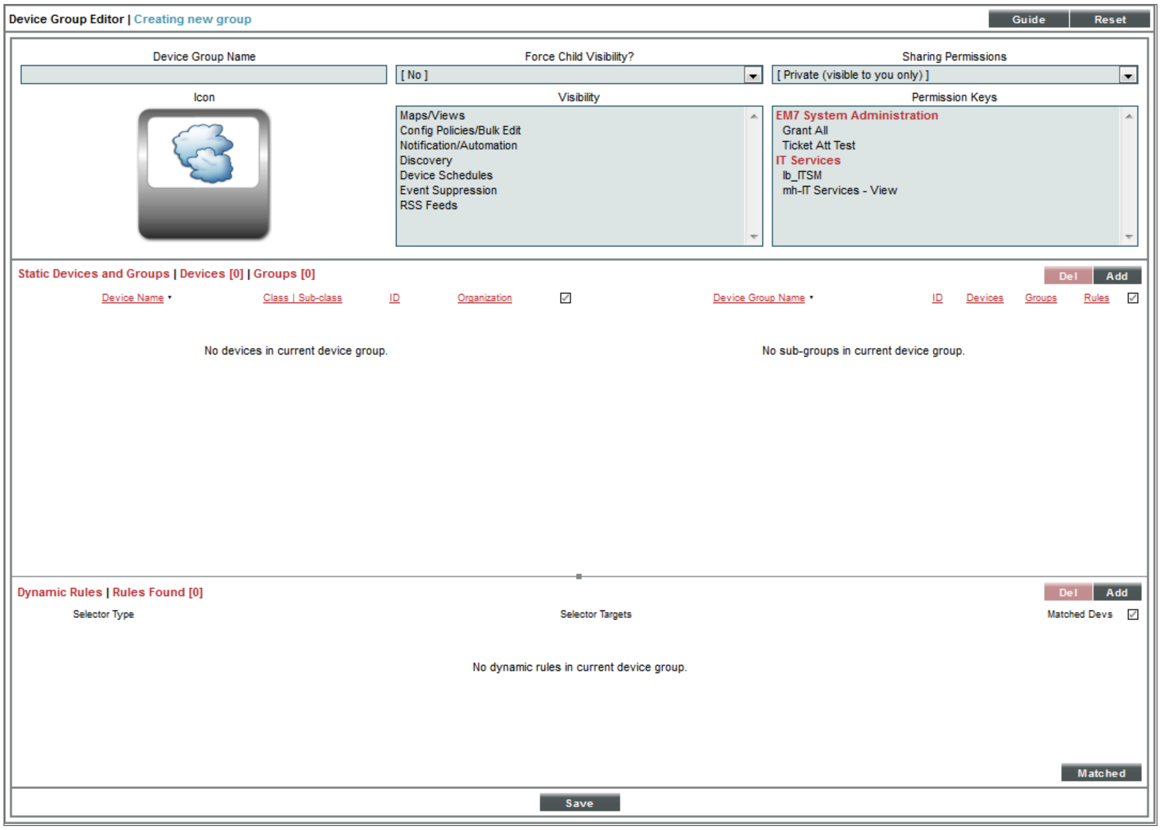
To suppress these events:

- Create a device group that contains the VMware devices for which you want to suppress availability events.
- Suppress that device group in the relevant Event Policies.

To create the device group:

1. Go to the **Device Groups** page (Devices > Device Groups or Registry > Devices > Device Groups in the SL1 classic user interface).

2. Click the **[Create]** button. The **Device Group Editor** page appears:



Device Group Editor | Creating new group

Device Group Name:

Force Child Visibility?: [No]

Sharing Permissions: [Private (visible to you only)]

Visibility: Maps/Views, Config Policies/Bulk Edit, Notification/Automation, Discovery, Device Schedules, Event Suppression, RSS Feeds

Permission Keys: EM7 System Administration (Grant All, Ticket Att Test); IT Services (lb_ITSM, mh-IT Services - View)

Static Devices and Groups | Devices [0] | Groups [0]

No devices in current device group.

No sub-groups in current device group.

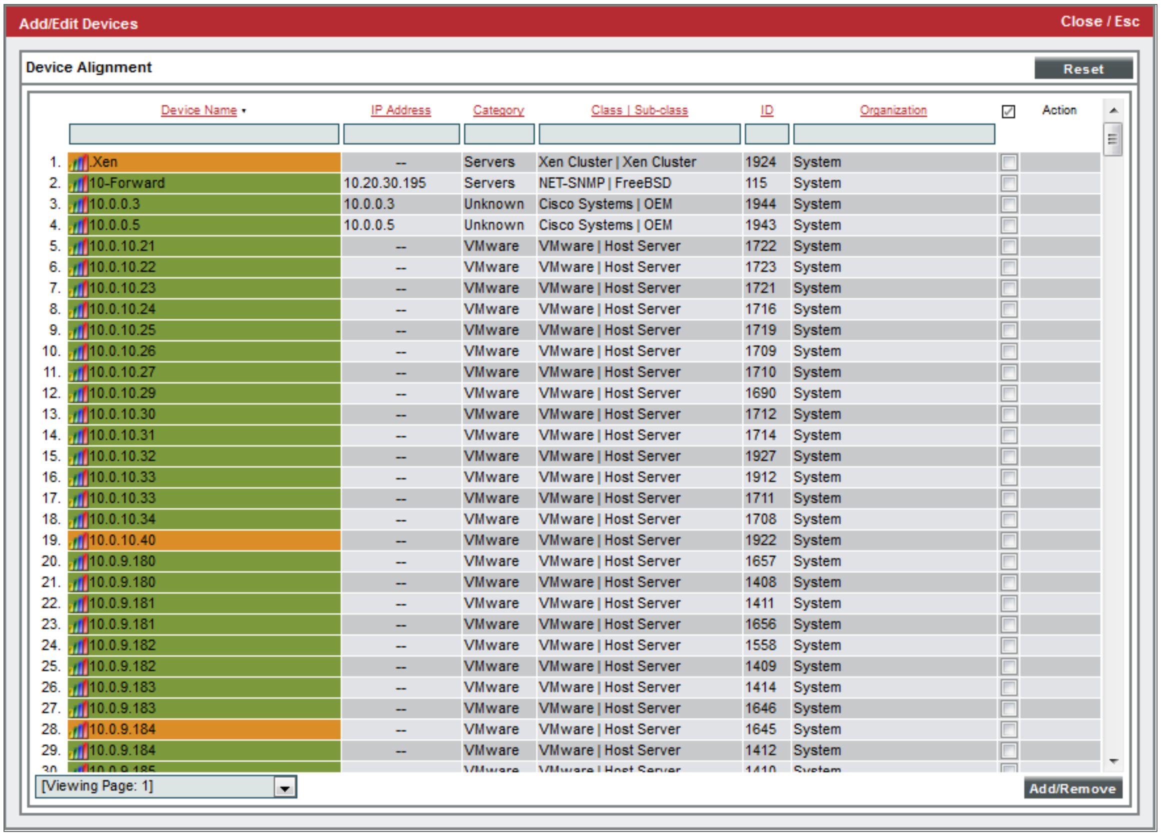
Dynamic Rules | Rules Found [0]

No dynamic rules in current device group.

3. Enter values in the following fields:

- ***Device Group Name***. In this field you can enter a customized Device Group Name. For example, "Event Suppressed VMs".
- ***Visibility***. Select *Event Suppression*.

4. If you want to suppress one or a few individual devices, click the **[Add]** button under the **Static Devices and Groups** pane and select *Add Devices*. The **Device Alignment** modal page appears:



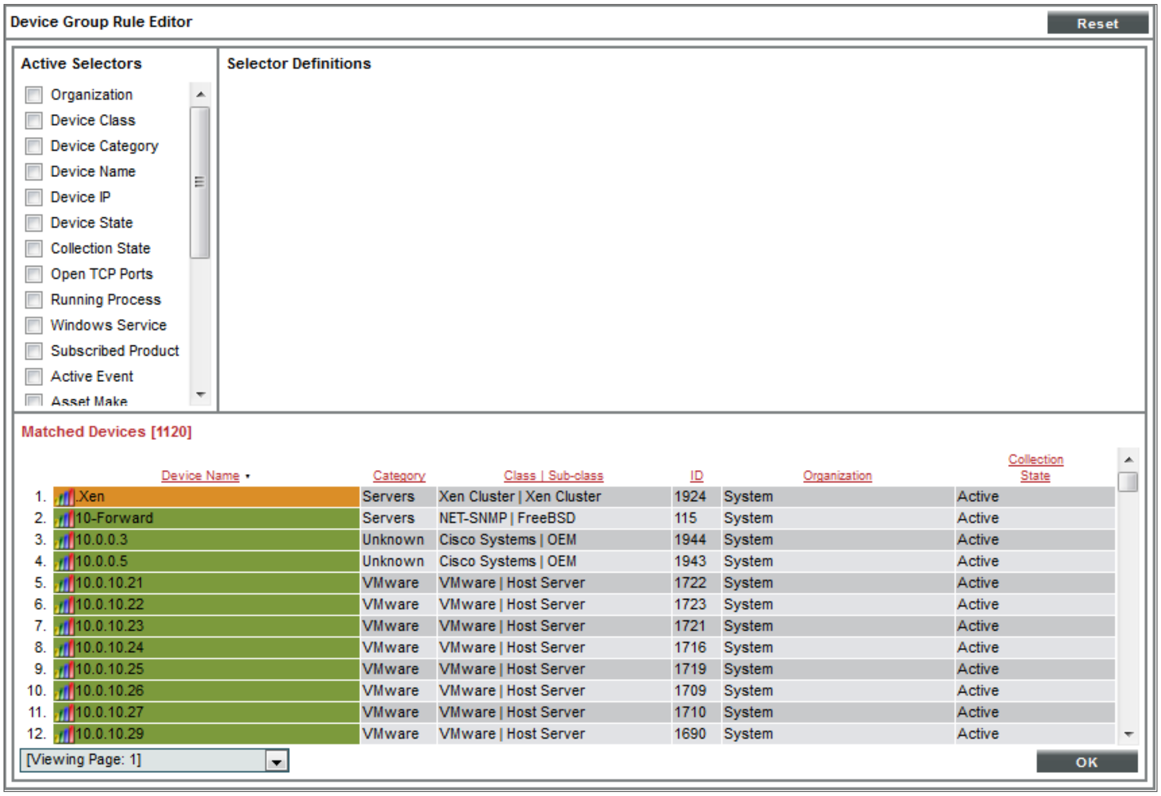
	Device Name ▾	IP Address	Category	Class | Sub-class	ID	Organization	☑	Action
1.	.Xen	--	Servers	Xen Cluster | Xen Cluster	1924	System	□	
2.	10-Forward	10.20.30.195	Servers	NET-SNMP | FreeBSD	115	System	□	
3.	10.0.0.3	10.0.0.3	Unknown	Cisco Systems | OEM	1944	System	□	
4.	10.0.0.5	10.0.0.5	Unknown	Cisco Systems | OEM	1943	System	□	
5.	10.0.10.21	--	VMware	VMware | Host Server	1722	System	□	
6.	10.0.10.22	--	VMware	VMware | Host Server	1723	System	□	
7.	10.0.10.23	--	VMware	VMware | Host Server	1721	System	□	
8.	10.0.10.24	--	VMware	VMware | Host Server	1716	System	□	
9.	10.0.10.25	--	VMware	VMware | Host Server	1719	System	□	
10.	10.0.10.26	--	VMware	VMware | Host Server	1709	System	□	
11.	10.0.10.27	--	VMware	VMware | Host Server	1710	System	□	
12.	10.0.10.29	--	VMware	VMware | Host Server	1690	System	□	
13.	10.0.10.30	--	VMware	VMware | Host Server	1712	System	□	
14.	10.0.10.31	--	VMware	VMware | Host Server	1714	System	□	
15.	10.0.10.32	--	VMware	VMware | Host Server	1927	System	□	
16.	10.0.10.33	--	VMware	VMware | Host Server	1912	System	□	
17.	10.0.10.33	--	VMware	VMware | Host Server	1711	System	□	
18.	10.0.10.34	--	VMware	VMware | Host Server	1708	System	□	
19.	10.0.10.40	--	VMware	VMware | Host Server	1922	System	□	
20.	10.0.9.180	--	VMware	VMware | Host Server	1657	System	□	
21.	10.0.9.180	--	VMware	VMware | Host Server	1408	System	□	
22.	10.0.9.181	--	VMware	VMware | Host Server	1411	System	□	
23.	10.0.9.181	--	VMware	VMware | Host Server	1656	System	□	
24.	10.0.9.182	--	VMware	VMware | Host Server	1558	System	□	
25.	10.0.9.182	--	VMware	VMware | Host Server	1409	System	□	
26.	10.0.9.183	--	VMware	VMware | Host Server	1414	System	□	
27.	10.0.9.183	--	VMware	VMware | Host Server	1646	System	□	
28.	10.0.9.184	--	VMware	VMware | Host Server	1645	System	□	
29.	10.0.9.184	--	VMware	VMware | Host Server	1412	System	□	
30.	10.0.9.185		VMware	VMware | Host Server	1410	System	□	

5. In the **Device Alignment** modal page, perform a search in the ***Class | Sub-class*** column for "Virtual Machine" to bring up the available VMware devices.

6. Find the device(s) for which you want to suppress availability events and select their checkbox (☑).

7. Click the **[Add/Remove]** button to add the device(s).

8. To add all VM devices to the device group, click the **[Add]** button in the **Dynamic Rules** pane of the **Device Group Editor** page. The **Device Group Rule Editor** page appears:



Active Selectors

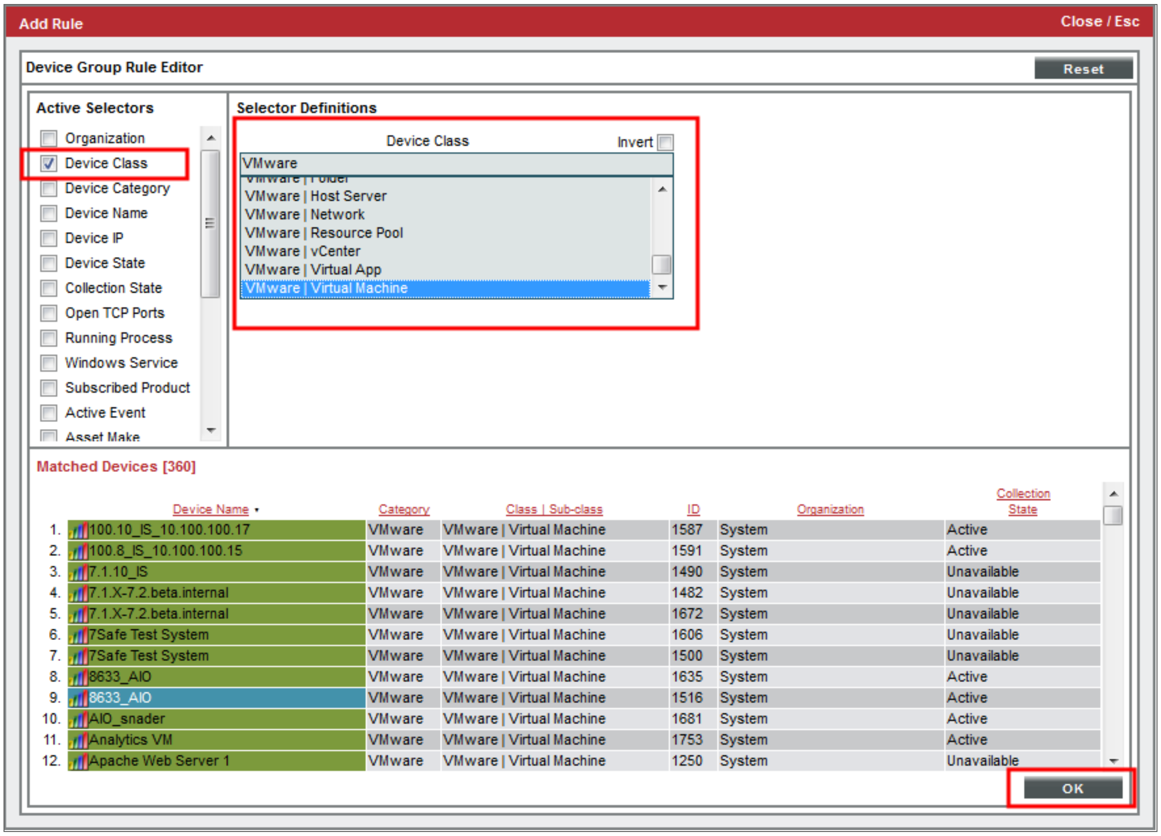
- □ Organization
- □ Device Class
- □ Device Category
- □ Device Name
- □ Device IP
- □ Device State
- □ Collection State
- □ Open TCP Ports
- □ Running Process
- □ Windows Service
- □ Subscribed Product
- □ Active Event
- □ Asset Make

Matched Devices [1120]

	Device Name	Category	Class | Sub-class	ID	Organization	Collection State
1.	.Xen	Servers	Xen Cluster | Xen Cluster	1924	System	Active
2.	10-Forward	Servers	NET-SNMP | FreeBSD	115	System	Active
3.	10.0.0.3	Unknown	Cisco Systems | OEM	1944	System	Active
4.	10.0.0.5	Unknown	Cisco Systems | OEM	1943	System	Active
5.	10.0.10.21	VMware	VMware | Host Server	1722	System	Active
6.	10.0.10.22	VMware	VMware | Host Server	1723	System	Active
7.	10.0.10.23	VMware	VMware | Host Server	1721	System	Active
8.	10.0.10.24	VMware	VMware | Host Server	1716	System	Active
9.	10.0.10.25	VMware	VMware | Host Server	1719	System	Active
10.	10.0.10.26	VMware	VMware | Host Server	1709	System	Active
11.	10.0.10.27	VMware	VMware | Host Server	1710	System	Active
12.	10.0.10.29	VMware	VMware | Host Server	1690	System	Active

9. In the **Device Group Rule Editor** page, select the checkbox (☑) for ***Device Class*** in the **Active Selectors** pane.

10. In the **Selector Definitions** pane, the ***Device Class*** field appears. Perform a search for "VMware" in the ***Device Class*** field, and select *VMware | Virtual Machine*. All virtual machines will appear in the **Matched Devices** pane:



Active Selectors

- □ Organization
- ☑ Device Class
- □ Device Category
- □ Device Name
- □ Device IP
- □ Device State
- □ Collection State
- □ Open TCP Ports
- □ Running Process
- □ Windows Service
- □ Subscribed Product
- □ Active Event
- □ Asset Make

Selector Definitions

Device Class: VMware — Invert □

- VMware | Folder
- VMware | Host Server
- VMware | Network
- VMware | Resource Pool
- VMware | vCenter
- VMware | Virtual App
- VMware | Virtual Machine

Matched Devices [360]

	Device Name	Category	Class | Sub-class	ID	Organization	Collection State
1.	100.10_IS_10.100.100.17	VMware	VMware | Virtual Machine	1587	System	Active
2.	100.8_IS_10.100.100.15	VMware	VMware | Virtual Machine	1591	System	Active
3.	7.1.10_IS	VMware	VMware | Virtual Machine	1490	System	Unavailable
4.	7.1.X-7.2.beta.internal	VMware	VMware | Virtual Machine	1482	System	Unavailable
5.	7.1.X-7.2.beta.internal	VMware	VMware | Virtual Machine	1672	System	Unavailable
6.	7Safe Test System	VMware	VMware | Virtual Machine	1606	System	Unavailable
7.	7Safe Test System	VMware	VMware | Virtual Machine	1500	System	Unavailable
8.	8633_AIO	VMware	VMware | Virtual Machine	1635	System	Active
9.	8633_AIO	VMware	VMware | Virtual Machine	1516	System	Active
10.	AIO_snader	VMware	VMware | Virtual Machine	1681	System	Active
11.	Analytics VM	VMware	VMware | Virtual Machine	1753	System	Active
12.	Apache Web Server 1	VMware	VMware | Virtual Machine	1250	System	Unavailable

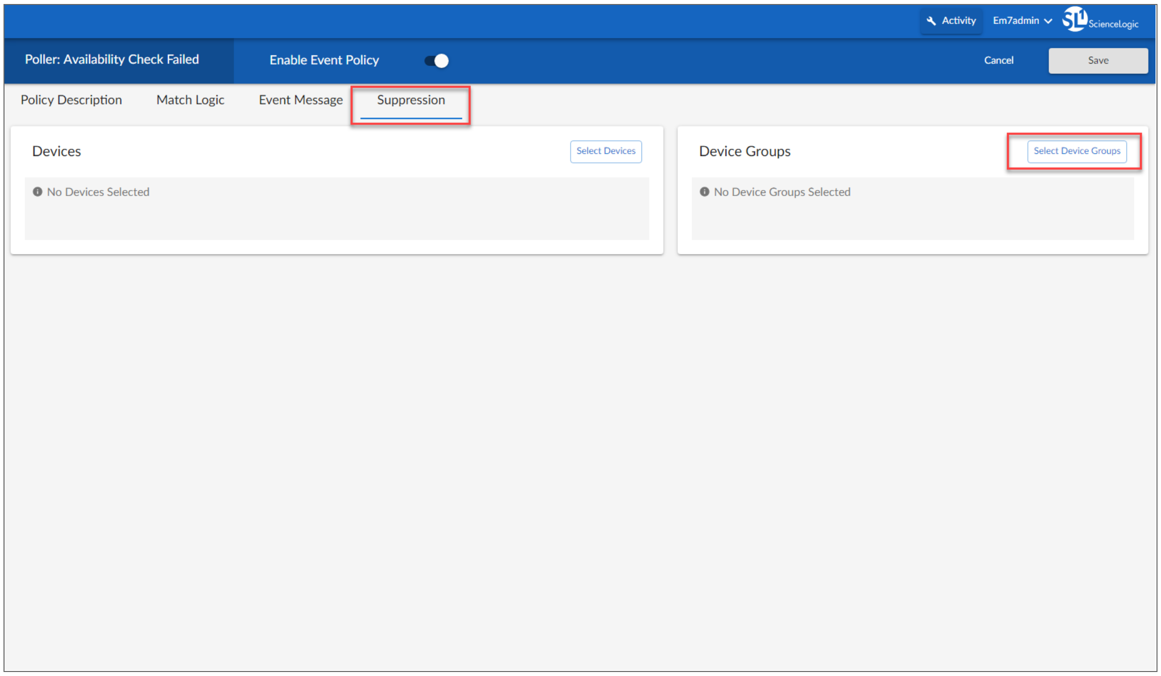
11. Click the **[OK]** button. The Device Class will appear in the **Dynamic Rules** pane.

Next, you need to suppress two Event Policies for this Device Group.

- *Suppressing the Event Policies in SL1*
- *Suppressing the Event Policies in the SL1 classic user interface*

To suppress two Event Policies for this Device Group:

1. Go to the **Event Policies** page (Events > Event Policies).
2. Perform a search for "Availability".
3. Locate the **Poller: Availability Check Failed** policy, click the actions icon (···) and select ***Edit***. The **Policy Description** page appears. Click the **[Suppression]** tab.

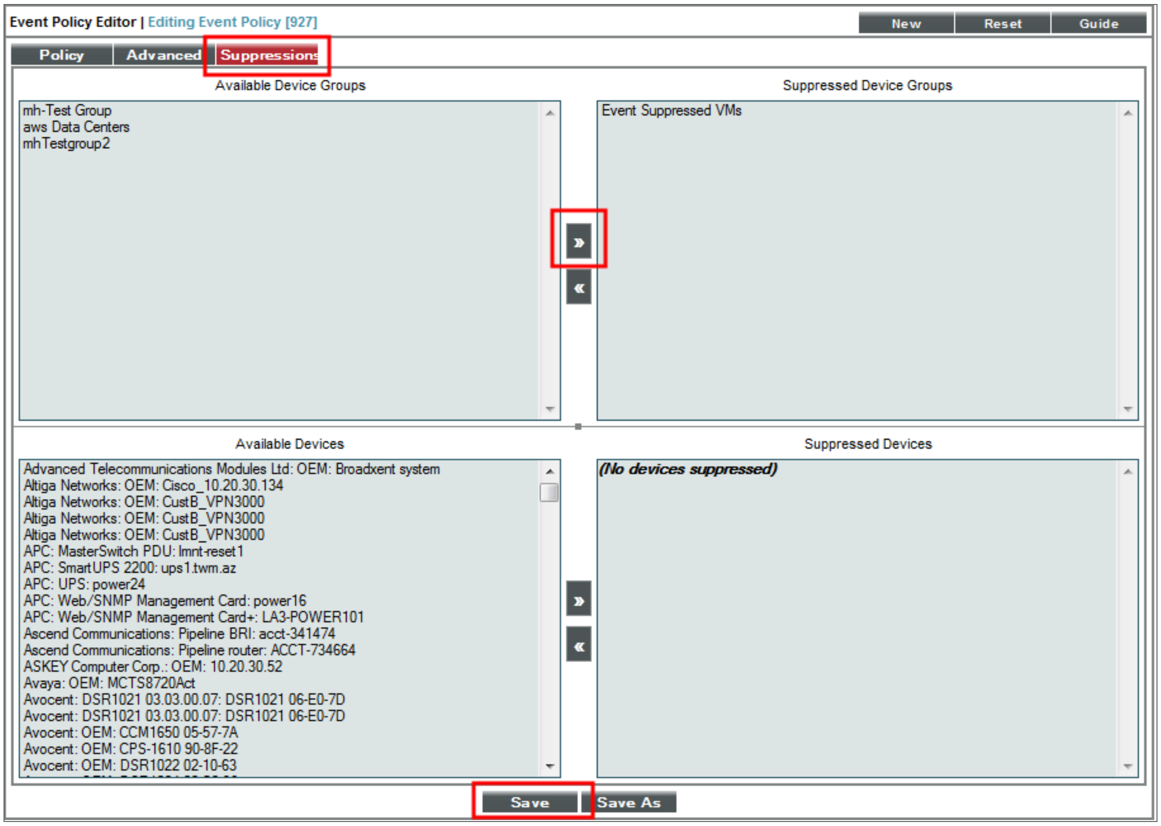


4. In the **Device Groups** pane, click the **[Select Device Groups]** button.
5. In the **Available Device Groups** window, locate the device group you created and select its checkbox. Click the **[Select]** button. The selected device group now appears in the **Device Groups** pane.
6. Click the **[Save]** button.
7. Repeat these steps for the **Poller: Availability Healthy** event policy to suppress events that will occur when a VMware device is turned back on again.

To suppress the two Event Policies in the SL1 classic user interface:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. Perform a search in the ***Event Policy Name*** column for "Availability".

3. Click the wrench icon ( ) for the **Poller: Availability Check Failed** policy. The **Event Policy Editor** page appears:



Event Policy Editor | Editing Event Policy [927]

Available Device Groups

mh-Test Group
aws Data Centers
mhTestgroup2

Suppressed Device Groups

Event Suppressed VMs

Available Devices

Advanced Telecommunications Modules Ltd: OEM: Broadxent system
Altiga Networks: OEM: Cisco_10.20.30.134
Altiga Networks: OEM: CustB_VPN3000
Altiga Networks: OEM: CustB_VPN3000
Altiga Networks: OEM: CustB_VPN3000
APC: MasterSwitch PDU: lmnt-reset1
APC: SmartUPS 2200: ups1.twm.az
APC: UPS: power24
APC: Web/SNMP Management Card: power16
APC: Web/SNMP Management Card+: LA3-POWER101
Ascend Communications: Pipeline BRI: acct-341474
Ascend Communications: Pipeline router: ACCT-734664
ASKEY Computer Corp.: OEM: 10.20.30.52
Avaya: OEM: MCTS8720Act
Avocent: DSR1021 03.03.00.07: DSR1021 06-E0-7D
Avocent: DSR1021 03.03.00.07: DSR1021 06-E0-7D
Avocent: OEM: CCM1650 05-57-7A
Avocent: OEM: CPS-1610 90-8F-22
Avocent: OEM: DSR1022 02-10-63

Suppressed Devices

(No devices suppressed)

4. Click the **[Suppressions]** tab in the **Event Policy Editor** page.
5. In the ***Available Device Groups*** field, select the device group you created. In this example, you would select *Event Suppressed VMs*.
6. Click the right arrow button, **[>>]**, and the device group moves to the ***Suppressed Device Groups*** field.
7. Click the **[Save]** button.
8. Repeat these steps for the **Poller: Availability Healthy** event policy to suppress events that will occur when a VMware device is turned back on again.

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