



Monitoring Video Devices

Skylar One version 12.5.20

Table of Contents

Introduction	5
Which Video Devices are Covered in this Manual?	5
Video Device PowerPacks	6
Monitoring Cisco Tandberg C Series Codecs	7
Configuring Cisco Tandberg C Series Codecs for Monitoring by Skylar One	7
Creating an SNMP Credential	12
Creating an SNMP Credential in the Classic Skylar One User Interface	13
Configuring SOAP/XML Credentials	13
Configuring SOAP/XML Credentials in the Classic Skylar One User Interface	15
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 Skylar One	19
Creating an SNMP Credential	22
Configuring SOAP/XML Credentials	23
Modifying the Credential Templates	23
Dynamic Applications for Cisco Tandberg MXP Series Endpoints	24
Monitoring Cisco CE Series Endpoints	27
Configuring Cisco CE Series Endpoints for Monitoring by Skylar One	27
Configuring SNMP Settings	27
Configuring the HTTP Request Password	29
Creating an SNMP Credential	30
Creating an SNMP Credential in the Classic Skylar One User Interface	31
Configuring SOAP/XML Credentials	32
Modifying the SOAP/XML Credential Templates	32
Modifying the SOAP/XML Credential Templates in the Classic Skylar One User Interface	33
Discovering Cisco CE Series Endpoints	34
Discovering Cisco CE Series Devices	36
Discovering Cisco CE Series Devices in the Classic Skylar One User Interface	37
Monitoring Cisco TelePresence Endpoints	38
Configuring TelePresence Endpoints for Monitoring by Skylar One	38
Creating an SNMP Credential	42
Monitoring Cisco TelePresence Conductor	44
Prerequisites	44
Monitoring Cluster Configurations vs. Non-Cluster Configurations	45

Creating Credentials	45
Creating a SOAP/XML Credential	45
Creating a SOAP/XML Credential in the Classic Skylar One User Interface	46
Creating an SNMP Credential	47
Creating an SNMP Credential in the Classic Skylar One User Interface	48
Creating and Discovering Virtual Devices	48
Discovering IP Devices	49
Viewing Cisco TelePresence Conductor Devices	50
Monitoring LifeSize Endpoints	51
Configuring LifeSize Endpoints for Monitoring by Skylar One	51
Creating an SNMP Credential for a LifeSize Endpoint	53
Monitoring Poly HDX and VSX Series Endpoints	54
Configuring Poly Endpoints for Monitoring by Skylar One	54
Creating an SNMP Credential	57
Creating an SNMPv2 Credential	57
Creating an SNMPv2 Credential in the Classic Skylar One User Interface	59
Creating an SNMPv3 Credential	59
SNMPv3 Credential in the Classic Skylar One User Interface	61
Performing Bulk Retrieval Using SNMPv3	62
Configuring SOAP/XML Credentials	63
Creating SOAP/XML Credentials	63
Creating SOAP/XML Credentials in the Classic Skylar One User Interface	65
Dynamic Applications for Poly Endpoints	66
Monitoring Tandberg Infrastructure	69
Tandberg Infrastructure Support	69
Creating a Credential for Tandberg Infrastructure Dynamic Applications	72
Creating a Credential for Tandberg Infrastructure in the Classic Skylar One User Interface	72
Creating a Credential for TelePresence Content Server	73
Creating a Credential for TelePresence Content Server in the Classic Skylar One User Interface	74
Video Communication Server	75
Dynamic Applications for VCS Devices	75
Creating a Credential for VCS Devices	76
Creating a Credential for VCS Devices in the Classic Skylar One User Interface	77
Discovering VCS Devices	78

Manually Aligning Dynamic Applications with VCS Devices	79
TelePresence Server	80
Creating a Credential for a TelePresence Server	80
Creating a Credential for a TelePresence Server in the Classic Skylar One User Interface	81
Discovering Devices with the TelePresence Server	82
Manually Aligning the Dynamic Applications with the TelePresence Server	83
TelePresence Control Unit	84
Creating a Credential for a TelePresence Control Unit	84
Creating a Credential for a TelePresence Control Unit in the Classic Skylar One User Interface	85
Discovering TelePresence Control Unit Devices	85
Manually Aligning the Dynamic Applications with the TelePresence Control Unit	87
Reports for Video Devices	88
TelePresence Inventory Report	89
Video Calls by Device Group, Call Type, and Bandwidth Report	90
Video Endpoint Availability Chart Report	91
Video Endpoint Availability Table Report	93
Video Endpoint Avg Jitter Column Chart Report	95
Video Endpoint Avg Jitter Line Chart Report	97
Video Endpoint Avg Jitter Table Report	100
Video Endpoint Call Detail Records Report	101
Video Endpoint Detailed Asset Inventory Report	104
Video Endpoint Detailed Jitter Line Chart Report	105
Video Endpoint Detailed Packet Loss Line Chart Report	108
Video Endpoint Packet Loss Column Chart Report	110
Video Endpoint Packet Loss Line Chart Report	112
Video Endpoint Packet Loss Table Report	114
Video Endpoint Performance Detail Report	115
Video Endpoint Unavailability Chart Report	117
Video Endpoint Unavailability Table Report	120
Video Usage Report	122
Video Usage Chart Report	123

Chapter

1

Introduction

Overview

This manual describes how to configure video devices for monitoring by Skylar One. It also lists the default custom reports and widgets that display data collected from video devices.

This chapter covers the following topics:

<i>Which Video Devices are Covered in this Manual?</i>	5
<i>Video Device PowerPacks</i>	6

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
- Poly 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 103
- Cisco: TelePresence: Traps, version 100
- Cisco: Video Endpoint, version 107
- LifeSize Endpoint, version 7.5.4
- Poly: Endpoint, version 103
- Tandberg: Infrastructure, version 108
- Video Reports, version 100

Chapter

2

Monitoring Cisco Tandberg C Series Codecs

Overview

This section describes how to configure Cisco Tandberg C Series devices for monitoring by Skylar One using the "Cisco: Video Endpoint" PowerPack.

This chapter covers the following topics:

<i>Configuring Cisco Tandberg C Series Codecs for Monitoring by Skylar One</i>	7
<i>Creating an SNMP Credential</i>	12
<i>Configuring SOAP/XML Credentials</i>	13
<i>Dynamic Applications for Cisco Tandberg C Series Codecs</i>	16

Configuring Cisco Tandberg C Series Codecs for Monitoring by Skylar One

Skylar One uses two protocols to monitor Cisco Tandberg C Series Codecs: SNMP and HTTP. This section describes how to configure a Cisco Tandberg C Series Codec to respond to both protocols. This section also describes how to configure a user account that Skylar One uses to connect to the Cisco Tandberg C Series Codec.

NOTE: These instructions assume that the Cisco Tandberg C Series Codec has an IP address and a Data Collector on the network can reach it.
--

To configure a Cisco Tandberg C Series Codec for monitoring by Skylar One:

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. Run the following command to enable SNMP:

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

NOTE: The default monitoring content for Cisco Tandberg that ScienceLogic supplies does not require SNMP Write access. However, if you plan to perform SNMP Write operations on this Cisco Tandberg C Series Codec, type `ReadWrite` instead of `ReadOnly` in the above command.

3. Run 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 Skylar One, you enter the community string that you just configured in the **SNMP Community (Read-Only)** field.

4. Run the following command to configure the device to send SNMP trap messages to Skylar One. Substitute `<collector_ip_address>` with the IP address of the Message Collector or Data Collector that collects the SNMP trap messages from the device:

```
xConfiguration NetworkServices SNMP Host 1 Address: <collector_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 run 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. Run the following command to enable the HTTP service:

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

NOTE: By default, Skylar One uses regular HTTP to connect to Cisco Tandberg C Series Codecs. If you want to use HTTPS instead of regular HTTP, type `HTTPS` instead of `HTTP` in the above command. When you configure 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:



The image shows a web browser window displaying the Cisco login interface. At the top left is the Cisco logo. Below it, the text "Sign In" is visible. On the right side, there is a "Please Sign In" box. Inside this box, there are two input fields: "Username:" and "Password:". Below the "Password:" field is a "Sign In" button.

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

The screenshot shows the Cisco System Information page. On the left is a navigation menu with links: System Information, Call, Snapshot, Users, Change Password, Wallpaper, Logon Banner, Upload Certificates, Audit Certificate, Logs, XML Files, Upgrade Software, Advanced Configuration, Restart, and Sign Out. The main content area is titled 'System Info' and displays details for 'LAB C20'. It includes system name, product (TANDBERG Codec C20), IP address (192.168.44.250), software version (TC4.1.0.247017), module serial number (F1AN23D00286), MAC address (00:50:60:0C:E0:89), and installed options (NaturalPresenter, HighDefinition). Below this is 'H323' information (Number: 888888888, ID: leoH323AliasID, Gatekeeper: Rejected) and 'SIP' information (Address, Proxy, Status: Failed). A 'Login Info' section shows the last successful login (Thu Oct 27 19:49:23 2011) and password expiration (Never). A 'Security' section shows 'Strong security mode: Disabled'.

System Info	
LAB C20	
System name: LAB C20	Software version: TC4.1.0.247017
Product: TANDBERG Codec C20	Module serial number: F1AN23D00286
IP address: 192.168.44.250	MAC address: 00:50:60:0C:E0:89
Valid release key: Yes	Installed options: NaturalPresenter, HighDefinition
H323	SIP
Number: 888888888	Address:
ID: leoH323AliasID	Proxy:
Gatekeeper: Rejected	Status: Failed
Login Info	
Last successful login: Thu Oct 27 19:49:23 2011	
Number of unsuccessful login attempts since last login: 0	
Password expires in: Never	
Security	
Strong security mode: Disabled	

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

The screenshot shows the Cisco User Management page. The left navigation menu is the same as in the previous screenshot, but 'Users' is highlighted. The main content area is titled 'User management' and shows a list of users: 'admin - ADMIN,USER,AUDIT'. Below the list is a 'Create new user' button. Below the user management section is a 'Security mode' section with two buttons: 'Enable strong security mode' and 'Disable strong security mode'.

User management	
• admin - ADMIN,USER,AUDIT	
<button>Create new user</button>	
Security mode	
<button>Enable strong security mode</button> <button>Disable strong security mode</button>	

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

System Information
Call
Snapshot
Users
Change Password
Wallpaper
Logon Banner
Upload Certificates
Audit Certificate
Logs
XML Files
Upgrade Software
Advanced Configuration
Restart
Sign Out

Create new user

Username:

Password:

PIN:

Roles: ☒ ADMIN
☐ USER
☐ AUDIT

Status: ☒ Active
☐ Inactive

☐ Require password change on next user logon
☐ Require PIN change on next user logon

11. Enter a value in the following fields:

- **Username.** Enter a username for the new user. When you configure a SOAP/XML credential for this device in Skylar One, you enter this value in the **HTTP Auth User** field.
- **Password.** Enter a password for the new user. When you configure a SOAP/XML credential for this device in Skylar One, you enter this value in the **HTTP Auth Password** field.
- **PIN.** Enter any valid PIN in this field. Skylar One does not use this value.
- **Roles.** Select the **ADMIN** checkbox.
- **Status.** Select the **Active** radio button.
- **Require password change on next user logon.** Clear this checkbox.
- **Require PIN change on next user logon.** Clear this checkbox.

12. Click the **[Save]** button to save the new user.

Creating an SNMP Credential

To monitor Cisco Tandberg C Series Codecs in Skylar One, you must create an SNMP credential for each Codec.

To create an SNMP credential for a Cisco Tandberg C Series Codec in Skylar One:

1. Go to the **Credentials** page (Manage > Credentials).
2. Click the **[Create New]** button and select *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 Skylar One stops 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 you configured on the Cisco Tandberg C Series Codec.
 - **SNMP Community (Read/Write).** Optional. Enter the community string for the Cisco Tandberg C Series Codec to grant Read/Write permissions.
4. Click **[Close]**.

Creating an SNMP Credential in the Classic Skylar One User Interface

To monitor Cisco Tandberg C Series Codecs in the classic Skylar One user interface, you must create an SNMP credential for each Codec.

To create an SNMP credential for a Cisco Tandberg C Series Codec in the classic Skylar One user interface:

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. Enter values in the following fields:
 - **Profile Name**. Enter a name for the credential.
 - **SNMP Version**. Select *SNMP V2*.
 - **SNMP Community (Read-Only)**. Enter 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]**.

Configuring SOAP/XML Credentials

To use the Dynamic Applications in the "Cisco: Video Endpoint" PowerPack in Skylar One, 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 Skylar One to collect configuration and performance data along with call detail records using a unique combination of URL, username, and password.

If you have multiple Cisco Tandberg C Series Codecs, you 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 - Configuration" credential, then click its actions icon (⋮) and select **Duplicate** from the drop-down field. The "Tandberg Endpoint-Credential copy" credential appears.
3. Click the actions 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 Skylar One stops 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 Classic Skylar One User Interface

To use the Dynamic Applications in the "Cisco: Video Endpoint" PowerPack in Skylar One, 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 Skylar One to collect configuration and performance data along with call detail records using a unique combination of URL, username, and password.

If you have multiple Cisco Tandberg C Series Codecs, you 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 Skylar One 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 appears.
3. In the **Profile Name** field, enter a new name for the credential.
4. In the **HTTP Auth User** field, enter the username of the user you configured on your Cisco Tandberg C Series Codec.
5. In the **HTTP Auth Password** field, enter 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 10 Dynamic Applications that you can use 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 only collect and cache data from Cisco Tandberg C Series Codecs.
- Seven Dynamic Applications use the cached data. For these Dynamic Applications to display data, you must align the Dynamic Applications that collect and cache data 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 its SOAP/XML credentials in the **Other Credentials** field on the **Discovery Session Editor** page, Skylar One automatically aligns the Dynamic Applications from the "Cisco: Video Endpoint" PowerPack to the 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:

1. Go to the **Configuration Templates** page (Devices > Templates, or Registry > Devices > Templates in the classic user interface).
2. Click the **[Create]** button. The **Device Template Editor** page appears.
3. Enter 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:
 - In the **Subtemplate Selection** pane, select *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 that the discovery session discovers. To apply a device template to all devices that a discovery session discovers, select the device template in the **Apply Device Template** field on the **Discovery Session Editor** page.

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 on the **Device Manager** page.

To apply the device template to the Codecs:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic 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*. Click the **[Go]** button. The **Bulk Device Configuration** modal 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 Dynamic Applications that populate the cache and the Dynamic Applications that use the cache, and the credential that you must align 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 (Tandberg C Series)	N/A	Consumes Cache	Cisco: Configuration Cache (Tandberg C Series)
Cisco: Environmental (Tandberg C Series)	N/A	Consumes Cache	Cisco: Configuration Cache (Tandberg C Series)

Dynamic Application	Credential	Caching Type	Dependencies
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 Skylar One runs the "Cisco: Device Discovery (Tandberg C Series)" Dynamic Application, the Dynamic Application triggers a run book action that aligns the appropriate Cisco Tandberg C Series Device Classes to your devices.

Chapter

3

Monitoring Cisco Tandberg MXP Series Endpoints

Overview

This section describes how to configure Cisco Tandberg MXP Series endpoints for monitoring by Skylar One using the "Cisco: Video Endpoint" PowerPack.

This chapter covers the following topics:

<i>Configuring Cisco Tandberg MXP Series Endpoints for Monitoring by Skylar One</i>	<i>19</i>
<i>Creating an SNMP Credential</i>	<i>22</i>
<i>Configuring SOAP/XML Credentials</i>	<i>23</i>
<i>Dynamic Applications for Cisco Tandberg MXP Series Endpoints</i>	<i>24</i>

Configuring Cisco Tandberg MXP Series Endpoints for Monitoring by Skylar One

Skylar One 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 Skylar One 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 describes how to:

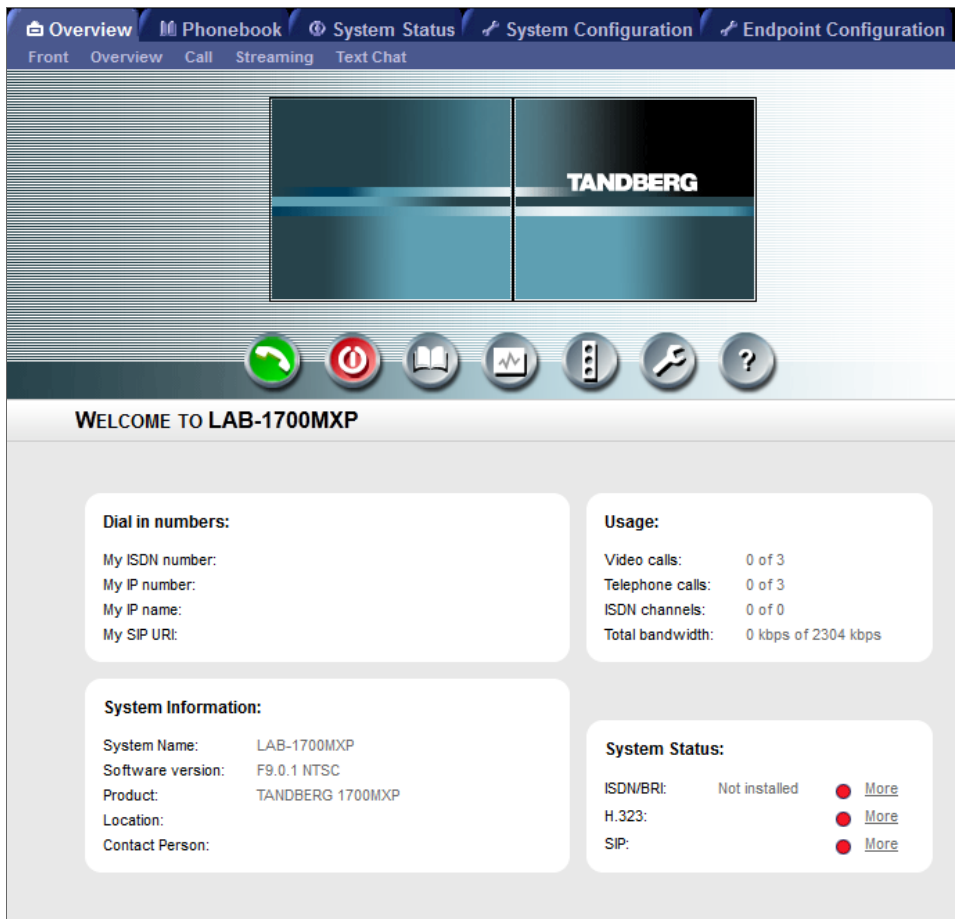
- Configure a new SNMP community string for a Cisco Tandberg MXP Series Endpoint.
- Configure a Cisco Tandberg MXP Series Endpoint to send SNMP Traps to Skylar One.
- Configure a new IP Access Password for HTTP requests.

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.

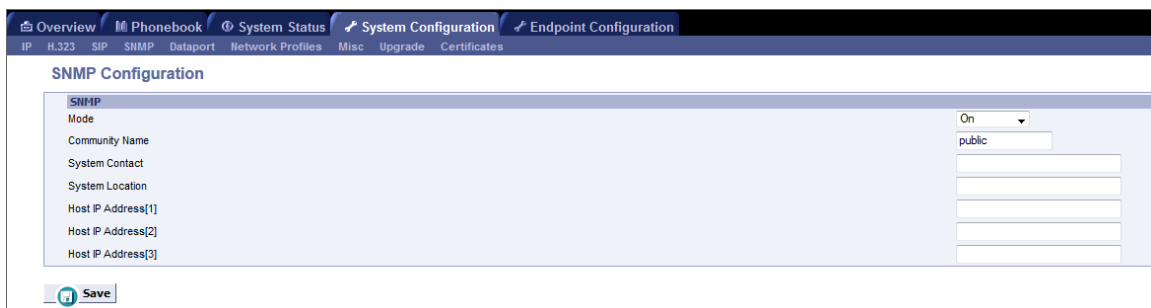
NOTE: These instructions assume that the Cisco Tandberg MXP Series Endpoint has an IP address and that a Data Collector on the network can see the endpoint.

To configure the SNMP settings on a Cisco Tandberg MXP Series Endpoint:

1. In a browser window, go to the IP address of the Cisco Tandberg MXP Series Endpoint.
2. A prompt for a username and password appears. 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 Skylar One, you 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 collects SNMP trap messages from the device. If the device already sends SNMP traps to another IP address and you want to retain those settings, 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.

To change the password that Skylar One uses to perform HTTP requests on this device:

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: Cisco Tandberg MXP Series Endpoints do not use usernames for authentication. If you enter a new value in this field, the password changes for all administrators of this device.

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

Creating an SNMP Credential

To monitor Cisco Tandberg MXP Series Endpoints in Skylar One, you must create an SNMP credential for each endpoint.

To create an SNMP credential for a Cisco Tandberg MXP Series Endpoint in Skylar One:

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 informationSkylar One, 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 Skylar One 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 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 page 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 Series Endpoint.
6. Click the **[Save As]** button.
7. Repeat steps 2 through 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 nine Dynamic Applications that 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.
- Six Dynamic Applications use the cached data. For these Dynamic Applications to display data, you must align the Dynamic Applications that collect and cache data 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. You can discover your Cisco Tandberg MXP Series Endpoint as an SNMP device. If you include all the SOAP/XML credentials you configured for the endpoint in the **Other Credentials** field in the **Discovery Session Editor** page, Skylar One automatically aligns the Dynamic Applications in the "Cisco: Video Endpoint" PowerPack to your endpoint. However, Dynamic ApplicationsCisco: Video EndpointPowerPackthis alignment might take a significant amount of time during discovery. If you discover multiple Cisco Tandberg endpoints, or if your 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:

1. Go to the **Configuration Templates** page (Devices > Templates, or Registry > Devices > Templates in the classic 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:
 - In the **Subtemplate Selection** pane, 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 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** page.

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 apply the device template to the endpoints:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic 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*. 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 Dynamic Applications that cache data and the Dynamic Applications that use the cached data, 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)
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 (Tandberg MXP)	N/A	Consumes Caches	Cisco: Configuration Cache (Tandberg 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 Skylar One runs the "Cisco: Device Discovery (Tandberg MXP Series)" Dynamic Application, the Dynamic Application triggers a run book action that aligns the appropriate Cisco Tandberg MXP Series Device Classes to your devices.

Chapter

4

Monitoring Cisco CE Series Endpoints

Overview

This section describes how to configure Cisco CE Series endpoints for monitoring by Skylar One using the "Cisco: Video Endpoint" PowerPack.

This chapter covers the following topics:

<i>Configuring Cisco CE Series Endpoints for Monitoring by Skylar One</i>	<i>27</i>
<i>Creating an SNMP Credential</i>	<i>30</i>
<i>Configuring SOAP/XML Credentials</i>	<i>32</i>
<i>Discovering Cisco CE Series Endpoints</i>	<i>34</i>

Configuring Cisco CE Series Endpoints for Monitoring by Skylar One

Skylar One uses two protocols to monitor 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 Skylar One, you must configure the SNMP community string and other information that Skylar One uses to connect to the endpoints. You 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. A prompt for a username and password appears.
2. Go to the **Network Services** page (Setup > Configuration > Network Services). Under the **SNMP** subheading, enter values in the following fields:

The screenshot shows the Cisco CE Series endpoint configuration page. The top navigation bar includes Home, Call Control, Setup, Security, Maintenance, Integration, and ScienceLogic. The left sidebar lists various configuration categories, with Network Services selected. The main content area is titled 'System Configuration' and 'NetworkServices'. It contains several expandable sections: CDP Mode, H323 Mode, HTTP Mode, SIP Mode, Telnet Mode, WelcomeText, XMLAPI Mode, HTTPS, OCSP, NTP, SNMP, SSH, and UPnP. The SNMP section is highlighted with a red box and contains the following fields:

Field	Value	Character Limit
CommunityName		(0 to 50 characters)
Host 1 Address		(0 to 255 characters)
Host 2 Address		(0 to 255 characters)
Host 3 Address		(0 to 255 characters)
Mode	ReadOnly	
SystemContact		(0 to 50 characters)
SystemLocation		(0 to 50 characters)

- **Community Name.** Enter a new SNMP community string for this device. *When you configure an SNMP credential* for this Cisco CE Series endpoint in Skylar One, enter this community string in the **SNMP Community (Read-Only)** field.
- **Host 1 Address.** Enter the IP address of the Message Collector or Data Collector that collects SNMP trap messages from the device. If the device already sends SNMP traps to another IP address and you want to keep those settings, enter 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, enter the contact information for the device's administrator.
- **SystemLocation.** Optionally, enter the device's location.

3. Click **[Save]**.

Configuring the HTTP Request Password

Optionally, if you *use a SOAP/XML credential* to collect configuration and performance data from a Cisco CE Series endpoint, you can configure the password for the account Skylar One uses to send HTTP requests to the endpoint.

To configure the HTTP request password:

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

Edit User: ScienceLogic Back

Username:

Roles: ☒ Admin, ☒ Audit, ☐ RoomControl, ☒ User

Status: ☒ Active, ☐ Inactive

Client Certificate DN:
If using client certificates for authentication, enter the client certificate's full Distinguished Name. Both the `/CN=alice/DC=example/DC=com` and the `CN=alice, DC=example, DC=com` formats are supported.

☐ Require passphrase change on next user sign in

Passphrase: ☒ Valid

Login attempts: 0 failed login attempts since last login today at 11:45

Your passphrase:
When creating or modifying admin users, you must enter your own passphrase for verification.

Edit user

Change passphrase

Passphrase:

Repeat passphrase:

Your passphrase:
When creating or modifying admin users, you must enter your own passphrase for verification.

Change passphrase

Delete user

Your passphrase:
When creating or modifying admin users, you must enter your own passphrase for verification.

Delete user...

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

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

Creating an SNMP Credential

To monitor Cisco CE Series endpoints in Skylar One, 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 *SNMP Credential* from the drop-down menu. The **Create Credential** page appears.
3. 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 (ms)**. Enter the time, in milliseconds, after which Skylar One stops trying to communicate with the Cisco CE Series endpoint. 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 CE Series endpoint you want to monitor.
 - **SNMP Community (Read/Write)**. Optional. Enter the community string for the Cisco CE Series endpoint to grant read/write permissions.
4. Click **[Save & Close]**.

Creating an SNMP Credential in the Classic Skylar One User Interface

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

To create an SNMP credential for a Cisco CE Series endpoint in the classic Skylar One 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 appears.
3. Enter values in the following fields:
 - **Profile Name**. Enter a name for the credential.
 - **SNMP Version**. Select *SNMP V2*.
 - **SNMP Community (Read-Only)**. Enter 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 *Discovery and Credentials* manual.

4. Click **[Save]**.

Configuring SOAP/XML Credentials

To monitor Cisco CE Series endpoints in Skylar One, 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 Skylar One 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 actions 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 Skylar One stops trying to communicate with the Cisco CE Series 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 Cisco CE Series endpoint username associated with the administrator account.
- **HTTP Auth Password.** Enter the password associated with the Cisco CE Series endpoint administrator account.
- **Embedded Password [%P].** Enter the embedded password associated with the Cisco CE Series endpoint administrator account.

5. Click [Save & Close].

Modifying the SOAP/XML Credential Templates in the Classic Skylar One 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 Skylar One user interface:

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 appears.

3. Enter values in the following fields:
 - **Profile Name.** Enter a name for the credential.
 - **HTTP Auth User.** Enter the username of the HTTP user account that you [configured on the Cisco CE Series endpoint](#).
 - **HTTP Auth Password.** Enter the password of the HTTP user account you configured on the Cisco CE Series 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

Skylar One uses Dynamic Applications from the "Cisco: Video Endpoint" PowerPack 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 only collect and cache data from Cisco CE Series endpoints.
- Nine Dynamic Applications use the cached data. For these Dynamic Applications to display data, you must align the Dynamic Applications that collect and cache data to the same device.
- Three Dynamic Applications 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 Dynamic Applications that populate cache and the Dynamic Applications that use the cache, and the credential you must align 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 Skylar One 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 Cisco CE Series Devices

To monitor Cisco CE Series endpoints, you must run a discovery session to discover each endpoint.

To create and run a discovery session for a Cisco CE Series endpoint:

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 the 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. Enter values in the following fields:
 - **Discovery Session Name.** Enter a unique name for this discovery session. This name displays in the list of discovery sessions on the **[Discovery Sessions]** tab.
 - **Description.** Optional. Enter 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 the Cisco CE Series endpoints.
7. Click **[Next]**. The **[Step 3 Discovery Session Details]** tab of the wizard appears.
8. Enter values in the following fields:
 - **List of IP/Hostnames.** Enter the IP address for the Cisco CE Series endpoint.
 - **Which collector will discover these devices?.** Required. Select an existing collector group 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 runs and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page includes a link to the **Device Investigator** page for the discovered device.
10. If you did not enable the **Run after save** option, click the **[Save and Close]** button. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.

Discovering Cisco CE Series Devices in the Classic Skylar One User Interface

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

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

To discover the devices that you want to monitor:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery or System > Manage > Discovery in the classic user interface).
2. Click the **[Create]** button. The **Discovery Session Editor** page appears.
3. Enter 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 Cisco CE Series endpoints.
 - **Other Credentials.** Select the credentials you created using the following templates:
 - 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 and Credentials* manual.
5. Click the **[Save]** button to save the discovery session.
6. Close the **Discovery Session Editor** page. The discovery session you created appears at the top of the **Discovery Control Panel** page.
7. Click the lightning-bolt icon (⚡) of the discovery session you created to run it. The **Discovery Session** window appears.
8. After Skylar One discovers the devices, 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 Skylar One using the "Cisco: TelePresence: Endpoints" PowerPack:

This chapter covers the following topics:

<i>Configuring TelePresence Endpoints for Monitoring by Skylar One</i>	38
<i>Creating an SNMP Credential</i>	42

Configuring TelePresence Endpoints for Monitoring by Skylar One

To configure a TelePresence endpoint for monitoring by Skylar One:

1. Log in to Cisco Unified Communications Manager.

2. Select **Device > Phone**. The **Find and List Phones** page appears.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | em7app | Search Documentation | About | Logout

System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help

Find and List Phones Related Links: Actively Logged In Device Report Go

+ Add New

Phone

Find Phone where Device Name begins with Find Clear Filter

Select item or enter search text

No active query. Please enter your search criteria using the options above.

Add New

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

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | em7app | Search Documentation | About | Logout

System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help

Find and List Phones Related Links: Actively Logged In Device Report Go

+ Add New Select All Clear All Delete Selected Reset Selected Apply Config to Selected

Status
5 records found

Phone (1 - 5 of 5) Rows per Page 50

Find Phone where Device Name begins with Find Clear Filter

Select item or enter search text

	Device Name(Line) ^	Description	Device Pool	Device Protocol	Status	IP Address	Copy	Super Copy
☐	SEP000F909341F2	CUCM 8 Phone 2 x1002	Default	SCCP	Unknown	Unknown		
☐	SEP001A6C8AC697	CUCM 8 Phone 1 x1001	Default	SCCP	Registered with 10.168.44.22	10.168.44.152		
☐	SEP04CSA4B0AD9F	CUCM 8 Phone 1 x3001	Default	SCCP	Unknown	Unknown		
☐	SEP30E4DBE89534	Cisco CTS 5---37	Default	SIP	Registered with 10.168.44.22	10.168.44.151		
☐	SEP44E4D945EF47	SEP44E4D945EF47	Default	SCCP	Unknown	Unknown		

Add New Select All Clear All Delete Selected Reset Selected Apply Config to Selected

- Click the Device name link for your TelePresence Endpoint. The **Phone Configuration** page appears.

The screenshot shows the Cisco Unified CM Administration interface. The top navigation bar includes links for System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The main title is "Cisco Unified CM Administration" with a sub-header "For Cisco Unified Communications Solutions". The "Phone Configuration" section is active, showing a "Status: Ready" message. Below this, the "Association Information" section lists 16 lines, with the first line selected. The "Phone Type" section shows "Product Type: Cisco TelePresence 500-37" and "Device Protocol: SIP". The "Device Information" section contains various fields: Registration (Registered with Cisco Unified Communications Manager 10.168.44.22), IP Address (10.168.44.151), Active Load ID (CTS_1.8.1(34)_P1), Device is Active (checked), Device is trusted (checked), MAC Address* (30E4DBE89534), Description (Cisco CTS 5---37), Device Pool* (Default), Common Device Configuration (< None >), Phone Button Template* (Standard_Cisco_TelePresence_500), Common Phone Profile* (Standard Common Phone Profile), Calling Search Space (OffNet-CSS), Media Resource Group List (< None >), Location* (Hub_None), User Locale (< None >), Network Locale (< None >), and Device Mobility Mode* (Default).

- Scroll down the **Phone Configuration** page until the **SNMP Configuration Parameters** section appears. Enter values in the **SNMP Configuration Parameters** section in the following fields:

The screenshot shows the "SNMP Configuration Parameters" section. It contains the following fields and values:

- Enable SNMP*: Enabled (v3)
- SNMP(v3) Security Level*: (v3) Authentication, Privacy
- SNMP(v3) Auth. Algorithm*: MD5
- SNMP(v3) Auth. Password*: [Redacted]
- SNMP(v3) Privacy Algorithm*: DES
- SNMP(v3) Privacy Password*: [Redacted]
- SNMP System Location*: Location
- SNMP System Contact*: Contact
- SNMP(v2c) Community Read Only*: public
- SNMP(v2c) Community Read Write*: public

- Enable SNMP.** Select *Enabled (v3)*.
- SNMP(v3) Security Level.** You can use one of three security levels with an SNMP v3 security name. Select the security level that is appropriate for your environment.
- SNMP(v3) Auth. Algorithm.** Select an authentication protocol for transmission of the authentication password. Skylar One supports both the *MD5* and *SHA* options.
- SNMP(v3) Auth. Password.** Enter an authentication password. The password must be at least 8 characters.

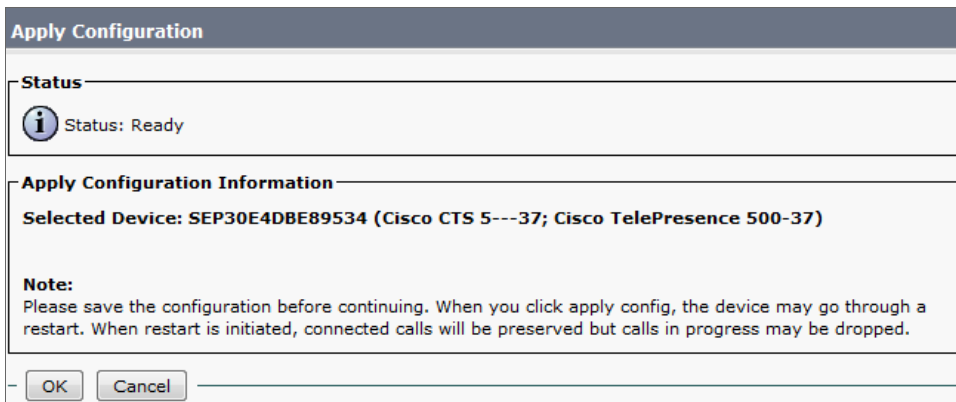
- **SNMP(v3) Privacy Algorithm.** Select a privacy protocol for the encryption of SNMP messages. Skylar One supports the *DES* and *AES128* options. Do not select *AES192* or *AES256* in this field.
- **SNMP(v3) Privacy Password.** Enter a privacy password. The password must be at least 8 characters.
- **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 the **SNMP Trap Receiver Parameters** section appears. Enter values in the **SNMP Trap Receiver Parameters** section in the following fields:

SNMP Trap Receiver Parameters	
1 SNMP Trap Receiver Address	10.0.9.103
--SNMP(v3) Trap Username	admin
--SNMP Security Level*	(v2c) Notification
--SNMP(v3) Auth. Algorithm*	MD5
--SNMP(v3) Auth Password	
--SNMP(v3) Privacy Algorithm*	DES
--SNMP(v3) Privacy Password	
--SNMP(v2c) Community String*	public

- **SNMP Trap Receiver Address.** Enter the IP address of the Message Collector or Data Collector that collects 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 click the **[Save]** button, then click the **[OK]** button in the pop-up window.

- Click **[Apply Config]**. A confirmation window appears.



The image shows a dialog box titled "Apply Configuration". It has a "Status" section with an information icon and the text "Status: Ready". Below this is the "Apply Configuration Information" section, which displays "Selected Device: SEP30E4DBE89534 (Cisco CTS 5---37; Cisco TelePresence 500-37)". A "Note" section follows, stating: "Please save the configuration before continuing. When you click apply config, the device may go through a restart. When restart is initiated, connected calls will be preserved but calls in progress may be dropped." At the bottom are "OK" and "Cancel" buttons.

- Click the **[OK]** button in the **Apply Configuration** window.

Creating an SNMP Credential

To create an SNMP Credential for a TelePresence Endpoint in Skylar One:

- Go to the **Credential Management** page (System > Manage > Credentials).
- Click the **[Create]** button, and then select *SNMP Credential*. The **Credential Editor** page appears.
- Supply values in the following fields:
 - Profile Name**. Enter a name for the credential.
 - SNMP Version**. Select *SNMP V3*.

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

- Security Name**. Enter the SNMP authentication name.
- 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 informationSkylar One, 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 Skylar One using the "Cisco: TelePresence Conductor" PowerPack:

This chapter covers the following topics:

<i>Prerequisites</i>	44
<i>Monitoring Cluster Configurations vs. Non-Cluster Configurations</i>	45
<i>Creating Credentials</i>	45
<i>Creating and Discovering Virtual Devices</i>	48
<i>Discovering IP Devices</i>	49
<i>Viewing Cisco TelePresence Conductor Devices</i>	50

Prerequisites

Before you perform 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 you create a SOAP/XML credential in Skylar One 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 you create an SNMP credential in Skylar One to monitor the Conductor.

Monitoring Cluster Configurations vs. Non-Cluster Configurations

Skylar One You can monitor Cisco TelePresence Conductor in either a cluster configuration or a non-cluster configuration. However, the monitoring method is different for each configuration.

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 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 Skylar One. To model the cluster using a virtual device, first create the virtual device in Skylar One. Then manually align a Dynamic Application to the virtual device to discover and model the devices in the cluster.

For **non-cluster configurations**, you can discover the Conductor as an SNMP-enabled IP device or an IP device that responds to ping. When you discover the IP address using the appropriate credential(s), Skylar One 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 Skylar One 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

Skylar One 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. 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 **[Actions]** icon (⋮) and select *Duplicate* from the drop-down field. The "Cisco: Conductor Example copy" credential appears, whether you chose a virtual device or an IP device.

3. Click the **[Actions]** icon (⋮) for the "Cisco: Conductor Example (Discov" or "Cisco: Conductor Example (Virtua" credential, then select *Edit*. The **Edit Credential** page appears.
4. 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. To align the credential to specific organizations, toggle off (gray), and then select one or more organizations from the **Select the organizations the credential belongs to** drop-down list.
 - **Timeout**. Enter the time, in milliseconds, after which Skylar One stops 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.
5. Click the **[Save & Close]** button.

Creating a SOAP/XML Credential in the Classic Skylar One User Interface

Skylar One 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 Skylar One 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 Skylar One 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. 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. To align the credential to specific organizations, toggle off (gray), and then select one or more organizations from the **Select the organizations the credential belongs to** drop-down list.
- **Timeout (ms).** Enter the time, in milliseconds, after which Skylar One stops trying to communicate with the Conductor 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 Unity ExpressConductor devices you want to monitor.
- **SNMP Community (Read/Write).** Optional. Enter the community string for the Cisco Unity

ExpressConductor devices to grant Read/Write permissions.

- For the other optional fields, you can use the default values.

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

Creating an SNMP Credential in the Classic Skylar One User Interface

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

To create an SNMP credential in the classic Skylar One user interface:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the actions icon (⋮).
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. 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 Skylar One. 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, Skylar One discovers the cluster first, and then automatically aligns the other Dynamic Applications in the "Cisco: TelePresence Conductor" 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 user interface).
2. Click the actions icon (⋮) 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 that you select limits which users 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 you create the Conductor cluster virtual device, you must manually align the "Cisco: TelePresence Conductor Discovery" Dynamic Application with the virtual device.

To align the Dynamic Application with the virtual device:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic 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" 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:

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** page, click the **[Create]** button. The **Discovery Session Editor** page appears.
3. **Discovery Session Editor** In the **Discovery Session Editor** page, enter 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, see the **Discovery & Credentials** manual.
 5. Click the **[Save]** button to save the discovery session. 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 Skylar One discovers the Conductor root device, click the device icon (🖨️) to view the **Device Properties** page for the root device.

Viewing Cisco TelePresence Conductor Devices

When Skylar One discovers your TelePresence Conductor devices, Skylar One creates 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. If you double-click a device, the page reloads with that device as the primary device.
- The **Device Components** page (Devices > Device Components) displays a list of all root devices and component devices discovered by Skylar One, in an indented view. The list shows 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 (+).
- On the **Component Map** page (Classic Maps > Device Maps > Components), you can view devices by root node. The map shows the relationships between root nodes, parent components, and child components. Skylar One automatically updates the **Component Map** as it discovers new component devices. Skylar One 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 navigation bar. For more information, **Component Map** see the **Views** manual.

Monitoring LifeSize Endpoints

Overview

This section describes how to configure LifeSize endpoints for monitoring by Skylar One using the "LifeSize Endpoint" PowerPack.

This chapter covers the following topics:

<i>Configuring LifeSize Endpoints for Monitoring by Skylar One</i>	51
<i>Creating an SNMP Credential for a LifeSize Endpoint</i>	53

Configuring LifeSize Endpoints for Monitoring by Skylar One

Skylar One 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, Skylar One automatically aligns 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. LifeSize endpoints enable the SNMP agent by default. To verify that the SNMP agent is enabled, run the following command:

```
get snmp enable
```

If the SNMP agent is enabled, the following message appears:

```
on
```

```
ok, 00
```

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

```
set snmp enable on
```

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

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

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

5. Optionally, you can run the following two commands to change the SNMP system contact and SNMP system location. Replace *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 SNMP v3 credential for a LifeSize Endpoint in Skylar One:

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**. 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 <i>Timeout (ms)</i> and <i>Retries</i> fields. You must leave all other fields on this page set to the default value.

4. Click 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. Skylar One discovers the LifeSize Endpoint as an SNMP device and automatically aligns the LifeSize Dynamic Applications. For more information Skylar One, see the *Discovery and Credentials* manual.

Monitoring Poly HDX and VSX Series Endpoints

Overview

This section describes how to configure Poly HDX and VSX Series endpoints for monitoring by Skylar One using the "Poly: Endpoint" PowerPack.

This chapter covers the following topics:

<i>Configuring Poly Endpoints for Monitoring by Skylar One</i>	54
<i>Creating an SNMP Credential</i>	57
<i>Configuring SOAP/XML Credentials</i>	63
<i>Dynamic Applications for Poly Endpoints</i>	66

Configuring Poly Endpoints for Monitoring by Skylar One

Skylar One 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 you or another administrator set in 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 describes how to:

- password for 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 you assigned an IP address to the Poly Endpoint and that a Data Collector on the network can reach it.

To log in to the web interface on a Poly Endpoint:

1. In a browser window, Poly Endpoint. The **Poly Welcome** page appears:

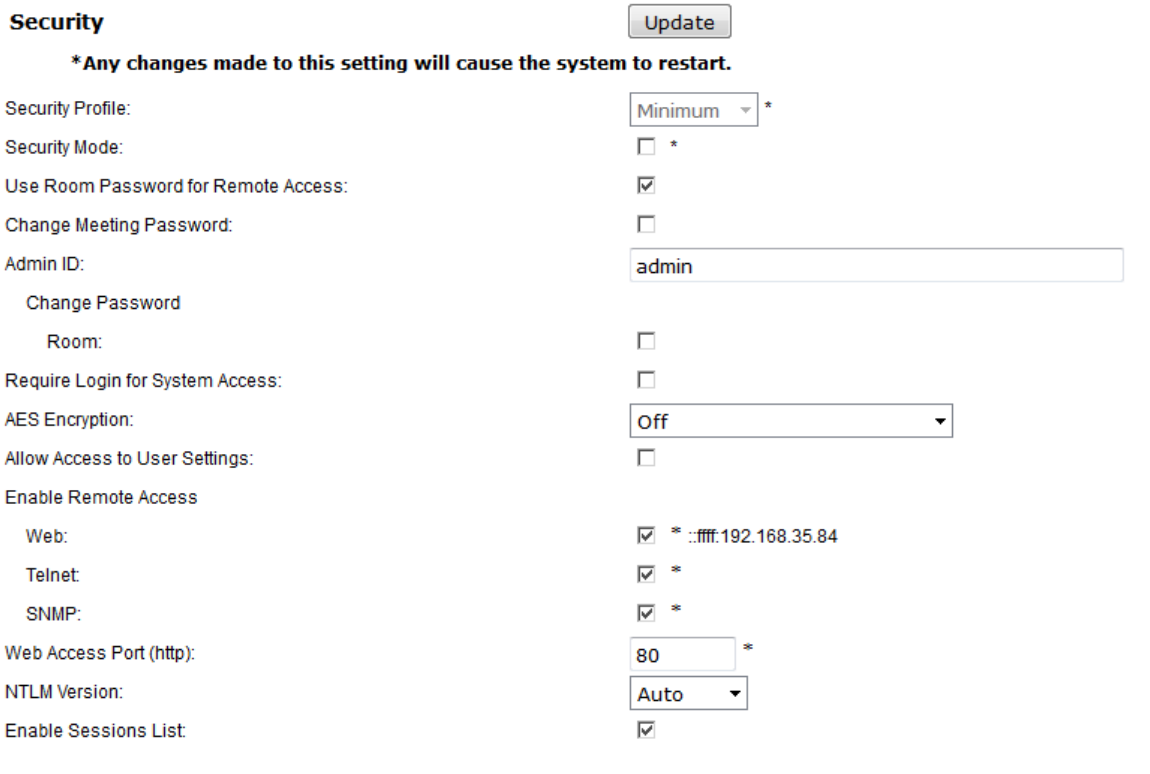


2. Click **[Admin Settings]** on the top navigation bar. A prompt for a username and password appears.
3. In the username field, type "admin".
4. In the password field, enter the room password for the "admin" user.
5. Click **[OK]**.

To change the password that Skylar One uses to perform HTTP requests on this device:

CAUTION: If you enter a new password, the password changes for all administrators that use the "admin" user on this device.

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



Security Update

Any changes made to this setting will cause the system to restart.

Security Profile: Minimum *

Security Mode: ☐ *

Use Room Password for Remote Access: ☒

Change Meeting Password: ☐

Admin ID: admin

Change Password

Room: ☐

Require Login for System Access: ☐

AES Encryption: Off

Allow Access to User Settings: ☐

Enable Remote Access

Web: ☒ * ::ffff:192.168.35.84

Telnet: ☒ *

SNMP: ☒ *

Web Access Port (http): 80 *

NTLM Version: Auto

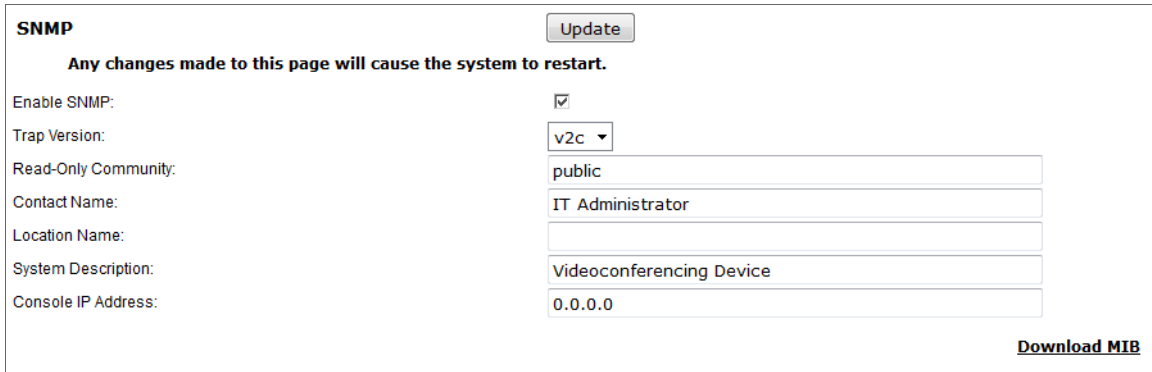
Enable Sessions List: ☒

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

To configure the SNMP settings on a Poly HDX or VSX Series Endpoint:

CAUTION: The device restarts automatically 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.** Select this checkbox if it is not already selected.
 - **Trap Version.** Select v2c in this field.
 - **Read-Only Community.** Enter the new SNMP community string for this device. When you configure an SNMP credential for this Poly Endpoint in Skylar One, you enter this community string in the **SNMP Community (Read-Only)** field.
 - **Contact Name.** Optionally, enter the contact information for the administrator of this device.
 - **Location Name.** Optionally, enter the location of this device.
 - **System Description.** Enter device.
 - **Console IP Address.** Enter the IP address of the Message Collector or Data Collector that collects SNMP trap messages from the device.
3. Click the **[Update]** button to save the new SNMP settings. The device restarts automatically.

Creating an SNMP Credential

SNMP credentials allow Skylar One to access SNMP data on a managed device. Skylar One 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. Select *Create SNMP Credential*. The **Create Credential** modal 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. Toggle off (gray) to align the credential to specific organizations, and then select one or more organizations from the **What organization manages this service?** drop-down list. This field is required.
 - **Timeout (ms)**. Time, in milliseconds, after which Skylar One stops 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 that Skylar One uses to communicate with the external device or application. The default value is *161*. This field is required.
 - **SNMP Retries**. Number of times Skylar One tries 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]**.

Creating an SNMPv2 Credential in the Classic Skylar One User Interface

To monitor Poly Endpoints in Skylar One, create an SNMP credential for each Endpoint.

To create an SNMP Credential for a Poly Endpoint in Skylar One:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the **[Create]** button. Select *SNMP Credential*. The **Credential Editor** page appears.
3. Supply values in the following fields:
 - **Profile Name**. Enter a name for the credential.
 - **SNMP Version**. Select *SNMP V2*.
 - **SNMP Community (Read-Only)**. Enter 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, see the section on "Running a Discovery Session" in the *Discovery and Credentials* manual.

Creating an SNMPv3 Credential

SNMP credentials allow Skylar One to access SNMP data on a managed device. Skylar One 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. Select *Create SNMP Credential*. The **Create Credential** modal 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. Toggle off (gray) to align the credential to specific organizations, and then select one or more organizations from the *What organization manages this service?* drop-down list. This field is required.
- **Timeout (ms).** Time, in milliseconds, after which Skylar One stops 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 that Skylar One uses to communicate with the external device or application. The default value is *161*. This field is required.
- **SNMP Retries.** Number of times Skylar One tries 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 generates the authentication and encryption keys from the associated passwords and the engine ID.) This field is optional.
- **Context.** A context is a mechanism within SNMPv3 (and AgentX) that you can use to run 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]**.

SNMPv3 Credential in the Classic Skylar One User Interface

To monitor Poly Endpoints in Skylar One, create an SNMP credential for each Endpoint.

To create an SNMP Credential for a Poly Endpoint in Skylar One:

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

2. Click the **[Create]** button. Select *SNMP Credential*. The **Credential Editor** page appears.
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 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, see the section on "Running a Discovery Session" in the *Discovery and Credentials* manual.

Performing Bulk Retrieval Using SNMPv3

Use the `snmpbulkwalk` command to perform a bulk retrieval of SNMP data from a device that uses 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
```

where:

- `-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 (for example, MD5 or SHA).
- `-A <security_passphrase>`: Specifies the passphrase for authentication.
- `-x <privacy_protocol>`: Specifies the privacy (encryption) protocol (for example, 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 Skylar One to access a web server on a managed device. Skylar One uses SOAP/XML credentials in several places, 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. Select *Create SOAP/XML Credential*. The **Create Credential** modal 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. Toggle off (gray) to align the credential to specific organizations, and then select one or more organizations from the *What organization manages this service?* drop-down list. This field is required.

- **Timeout (ms).** Time, in milliseconds, after which Skylar One stops 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: If you specify a port in the URL, Skylar One stores the port. If you do not specify a port, Skylar One uses the default port values 80 for HTTP and 443 for HTTPS.

- You can include the variable `%D` in this field. Skylar One replaces the variable with the IP address of the current device (the device that currently uses the credential).

NOTE: For component devices, Skylar One replaces `%D` with the IP address of the root device.

- You can include the variable `%N` in this field. Skylar One replaces the variable with the hostname of the current device (the device that currently uses the credential). If Skylar One cannot determine the hostname, Skylar One replaces 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 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. Skylar One sends the request 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. Skylar One encrypts the value in the request, masks it in the **Credential Editor**, and stores it in 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 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 list 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, see the cURL manpage at <http://curl.haxx.se/docs/manpage.html>.

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

Creating SOAP/XML Credentials in the Classic Skylar One 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"

Skylar One uses these credentials to monitor Poly Endpoints and to collect call detail records. Each credential uses a unique combination of URL, username, and password.

If you have multiple Poly Endpoints, you 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 credentials:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the wrench icon () for the "Poly - Advanced" credential. The **Credential Editor** modal appears.
3. In the **Profile Name** field, enter a new name for the credential.
4. In the **HTTP Auth Password** field, enter 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 you can use to monitor Poly Endpoints and Group Series (GS) devices. Some of the Dynamic Applications for Poly Endpoints use the caching feature:

- Four Dynamic Applications only collect and cache data from Poly Endpoints.
- Three Dynamic Applications use the cached data. For these Dynamic Applications to display data, you must align the Dynamic Applications that collect and cache data 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, you can include all the SOAP/XML credentials that you configured for your Poly Endpoint in the **Other Credentials** field of the **Discovery Session Editor** page. Skylar One then automatically aligns 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:

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

2. Click the **[Create]** button. The **Template Editor** page appears.
3. Enter 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. 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 apply the device template to your Poly Endpoints:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. Select the checkbox for each Poly Endpoint.
3. In the **Select Action** drop-down list, select *Modify By Template*. Click the **[Go]** button. The **Bulk Device Configuration** modal 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 table also lists the dependencies between the Dynamic Applications that populate the cache and the Dynamic Applications that consume the cache. Each row lists the credential that you must align with the 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

Dynamic Application	Credential	Caching Type	Dependencies
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

Monitoring Tandberg Infrastructure

Overview

The following sections describe how to configure Cisco Tandberg infrastructure devices for monitoring by Skylar One using the "Tandberg: Infrastructure" PowerPack:

This chapter covers the following topics:

<i>Tandberg Infrastructure Support</i>	69
<i>Creating a Credential for Tandberg Infrastructure Dynamic Applications</i>	72
<i>Creating a Credential for TelePresence Content Server</i>	73
<i>Video Communication Server</i>	75
<i>TelePresence Server</i>	80
<i>TelePresence Control Unit</i>	84

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. This credential is either the generic credential for Tandberg Infrastructure devices or a specific credential for that device type. The Credential column for each device type 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)	<i>Generic</i>	• 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)	<i>Generic</i>	• 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)	<i>Generic</i>	• Tandberg: Codian Performance • Tandberg: Codian Status • Tandberg: Codian ISDN Gateway Call Details
IP Gateways	4510 3520 3540 8350 (blade)	<i>Generic</i>	• Tandberg: Codian Status • Tandberg: Codian Performance
Media Gateway	3610	<i>Generic</i>	• Tandberg: Codian Status • Tandberg: Codian Performance
IP VCR	2210 2220 2240 8220 (blade)	<i>Generic</i>	• 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	TelePresence Content Server (TCS)	Specific credential. For more information, see the 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 credential. For more information, see the 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 credential. For more information, see the 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	TelePresence Control Unit (TCU)	Specific credential. For more information, see the 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, create a SOAP/XML credential and align it with the Dynamic Applications for that device.

To create a SOAP/XML credential for Tandberg infrastructure devices:

1. Use the manufacturer's instructions to find the username and password for the web service on the device.
2. Go to the **Credentials** page (Manage > Credentials).
3. Click the **[Create]** button and then select *SOAP/XML 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 Skylar One to stop trying to communicate with the web server.
 - **URL**. Type "http://%D/rpc2". Skylar One replaces the variable %D with the IP address of the device that uses the credential.
 - **HTTP Auth User**. Enter the username that you use to log in to the web server.
 - **HTTP Auth Password**. Enter the password with which you access the web server.
5. You can leave the remaining fields in the **Credential Editor** page blank or at their default values.
6. Click the **[Save]** button to save the credential.

Creating a Credential for Tandberg Infrastructure in the Classic Skylar One User Interface

For Tandberg infrastructure devices that use the generic credential, create a SOAP/XML credential and align it with the Dynamic Applications for that device.

To create a SOAP/XML credential for Tandberg infrastructure devices:

1. Use the manufacturer's instructions to find the username and password for 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. 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.** Type "http://%D/rpc2". Skylar One replaces the variable %D with the IP address of the device that uses the credential.
 - **HTTP Auth User.** Enter the username that you use to 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 Skylar One to stop trying to communicate with the web server.
5. You can leave the remaining fields in the **Credential Editor** page blank or at their default values.
 6. Click the **[Save]** button to save the credential.

Creating a Credential for TelePresence Content Server

For the Dynamic Applications that you align with the TelePresence Content Server, create a SOAP/XML credential and align it with the Dynamic Application.

To create the credential:

1. Use the manufacturer's instructions to find the username and password for 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. 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 Skylar One to stop trying to communicate with the web server.
 - **URL.** Type the URL that corresponds to the Dynamic Application. Skylar One replaces the variable %D with the IP address of the device that uses 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.** Enter the username that you use to log in to the web server.
 - **HTTP Auth Password.** Enter the password with which you access the web server.
5. You can leave the remaining fields in the **Create Credentials** page blank or at their default values.
 6. Click the **[Save]** button to save the credential.

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

For the Dynamic Applications that you align with the TelePresence Content Server, create a SOAP/XML credential and align it with the Dynamic Application.

To create the credential in the classic Skylar One user interface:

1. Use the manufacturer's instructions to find the username and password for 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. 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. Skylar One replaces the variable %D with the IP address of the device that uses 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.** Enter the username that you use to 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 Skylar One to stop trying to communicate with the web server.
5. You can leave the remaining fields in the **Credential Editor** page blank or at their default values.
6. Click the **[Save]** button to save the credential.

Video Communication Server

The Video Communication Server (VCS) has two products:

- VCS-Control
- VCS-Expressway

Both products use the same code base. Use the VCS-Control product for enterprise applications. The VCS-Control product provides gatekeeper and SIP proxy functionality.

The VCS-Expressway provides two functions:

- Host endpoints outside the corporate firewall. Users who work from home can then connect to internal video conferencing equipment without a virtual private network (VPN).
- Provide Border Gateway services for business-to-business (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 Simple Network Management Protocol (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 lists all registrations on the VCS. It also provides historical information about registrations that aged out and devices that unregistered.

Creating a Credential for VCS Devices

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

To create a credential for VCS devices:

1. Use the manufacturer's instructions to find the username and password for 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. Enter values in the following fields:
 - **Name**. Enter 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 that run version 7.2 or later, select *GET*. For VCS systems earlier than version 7.2, select *POST*.
 - **HTTP Version**. Leave this field at the default value of *HTTP /1.1*.
 - **URL**. Type "http://%D/configuration.xml". Skylar One replaces the variable %D with the IP address of the device that uses the credential.
 - **HTTP Auth User**. Enter the username you use to log in to the web server.
 - **HTTP Auth Password**. Enter the password you use to access the web server.
 - **Embedded Password [%P]**. Enter the embedded password associated with the web server.
 - **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 field:
 - **CDRIncludeSourceDomains**. Enter a comma-separated list of domains in this field to be filtered by the call's source domain. For example, `cisco.call.ciscopark` or `cisco.call.webex.com`. Do not include any colons (:) in the source domains in this field.

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

NOTE: If you leave these fields blank, the "Tandberg: VCS Status" Dynamic Application generates alerts for calls from all domains with cause codes in the default range of 500 to 599.

5. You can leave the remaining fields on the **Create Credential** page blank or at their default values.
6. Click the **[Save]** button to save the credential.

Creating a Credential for VCS Devices in the Classic Skylar One User Interface

For the Dynamic Applications in the "Tandberg: Infrastructure" PowerPack that can be aligned with VCS devices, you must create a SOAP/XML credential in the classic Skylar One user interface and align it with the Dynamic Application.

To create a credential for VCS devices:

1. Use the manufacturer's instructions to find the username and password for 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. Enter values in the following fields:
 - **Profile Name**. Enter a name for the credential. This name can be any combination of alphanumeric characters.
 - **Method**. For VCS systems that run version 7.2 or later, select *GET*. For VCS systems earlier than version 7.2, select *POST*.
 - **HTTP Version**. Leave this field at the default value of *HTTP /1.1*.
 - **URL**. Type `http://%D/configuration.xml`. Skylar One replaces the variable `%D` with the IP address of the device that uses the credential.
 - **HTTP Auth User**. Enter the username you use to log in to the web server.
 - **HTTP Auth Password**. Enter 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 field:

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

NOTE: If you leave these fields blank, the "Tandberg: VCS Status" Dynamic Application generates alerts for calls from all domains with cause codes in the default range of 500 to 599.

5. You can leave the remaining fields on the **Credential Editor** page blank or at their default values.
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 for a VCS device:

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 the 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**. Enter a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.
 - **Description**. Optional. Enter 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.** Enter 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 runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds a device, the **Discovery Logs** page includes a link to the **Device Investigator** page for that device.
 10. If you did not enable the **Run after save** option, click the **[Save and Close]** button. The new discovery session appears on the **Discovery Sessions** page (Devices > Discovery Sessions).

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 (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
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 appears. To align a Dynamic Application with a device on 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 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 "Tandberg: Infrastructure" PowerPack includes the following Dynamic Applications for monitoring a TelePresence Server:

- "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, create a SOAP/XML credential and align it 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 the "Tandberg: Codian TS Configuration" and "Tandberg: Codian TS Status" Dynamic Applications, type "15". For the remaining Dynamic 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. Skylar One replaces the variable %D with the IP address of the device that uses 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.** Enter the username with which you log in to the web server.
 - **HTTP Auth Password.** Enter the password for the username you entered in the **HTTP Auth User** field.
4. You can leave the remaining fields in the **Create Credential** page blank or at their default values.
 5. Click the **[Save]** button to save the credential.

Creating a Credential for a TelePresence Server in the Classic Skylar One User Interface

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

To create the credential in the classic Skylar One 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. Skylar One replaces the variable %D with the IP address of the device that uses 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**. Enter the username with which you log in to the web server.
 - **HTTP Auth Password**. Enter 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 Dynamic Applications, type "10".
4. You can leave the remaining fields in the **Credential Editor** page blank or at their default values.
 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 for a TelePresence device:

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 the 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**. Enter a unique name for this discovery session. This name appears in the list of discovery sessions on the **[Discovery Sessions]** tab.
 - **Description**. Optional. Enter 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**. Enter the IP address for the TelePresence device.
 - **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 runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds a device, the **Discovery Logs** page includes a link to the **Device Investigator** page for that device.
- 10. If you did not enable the **Run after save** option, click the **[Save and Close]** button. The new discovery session appears on the **Discovery Sessions** page (Devices > Discovery Sessions).

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 (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
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 appears. To align a Dynamic Application with a device on 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 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"
 - "Tandberg: Codian TS Participant Details"

- "Tandberg: Codian TS Conference Details"

NOTE: The "Tandberg: Codian TS Participant Details" and "Tandberg: Codian TS Conference Details" Dynamic Applications are only supported for TelePresence Server versions 4.2 and earlier. The API no longer provides this information for TelePresence Server versions 4.3 and later. If you align these Dynamic Applications, log messages such as "API version is not supported by application" appear.

TelePresence Control Unit

The "Tandberg: Infrastructure" PowerPack includes the following Dynamic Applications for monitoring a TelePresence Control Unit:

- "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, create a SOAP/XML credential and align it 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 **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).** Enter the time, in seconds, after which you want Skylar One 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. Skylar One replaces the variable `%D` with the IP address of the device that uses 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**. Enter the username with which you log in to the web server.
 - **HTTP Auth Password**. Enter the password for the username you entered in the **HTTP Auth User** field.
4. You can leave the remaining fields in the **Create Credential** page blank or at their default values.
 5. Click the **[Save]** button to save the credential.

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

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

To create the credential in the classic Skylar One 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. Skylar One replaces the variable `%D` with the IP address of the device that uses 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**. Enter the username with which you log in to the web server.
 - **HTTP Auth Password**. Enter the password for the username you entered in the **HTTP Auth User** field.
 - **Timeout (seconds)**. Enter the time, in seconds, after which you want Skylar One to stop trying to communicate with the web server.
4. You can leave the remaining fields in the **Credential Editor** page blank or at their default values.
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 for a TelePresence device:

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 the 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.** Enter a unique name for this discovery session. This name appears in the list of discovery sessions on the **[Discovery Sessions]** tab.
 - **Description.** Optional. Enter 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.** Enter the IP address for the TelePresence device.
 - **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 runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds a device, the **Discovery Logs** page includes a link to the **Device Investigator** page for that device.
10. If you did not enable the **Run after save** option, click the **[Save and Close]** button. The new discovery session appears on the **Discovery Sessions** page (Devices > Discovery Sessions).

Manually Aligning the Dynamic Applications with the TelePresence Control Unit

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 (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
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 appears. To align a Dynamic Application with a device on 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 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 display data collected from video devices:

This chapter covers the following topics:

<i>TelePresence Inventory Report</i>	89
<i>Video Calls by Device Group, Call Type, and Bandwidth Report</i>	90
<i>Video Endpoint Availability Chart Report</i>	91
<i>Video Endpoint Availability Table Report</i>	93
<i>Video Endpoint Avg Jitter Column Chart Report</i>	95
<i>Video Endpoint Avg Jitter Line Chart Report</i>	97
<i>Video Endpoint Avg Jitter Table Report</i>	100
<i>Video Endpoint Call Detail Records Report</i>	101
<i>Video Endpoint Detailed Asset Inventory Report</i>	104
<i>Video Endpoint Detailed Jitter Line Chart Report</i>	105
<i>Video Endpoint Detailed Packet Loss Line Chart Report</i>	108
<i>Video Endpoint Packet Loss Column Chart Report</i>	110
<i>Video Endpoint Packet Loss Line Chart Report</i>	112
<i>Video Endpoint Packet Loss Table Report</i>	114

Video Endpoint Performance Detail Report	115
Video Endpoint Unavailability Chart Report	117
Video Endpoint Unavailability Table Report	120
Video Usage Report	122
Video Usage Chart Report	123

NOTE: You can generate the reports in this chapter as quick reports on the **Run Quick Report** page (Reports > Run Report), or configure them as scheduled reports on the **Report Jobs** page (Reports > Create Report > Report Jobs). For more information, 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.



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	N/A	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 to include 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 in the "Video Reports" PowerPack. You or another user might have modified this report on your Skylar One 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.

				
Video Calls by DeviceGroup, Call Type, Bandwidth – Apr 2012 for 36 months				
Date: February 2015				
Organization: Customer A Video				
Call Type: Unknown				
	Bandwidth	Calls	Hours	
	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				
	Bandwidth	Calls	Hours	
	10500	110		0
Sum for Call Type: Unknown	10500	110		0
Call Type: Video				
	Bandwidth	Calls	Hours	
	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				
	Bandwidth	Calls	Hours	
	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 to display at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" displays at the top of the report.
- **Device Selection.** Select the devices to include in the report. The following options are available:
 - *All devices.* Select this checkbox if you want all devices in the system to be included in this report.
 - *Organizations.* If you do not select the **All devices** checkbox, select one or more organizations. The report contains 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 you do not select the **All devices** checkbox, the **Select individual devices** checkbox is available. Select this checkbox 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 options are available:
 - *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 contains 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 is arranged:
 - **Separated By.** Select whether the report separates the data 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.** Select whether the Device ID or the Organization ID appears 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. Skylar One uses data from that date as the starting point of the report. **Duration.** Specify the duration for the report, from 1 month to 36 months. Skylar One uses 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 time zone to use for date and time values in the report. Specify the time zone as the number of hours offset from Coordinated Universal Time (UTC).
- **Report Type.** Specify whether the report includes all selected devices or only a set number of the devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the "Video Reports" PowerPack. You or another user might have modified this report on your Skylar One system.

Video Endpoint Availability Chart Report

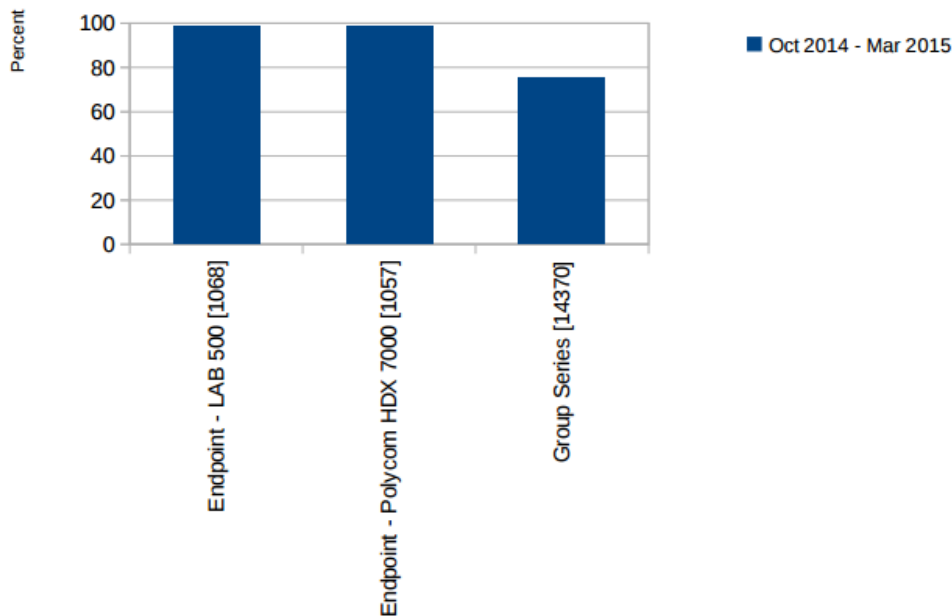
This report displays a bar graph of device availability for Tandberg, LifeSize, Cisco, and Polycom video endpoints. For each device included in the report, the report displays availability in percentage for the time period selected for the report.

You can customize the output to include only specific devices or to limit the number of devices in the report. You can also specify the time span to include in the report, the text at the top of the report, and how the report sorts and arranges the devices.



Video Endpoint Availability Chart – Oct 2014 for 6 months

Organization: Customer A Video



The following input options are available when generating the report:

- **Branding.** Optionally, enter text to display at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" displays at the top of the report.
- **Device Selection.** Select the devices to include in the report. The following options are available:
 - **All devices.** Select this checkbox if you want all devices in the system to be included in this report.
 - **Organizations.** If you do not select the **All devices** checkbox, select one or more organizations. The report contains 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 you do not select the **All devices** checkbox, the **Select individual devices** checkbox is available. Select this checkbox 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 options are available:
 - *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 contains 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 is arranged:
 - **Separated By.** Select whether the report separates the data 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.** Select whether the Device ID or the Organization ID appears in the report.
 - **Stacking.** Select the **Enable Stacking** checkbox to stack the data.
- **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. Skylar One uses data from that date as the starting point of the report. **Duration.** Specify the duration for the report, from 1 month to 36 months. Skylar One uses 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 time zone to use for date and time values in the report. Specify the time zone as the number of hours offset from Coordinated Universal Time (UTC).
- **Report Type.** Specify whether the report includes all selected devices or only a set number of the devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the "Video Reports" PowerPack. You or another user might have modified this report on your Skylar One 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 or to limit the number of devices in the report. You can also specify the time span to include in the report, the text at the top of the report, and how the report sorts and arranges the devices.



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 [1046]	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	12.84	16.63	12.53
Average for Organization: Customer A Video		11.09	16.65	16.02	15.58	15.39	16.18	15.15
Organization: Customer B Video								
Category	Device	Oct 2014	Nov 2014	Dec 2014	Jan 2015	Feb 2015	Mar 2015	Average
Video Endpoint	Endpoint - 17000LNP [1067]	16.64	16.66	16.2	16.45	16.66	15.96	16.43
Video Endpoint	EX000 [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 - L8635ae 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:		11.59	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 to display at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" displays at the top of the report.
- **Device Selection.** Select the devices to include in the report. The following options are available:
 - **All devices.** Select this checkbox if you want all devices in the system to be included in this report.
 - **Organizations.** If you do not select the **All devices** checkbox, select one or more organizations. The report contains 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 you do not select the **All devices** checkbox, the **Select individual devices** checkbox is available. Select this checkbox 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 options are available:
 - **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 contains 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 is arranged:
 - **Separated By.** Select whether the report separates the data 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.** Select whether the Device ID or the Organization ID appears 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. Skylar One uses data from that date as the starting point of the report. **Duration.** Specify the duration for the report, from 1 month to 36 months. Skylar One uses 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 time zone to use for date and time values in the report. Specify the time zone as the number of hours offset from Coordinated Universal Time (UTC).
- **Report Type.** Specify whether the report includes all selected devices or only a set number of the devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the "Video Reports" PowerPack. You or another user might have modified this report on your Skylar One system.

Video Endpoint Avg Jitter Column Chart Report

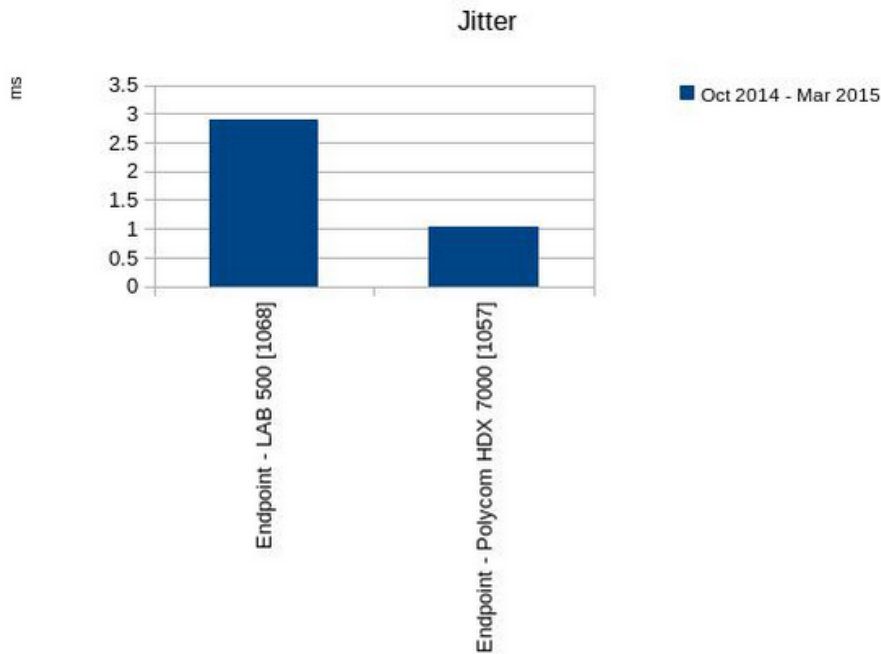
This report displays the average jitter for Tandberg, Polycom, LifeSize and Cisco TelePresence devices. For each device included in the report, the report displays the jitter average in milliseconds for the time period selected for the report.

You can customize the output to include only specific devices or to limit the number of devices in the report. You can also specify the time span to include in the report, the text at the top of the report, and how the report sorts and arranges the devices.



Video Endpoint Avg Jitter Column Chart – Oct 2014 for 6 months

Organization: Customer A Video



The following input options are available when generating the report:

- **Branding.** Optionally, enter text to display at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" displays at the top of the report.
- **Device Selection.** Select the devices to include in the report. The following options are available:
 - **All devices.** Select this checkbox if you want all devices in the system to be included in this report.
 - **Organizations.** If you do not select the **All devices** checkbox, select one or more organizations. The report contains 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 you do not select the **All devices** checkbox, the **Select individual devices** checkbox is available. Select this checkbox 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 options are available:
 - *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 contains 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 is arranged:
 - **Separated By.** Select whether the report separates the data 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.** Select whether the Device ID or the Organization ID appears in the report.
 - **Stacking.** Select the **Enable Stacking** checkbox to stack the data.
- **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. Skylar One uses data from that date as the starting point of the report.
- **Duration.** Specify the duration for the report, from 1 month to 36 months. Skylar One uses 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 time zone to use for date and time values in the report. Specify the time zone as the number of hours offset from Coordinated Universal Time (UTC).
- **Report Type.** Specify whether the report includes all selected devices or only a set number of the devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the "Video Reports" PowerPack. You or another user might have modified this report on your Skylar One system.

Video Endpoint Avg Jitter Line Chart Report

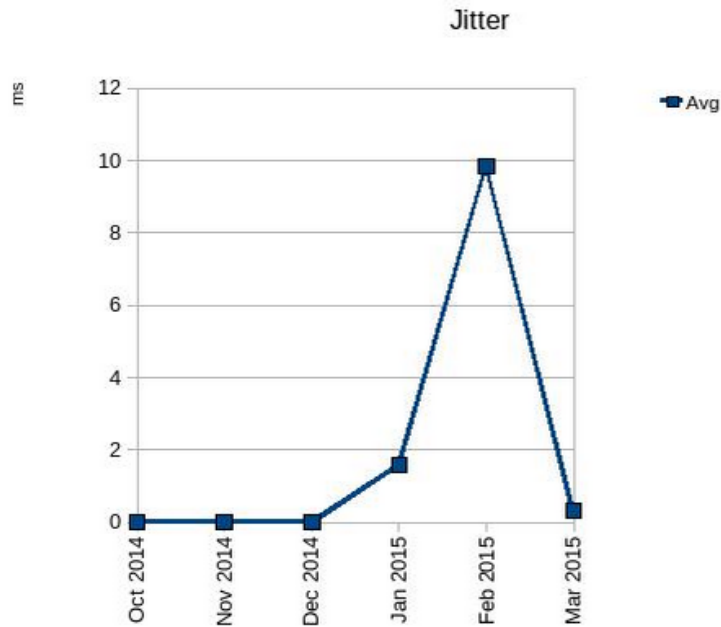
This report displays the average jitter for Tandberg, Polycom, LifeSize and Cisco TelePresence devices. For each device included in the report, the report displays the jitter average in milliseconds for the time period selected for the report.

You can customize the output to include only specific devices or to limit the number of devices in the report. You can also specify the time span to include in the report, the text at the top of the report, and how the report sorts and arranges the devices.



Video Endpoint Avg Jitter Line Chart – Oct 2014 for 6 months

Organization: Customer A Video



The following input options are available when generating the report:

- **Branding.** Optionally, enter text to display at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" displays at the top of the report.
- **Device Selection.** Select the devices to include in the report. The following options are available:
 - **All devices.** Select this checkbox if you want all devices in the system to be included in this report.
 - **Organizations.** If you do not select the **All devices** checkbox, select one or more organizations. The report contains 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 you do not select the **All devices** checkbox, the **Select individual devices** checkbox is available. Select this checkbox 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 options are available:
 - *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 contains 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 is arranged:
 - **Separated By.** Select whether the report separates the data 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.** Select whether the Device ID or the Organization ID appears in the report.
 - **Stacking.** Select the **Enable Stacking** checkbox to stack the data.
- **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. Skylar One uses data from that date as the starting point of the report. **Duration.** Specify the duration for the report, from 1 month to 36 months. Skylar One uses 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 time zone to use for date and time values in the report. Specify the time zone as the number of hours offset from Coordinated Universal Time (UTC).
- **Report Type.** Specify whether the report includes all selected devices or only a set number of the devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the "Video Reports" PowerPack. You or another user might have modified this report on your Skylar One 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 or to limit the number of devices in the report. You can also specify the time span to include in the report, the text at the top of the report, and how the report sorts and arranges the devices.

								
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 - LAR 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 - 1700NDP [1067]	0.00	0.00	0.00	1.91	5.70	0.64	1.38
	EX200 [9826]	0.00	0.00	0.00	1.04	3.41	0.44	0.51
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 to display at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" displays at the top of the report.
- **Device Selection.** Select the devices to include in the report. The following options are available:
 - **All devices.** Select this checkbox if you want all devices in the system to be included in this report.
 - **Organizations.** If you do not select the **All devices** checkbox, select one or more organizations. The report contains 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 you do not select the **All devices** checkbox, the **Select individual devices** checkbox is available. Select this checkbox 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 options are available:
 - *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 contains 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 is arranged:
 - **Separated By.** Select whether the report separates the data 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.** Select whether the Device ID or the Organization ID appears 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. Skylar One uses data from that date as the starting point of the report. **Duration.** Specify the duration for the report, from 1 month to 36 months. Skylar One uses 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 time zone to use for date and time values in the report. Specify the time zone as the number of hours offset from Coordinated Universal Time (UTC).
- **Report Type.** Specify whether the report includes all selected devices or only a set number of the devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the "Video Reports" PowerPack. You or another user might have modified this report on your Skylar One system.

Video Endpoint Call Detail Records Report

This report displays call detail records (CDRs) 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 to include in the report, the text at the top of the report, and how the report sorts and arranges the devices.



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	3102	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	3102	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	3102	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	3102	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		up	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 07:33:47 AM																	

Generated on: April 17th, 2015 07:53:47 AM

The following input options are available when generating the report:

- **Branding.** Optionally, enter text to display at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" displays at the top of the report.
- **Device Selection.** Select the devices to include in the report. The following options are available:
 - **All devices.** Select this checkbox if you want all devices in the system to be included in this report.
 - **Organizations.** If you do not select the **All devices** checkbox, select one or more organizations. The report contains 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 you do not select the **All devices** checkbox, the **Select individual devices** checkbox is available. Select this checkbox 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 options are available:

- **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 contains 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 Skylar One system uses data from that date as the start of the report.
- **Duration.** Specify the duration for the report, from 1 month to 36 months. The Skylar One system uses data from the **Starting** date as the start of the report and data from the last day of the **Duration** as the end of the report.
- **Included Columns.** Select the **All Columns** checkbox or select columns individually from the list.
- **CDR Output Options.** Specify whether the report presents the duration 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 separates the data 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.** Select whether the Device ID or the Organization ID appears 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, enter 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 for each CDR application type.

This description covers the latest version of this report as shipped by ScienceLogic in the "Video Reports" PowerPack. You or another user might have modified this report on your Skylar One 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 or to limit the number of devices in the report. You can also specify the time span to include in the report, the text at the top of the report, and how the report sorts and arranges the devices.



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]	39836660	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 to display at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" displays at the top of the report.
- **Device Selection.** Select the devices to include in the report. The following options are available:
 - **All devices.** Select this checkbox if you want all devices in the system to be included in this report.
 - **Organizations.** If you do not select the **All devices** checkbox, select one or more organizations. The report contains 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 you do not select the **All devices** checkbox, the **Select individual devices** checkbox is available. Select this checkbox 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 options are available:
 - **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 contains only the devices in the device groups you select.

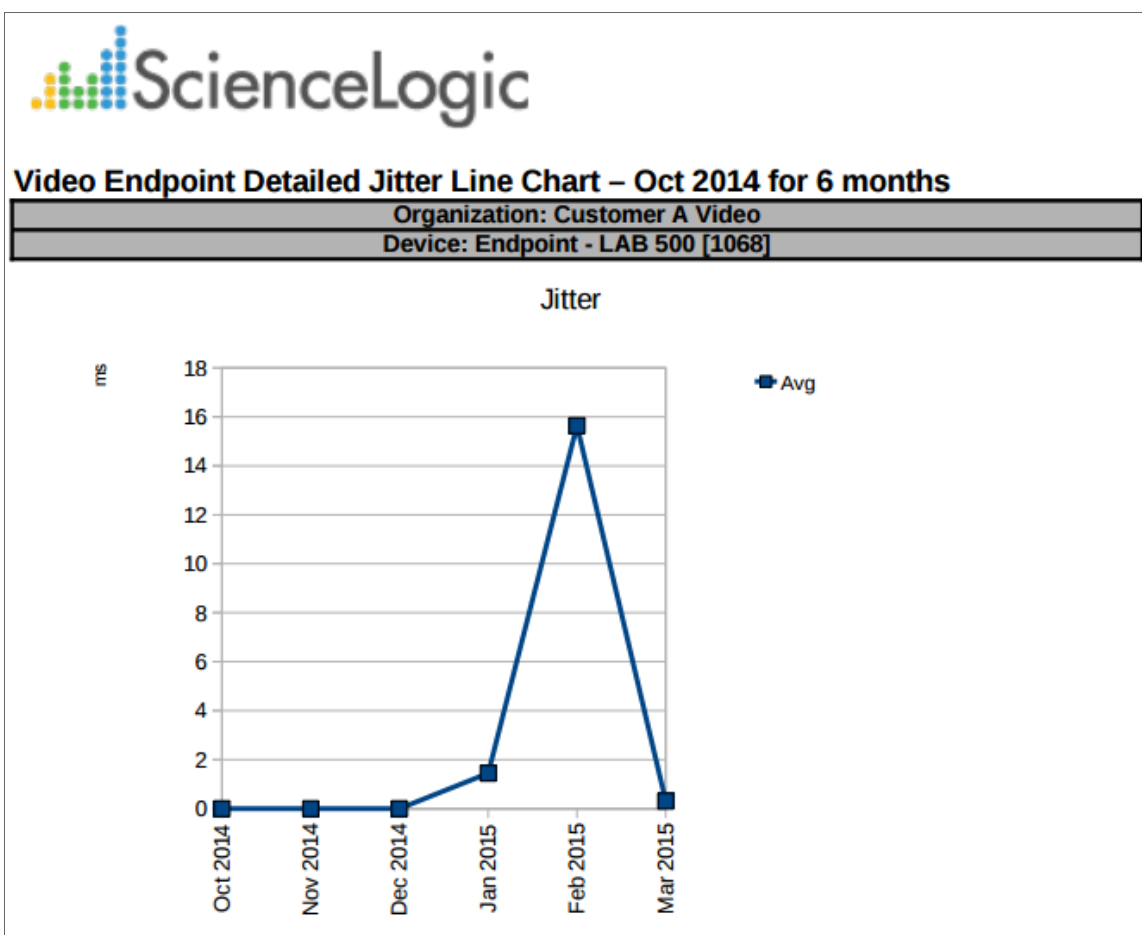
- **Device Categories.** By default, the **All Device Categories** checkbox is selected. To limit the report to one or more specific device categories, select one or more device categories from the list of *Device Categories*.
- **General Display Options.** Specify how the report is arranged:
 - **Separated By.** Select whether the report separates the data 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.** Select whether the Device ID or the Organization ID appears in the report.

This description covers the latest version of this report as shipped by ScienceLogic in the "Video Reports" PowerPack. You or another user might have modified this report on your Skylar One 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 or to limit the number of devices in the report. You can also specify the time span to include in the report, the text at the top of the report, and how the report sorts and arranges the devices.



The following input options are available when generating the report:

- **Branding.** Optionally, enter text to display at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" displays at the top of the report.
- **Device Selection.** Select the devices to include in the report. The following options are available:
 - **All devices.** Select this checkbox if you want all devices in the system to be included in this report.
 - **Organizations.** If you do not select the **All devices** checkbox, select one or more organizations. The report contains 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 you do not select the **All devices** checkbox, the **Select individual devices** checkbox is available. Select this checkbox to use the **Devices by Organization** field to select the individual devices to include in the report.

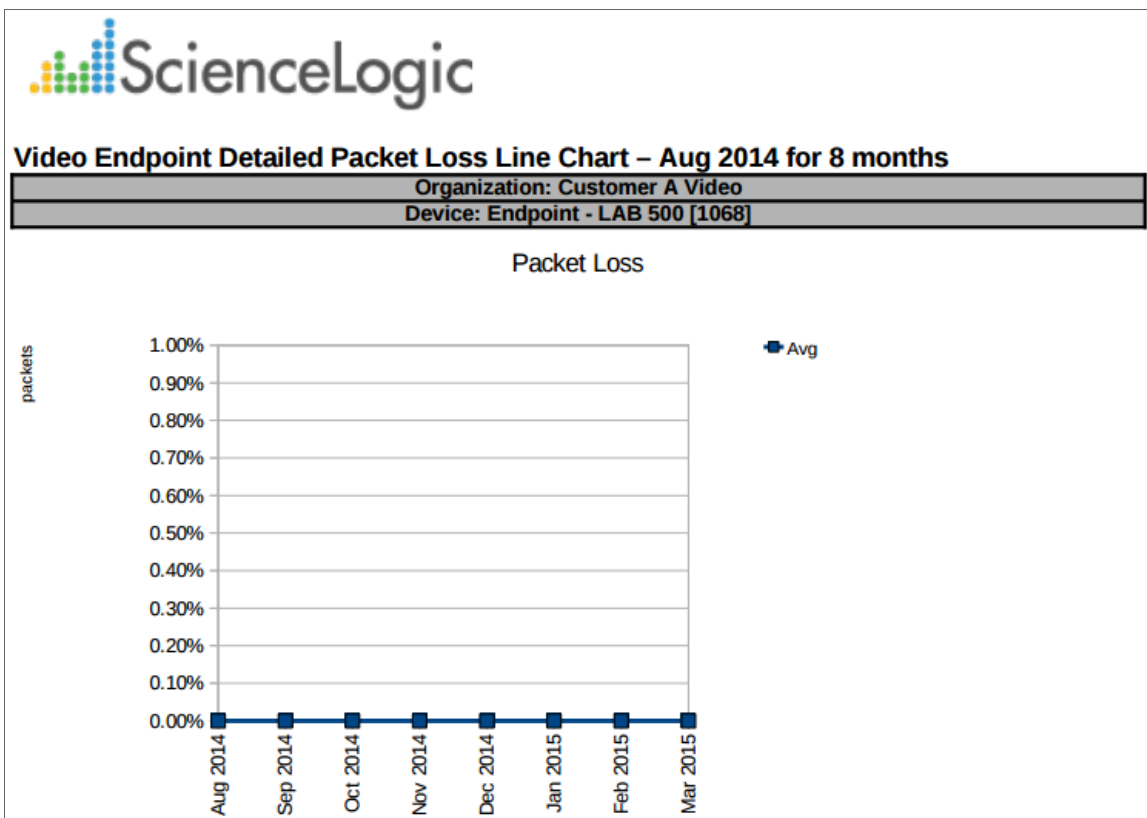
- *Devices by Organization.* This field displays a list of all devices in the organizations selected in the **Organizations** field. If the **Select individual devices** checkbox is selected, you can select one or more devices to include in the report.
- **Device Group Selector.** Select the device groups that will appear in the report. The following options are available:
 - *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 contains 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 is arranged:
 - **Separated By.** Select whether the report separates the data 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.** Select whether the Device ID or the Organization ID appears in the report.
 - **Stacking.** Select the **Enable Stacking** checkbox to stack the data.
- **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. Skylar One uses data from that date as the starting point of the report. **Duration.** Specify the duration for the report, from 1 month to 36 months. Skylar One uses 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 time zone to use for date and time values in the report. Specify the time zone as the number of hours offset from Coordinated Universal Time (UTC).
- **Report Type.** Specify whether the report includes all selected devices or only a set number of the devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the "Video Reports" PowerPack. You or another user might have modified this report on your Skylar One 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 or to limit the number of devices in the report. You can also specify the time span to include in the report, the text at the top of the report, and how the report sorts and arranges the devices.



The following input options are available when generating the report:

- **Branding.** Optionally, enter text to display at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" displays at the top of the report.

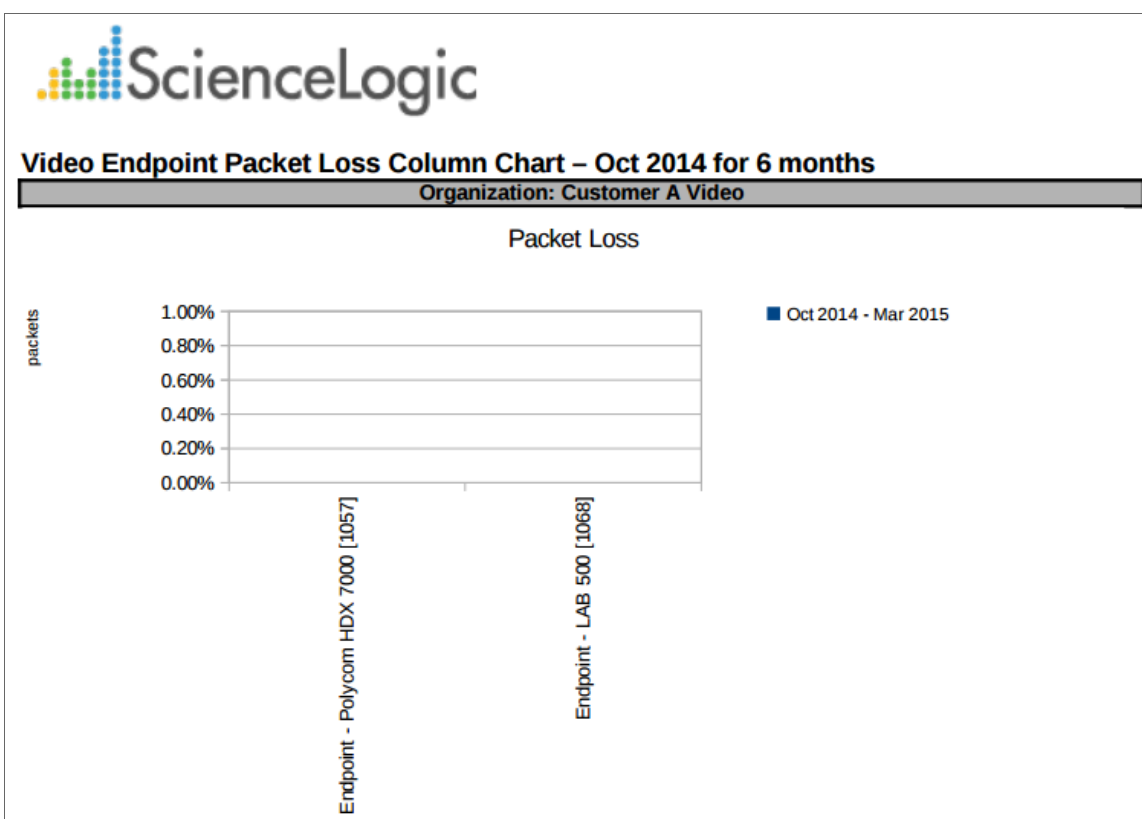
- **Device Selection.** Select the devices to include in the report. The following options are available:
 - *All devices.* Select this checkbox if you want all devices in the system to be included in this report.
 - *Organizations.* If you do not select the **All devices** checkbox, select one or more organizations. The report contains 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 you do not select the **All devices** checkbox, the **Select individual devices** checkbox is available. Select this checkbox 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 options are available:
 - *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 contains 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 is arranged:
 - **Separated By.** Select whether the report separates the data 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.** Select whether the Device ID or the Organization ID appears in the report.
 - **Stacking.** Select the **Enable Stacking** checkbox to stack the data.
- **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. Skylar One uses data from that date as the starting point of the report. **Duration.** Specify the duration for the report, from 1 month to 36 months. Skylar One uses 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 time zone to use for date and time values in the report. Specify the time zone as the number of hours offset from Coordinated Universal Time (UTC).
- **Report Type.** Specify whether the report includes all selected devices or only a set number of the devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the "Video Reports" PowerPack. You or another user might have modified this report on your Skylar One 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 or to limit the number of devices in the report. You can also specify the time span to include in the report, the text at the top of the report, and how the report sorts and arranges the devices.



The following input options are available when generating the report:

- **Branding.** Optionally, enter text to display at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" displays at the top of the report.
- **Device Selection.** Select the devices to include in the report. The following options are available:
 - *All devices.* Select this checkbox if you want all devices in the system to be included in this report.
 - *Organizations.* If you do not select the **All devices** checkbox, select one or more organizations. The report contains 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.

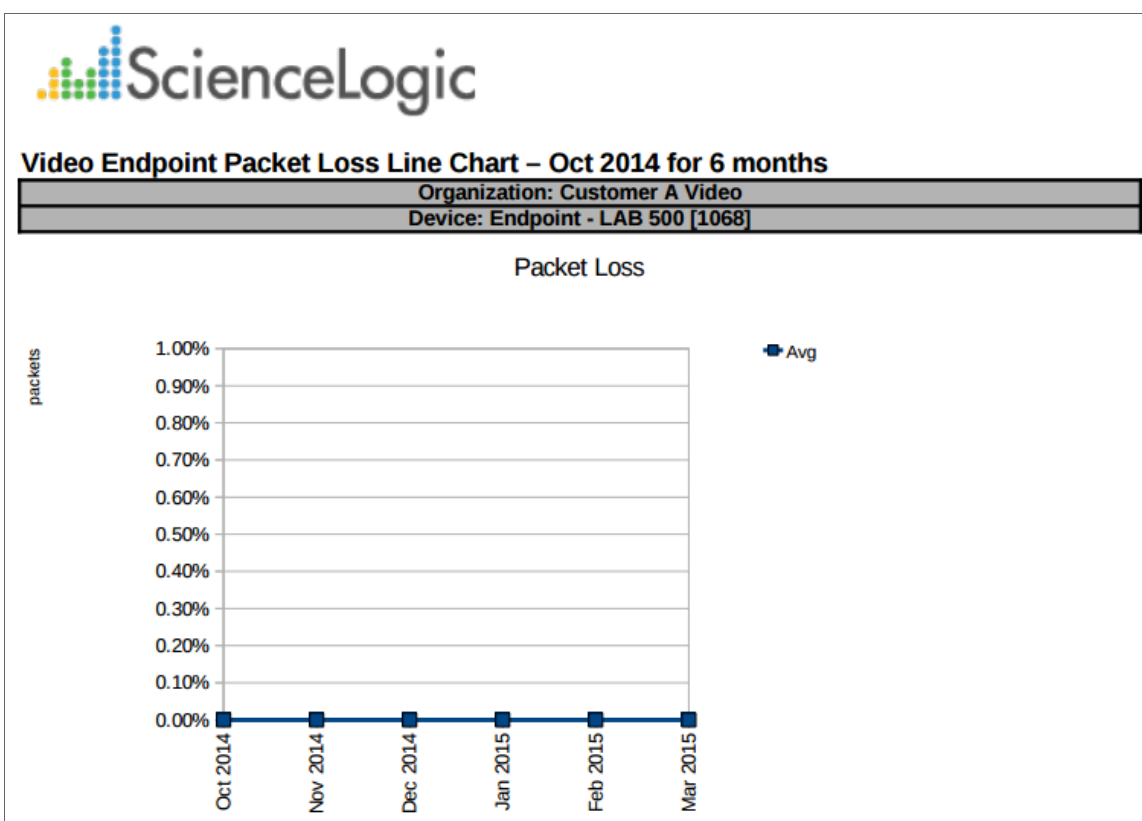
- *Select individual devices.* If you do not select the **All devices** checkbox, the **Select individual devices** checkbox is available. Select this checkbox to use the **Devices by Organization** field to select the individual devices to include in the report.
- *Devices by Organization.* This field 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 options are available:
 - *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 contains 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 is arranged:
 - **Separated By.** Select whether the report separates the data 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.** Select whether the Device ID or the Organization ID appears in the report.
 - **Stacking.** Select the **Enable Stacking** checkbox to stack the data.
- **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. Skylar One uses data from that date as the starting point of the report. **Duration.** Specify the duration for the report, from 1 month to 36 months. Skylar One uses 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 time zone to use for date and time values in the report. Specify the time zone as the number of hours offset from Coordinated Universal Time (UTC).
- **Report Type.** Specify whether the report includes all selected devices or only a set number of the devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the "Video Reports" PowerPack. You or another user might have modified this report on your Skylar One 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 or to limit the number of devices in the report. You can also specify the time span to include in the report, the text at the top of the report, and how the report sorts and arranges the devices.



The following input options are available when generating the report:

- **Branding.** Optionally, enter text to display at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" displays at the top of the report.
- **Device Selection.** Select the devices to include in the report. The following options are available:
 - **All devices.** Select this checkbox if you want all devices in the system to be included in this report.
 - **Organizations.** If you do not select the **All devices** checkbox, select one or more organizations. The report contains 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 you do not select the **All devices** checkbox, the **Select individual devices** checkbox is available. Select this checkbox 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 options are available:
 - *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 contains 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 is arranged:
 - **Separated By.** Select whether the report separates the data 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.** Select whether the Device ID or the Organization ID appears in the report.
 - **Stacking.** Select the **Enable Stacking** checkbox to stack the data.
- **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. Skylar One uses data from that date as the starting point of the report. **Duration.** Specify the duration for the report, from 1 month to 36 months. Skylar One uses 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 time zone to use for date and time values in the report. Specify the time zone as the number of hours offset from Coordinated Universal Time (UTC).
- **Report Type.** Specify whether the report includes all selected devices or only a set number of the devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the "Video Reports" PowerPack. You or another user might have modified this report on your Skylar One 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 or to limit the number of devices in the report. You can also specify the time span to include in the report, the text at the top of the report, and how the report sorts and arranges the devices.



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 - LAR 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 to display at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" displays at the top of the report.
- **Device Selection.** Select the devices to include in the report. The following options are available:
 - **All devices.** Select this checkbox if you want all devices in the system to be included in this report.
 - **Organizations.** If you do not select the **All devices** checkbox, select one or more organizations. The report contains 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 you do not select the **All devices** checkbox, the **Select individual devices** checkbox is available. Select this checkbox 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 options are available:
 - **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 contains 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 is arranged:
 - **Separated By.** Select whether the report separates the data 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.** Select whether the Device ID or the Organization ID appears 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. Skylar One uses data from that date as the starting point of the report. **Duration.** Specify the duration for the report, from 1 month to 36 months. Skylar One uses 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 time zone to use for date and time values in the report. Specify the time zone as the number of hours offset from Coordinated Universal Time (UTC).
- **Report Type.** Specify whether the report includes all selected devices or only a set number of the devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the "Video Reports" PowerPack. You or another user might have modified this report on your Skylar One system.

Video Endpoint Performance Detail Report

This report displays performance details for Tandberg, LifeSize, Cisco, and Polycom video endpoints. The report displays the organizations, device groups, device names, average receive (RX) audio and video packet loss, average transmit (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 or to limit the number of devices in the report. You can also specify the time span to include in the report, the text at the top of the report, and how the report sorts and arranges the devices.

		
Video Endpoint Performance Detail – Oct 2014 for 6 months		
Organization: Customer A Video		
	Category	Device
	Video.Endpoint	Endpoint - LAB 500 [1068]
	Video.Endpoint	Endpoint - Polycom HDX 7000 [1057]
Generated on: April 17th, 2015 07:45:38 AM		

The following input options are available when generating the report:

- **Branding.** Optionally, enter text to display at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" displays at the top of the report.
- **Device Selection.** Select the devices to include in the report. The following options are available:
 - *All devices.* Select this checkbox if you want all devices in the system to be included in this report.
 - *Organizations.* If you do not select the **All devices** checkbox, select one or more organizations. The report contains 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 you do not select the **All devices** checkbox, the **Select individual devices** checkbox is available. Select this checkbox 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 options are available:
 - *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 contains 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 is arranged:
 - **Separated By.** Select whether the report separates the data 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.** Select whether the Device ID or the Organization ID appears 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 appears in *Ascending* or *Descending* order and select the type of packet loss.

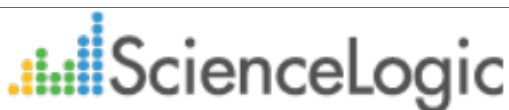
- **Report Span.** Specify a *Daily*, *Weekly*, or *Monthly* span to include in the report. **Starting.** Use the *Year*, *Month*, and *Date* fields to specify a start date for the report. Skylar One uses data from that date as the starting point of the report. **Duration.** Specify the duration for the report, from 1 month to 36 months. Skylar One uses 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 time zone to use for date and time values in the report. Specify the time zone as the number of hours offset from Coordinated Universal Time (UTC).
- **Report Type.** Specify whether the report includes all selected devices or only a set number of the devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the "Video Reports" PowerPack. You or another user might have modified this report on your Skylar One system.

Video Endpoint Unavailability Chart Report

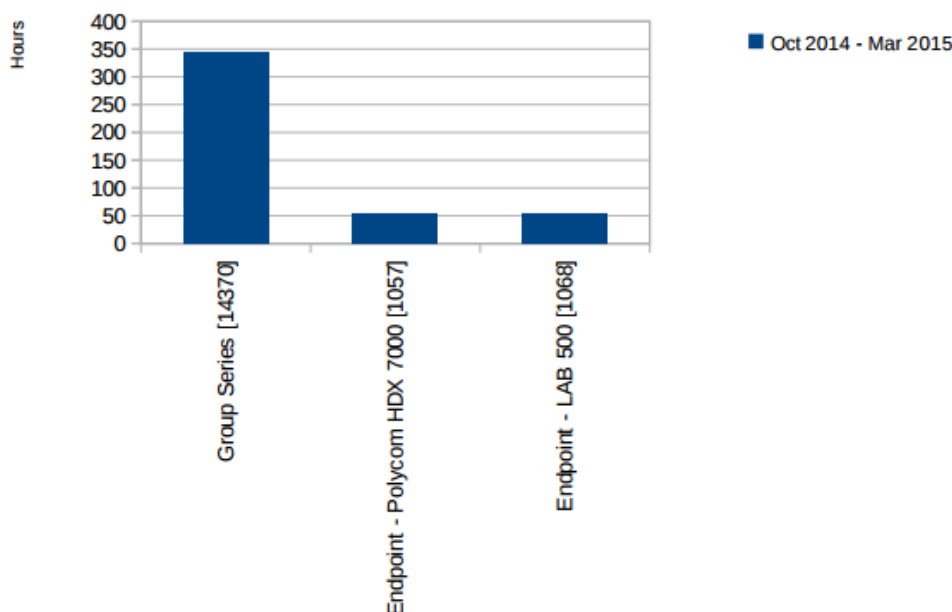
This report displays a bar graph of unavailability for Tandberg, Polycom, LifeSize and Cisco TelePresence devices. For each device included in the report, the report displays the number of hours the device was unavailable during the time period selected for the report.

You can customize the output to include only specific devices or to limit the number of devices in the report. You can also specify the time span to include in the report, the text at the top of the report, and how the report sorts and arranges the devices.



Video Endpoint Unavailability Chart – Oct 2014 for 6 months

Organization: Customer A Video



The following input options are available when generating the report:

- **Branding.** Optionally, enter text to display at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" displays at the top of the report.
- **Device Selection.** Select the devices to include in the report. The following options are available:
 - **All devices.** Select this checkbox if you want all devices in the system to be included in this report.
 - **Organizations.** If you do not select the **All devices** checkbox, select one or more organizations. The report contains 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 you do not select the **All devices** checkbox, the **Select individual devices** checkbox is available. Select this checkbox 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 options are available:
 - *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 contains 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 is arranged:
 - **Separated By.** Select whether the report separates the data 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.** Select whether the Device ID or the Organization ID appears in the report.
 - **Stacking.** Select the **Enable Stacking** checkbox to stack the data.
- **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. Skylar One uses data from that date as the starting point of the report. **Duration.** Specify the duration for the report, from 1 month to 36 months. Skylar One uses 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 time zone to use for date and time values in the report. Specify the time zone as the number of hours offset from Coordinated Universal Time (UTC).
- **Report Type.** Specify whether the report includes all selected devices or only a set number of the devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the "Video Reports" PowerPack. You or another user might have modified this report on your Skylar One 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 or to limit the number of devices in the report. You can also specify the time span to include in the report, the text at the top of the report, and how the report sorts and arranges the devices.

								
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 [1067]								
	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 [1067]		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	452.97
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	156.22
Organization: Enterprise Video								
Device: Endpoint - CTS-600 [1066]								
	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-600 [1066]		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	0.54	31.67	53.51
Sum for Device: Endpoint - LifeSize 200 [1072]		0.27	0.25	20.7	0.08	0.54	31.67	53.51
Sum for Organization: Enterprise Video		72.27	672.25	764.7	744.08	672.54	775.67	3701.51
Overall Totals:		73.07	765.17	873.06	897.61	817.6	872.59	4369.1
Generated on: April 17th, 2015 07:37:25 AM								

The following input options are available when generating the report:

- **Branding.** Optionally, enter text to display at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" displays at the top of the report.

- **Device Selection.** Select the devices to include in the report. The following options are available:
 - *All devices.* Select this checkbox if you want all devices in the system to be included in this report.
 - *Organizations.* If you do not select the **All devices** checkbox, select one or more organizations. The report contains 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 you do not select the **All devices** checkbox, the **Select individual devices** checkbox is available. Select this checkbox 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 options are available:
 - *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 contains 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 is arranged:
 - **Separated By.** Select whether the report separates the data 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.** Select whether the Device ID or the Organization ID appears 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. Skylar One uses data from that date as the starting point of the report. **Duration.** Specify the duration for the report, from 1 month to 36 months. Skylar One uses 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 time zone to use for date and time values in the report. Specify the time zone as the number of hours offset from Coordinated Universal Time (UTC).
- **Report Type.** Specify whether the report includes all selected devices or only a set number of the devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the "Video Reports" PowerPack. You or another user might have modified this report on your Skylar One 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 or to limit the number of devices in the report. You can also specify the time span to include in the report, the text at the top of the report, and how the report sorts and arranges the devices.



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 [1048]	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 - 7000/DCP [1047]	0	0	0	0	
Video Endpoint	Endpoint [6826]	0	142.29	30.53	172.82	
Video Server	server [6825]	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 [1045]	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, 2012 07:44:01 AM

The following input options are available when generating the report:

- **Branding.** Optionally, enter text to display at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" displays at the top of the report.
- **Device Selection.** Select the devices to include in the report. The following options are available:
 - **All devices.** Select this checkbox if you want all devices in the system to be included in this report.
 - **Organizations.** If you do not select the **All devices** checkbox, select one or more organizations. The report contains 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 you do not select the **All devices** checkbox, the **Select individual devices** checkbox is available. Select this checkbox 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 options are available:
 - **Select By Device Group.** Select this checkbox if you want to select which device groups to include in the report.

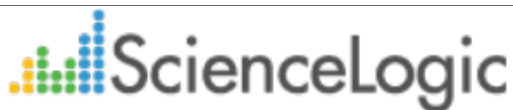
- **Device Groups.** If the *Select By Device Group* checkbox is selected, select one or more device groups. The report contains only the devices in the device groups you select.
- **Device Categories.** Select the device categories that will appear in the report. The following input elements appear 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 you clear the **All Device Categories** checkbox, you can select one or more device categories to include in the report.
- **General Display Options.** Specify how the report is arranged:
 - **Separated By.** Select whether the report separates the data 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.** Select whether the Device ID or the Organization ID appears in the report.
 - **Report Sections.** Select whether you want the report to display *Details Only*, *Totals Only*, or *Both*.
 - **Misc. Options.** Select this checkbox 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. Skylar One uses data from that date as the starting point of the report. **Duration.** Specify the duration for the report, from 1 month to 36 months. Skylar One uses 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 time zone to use for date and time values in the report. Specify the time zone as the number of hours offset from Coordinated Universal Time (UTC).
- **Report Type.** Specify whether the report includes all selected devices or only a set number of the devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the "Video Reports" PowerPack. You or another user might have modified this report on your Skylar One system.

Video Usage Chart Report

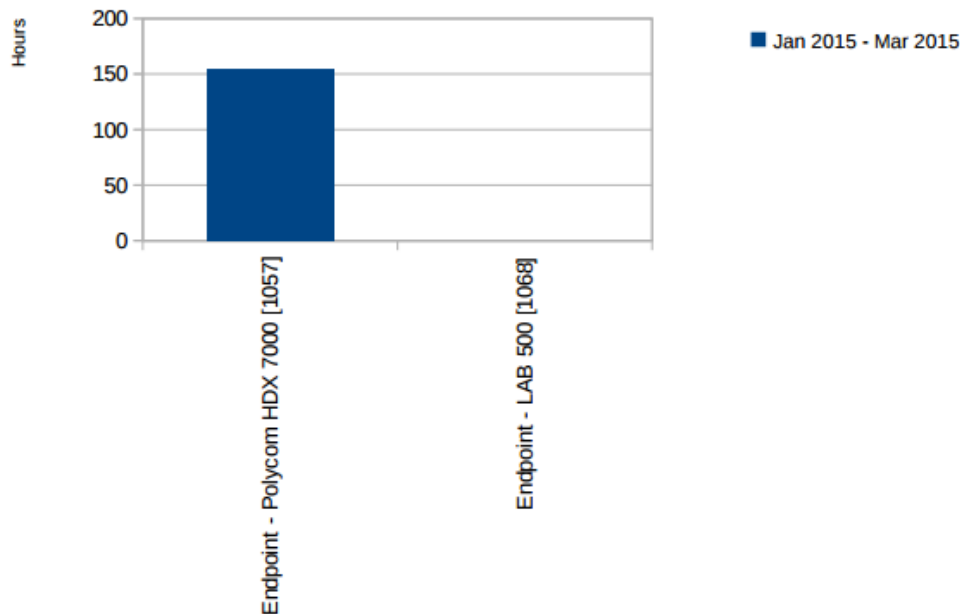
This report displays a bar graph of usage based on call detail records for Tandberg, Polycom, LifeSize and Cisco TelePresence devices. For each device included in the report, the report displays the total number of hours the device was on a call for the time period selected for the report.

You can customize the output to include only specific devices or to limit the number of devices in the report. You can also specify the time span to include in the report, the text at the top of the report, and how the report sorts and arranges the devices.



Video Usage Chart – Jan 2015 for 3 months

Organization: Customer A Video



The following input options are available when generating the report:

- **Branding.** Optionally, enter text to display at the top of the report. If you do not enter a value in this field, "Video Endpoint Report" displays at the top of the report.
- **Device Selection.** Select the devices to include in the report. The following options are available:
 - **All devices.** Select this checkbox if you want all devices in the system to be included in this report.
 - **Organizations.** If you do not select the **All devices** checkbox, select one or more organizations. The report contains 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 you do not select the **All devices** checkbox, the **Select individual devices** checkbox is available. Select this checkbox 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 options are available:
 - *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 contains 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 you clear the **All Device Categories** checkbox, you can select one or more device categories to include in the report.
- **General Display Options.** Specify how the report is arranged:
 - **Separated By.** Select whether the report separates the data 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.** Select whether the Device ID or the Organization ID appears 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. Skylar One uses data from that date as the starting point of the report. **Duration.** Specify the duration for the report, from 1 month to 36 months. Skylar One uses 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 time zone to use for date and time values in the report. Specify the time zone as the number of hours offset from Coordinated Universal Time (UTC).
- **Report Type.** Specify whether the report includes all selected devices or only a set number of the devices with the highest utilization.

This description covers the latest version of this report as shipped by ScienceLogic in the "Video Reports" PowerPack. You or another user might have modified this report on your Skylar One system.

© 2003 - 2026, ScienceLogic, Inc.

All rights reserved.

ScienceLogic™, the ScienceLogic logo, and ScienceLogic's product and service names are trademarks or service marks of ScienceLogic, Inc. and its affiliates. Use of ScienceLogic's trademarks or service marks without permission is prohibited.

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 herein, the information provided in this document 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 herein at any time without notice.



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

International: +1-703-354-1010