Monitoring Video Devices

SL1 version 12.3.5

Table of Contents

Introduction 6
Which Video Devices are Covered in this Manual? 6
Video Device PowerPacks 7
Monitoring Cisco Tandberg C Series Codecs 8
Configuring Cisco Tandberg C Series Codecs for Monitoring by SL1 8
Creating an SNMP Credential 13
Creating an SNMP Credential in the SL1 Classic User Interface 14
Configuring SOAP/XML Credentials 14
Configuring SOAP/XML Credentials in the SL1 Classic User Interface 16
Dynamic Applications for Cisco Tandberg C Series Codecs 16
Monitoring Cisco Tandberg MXP Series Endpoints 19
Configuring Cisco Tandberg MXP Series Endpoints for Monitoring by SL1 19
Creating an SNMP Credential 22
Configuring SOAP/XML Credentials 22
Modifying the Credential Templates 23
Dynamic Applications for Cisco Tandberg MXP Series Endpoints 23
Monitoring Cisco CE Series Endpoints 26
Configuring Cisco CE Series Endpoints for Monitoring by SL1 26
Configuring SNMP Settings 26
Configuring the HTTP Request Password 28
Creating an SNMP Credential 29
Creating an SNMP Credential in the SL1 Classic User Interface 30
Configuring SOAP/XML Credentials 31
Modifying the SOAP/XML Credential Templates 31
Modifying the SOAP/XML Credential Templates in the SL1 ADS Classic User Interface 32
Discovering Cisco CE Series Endpoints 33
Discovering CE Series Devices 34
Discovering CE Series Devices in the SL1 Classic User Interface 36
Monitoring Cisco TelePresence Endpoints 37
Configuring TelePresence Endpoints for Monitoring by SL1 37
Creating an SNMP Credential 40

Monitoring Cisco TelePresence Conductor 42
Prerequisites 42
Monitoring Cluster Configurations vs. Non-Cluster Configurations 43
Creating Credentials 43
Creating a SOAP/XML Credential 43
Creating SOAP/XML Credential in the SL1 Classic User Interface 44
Creating an SNMP Credential 45
Creating an SNMP Credential in the SL1 Classic User Interface 46
Creating and Discovering Virtual Devices 46
Discovering IP Devices 48
Viewing Cisco TelePresence Conductor Devices 50
Monitoring LifeSize Endpoints 53
Configuring LifeSize Endpoints for Monitoring by SL1 53
Creating an SNMP Credential for a LifeSize Endpoint 54
Monitoring Poly HDX and VSX Series Endpoints 56
Configuring Poly Endpoints for Monitoring by SL1 56
Creating an SNMP Credential 59
Creating an SNMPv2 Credential 59
Creating an SNMPv2 Credential in the Classic User Interface 61
Creating an SNMPv3 Credential 61
Creating an SNMP v3 Credential in the Classic User Interface 64
Performing Bulk Retrieval Using SNMPv3 64
Configuring SOAP/XML Credentials 65
Creating SOAP/XML Credentials 65
Creating SOAP/XML Credentials in the Classic User Interface 68
Dynamic Applications for Poly Endpoints 69
Monitoring Tandberg Infrastructure 71
Tandberg Infrastructure Support 71
Creating a Credential for Tandberg Infrastructure Dynamic Applications 74
Creating a Credential for Tandberg Infrastructure in the SL1 Classic User Interface 74
Creating a Credential for TelePresence Content Server 75
Creating a Credential for TelePresence Content Server in the SL1 Classic User Interface 76

Video Communication Server 76
Dynamic Applications for VCS Devices 77
Creating a Credential for VCS Devices 78
Creating a Credential for VCS Devices in the SL1 Classic User Interface 79
Discovering VCS Devices 80
Manually Aligning Dynamic Applications with VCS Devices 81
TelePresence Server 83
Creating a Credential for a TelePresence Server 83
Creating a Credential for a TelePresence Server in the SL1 Classic User Interface 84
Discovering Devices with the TelePresence Server 85
Manually Aligning the Dynamic Applications with the TelePresence Server 86
TelePresence Control Unit 88
Creating a Credential for a TelePresence Control Unit 88
Creating a Credential for a TelePresence Control Unit in the SL1 Classic User Interface 89
Discovering TelePresence Control Unit Devices 90
Manually Aligning the Dynamic Applications with the TelePresence Server 91
Reports for Video Devices 93
TelePresence Inventory Report 94
Video Calls by Device Group, Call Type, and Bandwidth Report 94
Video Endpoint Availability Chart Report 96
Video Endpoint Availability Table Report 98
Video Endpoint Avg Jitter Column Chart Report 100
Video Endpoint Avg Jitter Line Chart Report 102
Video Endpoint Avg Jitter Table Report 105
Video Endpoint Call Detail Records Report 106
Video Endpoint Detailed Asset Inventory Report 109
Video Endpoint Detailed Jitter Line Chart Report 110
Video Endpoint Detailed Packet Loss Line Chart Report 113
Video Endpoint Packet Loss Column Chart Report 115
Video Endpoint Packet Loss Line Chart Report 117
Video Endpoint Packet Loss Table Report 119
Video Endpoint Performance Detail Report 120

Video Endpoint Unavailability Chart Report 122
Video Endpoint Unavailability Table Report 124
Video Usage Report 126
Video Usage Chart Report 127

Chapter 1

Introduction

Overview

This manual describes how to configure video devices for monitoring by SL1. It also includes a list of default custom reports and widgets that are specifically designed to display data collected from video devices.

The following sections describe the types of video devices that SL1 can monitor:

This chapter covers the following topics:

Which Video Devices are Covered in this Manual? 6

Video Device PowerPacks 7

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.

Which Video Devices are Covered in this Manual?

This manual describes how to configure the following types of video devices for monitoring:

- Cisco C Series endpoints
- Cisco CE Series endpoints
- Cisco MXP Series endpoints
- Cisco TelePresence endpoints

- Cisco TelePresence Conductor arrays
- Cisco Video Infrastructure devices
- LifeSize endpoints
- Poly HDX Series endpoints
- Polycom Group Series endpoints
- Poly VSX Series endpoints

Video Device PowerPacks

This manual describes content from the following PowerPack versions:

- Cisco: TelePresence Conductor, version 1.0
- Cisco: TelePresence: Endpoints, version 102
- Cisco: TelePresence: Traps, version 100
- Cisco: Video Endpoint, version 107
- LifeSize Endpoint, version 7.5.4
- Poly Endpoint, version 103
- Polycom Infrastructure, version 100
- Tandberg: Infrastructure, version 108
- Video Reports, version 100

Chapter 2

Monitoring Cisco Tandberg C Series Codecs

Overview

The following sections describe how to configure Cisco Tandberg C Series devices for monitoring by SL1 using the *Cisco: Video Endpoint* PowerPack:

This chapter covers the following topics:

Configuring Cisco Tandberg C Series Codecs for Monitoring by SL1 8

Creating an SNMP Credential 13

Configuring SOAP/XML Credentials 14

Dynamic Applications for Cisco Tandberg C Series Codecs 16

Configuring Cisco Tandberg C Series Codecs for Monitoring by SL1

SL1 uses two protocols for monitoring Cisco Tandberg C Series Codecs: SNMP and HTTP. This section will describe how to configure a Cisco Tandberg C Series Codec to respond to both protocols and how to configure a user account that the ScienceLogic platform will use to connect to the Cisco Tandberg C Series Codec.

NOTE: These instructions assume that the Cisco Tandberg C Series Codec has been assigned an IP address and is visible to a Data Collector on the network.

To configure a Cisco Tandberg C Series Codec for monitoring by SL1, perform the following steps:

1. Connect to the Cisco Tandberg C Series Codec using an SSH client as a user that has ADMIN permissions. Cisco Tandberg C Series Codecs have SSH enabled by default. The default username is "admin", which does not have a password by default.
2. Execute the following command to enable SNMP:

```
xConfiguration NetworkServices SNMP Mode: ReadOnly
```

NOTE: The default monitoring content for Cisco Tandberg supplied by ScienceLogic does not require SNMP Write access. However, if you are planning to perform SNMP Write operations on this Cisco Tandberg C Series Codec, enter "ReadWrite" instead of "ReadOnly" in the above command.

3. Execute the following command to change the SNMP community string, substituting *community_string* with the community string you want to assign to this device:

```
xConfiguration NetworkServices SNMP CommunityName: community_string
```

When you configure an SNMP credential for this Cisco Tandberg C Series Codec in SL1, you will enter the community string that you just configured in the ***SNMP Community (Read-Only)*** field.

4. Execute the following command to configure the device to send SNMP trap messages to SL1, substituting *em7_ip_address* with the IP address of the Message Collector or Data Collector that will collect SNMP trap messages from the device:

```
xConfiguration NetworkServices SNMP Host 1 Address: em7_ip_address
```

NOTE: If the device is already configured to send SNMP traps to another IP address and you want to retain those settings, replace "Host 1" with either "Host 2" or "Host 3" in the above command.

5. Optionally, you can execute the following two commands to change the SNMP system contact and SNMP system location. Substitute *system_contact* and *system_location* with the system contact and system location you want to assign to this device:

```
xConfiguration NetworkServices SNMP SystemContact: system_contact
```

```
xConfiguration NetworkServices SNMP SystemLocation: system_location
```

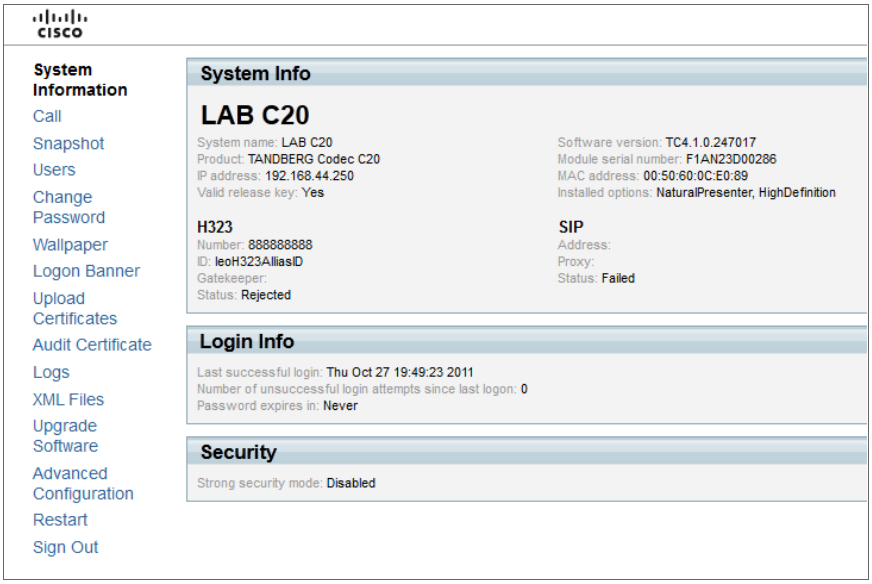
6. Execute the following command to enable the HTTP service:

```
xConfiguration NetworkServices HTTP Mode: On
```

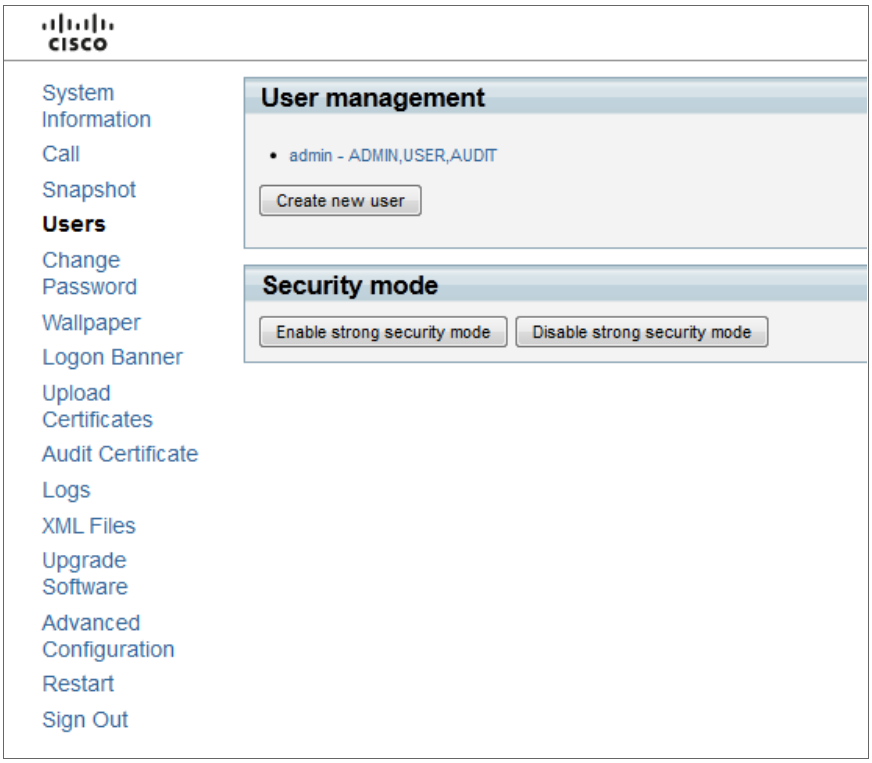
NOTE: By default, SL1 uses regular HTTP to connect to Cisco Tandberg C Series Codecs. If you want to use HTTPS instead of regular HTTP, enter "HTTPS" instead of "HTTP" in the above command. When you follow the instructions for configuring a SOAP/XML credential for this device, you must perform the steps that describe how to change the credential to use HTTPS instead of regular HTTP.

7. In a browser window, go to the IP address of the Cisco Tandberg C Series Codec. A login screen appears:

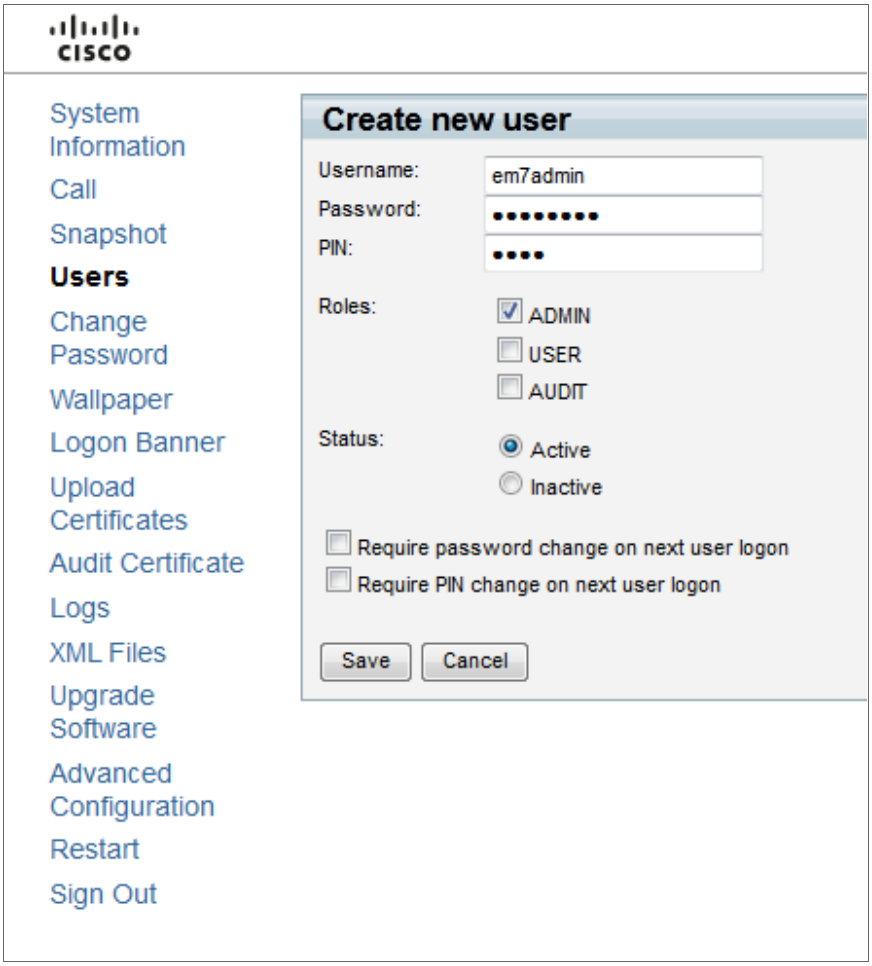
8. Log in as a user that has ADMIN permissions. The **System Information** page appears:



9. In the left navigation bar, click *Users*. The **User Management** page appears:



10. Click the **[Create new user]** button. The **Create New User** page appears:



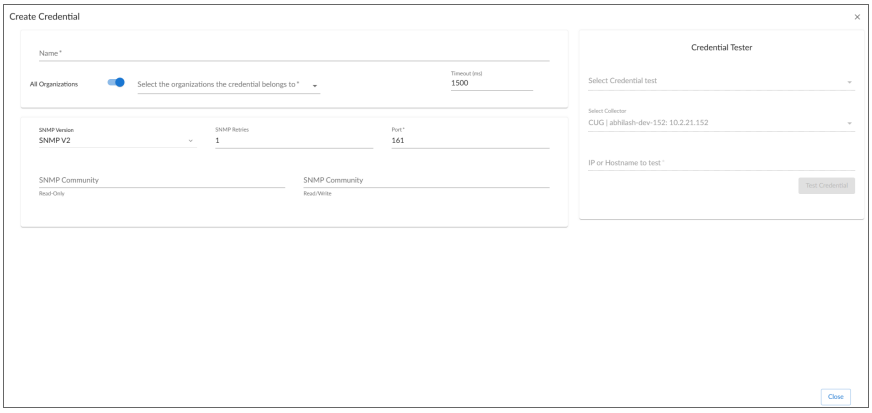
11. Supply a value in the following fields:
    - ***Username***. Type a username for the new user. When you configure a SOAP/XML credential for this device in SL1, you will type this value in the ***HTTP Auth User*** field.
    - ***Password***. Type a password for the new user. When you configure a SOAP/XML credential for this device in SL1, you will type this value in the ***HTTP Auth Password*** field.
    - ***PIN***. Type any valid PIN in this field. SL1 does not use this value.
    - ***Roles***. Select the *ADMIN* checkbox.
    - ***Status***. Select the *Active* radio button.
    - ***Require password change on next user logon***. Uncheck this checkbox.
    - ***Require PIN change on next user logon***. Uncheck this checkbox.
12. Click the **[Save]** button to save the new user.

Creating an SNMP Credential

To monitor Cisco Tandberg C Series Codecs in SL1, you will need to create an SNMP Credential for each Codec.

To create an SNMP Credential for a Cisco Tandberg C Series Codec, perform the following steps in SL1:

1. Go to the **Credentials** page (Manage > Credentials).
2. Click the **[Create New]** button and select *Create SNMP Credential* from the drop-down list that appears.
3. Complete the following fields:



- ***Name***. Enter a new name for the credential. This field is required.
- ***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 ***Select the organizations the credential belongs to*** drop-down field to align the credential with those specific organizations.
- ***Timeout (ms)***. Enter the time, in milliseconds, after which SL1 will stop trying to communicate with the Cisco Tandberg C Series Codec device. The default value is *1500*. This field is required.
- ***SNMP Version***. Select *SNMP V2* from the drop-down list.
- ***SNMP Retries***. Keep the default. The default value is "1".
- ***Port***. Keep the default. The default port is "161".
- ***SNMP Community (Read Only)***. Enter the community string for the Cisco Tandberg C Series Codec voice mailbox you want to monitor.
- ***SNMP Community (Read/Write)***. Optional. Enter the community string for the Cisco Tandberg C Series Codec to grant Read/Write permissions.
- Click **[Close]**.

Creating an SNMP Credential in the SL1 Classic User Interface

To monitor Cisco Tandberg C Series Codecs in the SL1 classic user inferface, you will need to create an SNMP Credential for each Codec.

To create an SNMP Credential for a Cisco Tandberg C Series Codec, perform the following steps in SL1:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click **[Actions]**, and then select *Create SNMP Credential*. The **Credential Editor** page appears.
3. Supply values in the following fields:
    - ***Profile Name***. Type a name for the credential.
    - ***SNMP Version***. Select *SNMP V2*.
    - ***SNMP Community (Read-Only)***. Type the SNMP community string you configured on the Cisco Tandberg C Series Codec.

NOTE: You can optionally change the values in the ***Timeout (ms)*** and ***Retries*** fields.

4. Click **[Save]**.
5. When you configure a discovery session that includes the IP address of the Cisco Tandberg C Series Codec, select the SNMP credential you created in the ***SNMP Credentials*** field. For more information about discovery in SL1, see the ***Discovery and Credentials*** manual.

Configuring SOAP/XML Credentials

To use the Dynamic Applications in the "Cisco: Video Endpoint" PowerPack in SL1, you must configure three SOAP/XML credentials for your Cisco Tandberg C Series Codec. The three credentials are:

- Tandberg Endpoint - Configuration
- Tandberg Endpoint - History
- Tandberg Endpoint - Status

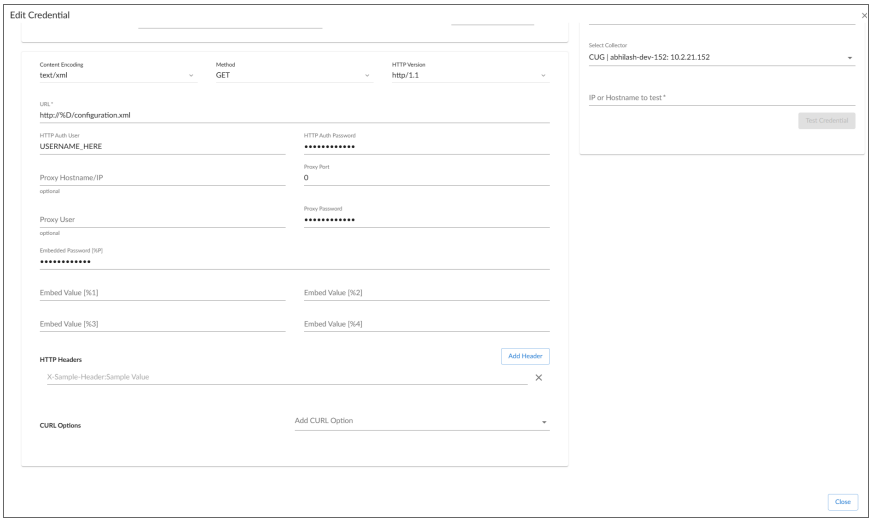
These credentials enable SL1 to collect configuration and performance data along with call detail records using unique URL, username, and password combinations.

If you have multiple Cisco Tandberg C Series Codecs, you will need one set of credentials for each unique username and password. For example, if you have configured three Cisco Tandberg C Series Codecs with the same username and password, you need only one set of credentials.

The "Cisco: Video Endpoint" PowerPack includes a template for each SOAP/XML credential that you can edit for use with your Cisco Tandberg C Series devices.

To create a SOAP/XML credential:

1. Go to the **Credentials** page (Manage > Credentials).
2. Locate the "Tandberg Endpoint-Credential", then click its **[Actions]** icon (⋮) and select *Duplicate* from the drop-down field. The "Tandberg Endpoint-Credential copy" credential appears.
3. Click the **[Action]** icon (⋮) for the "Tandberg Endpoint-Credential copy" credential, then select *Edit*. The **Edit Credential** page appears.



4. Enter values in the following fields:
    - ***Name***. Enter a new name for the credential. This field is required.
    - ***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 ***Select the organizations the credential belongs to*** drop-down field to align the credential with those specific organizations.
    - ***Timeout***. Enter the time, in milliseconds, after which SL1 will stop trying to communicate with the Video Endpoint device. The default value is *10000*. This field is required.
    - ***URL***. Keep the default URL as "http://%D/configuration.xml".
    - ***HTTP Auth User***. Enter the Video Endpoint username associated with the administrator account.
    - ***HTTP Auth Password***. Enter the password associated with the Video Endpoint administrator account.
    - ***Embedded Password [%P]***. Enter the embedded password associated with the Video Endpoint administrator account.
    - ***Embed Value [%1]***. Keep the default.
5. Click **[Save & Close]**.
6. Repeat steps 2 - 5 for the "Tandberg Endpoint - History" and "Tandberg Endpoint - Status" credentials.

Configuring SOAP/XML Credentials in the SL1 Classic User Interface

To use the Dynamic Applications in the "Cisco: Video Endpoint" PowerPack in SL1, you must configure three SOAP/XML credentials for your Cisco Tandberg C Series Codec. The three credentials are:

- Tandberg Endpoint - Configuration
- Tandberg Endpoint - History
- Tandberg Endpoint - Status

These credentials enable SL1 to collect configuration and performance data along with call detail records using unique URL, username, and password combinations.

If you have multiple Cisco Tandberg C Series Codecs, you will need one set of credentials for each unique username and password. For example, if you have configured three Cisco Tandberg C Series Codecs with the same username and password, you need only one set of credentials.

The "Cisco: Video Endpoint" PowerPack includes a template for each SOAP/XML credential that you can edit for use with your Cisco Tandberg C Series devices.

To configure these credentials in the classic user interface:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the wrench icon ( ) for the "Tandberg Endpoint - Configuration" credential. The **Credential Editor** modal window appears.
3. In the ***Profile Name*** field, type a new name for the credential.
4. In the ***HTTP Auth User*** field, type the username of the user you configured on your Cisco Tandberg C Series Codec.
5. In the ***HTTP Auth Password*** field, type the password for the username you entered in the ***HTTP Auth User*** field.
6. Click the **[Save As]** button.
7. Repeat steps 2 - 6 for the "Tandberg Endpoint - History" and "Tandberg Endpoint - Status" credentials.

Dynamic Applications for Cisco Tandberg C Series Codecs

The "Cisco: Video Endpoint" PowerPack contains nine Dynamic Applications that can be used to monitor Cisco Tandberg C Series Codecs. Some of the Dynamic Applications for Cisco Tandberg C Series Codecs use the caching feature:

- Two Dynamic Applications are used only to collect and cache data from Cisco Tandberg C Series Codecs.
- Six Dynamic Applications use the cached data. For these six Dynamic Applications to display data, the Dynamic Applications that collect and cache data must be aligned to the same device.
- One Dynamic Application for Cisco Tandberg C Series Codecs does not use the caching feature.

The Dynamic Applications in the "Cisco: Video Endpoint" PowerPack include discovery objects. If you discover your Cisco Tandberg C Series Codec as an SNMP device and include all of the SOAP/XML credentials you

configured for your Cisco Tandberg C Series Codec in the ***Other Credentials*** field in the **Discovery Session Editor**, SL1 will automatically align the Dynamic Applications from the *Cisco: Video Endpoint* PowerPack to your Cisco Tandberg C Series Codec. However, the Dynamic Applications in the *Cisco: Video Endpoint* PowerPack might take a significant amount of time to align with Cisco Tandberg C Series devices during discovery. If you are discovering multiple Cisco Tandberg endpoints or your Cisco Tandberg endpoints take several seconds to respond to HTTP requests, ScienceLogic recommends that you do not include SOAP/XML credentials in the discovery session.

If you do not include SOAP/XML credentials in the discovery session for your Cisco Tandberg C Series codecs, you can manually align the Tandberg Dynamic Applications using a device template. To create a device template for a Cisco Tandberg C Series codec, perform the following steps:

1. Go to the **Configuration Templates** page (Devices > Templates, or Registry > Devices > Templates in the classic SL1 user interface).
2. Click the **[Create]** button. The **Device Template Editor** page appears.
3. Type a name for your device template in the ***Template Name*** field.
4. Click the **[Dyn Apps]** tab.
5. For each Dynamic Application listed in the table below:
    - Click **Add New Dynamic App Sub-Template**.
    - Click the Dynamic Application in the ***Dynamic Application*** field.
    - Click the ***Credentials*** field, then select the credential listed for the Dynamic Application in the table below.
6. Click the **[Save]** button.

If your discovery session includes IP addresses for only Cisco Tandberg C Series codecs, you can apply the device template to all devices discovered by that discovery session. To apply a device template to all devices discovered by a discovery session, select the device template in the ***Apply Device Template*** field in the **Discovery Session Editor**.

If your discovery session includes IP addresses for other types of devices in addition to Cisco Tandberg C Series codecs, you can apply the device template to your Cisco Tandberg C Series codecs after discovery in the **Device Manager** page. To do this:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface).
2. Select the checkbox for each Cisco Tandberg C Series codec.
3. In the ***Select Action*** drop-down list, select *Modify By Template* and then click the **[Go]** button. The **Bulk Device Configuration** modal page appears.
4. Select the device template in the ***Template*** field.
5. Click the **[Apply]** button.
6. In the confirmation page that appears, click the **[Confirm]** button.

The following table lists the Dynamic Applications for Cisco Tandberg C Series Codecs, the dependencies between the caching and cache consuming Dynamic Applications, and the credential that must be aligned with each Dynamic Application:

Dynamic Application	Credential	Caching Type	Dependencies
Cisco: Active Call (Tandberg C Series)	N/A	Consumes Cache	Cisco: Status Cache (Tandberg C Series)
Cisco: Audio/Video (Tandberg C Series)	N/A	Consumes Cache	Cisco: Status Cache (Tandberg C Series)
Cisco: Call Detail Records (Tandberg C Series)	Tandberg Endpoint - History	No Caching	N/A
Cisco: Call Quality Statistics (Tandberg C Series)	N/A	Consumes Cache	Cisco: Status Cache (Tandberg C Series)
Cisco: Configuration (Tandberg C Series)	N/A	Consumes Cache	Cisco: Status Cache (Tandberg C Series) and Cisco: Configuration Cache (Tandberg C Series)
Cisco: Configuration Cache (Tandberg C Series)	Tandberg Endpoint - Configuration	Populates Cache	N/A
Cisco: Device Discovery (Tanberg C Series)	N/A	Consumes Cache	Cisco: Configuration Cache (Tanberg C Series)
Cisco: Environmental (Tandberg C Series)	N/A	Consumes Cache	Cisco: Configuration Cache (Tandberg C Series)
Cisco: Remote Management (Tandberg C Series)	N/A	Consumes Cache	Cisco: Status Cache (Tandberg C Series) and Cisco: Configuration Cache (Tandberg C Series)
Cisco: Status Cache (Tandberg C Series)	Tandberg Endpoint - Status	Populates Cache	N/A

NOTE: When SL1 runs the "Cisco: Device Discovery (Tanberg CSeries)" Dynamic Application, the Dynamic Application triggers a Run Book Action that aligns the appropriate Cisco Tanberg C Series Device Classes to your devices.

Chapter 3

Monitoring Cisco Tandberg MXP Series Endpoints

Overview

The following sections describe how to configure Cisco Tandberg MXP Series endpoints for monitoring by SL1 using the *Cisco: Video Endpoint* PowerPack:

This chapter covers the following topics:

Configuring Cisco Tandberg MXP Series Endpoints for Monitoring by SL1 19

Creating an SNMP Credential 22

Configuring SOAP/XML Credentials 22

Dynamic Applications for Cisco Tandberg MXP Series Endpoints 23

Configuring Cisco Tandberg MXP Series Endpoints for Monitoring by SL1

SL1 uses two protocols for monitoring Cisco Tandberg MXP Series Endpoints: SNMP and HTTP. By default, Cisco Tandberg MXP Series Endpoints respond to both SNMP and HTTP requests using the following credentials:

- For SNMP requests, Cisco Tandberg MXP Series Endpoints accept the public community string; you can use the SNMP Public V2 credential that is included by default in SL1 to monitor Cisco Tandberg MXP Series Endpoints that use the default configuration.
- For HTTP requests, Cisco Tandberg MXP Series Endpoints do not use a username for authentication and accept the password "TANDBERG" by default. From the **Control Panel** on a Cisco Tandberg MXP Series Endpoint, you can change this password by entering a value in the ***IP Access Password*** field in the **Security** menu.

This section will describe how to:

- Configure a new SNMP community string for a Cisco Tandberg MXP Series Endpoint.
- Configure a Cisco Tandberg MXP Series Endpoint to send SNMP Traps to SL1.
- Configure a new IP Access Password for HTTP requests.

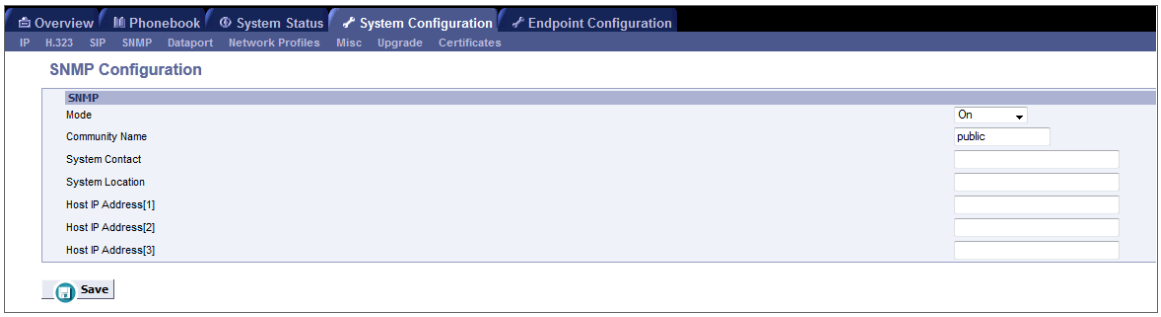
This section describes how to perform these tasks remotely from the web interface on a Cisco Tandberg MXP Series Endpoint. To perform these tasks, you must know the current ***IP Access Password*** for the device.

> **NOTE:** These instructions assume that the Cisco Tandberg MXP Series Endpoint has been assigned an IP address and is visible to a Data Collector on the network.

To configure the SNMP settings on a Cisco Tandberg MXP Series Endpoint, perform the following steps:

1. In a browser window, go to the IP address of the Cisco Tandberg MXP Series Endpoint.
2. You will be prompted for a username and password. Cisco Tandberg MXP Series Endpoints do not use a username for authentication. In the ***Password*** field, type the IP Access Password for this device. The default IP Access Password is "TANDBERG".
3. Click the **[OK]** button. The **Tandberg Overview** page appears:

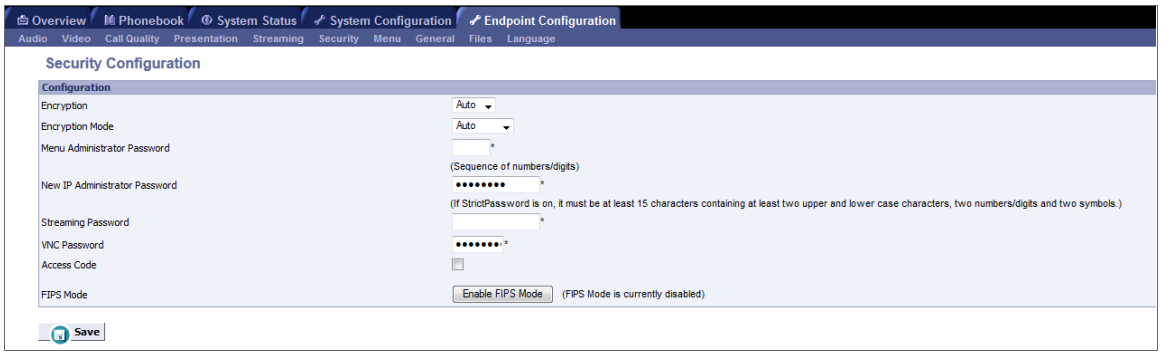
4. Click the **[System Configuration]** tab, and then click **SNMP** from the set of sub-tabs that appear. The **SNMP Configuration** page appears:



5. Supply values in the following fields:
   - ***Mode***. Select *On* from the drop-down list.
   - ***Community Name***. Type the new SNMP community string for this device. When you configure an SNMP credential for this Cisco Tandberg MXP Series Endpoint in SL1, you will type this community string in the ***SNMP Community (Read-Only)*** field.
   - ***System Contact***. Optionally, type the contact information for the administrator of this device.
   - ***System Location***. Optionally, type the location of this device.
   - ***Host IP Address[1]***. Type the IP address of the Message Collector or Data Collector that will collect SNMP trap messages from the device. If the device is already configured to send SNMP traps to another IP address and you want to retain those settings, you can type the IP address of the Message Collector or Data Collector in the ***Host IP Address[2]*** or ***Host IP Address[3]*** field.
6. Click the **[Save]** button to save the new SNMP settings.

If you want to change the password that SL1 will use to perform HTTP requests on this device, perform the following steps:

1. Click the **[Endpoint Configuration]** tab, then click **Security** from the set of sub-tabs that appear. The **Security Configuration** page appears:



2. Type the new password in the ***New IP Administrator Password*** field.

> **CAUTION:** Because Cisco Tandberg MXP Series Endpoints do not use usernames for authentication, entering a new value in this field will change the password for all administrators of this device.

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

Creating an SNMP Credential

To monitor Cisco Tandberg MXP Series Endpoints in SL1, you will need to create an SNMP Credential for each Endpoint.

To create an SNMP Credential for a Cisco Tandberg MXP Series Endpoint, perform the following steps in SL1:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click **[Actions]**, and then select *Create SNMP Credential*. The **Credential Editor** page appears.
3. Supply values in the following fields:
   - ***Profile Name***. Type a name for the credential.
   - ***SNMP Version***. Select *SNMP V2*.
   - ***SNMP Community (Read-Only)***. Type the SNMP community string you configured on the Cisco Tandberg MXP Series Endpoint.

> **NOTE:** You can optionally change the values in the ***Timeout(ms)*** and ***Retries*** fields.

4. Click **[Save]**.
5. When you configure a discovery session that includes the IP address of the Cisco Tandberg MXP Series Endpoint, select the SNMP credential you created in the ***SNMP Credentials*** field. For more information about discovery in SL1, see the ***Discovery and Credentials*** manual.

Configuring SOAP/XML Credentials

To use the Dynamic Applications in the *Cisco: Video Endpoint* PowerPack, you must configure three SOAP/XML credentials for your Cisco Tandberg MXP Series Endpoint. The three credentials are:

- Tandberg Endpoint - Configuration
- Tandberg Endpoint - History
- Tandberg Endpoint - Status

These credentials enable SL1 to collect configuration and performance data along with call detail records using unique combinations of URL, username, and password.

If you have multiple Cisco Tandberg MXP Series Endpoints, you will need one set of credentials for each unique password. For example, if you have configured three Cisco Tandberg MXP Series Endpoints with the same password, you need only one set of credentials.

The *Cisco: Video Endpoint* PowerPack includes a template for each SOAP/XML credential that you can edit for use with your Cisco Tandberg devices.

Modifying the Credential Templates

To modify the templates, perform the following steps:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the wrench icon ( ) for the "Tandberg Endpoint - Configuration" credential. The **Credential Editor** modal window appears.
3. In the ***Profile Name*** field, type a new name for the credential.
4. In the ***HTTP Auth User*** field, type "admin".
5. In the ***HTTP Auth Password*** field, type the password you configured on the Cisco Tandberg MXP Endpoint.
6. Click the **[Save As]** button.
7. Repeat steps 2 - 6 for the "Tandberg Endpoint - History" and "Tandberg Endpoint - Status" credentials.

Dynamic Applications for Cisco Tandberg MXP Series Endpoints

The *Cisco: Video Endpoint* PowerPack contains eight Dynamic Applications that can be used to monitor Cisco Tandberg MXP Series Endpoints. Some of the Dynamic Applications for Cisco Tandberg MXP Series Endpoints use the caching feature:

- Two Dynamic Applications are used only to collect and cache data from Cisco Tandberg MXP Series Endpoints.
- Five Dynamic Applications use the cached data. For these five Dynamic Applications to display data, the Dynamic Applications that collect and cache data must be aligned to the same device.
- One Dynamic Application for Cisco Tandberg MXP Series Endpoints does not use the caching feature.

The Dynamic Applications in the *Cisco: Video Endpoint* PowerPack include discovery objects. If you discover your Cisco Tandberg MXP Series Endpoint as an SNMP device and include all the SOAP/XML credentials you configured for your Cisco Tandberg MXP Series Endpoint in the ***Other Credentials*** field in the **Discovery Session Editor**, SL1 will automatically align the Dynamic Applications from the *Cisco: Video Endpoint* PowerPack to your Cisco Tandberg MXP Series Endpoint. However, the Dynamic Applications in the *Cisco: Video Endpoint* PowerPack might take a significant amount of time to align with Cisco Tandberg devices during discovery. If you are discovering multiple Cisco Tandberg Endpoints or your Cisco Tandberg Endpoints take several seconds to respond to HTTP requests, ScienceLogic recommends that you do not include SOAP/XML credentials in the discovery session.

If you do not include SOAP/XML credentials in the discovery session for your Cisco Tandberg MXP Series endpoints, you can manually align the Tandberg Dynamic Applications using a device template. To create a device template for a Cisco Tandberg MXP Series Endpoint, perform the following steps:

1. Go to the **Configuration Templates** page (Devices > Templates, or Registry > Devices > Templates in the classic SL1 user interface).
2. Click the **[Create]** button. The **Device Template Editor** page appears.
3. Type a name for your device template in the ***Template Name*** field.
4. Type the **[Dyn Apps]** tab.
5. For each Dynamic Application listed in the table below:
    - Click ***Add New Dynamic App Sub-Template***.
    - Select the Dynamic Application in the ***Dynamic Application*** field.
    - Click the ***Credentials*** field, then select the credential listed for the Dynamic Application in the table below.
6. Click the **[Save]** button.

If your discovery session includes IP addresses for only Cisco Tandberg MXP Series endpoints, you can apply the device template to all devices discovered by that discovery session. To apply a device template to all devices discovered by a discovery session, select the device template in the ***Apply Device Template*** field in the **Discovery Session Editor**.

If your discovery session includes IP addresses for other types of devices in addition to Cisco Tandberg MXP Series endpoints, you can apply the device template to your Cisco Tandberg MXP Series endpoints after discovery in the **Device Manager** page. To do this:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface).
2. Select the checkbox for each Cisco Tandberg MXP Series endpoint.
3. In the ***Select Action*** drop-down list, select *Modify By Template* and then click the **[Go]** button. The **Bulk Device Configuration** modal page appears.
4. Select the device template in the ***Template*** field.
5. Click the **[Apply]** button.
6. In the confirmation page that appears, click the **[Confirm]** button.

The following table lists the Dynamic Applications for Cisco Tandberg MXP Series Endpoints, the dependencies between the caching and cache consuming Dynamic Applications, and the credential that must be aligned with each Dynamic Application:

Dynamic Application	Credential	Caching Type	Dependencies
Cisco: Active Call (Tandberg MXP)	N/A	Consumes Cache	Cisco: Status Cache (Tandberg MXP)
Cisco: Audio/Video (Tandberg MXP)	N/A	Consumes Cache	Cisco: Status Cache (Tandberg MXP)
Cisco: Call Detail Records (Tandberg MXP)	Tandberg Endpoint - History	No Caching	N/A
Cisco: Call Quality Statistics (Tandberg MXP)	N/A	Consumes Cache	Cisco: Status Cache (Tandberg MXP)

Dynamic Application	Credential	Caching Type	Dependencies
Cisco: Configuration (Tandberg MXP)	N/A	Consumes Cache	Cisco: Status Cache (Tandberg MXP) and Cisco: Configuration Cache (Tandberg MXP)
Cisco: Configuration Cache (Tandberg MXP)	Tandberg Endpoint - Configuration	Populates Cache	N/A
Cisco: Device Discovery (Tanberg MXP)	N/A	Consumes Caches	Cisco: Configuration Cache (Tanberg MXP Series)
Cisco: Remote Management (Tandberg MXP)	N/A	Consumes Cache	Cisco: Status Cache (Tandberg MXP) and Cisco: Configuration Cache (Tandberg MXP)
Cisco: Status Cache (Tandberg MXP)	Tandberg Endpoint - Status	Populates Cache	N/A

NOTE: When SL1 runs the "Cisco: Device Discovery (Tanberg MXP Series)" Dynamic Application, the Dynamic Application triggers a Run Book Action that aligns the appropriate Cisco Tanberg MXP Series Device Classes to your devices.

Chapter 4

Monitoring Cisco CE Series Endpoints

Overview

The following sections describe how to configure Cisco CE Series endpoints for monitoring by SL1 using the *Cisco: Video Endpoint* PowerPack:

This chapter covers the following topics:

Configuring Cisco CE Series Endpoints for Monitoring by SL1 ..... *26*

Creating an SNMP Credential *29*

Configuring SOAP/XML Credentials *31*

Discovering Cisco CE Series Endpoints *33*

Configuring Cisco CE Series Endpoints for Monitoring by SL1

SL1 uses two protocols for monitoring Cisco CE Series endpoints: SNMP and HTTP. This section describes how to configure Cisco CE Series endpoints for both of those protocols.

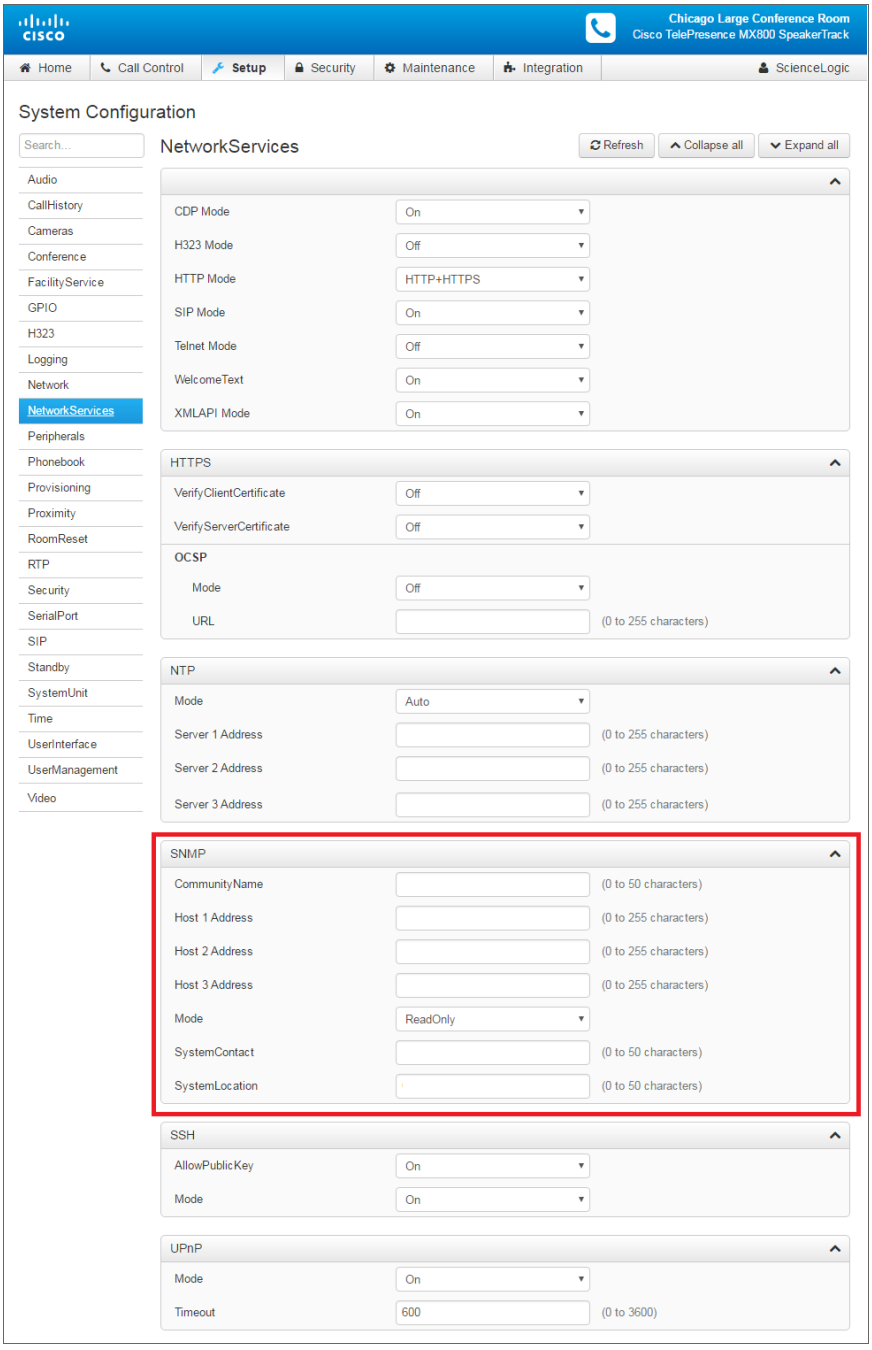
Configuring SNMP Settings

To monitor Cisco CE Series endpoints in SL1, you must configure the SNMP community string and other information that the platform will use to connect to the endpoints. You will use this information to *create an SNMP credential* to monitor the endpoints.

To configure the SNMP settings on a Cisco CE Series endpoint:

1. In a browser window, go to the IP address of the Cisco CE Series endpoint. You are prompted for a username and password.

2. Go to the **Network Services** page (Setup > Configuration > Network Services). Under the **SNMP** subheading, supply values in the following fields:



- ***Community Name***. Type a new SNMP community string for this device. *When you configure an SNMP credential* for this Cisco CE Series endpoint in SL1, you will type this community string in the ***SNMP Community (Read-Only)*** field.

- ***Host 1 Address***. Type the IP address of the Message Collector or Data Collector that will collect SNMP trap messages from the device. If the device is already configured to send SNMP traps to another IP address and you want to retain those settings, you can type the IP address of the Message Collector or Data Collector in the ***Host 2 Address*** or ***Host 3 Address*** field.
- ***Mode***. Select *ReadOnly*.
- ***SystemContact***. Optionally, type the contact information for the device's administrator.
- ***SystemLocation***. Optionally, type the device's location.

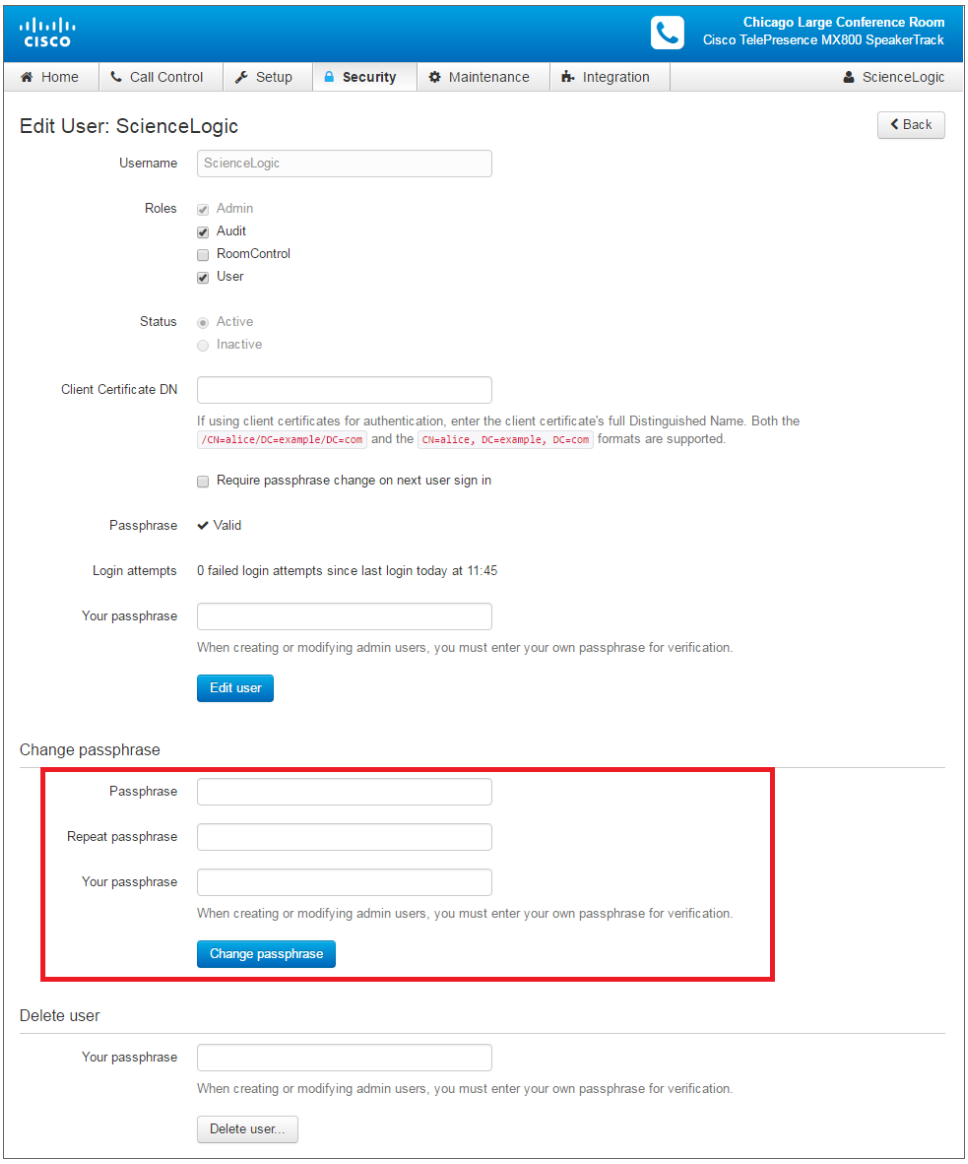
3. Click **[Save]**.

Configuring the HTTP Request Password

Optionally, if you are *using a SOAP/XML credential* to collect configuration and performance data from a Cisco CE Series endpoint, you can configure the password for the account SL1 will use to perform HTTP requests on the Cisco CE Series endpoint.

To configure the HTTP request password:

1. Go to the **Users** page (Security > Users) and select the username of the account SL1 will use to perform HTTP requests to this device. The **Edit User** page appears.
2. On the **Edit User** page, supply values in the following fields:



- ***Passphrase***. Type the user account's new passphrase.
- ***Repeat passphrase***. Retype the user account's new passphrase.
- ***Your passphrase***. Type your current administrator passphrase.

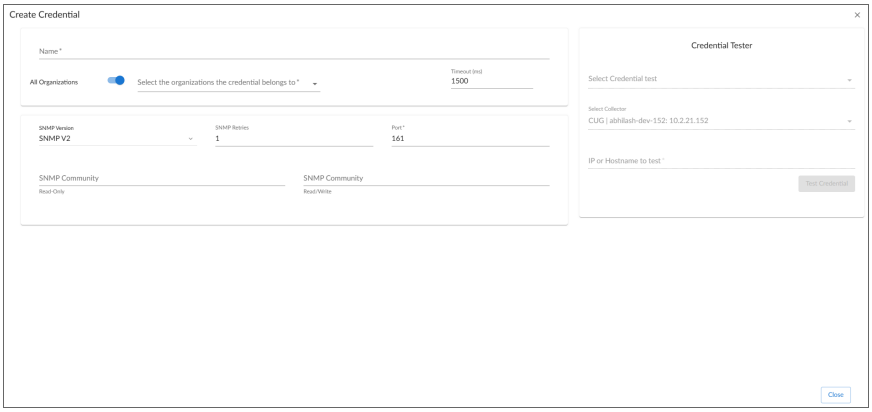
3. Click **[Change passphrase]**.

Creating an SNMP Credential

To monitor Cisco CE Series endpoints in SL1, you must create an SNMP credential for each endpoint.

To create an SNMP Credential:

1. Go to the **Credentials** page (Manage > Credentials).
2. Click the **[Create New]** button and select *Create an SNMP Credential* from the drop-down menu. The **Create Credential** page appears.
3. Complete the following fields:



4. ***Name***. Enter a new name for the credential. This field is required.
5. ***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 ***Select the organizations the credential belongs to*** drop-down field to align the credential with those specific organizations.
6. ***Timeout (ms)***. Enter the time, in milliseconds, after which SL1 will stop trying to communicate with the Cisco Unity Express device. The default value is *1500*. This field is required.
7. ***SNMP Version***. Select *SNMP V2* from the drop-down list.
8. ***SNMP Retries***. Keep the default. The default value is "1".
9. ***Port***. Keep the default. The default port is "161".
10. ***SNMP Community (Read Only)***. Enter the community string for the Cisco Unity Express voice mailbox you want to monitor.
11. ***SNMP Community (Read/Write)***. Optional. Enter the community string for the Cisco Unity Express to grant Read/Write permissions.
12. Click **[Close]**.

Creating an SNMP Credential in the SL1 Classic User Interface

To monitor Cisco CE Series endpoints in SL1, you must create an SNMP credential for each endpoint.

To create an SNMP credential for a Cisco CE Series endpoint in the classic user interface:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click **[Actions]**, and then select *Create SNMP Credential*. The **Credential Editor** modal page appears.
3. Supply values in the following fields:
    - ***Profile Name***. Type a name for the credential.

- ***SNMP Version***. Select *SNMP V2*.
- ***SNMP Community (Read-Only)***. Type the SNMP community string you *configured on the Cisco CE Series endpoint*.

> **NOTE:** You can optionally change the values in the ***Timeout(ms)*** and ***Retries*** fields. For more information about all fields in the **Credential Editor** page, see the ***Credentials and Discovery*** manual.

4. Click **[Save]**.

Configuring SOAP/XML Credentials

To monitor Cisco CE Series endpoints in SL1, you must configure three SOAP/XML credentials for your Cisco CE Series endpoints. The three credentials are:

- Cisco CE Series Configuration
- Cisco CE Series History
- Cisco CE Series Status

These credentials enable SL1 to collect configuration and performance data along with call detail records using unique combinations of a URL, username, and password.

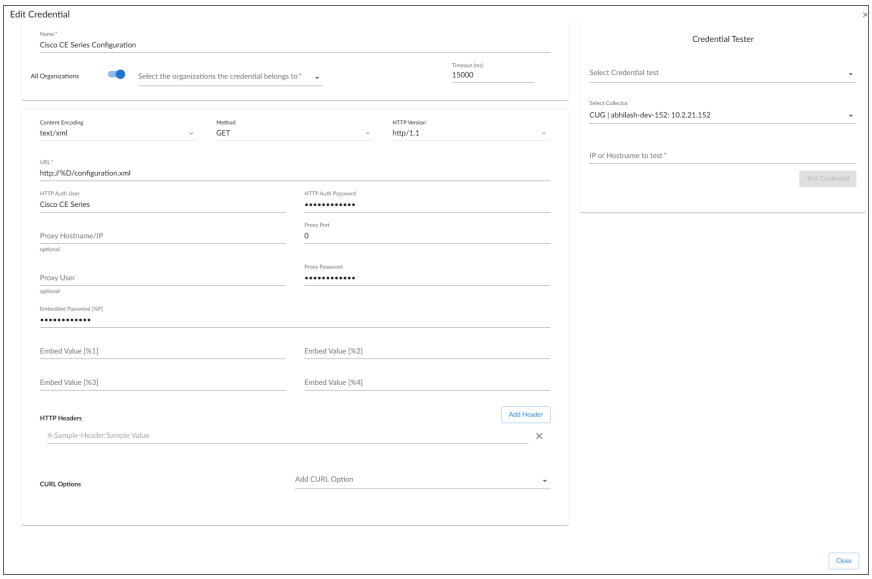
If you have multiple Cisco CE Series endpoints, you need one set of credentials for each unique password. For example, if you have configured three Cisco CE Series endpoints with the same password, you need only one set of credentials. If you have configured three Cisco CE Series endpoints with three unique passwords, you need three sets of credentials.

Modifying the SOAP/XML Credential Templates

The "Cisco: Video Endpoint" PowerPack includes a template for each SOAP/XML credential that you can edit for use with your Cisco device.

To modify the SOAP/XML credential:

1. Go to the Credentials page (Manage > Credentials).
2. Locate the "Cisco CE Series Credential", then click its **[Actions]** icon ( ) and select *Duplicate* from the drop-down field. The "Cisco CE Series Credential copy" credential appears.
3. Click the **[Action]** icon ( ) for the "Cisco CE Series Credential copy" credential, then select *Edit*. The **Edit Credential** page appears.



4. Enter values in the following fields:
    - ***Name***. Enter a new name for the credential. This field is required.
    - ***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 ***Select the organizations the credential belongs to*** drop-down field to align the credential with those specific organizations.
    - ***Timeout***. Enter the time, in milliseconds, after which SL1 will stop trying to communicate with the Video Endpoint device. The default value is *15000*. This field is required.
    - ***URL***. Keep the default url of "http://%D/configuration.xml".
    - ***HTTP Auth User***. Enter the Video Endpoint username associated with the administrator account.
    - ***HTTP Auth Password***. Enter the password associated with the Video Endpoint administrator account.
    - ***Embedded Password [%P]***. Enter the embedded password associated with the Video Endpoint administrator account.
    - Click **[Save & Close]**.

Modifying the SOAP/XML Credential Templates in the SL1 ADS Classic User Interface

The "Cisco: Video Endpoint" PowerPack includes a template for each SOAP/XML credential that you can edit for use with your Cisco device.

To modify the SOAP/XML credential templates in the classic user iterface:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the wrench icon ( ) for the "Cisco CE Series Configuration" credential. The **Credential Editor** modal page appears.

3. Supply values in the following fields:
    - ***Profile Name***. Type a name for the credential.
    - ***HTTP Auth User***. Type the username of the HTTP user account that you *configured on the Cisco CE endpoint*.
    - ***HTTP Auth Password***. Type the passphrase of the HTTP user account you configured on the Cisco CE endpoint.
4. Click **[Save As]**.
5. Repeat steps 2-4 for the "Cisco CE Series History" and "Cisco CE Series Status" credentials.

Discovering Cisco CE Series Endpoints

The *Cisco: Video Endpoint* PowerPack contains Dynamic Applications that can be used to discover and monitor Cisco CE Series endpoints. Some of the Dynamic Applications for Cisco CE Series endpoints use the caching feature:

- Two Dynamic Applications are used only to collect and cache data from Cisco CE Series endpoints.
- Eight Dynamic Applications use the cached data. For these Dynamic Applications to display data, the Dynamic Applications that collect and cache data must be aligned to the same device.
- ThreeDynamic Application that do not use the caching feature.

NOTE: For more information about the Dynamic Application caching feature, see the ***Dynamic Application Development*** manual.

The following table lists the Dynamic Applications for Cisco CE Series endpoints, the dependencies between the caching and cache consuming Dynamic Applications, and the credential that must be aligned with each Dynamic Application:

Dynamic Application	Credential	Caching Type	Dependencies
Cisco: Active Call (CE Series)	N/A	Consumes Cache	Cisco: Status Cache (CE Series)
Cisco: Audio/Video (CE Series)	N/A	Consumes Cache	Cisco: Status Cache (CE Series)
Cisco: Call Detail Records (CE Series)	Cisco CE Series History	No Caching	N/A
Cisco: Call Quality Statistics (CE Series)	N/A	Consumes Cache	Cisco: Status Cache (CE Series)

Dynamic Application	Credential	Caching Type	Dependencies
Cisco: Configuration (CE Series)	N/A	Consumes Cache	Cisco: Status Cache (CE Series) and Cisco: Configuration Cache (CE Series)
Cisco: Configuration Cache (CE Series)	Cisco CE Series Configuration	Populates Cache	N/A
Cisco: Configuration Discovery (CE Series)	Cisco CE Series Configuration	No caching	N/A
Cisco: Device Discovery (CE Series)	N/A	Consumes Caches	Cisco: Configuration Cache (CE Series)
Cisco: Environmental (CE Series)	N/A	Consumes Cache	Cisco: Configuration Cache (CE Series)
Cisco: IC Detail (CE Series)	N/A	Consumes Cache	Cisco: Status Cache (CE Series)
Cisco: Remote Management (CE Series)	N/A	Consumes Cache	Cisco: Status Cache (CE Series) and Cisco: Configuration Cache (CE Series)
Cisco: Status (CE Series)	N/A	Consumes Cache	Cisco: Status Cache (CE Series)
Cisco: Status Cache (CE Series)	Cisco CE Series Status	Populates Cache	N/A
Cisco: Status Discovery (CE Series)	Cisco CE Series Status	No caching	N/A

NOTE: The "Cisco: IC Detail (CE Series)" Dynamic Application is disabled by default. To enable it, go to the **Dynamic Applications Manager** page (System > Manage > Applications), locate the Dynamic Application and click its wrench icon (), select *Enabled* in the ***Operational State*** field, and then click **[Save]**.

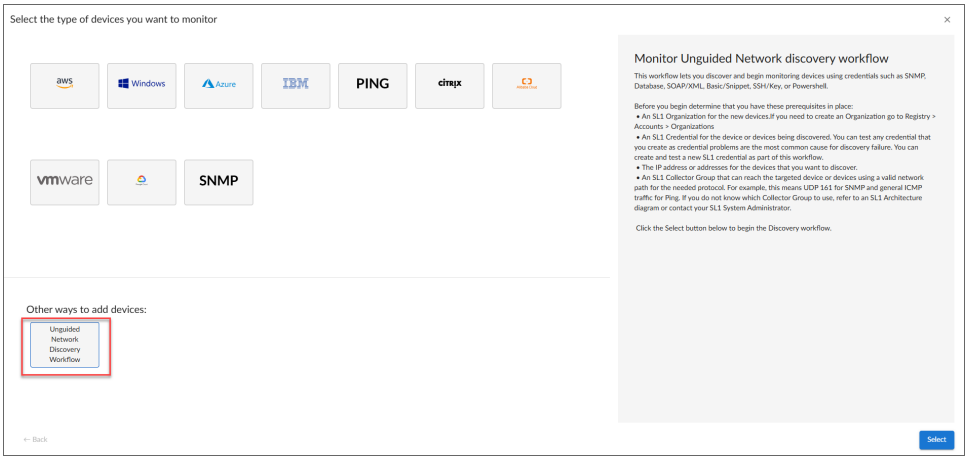
NOTE: When SL1 runs the "Cisco: Device Discovery (CE Series)" Dynamic Application, the Dynamic Application triggers a Run Book Action that aligns the appropriate Cisco CE Series Device Classes to your devices.

Discovering CE Series Devices

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

To create and run a discovery session that will discover a CE Series appliance:

1. Go to the **Devices** page (🖥) or the **Discovery Sessions** page (Devices > Discovery Sessions) and click the **[Add Devices]** button.
2. Click the **[Unguided Network Discovery Workflow]** button. Additional information about that requirements for discovery appears in the **General Information** pane to the right.



3. Click **[Select]**. The three-step wizard appears starting with the **[Step 1 Basic Information]** tab.
4. Complete the following fields:
   - ***Discovery Session 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 **[Step 2 Credential Selection]** tab of the wizard appears.
6. On the **[Credential Selection]** tab, locate and select the SOAP/XML credential you created for CE Series appliances.
7. Click **[Next]**. The **[Step 3 Discovery Session Details]** tab of the wizard appears.
8. Complete the following fields:
   - ***List of IP/Hostnames***. Type the IP address for the CE Series appliance.
   - ***Which collector will discover these devices?***. Required. Select an existing collector to monitor the discovered devices.
   - ***Run after save***. Toggle on (blue) to run this discovery session as soon as you save the session.
   - ***Advanced options***. Click the down arrow (⌄) to complete the following fields:
     - ***Discover Non-SNMP***. Toggle on (blue) to enable this setting.
     - ***Model Devices***. Toggle on (blue) to enable this setting.
     - ***Select Device Template***. If you configured a CE Series device template, select it here. Otherwise, leave the default selection.

9. If you enabled the ***Run after save*** option, click the**[Save and Run]** button. The discovery session will run and the **Discovery Logs** page will display any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page will include a link to the **Device Investigator** page for the discovered device.
10. If you did not enable the ***Run after save*** option, click the **[Save and Close]** button. The **Discovery Sessions** page (Devices > Discovery Sessions) will display the new discovery session.

Discovering CE Series Devices in the SL1 Classic User Interface

To model and monitor your Cisco CE Series devices, you must run a discovery session to discover the Cisco device that SL1 will use as the root device for monitoring.

Several minutes after the discovery session has completed, the Dynamic Applications should automatically align to the root device and then discover, model, and monitor the remaining Cisco CE Series devices.

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

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery or System > Manage > Discovery in the classic user interface).
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***. Enter the IP address(es) and/or hostname(s) for the device(s) you want to discover.
    - ***SNMP Credentials***. This field is optional. Select the SNMP credential you created for the device clusters.
    - ***Other Credentials***. Select the credentials you created using the following templates (the name of the credential might have been changed when it was saved):
        - Cisco CE Series Configuration
        - Cisco CE Series History
        - Cisco CE Series Status
    - ***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(s) are discovered, click the device icon ( ) to view the **Device Properties** page for each device.

Chapter 5

Monitoring Cisco TelePresence Endpoints

Overview

The following sections describe how to configure Cisco TelePresence endpoints for monitoring by SL1 using the *Cisco: TelePresence: Endpoints* PowerPack:

This chapter covers the following topics:

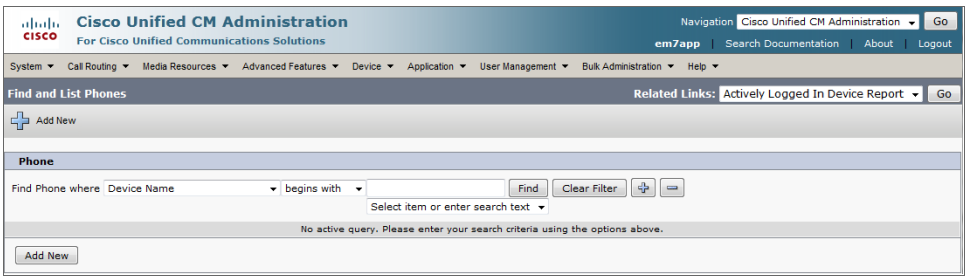
Configuring TelePresence Endpoints for Monitoring by SL1 ..... *37*

Creating an SNMP Credential *40*

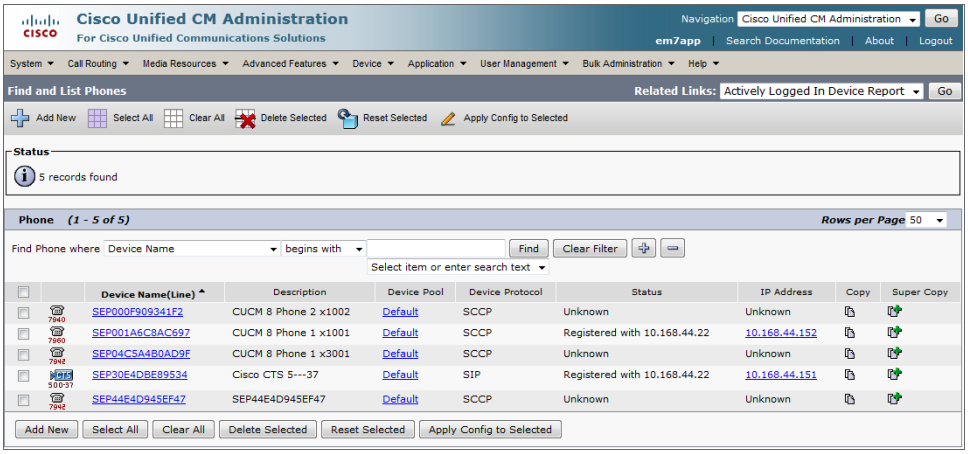
Configuring TelePresence Endpoints for Monitoring by SL1

To configure a TelePresence endpoint for monitoring by SL1

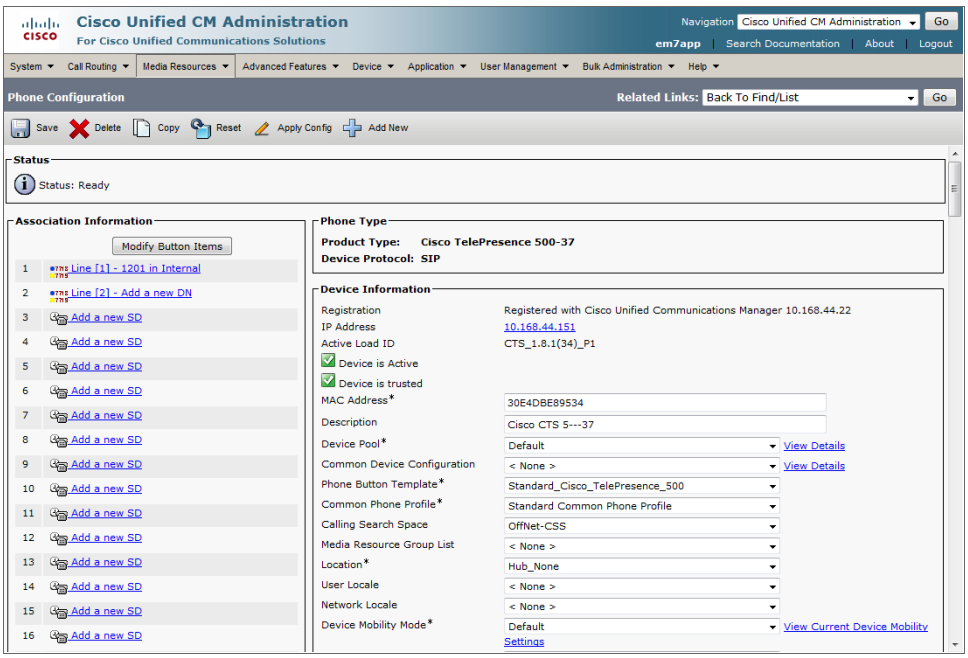
1. Log in to Cisco Unified Call Manager.
2. Select Device > Phone. The **Find and List Phones** page appears.



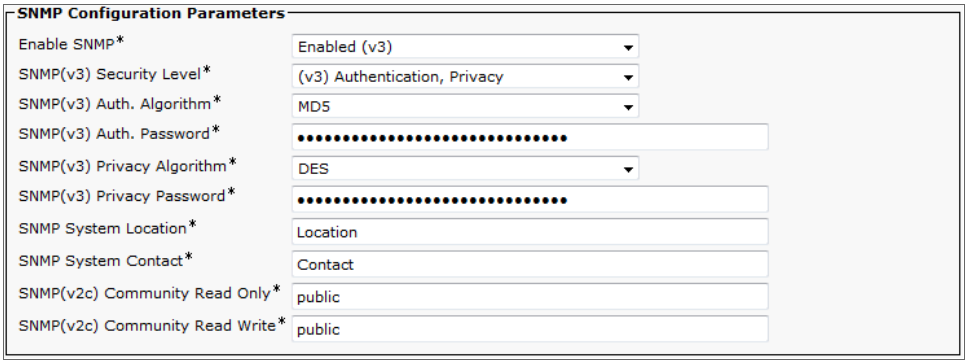
3. In the **Find and List Phones** page, search for the phone, or select the **[Find]** button to see all phones.



4. Select the Device name link for your TelePresence Endpoint. This brings up the **Phone Configuration** page.

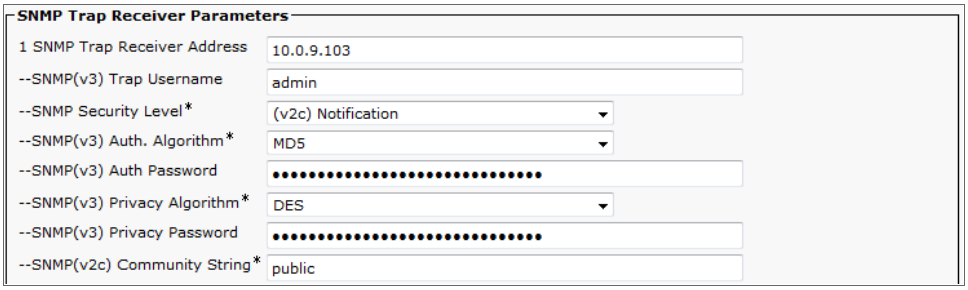


5. Scroll down the **Phone Configuration** page until you come to the **SNMP Configuration Parameters** section. Enter values in the **SNMP Configuration Parameters** section in the following fields:



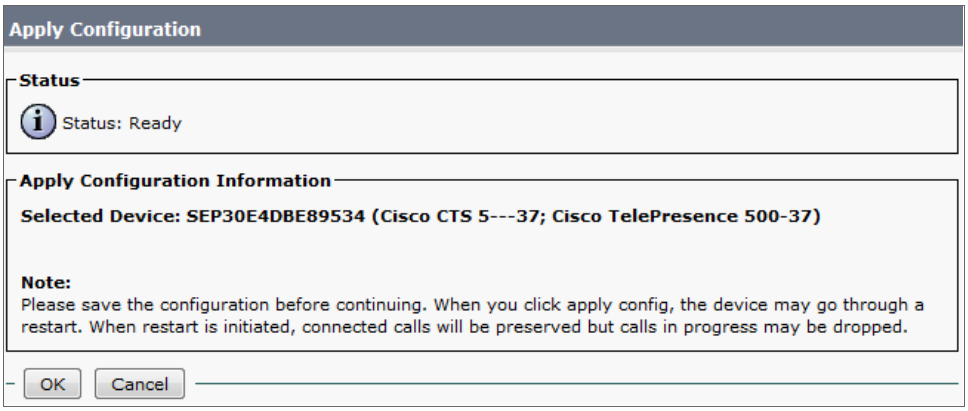
- ***Enable SNMP***. Select *Enabled (v3)*.
- ***SNMP(v3) Security Level***. There are three levels of security that can be used with an SNMP v3 security name. You must determine which security level is appropriate for your environment.
- ***SNMP(v3) Auth. Algorithm***. Select an authentication protocol for transmission of the authentication password. The ScienceLogic platform supports both the *MD5* and *SHA* options.
- ***SNMP(v3) Auth. Password***. Enter an authentication password. The password must be at least 8 characters.
- ***SNMP(v3) Privacy Algorithm***. Select an authentication protocol for transmission of the authentication password. The ScienceLogic platform supports the *DES* and *AES128* options. Do not select *AES192* or *AES256* in this field.
- ***SNMP(v3) Privacy Password***. Enter a privacy password. The password must be at least 8 characters.
- ***SNMP System Location***. Enter the location of the device.
- ***SNMP System Contact***. Enter the contact information for the administrator of this device.
- ***SNMP(v2c) Community Read Only***. This field is not used. Leave this field set to the default value.
- ***SNMP(v2c) Community Read Write***. This field is not used. Leave this field set to the default value.

6. Continue to scroll down the **Phone Configuration** page until you reach the **SNMP Trap Receiver Parameters** section. Enter values in the **SNMP Trap Receiver Parameters** section in the following fields:



- ***SNMP Trap Receiver Address***.Enter the IP address of the Message Collection Unit or Data Collection Unit that will collect SNMP trap messages from the device.
- ***SNMP Security Level***. Select *(v2c) Notification*.
- ***SNMP(v3) Auth. Algorithm***. Leave this required field at its default setting.
- ***SNMP(v3) Privacy Algorithm***. Leave this required field at its default setting.
- ***SNMP(v2c) Community String***. Leave this required field at its default setting.

7. Scroll down the **Phone Configuration** page again and select the **[Save]** button, then select the **[OK]** button in the popup window.
8. Select *Apply Config*, and a confirmation window will appear.



9. Select the **OK** button in the **Apply Configuration** window.

Creating an SNMP Credential

To create an SNMP Credential for a TelePresence Endpoint, perform the following steps in SL1:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Select the **[Create]** button, and then select *SNMP Credential*. The **Credential Editor** page is displayed.

3. Supply values in the following fields:
    - ***Profile Name***. Enter a name for the credential.
    - ***SNMP Version***. Select *SNMP V3*.
    - ***SNMP Community (Read-Only)***. Enter the SNMP community string you configured on the TelePresence Endpoint.

NOTE: You can optionally change the values in the ***Timeout (ms)*** and ***Retries*** fields.

    - ***Security Name***. Enter the value you configured in the ***User Name*** field.
    - ***Security Passphrase***. If you are using the ***Authentication Only*** or ***Authentication and Encryption*** security levels, enter the value you configured in the ***SNMP(v3) Auth. Password*** field in the **SNMP Configuration Parameters** section.
    - ***Authentication Protocol***. If you are using the ***Authentication Only*** or ***Authentication and Encryption*** security levels, select the value you configured in the ***SNMP(v3) Auth. Algorithm*** field in the **SNMP Configuration Parameters** section.
    - ***Security Level***. Select the security level you configured for the security name.
    - ***Privacy Protocol***. If you are using the ***Authentication and Encryption*** security level, select the value you configured in the ***SNMP(v3) Privacy Algorithm*** field in the **SNMP Configuration Parameters** section.
    - ***Privacy Protocol Pass Phrase***. If you are using the ***Authentication and Encryption*** security level, enter the value you configured in the ***SNMP(v3) Privacy Password*** field in the **SNMP Configuration Parameters** section.
4. Select the **[Save]** button.
5. When you configure a discovery session that includes the IP address of the TelePresence Endpoint, select the SNMP credential you created in the ***SNMP Credentials*** field. For more information about discovery in SL1, see the ***Discovery and Credentials*** manual.

Chapter 6

Monitoring Cisco TelePresence Conductor

Overview

The following sections describe how to configure Cisco TelePresence Conductor devices for monitoring by SL1 using the *Cisco: TelePresence Conductor* PowerPack:

This chapter covers the following topics:

Prerequisites *42*

Monitoring Cluster Configurations vs. Non-Cluster Configurations *43*

Creating Credentials *43*

Creating and Discovering Virtual Devices *46*

Discovering IP Devices *48*

Viewing Cisco TelePresence Conductor Devices *50*

Prerequisites

Before performing the tasks in this chapter, you must enable API access for at least one user account in the Cisco TelePresence Conductor user interface. You can do so either for an administrator account or for a dedicated service account that has only API access. Use this account information when creating a SOAP/XML credential in SL1 to monitor Cisco TelePresence Conductor. For more information, see http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-installation-and-configuration-guides-list.html.

Additionally, if you are using SNMP to monitor the Conductor, then you must enable SNMP in the Conductor. Use this SNMP information when creating an SNMP credential in SL1 to monitor the Conductor.

Monitoring Cluster Configurations vs. Non-Cluster Configurations

SL1 enables you to monitor Cisco TelePresence Conductor in either a cluster configuration or a non-cluster configuration. However, there are differences in how each is monitored.

For ***cluster configurations***, ScienceLogic recommends that you use a virtual device to model the cluster. If you model the cluster using an IP device and that IP device becomes unresponsive, then all Dynamic Applications will stop collecting data until the IP responds. Modeling the cluster using a virtual device, however, maintains monitoring integrity if one or more nodes become unresponsive to SL1. To model the cluster using a virtual device, first you must create the virtual device in the platform and then you must manually align a Dynamic Application to discover and model the devices in the cluster.

For ***non-cluster configurations***, you can discover the Conductor as an SNMP-enabled or pingable IP device. When you discover the IP address using the appropriate credential(s), SL1 automatically aligns a Dynamic Application to discover and model the Conductor devices.

Creating Credentials

To monitor Cisco TelePresence Conductor, you must create a SOAP/XML credential with the appropriate API information. This credential enables SL1 to communicate with the Conductor, regardless of whether you are discovering an IP device or creating a virtual device to act as the cluster root device.

If you are monitoring SNMP-enabled IP devices, then you must also create an SNMP credential.

This section describes how to create both credentials.

Creating a SOAP/XML Credential

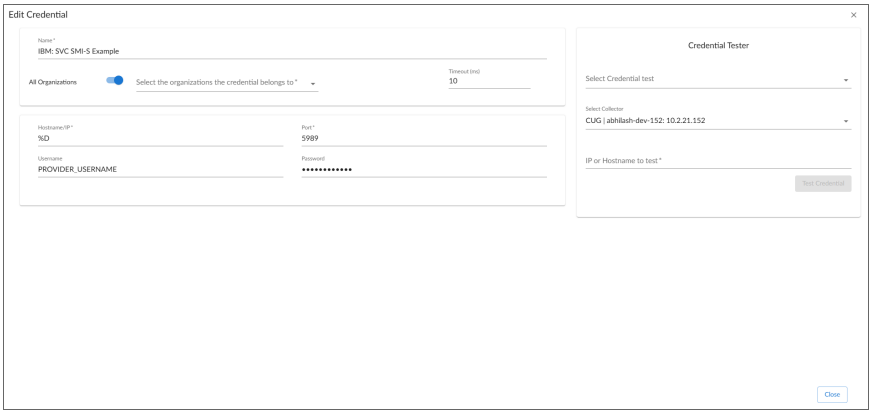
SL1 uses REST API and RPC API queries to monitor cluster operations for Cisco TelePresence Conductor. Therefore, you must align the Dynamic Applications in the *Cisco: TelePresence Conductor*PowerPack with a SOAP/XML credential that includes the REST API and RPC API login information.

The "Cisco:Telepresence Conductor" PowerPack includes two example SOAP/XML credentials (one for virtual devices and one for IP devices) that you can edit for your own use.

To create a SOAP/XML credential with one of the two example credentials:

1. Go to the **Credentials** page (Manage > Credentials).
2. f you are using a virtual device, locate the "Cisco: Conductor Example (Virtua" credential. If you are discovering an IP device, locate the "Cisco: Conductor Example (Discov" credential. Click its **[Actions]** icon (⋮) and select *Duplicate* from the drop-down field. The "Cisco: Conductor Example copy" credential appears, respective of the whether you chose a virtual device or an IP device.
3. Click the **[Action]** icon (⋮) for the "Cisco: Conductor Example (Discov" or "Cisco: Conductor Example

(Virtua" credential, then select *Edit*.The **Edit Credential** page appears.



3. Enter values in the following fields:
    - ***Name***. Enter a name for your TelePresence Conductor 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 ***Select the organizations the credential belongs to*** drop-down field to align the credential with those specific organizations.
    - ***Timeout***. Enter the time, in milliseconds, after which SL1 will stop trying to communicate with the TelePresence device. The default value is *5000*. This field is required.
    - ***Content Encoding***. Leave the default value "text/xml".
    - ***Method***. Leave the default set to "POST".
    - ***HTTP Version***. Leave the default value "HTTP/1.1".
    - ***URL***. If you are creating a virtual device as the root device, enter the URL of the master Conductor system. If you are discovering an IP device as the root device, enter "http://%D".
    - ***HTTP Auth User***. Enter the username for a Conductor account with API access.
    - ***HTTP Auth Password***. Enter the password for a Conductor account with API access.
    - ***Embedded Password [%P]***. Enter the embedded password associated with the TelePresence administrator account.
4. Click the **[Save & Close]** button.

Creating SOAP/XML Credential in the SL1 Classic User Interface

SL1 uses REST API and RPC API queries to monitor cluster operations for Cisco TelePresence Conductor. Therefore, you must align the Dynamic Applications in the "Cisco: TelePresence Conductor" PowerPack with a SOAP/XML credential that includes the REST API and RPC API login information.

The "Cisco: TelePresence Conductor" PowerPack includes two example SOAP/XML credentials (one for virtual devices and one for IP devices) that you can edit for your own use.

To create a SOAP/XML Credential in the classic user interface:

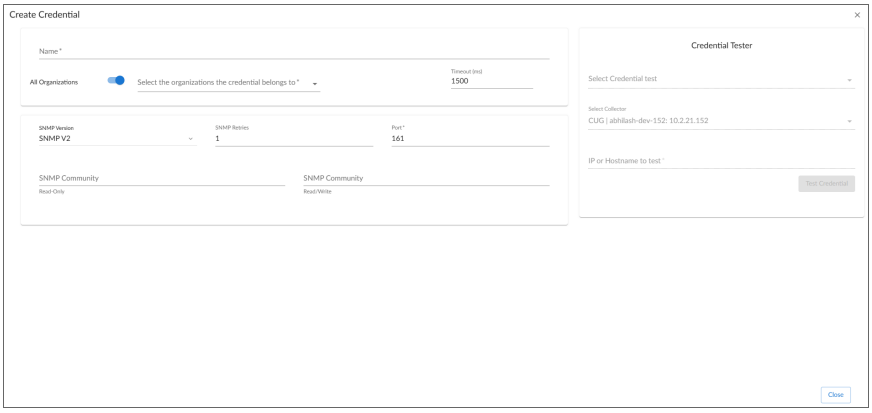
1. Go to the **Credential Management** page (System > Manage > Credentials).
2. If you are using a virtual device, locate the **Cisco: Conductor Example (Virtua** credential. If you are discovering an IP device, locate the **Cisco: Conductor Example (Discov** credential. Click its wrench icon ( ). The **Edit SOAP/XML Credential** modal page appears.
3. Enter values in the following fields:
   - ***Profile Name***. Enter a name for your TelePresence Conductor credential.
   - ***Content Encoding***. Select *text/xml*.
   - ***Method***. Select POST.
   - ***HTTP Version***. Select HTTP/1.1.
   - ***URL***. If you are creating a virtual device as the root device, enter the URL of the master Conductor system. If you are discovering an IP device as the root device, enter "http://%D".
   - ***HTTP Auth User***. Enter the username for a Conductor account with API access.
   - ***HTTP Auth Password***. Enter the password for a Conductor account with API access.
   - ***Timeout(seconds)***. Enter "10".
4. Click the **[Save]** button.

Creating an SNMP Credential

If you want to monitor SNMP-enabled Conductor devices, then you must also create an SNMP credential to enable SL1 to communicate with those devices.

To create an SNMP credential:

1. Go to the **Credentials** page (Manage > Credentials).
2. Click the **[Create New]** button and select *Create SNMP Credential* from the drop-down menu.
3. Complete the following fields:



4. ***Name***. Enter a new name for the credential. This field is required.

5. ***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 ***Select the organizations the credential belongs to*** drop-down field to align the credential with those specific organizations.
6. ***Timeout (ms)***. Enter the time, in milliseconds, after which SL1 will stop trying to communicate with the Cisco Unity Express device. The default value is *1500*. This field is required.
7. ***SNMP Version***. Select *SNMP V2* from the drop-down list.
8. ***SNMP Retries***. Keep the default. The default value is "1".
9. ***Port***. Keep the default. The default port is "161".
10. ***SNMP Community (Read Only)***. Enter the community string for the Cisco Unity Express voice mailbox you want to monitor.
11. ***SNMP Community (Read/Write)***. Optional. Enter the community string for the Cisco Unity Express to grant Read/Write permissions.
12. For the other optional fields, you can use the default values.
13. Click **[Close]**.

Creating an SNMP Credential in the SL1 Classic User Interface

If you want to monitor SNMP-enabled Conductor devices, then you must also create an SNMP credential to enable SL1 to communicate with those devices.

To create an SNMP credential in the classic user interface:

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.
4. Enter values in the following fields:
    - ***SNMP Version***. Select *SNMP V2*.
    - ***Profile Name***. Enter a name for the credential.
    - ***SNMP Community (Read Only)***. Enter the community string for the Conductor devices.
    - Optionally, supply values in the other fields in this page. In most cases, you can use the default values for the other fields.
5. Click the **[Save]** button.

Creating and Discovering Virtual Devices

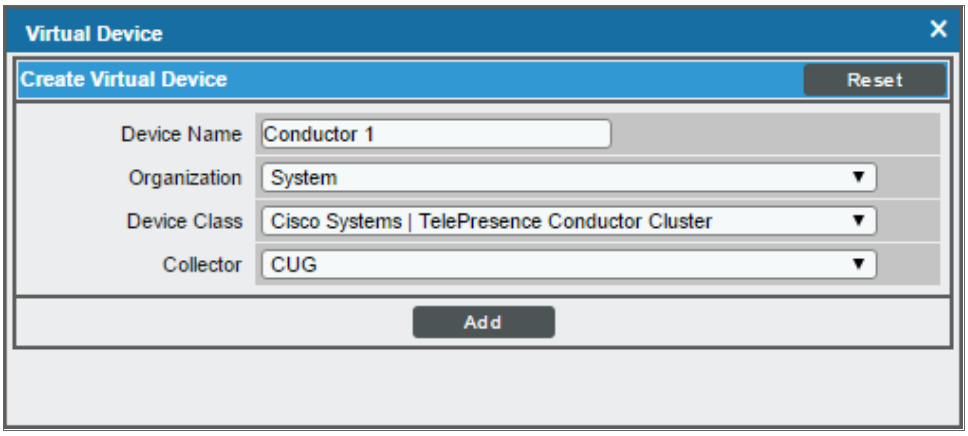
For Conductor cluster configurations, ScienceLogic recommends that you use a virtual device to represent the cluster.

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 model and monitor Cisco TelePresence Conductor using a virtual device to represent the cluster, you must first create the virtual device and then manually align the "Cisco: TelePresence Conductor Discovery" Dynamic Application to the virtual device. When you do so, SL1 discovers the cluster first, and then automatically aligns the other Dynamic Applications in the "Cisco: TelePresence Conductor Discovery" PowerPack to the cluster virtual device. These additional Dynamic Applications discover, model, and monitor the remaining Conductor component devices.

To create a virtual device that represents your TelePresence Conductor cluster:

1. Go to the **Device Manager** page (Devices > Classic Devices, 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:

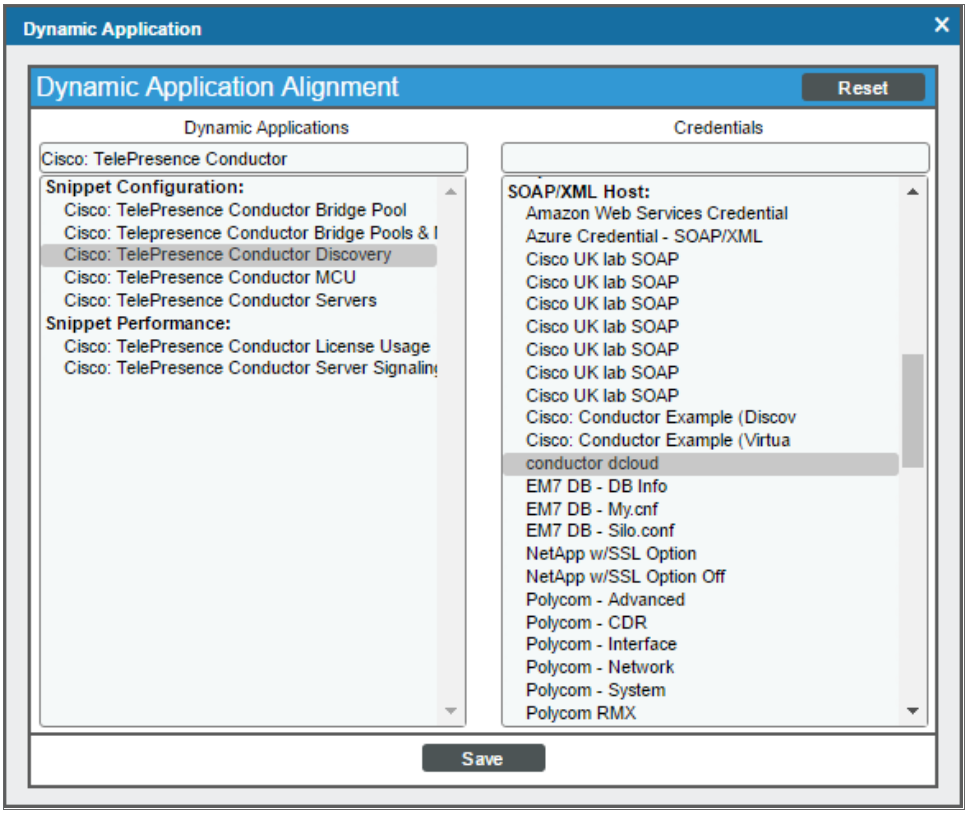


   - ***Device Name***. Enter a name for the virtual device. For example, you could enter "Conductor Cluster" in this field.
   - ***Organization***. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization can view and edit the device.
   - ***Device Class***. Select *Cisco Systems | TelePresence Conductor Cluster*.
   - ***Collector***. Select the collector group to monitor the cluster.
4. Click the **[Add]** button to create the virtual device.

After creating the Conductor cluster virtual device, you must manually align the *Cisco: TelePresence Conductor Discovery* Dynamic Application with the virtual device. To do so, perform the following steps:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface).
2. Click the wrench icon ( ) for your Conductor cluster 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, enter values in the following fields:



- ***Dynamic Applications***. Select the *Cisco: TelePresence Conductor Discovery* Dynamic Application.
- ***Credentials***. Select the SOAP/XML credential you created for the Conductor devices.

6. Click the **[Save]** button to align the Dynamic Application with the Conductor cluster virtual device.

Discovering IP Devices

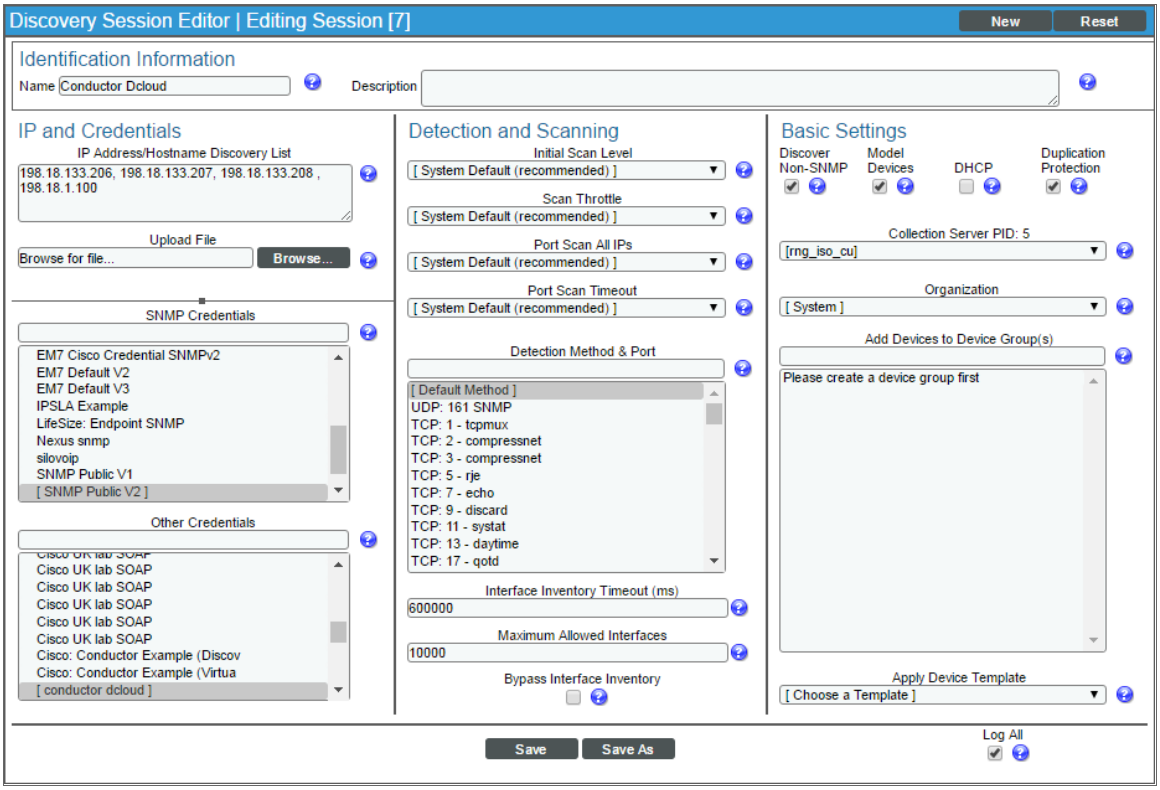
To model and monitor Cisco TelePresence Conductor IP devices, you must run a discovery session to discover a Conductor root device.

Several minutes after the discovery session completes, the Dynamic Applications in the "Cisco: TelePresence Conductor Discovery" PowerPack automatically align to the Conductor root device and then discover, model, and monitor the remaining Conductor component devices.

To discover the Cisco TelePresence Conductor devices that you want to monitor, perform the following steps:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery or System > Manage > Discovery in the classic user interface).
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***. Enter the IP address(es) for the Conductor root device(s) you want to discover.
- ***SNMP Credentials***. If the devices are SNMP-enabled, select the SNMP credential you created for the Conductor devices.
- ***Other Credentials***. Select the SOAP/XML credential you created for the Conductor devices.
- ***Discover Non-SNMP***. Select this checkbox.
- ***Model Devices***. Select this checkbox.

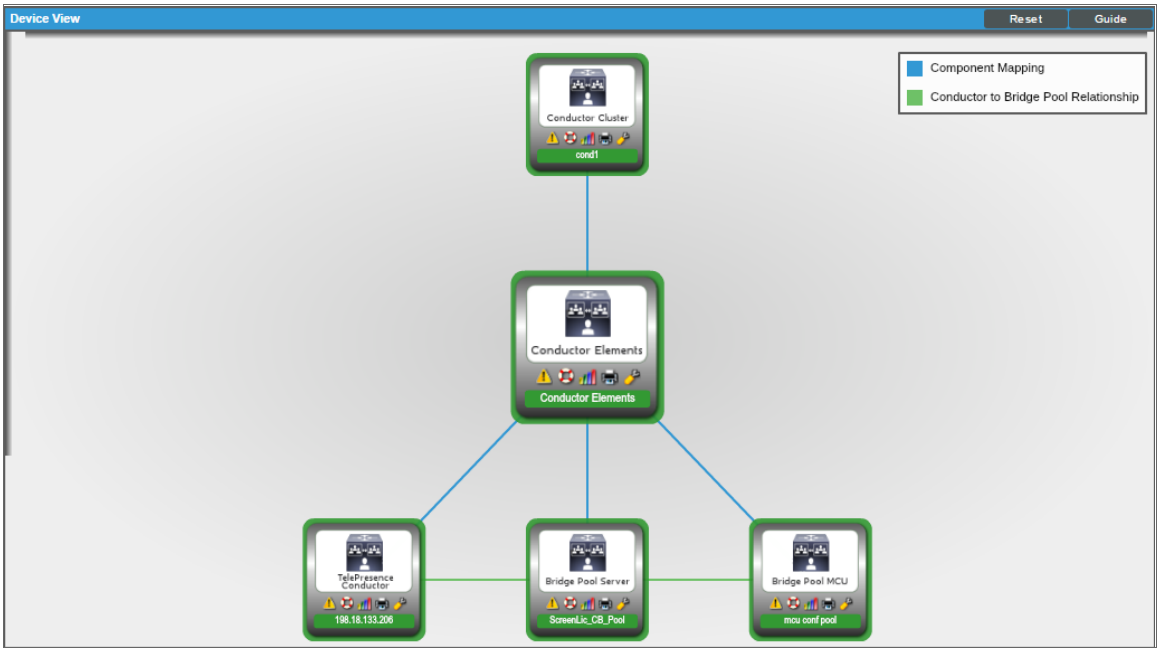
4. Optionally, you can enter values in the other fields on this page. For more information about the other fields on this page, see the ***Discovery & Credentials*** manual.
5. Click the **[Save]** button to save the discovery session and then close the **Discovery Session Editor** window.
6. The discovery 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. When the Conductor root device is discovered, click the device icon ( ) to view the **Device Properties** page for the root device.

Viewing Cisco TelePresence Conductor Devices

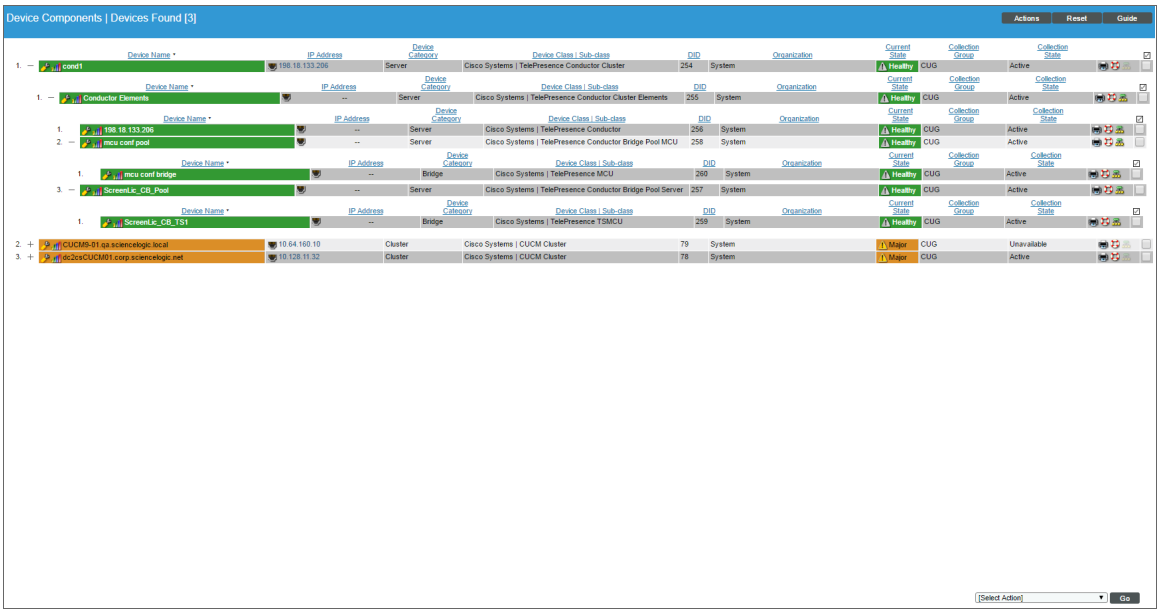
When SL1 discovers your TelePresence Conductor devices, SL1 will create component devices that represent each component in your Conductor cluster.

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

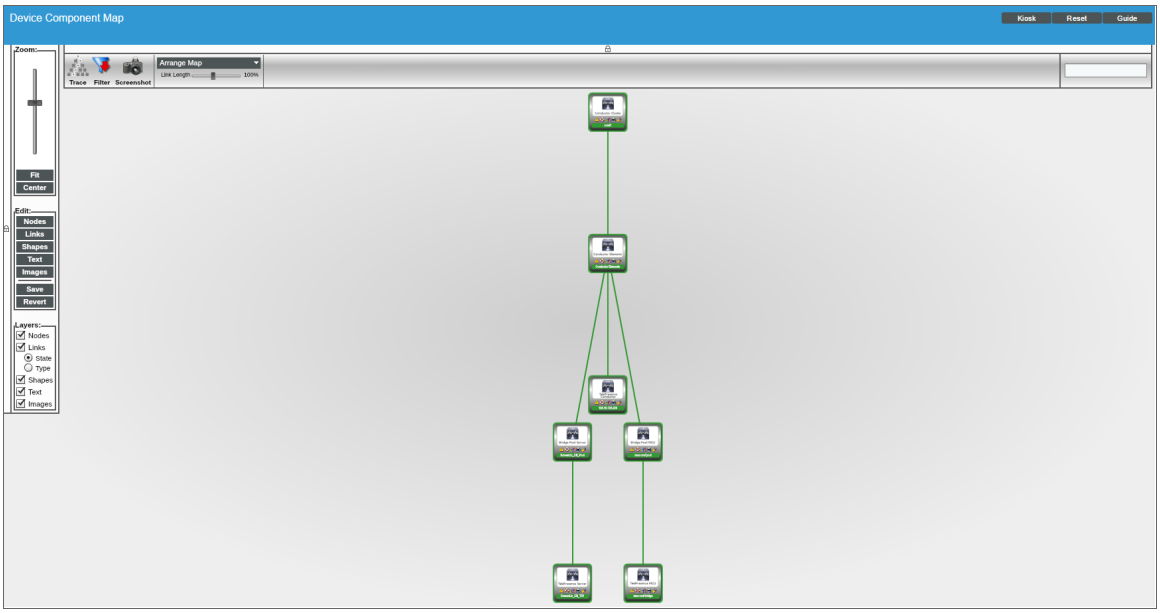
- The **Device View** modal page (click the bar-graph icon [ ]for a device, then click the **Topology** tab) displays a map of the selected device and all of the devices with which it has parent-child relationships. Double-clicking any of the devices reloads the page with the selected device as the primary device:



- The **Device Components** page (Devices > Device Components) displays a list of all root devices and component devices discovered by SL1, in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with your Conductor cluster, find a cluster 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 your Conductor cluster, 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 7

Monitoring LifeSize Endpoints

Overview

The following sections describe how to configure LifeSize endpoints for monitoring by SL1 using the *LifeSize Endpoint* PowerPack:

This chapter covers the following topics:

Configuring LifeSize Endpoints for Monitoring by SL1 ..... *53*

Creating an SNMP Credential for a LifeSize Endpoint *54*

Configuring LifeSize Endpoints for Monitoring by SL1

SL1 uses SNMP Dynamic Applications to collect the following information from the LifeSize Endpoint SNMP agent:

- LifeSize: Active Call Details
- LifeSize: Audio/Video Settings
- LifeSize: Call Quality Statistics
- LifeSize: Configuration
- LifeSize: Remote Management

Each of these Dynamic Applications includes a discovery object. If you discover your LifeSize Endpoints as SNMP devices, SL1 will automatically align these Dynamic Applications to those Endpoints during discovery.

LifeSize Endpoints support SNMP v3 only. Instead of specifying a community string, SNMP v3 uses a username, password, and other optional security phrases.

To verify that the SNMP agent is running on a LifeSize Endpoint and to configure an SNMP v3 username on a LifeSize Endpoint:

1. Connect to the LifeSize Endpoint using an SSH client as the "auto" user. LifeSize Endpoints have SSH enabled by default. The default password for the "auto" user is "lifesize".
2. The SNMP agent is enabled by default on all LifeSize endpoints. To verify that the SNMP agent is enabled, execute the following command:

   ```
   get snmp enable
   ```

   If the SNMP agent is enabled, you will see the following message:

   ```
   on

   ok,00
   ```

3. If the SNMP agent is disabled, execute the following command to enable the SNMP agent:

   ```
   set snmp enable on
   ```

4. To create an SNMP v3 user, execute the following command, substituting *username* and *password* with the username and password for the user:

   ```
   set snmp user -a username password
   ```

   When you create an SNMP credential in SL1 for this LifeSize Endpoint, you will enter the username in the ***Security Name*** field and the password in the ***Security Passphrase*** field.

5. Optionally, you can execute the following two commands to change the SNMP system contact and SNMP system location. Substitute *system_contact* and *system_location* with the system contact and system location you want to assign to this device:

   ```
   set snmp contact system_contact

   set snmp location system_location
   ```

> **NOTE:** If the system contact or system location value you want to assign to this device includes a space, you must enclose the value in double quotes (").

Creating an SNMP Credential for a LifeSize Endpoint

To create an SNMPv3 Credential for a LifeSize Endpoint, perform the following steps in SL1:

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

2. Select the **[Create]** button, and then select *SNMP Credential*. The **Credential Editor** page is displayed.
3. Supply values in the following fields:
    - ***Profile Name***. Enter a name for the credential.
    - ***SNMP Version***. Select *SNMP V3*.
    - ***Security Name***. Enter the SNMP v3 username you configured on the LifeSize Endpoint.
    - ***Security Passphrase***. Enter the SNMP v3 password you configured on the LifeSize Endpoint.

> **NOTE:** You can optionally change the values in the ***Timeout(ms)*** and ***Retries*** fields. You must leave all other fields in this page set to the default value.

4. Select the **[Save]** button.
5. When you configure a discovery session that includes the IP address of the LifeSize Endpoint, select the SNMP v3 credential you created in the ***SNMP Credentials*** field. The LifeSize Endpoint will be discovered as an SNMP device with the LifeSize Dynamic Applications automatically aligned. For more information about discovery in SL1, see the ***Discovery and Credentials*** manual.

Chapter 8

Monitoring Poly HDX and VSX Series Endpoints

Overview

The following sections describe how to configure Poly HDX and VSX Series endpoints for monitoring by SL1 using the "Poly Endpoint" PowerPack:

This chapter covers the following topics:

Configuring Poly Endpoints for Monitoring by SL1 56

Creating an SNMP Credential 59

Configuring SOAP/XML Credentials 65

Dynamic Applications for Poly Endpoints 69

Configuring Poly Endpoints for Monitoring by SL1

SL1 uses two protocols for monitoring Poly Endpoints: SNMP and HTTP. Poly Endpoints respond to HTTP requests that use the "admin" username and the room password that was configured using the initial Setup Wizard on the device. The default room password for the "admin" user is the 14-digit serial number of the system.

This section will describe how to:

- Configure a new room password the "admin" user.
- Configure SNMP on a Poly Endpoint.

This section describes how to perform these tasks remotely from the web interface on a Poly Endpoint. To perform these tasks, you must know the current ***room password*** for the "admin" user on the device.

NOTE: These instructions assume that the Poly Endpoint has been assigned an IP address and is visible to a Data Collector on the network.

To log in to the web interface on a Poly Endpoint, perform the following steps:

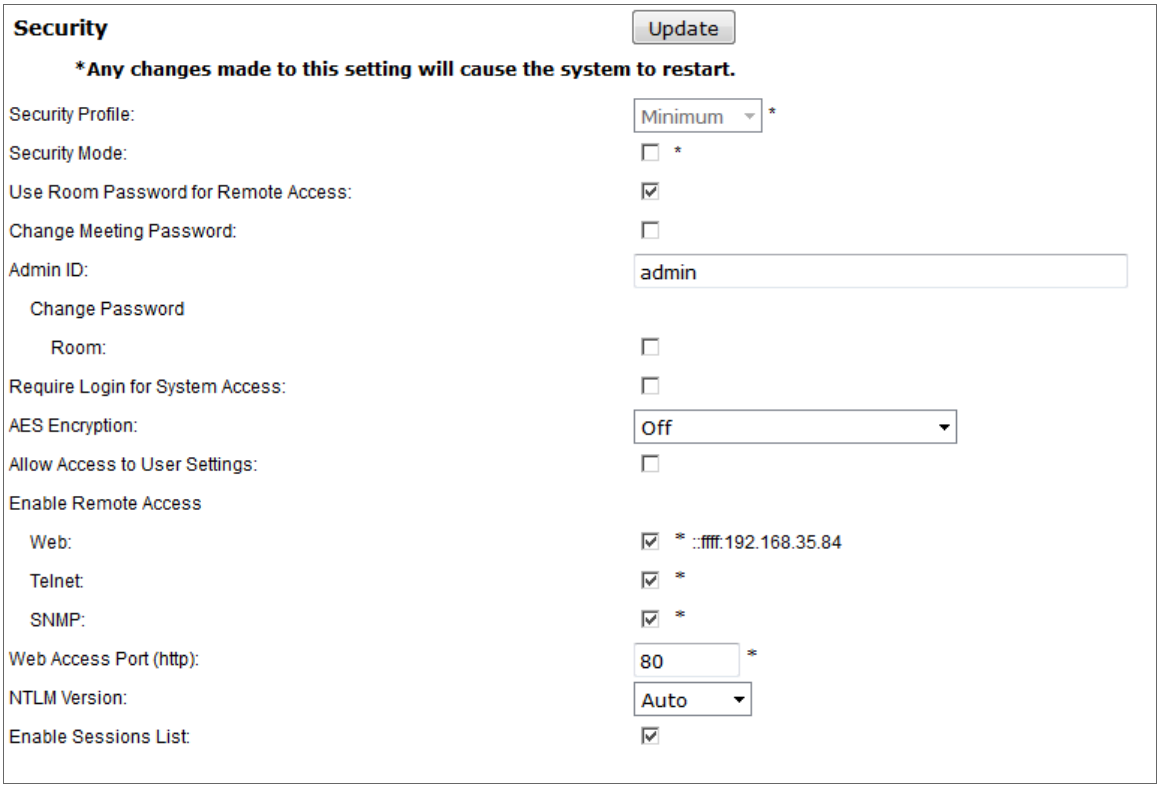
1. In a browser window, go to the IP address of the Poly Series Endpoint. The **Poly Welcome** page appears:

2. Click **[Admin Settings]** on the top navigation bar. You will be prompted for a username and password. In the username field, enter "admin". In the password field, enter the room password for the admin user. The default room password for the "admin" user is the 14-digit serial number of the system. Click the **[OK]** button.

If you want to change the password that SL1 will use to perform HTTP requests on this device, perform the following steps:

> **CAUTION:** Entering a new password will change the password for all administrators of this device that use the "admin" user.

1. In the left navigation bar, click General Settings > Security > Security Settings. The Security page appears:

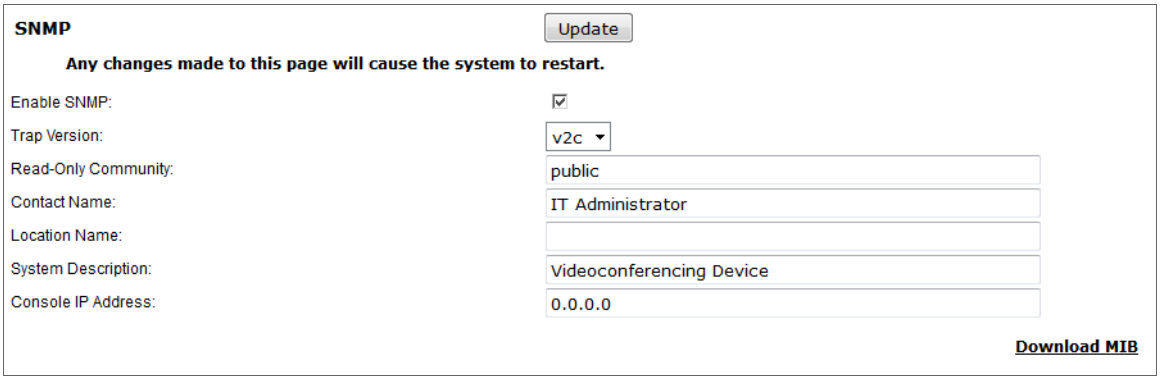


2. Select the ***Change Password - Room*** checkbox.
3. Supply values in the following fields:
   - ***Current Password***. Type the current room password for the "admin" user.
   - ***New Password***. Type the new password for the "admin" user.
   - ***Confirm Password***. Re-type the new password for the "admin" user.
4. Click the **[Update]** button.

To configure the SNMP settings on a Poly HDX or VSX Series Endpoint, perform the following steps:

> **CAUTION:** The device will automatically restart after you perform these steps.

1. In the left navigation bar, click Global Services > SNMP. The SNMP page appears:



2. Supply values in the following fields:
   - ***Enable SNMP***. Ensure that this checkbox is selected.
   - ***Trap Version***. Select *v2c* in this field.
   - ***Read-Only Community***. Type the new SNMP community string for this device. When you configure an SNMP credential for this Poly Endpoint in SL1, you will enter this community string in the ***SNMP Community (Read-Only)*** field.
   - ***Contact Name***. Optionally, type the contact information for the administrator of this device.
   - ***Location Name***. Optionally, type the location of this device.
   - ***System Description***. Type a description of this device
   - ***Console IP Address***. Type the IP address of the Message Collection Unit or Data Collection Unit that will collect SNMP trap messages from the device.
3. Click the **[Update]** button to save the new SNMP settings. The device will automatically restart.

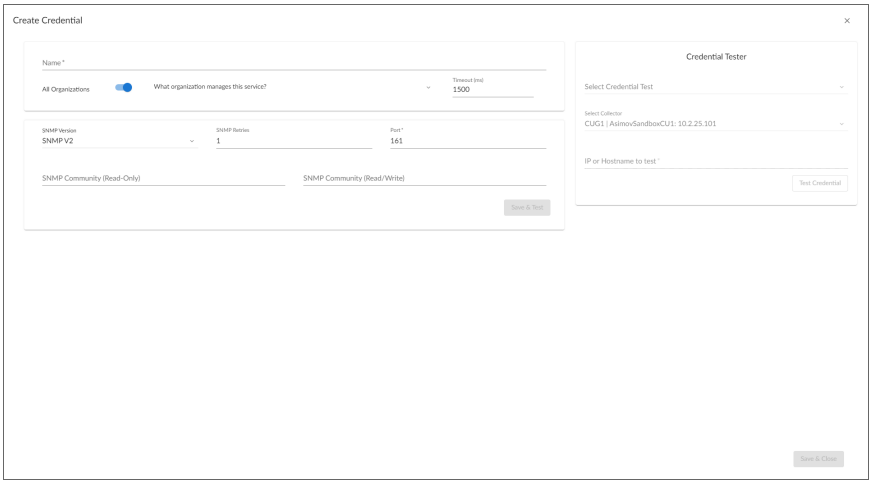
Creating an SNMP Credential

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.

Creating an SNMPv2 Credential

To create an SNMPv2 credential:

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



3. Supply values in the following fields:
    - ***Name***. Name of the credential. Can be any combination of alphanumeric characters, up to 64 characters. This is a required field.
    - ***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. This field is required.

NOTE: To learn more about credentials and organizations, see the section *Aligning Organizations With a Credential*.

- ***Timeout (ms)***. Time, in milliseconds, after which SL1 will stop trying to communicate with the device. The default value is *1500*.
- ***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*. This field is required.
- ***SNMP Retries***. Number of times SL1 will try to authenticate and communicate with the external device. The default value is *1*.

SNMP V1/V2 Settings

If you selected *SNMP V1* or *SNMP V2* in the ***SNMP Version*** field, complete these fields. These 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.

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.

Creating an SNMPv2 Credential in the Classic User Interface

To monitor Poly Endpoints in SL1, you will need to create an SNMP Credential for each Endpoint.

To create an SNMP Credential for a Poly Endpoint, perform the following steps in SL1:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the **[Create]** button, and then select *SNMP Credential*. The **Credential Editor** page appears.
3. Supply values in the following fields:
   - ***Profile Name***. Type a name for the credential.
   - ***SNMP Version***. Select *SNMP V2*.
   - ***SNMP Community (Read-Only)***. Type the SNMP Read-Only community string you configured on the Poly Endpoint.

> **NOTE:** You can optionally change the values in the ***Timeout (ms)*** and ***Retries*** fields.

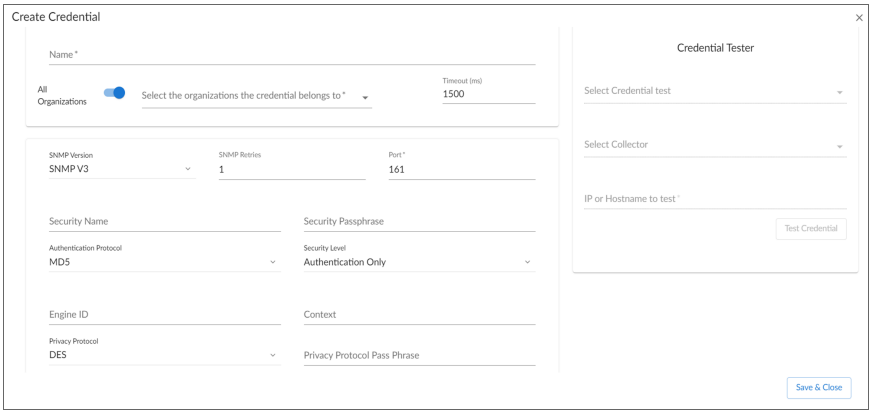
4. Click the **[Save]** button.
5. When you configure a discovery session that includes the IP address of the Poly Endpoint, select the SNMP credential you created in the ***SNMP Credentials*** field. For more information about discovery, see the ***Discovery and Credentials*** manual.

Creating an SNMPv3 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 SNMPv3 credential:

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



3. Supply values in the following fields:
    - ***Name***. Name of the credential. Can be any combination of alphanumeric characters, up to 64 characters. This is a required field.
    - ***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. This field is required.

NOTE: To learn more about credentials and organizations, see the section *Aligning Organizations With a Credential*.

- ***Timeout (ms)***. Time, in milliseconds, after which SL1 will stop trying to communicate with the device. The default value is *1500*.
- ***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*. This field is required.
- ***SNMP Retries***. Number of times SL1 will try to authenticate and communicate with the external device. The default value is *1*.

SNMP V3 Settings

If you selected *SNMP V3* in the ***SNMP Version*** field, complete these fields. 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.

In addition to alphanumeric characters, you ***can*** also use the following special characters in an SNMP V3 security passphrase: ? - _ = , . : # + % $ [ ] { } & ! ( ) | /

You ***cannot*** use the following special characters in an SNMP V3 security passphrase: " ' \

- ***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*.
- ***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***. 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*
  - *AES-256-C*. This option is for discovering Cisco devices only.
- ***Privacy Protocol Passphrase***. Privacy password for the credential. This field is optional.

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

Creating an SNMP v3 Credential in the Classic User Interface

To monitor Poly Endpoints in SL1, you will need to create an SNMP Credential for each Endpoint.

To create an SNMP Credential for a Poly Endpoint, perform the following steps in SL1:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the **[Create]** button, and then select *SNMP Credential*. The **Credential Editor** page appears.
3. Supply values in the following fields:
    - ***Profile Name***. Type a name for the credential.
    - ***SNMP Version***. Select *SNMP V3*.
    - ***SNMP Community (Read-Only)***. Type the SNMP Read-Only community string you configured on the Poly Endpoint.

NOTE: You can optionally change the values in the ***Timeout (ms)*** and ***Retries*** fields.

4. Click the **[Save]** button.
5. When you configure a discovery session that includes the IP address of the Poly Endpoint, select the SNMP credential you created in the ***SNMP Credentials*** field. For more information about discovery, see the ***Discovery and Credentials*** manual.

Performing Bulk Retrieval Using SNMPv3

The `snmpbulkwalk` command is used to perform a bulk retrieval of SNMP data from a device using SNMPv3. You can use this command for device discovery and inventory tasks in network management, as it efficiently gathers detailed information from network devices.

At the shell prompt, run the following command:

```
snmpbulkwalk -v3 -n <context> -l authPriv -u <security_name> -a
<authentication_protocol> -A <security_passphrase> -x <privacy_protocol> -X
<privacy_protocol_pass_phrase> -ObentU <device_ip> .1 > device.walk
```

- `-v3`: Specifies the SNMP version (v3).
- `-n <context>`: Specifies the context name for SNMPv3 (optional, typically used in multi-context environments).
- `-l authPriv:` : Specifies the security level. `authPriv` means both authentication and encryption (privacy) are used.
- `-u <security name>`: Specifies the username for SNMPv3.
- `-a <authentication protocol>`: Specifies the authentication protocol (e.g., MD5 or SHA).
- `-A <security_passphrase>`: Specifies the passphrase for authentication.
- `-x <privacy_protocol>`: Specifies the privacy (encryption) protocol (e.g., DES, AES).
- `-X <privacy_protocol_pass_phrase>`: Specifies the passphrase for the privacy protocol.

- `-ObentU`: Specifies options to format the output, such as showing numeric OIDs (-O), and excluding the leading dot from OIDs (-Ob).
- `<device_ip>`: Specifies the IP address of the device to query.
- `.1`: Indicates that the SNMP walk should start from the root of the MIB tree.
- `>device.walk`: Redirects the output to a file named *device.walk*.

Configuring SOAP/XML Credentials

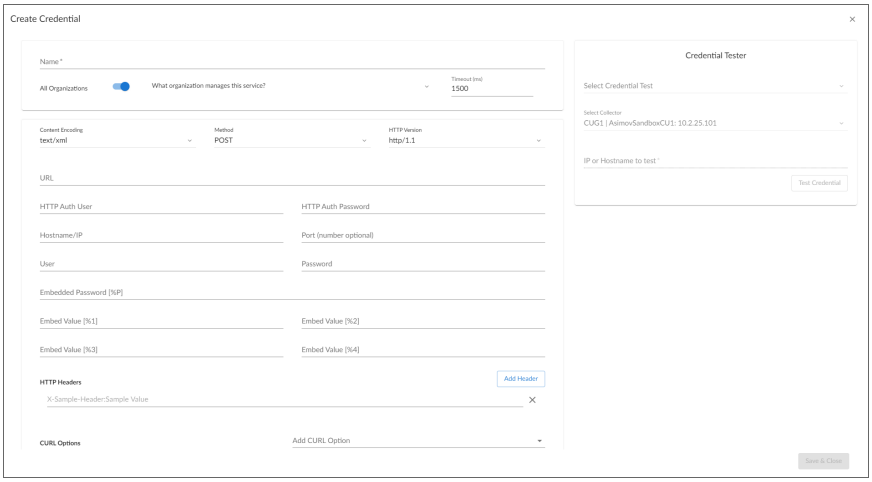
SOAP/XML credentials allow SL1 to access a web server on a managed device. SOAP/XML credentials are used in several places in SL1, including:

- ***With Dynamic Applications of type "SOAP"***.
- ***With Dynamic Applications of type "XML"***.
- ***With Dynamic Applications of type "XSLT"***.
- ***With Dynamic Applications of type "snippet"***. The snippet code must define the authentication protocol. Dynamic Applications of type "snippet" can use any type of credential.

Creating SOAP/XML Credentials

To create a SOAP/XML credential:

1. Go to the **Credentials** page (Manage > Credentials).
2. Click the **[Create New]** button and then select *Create SOAP/XML Credential*. The **Create Credential** modal page appears:



3. Supply values in the following fields:
    - ***Name***. Name of the credential. Can be any combination of alphanumeric characters, up to 64 characters. This field is required.

- ***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. This field is required.

NOTE: To learn more about credentials and organizations, see the section *Aligning Organizations With a Credential*.

- ***Timeout (ms)***. Time, in milliseconds, after which SL1 will stop trying to communicate with the web service.
- ***Content Encoding***. Tells the SOAP server or XML data-store how the content is encoded, so the SOAP server or XML data-store knows how to decode the message. Select the encoding that is appropriate for your request and response.
- ***Method***. HTTP method to use to exchange credential data from the managed device. Choices are *GET* or *POST*.

NOTE: Typically, Dynamic Applications of type "XML" use GET methods. Dynamic Applications of type "SOAP" and of type "XSLT" use POST methods.

- ***HTTP Version***. Version of HTTP to use. Choices are *1.0* or *1.1*.
- ***URL***. Address of the SOAP server, HTML document, or XML document. This field is required and should be of the following format:

  https://IP address:port/full path to desired SOAP, HTML, or XML document

NOTE: The port is stored if it is specified in the URL; otherwise, SL1 uses the default port values 80 for HTTP and 43 for HTTPS.

  - You can include the variable **%D** in this field. SL1 will replace the variable with the IP address of the current device (device that is currently using the credential).

NOTE: For component devices, SL1 will replace %D with the IP address of the root device.

  - You can include the variable **%N** in this field. SL1 will replace the variable with the hostname of the current device (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 current device.

- ***HTTP Auth User***. Username with which to log in to the web server.
- ***HTTP Auth Password***. Password with which to access the web server.

Proxy Settings

If you use a proxy server in front of the SOAP server(s) or XML data-store(s) you want to communicate with, enter values in these fields. Otherwise, you can skip these fields.

- ***Hostname/IP***. The host name or IP address of the proxy server.
- ***Port***. Port on the proxy server to which you will connect.
- ***User***. Username to use to access the proxy server.
- ***Password***. Password to use to access the proxy server.

SOAP Options

These fields are optional. When a SOAP/XML credential is aligned with a SOAP or XSLT Dynamic Application, the requests defined in the Dynamic Application can use the values defined in these fields. To use a value defined in one of these fields, the request must include the substitution character associated with that value. For example, suppose a Dynamic Application request includes the XML tag <high_value=%1>. Suppose you specified "100" in the ***Embed Value [%1]*** field in the credential aligned with that Dynamic Application. The request will be sent with the XML tag <high_value=100>.

- ***Embedded Password [%P]***. Specifies a password value to include in a request. The value defined in this field is substituted in to the %P substitution character. The value will be encrypted in the request, will be masked in the **Credential Editor**, and will be stored in an encrypted form in the database.
- ***Embed Value [%1]***. The value defined in this field is substituted in to the %1 substitution character.
- ***Embed Value [%2]***. The value defined in this field is substituted in to the %2 substitution character.
- ***Embed Value [%3]***. The value defined in this field is substituted in to the %3 substitution character.
- ***Embed Value [%4]***. The value defined in this field is substituted in to the %4 substitution character.

HTTP Headers

- If you require custom HTTP headers to communicate with the SOAP server, you can build the custom header here. To add a header, click the **[Add Header]** button

cURL Options

- You can include the cURL command and various options in your credential. The list of cURL options lists all the options you can include in your credential. To include a cURL option in the credential, click the ***Add CURL Option*** drop-down and then select it from the list. You can then supply arguments in the blank text field to the right of the option.
- For more information on cURL commands, see the cURL manpage at http://curl.haxx.se/docs/manpage.html.

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.

Creating SOAP/XML Credentials in the Classic User Interface

To use the Dynamic Applications in the Poly Endpoint PowerPack, you must configure five SOAP/XML credentials for your Poly device. The five credentials are:

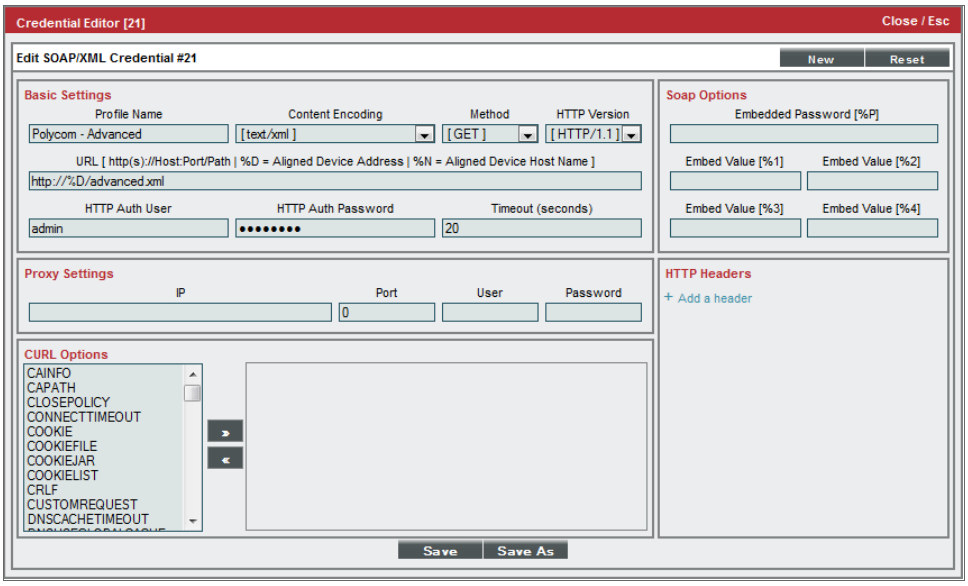
- Poly - Advanced
- Poly - Interface
- Poly - Network
- Poly - System
- Poly CDR

These credentials enable SL1 to monitor and collect call detail records for Poly Endpoints using unique combinations of URL, username, and password.

If you have multiple Poly Endpoints, you will need one set of credentials for each unique room password for the "admin" user. For example, if you have configured three Poly Endpoints with the same room password for the "admin" user, you need only one set of credentials.

To modify the templates, perform the following steps:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the wrench icon ( ) for the "Poly - Advanced" credential. The **Credential Editor** modal window appears:



3. In the ***Profile Name*** field, type a new name for the credential.
4. In the ***HTTP Auth Password*** field, type the room password you configured for the "admin" user on the Poly Endpoint.
5. Click the **[Save As]** button.

6. Repeat steps 2 - 5 for the following credentials:
    - Poly - CDR
    - Poly - Interface
    - Poly - Network
    - Poly - System

Dynamic Applications for Poly Endpoints

The *Poly Endpoint* PowerPack contains 13 Dynamic Applications that can be used to monitor Poly Endpoints and Group Series (GS) devices. Some of the Dynamic Applications for Poly Endpoints use the caching feature:

- Four Dynamic Applications are used only to collect and cache data from Poly Endpoints.
- Three Dynamic Applications use the cached data. For these Dynamic Applications to display data, the Dynamic Applications that collect and cache data must be aligned to the same device.

Six Dynamic Applications for Poly Endpoints and GS devices do not use the caching feature.

The Dynamic Applications in the "Poly Endpoint" PowerPack include discovery objects. If you discover your Poly Endpoint as an SNMP device and include all the SOAP/XML credentials you configured for your Poly Endpoint in the ***Other Credentials*** field in the **Discovery Session Editor** page, SL1 will automatically align the Dynamic Applications from the "Poly Endpoint" PowerPack to your Poly Endpoint. However, the Dynamic Applications in the "Poly Endpoint" PowerPack might take a significant amount of time to align with Poly devices during discovery. If you are discovering multiple Poly Endpoints or your Poly Endpoints take several seconds to respond to HTTP requests, ScienceLogic recommends that you do not include SOAP/XML credentials in the discovery session.

If you do not include SOAP/XML credentials in the discovery session for your Poly endpoints, you can manually align the Poly Dynamic Applications using a device template. To create a device template for a Poly Endpoint, perform the following steps:

1. Go to the **Configuration Templates** page (Devices > Templates, or Registry > Devices > Templates in the classic SL1 user interface).
2. Click the **[Create]** button. The **Template Editor** page appears.
3. Type a name for your device template in the ***Template Name*** field.
4. Click the **[Dyn Apps]** tab.
5. For each Dynamic Application listed in the table below:
    - Select *Add New Dynamic App Sub-Template*.
    - Select the Dynamic Application in the ***Dynamic Application*** field.
    - Click the ***Credentials*** field, then select the credential listed for the Dynamic Application in the table below.
6. Click the **[Save]** button.

If your discovery session includes IP addresses for only Poly Endpoints, you can apply the device template to all devices discovered by that discovery session. To apply a device template to all devices discovered by a discovery session, select the device template in the ***Apply Device Template*** field in the **Discovery Session Editor** page.

If your discovery session includes IP addresses for other types of devices in addition to Poly Endpoints, you can apply the device template to your Poly Endpoints after discovery in the **Device Manager** page. To do this:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface).
2. Select the checkbox for each Poly Endpoint.
3. In the ***Select Action*** drop-down list, select *Modify By Template* and then click the **[Go]** button. The **Bulk Device Configuration** modal page appears.
4. Select the device template in the ***Template*** field.
5. Click the **[Apply]** button.
6. In the confirmation page that appears, click the **[Confirm]** button.

The following table lists the Dynamic Applications in the "Poly Endpoint" PowerPack, the dependencies between the caching and cache consuming Dynamic Applications, and the credential that must be aligned with each Dynamic Application:

Dynamic Application	Credential	Caching Type	Dependencies
Poly: Active Call	N/A	Consumes Cache	Poly: Cache Network
Poly: Cache Advanced	Poly - Advanced	Populates Cache	N/A
Poly: Cache Interface	Poly - Interface	Populates Cache	N/A
Poly: Cache Network	Poly - Network	Populates Cache	N/A
Poly: Cache System	Poly - System	Populates Cache	N/A
Poly: Call Detail Records	Poly CDR	No Caching	N/A
Poly: Call Quality Statistics	N/A	Consumes Cache	Poly: Cache Network and Poly: Cache Advanced
Poly: Configuration	N/A	Consumes Cache	Poly: Cache System and Poly: Cache Interface
Poly: SNMP Configuration	SNMP Credential for Device	No Caching	N/A
Poly GS: Active Call	SNMP Credential for Device	No Caching	N/A
Poly GS: Asset and Network Service	SNMP Credential for Device	No Caching	N/A
Poly GS: Call Quality	SNMP Credential for Device	No Caching	N/A
Poly GS: Status	SNMP Credential for Device	No Caching	N/A

Chapter 9

Monitoring Tandberg Infrastructure

Overview

The following sections describe how to configure Cisco Tandberg infrastructure devices for monitoring by SL1 using the *Tandberg: Infrastructure* PowerPack:

This chapter covers the following topics:

Tandberg Infrastructure Support *71*

Creating a Credential for Tandberg Infrastructure Dynamic Applications *74*

Creating a Credential for TelePresence Content Server *75*

Video Communication Server *76*

TelePresence Server *83*

TelePresence Control Unit *88*

Tandberg Infrastructure Support

The following table lists the devices that can be monitored using the Dynamic Applications in the *Tandberg: Infrastructure* PowerPack. For each device type, the table lists:

- The credential to use for the device. The credential to use will either be the generic credential for Tandberg Infrastructure devices or a specific credential for that device type. The credential field for each device links to the section in this chapter that describes how to create the credential.
- The Dynamic Applications in the *Tandberg: Infrastructure* PowerPack that can be used to monitor the device.

Product Family	Products	Credential	Dynamic Application
MCU 4200 Series	4205 4210 4215 4220 8420 (blade)	*Generic*	• Tandberg: Codian MCU Configuration • Tandberg: Codian Performance • Tandberg Codian Status • Tandberg: Codian MCU CDR Participants Log • Tandberg: Codian MCU CDR Conference Log
MCU 4500 Series	4501 4505 4510 4515 4520 8510 (blade)	*Generic*	• Tandberg: Codian MCU Configuration • Tandberg Codian Status • Tandberg: Codian Performance • Tandberg: Codian MCU CDR Participants Log • Tandberg: Codian MCU CDR Conference Log
ISDN Gateways	3210 3220 3240 3280 8321 (blade)	*Generic*	• Tandberg: Codian Performance • Tandberg Codian Status • Tandberg: Codian ISDN Gateway Call Details
IP Gateways	4510 3520 3540 8350 (blade)	*Generic*	• Tandberg: Codian Status • Tandberg Codian Performance
Media Gateway	3610	*Generic*	• Tandberg Codian Status • Tandberg: Codian Performance
IP VCR	2210 2220 2240 8220 (blade)	*Generic*	• Tandberg: Codian Status • Tandberg: Codian Performance

Product Family	Products	Credential	Dynamic Application
Codian Supervisor	8050 (blade)	*Generic*	• Tandberg: Codian MSE Supervisor Configuration • Tandberg: Codian MSE Supervisor Performance
TelePresence Content Server	TCS	Specific - see *TelePresence Content Server* section.	• Tandberg: TCS Status • Tandberg: TCS Configuration • Tandberg: TCS Performance • Tandberg: TCS Cluster Node Performance • Tandberg: TCS System Health
Video Communication Server	VCS-Expressway VCS-Control	Specific - see *Video Communication Server* section.	• Tandberg: VCS Configuration • Tandberg: VCS Status • Tandberg: VCS Call Details • Tandberg: VCS Registration Status
TelePresence Server	MSE 8710 TelePresence Server 7010	Specific - see *TelePresence Server* section.	• Tandberg: Codian TS Port Utilization • Tandberg: Codian TS Configuration • Tandberg: Codian TS Conference Details • Tandberg: Codian TS Participant Details • Tandberg: Codian TS Status
TelePresence Control Unit	TCU	Specific - see *TelePresence Control Unit* section.	• Tandberg: TCU Configuration • Tandberg: TCU Status

Creating a Credential for Tandberg Infrastructure Dynamic Applications

For Tandberg infrastructure devices that use the generic credential, you will need to create a SOAP/XML credential to align with the Dynamic Applications for that device.

To create a SOAP/XML for Tandberg infrastructure devices:

1. Using the manufacturer's instructions, determine the username and password that can be used to access the web service on the device.
2. Go to the **Credentials** page (Manage > Credentials).
3. In the **Credential Management** page, select the **[Create]** menu. Select *SOAP/XML Host Credential*.
4. The **Credential Editor** page appears. Enter 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 ***Select the organizations the credential belongs to*** drop-down field to align the credential with those specific organizations.
    - ***Timeout (seconds)***. Enter the time, in seconds, after which you want the platform to stop trying to communicate with the web server.
    - ***URL***. Enter "http://%D/rpc2". The variable **%D** will be replaced with the IP address of the current device that is using the credential.
    - ***HTTP Auth User***. Enter your username with which you log in to the web server.
    - ***HTTP Auth Password***. Enter the password with which you access the web server.
5. The remaining fields in the **Credential Editor** page can be left blank or at their default settings.
6. Select the **[Save]** button to save the credential.

Creating a Credential for Tandberg Infrastructure in the SL1 Classic User Interface

For Tandberg infrastructure devices that use the generic credential, you will need to create a SOAP/XML credential to align with the Dynamic Applications for that device.

To create a SOAP/XML for Tandberg infrastructure devices:

1. Using the manufacturer's instructions, determine the username and password that can be used to access the web service on the device.
2. Go to the **Credential Management** page (System > Manage > Credentials).
3. In the **Credential Management** page, select the **[Create]** menu. Select *SOAP/XML Host Credential*.
4. The **Credential Editor** page appears. Enter values in the following fields:
    - ***Profile Name***. Name of the credential. Can be any combination of alphanumeric characters.

- ***URL***. Enter "http://%D/rpc2". The variable **%D** will be replaced with the IP address of the current device that is using the credential.
- ***HTTP Auth User***. Enter your username with which you log in to the web server.
- ***HTTP Auth Password***. Enter the password with which you access the web server.
- ***Timeout (seconds)***. Enter the time, in seconds, after which you want the platform to stop trying to communicate with the web server.

5. The remaining fields in the **Credential Editor** page can be left blank or at their default settings.
6. Select the **[Save]** button to save the credential.

Creating a Credential for TelePresence Content Server

For the Dynamic Applications that will be aligned with the TelePresence Content Server, you will need to create a SOAP/XML credential to align with the Dynamic Application.

To create the credential:

1. Using the manufacturer's instructions, determine the username and password that can be used to access the web service on the device.
2. Go to the **Credentials** page (Manage > Credentials).
3. In the **Credentials** page, click the **[Create]** menu and then select *SOAP/XML Credential*.
4. The **Create Credentials** page appears. In this page, you will define the credential. Enter 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 ***Select the organizations the credential belongs to*** drop-down field to align the credential with those specific organizations.
    - ***Timeout (seconds)***. Type the time, in seconds, after which you want SL1 to stop trying to communicate with the web server.
    - ***URL***. Type the URL that corresponds to the Dynamic Application. The variable **%D** will be replaced with the IP address of the current device that is using the credential. The URL for each Dynamic Application is listed below:
        - *Tandberg: TCS Status*. Type "http://%D/tcs/status.xml" in the ***URL*** field.
        - *Tandberg: TCS Configuration*. Type "http://%D/tcs/configuration.xml" in the ***URL*** field.
        - *Tandberg: TCS Performance*. Type "http://%D/tcs/status.xml" in the ***URL*** field.
        - *Tandberg: TCS Cluster Node*. Type "http://%D/tcs/clusterstatus.xml" in the ***URL*** field.
        - *Tandberg: TCS System Health*. Type "http://%D/tcs/SoapServer.php" in the ***URL*** field.
    - ***HTTP Auth User***. Type your username with which you log in to the web server.
    - ***HTTP Auth Password***. Type the password with which you access the web server.

5. The rest of the fields in the **Create Credentials** page can be left blank or at their default settings.
6. Click the **[Save]** button to save the credential.

Creating a Credential for TelePresence Content Server in the SL1 Classic User Interface

For the Dynamic Applications that will be aligned with the TelePresence Content Server, you will need to create a SOAP/XML credential to align with the Dynamic Application.

To create the credential in the classic user interface:

1. Using the manufacturer's instructions, determine the username and password that can be used to access the web service on the device.
2. Go to the **Credential Management** page (System > Manage > Credentials).
3. In the **Credential Management** page, click the **[Create]** menu and then select *SOAP/XML Host Credential*.
4. The **Credential Editor** page appears. In this page, you will define the credential. Enter values in the following fields:
    - ***Profile Name***. Name of the credential. Can be any combination of alphanumeric characters.
    - ***URL***. Type the URL that corresponds to the Dynamic Application. The variable **%D** will be replaced with the IP address of the current device that is using the credential. The URL for each Dynamic Application is listed below:
        - *Tandberg: TCS Status*. Type "http://%D/tcs/status.xml" in the ***URL*** field.
        - *Tandberg: TCS Configuration*. Type "http://%D/tcs/configuration.xml" in the ***URL*** field.
        - *Tandberg: TCS Performance*. Type "http://%D/tcs/status.xml" in the ***URL*** field.
        - *Tandberg: TCS Cluster Node*. Type "http://%D/tcs/clusterstatus.xml" in the ***URL*** field.
        - *Tandberg: TCS System Health*. Type "http://%D/tcs/SoapServer.php" in the ***URL*** field.
    - ***HTTP Auth User***. Type your username with which you log in to the web server.
    - ***HTTP Auth Password***. Type the password with which you access the web server.
    - ***Timeout (seconds)***. Type the time, in seconds, after which you want SL1 to stop trying to communicate with the web server.
5. The rest of the fields in the **Credential Editor** page can be left blank or at their default settings.
6. Click the **[Save]** button to save the credential.

Video Communication Server

The Video Communication Server (VCS) constitutes two products:

- ***VCS-Control***.
- ***VCS-Expressway***.

These products use the same code base but the VCS-Control product is used for enterprise applications and provides gatekeeper and SIP proxy functionality.

The VCS-Expressway provides two functions:

- Hosting endpoints outside the corporate firewall. This allows work at home users to connect to internal video conferencing equipment without the need for VPN.
- Providing Border Gateway services, which enables B2B video calls.

The VCS-Control and the VCS-Expressway are available as stand-alone appliances that can run as a virtual machine.

Dynamic Applications for VCS Devices

The following Dynamic Applications must be manually aligned to VCS devices:

- *Tandberg: VCS Configuration*. This Dynamic Application collects the following groups of information:
    - *Service Details*. Indicates the status of services like SNMP.
    - *Transform Details*. Shows the transformation rules configured on the system.
    - *Bandwidth Details*. Provides information about bandwidth settings.
    - *Pipe Details*. Provides information about the configured Pipe settings.
    - *Link Details*. Provides information about the configured links.
- *Tandberg: VCS Status*. This Dynamic Application retrieves system-related information such as the following:
    - *System Details*.
    - *Package Details*.
    - *Ethernet Details*.
    - *Features Installed*.
    - *Sip Information*.
    - *H.323 Information*.
- *Tandberg: VCS Call Details*. This Dynamic Application collects details about the calls that VCS processes.
- *Tandberg: VCS Registration Details*. This Dynamic Application provides a list of all the registrations on the VCS and provides historical information about all the registrations that have aged out or the devices unregistered.

Creating a Credential for VCS Devices

For the Dynamic Applications in the "Tandberg: Infrastructure" PowerPack that can be aligned with VCS devices, you will need to create a SOAP/XML credential to align with the Dynamic Application.

To create a credential for VCS devices:

1. Using the manufacturer's instructions, determine the username and password that can be used to access the web service on the device.
2. Go to the **Credentials** page (Manage > Credentials).
3. In the **Credentials** page, click **[Create]** and then select *SOAP/XML Credential*.
4. The **Create Credential** page appears. On this page, you will define the credential. Type values in the following fields:
    - ***Name***. Type a name for the credential. This name 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 ***Select the organizations the credential belongs to*** drop-down field to align the credential with those specific organizations.
    - ***Timeout (seconds)***. For the "Tandberg: VCS Configuration" Dynamic Application, type "10". For the remaining Dynamic Applications, type "5".
    - ***Method***. For VCS systems running version 7.2 and higher, select *GET*. For VCS systems prior to version 7.2, select *POST*.
    - ***HTTP Version***. Leave this field at the default value of *HTTP /1.1*.
    - ***URL***. Type "http://%D/configuration.xml". The variable **%D** will be replaced with the IP address of the current device that is using the credential.
    - ***HTTP Auth User***. Type the username you use to log in to the web server.
    - ***HTTP Auth Password***. Type the password you use to access the web server.
    - ***Embedded Password [%P]***. Enter the embedded password associated with the Couchbase administrator account.
    - ***Embed Value [%1]***. Keep the default.
    - ***HTTP Headers***. If you are using the "Tandberg: VCS Status" sample credential to filter alerts generated by the "Tandberg: VCS Call Details" Dynamic Application, edit the three entries in this pane:
        - *CDRIncludeSourceDomains*. Type a comma-separated list of domains in this field to be filtered by the call's source domain. For example, cisco.call.ciscospark or cisco.call.webex.com. Do not include any colons (:) in the source domains in this field.
        - *CDRIncludeDestinationDomains*. Type a comma-separated list of domains in this field to be filtered by the call's destination domain. For example, cisco.call.ciscospark or cisco.call.webex.com. Do not include any colons (:) in the destination domains in this field.

- *CDRAdditionalCauseCodes*. Type a comma-separated list of additional cause codes to generate alerts on cause codes outside the default range.

> **NOTE:** These fields are optional. If left blank, the "Tandberg: VCS Status" Dynamic Application will generate alerts for calls from all domains, whose cause codes fall in the default range of 500 to 599.

5. The rest of the fields on the **Create Credential** page can be left blank or at their default settings.
6. Click the **[Save]** button to save the credential.

Creating a Credential for VCS Devices in the SL1 Classic User Interface

For the Dynamic Applications in the "Tandberg: Infrastructure" PowerPack that can be aligned with VCS devices, you will need to create a SOAP/XML credential in the classic user interface to align with the Dynamic Application.

To create a credential for VCS devices:

1. Using the manufacturer's instructions, determine the username and password that can be used to access the web service on the device.
2. Go to the **Credential Management** page (System > Manage > Credentials).
3. In the **Credential Management** page, click **[Create]** and then select *SOAP/XML Host Credential*.
4. The **Credential Editor** page appears. On this page, you will define the credential. Type values in the following fields:
   - ***Profile Name***. Type a name for the credential. This name can be any combination of alphanumeric characters.
   - ***Method***. For VCS systems running version 7.2 and higher, select *GET*. For VCS systems prior to version 7.2, select *POST*.
   - ***HTTP Version***. Leave this field at the default value of *HTTP /1.1*.
   - ***URL***. Type "http://%D/configuration.xml". The variable **%D** will be replaced with the IP address of the current device that is using the credential.
   - ***HTTP Auth User***. Type the username you use to log in to the web server.
   - ***HTTP Auth Password***. Type the password you use to access the web server.
   - ***Timeout (seconds)***. For the "Tandberg: VCS Configuration" Dynamic Application, type "10". For the remaining Dynamic Applications, type "5".
   - ***HTTP Headers***. If you are using the "Tandberg: VCS Status" sample credential to filter alerts generated by the "Tandberg: VCS Call Details" Dynamic Application, edit the three entries in this pane:
     - *CDRIncludeSourceDomains*. Type a comma-separated list of domains in this field to be filtered by the call's source domain. For example, cisco.call.ciscospark or cisco.call.webex.com. Do not include any colons (:) in the source domains in this field.

- *CDRIncludeDestinationDomains*. Type a comma-separated list of domains in this field to be filtered by the call's destination domain. For example, cisco.call.ciscospark or cisco.call.webex.com. Do not include any colons (:) in the destination domains in this field.
- *CDRAdditionalCauseCodes*. Type a comma-separated list of additional cause codes to generate alerts on cause codes outside the default range.

> **NOTE:** These fields are optional. If left blank, the "Tandberg: VCS Status" Dynamic Application will generate alerts for calls from all domains, whose cause codes fall in the default range of 500 to 599.

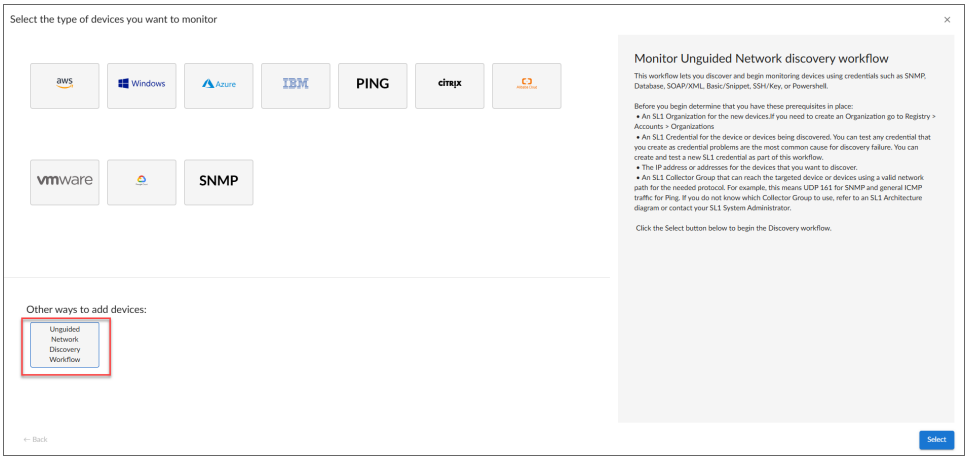
5. The rest of the fields on the **Credential Editor** page can be left blank or at their default settings.
6. Click the **[Save]** button to save the credential.

Discovering VCS Devices

To monitor your VCS devices, you must run a discovery session to discover the server on which the VCS device is installed.

To create and run a discovery session that will discover a VCS device appliance:

1. Go to the **Devices** page ( ) or the **Discovery Sessions** page (Devices > Discovery Sessions) and click the **[Add Devices]** button.
2. Click the **[Unguided Network Discovery Workflow]** button. Additional information about that requirements for discovery appears in the **General Information** pane to the right.



3. Click **[Select]**. The three-step wizard appears starting with the **[Step 1 Basic Information]** tab.
4. Complete the following fields:
   - ***Discovery Session 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 **[Step 2 Credential Selection]** tab of the wizard appears.
6. On the **[Credential Selection]** tab, locate and select the SOAP/XML credential you created for your VCS appliances.
7. Click **[Next]**. The **[Step 3 Discovery Session Details]** tab of the wizard appears.
8. Complete the following fields:
    - ***List of IP/Hostnames***. Type the IP address for the VCS device appliance.
    - ***Which collector will discover these devices?***. Required. Select an existing collector to monitor the discovered devices.
    - ***Run after save***. Toggle on (blue) to run this discovery session as soon as you save the session.
    - ***Advanced options***. Click the down arrow (⌄) to complete the following fields:
        - ***Discover Non-SNMP***. Toggle on (blue) to enable this setting.
        - ***Model Devices***. Toggle on (blue) to enable this setting.
        - ***Select Device Template***. If you configured a VCS device template, select it here. Otherwise, leave the default selection.
9. If you enabled the ***Run after save*** option, click the**[Save and Run]** button. The discovery session will run and the **Discovery Logs** page will display any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page will include a link to the **Device Investigator** page for the discovered device.
10. If you did not enable the ***Run after save*** option, click the **[Save and Close]** button. The **Discovery Sessions** page (Devices > Discovery Sessions) will display the new discovery session.

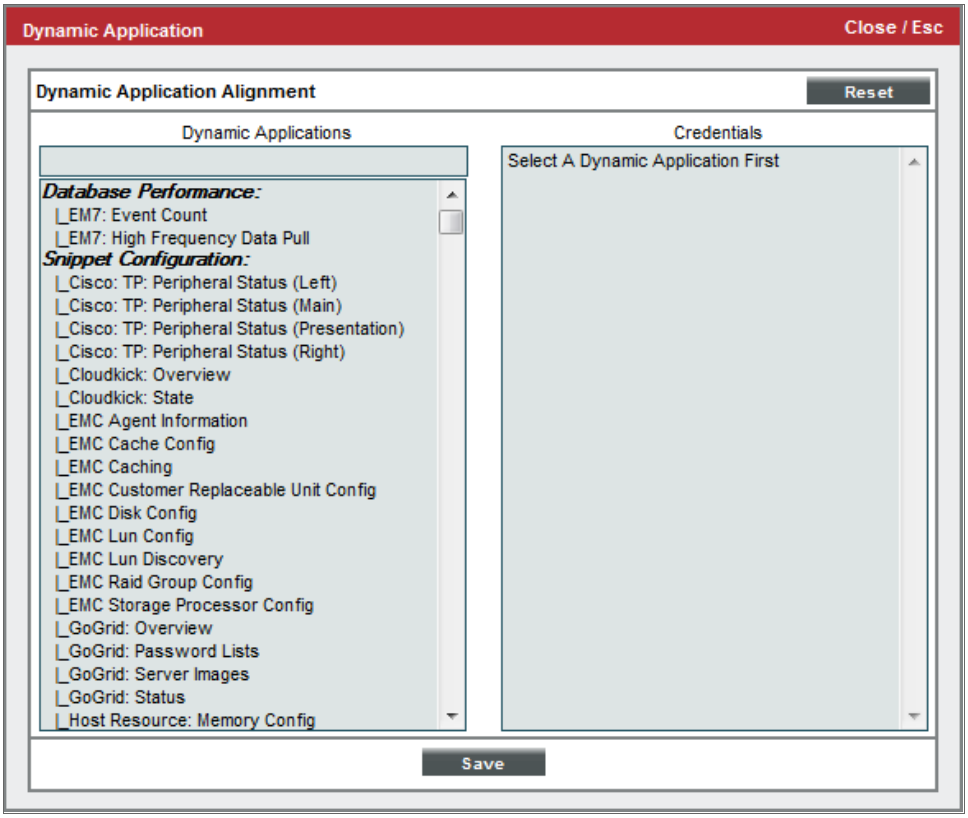
Manually Aligning Dynamic Applications with VCS Devices

From the **Dynamic Application Collections** page, you can manually align a Dynamic Application with a VCS device.

To manually align the Dynamic Applications from the *Tandberg: Infrastructure* PowerPack with a VCS device:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. In the **Device Manager** page, find the VCS device you want to associate with a Dynamic Application. Click its wrench icon ( ).
3. In the **Device Administration** panel, click the **[Collections]** tab.
4. In the **Dynamic Application Collections** page, click the **[Action]** menu and then select *Add Dynamic Application*.

5. The **Dynamic Application Alignment** modal page appears. To align a Dynamic Application with a device in this page:



   - Select *Tandberg: VCS Configuration* in the ***Dynamic Applications*** field. You can filter the list of Dynamic Applications using the search field above the ***Dynamic Applications*** field.
   - Select the credential you created for *Tandberg: VCS Configuration* from the ***Credentials*** list.

NOTE: Your organization membership(s) might affect the list of credentials you can see in the ***Credentials*** field.

6. Click the **[Save]** button in the **Dynamic Application Alignment** modal page to align the Dynamic Application and the Credential to the device.
7. Repeat steps 4-6 for the remaining Dynamic Applications:
   - *Tandberg: VCS Status*
   - *Tandberg: VCS Call Details*
   - *Tandberg: VCS Registration Details*

TelePresence Server

The Cisco TelePresence Server is available in two models:

- A chassis-based MSE 8710
- An appliance-based TelePresence Server 7010

The following Dynamic Applications for monitoring a TelePresence Server are included in the *Tandberg: Infrastructure* PowerPack:

- *Tandberg: Codian TS Port Utilization*
- *Tandberg: Codian TS Configuration*
- *Tandberg: Codian TS Conference Details*
- *Tandberg: Codian TS Participant Details*
- *Tandberg: Codian TS Status*

Creating a Credential for a TelePresence Server

For the Dynamic Applications in the "Tandberg: Infrastructure" PowerPack that can be aligned with TelePresence Servers, you will need to create a SOAP/XML credential to align with the Dynamic Application.

To create the credential:

1. Go to the **Credentials** page (Manage > Credentials).
2. In the **Credentials** page, click the **[Create]** button and then select *SOAP/XML Credential*.
3. The **Credential Editor** page appears. Enter 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 ***Select the organizations the credential belongs to*** drop-down field to align the credential with those specific organizations.
    - ***Timeout (seconds)***. For "Tandberg: Codian TS Configuration"and "Tandberg: Codian TS STatus" Dynamic Applications, Type "15". For the remaining Applications, Type "10".
    - ***Method***. For "Tandberg: Codian TS Configuration"and "Tandberg: Codian TS STatus", select *GET*. For the remaining Dynamic Applications, leave this field at the default value of *POST*.
    - ***HTTP Version***. Leave this field at the default value of *HTTP /1.1*.
    - ***URL***. Type the URL that corresponds to the Dynamic Application. The variable **%D** will be automatically replaced with the IP address of the device that is using the credential. The URL for each Dynamic Application is listed below:
        - *Tandberg: Codian TS Port Utilization*. Type "http://%D" in the ***URL*** field.

- *Tandberg: Codian TS Configuration*. Type "http://%D/system.xml" in the ***URL*** field.
- *Tandberg: Codian TS Conference Details*. Type "http://%D/" in the ***URL*** field.
- *Tandberg: Codian TS Participant Details*. Type "http://%D/" in the ***URL*** field.
- *Tandberg: Codian TS Status*. Type "http://%D/system.xml" in the ***URL*** field.

- ***HTTP Auth User***. Type the username with which you log in to the web server.
- ***HTTP Auth Password***. Type the password for the username you entered in the ***HTTP Auth User***field .

4. The rest of the fields in the **Create Credential** page can be left blank or at their default settings.
5. Click the **[Save]** button to save the credential.

Creating a Credential for a TelePresence Server in the SL1 Classic User Interface

For the Dynamic Applications in the "Tandberg: Infrastructure" PowerPack that can be aligned with TelePresence Servers, you will need to create a SOAP/XML credential to align with the Dynamic Application.

To create the credential in the classic user interface:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. In the **Credential Management** page, click the **[Create]** button and then select *SOAP/XML Host Credential*.
3. The **Credential Editor** page appears. Enter values in the following fields:
   - ***Profile Name***. Name of the credential. Can be any combination of alphanumeric characters.
   - ***Method***. For *Tandberg: Codian TS Configuration* and *Tandberg: Codian TS Status*, select *GET*. For the remaining Dynamic Applications, leave this field at the default value of *POST*.
   - ***HTTP Version***. Leave this field at the default value of *HTTP /1.1*.
   - ***URL***. Type the URL that corresponds to the Dynamic Application. The variable **%D** will be automatically replaced with the IP address of the device that is using the credential. The URL for each Dynamic Application is listed below:
     - *Tandberg: Codian TS Port Utilization*. Type "http://%D" in the ***URL*** field.
     - *Tandberg: Codian TS Configuration*. Type "http://%D/system.xml" in the ***URL*** field.
     - *Tandberg: Codian TS Conference Details*. Type "http://%D/" in the ***URL*** field.
     - *Tandberg: Codian TS Participant Details*. Type "http://%D/" in the ***URL*** field.
     - *Tandberg: Codian TS Status*. Type "http://%D/system.xml" in the ***URL*** field.
   - ***HTTP Auth User***. Type the username with which you log in to the web server.
   - ***HTTP Auth Password***. Type the password for the username you entered in the ***HTTP Auth User***field .
   - ***Timeout (seconds)***. For *Tandberg: Codian TS Configuration* and *Tandberg: Codian TS Status*, Type *15*. For the remaining Applications, Type *10*.

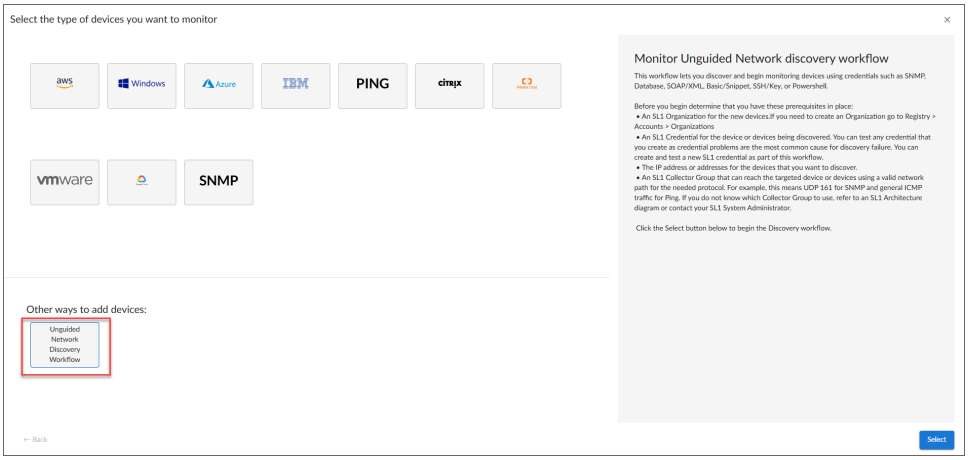
4. The rest of the fields in the **Credential Editor** page can be left blank or at their default settings.
5. Click the **[Save]** button to save the credential.

Discovering Devices with the TelePresence Server

To monitor your TelePresence Server devices, you must run a discovery session to discover the server on which the TelePresence device is installed.

To create and run a discovery session that will discover a TelePresence Server device appliance:

1. Go to the **Devices** page ( ) or the **Discovery Sessions** page (Devices > Discovery Sessions) and click the **[Add Devices]** button.
2. Click the **[Unguided Network Discovery Workflow]** button. Additional information about that requirements for discovery appears in the **General Information** pane to the right.



3. Click **[Select]**. The three-step wizard appears starting with the **[Step 1 Basic Information]** tab.
4. Complete the following fields:
    - ***Discovery Session 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 **[Step 2 Credential Selection]** tab of the wizard appears.
6. On the **[Credential Selection]** tab, locate and select the SOAP/XML credential you created for your TelePresence appliances.
7. Click **[Next]**. The **[Step 3 Discovery Session Details]** tab of the wizard appears.
8. Complete the following fields:

- ***List of IP/Hostnames***. Type the IP address for the TelePresence device appliance.
- ***Which collector will discover these devices?***. Required. Select an existing collector to monitor the discovered devices.
- ***Run after save***. Toggle on (blue) to run this discovery session as soon as you save the session.
- ***Advanced options***. Click the down arrow (⌄) to complete the following fields:
    - ***Discover Non-SNMP***. Toggle on (blue) to enable this setting.
    - ***Model Devices***. Toggle on (blue) to enable this setting.
    - ***Select Device Template***. If you configured a TelePresence device template, select it here. Otherwise, leave the default selection.

9. If you enabled the ***Run after save*** option, click the**[Save and Run]** button. The discovery session will run and the **Discovery Logs** page will display any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page will include a link to the **Device Investigator** page for the discovered device.
10. If you did not enable the ***Run after save*** option, click the **[Save and Close]** button. The **Discovery Sessions** page (Devices > Discovery Sessions) will display the new discovery session.

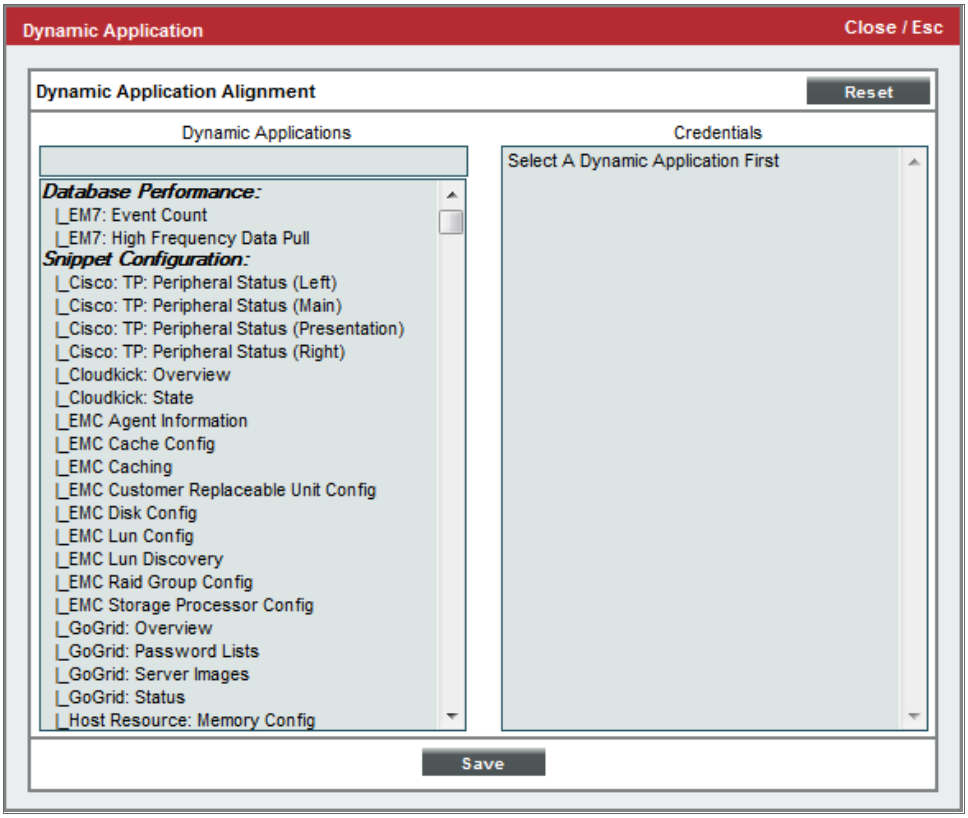
Manually Aligning the Dynamic Applications with the TelePresence Server

From the **Dynamic Application Collections** page, you can manually align a Dynamic Application with a TelePresence Server.

To manually align a Dynamic Application with a TelePresence Server:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. In the **Device Manager** page, find the TelePresence Server. Click its wrench icon ( ).
3. In the **Device Administration** panel, click the **[Collections]** tab.
4. In the **Dynamic Application Collections** page, click the **[Action]** menu and then select *Add Dynamic Application*.

5. The **Dynamic Application Alignment** modal page appears. To align a Dynamic Application with a device in this page:



- Select *Tandberg: Codian TS Configuration* in the ***Dynamic Applications*** field. You can filter the list of Dynamic Applications using the search field above the ***Dynamic Applications*** field.
- Select the credential you created for *Tandberg: Codian TS Configuration* from the ***Credentials*** list.

NOTE: Your organization membership(s) might affect the list of credentials you can see in the ***Credentials*** field.

6. Click the **[Save]** button in the **Dynamic Application Alignment** modal page to align the Dynamic Application and the credential to the device.
7. Repeat steps 4-6 for the remaining Dynamic Applications:

- *Tandberg: Codian TS Port Utilization*
- *Tandberg: Codian TS Status*

> **NOTE:** The following two Dynamic Applications are only supported for TelePresence Server versions 4.2 and below. The API no longer provides this information for TelePresence Server versions 4.3 and higher, and if you align these Dynamic Applications, you will see log messages such as "API version is not supported by application".

- *Tandberg: Codian TS Participant Details*
- *Tandberg: Codian TS Conference Details*

TelePresence Control Unit

The following Dynamic Applications for monitoring a TelePresence Control Unit are included in the *Tandberg: Infrastructure* PowerPack:

- ***Tandberg: TCU Configuration***
- ***Tandberg: TCU Status***

Creating a Credential for a TelePresence Control Unit

For the Dynamic Applications in the "Tandberg: Infrastructure" PowerPack that can be aligned with TelePresence Control Units, you will need to create a SOAP/XML credential to align with the Dynamic Application.

To create the credential in the classic user interface:

1. Go to the **Credentials** page (Manage > Credentials).
2. In the **Credentials** page, click the **[Create]** button and then select *SOAP/XML Credential*.
3. The **Create Credential** page appears. Enter 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 ***Select the organizations the credential belongs to*** drop-down field to align the credential with those specific organizations.
    - ***Timeout (seconds)***. Type the time, in seconds, after which you want SL1 to stop trying to communicate with the web server.
    - ***Method***. For both "Tandberg: TCU Configuration" and "Tandberg: TCU Status" Dynamic Applications, select *GET*.
    - ***HTTP Version***. Leave this field at the default value of *HTTP /1.1*.

- ***URL***. Type the URL that corresponds to the Dynamic Application. The variable **%D** will be automatically replaced with the IP address of the device that is using the credential. The URL for each Dynamic Application is listed below:
    - *Tandberg: TCU Configuration*. Type "http://%D/configuration.xml" in the ***URL*** field.
    - *Tandberg: TCU Status*. Type "http://%D/status.xml" in the ***URL*** field.
- ***HTTP Auth User***. Type the username with which you log in to the web server.
- ***HTTP Auth Password***. Type the password for the username you entered in the ***HTTP Auth User*** field .

4. The rest of the fields in the **Create Credential** page can be left blank or at their default settings.
5. Click the **[Save]** button to save the credential.

Creating a Credential for a TelePresence Control Unit in the SL1 Classic User Interface

For the Dynamic Applications in the "Tandberg: Infrastructure" PowerPack that can be aligned with TelePresence Control Units, you will need to create a SOAP/XML credential to align with the Dynamic Application.

To create the credential in the classic user interface:

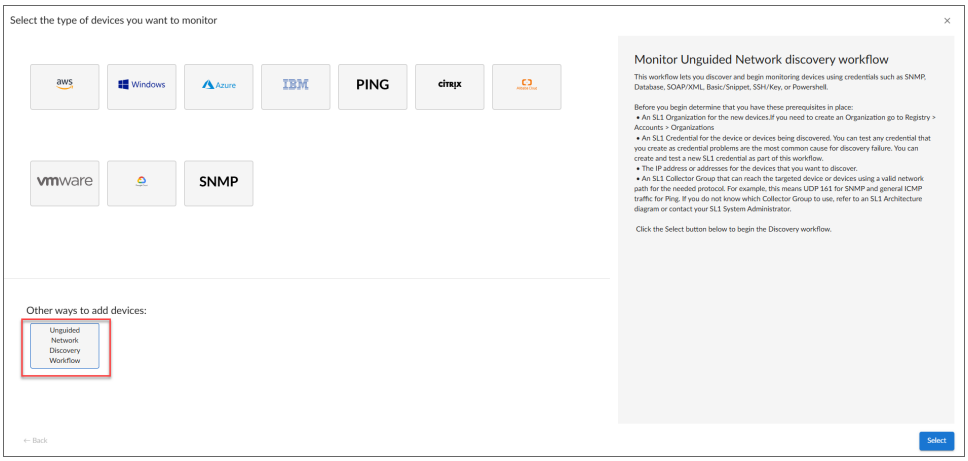
1. Go to the **Credential Management** page (System > Manage > Credentials).
2. In the **Credential Management** page, click the **[Create]** button and then select *SOAP/XML Host Credential*.
3. The **Credential Editor** page appears. Enter values in the following fields:
    - ***Profile Name***. Name of the credential. Can be any combination of alphanumeric characters.
    - ***Method***. For both *Tandberg: TCU Configuration* and *Tandberg: TCU Status*, select *GET*.
    - ***HTTP Version***. Leave this field at the default value of *HTTP /1.1*.
    - ***URL***. Type the URL that corresponds to the Dynamic Application. The variable **%D** will be automatically replaced with the IP address of the device that is using the credential. The URL for each Dynamic Application is listed below:
        - *Tandberg: TCU Configuration*. Type "http://%D/configuration.xml" in the ***URL*** field.
        - *Tandberg: TCU Status*. Type "http://%D/status.xml" in the ***URL*** field.
    - ***HTTP Auth User***. Type the username with which you log in to the web server.
    - ***HTTP Auth Password***. Type the password for the username you entered in the ***HTTP Auth User*** field .
    - ***Timeout (seconds)***. Type the time, in seconds, after which you want SL1 to stop trying to communicate with the web server.
4. The rest of the fields in the **Credential Editor** page can be left blank or at their default settings.
5. Click the **[Save]** button to save the credential.

Discovering TelePresence Control Unit Devices

To monitor your TelePresence Server devices, you must run a discovery session to discover the server on which the TelePresence device is installed.

To create and run a discovery session that will discover a TelePresence Server device appliance:

1. Go to the **Devices** page ( ) or the **Discovery Sessions** page (Devices > Discovery Sessions) and click the **[Add Devices]** button.
2. Click the **[Unguided Network Discovery Workflow]** button. Additional information about that requirements for discovery appears in the **General Information** pane to the right.



3. Click **[Select]**. The three-step wizard appears starting with the **[Step 1 Basic Information]** tab.
4. Complete the following fields:
    - ***Discovery Session 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 **[Step 2 Credential Selection]** tab of the wizard appears.
6. On the **[Credential Selection]** tab, locate and select the SOAP/XML credential you created for your TelePresence appliances.
7. Click **[Next]**. The **[Step 3 Discovery Session Details]** tab of the wizard appears.
8. Complete the following fields:
    - ***List of IP/Hostnames***. Type the IP address for the TelePresence device appliance.
    - ***Which collector will discover these devices?***. Required. Select an existing collector to monitor the discovered devices.
    - ***Run after save***. Toggle on (blue) to run this discovery session as soon as you save the session.

- ***Advanced options***. Click the down arrow (⌄) to complete the following fields:
    - ***Discover Non-SNMP***. Toggle on (blue) to enable this setting.
    - ***Model Devices***. Toggle on (blue) to enable this setting.
    - ***Select Device Template***. If you configured a TelePresence device template, select it here. Otherwise, leave the default selection.

9. If you enabled the ***Run after save*** option, click the**[Save and Run]** button. The discovery session will run and the **Discovery Logs** page will display any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page will include a link to the **Device Investigator** page for the discovered device.
10. If you did not enable the ***Run after save*** option, click the **[Save and Close]** button. The **Discovery Sessions** page (Devices > Discovery Sessions) will display the new discovery session.

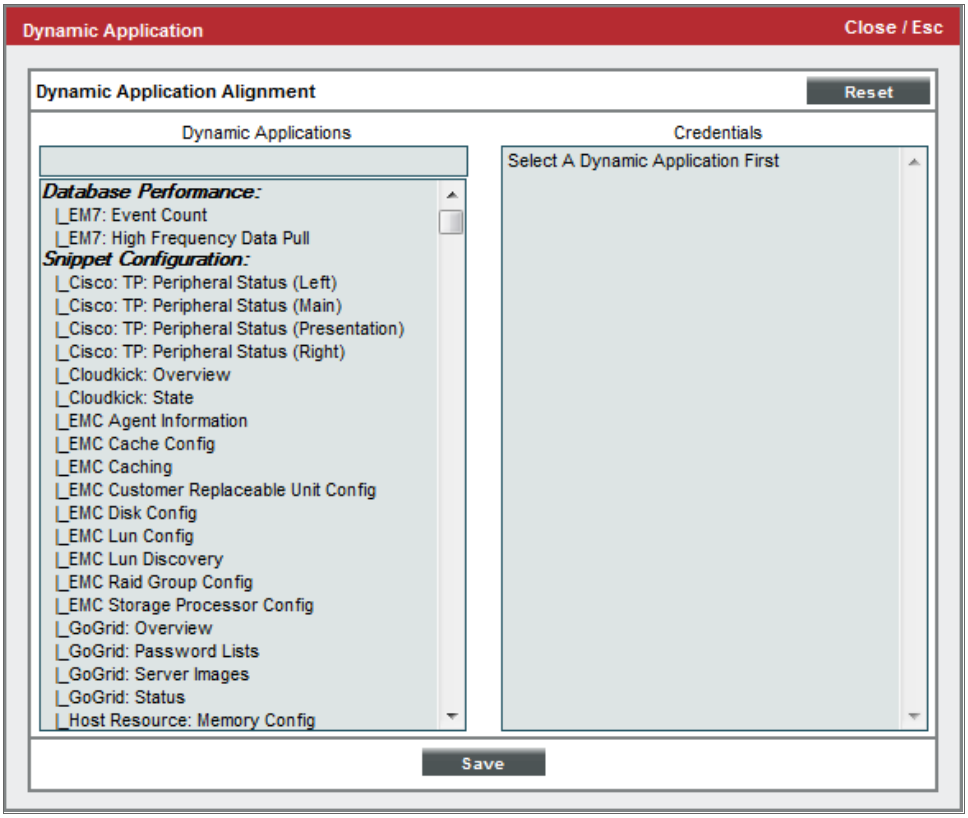
Manually Aligning the Dynamic Applications with the TelePresence Server

From the **Dynamic Application Collections** page, you can manually align a Dynamic Application with a TelePresence Control Unit.

To manually align a Dynamic Application with a TelePresence Control Unit:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. In the **Device Manager** page, find the TelePresence Control Unit. Click its wrench icon ( ).
3. In the **Device Administration** panel, click the **[Collections]** tab.
4. In the **Dynamic Application Collections** page, click the **[Action]** menu and then select *Add Dynamic Application*.

5. The **Dynamic Application Alignment** modal page appears. To align a Dynamic Application with a device in this page:



- Select *Tandberg: TCU Configuration* in the ***Dynamic Applications*** field. You can filter the list of Dynamic Applications using the search field above the ***Dynamic Applications*** field.
- Select the credential you created for *Tandberg: TCU Configuration* from the ***Credentials*** list.

NOTE: Your organization membership(s) might affect the list of credentials you can see in the ***Credentials*** field.

6. Click the **[Save]** button in the **Dynamic Application Alignment** modal page to align the Dynamic Application and the credential to the device.
7. Repeat steps 4-6 for the *Tandberg: TCU Status*Dynamic Application.

Chapter 10

Reports for Video Devices

Overview

The following sections describe the default custom reports that are designed to display data collected from video devices:

This chapter covers the following topics:

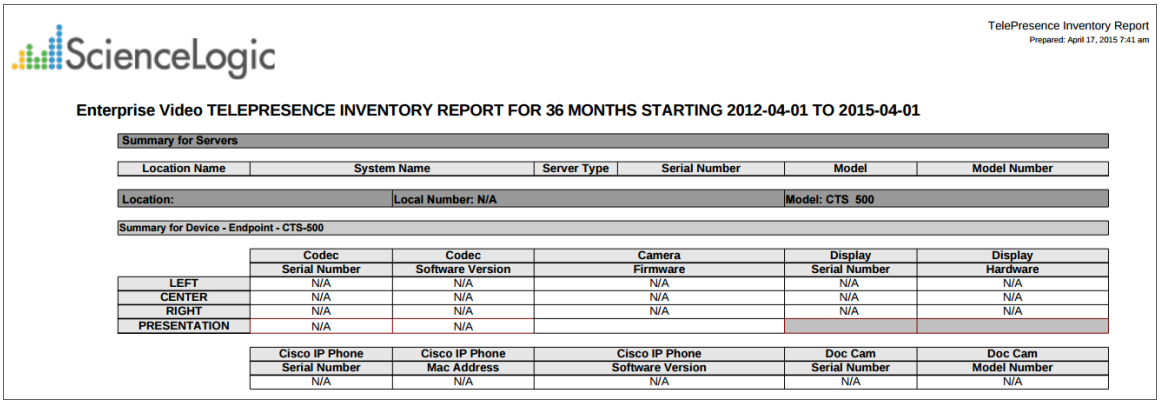
TelePresence Inventory Report *94*
Video Calls by Device Group, Call Type, and Bandwidth Report *94*
Video Endpoint Availability Chart Report *96*
Video Endpoint Availability Table Report *98*
Video Endpoint Avg Jitter Column Chart Report *100*
Video Endpoint Avg Jitter Line Chart Report *102*
Video Endpoint Avg Jitter Table Report *105*
Video Endpoint Call Detail Records Report *106*
Video Endpoint Detailed Asset Inventory Report *109*
Video Endpoint Detailed Jitter Line Chart Report *110*
Video Endpoint Detailed Packet Loss Line Chart Report *113*
Video Endpoint Packet Loss Column Chart Report *115*
Video Endpoint Packet Loss Line Chart Report *117*
Video Endpoint Packet Loss Table Report *119*
Video Endpoint Performance Detail Report *120*
Video Endpoint Unavailability Chart Report *122*
Video Endpoint Unavailability Table Report *124*

Video Usage Report *126*
Video Usage Chart Report *127*

NOTE: The reports listed in this chapter can be generated as quick reports on the **Run Quick Report** page (Reports > Run Report) or configured as scheduled reports on the **Report Jobs** page (Reports > Create Report > Report Jobs). For more information about generating reports, see the ***Reports*** manual.

TelePresence Inventory Report

This report displays a summary of TelePresence servers, including the location name, system name, server type, serial number, model, and model number for each server.



ScienceLogic

TelePresence Inventory Report
Prepared: April 17, 2015 7:41 am

Enterprise Video TELEPRESENCE INVENTORY REPORT FOR 36 MONTHS STARTING 2012-04-01 TO 2015-04-01

Summary for Servers

Location Name	System Name	Server Type	Serial Number	Model	Model Number

Location:	Local Number: N/A	Model: CTS 500

Summary for Device - Endpoint - CTS-500

	Codec Serial Number	Codec Software Version	Camera Firmware	Display Serial Number	Display Hardware
LEFT	N/A	N/A	N/A	N/A	N/A
CENTER	N/A	N/A	N/A	N/A	N/A
RIGHT	N/A	N/A	N/A	N/A	N/A
PRESENTATION	N/A	N/A			

Cisco IP Phone Serial Number	Cisco IP Phone Mac Address	Cisco IP Phone Software Version	Doc Cam Serial Number	Doc Cam Model Number
N/A	N/A	N/A	N/A	N/A

The following options are available when generating the report:

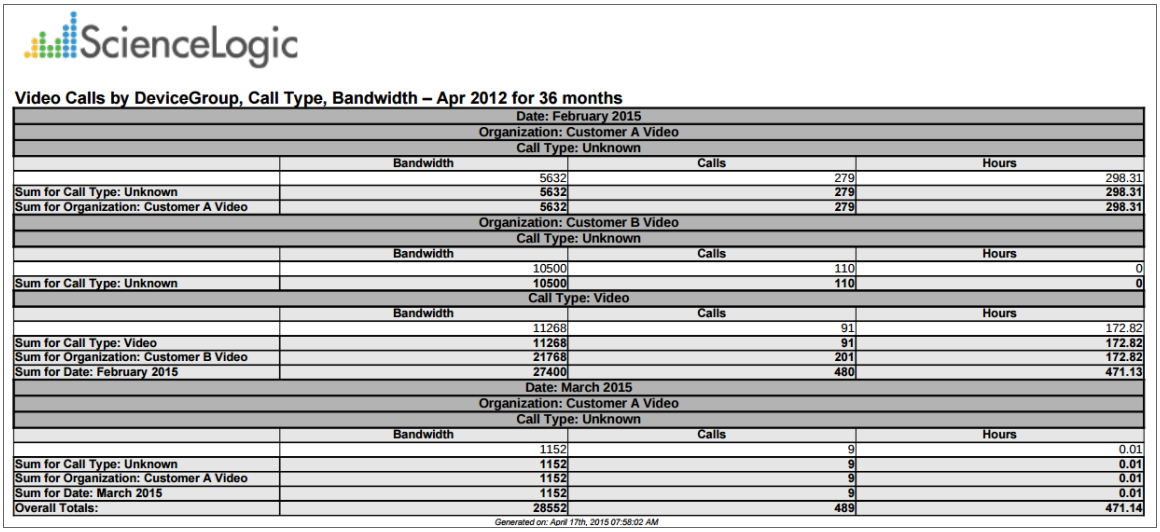
- ***Tandberg and TelePresence Organization Selection***. Select the organization that you want represented in the report.
- ***Report Span***. Specify a Daily, Weekly, or Monthly span to include in the report. Specify a Starting date and a Duration for the report.

This description covers the latest version of this report as shipped by ScienceLogic. This report might have been modified on your SL1 system.

Video Calls by Device Group, Call Type, and Bandwidth Report

This report displays usage information for Tandberg, Polycom, Lifesize and Cisco TelePresence devices. For each device included in the report, the report displays a table for each type of call. For each type of call, the report displays the number of calls and total hours the device was on a call for each bandwidth type. The report includes only calls that were made during the time period selected for the report.

You can customize the output to include only specific devices. You can also specify the time span of information to include in the report.



ScienceLogic

Video Calls by DeviceGroup, Call Type, Bandwidth – Apr 2012 for 36 months

	Bandwidth	Calls	Hours
Date: February 2015			
Organization: Customer A Video			
Call Type: Unknown			
	5632	279	298.31
Sum for Call Type: Unknown	**5632**	**279**	**298.31**
Sum for Organization: Customer A Video	**5632**	**279**	**298.31**
Organization: Customer B Video			
Call Type: Unknown			
	10500	110	0
Sum for Call Type: Unknown	**10500**	**110**	**0**
Call Type: Video			
	11268	91	172.82
Sum for Call Type: Video	**11268**	**91**	**172.82**
Sum for Organization: Customer B Video	**21768**	**201**	**172.82**
Sum for Date: February 2015	**27400**	**480**	**471.13**
Date: March 2015			
Organization: Customer A Video			
Call Type: Unknown			
	1152	9	0.01
Sum for Call Type: Unknown	**1152**	**9**	**0.01**
Sum for Organization: Customer A Video	**1152**	**9**	**0.01**
Sum for Date: March 2015	**1152**	**9**	**0.01**
Overall Totals:	**28552**	**489**	**471.14**

Generated on: April 17th, 2015 07:58:02 AM

The following input options are available when generating the report:

- ***Branding***. Optionally enter text that will be displayed at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" will be displayed at the top of the report.
- ***Device Selection***: Select the devices that will appear in the report. The choices are:
    - *All devices*. Select this checkbox if you want all devices in the system to be included in this report.
    - *Organizations*. If the *All devices* checkbox is unselected, select one or more Organizations. The report will contain only the devices in the organizations you select. You can further filter the list of devices to include in the report by selecting devices in the *Devices by Organization* field.
    - *Select individual devices*. If the *All devices* checkbox is unselected, the *Select individual devices* checkbox is available. Select this checkbox if you would like to use the *Devices by Organization* field to select the individual devices to include in the report.
    - *Devices by Organization*. This field displays a list of all devices in the organizations selected in the *Organizations field*. If the *Select individual devices* checkbox is selected, you can select one or more devices to include in the report.
- ***Device Group Selector***: Select the device groups that will appear in the report. The following input elements appear in this component:
    - *Select By Device Group*. Select this checkbox if you want to select which device groups to include in the report.
    - *Device Groups*. If the *Select By Device Group* checkbox is selected, select one or more device groups. The report will contain only the devices in the device groups you select.
- ***Device Categories***. By default, the *All Device Categories* checkbox is selected. To limit the report to one or more specific device categories, select one or more device categories from the list of *Device Categories*.
- ***General Display Options***. Specify how the report will be arranged:

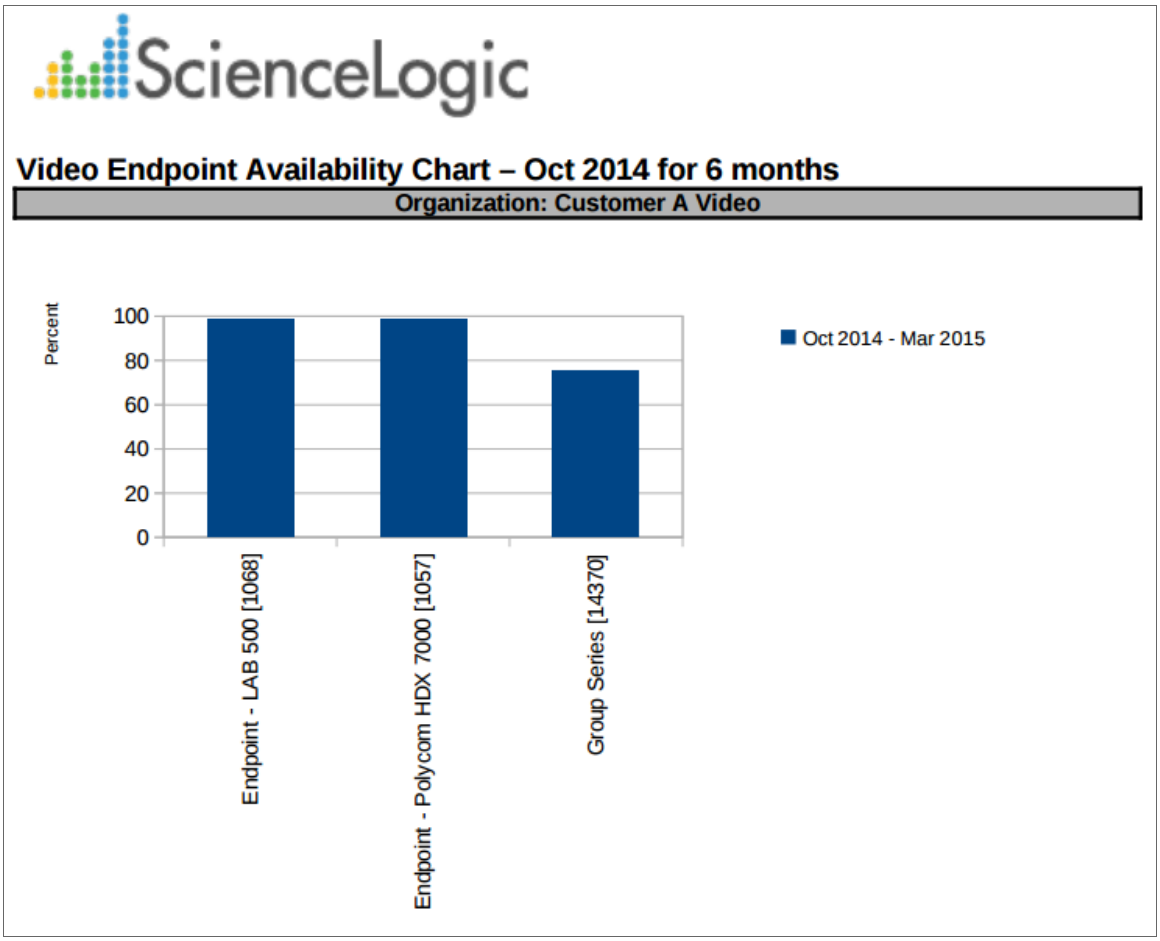
    - ***Separated By***. Select whether the report will be separated into multiple tables. The report can be separated to include one table per organization, one table per device group, one table per device category, or one table per device.
    - ***Naming***. These checkboxes allow you to select whether the Device ID or the Organization ID will appear in the report.
    - ***Report Sections***. Select whether you want the report to display *Details Only*, *Totals Only*, or *Both*.
- ***Report Span***. Specify a *Daily*, *Weekly*, or *Monthly* span to include in the report. ***Starting***. Use the *Year*, *Month*, and *Date* fields to specify a Start Date for the report. The SL1 system will use data from that date as the starting point of the report.***Duration***. Specify the duration for the report, from 1 month to 36 months. The SL1 system will use data from the Starting date as the start point of the report and data from the last day of the Duration as the ending point of the report.***Timezone***. Specify the timezone to use for date and time values in the report. Specify the timezone by number of hours offset from UTC.
- ***Report Type***. Specify that the report should include all selected devices or that the report should be limited to include a set number of devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the Video Reports PowerPack. This report might have been modified on your SL1 system.

Video Endpoint Availability Chart Report

This report displays a bar graph of device availability for Tandberg, Lifesize, Cisco, and Polycom video endpoints. For each device included in the report, the report displays availability in percentage for the time period selected for the report.

You can customize the output to include only specific devices and/or limit the number of devices that are included in the report. You can also specify the time span of information to include in the report, text that will appear at the top of the report, and how the devices will be sorted and arranged in the report.



The following input options are available when generating the report:

- ***Branding***. Optionally enter text that will be displayed at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" will be displayed at the top of the report.
- ***Device Selection***: Select the devices that will appear in the report. The choices are:
    - *All devices*. Select this checkbox if you want all devices in the system to be included in this report.
    - *Organizations*. If the *All devices* checkbox is unselected, select one or more Organizations. The report will contain only the devices in the organizations you select. You can further filter the list of devices to include in the report by selecting devices in the *Devices by Organization* field.
    - *Select individual devices*. If the *All devices* checkbox is unselected, the *Select individual devices* checkbox is available. Select this checkbox if you would like to use the *Devices by Organization* field to select the individual devices to include in the report.
    - *Devices by Organization*. This field displays a list of all devices in the organizations selected in the *Organizations field*. If the *Select individual devices* checkbox is selected, you can select one or more devices to include in the report.

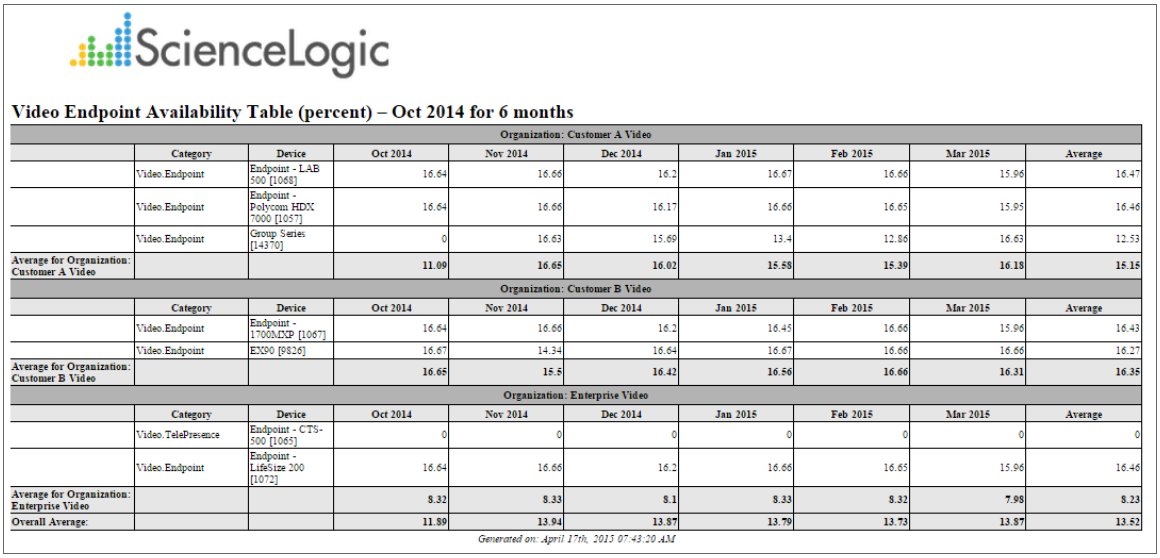
- ***Device Group Selector***: Select the device groups that will appear in the report. The following input elements appear in this component:
    - *Select By Device Group*. Select this checkbox if you want to select which device groups to include in the report.
    - *Device Groups*. If the *Select By Device Group* checkbox is selected, select one or more device groups. The report will contain only the devices in the device groups you select.
- ***Device Categories***. By default, the *All Device Categories* checkbox is selected. To limit the report to one or more specific device categories, select one or more device categories from the list of *Device Categories*.
- ***General Display Options***. Specify how the report will be arranged:
    - ***Separated By***. Select whether the report will be separated into multiple tables. The report can be separated to include one table per organization, one table per device group, one table per device category, or one table per device.
    - ***Naming***. These checkboxes allow you to select whether the Device ID or the Organization ID will appear in the report.
    - ***Stacking***. Select the *Enable Stacking* checkbox to allow data to be stacked.
- ***Report Span***. Specify a *Daily*, *Weekly*, or *Monthly* span to include in the report. ***Starting***. Use the *Year*, *Month*, and *Date* fields to specify a Start Date for the report. The SL1 system will use data from that date as the starting point of the report.***Duration***. Specify the duration for the report, from 1 month to 36 months. The SL1 system will use data from the Starting date as the start point of the report and data from the last day of the Duration as the ending point of the report.***Timezone***. Specify the timezone to use for date and time values in the report. Specify the timezone by number of hours offset from UTC.
- ***Report Type***. Specify that the report should include all selected devices or that the report should be limited to include a set number of devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the Video Reports PowerPack. This report might have been modified on your SL1 system.

Video Endpoint Availability Table Report

This report displays an overview of device availability for Tandberg, Polycom, Lifesize and Cisco TelePresence devices. For each device included in the report, the report displays availability in percentage for the time period selected for the report.

You can customize the output to include only specific devices and/or limit the number of devices that are included in the report. You can also specify the time span of information to include in the report, text that will appear at the top of the report, and how the devices will be sorted and arranged in the report.



Video Endpoint Availability Table (percent) – Oct 2014 for 6 months

Organization: Customer A Video									
	Category	Device	Oct 2014	Nov 2014	Dec 2014	Jan 2015	Feb 2015	Mar 2015	Average
	Video.Endpoint	Endpoint - LAB 500 [1068]	16.64	16.66	16.2	16.67	16.66	15.96	16.47
	Video.Endpoint	Endpoint - Polycom HDX 7000 [1057]	16.64	16.66	16.17	16.66	16.65	15.95	16.46
	Video.Endpoint	Group Series [14370]	0	16.63	15.69	13.4	12.86	16.63	12.53
Average for Organization: Customer A Video			**11.09**	**16.65**	**16.02**	**15.58**	**15.39**	**16.18**	**15.16**
Organization: Customer B Video									
	Category	**Device**	**Oct 2014**	**Nov 2014**	**Dec 2014**	**Jan 2015**	**Feb 2015**	**Mar 2015**	**Average**
	Video.Endpoint	Endpoint - 1700MXP [1067]	16.64	16.66	16.2	16.45	16.66	15.96	16.43
	Video.Endpoint	EX90 [9826]	16.67	14.34	16.64	16.67	16.66	16.66	16.27
Average for Organization: Customer B Video			**16.65**	**15.5**	**16.42**	**16.56**	**16.66**	**16.31**	**16.35**
Organization: Enterprise Video									
	Category	**Device**	**Oct 2014**	**Nov 2014**	**Dec 2014**	**Jan 2015**	**Feb 2015**	**Mar 2015**	**Average**
	Video.TelePresence	Endpoint - CTS-500 [1065]	0	0	0	0	0	0	0
	Video.Endpoint	Endpoint - LifeSize 200 [1072]	16.64	16.66	16.2	16.66	16.65	15.96	16.46
Average for Organization: Enterprise Video			**8.32**	**8.33**	**8.1**	**8.33**	**8.32**	**7.98**	**8.23**
Overall Average:			**11.89**	**13.94**	**13.87**	**13.79**	**13.73**	**13.87**	**13.52**

Generated on: April 17th, 2015 07:43:20 AM

The following input options are available when generating the report:

- ***Branding***. Optionally enter text that will be displayed at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" will be displayed at the top of the report.
- ***Device Selection***: Select the devices that will appear in the report. The choices are:
    - *All devices*. Select this checkbox if you want all devices in the system to be included in this report.
    - *Organizations*. If the *All devices* checkbox is unselected, select one or more Organizations. The report will contain only the devices in the organizations you select. You can further filter the list of devices to include in the report by selecting devices in the *Devices by Organization* field.
    - *Select individual devices*. If the *All devices* checkbox is unselected, the *Select individual devices* checkbox is available. Select this checkbox if you would like to use the *Devices by Organization* field to select the individual devices to include in the report.
    - *Devices by Organization*. This field displays a list of all devices in the organizations selected in the *Organizations field*. If the *Select individual devices* checkbox is selected, you can select one or more devices to include in the report.
- ***Device Group Selector***: Select the device groups that will appear in the report. The following input elements appear in this component:
    - *Select By Device Group*. Select this checkbox if you want to select which device groups to include in the report.
    - *Device Groups*. If the *Select By Device Group* checkbox is selected, select one or more device groups. The report will contain only the devices in the device groups you select.

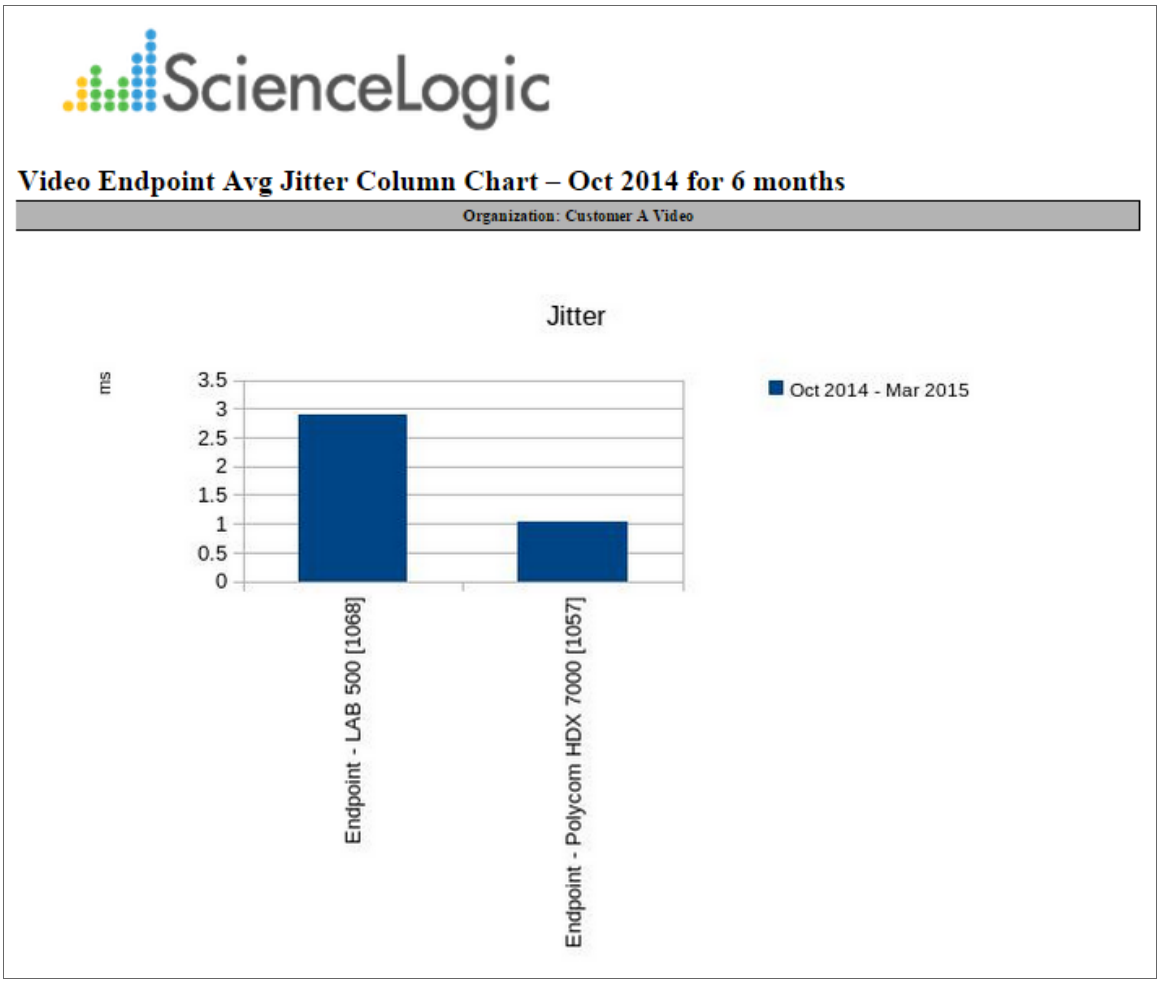
- ***Device Categories***. By default, the *All Device Categories* checkbox is selected. To limit the report to one or more specific device categories, select one or more device categories from the list of *Device Categories*.
- ***General Display Options***. Specify how the report will be arranged:
    - ***Separated By***. Select whether the report will be separated into multiple tables. The report can be separated to include one table per organization, one table per device group, one table per device category, or one table per device.
    - ***Naming***. These checkboxes allow you to select whether the Device ID or the Organization ID will appear in the report.
    - ***Report Sections***. Select whether you want the report to display *Details Only*, *Totals Only*, or *Both*.
- ***Report Span***. Specify a *Daily*, *Weekly*, or *Monthly* span to include in the report. ***Starting***. Use the *Year*, *Month*, and *Date* fields to specify a Start Date for the report. The SL1 system will use data from that date as the starting point of the report.***Duration***. Specify the duration for the report, from 1 month to 36 months. The SL1 system will use data from the Starting date as the start point of the report and data from the last day of the Duration as the ending point of the report.***Timezone***. Specify the timezone to use for date and time values in the report. Specify the timezone by number of hours offset from UTC.
- ***Report Type***. Specify that the report should include all selected devices or that the report should be limited to include a set number of devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the Video Reports PowerPack. This report might have been modified on your SL1 system.

Video Endpoint Avg Jitter Column Chart Report

This report displays the average jitter for Tandberg, Polycom, Lifesize and Cisco TelePresence devices. For each device included in the report, the report displays the jitter average in milliseconds for the time period selected for the report.

You can customize the output to include only specific devices and/or limit the number of devices that are included in the report. You can also specify the time span of information to include in the report, text that will appear at the top of the report, and how the devices will be sorted and arranged in the report.



The following input options are available when generating the report:

- ***Branding***. Optionally enter text that will be displayed at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" will be displayed at the top of the report.
- ***Device Selection***: Select the devices that will appear in the report. The choices are:
    - *All devices*. Select this checkbox if you want all devices in the system to be included in this report.
    - *Organizations*. If the *All devices* checkbox is unselected, select one or more Organizations. The report will contain only the devices in the organizations you select. You can further filter the list of devices to include in the report by selecting devices in the *Devices by Organization* field.
    - *Select individual devices*. If the *All devices* checkbox is unselected, the *Select individual devices* checkbox is available. Select this checkbox if you would like to use the *Devices by Organization* field to select the individual devices to include in the report.
    - *Devices by Organization*. This field displays a list of all devices in the organizations selected in the *Organizations field*. If the *Select individual devices* checkbox is selected, you can select one or more devices to include in the report.

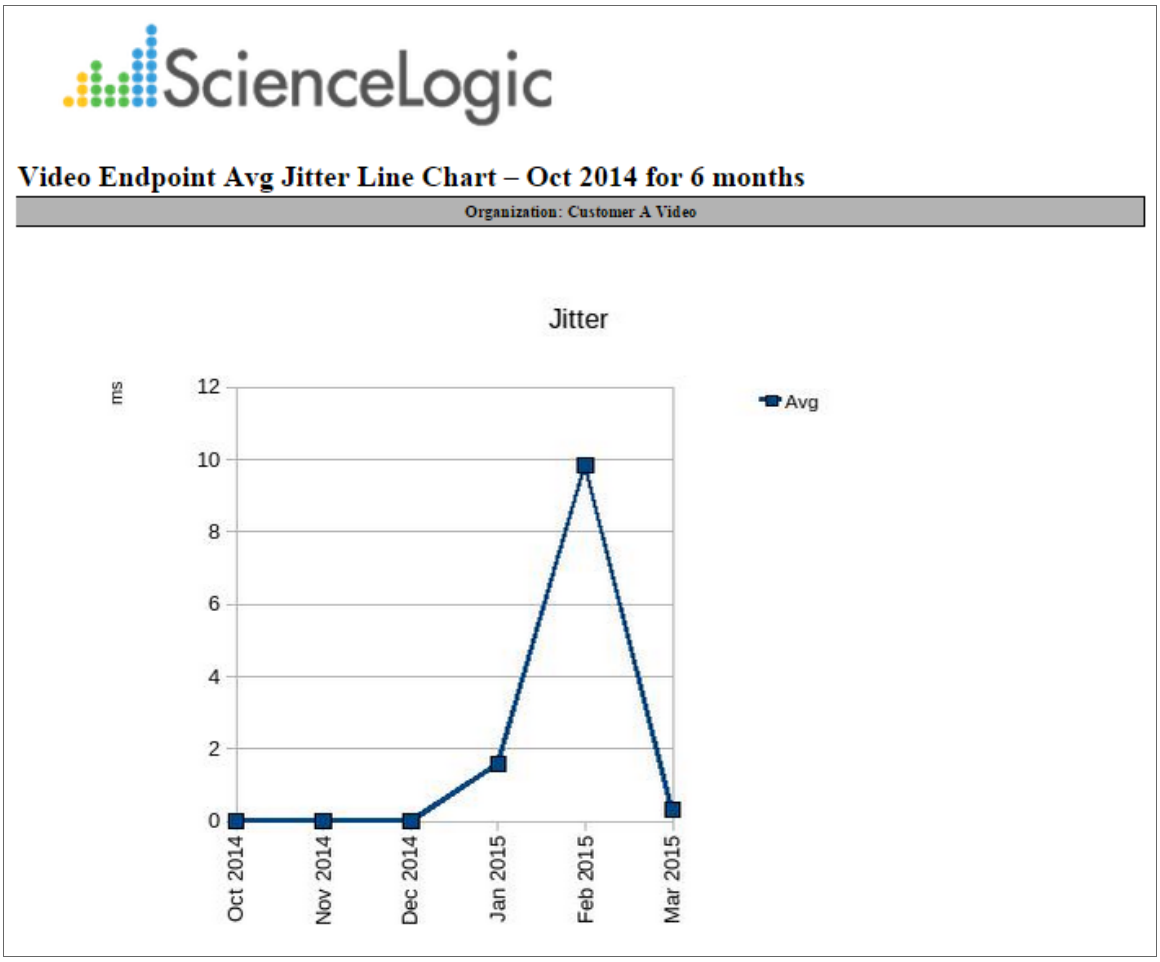
- ***Device Group Selector***: Select the device groups that will appear in the report. The following input elements appear in this component:
    - *Select By Device Group*. Select this checkbox if you want to select which device groups to include in the report.
    - *Device Groups*. If the *Select By Device Group* checkbox is selected, select one or more device groups. The report will contain only the devices in the device groups you select.
- ***Device Categories***. By default, the *All Device Categories* checkbox is selected. To limit the report to one or more specific device categories, select one or more device categories from the list of *Device Categories*.
- ***General Display Options***. Specify how the report will be arranged:
    - ***Separated By***. Select whether the report will be separated into multiple tables. The report can be separated to include one table per organization, one table per device group, one table per device category, or one table per device.
    - ***Naming***. These checkboxes allow you to select whether the Device ID or the Organization ID will appear in the report.
    - ***Stacking***. Select the *Enable Stacking* checkbox to allow data to be stacked.
- ***Report Span***. Specify a *Daily*, *Weekly*, or *Monthly* span to include in the report.
- ***Starting***. Use the *Year*, *Month*, and *Date* fields to specify a Start Date for the report. The SL1 system will use data from that date as the starting point of the report.
- ***Duration***. Specify the duration for the report, from 1 month to 36 months. The SL1 system will use data from the Starting date as the start point of the report and data from the last day of the Duration as the ending point of the report.
- ***Timezone***. Specify the timezone to use for date and time values in the report. Specify the timezone by number of hours offset from UTC.
- ***Report Type***. Specify that the report should include all selected devices or that the report should be limited to include a set number of devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the Video Reports PowerPack. This report might have been modified on your SL1 system.

Video Endpoint Avg Jitter Line Chart Report

This report displays the average jitter for Tandberg, Polycom, Lifesize and Cisco TelePresence devices. For each device included in the report, the report displays the jitter average in milliseconds for the time period selected for the report.

You can customize the output to include only specific devices and/or limit the number of devices that are included in the report. You can also specify the time span of information to include in the report, text that will appear at the top of the report, and how the devices will be sorted and arranged in the report.



The following input options are available when generating the report:

- ***Branding***. Optionally enter text that will be displayed at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" will be displayed at the top of the report.
- ***Device Selection***: Select the devices that will appear in the report. The choices are:
    - *All devices*. Select this checkbox if you want all devices in the system to be included in this report.
    - *Organizations*. If the *All devices* checkbox is unselected, select one or more Organizations. The report will contain only the devices in the organizations you select. You can further filter the list of devices to include in the report by selecting devices in the *Devices by Organization* field.
    - *Select individual devices*. If the *All devices* checkbox is unselected, the *Select individual devices* checkbox is available. Select this checkbox if you would like to use the *Devices by Organization* field to select the individual devices to include in the report.
    - *Devices by Organization*. This field displays a list of all devices in the organizations selected in the *Organizations field*. If the *Select individual devices* checkbox is selected, you can select one or more devices to include in the report.

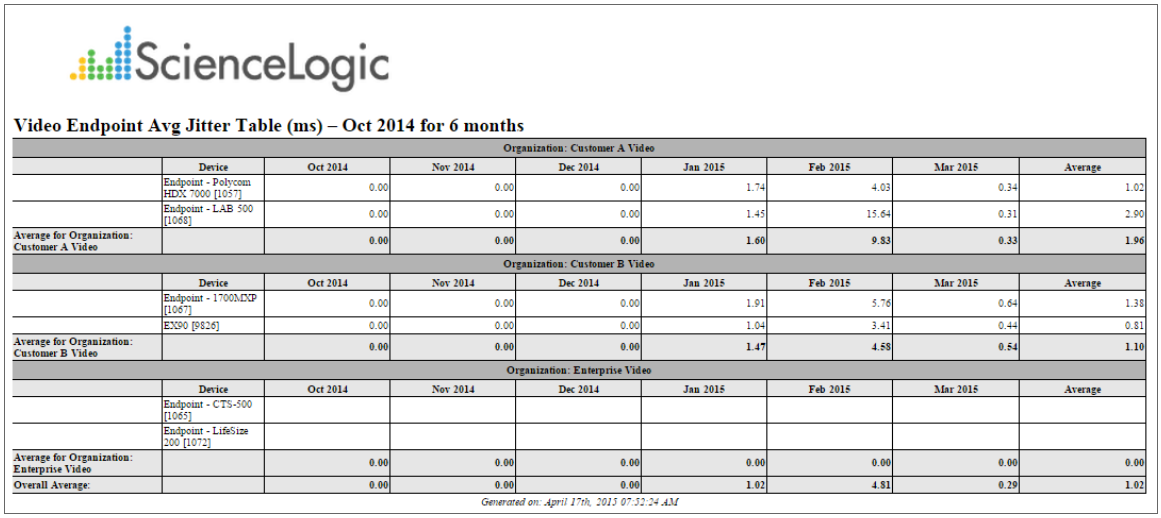
- ***Device Group Selector***: Select the device groups that will appear in the report. The following input elements appear in this component:
    - *Select By Device Group*. Select this checkbox if you want to select which device groups to include in the report.
    - *Device Groups*. If the *Select By Device Group* checkbox is selected, select one or more device groups. The report will contain only the devices in the device groups you select.
- ***Device Categories***. By default, the *All Device Categories* checkbox is selected. To limit the report to one or more specific device categories, select one or more device categories from the list of *Device Categories*.
- ***General Display Options***. Specify how the report will be arranged:
    - ***Separated By***. Select whether the report will be separated into multiple tables. The report can be separated to include one table per organization, one table per device group, one table per device category, or one table per device.
    - ***Naming***. These checkboxes allow you to select whether the Device ID or the Organization ID will appear in the report.
    - ***Stacking***. Select the *Enable Stacking* checkbox to allow data to be stacked.
- ***Report Span***. Specify a *Daily*, *Weekly*, or *Monthly* span to include in the report. ***Starting***. Use the *Year*, *Month*, and *Date* fields to specify a Start Date for the report. The SL1 system will use data from that date as the starting point of the report.***Duration***. Specify the duration for the report, from 1 month to 36 months. The SL1 system will use data from the Starting date as the start point of the report and data from the last day of the Duration as the ending point of the report.***Timezone***. Specify the timezone to use for date and time values in the report. Specify the timezone by number of hours offset from UTC.
- ***Report Type***. Specify that the report should include all selected devices or that the report should be limited to include a set number of devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the Video Reports PowerPack. This report might have been modified on your SL1 system.

Video Endpoint Avg Jitter Table Report

This report displays the average jitter for Tandberg, Lifesize, Cisco, and Polycom video endpoints. For each device included in the report, the report displays the jitter average in milliseconds for the time period selected for the report.

You can customize the output to include only specific devices and/or limit the number of devices that are included in the report. You can also specify the time span of information to include in the report, text that will appear at the top of the report, and how the devices will be sorted and arranged in the report.



ScienceLogic

Video Endpoint Avg Jitter Table (ms) – Oct 2014 for 6 months

Organization: Customer A Video								
	Device	Oct 2014	Nov 2014	Dec 2014	Jan 2015	Feb 2015	Mar 2015	Average
	Endpoint - Polycom HDX 7000 [1057]	0.00	0.00	0.00	1.74	4.03	0.34	1.02
	Endpoint - LAB 500 [1068]	0.00	0.00	0.00	1.45	15.64	0.31	2.90
Average for Organization: Customer A Video		**0.00**	**0.00**	**0.00**	**1.60**	**9.83**	**0.33**	**1.96**
Organization: Customer B Video								
	Device	**Oct 2014**	**Nov 2014**	**Dec 2014**	**Jan 2015**	**Feb 2015**	**Mar 2015**	**Average**
	Endpoint - 1700MXP [1067]	0.00	0.00	0.00	1.91	5.76	0.64	1.38
	EX90 [9826]	0.00	0.00	0.00	1.04	3.41	0.44	0.81
Average for Organization: Customer B Video		**0.00**	**0.00**	**0.00**	**1.47**	**4.58**	**0.54**	**1.10**
Organization: Enterprise Video								
	Device	**Oct 2014**	**Nov 2014**	**Dec 2014**	**Jan 2015**	**Feb 2015**	**Mar 2015**	**Average**
	Endpoint - CTS-500 [1065]							
	Endpoint - LifeSize 200 [1072]							
Average for Organization: Enterprise Video		**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
Overall Average:		**0.00**	**0.00**	**0.00**	**1.02**	**4.81**	**0.29**	**1.02**

Generated on: April 17th, 2015 07:52:24 AM

The following input options are available when generating the report:

- ***Branding***. Optionally enter text that will be displayed at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" will be displayed at the top of the report.
- ***Device Selection***: Select the devices that will appear in the report. The choices are:
    - *All devices*. Select this checkbox if you want all devices in the system to be included in this report.
    - *Organizations*. If the *All devices* checkbox is unselected, select one or more Organizations. The report will contain only the devices in the organizations you select. You can further filter the list of devices to include in the report by selecting devices in the *Devices by Organization* field.
    - *Select individual devices*. If the *All devices* checkbox is unselected, the *Select individual devices* checkbox is available. Select this checkbox if you would like to use the *Devices by Organization* field to select the individual devices to include in the report.
    - *Devices by Organization*. This field displays a list of all devices in the organizations selected in the *Organizations field*. If the *Select individual devices* checkbox is selected, you can select one or more devices to include in the report.
- ***Device Group Selector***: Select the device groups that will appear in the report. The following input elements appear in this component:

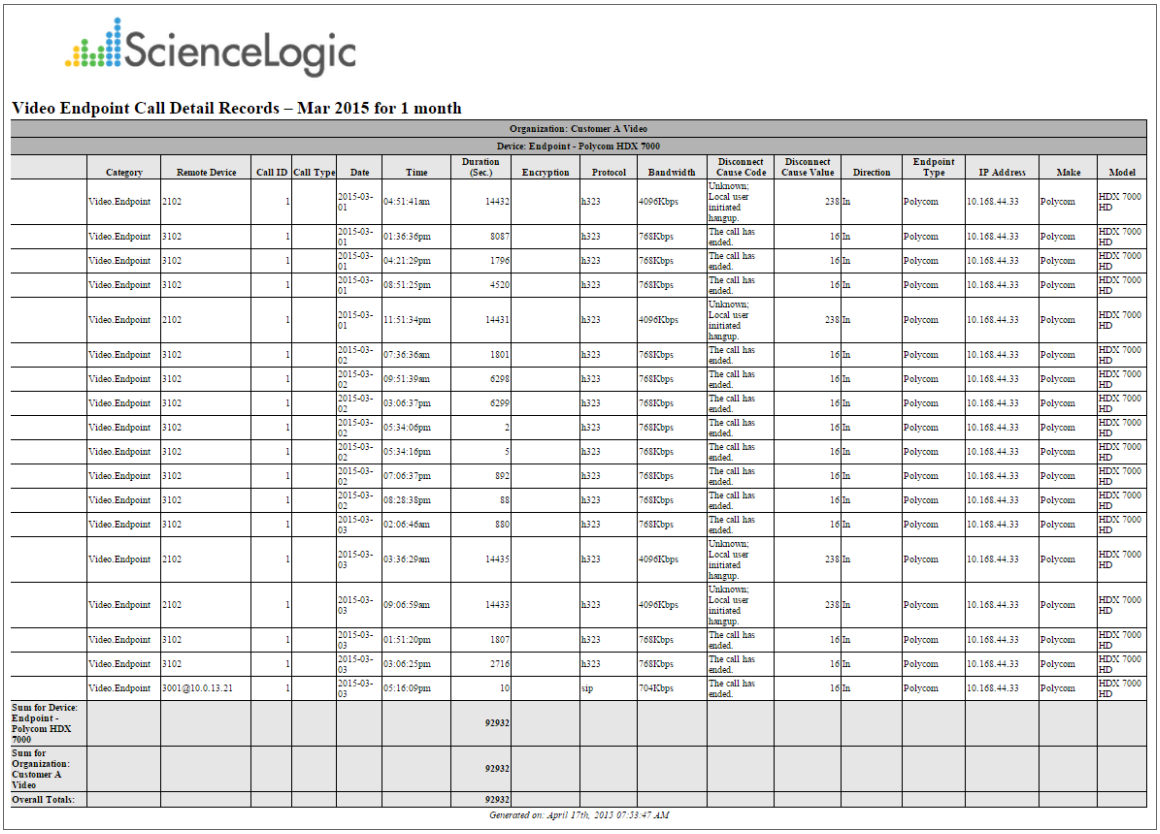
    - *Select By Device Group*. Select this checkbox if you want to select which device groups to include in the report.
    - *Device Groups*. If the *Select By Device Group* checkbox is selected, select one or more device groups. The report will contain only the devices in the device groups you select.
- ***Device Categories***. By default, the *All Device Categories* checkbox is selected. To limit the report to one or more specific device categories, select one or more device categories from the list of *Device Categories*.
- ***General Display Options***. Specify how the report will be arranged:
    - ***Separated By***. Select whether the report will be separated into multiple tables. The report can be separated to include one table per organization, one table per device group, or one table per device.
    - ***Naming***. These checkboxes allow you to select whether the Device ID or the Organization ID will appear in the report.
    - ***Report Sections***. Select whether you want the report to display *Details Only*, *Totals Only*, or *Both*.
- ***Report Span***. Specify a *Daily*, *Weekly*, or *Monthly* span to include in the report. ***Starting***. Use the *Year*, *Month*, and *Date* fields to specify a Start Date for the report. The SL1 system will use data from that date as the starting point of the report.***Duration***. Specify the duration for the report, from 1 month to 36 months. The SL1 system will use data from the Starting date as the start point of the report and data from the last day of the Duration as the ending point of the report.***Timezone***. Specify the timezone to use for date and time values in the report. Specify the timezone by number of hours offset from UTC.
- ***Report Type***. Specify that the report should include all selected devices or that the report should be limited to include a set number of devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the Video Reports PowerPack. This report might have been modified on your SL1 system.

Video Endpoint Call Detail Records Report

This report displays call detail records for Cisco CE Series, Tandberg, LifeSize, and Polycom video endpoints. For each device included in the report, the report displays information about each call during the time period selected for the report. The report displays columns for Call ID, Remote Device, Date, Time, Duration in minutes, Encryption, Protocol, Disconnect Cause Code, Disconnect Cause Value, and Direction (In or Out).

You can customize the output to include only specific devices and call parameters. You can also specify the time span of information to include in the report, text that will appear at the top of the report, and how the devices will be sorted and arranged in the report.



ScienceLogic

Video Endpoint Call Detail Records – Mar 2015 for 1 month

	Organization: Customer A Video																
	Device: Endpoint - Polycom HDX 7000																
	Category	Remote Device	Call ID	Call Type	Date	Time	Duration (Sec.)	Encryption	Protocol	Bandwidth	Disconnect Cause Code	Disconnect Cause Value	Direction	Endpoint Type	IP Address	Make	Model
	Video.Endpoint	2102	1		2015-03-01	04:51:41am	14432		h323	4096Kbps	Unknown; Local user initiated hangup.	238	In	Polycom	10.168.44.33	Polycom	HDX 7000 HD
	Video.Endpoint	3102	1		2015-03-01	01:36:36pm	8087		h323	768Kbps	The call has ended.	16	In	Polycom	10.168.44.33	Polycom	HDX 7000 HD
	Video.Endpoint	3102	1		2015-03-01	04:21:29pm	1796		h323	768Kbps	The call has ended.	16	In	Polycom	10.168.44.33	Polycom	HDX 7000 HD
	Video.Endpoint	3102	1		2015-03-01	08:51:25pm	4520		h323	768Kbps	The call has ended.	16	In	Polycom	10.168.44.33	Polycom	HDX 7000 HD
	Video.Endpoint	2102	1		2015-03-01	11:51:34pm	14431		h323	4096Kbps	Unknown; Local user initiated hangup.	238	In	Polycom	10.168.44.33	Polycom	HDX 7000 HD
	Video.Endpoint	3102	1		2015-03-02	07:36:36am	1801		h323	768Kbps	The call has ended.	16	In	Polycom	10.168.44.33	Polycom	HDX 7000 HD
	Video.Endpoint	3102	1		2015-03-02	09:51:39am	6298		h323	768Kbps	The call has ended.	16	In	Polycom	10.168.44.33	Polycom	HDX 7000 HD
	Video.Endpoint	3102	1		2015-03-02	03:06:37pm	6299		h323	768Kbps	The call has ended.	16	In	Polycom	10.168.44.33	Polycom	HDX 7000 HD
	Video.Endpoint	3102	1		2015-03-02	05:34:06pm	2		h323	768Kbps	The call has ended.	16	In	Polycom	10.168.44.33	Polycom	HDX 7000 HD
	Video.Endpoint	3102	1		2015-03-02	05:34:16pm	5		h323	768Kbps	The call has ended.	16	In	Polycom	10.168.44.33	Polycom	HDX 7000 HD
	Video.Endpoint	3102	1		2015-03-02	07:06:37pm	892		h323	768Kbps	The call has ended.	16	In	Polycom	10.168.44.33	Polycom	HDX 7000 HD
	Video.Endpoint	3102	1		2015-03-02	08:28:38pm	88		h323	768Kbps	The call has ended.	16	In	Polycom	10.168.44.33	Polycom	HDX 7000 HD
	Video.Endpoint	3102	1		2015-03-03	02:06:46am	880		h323	768Kbps	The call has ended.	16	In	Polycom	10.168.44.33	Polycom	HDX 7000 HD
	Video.Endpoint	2102	1		2015-03-03	03:36:29am	14435		h323	4096Kbps	Unknown; Local user initiated hangup.	238	In	Polycom	10.168.44.33	Polycom	HDX 7000 HD
	Video.Endpoint	2102	1		2015-03-03	09:06:59am	14433		h323	4096Kbps	Unknown; Local user initiated hangup.	238	In	Polycom	10.168.44.33	Polycom	HDX 7000 HD
	Video.Endpoint	3102	1		2015-03-03	01:51:20pm	1807		h323	768Kbps	The call has ended.	16	In	Polycom	10.168.44.33	Polycom	HDX 7000 HD
	Video.Endpoint	3102	1		2015-03-03	03:06:25pm	2716		h323	768Kbps	The call has ended.	16	In	Polycom	10.168.44.33	Polycom	HDX 7000 HD
	Video.Endpoint	3001@10.0.13.21	1		2015-03-03	05:16:09pm	10		sip	704Kbps	The call has ended.	16	In	Polycom	10.168.44.33	Polycom	HDX 7000 HD
Sum for Device: Endpoint - Polycom HDX 7000							92932										
Sum for Organization: Customer A Video							92932										
Overall Totals:							92932										

Generated on: April 17th, 2015 07:38:47 AM

The following input options are available when generating the report:

- ***Branding***. Optionally enter text that will be displayed at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" will be displayed at the top of the report.
- ***Device Selection***: Select the devices that will appear in the report. The choices are:
    - *All devices*. Select this checkbox if you want all devices in the system to be included in this report.
    - *Organizations*. If the *All devices* checkbox is unselected, select one or more Organizations. The report will contain only the devices in the organizations you select. You can further filter the list of devices to include in the report by selecting devices in the *Devices by Organization* field.
    - *Select individual devices*. If the *All devices* checkbox is unselected, the *Select individual devices* checkbox is available. Select this checkbox if you would like to use the *Devices by Organization* field to select the individual devices to include in the report.
    - *Devices by Organization*. This field displays a list of all devices in the organizations selected in the *Organizations field*. If the *Select individual devices* checkbox is selected, you can select one or more devices to include in the report.
- ***Device Group Selector***: Select the device groups that will appear in the report. The following input elements appear in this component:
    - *Select By Device Group*. Select this checkbox if you want to select which device groups to include in the report.

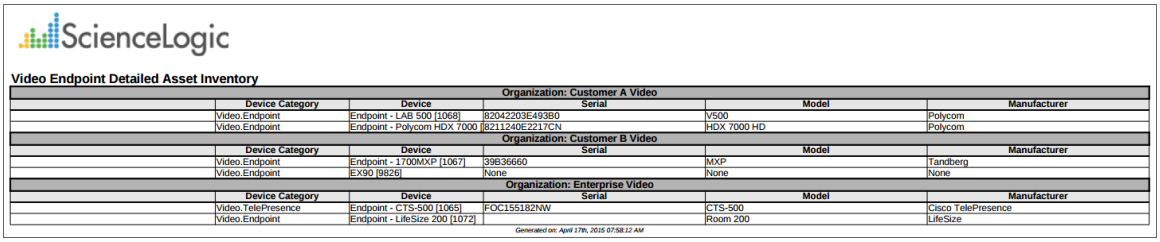
    - *Device Groups*. If the *Select By Device Group* checkbox is selected, select one or more device groups. The report will contain only the devices in the device groups you select.
- ***Report Span***. Specify a *Daily*, *Weekly*, or *Monthly* span to include in the report.
- ***Starting***. Use the *Year*, *Month*, and *Date* fields to specify a Start Date for the report. The SL1 system will use data from that date as the starting point of the report.
- ***Duration***. Specify the duration for the report, from 1 month to 36 months. The SL1 system will use data from the Starting date as the start point of the report and data from the last day of the Duration as the ending point of the report.
- ***Included Columns***. Select the All Columns checkbox or select columns individually from the list.
- ***CDR Output Options***. Specify if you want the duration to be presented in seconds or in hh:mm:ss format.
- ***Device Categories***. By default, the *All Device Categories* checkbox is selected. To limit the report to one or more specific device categories, select one or more device categories from the list of *Device Categories*.
- ***Separated By***. Select whether the report will be separated into multiple tables. The report can be separated to include one table per organization, one table per device group, one table per device category, or one table per device.
- ***Naming***. These checkboxes allow you to select whether the Device ID or the Organization ID will appear in the report.
- ***Report Sections***. Select whether you want the report to display *Details Only*, *Totals Only*, or *Both*.
- ***Filter Options***. Specify the calls to include in the report by selecting one or more of the following filters:
    - *Disconnect Codes*. To include only calls that had a specific disconnect code, select a value in this field. If you select *Specific disconnect codes* in this field, supply a comma-delimited list of disconnect codes in the ***CSV list of specific codes*** field.
    - *Duration*. To include only calls that had a specific duration, enter a minimum duration and a maximum duration.
    - *Encryption Setting*. To include only calls that used a specific encryption setting, select an encryption setting in this field.
    - *Protocol*. To include only calls that used a specific protocol, select a protocol in this field.
- ***Device Specific Columns***. Select additional columns from the list, per CDR application type.

This description covers the latest version of this report as shipped by ScienceLogic in the Video Reports PowerPack. This report might have been modified on your SL1 system.

Video Endpoint Detailed Asset Inventory Report

This report displays a detailed inventory of assets for Tandberg, Polycom, Lifesize, and Cisco TelePresence devices. For each device included in the report, the report displays the device group, device name, serial number, model number, and manufacturer.

You can customize the output to include only specific devices and/or limit the number of devices that are included in the report. You can also specify the time span of information to include in the report, text that will appear at the top of the report, and how the devices will be sorted and arranged in the report.



ScienceLogic

Video Endpoint Detailed Asset Inventory

Organization: Customer A Video					
	Device Category	**Device**	**Serial**	**Model**	**Manufacturer**
	Video.Endpoint	Endpoint - LAB 500 [1068]	82042203E493B0	V500	Polycom
	Video.Endpoint	Endpoint - Polycom HDX 7000 [	8211240E2217CN	HDX 7000 HD	Polycom
Organization: Customer B Video					
	Device Category	**Device**	**Serial**	**Model**	**Manufacturer**
	Video.Endpoint	Endpoint - 1700MXP [1067]	39B36660	MXP	Tandberg
	Video.Endpoint	EX90 [9826]	None	None	None
Organization: Enterprise Video					
	Device Category	**Device**	**Serial**	**Model**	**Manufacturer**
	Video.TelePresence	Endpoint - CTS-500 [1065]	FOC155182NW	CTS-500	Cisco TelePresence
	Video.Endpoint	Endpoint - LifeSize 200 [1072]		Room 200	LifeSize

Generated on: April 17th, 2015 07:58:12 AM

The following input options are available when generating the report:

- ***Branding***. Optionally enter text that will be displayed at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" will be displayed at the top of the report.
- ***Device Selection***: Select the devices that will appear in the report. The choices are:
    - *All devices*. Select this checkbox if you want all devices in the system to be included in this report.
    - *Organizations*. If the *All devices* checkbox is unselected, select one or more Organizations. The report will contain only the devices in the organizations you select. You can further filter the list of devices to include in the report by selecting devices in the *Devices by Organization* field.
    - *Select individual devices*. If the *All devices* checkbox is unselected, the *Select individual devices* checkbox is available. Select this checkbox if you would like to use the *Devices by Organization* field to select the individual devices to include in the report.
    - *Devices by Organization*. This field displays a list of all devices in the organizations selected in the *Organizations field*. If the *Select individual devices* checkbox is selected, you can select one or more devices to include in the report.
- ***Device Group Selector***: Select the device groups that will appear in the report. The following input elements appear in this component:
    - *Select By Device Group*. Select this checkbox if you want to select which device groups to include in the report.
    - *Device Groups*. If the *Select By Device Group* checkbox is selected, select one or more device groups. The report will contain only the devices in the device groups you select.

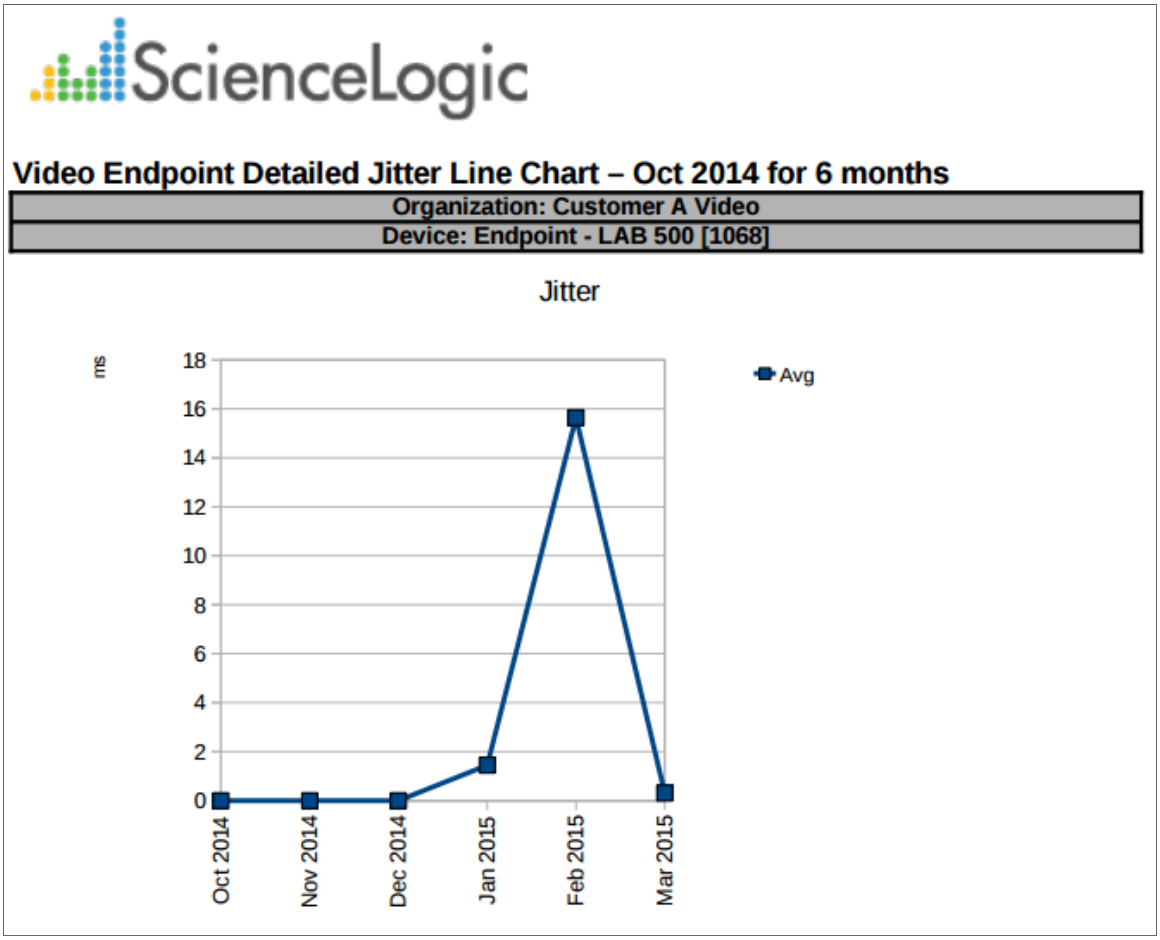
- ***Device Categories***. By default, the *All Device Categories* checkbox is selected. To limit the report to one or more specific device categories, select one or more device categories from the list of *Device Categories*.
- ***General Display Options***. Specify how the report will be arranged:
    - ***Separated By***. Select whether the report will be separated into multiple tables. The report can be separated to include one table per organization, one table per device group, one table per device category, or one table per device.
    - ***Naming***. These checkboxes allow you to select whether the Device ID or the Organization ID will appear in the report.

This description covers the latest version of this report as shipped by ScienceLogic in the Video Reports PowerPack. This report might have been modified on your SL1 system.

Video Endpoint Detailed Jitter Line Chart Report

This report displays the average jitter for Tandberg, Polycom, Lifesize and Cisco TelePresence devices. For each device included in the report, the report displays the jitter average in milliseconds for the time period selected for the report.

You can customize the output to include only specific devices and/or limit the number of devices that are included in the report. You can also specify the time span of information to include in the report, text that will appear at the top of the report, and how the devices will be sorted and arranged in the report.



The following input options are available when generating the report:

- ***Branding***. Optionally enter text that will be displayed at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" will be displayed at the top of the report.
- ***Device Selection***: Select the devices that will appear in the report. The choices are:
    - *All devices*. Select this checkbox if you want all devices in the system to be included in this report.
    - *Organizations*. If the *All devices* checkbox is unselected, select one or more Organizations. The report will contain only the devices in the organizations you select. You can further filter the list of devices to include in the report by selecting devices in the *Devices by Organization* field.
    - *Select individual devices*. If the *All devices* checkbox is unselected, the *Select individual devices* checkbox is available. Select this checkbox if you would like to use the *Devices by Organization* field to select the individual devices to include in the report.

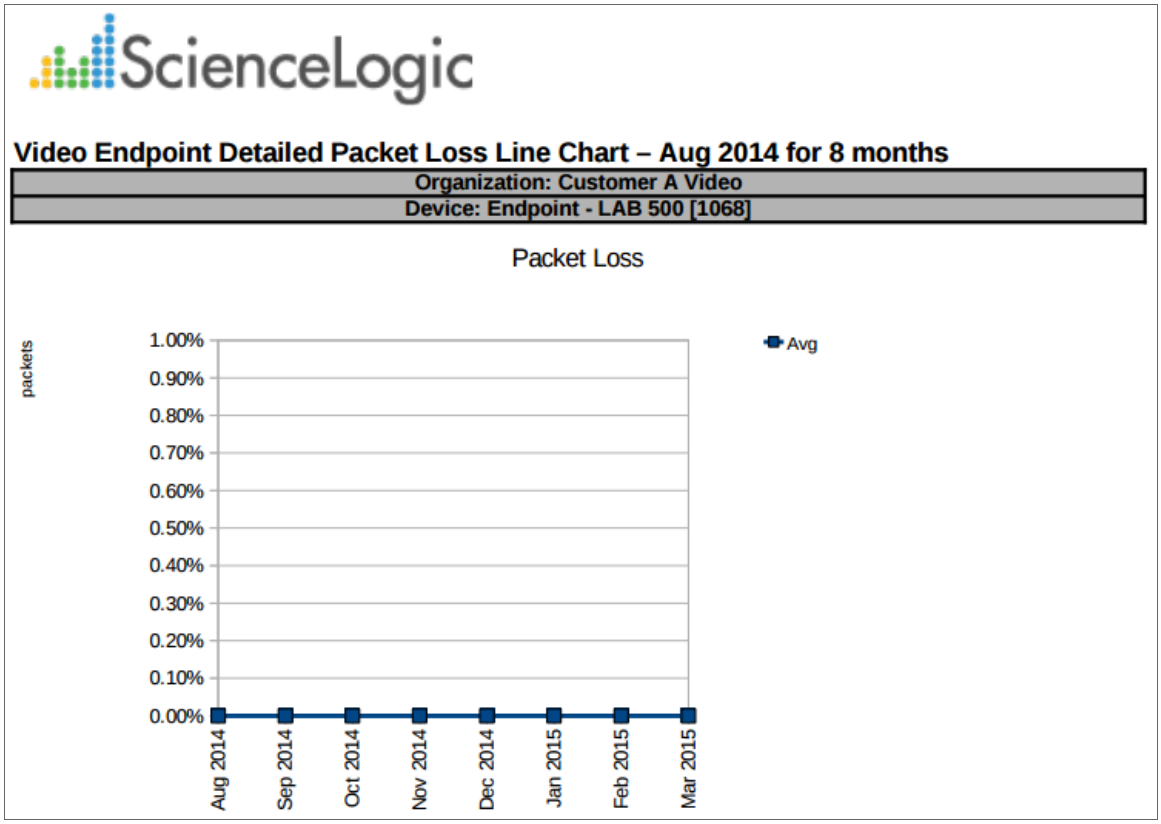
    - *Devices by Organization*. This field displays a list of all devices in the organizations selected in the *Organizations field*. If the *Select individual devices* checkbox is selected, you can select one or more devices to include in the report.
- ***Device Group Selector***: Select the device groups that will appear in the report. The following input elements appear in this component:
    - *Select By Device Group*. Select this checkbox if you want to select which device groups to include in the report.
    - *Device Groups*. If the *Select By Device Group* checkbox is selected, select one or more device groups. The report will contain only the devices in the device groups you select.
- ***Device Categories***. By default, the *All Device Categories* checkbox is selected. To limit the report to one or more specific device categories, select one or more device categories from the list of *Device Categories*.
- ***General Display Options***. Specify how the report will be arranged:
    - ***Separated By***. Select whether the report will be separated into multiple tables. The report can be separated to include one table per organization, one table per device group, or one table per device category.
    - ***Naming***. These checkboxes allow you to select whether the Device ID or the Organization ID will appear in the report.
    - ***Stacking***. Select the *Enable Stacking* checkbox to allow data to be stacked.
- ***Report Span***. Specify a *Daily*, *Weekly*, or *Monthly* span to include in the report. ***Starting***. Use the *Year*, *Month*, and *Date* fields to specify a Start Date for the report. The SL1 system will use data from that date as the starting point of the report.***Duration***. Specify the duration for the report, from 1 month to 36 months. The SL1 system will use data from the Starting date as the start point of the report and data from the last day of the Duration as the ending point of the report.***Timezone***. Specify the timezone to use for date and time values in the report. Specify the timezone by number of hours offset from UTC.
- ***Report Type***. Specify that the report should include all selected devices or that the report should be limited to include a set number of devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the Video Reports PowerPack. This report might have been modified on your SL1 system.

Video Endpoint Detailed Packet Loss Line Chart Report

This report displays the packet loss for Tandberg, Lifesize, Cisco, and Polycom video endpoints. For each device included in the report, the report displays the packet loss by percentage over the time period selected for the report.

You can customize the output to include only specific devices and/or limit the number of devices that are included in the report. You can also specify the time span of information to include in the report, text that will appear at the top of the report, and how the devices will be sorted and arranged in the report.



The following input options are available when generating the report:

- ***Branding***. Optionally enter text that will be displayed at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" will be displayed at the top of the report.

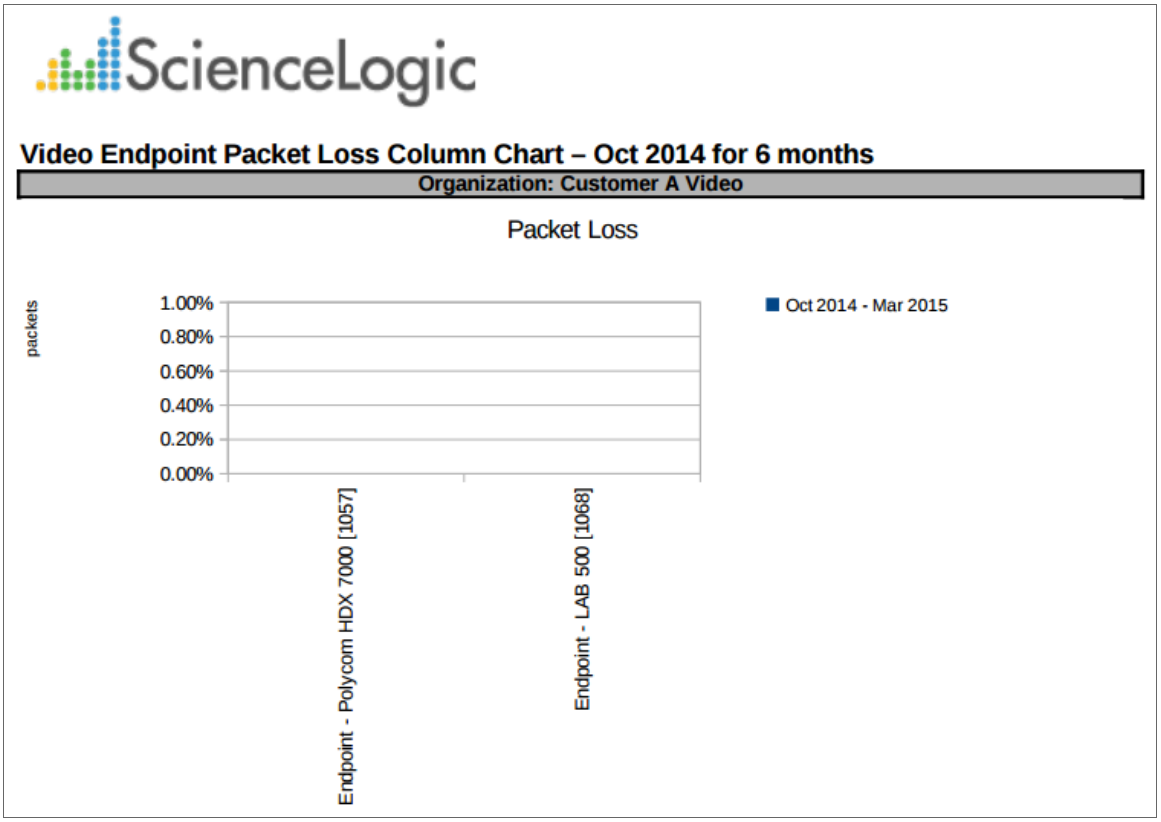
- ***Device Selection***: Select the devices that will appear in the report. The choices are:
    - *All devices*. Select this checkbox if you want all devices in the system to be included in this report.
    - *Organizations*. If the *All devices* checkbox is unselected, select one or more Organizations. The report will contain only the devices in the organizations you select. You can further filter the list of devices to include in the report by selecting devices in the *Devices by Organization* field.
    - *Select individual devices*. If the *All devices* checkbox is unselected, the *Select individual devices* checkbox is available. Select this checkbox if you would like to use the *Devices by Organization* field to select the individual devices to include in the report.
    - *Devices by Organization*. This field displays a list of all devices in the organizations selected in the *Organizations field*. If the *Select individual devices* checkbox is selected, you can select one or more devices to include in the report.
- ***Device Group Selector***: Select the device groups that will appear in the report. The following input elements appear in this component:
    - *Select By Device Group*. Select this checkbox if you want to select which device groups to include in the report.
    - *Device Groups*. If the *Select By Device Group* checkbox is selected, select one or more device groups. The report will contain only the devices in the device groups you select.
- ***Device Categories***. By default, the *All Device Categories* checkbox is selected. To limit the report to one or more specific device categories, select one or more device categories from the list of *Device Categories*.
- ***General Display Options***. Specify how the report will be arranged:
    - ***Separated By***. Select whether the report will be separated into multiple tables. The report can be separated to include one table per organization, one table per device group, or one table per device category.
    - ***Naming***. These checkboxes allow you to select whether the Device ID or the Organization ID will appear in the report.
    - ***Stacking***. Select the *Enable Stacking* checkbox to allow data to be stacked.
- ***Report Span***. Specify a *Daily*, *Weekly*, or *Monthly* span to include in the report. ***Starting***. Use the *Year*, *Month*, and *Date* fields to specify a Start Date for the report. The SL1 system will use data from that date as the starting point of the report.***Duration***. Specify the duration for the report, from 1 month to 36 months. The SL1 system will use data from the Starting date as the start point of the report and data from the last day of the Duration as the ending point of the report.***Timezone***. Specify the timezone to use for date and time values in the report. Specify the timezone by number of hours offset from UTC.
- ***Report Type***. Specify that the report should include all selected devices or that the report should be limited to include a set number of devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the Video Reports PowerPack. This report might have been modified on your SL1 system.

Video Endpoint Packet Loss Column Chart Report

This report displays the packet loss for Tandberg, Lifesize, Cisco, and Polycom video endpoints. For each device included in the report, the report displays the packet loss by percentage over the time period selected for the report.

You can customize the output to include only specific devices and/or limit the number of devices that are included in the report. You can also specify the time span of information to include in the report, text that will appear at the top of the report, and how the devices will be sorted and arranged in the report.



The following input options are available when generating the report:

- ***Branding***. Optionally enter text that will be displayed at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" will be displayed at the top of the report.
- ***Device Selection***: Select the devices that will appear in the report. The choices are:
    - *All devices*. Select this checkbox if you want all devices in the system to be included in this report.
    - *Organizations*. If the *All devices* checkbox is unselected, select one or more Organizations. The report will contain only the devices in the organizations you select. You can further filter the list of devices to include in the report by selecting devices in the *Devices by Organization* field.

- *Select individual devices*. If the *All devices* checkbox is unselected, the *Select individual devices* checkbox is available. Select this checkbox if you would like to use the *Devices by Organization* field to select the individual devices to include in the report.
- *Devices by Organization*. This field displays a list of all devices in the organizations selected in the *Organizations field*. If the *Select individual devices* checkbox is selected, you can select one or more devices to include in the report.

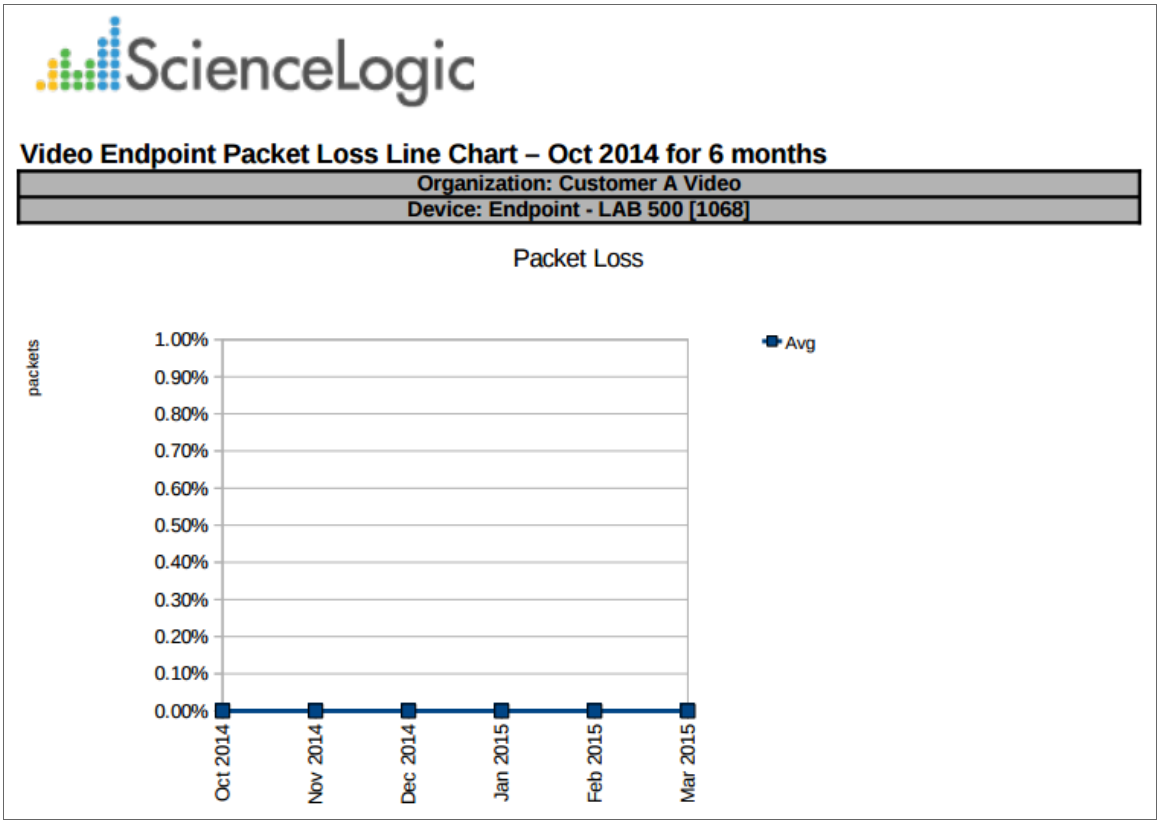
- ***Device Group Selector***: Select the device groups that will appear in the report. The following input elements appear in this component:
  - *Select By Device Group*. Select this checkbox if you want to select which device groups to include in the report.
  - *Device Groups*. If the *Select By Device Group* checkbox is selected, select one or more device groups. The report will contain only the devices in the device groups you select.
- ***Device Categories***. By default, the *All Device Categories* checkbox is selected. To limit the report to one or more specific device categories, select one or more device categories from the list of *Device Categories*.
- ***General Display Options***. Specify how the report will be arranged:
  - ***Separated By***. Select whether the report will be separated into multiple tables. The report can be separated to include one table per organization, one table per device group, one table per device category, or one table per device.
  - ***Naming***. These checkboxes allow you to select whether the Device ID or the Organization ID will appear in the report.
  - ***Stacking***. Select the *Enable Stacking* checkbox to allow data to be stacked.
- ***Report Span***. Specify a *Daily*, *Weekly*, or *Monthly* span to include in the report. ***Starting***. Use the *Year*, *Month*, and *Date* fields to specify a Start Date for the report. The SL1 system will use data from that date as the starting point of the report.***Duration***. Specify the duration for the report, from 1 month to 36 months. The SL1 system will use data from the Starting date as the start point of the report and data from the last day of the Duration as the ending point of the report.***Timezone***. Specify the timezone to use for date and time values in the report. Specify the timezone by number of hours offset from UTC.
- ***Report Type***. Specify that the report should include all selected devices or that the report should be limited to include a set number of devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the Video Reports PowerPack. This report might have been modified on your SL1 system.

Video Endpoint Packet Loss Line Chart Report

This report displays the packet loss for Tandberg, Lifesize, Cisco, and Polycom video endpoints. For each device included in the report, the report displays the packet loss by percentage over the time period selected for the report.

You can customize the output to include only specific devices and/or limit the number of devices that are included in the report. You can also specify the time span of information to include in the report, text that will appear at the top of the report, and how the devices will be sorted and arranged in the report.



The following input options are available when generating the report:

- ***Branding***. Optionally enter text that will be displayed at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" will be displayed at the top of the report.
- ***Device Selection***: Select the devices that will appear in the report. The choices are:
    - *All devices*. Select this checkbox if you want all devices in the system to be included in this report.
    - *Organizations*. If the *All devices* checkbox is unselected, select one or more Organizations. The report will contain only the devices in the organizations you select. You can further filter the list of devices to include in the report by selecting devices in the *Devices by Organization* field.

- *Select individual devices*. If the *All devices* checkbox is unselected, the *Select individual devices* checkbox is available. Select this checkbox if you would like to use the *Devices by Organization* field to select the individual devices to include in the report.
- *Devices by Organization*. This field displays a list of all devices in the organizations selected in the *Organizations field*. If the *Select individual devices* checkbox is selected, you can select one or more devices to include in the report.

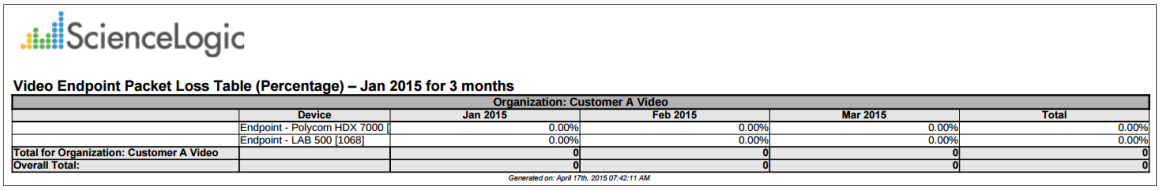
- ***Device Group Selector***: Select the device groups that will appear in the report. The following input elements appear in this component:
  - *Select By Device Group*. Select this checkbox if you want to select which device groups to include in the report.
  - *Device Groups*. If the *Select By Device Group* checkbox is selected, select one or more device groups. The report will contain only the devices in the device groups you select.
- ***Device Categories***. By default, the *All Device Categories* checkbox is selected. To limit the report to one or more specific device categories, select one or more device categories from the list of *Device Categories*.
- ***General Display Options***. Specify how the report will be arranged:
  - ***Separated By***. Select whether the report will be separated into multiple tables. The report can be separated to include one table per organization, one table per device group, one table per device category, or one table per device.
  - ***Naming***. These checkboxes allow you to select whether the Device ID or the Organization ID will appear in the report.
  - ***Stacking***. Select the *Enable Stacking* checkbox to allow data to be stacked.
- ***Report Span***. Specify a *Daily*, *Weekly*, or *Monthly* span to include in the report. ***Starting***. Use the *Year*, *Month*, and *Date* fields to specify a Start Date for the report. The SL1 system will use data from that date as the starting point of the report.***Duration***. Specify the duration for the report, from 1 month to 36 months. The SL1 system will use data from the Starting date as the start point of the report and data from the last day of the Duration as the ending point of the report.***Timezone***. Specify the timezone to use for date and time values in the report. Specify the timezone by number of hours offset from UTC.
- ***Report Type***. Specify that the report should include all selected devices or that the report should be limited to include a set number of devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the Video Reports PowerPack. This report might have been modified on your SL1 system.

Video Endpoint Packet Loss Table Report

This report displays the packet loss for Tandberg, Lifesize, Cisco, and Polycom video endpoints. For each device included in the report, the report displays the packet loss by percentage over the time period selected for the report.

You can customize the output to include only specific devices and/or limit the number of devices that are included in the report. You can also specify the time span of information to include in the report, text that will appear at the top of the report, and how the devices will be sorted and arranged in the report.



ScienceLogic

Video Endpoint Packet Loss Table (Percentage) – Jan 2015 for 3 months

Organization: Customer A Video					
	Device	Jan 2015	Feb 2015	Mar 2015	Total
	Endpoint - Polycom HDX 7000 [	0.00%	0.00%	0.00%	0.00%
	Endpoint - LAB 500 [1068]	0.00%	0.00%	0.00%	0.00%
Total for Organization: Customer A Video		**0**	**0**	**0**	**0**
Overall Total:		**0**	**0**	**0**	**0**

Generated on: April 17th, 2015 07:42:11 AM

The following input options are available when generating the report:

- ***Branding***. Optionally enter text that will be displayed at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" will be displayed at the top of the report.
- ***Device Selection***: Select the devices that will appear in the report. The choices are:
    - *All devices*. Select this checkbox if you want all devices in the system to be included in this report.
    - *Organizations*. If the *All devices* checkbox is unselected, select one or more Organizations. The report will contain only the devices in the organizations you select. You can further filter the list of devices to include in the report by selecting devices in the *Devices by Organization* field.
    - *Select individual devices*. If the *All devices* checkbox is unselected, the *Select individual devices* checkbox is available. Select this checkbox if you would like to use the *Devices by Organization* field to select the individual devices to include in the report.
    - *Devices by Organization*. This field displays a list of all devices in the organizations selected in the *Organizations field*. If the *Select individual devices* checkbox is selected, you can select one or more devices to include in the report.
- ***Device Group Selector***: Select the device groups that will appear in the report. The following input elements appear in this component:
    - *Select By Device Group*. Select this checkbox if you want to select which device groups to include in the report.
    - *Device Groups*. If the *Select By Device Group* checkbox is selected, select one or more device groups. The report will contain only the devices in the device groups you select.

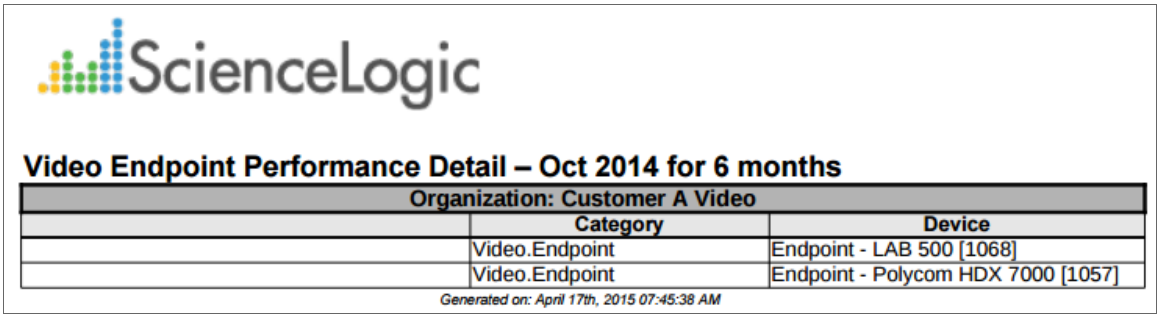
- ***Device Categories***. By default, the *All Device Categories* checkbox is selected. To limit the report to one or more specific device categories, select one or more device categories from the list of *Device Categories*.
- ***General Display Options***. Specify how the report will be arranged:
    - ***Separated By***. Select whether the report will be separated into multiple tables. The report can be separated to include one table per organization, one table per device group, one table per device category, or one table per device.
    - ***Naming***. These checkboxes allow you to select whether the Device ID or the Organization ID will appear in the report.
    - ***Report Sections***. Select whether you want the report to display *Details Only*, *Totals Only*, or *Both*.
- ***Report Span***. Specify a *Daily*, *Weekly*, or *Monthly* span to include in the report. ***Starting***. Use the *Year*, *Month*, and *Date* fields to specify a Start Date for the report. The SL1 system will use data from that date as the starting point of the report.***Duration***. Specify the duration for the report, from 1 month to 36 months. The SL1 system will use data from the Starting date as the start point of the report and data from the last day of the Duration as the ending point of the report.***Timezone***. Specify the timezone to use for date and time values in the report. Specify the timezone by number of hours offset from UTC.
- ***Report Type***. Specify that the report should include all selected devices or that the report should be limited to include a set number of devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the Video Reports PowerPack. This report might have been modified on your SL1 system.

Video Endpoint Performance Detail Report

This report displays a performance detail for Tandberg, Lifesize, Cisco, and Polycom video endpoints. The report displays the organizations, device groups, device names, average RX audio and video packet loss, average TX audio and video packet loss, average RX audio and video jitter, and average RX and TX bandwidth.

You can customize the output to include only specific devices and/or limit the number of devices that are included in the report. You can also specify the time span of information to include in the report, text that will appear at the top of the report, and how the devices will be sorted and arranged in the report.



The following input options are available when generating the report:

- ***Branding***. Optionally enter text that will be displayed at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" will be displayed at the top of the report.

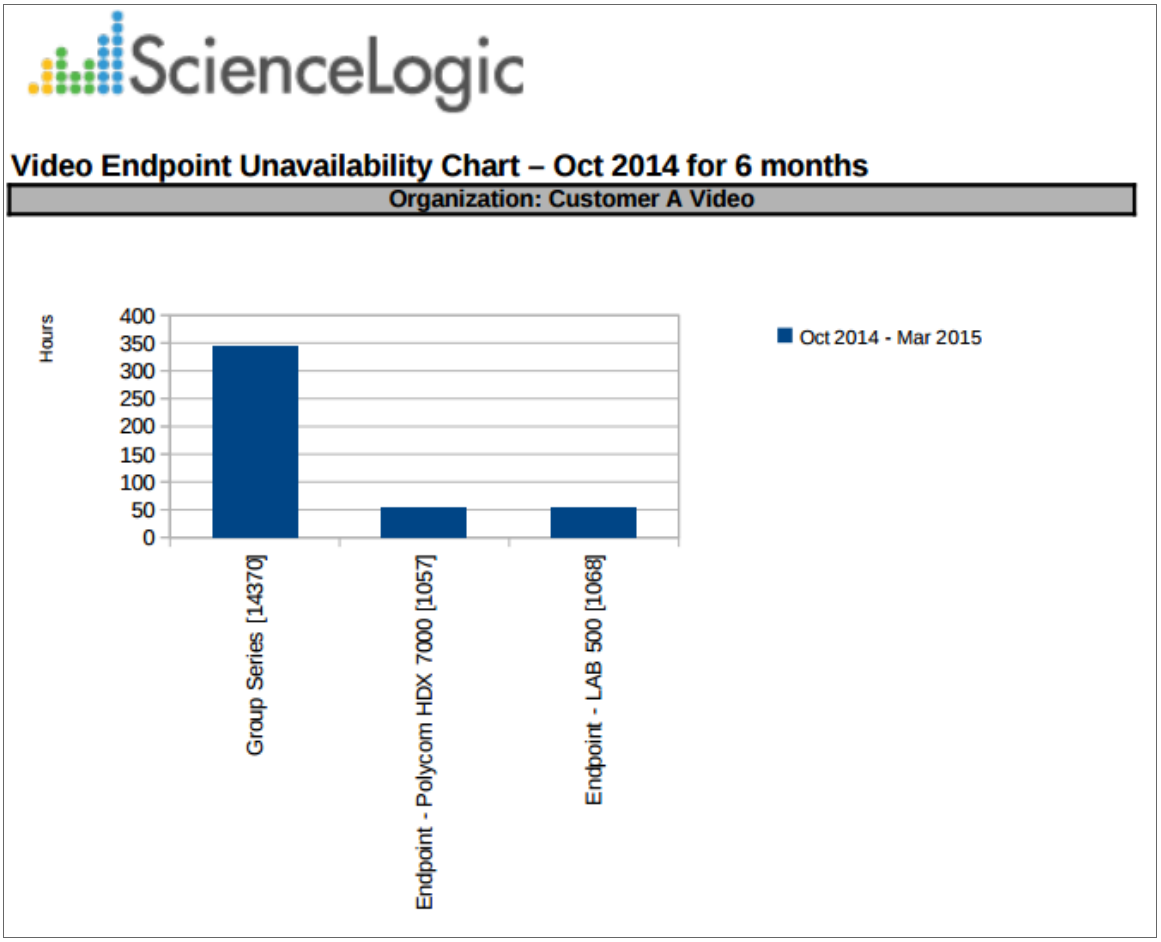
- ***Device Selection***: Select the devices that will appear in the report. The choices are:
    - *All devices*. Select this checkbox if you want all devices in the system to be included in this report.
    - *Organizations*. If the *All devices* checkbox is unselected, select one or more Organizations. The report will contain only the devices in the organizations you select. You can further filter the list of devices to include in the report by selecting devices in the *Devices by Organization* field.
    - *Select individual devices*. If the *All devices* checkbox is unselected, the *Select individual devices* checkbox is available. Select this checkbox if you would like to use the *Devices by Organization* field to select the individual devices to include in the report.
    - *Devices by Organization*. This field displays a list of all devices in the organizations selected in the *Organizations field*. If the *Select individual devices* checkbox is selected, you can select one or more devices to include in the report.
- ***Device Group Selector***: Select the device groups that will appear in the report. The following input elements appear in this component:
    - *Select By Device Group*. Select this checkbox if you want to select which device groups to include in the report.
    - *Device Groups*. If the *Select By Device Group* checkbox is selected, select one or more device groups. The report will contain only the devices in the device groups you select.
- ***Device Categories***. By default, the *All Device Categories* checkbox is selected. To limit the report to one or more specific device categories, select one or more device categories from the list of *Device Categories*.
- ***General Display Options***. Specify how the report will be arranged:
    - ***Separated By***. Select whether the report will be separated into multiple tables. The report can be separated to include one table per organization, one table per device group, one table per device category, or one table per device.
    - ***Naming***. These checkboxes allow you to select whether the Device ID or the Organization ID will appear in the report.
    - ***Report Sections***. Select whether you want the report to display *Details Only*, *Totals Only*, or *Both*.
    - ***Sort By***. Select whether the report will appear in Ascending or Descending order and the type of packet loss.
- ***Report Span***. Specify a *Daily*, *Weekly*, or *Monthly* span to include in the report. ***Starting***. Use the *Year*, *Month*, and *Date* fields to specify a Start Date for the report. The SL1 system will use data from that date as the starting point of the report.***Duration***. Specify the duration for the report, from 1 month to 36 months. The SL1 system will use data from the Starting date as the start point of the report and data from the last day of the Duration as the ending point of the report.***Timezone***. Specify the timezone to use for date and time values in the report. Specify the timezone by number of hours offset from UTC.
- ***Report Type***. Specify that the report should include all selected devices or that the report should be limited to include a set number of devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the Video Reports PowerPack. This report might have been modified on your SL1 system.

Video Endpoint Unavailability Chart Report

This report displays a bar graph of unavailability for Tandberg, Polycom, Lifesize and Cisco TelePresence devices. For each device included in the report, the report displays the number of hours the device was unavailable during the time period selected for the report.

You can customize the output to include only specific devices and/or limit the number of devices that are included in the report. You can also specify the time span of information to include in the report, text that will appear at the top of the report, and how the devices will be sorted and arranged in the report.



The following input options are available when generating the report:

- ***Branding***. Optionally enter text that will be displayed at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" will be displayed at the top of the report.
- ***Device Selection***: Select the devices that will appear in the report. The choices are:
    - *All devices*. Select this checkbox if you want all devices in the system to be included in this report.

- *Organizations*. If the *All devices* checkbox is unselected, select one or more Organizations. The report will contain only the devices in the organizations you select. You can further filter the list of devices to include in the report by selecting devices in the *Devices by Organization* field.
- *Select individual devices*. If the *All devices* checkbox is unselected, the *Select individual devices* checkbox is available. Select this checkbox if you would like to use the *Devices by Organization* field to select the individual devices to include in the report.
- *Devices by Organization*. This field displays a list of all devices in the organizations selected in the *Organizations field*. If the *Select individual devices* checkbox is selected, you can select one or more devices to include in the report.

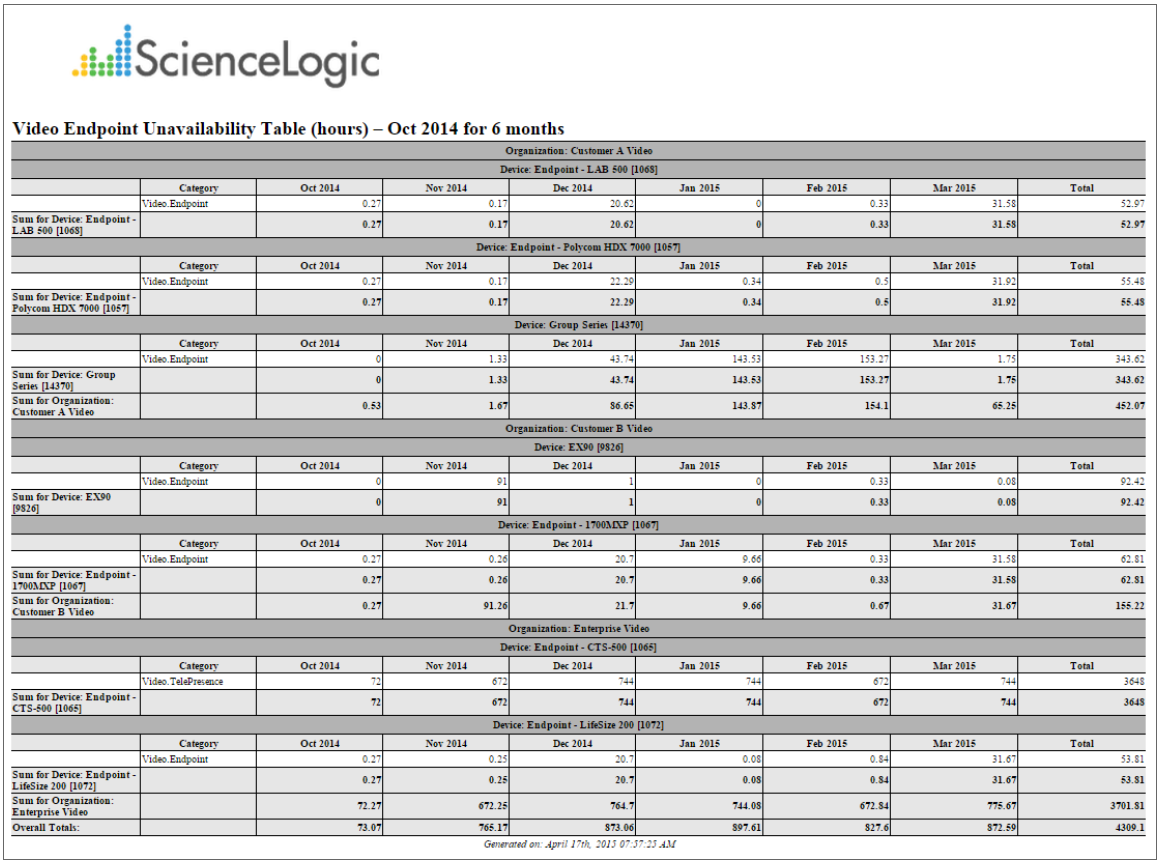
- ***Device Group Selector***: Select the device groups that will appear in the report. The following input elements appear in this component:
  - *Select By Device Group*. Select this checkbox if you want to select which device groups to include in the report.
  - *Device Groups*. If the *Select By Device Group* checkbox is selected, select one or more device groups. The report will contain only the devices in the device groups you select.
- ***Device Categories***. By default, the *All Device Categories* checkbox is selected. To limit the report to one or more specific device categories, select one or more device categories from the list of *Device Categories*.
- ***General Display Options***. Specify how the report will be arranged:
  - ***Separated By***. Select whether the report will be separated into multiple tables. The report can be separated to include one table per organization, one table per device group, one table per device category, or one table per device.
  - ***Naming***. These checkboxes allow you to select whether the Device ID or the Organization ID will appear in the report.
  - ***Stacking***. Select the *Enable Stacking* checkbox to allow data to be stacked.
- ***Report Span***. Specify a *Daily*, *Weekly*, or *Monthly* span to include in the report. ***Starting***. Use the *Year*, *Month*, and *Date* fields to specify a Start Date for the report. The SL1 system will use data from that date as the starting point of the report.***Duration***. Specify the duration for the report, from 1 month to 36 months. The SL1 system will use data from the Starting date as the start point of the report and data from the last day of the Duration as the ending point of the report.***Timezone***. Specify the timezone to use for date and time values in the report. Specify the timezone by number of hours offset from UTC.
- ***Report Type***. Specify that the report should include all selected devices or that the report should be limited to include a set number of devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the Video Reports PowerPack. This report might have been modified on your SL1 system.

Video Endpoint Unavailability Table Report

This report displays a table of unavailability for Tandberg, Polycom, Lifesize and Cisco TelePresence devices. For each device included in the report, the report displays the number of hours the device was unavailable during the time period selected for the report.

You can customize the output to include only specific devices and/or limit the number of devices that are included in the report. You can also specify the time span of information to include in the report, text that will appear at the top of the report, and how the devices will be sorted and arranged in the report.



Video Endpoint Unavailability Table (hours) – Oct 2014 for 6 months

Organization: Customer A Video								
Device: Endpoint - LAB 500 [1068]								
	Category	**Oct 2014**	**Nov 2014**	**Dec 2014**	**Jan 2015**	**Feb 2015**	**Mar 2015**	**Total**
	Video.Endpoint	0.27	0.17	20.62	0	0.33	31.58	52.97
Sum for Device: Endpoint - LAB 500 [1068]		**0.27**	**0.17**	**20.62**	**0**	**0.33**	**31.58**	**52.97**
Device: Endpoint - Polycom HDX 7000 [1057]								
	Category	**Oct 2014**	**Nov 2014**	**Dec 2014**	**Jan 2015**	**Feb 2015**	**Mar 2015**	**Total**
	Video.Endpoint	0.27	0.17	22.29	0.34	0.5	31.92	55.48
Sum for Device: Endpoint - Polycom HDX 7000 [1057]		**0.27**	**0.17**	**22.29**	**0.34**	**0.5**	**31.92**	**55.48**
Device: Group Series [14370]								
	Category	**Oct 2014**	**Nov 2014**	**Dec 2014**	**Jan 2015**	**Feb 2015**	**Mar 2015**	**Total**
	Video.Endpoint	0	1.33	43.74	143.53	153.27	1.75	343.62
Sum for Device: Group Series [14370]		**0**	**1.33**	**43.74**	**143.53**	**153.27**	**1.75**	**343.62**
Sum for Organization: Customer A Video		**0.53**	**1.67**	**86.65**	**143.87**	**154.1**	**65.25**	**452.07**
Organization: Customer B Video								
Device: EX90 [9826]								
	Category	**Oct 2014**	**Nov 2014**	**Dec 2014**	**Jan 2015**	**Feb 2015**	**Mar 2015**	**Total**
	Video.Endpoint	0	91	1	0	0.33	0.08	92.42
Sum for Device: EX90 [9826]		**0**	**91**	**1**	**0**	**0.33**	**0.08**	**92.42**
Device: Endpoint - 1700MXP [1067]								
	Category	**Oct 2014**	**Nov 2014**	**Dec 2014**	**Jan 2015**	**Feb 2015**	**Mar 2015**	**Total**
	Video.Endpoint	0.27	0.26	20.7	9.66	0.33	31.58	62.81
Sum for Device: Endpoint - 1700MXP [1067]		**0.27**	**0.26**	**20.7**	**9.66**	**0.33**	**31.58**	**62.81**
Sum for Organization: Customer B Video		**0.27**	**91.26**	**21.7**	**9.66**	**0.67**	**31.67**	**155.22**
Organization: Enterprise Video								
Device: Endpoint - CTS-500 [1065]								
	Category	**Oct 2014**	**Nov 2014**	**Dec 2014**	**Jan 2015**	**Feb 2015**	**Mar 2015**	**Total**
	Video.TelePresence	72	672	744	744	672	744	3648
Sum for Device: Endpoint - CTS-500 [1065]		**72**	**672**	**744**	**744**	**672**	**744**	**3648**
Device: Endpoint - LifeSize 200 [1072]								
	Category	**Oct 2014**	**Nov 2014**	**Dec 2014**	**Jan 2015**	**Feb 2015**	**Mar 2015**	**Total**
	Video.Endpoint	0.27	0.25	20.7	0.08	0.84	31.67	53.81
Sum for Device: Endpoint - LifeSize 200 [1072]		**0.27**	**0.25**	**20.7**	**0.08**	**0.84**	**31.67**	**53.81**
Sum for Organization: Enterprise Video		**72.27**	**672.25**	**764.7**	**744.08**	**672.84**	**775.67**	**3701.81**
Overall Totals:		**73.07**	**765.17**	**873.06**	**897.61**	**827.6**	**872.59**	**4309.1**

Generated on: April 17th, 2013 07:37:25 AM

The following input options are available when generating the report:

- ***Branding***. Optionally enter text that will be displayed at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" will be displayed at the top of the report.

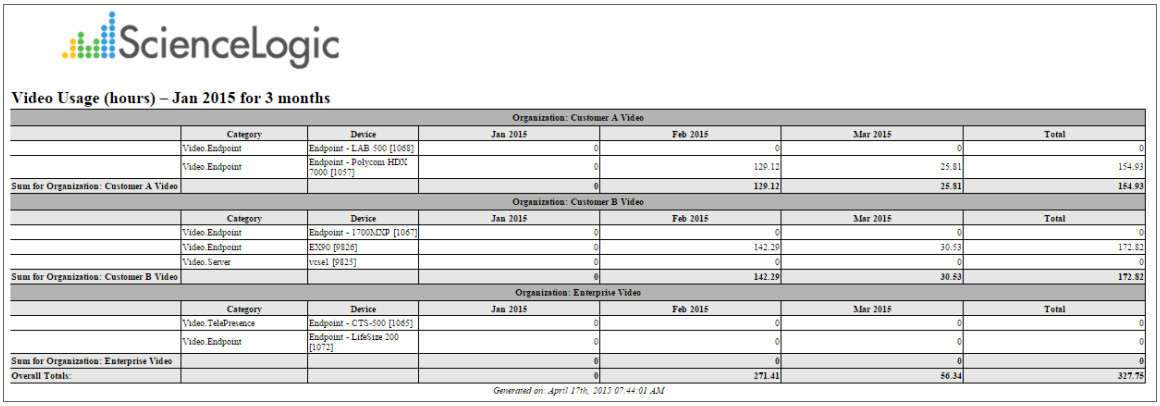
- ***Device Selection***: Select the devices that will appear in the report. The choices are:
    - *All devices*. Select this checkbox if you want all devices in the system to be included in this report.
    - *Organizations*. If the *All devices* checkbox is unselected, select one or more Organizations. The report will contain only the devices in the organizations you select. You can further filter the list of devices to include in the report by selecting devices in the *Devices by Organization* field.
    - *Select individual devices*. If the *All devices* checkbox is unselected, the *Select individual devices* checkbox is available. Select this checkbox if you would like to use the *Devices by Organization* field to select the individual devices to include in the report.
    - *Devices by Organization*. This field displays a list of all devices in the organizations selected in the *Organizations field*. If the *Select individual devices* checkbox is selected, you can select one or more devices to include in the report.
- ***Device Group Selector***: Select the device groups that will appear in the report. The following input elements appear in this component:
    - *Select By Device Group*. Select this checkbox if you want to select which device groups to include in the report.
    - *Device Groups*. If the *Select By Device Group* checkbox is selected, select one or more device groups. The report will contain only the devices in the device groups you select.
- ***Device Categories***. By default, the *All Device Categories* checkbox is selected. To limit the report to one or more specific device categories, select one or more device categories from the list of *Device Categories*.
- ***General Display Options***. Specify how the report will be arranged:
    - ***Separated By***. Select whether the report will be separated into multiple tables. The report can be separated to include one table per organization, one table per device group, one table per device category, or one table per device.
    - ***Naming***. These checkboxes allow you to select whether the Device ID or the Organization ID will appear in the report.
    - ***Report Sections***. Select whether you want the report to display *Details Only*, *Totals Only*, or *Both*.
- ***Report Span***. Specify a *Daily*, *Weekly*, or *Monthly* span to include in the report. ***Starting***. Use the *Year*, *Month*, and *Date* fields to specify a Start Date for the report. The SL1 system will use data from that date as the starting point of the report.***Duration***. Specify the duration for the report, from 1 month to 36 months. The SL1 system will use data from the Starting date as the start point of the report and data from the last day of the Duration as the ending point of the report.***Timezone***. Specify the timezone to use for date and time values in the report. Specify the timezone by number of hours offset from UTC.
- ***Report Type***. Specify that the report should include all selected devices or that the report should be limited to include a set number of devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the Video Reports PowerPack. This report might have been modified on your SL1 system.

Video Usage Report

This report displays usage based on call detail records for Tandberg, Polycom, Lifesize and Cisco TelePresence devices. For each device included in the report, the report displays the total number of hours the device was on a call for the time period selected for the report.

You can customize the output to include only specific devices and/or limit the number of devices that are included in the report. You can also specify the time span of information to include in the report, text that will appear at the top of the report, and how the devices will be sorted and arranged in the report.



ScienceLogic

Video Usage (hours) – Jan 2015 for 3 months

Organization: Customer A Video						
	Category	**Device**	**Jan 2015**	**Feb 2015**	**Mar 2015**	**Total**
	Video.Endpoint	Endpoint - LAB 500 [1068]	0	0	0	0
	Video.Endpoint	Endpoint - Polycom HDX 7000 [1057]	0	129.12	25.81	154.93
Sum for Organization: Customer A Video			**0**	**129.12**	**25.81**	**154.93**
Organization: Customer B Video						
	Category	**Device**	**Jan 2015**	**Feb 2015**	**Mar 2015**	**Total**
	Video.Endpoint	Endpoint - 1700MXP [1067]	0	0	0	0
	Video.Endpoint	EX90 [9826]	0	142.29	30.53	172.82
	Video.Server	vcse1 [9825]	0	0	0	0
Sum for Organization: Customer B Video			**0**	**142.29**	**30.53**	**172.82**
Organization: Enterprise Video						
	Category	**Device**	**Jan 2015**	**Feb 2015**	**Mar 2015**	**Total**
	Video.TelePresence	Endpoint - CTS-500 [1065]	0	0	0	0
	Video.Endpoint	Endpoint - LifeSize 200 [1072]	0	0	0	0
Sum for Organization: Enterprise Video			**0**	**0**	**0**	**0**
Overall Totals:			**0**	**271.41**	**56.34**	**327.75**

Generated on: April 17th, 2015 07:44:01 AM

The following input options are available when generating the report:

- ***Branding***. Optionally enter text that will be displayed at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" will be displayed at the top of the report.
- ***Device Selection***: Select the devices that will appear in the report. The choices are:
    - *All devices*. Select this checkbox if you want all devices in the system to be included in this report.
    - *Organizations*. If the *All devices* checkbox is unselected, select one or more Organizations. The report will contain only the devices in the organizations you select. You can further filter the list of devices to include in the report by selecting devices in the *Devices by Organization* field.
    - *Select individual devices*. If the *All devices* checkbox is unselected, the *Select individual devices* checkbox is available. Select this checkbox if you would like to use the *Devices by Organization* field to select the individual devices to include in the report.
    - *Devices by Organization*. This field displays a list of all devices in the organizations selected in the *Organizations field*. If the *Select individual devices* checkbox is selected, you can select one or more devices to include in the report.
- ***Device Group Selector***: Select the device groups that will appear in the report. The following input elements appear in this component:
    - *Select By Device Group*. Select this checkbox if you want to select which device groups to include in the report.

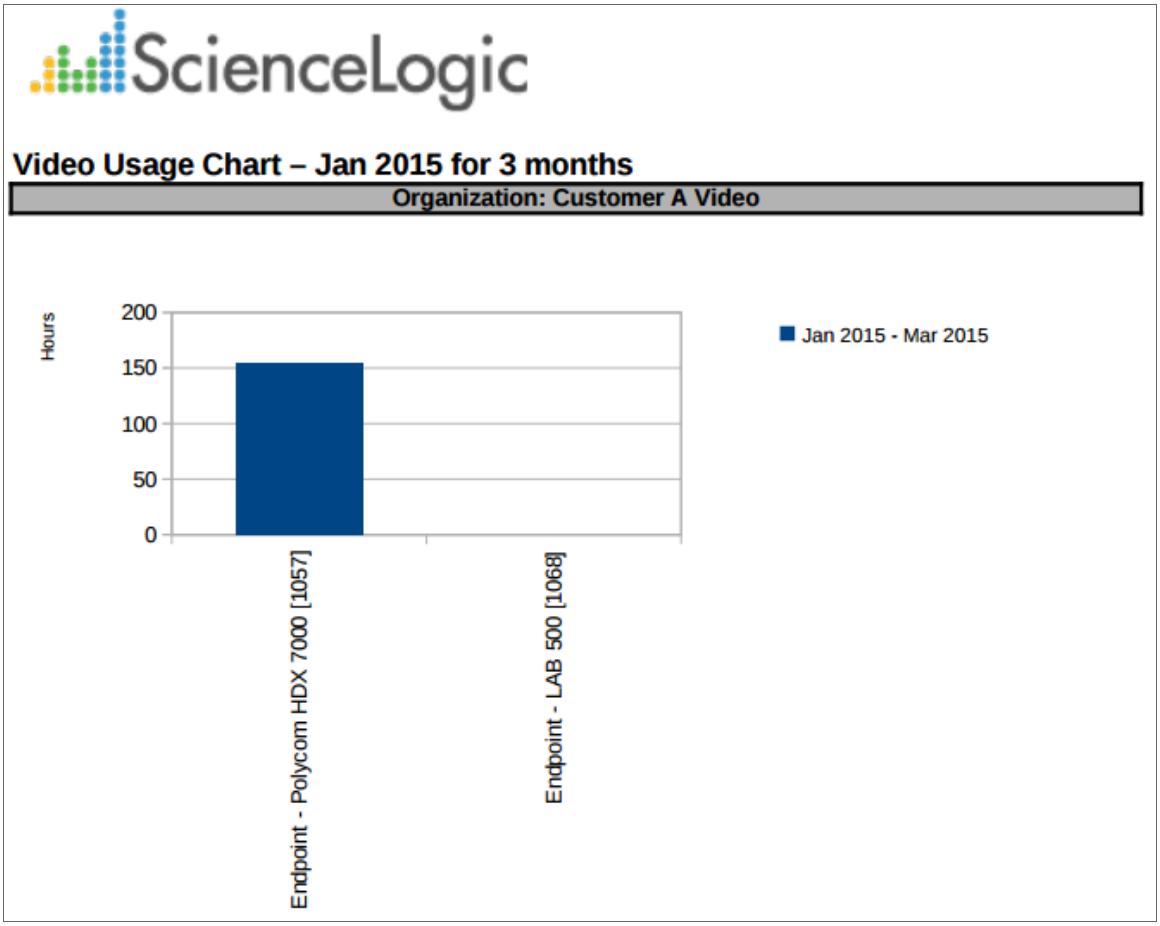
    - *Device Groups*. If the *Select By Device Group* checkbox is selected, select one or more device groups. The report will contain only the devices in the device groups you select.
- ***Device Categories***. Select the device categories that will appear in the report. The following input elements appear in this component:
    - *All Device Categories*. Select this checkbox if you want all device categories in the system to be included in this report.
    - *Device Categories*. If the *All Device Categories* checkbox is unselected, you can select one or more device categories to include in the report.
- ***General Display Options***. Specify how the report will be arranged:
    - *Separated By*. Select whether the report will be separated into multiple tables. The report can be separated to include one table per organization, one table per device group, one table per device category, or one table per device.
    - *Naming*. These checkboxes allow you to select whether the Device ID or the Organization ID will appear in the report.
    - *Report Sections*. Select whether you want the report to display *Details Only*, *Totals Only*, or *Both*.
    - *Misc. Options*. This checkbox allows you to aggregate the final separation column.
- ***Report Span***. Specify a *Daily*, *Weekly*, or *Monthly* span to include in the report. ***Starting***. Use the *Year*, *Month*, and *Date* fields to specify a Start Date for the report. The SL1 system will use data from that date as the starting point of the report.***Duration***. Specify the duration for the report, from 1 month to 36 months. The SL1 system will use data from the Starting date as the start point of the report and data from the last day of the Duration as the ending point of the report.***Timezone***. Specify the timezone to use for date and time values in the report. Specify the timezone by number of hours offset from UTC.
- ***Report Type***. Specify that the report should include all selected devices or that the report should be limited to include a set number of devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the Video Reports PowerPack. This report might have been modified on your SL1 system.

Video Usage Chart Report

This report displays a bar graph of usage based on call detail records for Tandberg, Polycom, Lifesize and Cisco TelePresence devices. For each device included in the report, the report displays the total number of hours the device was on a call for the time period selected for the report.

You can customize the output to include only specific devices and/or limit the number of devices that are included in the report. You can also specify the time span of information to include in the report, text that will appear at the top of the report, and how the devices will be sorted and arranged in the report.



The following input options are available when generating the report:

- ***Branding***. Optionally enter text that will be displayed at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" will be displayed at the top of the report.
- ***Device Selection***: Select the devices that will appear in the report. The choices are:
    - *All devices*. Select this checkbox if you want all devices in the system to be included in this report.
    - *Organizations*. If the *All devices* checkbox is unselected, select one or more Organizations. The report will contain only the devices in the organizations you select. You can further filter the list of devices to include in the report by selecting devices in the *Devices by Organization* field.
    - *Select individual devices*. If the *All devices* checkbox is unselected, the *Select individual devices* checkbox is available. Select this checkbox if you would like to use the *Devices by Organization* field to select the individual devices to include in the report.
    - *Devices by Organization*. This field displays a list of all devices in the organizations selected in the *Organizations field*. If the *Select individual devices* checkbox is selected, you can select one or more devices to include in the report.
- ***Device Group Selector***: Select the device groups that will appear in the report. The following input elements appear in this component:

- *Select By Device Group*. Select this checkbox if you want to select which device groups to include in the report.
- *Device Groups*. If the *Select By Device Group* checkbox is selected, select one or more device groups. The report will contain only the devices in the device groups you select.

- ***Device Categories***. Select the device categories that will appear in the report. The following input elements appear in this component:
  - *All Device Categories*. Select this checkbox if you want all device categories in the system to be included in this report.
  - *Device Categories*. If the *All Device Categories* checkbox is unselected, you can select one or more device categories to include in the report.
- ***General Display Options***. Specify how the report will be arranged:
  - *Separated By*. Select whether the report will be separated into multiple tables. The report can be separated to include one table per organization, one table per device group, one table per device category, or one table per device.
  - *Naming*. These checkboxes allow you to select whether the Device ID or the Organization ID will appear in the report.
  - *Charting Options*. Select whether you want the report to aggregate the final separation column, show devices as a series, or enable stacking.
- ***Report Span***. Specify a *Daily*, *Weekly*, or *Monthly* span to include in the report. ***Starting***. Use the *Year*, *Month*, and *Date* fields to specify a Start Date for the report. The SL1 system will use data from that date as the starting point of the report.***Duration***. Specify the duration for the report, from 1 month to 36 months. The SL1 system will use data from the Starting date as the start point of the report and data from the last day of the Duration as the ending point of the report.***Timezone***. Specify the timezone to use for date and time values in the report. Specify the timezone by number of hours offset from UTC.
- ***Report Type***. Specify that the report should include all selected devices or that the report should be limited to include a set number of devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the Video Reports PowerPack. This report might have been modified on your SL1 system.

© 2003 - 2025, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com. For more information, see https://sciencelogic.com/company/legal.

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

International: +1-703-354-1010