Videoscape Control Suite Endpoint Manager Service

User Guide

Please Read

Important

Please read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgments

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: **www.cisco.com/go/trademarks**.

Third party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

Copyright

Contents

About This Guide v

Chapter 1 Before You Begin the Endpoint Manager Configuration 1

Before You Begin 2

Chapter 2 Configure Endpoints Using the Endpoint Manager Service 5

Endpoint Manager Overview 6
Endpoint Overview 7
Endpoint Parameters 16
Endpoint Configurations 17
Endpoint Group Rules 21
Endpoint Groups 23
Endpoint Topics 27
Endpoint Watches 28
Endpoint Settings 29
Endpoint Performance Parameters 33
Endpoint Debug Commands 38
Manage Installed Items 41
Manage Reboot Log Files 43
Manage Endpoint Restore 44
Endpoint Application Images 45
Manage vsCVTs 48
Endpoint Notification Access 51
Endpoint Analytics 53
Endpoint Diagnostics 58
Endpoint Management Settings 60
SNMP Alarms 62
Manage Endpoint Manager Logs 63

Chapter 3 Troubleshooting the Endpoint Manager Service 65

Endpoint Manager Troubleshooting 66

Chapter 4 Troubleshooting EPM Analytics 69

EPM Analytics Troubleshooting 70

Chapter 5 Customer Information 73

Appendix A Endpoint Manager Operational Scenarios 75

Endpoint Manager Overview 76
Typical Endpoint Scenarios 78

About This Guide

Purpose

This document provides user instructions regarding the Endpoint Manager service for the Videoscape Control Suite.

The Endpoint Manager (EPM) service allows for the control and monitoring of various types of application software hosted on hardware components attached to the Videoscape platform. EPM provides a central control point to manage this application software.

Audience

The audience for this document includes system administrators, operators, and installation engineers who deploy Videoscape Conductor systems.

Document Version

This is the fourth formal release of this document. This release was updated for Videoscape Control Suite 3.0.

1

Before You Begin the Endpoint Manager Configuration

Introduction

Before you begin configuring the Endpoint Manager Service, be sure you have met the requirements in this chapter.

In This Chapter

- Before You Begin..... 2

Before You Begin

Software Requirements

- Be certain that you have installed the Videoscape Control Suite software. Refer to *Videoscape Control Suite Installation and Upgrade Guide* (part number OL-29939) for details.
- Be certain that the following components have been installed. Details are available in *Installing COP Files for the Videoscape Control Suite* (part number OL-27753).
  - HornetQ
  - UPMCDA
  - UPM

COP File Installation

Before you can begin configuring the Endpoint Manager Service, the Cisco Options Package (COP) file for that service must already be installed. To install the COP file for the EPM service, follow the instructions in *Installing COP Files for the Videoscape Control Suite* (part number OL-27753).

COP File Requirements

- cisco.conductor-endpointmanager.x.cop.sgn
- cisco.conductor-epmFiler-x.cop.sgn
- cisco.conductor-nosqlcb-x.cop

Note: COP files cannot be downloaded from the desktop.

Template File Requirements

- cisco.conductor-nosqlcb-x.tmp.xml
- cisco.conductor-endpointmanager.x.tmp.xml
- cisco.conductor-epmFiler.x.tmp.xml

Note: The template file can be downloaded from the desktop or through the SSH File Transfer Protocol (SFTP).

Browser Requirements

- Internet Explorer 8
- Internet Explorer 9
- Mozilla Firefox 5

2

Configure Endpoints Using the Endpoint Manager Service

Introduction

The information in this chapter describes how to configure Endpoints using Endpoint Manager.

In This Chapter

- Endpoint Manager Overview 6
- Endpoint Overview 7
- Endpoint Parameters 16
- Endpoint Configurations 17
- Endpoint Group Rules 21
- Endpoint Groups 23
- Endpoint Topics 27
- Endpoint Watches 28
- Endpoint Settings 29
- Endpoint Performance Parameters 33
- Endpoint Debug Commands 38
- Manage Installed Items 41
- Manage Reboot Log Files 43
- Manage Endpoint Restore 44
- Endpoint Application Images 45
- Manage vsCVTs 48
- Endpoint Notification Access 51
- Endpoint Analytics 53
- Endpoint Diagnostics 58
- Endpoint Management Settings 60
- SNMP Alarms 62
- Manage Endpoint Manager Logs 63

Endpoint Manager Overview

The Endpoint Manager (EPM) subsystem allows for the control and monitoring of various types of application software hosted on hardware components attached to the Videoscape platform. The subsystem uses APIs to allow other components of the control suite to manage these application software entities.

The EPM subsystem provides a central control point for all application software that is compatible with the Videoscape platform, and allows for the monitoring of Endpoints and diagnostic output.

Endpoint Overview

The Endpoint Manager provides end-point management for VSR5 devices and Softclient provisioning, event collection and reporting, diagnostics, and firmware/configuration services as specified further in the Control Suite PRD [EDCS-1004068]. It does so by supporting the following major functions:

- **Endpoint Inventory —** Provides a database of managed devices, along with metadata about those Endpoints, and allows the administrator to add, remove, and browse Endpoints.
- **Endpoint Configuration —** Provides a way to manage configuration files for Endpoints.
- **Device Software Management —** Allows Endpoint software to be published to a web server/CDN, as well as for messaging triggers to be sent to groups of devices to trigger upgrades.
- **Device Monitoring —** Allows device data models to be queried, data sets to be built, and for the pass-through of monitoring data to northbound management systems.
- **Reboot/Debug Log Management —** Allows for the storage of Endpoint Reboot and Debug logs.

Videoscape Control Suite

The Videoscape Control Suite supports three different types of devices:

- **Managed devices —** Managed devices are physical devices under the control of the Videoscape architecture and hence are managed by the Endpoint Manager. A fully managed device includes factory-installed information such as device credentials (in the form of a certificate). A typical managed device is an IP set-top box.
- **Partially managed devices —** Partially managed devices contain software installed and/or controlled by the overall Videoscape architecture. However, the hardware device itself is not under the control of Videoscape. Examples include Apple iOS and Android devices, where Videoscape provides an application to install and run on the device. The install process may require certain information to be installed on the device and the device identifying itself to the Videoscape Control Suite (for example, by having a device identity created).
- **Unmanaged devices —** Unmanaged devices are all other devices that need to access the Videoscape Control Suite. Note that unmanaged devices do not install applications controlled by Videoscape. An example is a PC/Mac web browser. Unmanaged devices allow the Videoscape system to model the content consumption endpoint.

Consumption Endpoint

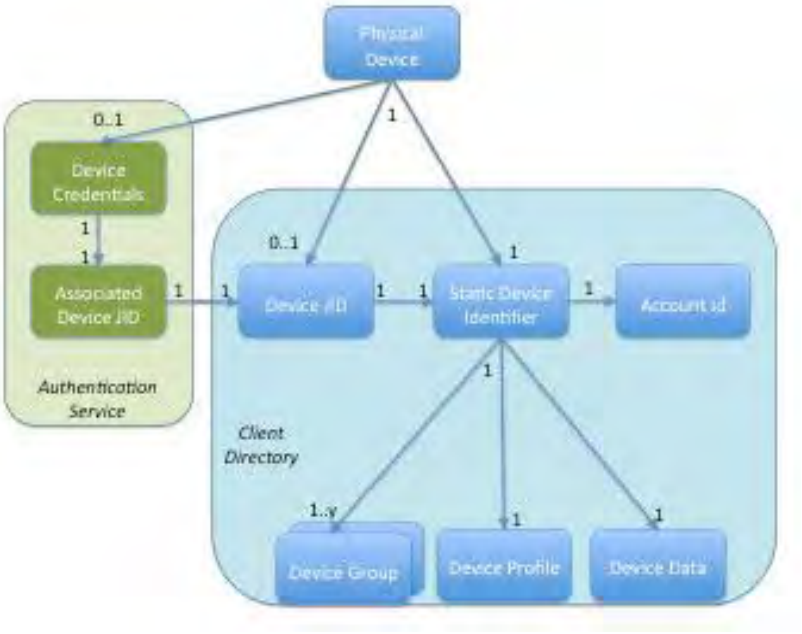
Device Type	Static Device ID	Dynamic Device ID	Device Jabber ID
Managed	Yes	No	Yes
Partially Managed	Yes	No	No
Unmanaged	No	Yes	No

Device Identifiers

Device identifiers are defined as follows:

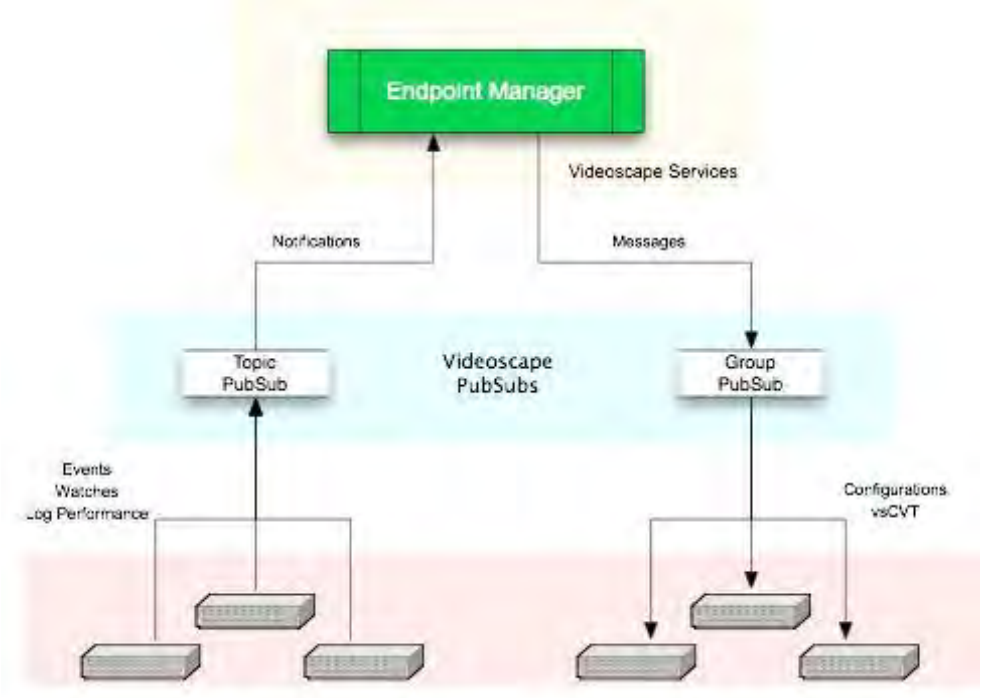
- **Static Device ID —** Static device IDs are globally unique and long-lived identifiers that uniquely identify a managed or a partially managed device. The static device ID will be stored in the Videoscape Control Suite Client Directory and associated with an account. Static device IDs uniquely identify a physical Videoscape Control Suite device. However, they do not provide an addressable identifier for the Videoscape Control Suite by themselves (device JIDs are used for this). Static device IDs may be authenticated (such as, for managed devices). In any case, static device IDs may be used as identifiers for resource binding when a given user is associated with a device.
- **Dynamic Device ID —** Dynamic device IDs are globally unique identifiers that uniquely identify an unmanaged device instantiation, such as a virtual device. Dynamic device IDs are not long-lived; they may change after a reboot, or even between sessions, and hence they are not provisioned in the system. Otherwise, dynamic device IDs support the same properties as static device IDs (except they are never authenticated), and hence they can be used for resource binding and to store device capabilities for the duration of the virtual device lifetime.
- **Device JID —** Device Jabber Identifiers (device JIDs) are globally unique and long-lived Jabber Identifiers that uniquely name a managed device. Device JIDs are authenticated and they provide an addressable identifier for the Videoscape Control Suite to use. Device JIDs are associated with exactly one (static) device identifier, and hence only devices with static device ids (and hence physical devices) can have device JIDs. From an XMPP point of view, the device JID performs resource binding with the (static) device identifier.

These concepts are illustrated in the following diagram:



Pubsub Information

A PubSub is defined as an area where messages or notifications are sent from multiple entities to one receiver.

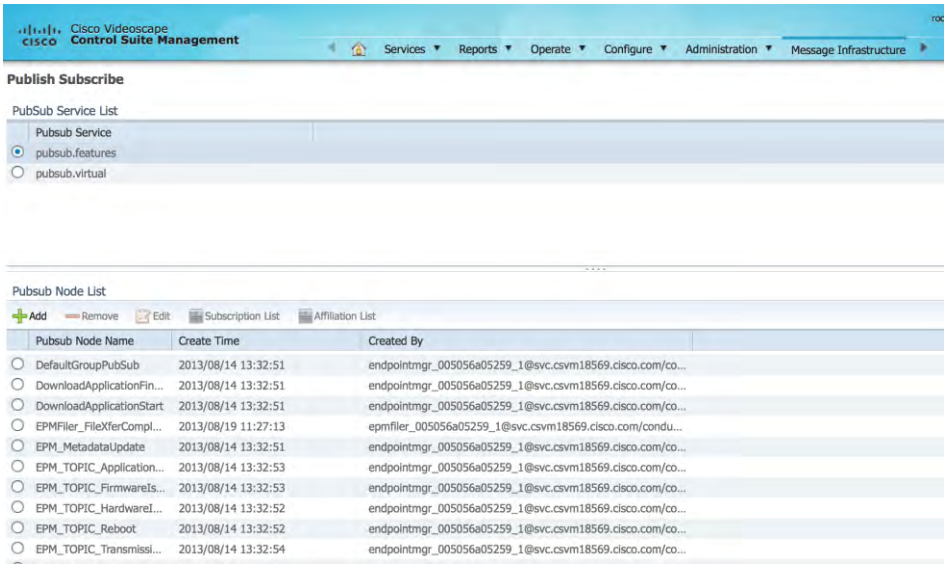


Upon the installation of Endpoint Manager, the following ten PubSubs are created:

- DefaultGroupPubSub
- DownloadApplicationFinish
- DownloadApplicationStart
- EndpointProvison
- EPM_MetadataUpdate
- EPM_TOPIC_ApplicationIssue
- EPM_TOPIC_FirmwareIssue
- EPM_TOPIC_HardwareIssue
- EPM_TOPIC_Reboot
- EPM_TOPIC_TransmissionIssue

Before proceeding, verify that these PubSubs are present.

1. Log into the Videoscape Control Suite management console UI.
2. Click **Message Infrastructure**.
3. Click **Publish Subscribe**.
4. Choose the PubSub node that you defined when you installed EPM.
   Example: pubsub.features
5. Verify that the PubSubs are present.



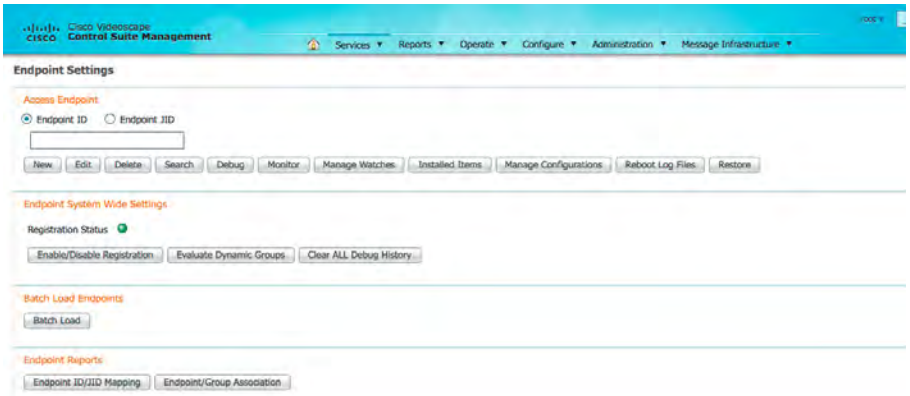
Notes:

- Refer to ***Troubleshooting the Endpoint Manager Service*** (on page 65) if the PubSubs are not displayed.
- PubSubs are also created when Endpoint Topics and Endpoint Groups are created.

Registration Status

The Endpoint Manager provides the capability to allow or prevent the registration of new Endpoints, using the **Endpoint Activation Flag** setting.

1. Choose **Services > Endpoint Management**.
2. Click **Endpoint Settings**.



3. In the **Endpoint System Wide Settings** section, check the color of the **Registration Status**. If the status displays green, Endpoints can register. If the status displays red, Endpoints can no longer register.
4. Click **Enable/Disable Registration** to enable or disable registration.
5. Note that the **Access Endpoint** fields allow the user to perform the following tasks:
   - Create a new Endpoint
   - Edit an existing Endpoint
   - Delete an Endpoint
   - Search for an Endpoint
   - Retrieve/Send Debug commands to an Endpoint
   - Set/Monitor performance parameters on an Endpoint
   - Set/Retrieve Watches on an Endpoint
   - View/Delete Installed Items on an Endpoint
   - Send/Cancel Configuration of an Endpoint
   - Retrieve/View Reboot Log Files
   - Restore an Endpoint
6. Click **Clear All Debug History** to clear all debug records received for all Endpoints.
7. Click **Batch Load** to allow for a batch load from a file of multiple Endpoints.

8 Click **Endpoint ID/JID Mapping** to create a report which shows Endpoints and their associated JIDs.

9 Click **Endpoint/Group Association** to create a report that displays the Endpoints and the groups to which they are assigned.

Note: See the collection of notes that follow for additional information on steps 6 through 9.

Batch Load

This option allows for multiple Endpoints located in a file to be uploaded to the system.

1 Navigate to **Services** > **Endpoints**.

2 Select **Batch Load**.

3 Browse to choose the file.

4 Click **Upload**.

5 At the Security Warning message, click **Continue**.

Notes:

- The batch load file report is located at /common/log/taos-log-a/EPM_Reports.
- To view the report, enter a CLI command similar to the following:
  `file dump activelog EPM_Reports/batchload.10072013-15:50:40.839.rpt.gz`

Endpoint ID/JID Mapping

1 Navigate to **Services** > **Endpoint Settings**.

2 In the Endpoint Reports section, click **Endpoint ID/JID Mapping**.

Result: The EPM generates the report and indicates the name of the file and its location in the /common/log/taos-log-a/EPM_Reports directory.

3 To view the report, enter a CLI command similar to the following:
`file dump activelog EPM_Reports/endpointidtojid.10072013-15:59:40.rpt.gz`

Endpoint Group Association

The EPM allows for the reporting of all Endpoints and the groups to which they are assigned.

1 Navigate to **Services** > **Endpoint Settings**.

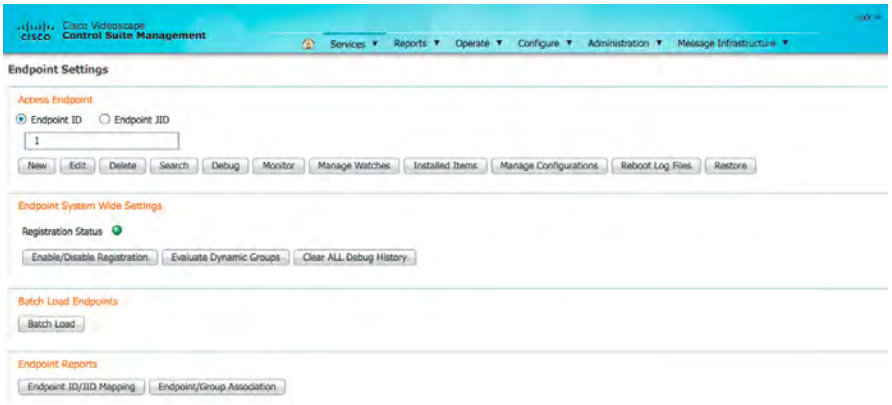
2 In the Endpoint Reports section, click **Endpoint/Group Association**.

Result: The EPM generates a report for all Endpoints and the groups to which they are associated, and indicates the file name and location in /common/log/taos-log-a/EPM_Reports where the file can be found.

3 To view the report, enter a CLI command similar to the following:
`file dump activelog EPM_Reports/endpointgroupassociations.10072013-16:00:00.rpt.gz`

Creating an Endpoint

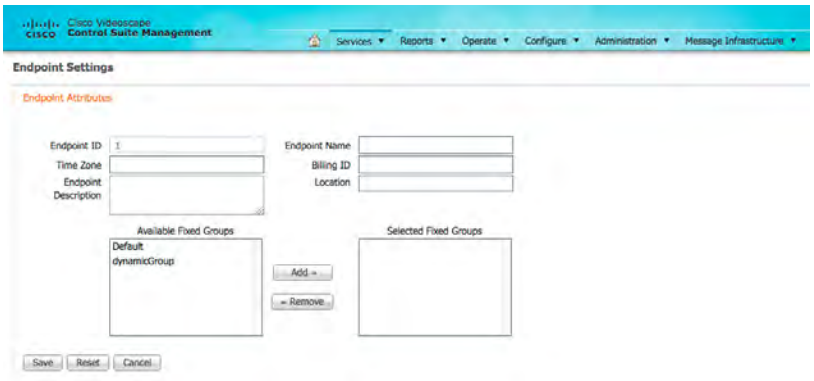
1. Click **Services**.
2. Under the **Endpoint Management** heading, click **Endpoint Settings**.



3. Type a unique number for the **Endpoint ID** and then click **New**.

   Note: The Endpoint ID is a string with a minimum size of 1 and a maximum size of 128 items.

4. Enter the **Time Zone**, **Location**, **Endpoint Name**, **Billing ID**, and choose a **Group** for the Endpoint. These are all required fields for the creation of an Endpoint. Then, **Save** the information.

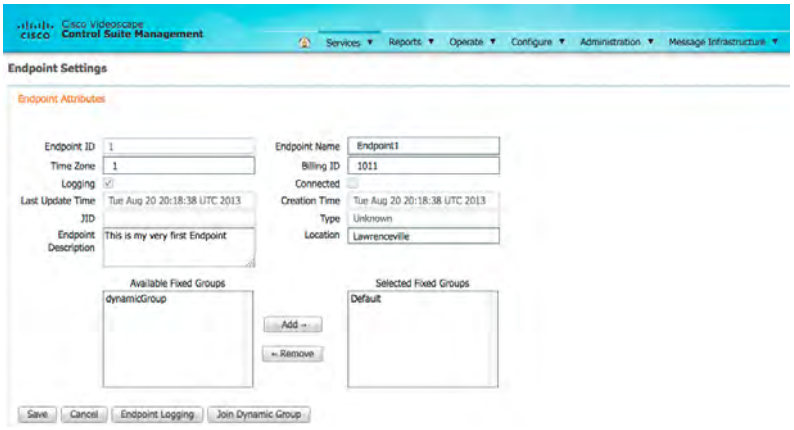


Notes:

- The Default group is automatically created when Endpoint Manager is installed. If the Default group is not present, see ***Troubleshooting the Endpoint Manager Service*** (on page 65).
- Use these guidelines when creating the Endpoint:
  - **Endpoint Name** — String, length from 3 to 256 characters
  - **Time Zone** — Range from 12 to -12
  - **Billing ID** — Integer, range from 1 to 2,147,483,647. The Billing ID is received from the billing vendor.
  - **Location** — Geographic location
  - **Endpoint Description** — String, maximum of 256 characters

Editing the Endpoint

1. Choose **Services > Endpoint Management**.
2. Click **Endpoint Settings**.
3. Type the **Endpoint ID** and click **Edit**. The Endpoint Attributes window opens. You can edit the fields that are not dimmed
4. Click **Endpoint Logging** (located at the bottom of the Endpoint Attributes window) to either activate or deactivate logging on the Endpoint.



Notes:

- The Endpoint will be assigned to the Default Group if no other group is selected.
- If the **Logging** field has a check-mark next to it, logging is activated. If the field is unchecked, logging is deactivated. Logging allows Endpoints to send logs to the EPM. An Endpoint can still send logs to the EPM if logging is deactivated. However, in such a case, the EPM will not store these logs in the database.
- Click **Join Dynamic Group** to allow the Endpoint to join a specific Dynamic Group based on the rules of the group and the Endpoint settings. If the Endpoint settings match those of a rule, and if the rules are assigned to a Dynamic Group, the Endpoint becomes a member of that group when you click **Join Dynamic Group**.
- The Connected field will be selected once the Endpoint has "attached" or signed on to Endpoint Manager.

5. Click **Save**.

Deleting an Endpoint

1. Choose **Services > Endpoint Management > Endpoint Settings**.
2. Enter the Endpoint ID and then click **Delete**.

Search for an Endpoint by Endpoint ID or Endpoint JID

Users can search for Endpoints that match an input string. When complete, the search returns a set of matching Endpoint values, either the Endpoint ID or the Endpoint JID.

The search string may be a partial match and/or include a single wild card character (*). For example, a JID search string could be **`username1*ipad@cisco.com`**.

1. Choose **Services > Endpoint Management > Endpoint Settings**.
2. Enter the **Endpoint ID** or **Endpoint JID** and then click **Search**.

   Notes:

   - Searches can be performed using the complete Endpoint ID or JID, as well as using wildcard characters, such as *.
   - There is a limit of 1,000 records that a search result can return. If a search contains more than 1,000 records, the following error message appears:

     Error searching for endpoint by ID key. mex result set exceeded (1000+ matches found), aborting search

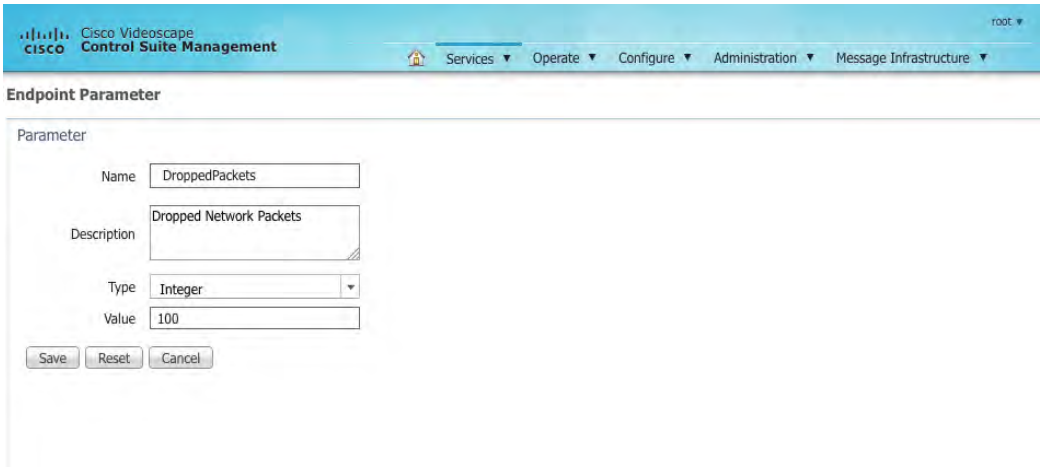
Endpoint Parameters

A Parameter is defined as a value in an Endpoint that needs to be monitored or configured. An example of a value that should be monitored is the amount of RAM in use. Currently, the process for assigning a Parameter to an internal value on an Endpoint is based upon the software resident in the Endpoint.

The GUI allows for the creation, deletion, editing, or viewing of an Endpoint Parameter. Parameters are building blocks for either Configurations, Watches, or Log Performance operations.

Creating an Endpoint Parameter

1. Choose **Services > Endpoint Management > Parameters**.
2. Click **Create**.
3. Type the **Name**, **Description**, **Type**, and **Value**, for the Parameter you are creating.
4. Click **Save**.



Notes:

- The Endpoint Manager can contain a maximum of 10,000 parameters.
- **Name** — Unique; string, from 3 to 256 characters
- **Description** — String, maximum of 256 characters
- **Type** — Drop-down menu; integer or string
- **Value** — Integer or string

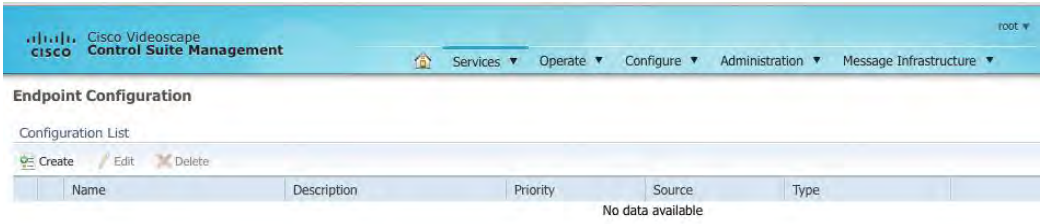
  Example: `http:\\10.90.70.5\guide\atlanta`

Endpoint Configurations

A Configuration is composed of one to many parameters. A Configuration can be used to configure a single Endpoint or a group of Endpoints. In addition, the UI provides the capability to publish a Configuration to the PubSub associated with a Group.

Creating an Endpoint Configuration

1 Choose **Services > Endpoint Management > Configuration**. The Endpoint Configuration list appears.

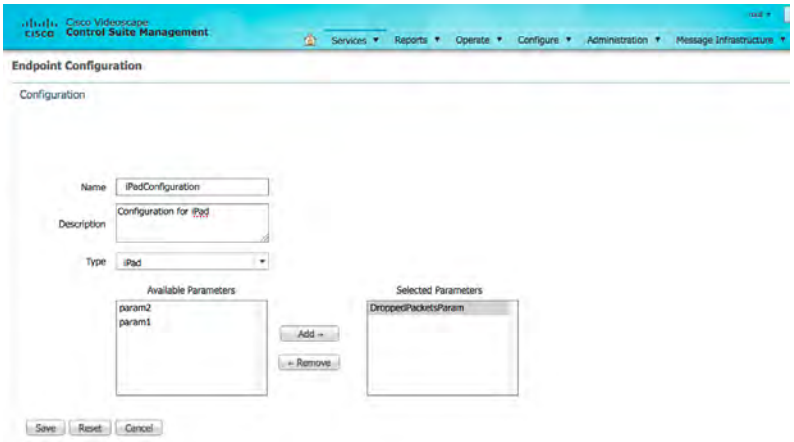


2 Click **Create**.

3 Type the **Name**, **Description**, and **Type** of the Configuration to be created.

4 Select a Parameter from the **Available Parameters** list.

5 Click **Save**.



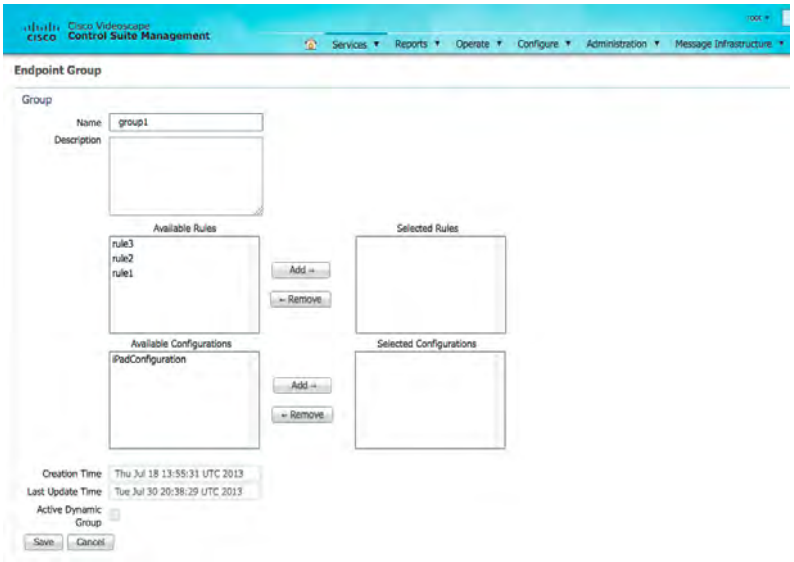
Notes:

- **Name** — String, from 3 to 256 characters; a unique string within the context of the Configuration
- **Description** — String, maximum of 256 characters
- **Type** — Drop-down menu; **iPad**, **iPad2**, **iPhone**, **FireFox**, **IE**, **Safari**, **Unknown**
- The maximum number of Parameters per Configuration is 100.
- The Endpoint Manager service contains a maximum of 1,000 Configurations.

Publishing a Configuration to a Group

In order to publish a configuration to a group, the configuration first needs to be associated to the group.

1. From the **Services** menu, navigate to the **Endpoint Management** section and click **Groups**.
2. Choose the desired group from the **Groups** list and click **Edit**.
3. From the **Configuration** drop-down list, choose the desired configuration; then, click **Save**.



4. From the Endpoint Group list, choose the group that has been associated with the Configuration; then, click **Publish Configuration**.

   Results:

   - The EPM displays a message stating that the publish configuration action was successful.
   - All Configurations associated with the Group are published.

   Note: All Endpoints that are members of the group receive the Configuration.

Canceling Configurations from a Group

1. From the **Services** menu, navigate to the Endpoint Management section and choose **Groups**.
2. Choose the desired group from which to cancel the Configuration or Configurations.
3. Click **Cancel Configuration**.

   Result: All Configurations published to the group are canceled.

Note: To further disassociate the configuration from the group, complete the following steps:

1. Select the **Group** and click **Edit**.
2. From the **Selected Configurations** list, choose the configuration to be removed and click **Remove**.

Sending a Configuration Directly to an Endpoint

A Configuration can be sent directly to an Endpoint.

1. From the **Services** menu, navigate to **Endpoint Management**; then, choose **Endpoint Settings**.
2. From the Endpoint Settings window, enter the desired **Endpoint ID** or **JID**; then, click **Manage Configurations**.
3. From the Endpoint Settings window, navigate to the **Available Configurations** list and choose the desired **Configuration** to send to the Endpoint.
4. Click **Send**. The EPM sends the Configuration directly to the Endpoint.

   Note: Only the last Configuration sent directly to an Endpoint is stored by the Endpoint.

Canceling a Configuration from an Endpoint

1. From the **Services** menu, navigate to **Endpoint Management**, and then choose **Endpoint Settings**.
2. In the Endpoint Settings window, enter the **Endpoint ID** or **JID** and then click **Manage Configurations**.
3. Navigate to the **Configuration List** on the Endpoint at the top of the page, and choose **Remove Configuration**.

   Result: The Configuration is removed from the Endpoint.

Editing a Configuration

1. From the **Services** menu, navigate to **Endpoint Management** and then choose **Configurations**.
2. Choose the configuration to edit and click **Edit**.
3. Make the necessary changes and click **Save**.

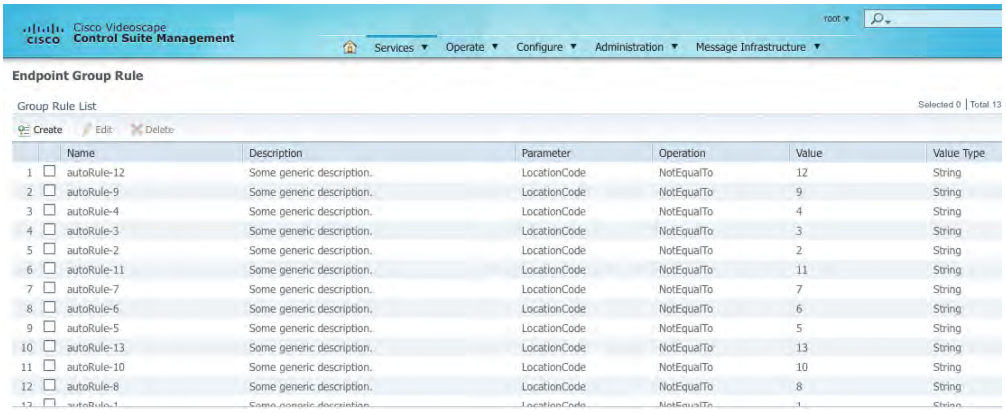
Note: A configuration cannot be edited if it has been published to a group or sent directly to an Endpoint. The configuration has to first be canceled from the group or Endpoint before it can be edited.

Endpoint Group Rules

An Endpoint Group Rule is an expression that is composed of a parameter, an operation, and a value. The expression evaluates to either true or false.

Creating Endpoint Group Rules

1. Choose **Service > Endpoint Management > Group Rules**. The Endpoint Group Rule window opens.



2. Click **Create**.
3. Configure the Endpoint Group Rule.

Notes:

- Click **Reset** to reset all values that have been entered.
- Click **Cancel** to cancel any changes that you have made and to exit the window.
- **Name —** String, from 3 to 256 characters
- **Description —** String, maximum of 256 characters
- **Parameter —** Drop-down menu: **TypeID**, **JID**, **Time Zone**, **Location Code**, **Billing ID**
- **Operation —** Drop-down menu: **Equal To**, **Not Equal To**, **Starts With**, **Contains**
- **Value —** Drop-down menu: **Integer**, **String**
- **Value Type —** Drop-down menu: **Integer**, **String**

4 Click **Save**.

Endpoint Groups

Groups allow for the division of the entire population of Endpoints into sets. This provides the capability to apply configurations to geographic areas, Endpoint types, or specially defined test groups, such as *friendlies*. Associated with each Group is a PubSub node, named by adding the Group ID to "EPM_Group."

Notes:

- Groups can be either Fixed or Dynamic.
- A Fixed Group is a group without rules.
- A Dynamic Group includes at least one rule. That group must also be activated.
- The maximum number of groups that the Endpoint Manager is required to store is 200.
- The GroupName is a unique string within the context of the Group definitions.

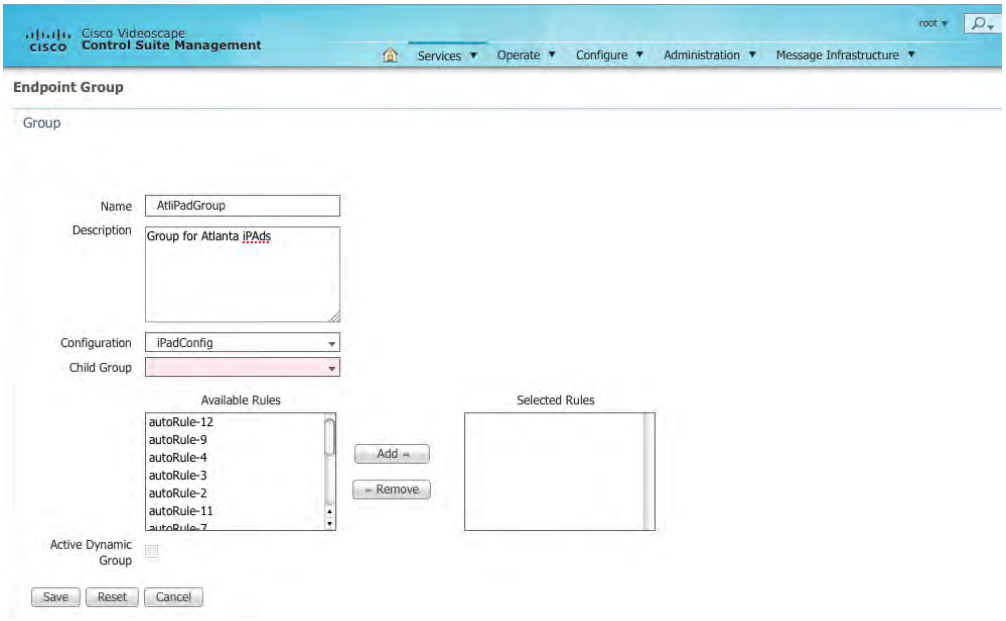
Creating a Fixed Endpoint Group

1 Choose **Services > Endpoint Management > Groups**. The Endpoint Group window opens.

2 Click **Create**.

3 Enter or select the **Name**, **Description**, and **Configuration**.

4 Click **Save**.

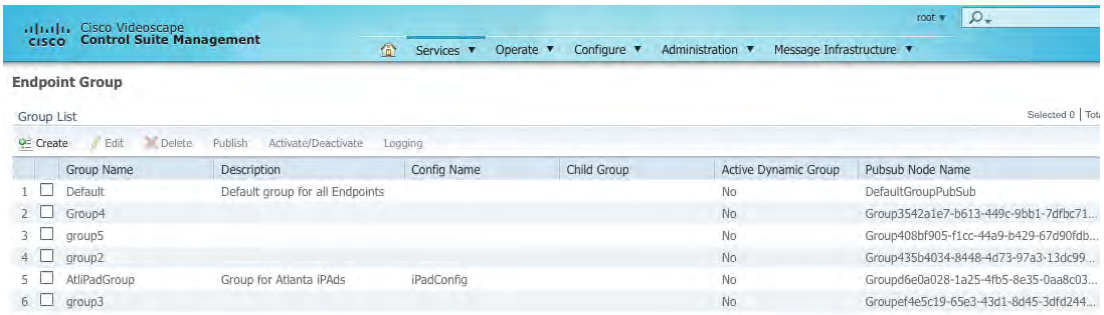


Notes:

- **Name** — String, from 3 to 256 characters
- **Description** — String, maximum of 256 characters

Creating a Dynamic Endpoint Group

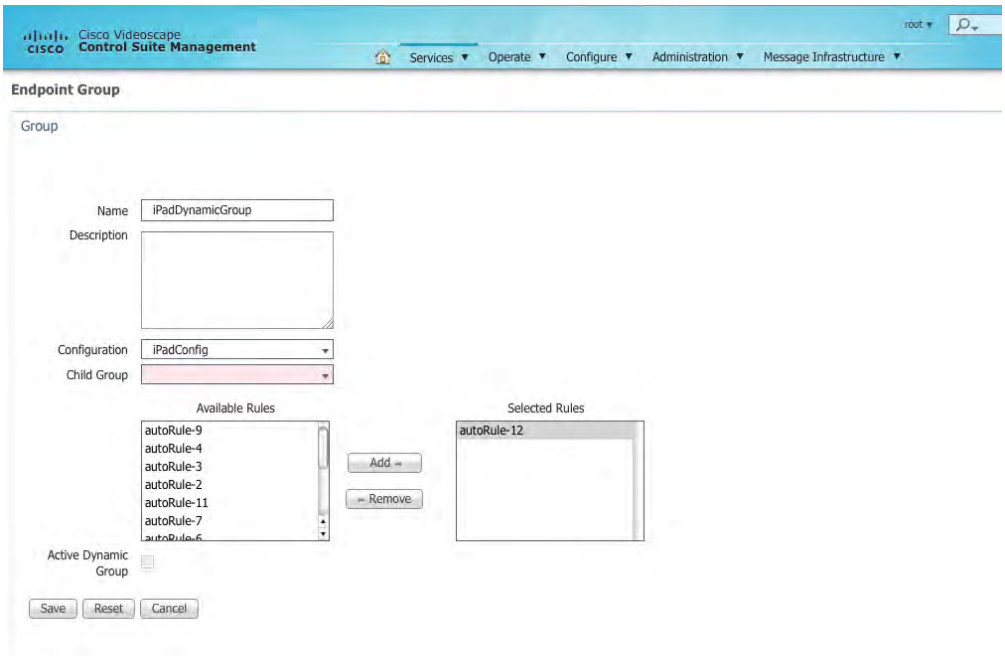
1 Choose **Services > Endpoint Management > Groups**. The Endpoint Group window opens.



2 Click **Create**.

3 Enter or select the **Name**, **Description**, and **Configuration**.

4 Select at least one rule from the **Available Rules** list.



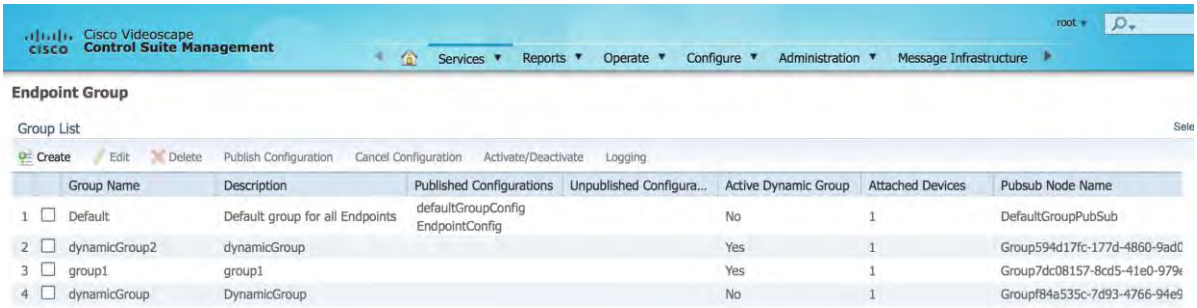
Notes:

- **Name** — String, from 3 to 256 characters
- **Description** — String, maximum of 256 characters

5 Click **Save**. The group is added to the Group List.

6 Choose the group from the Group List and click **Activate/Deactivate**. The system activates the group and displays **Yes** in the Active Dynamic Group column.

Note: To deactivate a group, click **Activate/Deactivate**. The system deactivates the group and displays **No** in the Active Dynamic Group column.



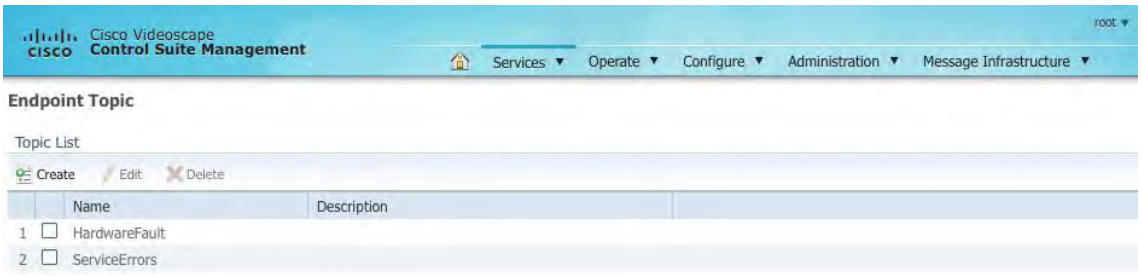
Endpoint Topics

A Topic is an area where an Endpoint sends data. Each Topic has a corresponding PubSub node to which Events, Watches, or Notifications on Endpoints can publish. The associated data is then handled by other components of the EPM Videoscape system.

Note: A Topic is needed to create a Watch.

Creating an Endpoint Topic

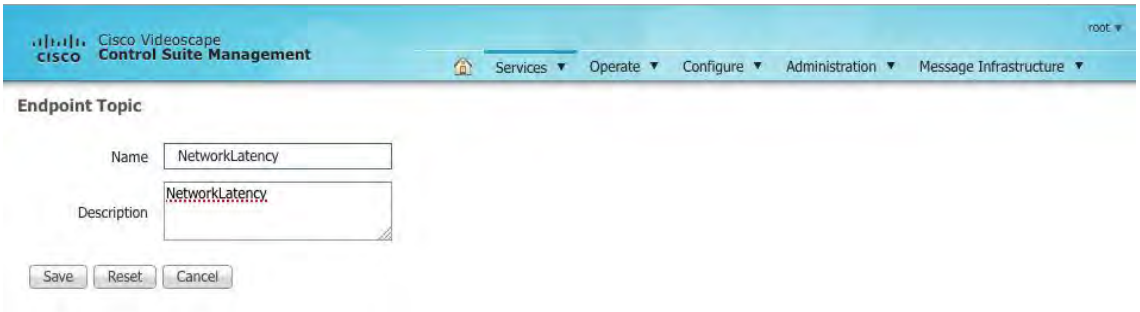
1 Choose **Services > Endpoint Management > Topic**. The Endpoint Topic window opens.



2 Click **Create**.

3 Enter the Topic **Name** and **Description**.

4 Click **Save**.



Notes:

- **Name** — String, from 3 to 256 characters
- **Description** — String, maximum of 256 characters

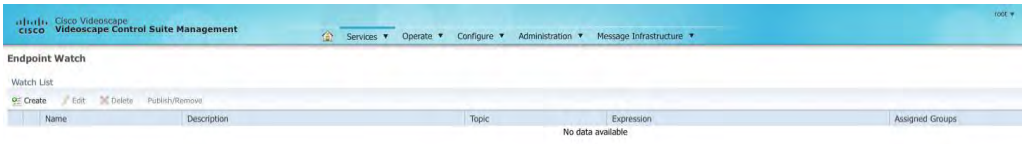
Endpoint Watches

A Watch is a trigger that occurs when one or more conditions have been met. When a trigger occurs, the Endpoint publishes the data that matched the conditions to the specified PubSub. A condition is composed of a Parameter, an operation, and a value. Conditions may be concatenated using logical operators.

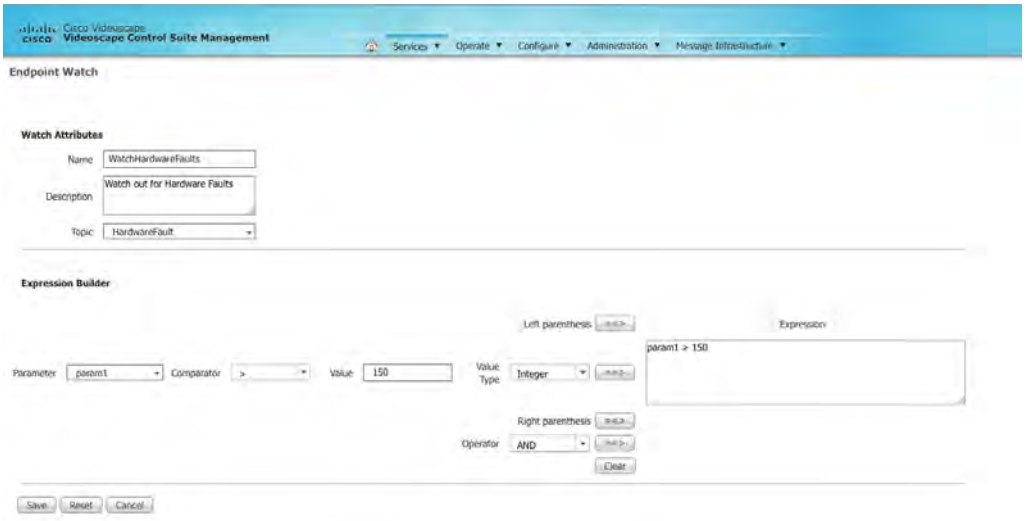
Example: `If Number of Movies = 5 and Maximum Movie Rental = 5`

Creating an Endpoint Watch

1. Choose **Services > Endpoint Management > Watch**. The Endpoint Watch window opens.



2. Click **Create**.
3. Type the Watch **Name** and **Description**. Then, select the **Topic** to which the Watch is tied.
4. Build the watch expression in **Expression Builder.**
5. Click **Save**.



Notes:

- **Name** — String, from 3 to 256 characters
- **Description** — String, maximum of 256 characters

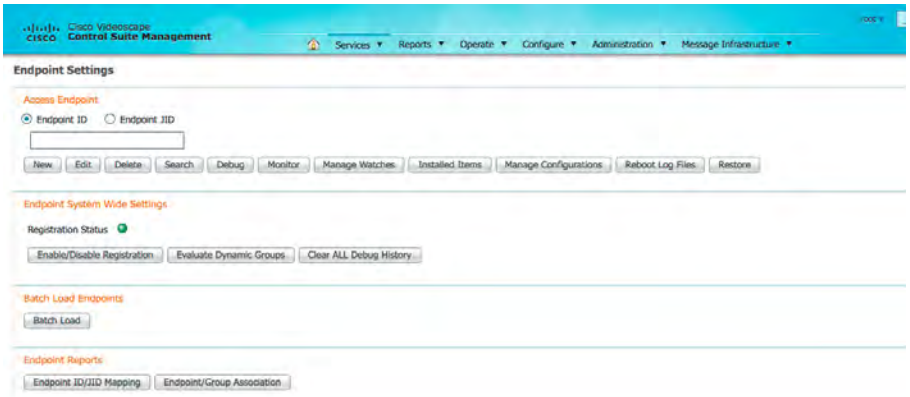
Endpoint Settings

Deploying Watches to Endpoints

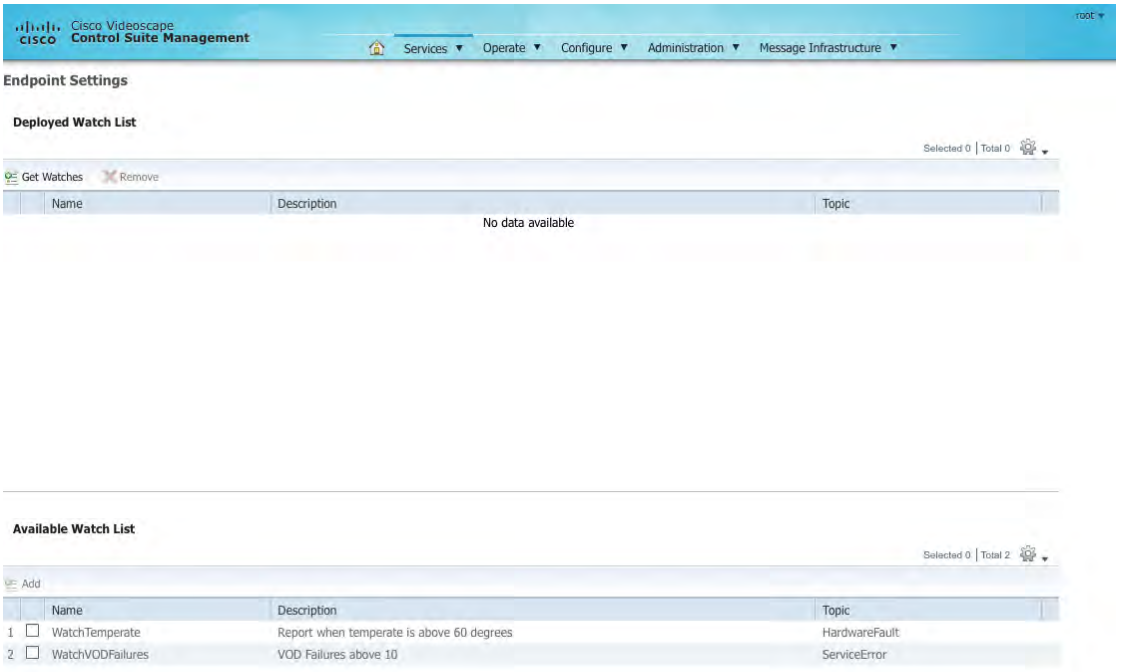
Notes:

- Watches can be deployed through the Access Endpoint window or through the Endpoint Attribute window.
- An Endpoint Watch needs to have been previously created. See ***Creating an Endpoint Watch*** (on page 28).

1 Choose **Services > Endpoint Management > Endpoint Settings**. The Endpoint Settings window opens.



2 Type an **Endpoint ID** and then click **Manage Watches**. The Deployed and Available Watch List window opens.



3 In the **Available Watch List** portion of the window, choose a Watch to deploy to an Endpoint.

4 Click **Add**. The Watch is added to the Endpoint and is now visible on the Deployed Watch List.

Retrieving all Watches from an Endpoint

To retrieve all Watches from an Endpoint, from the Deployed Watch List, click **Get Watches**. All the Watches deployed to an Endpoint are displayed.

Removing a Watch from an Endpoint

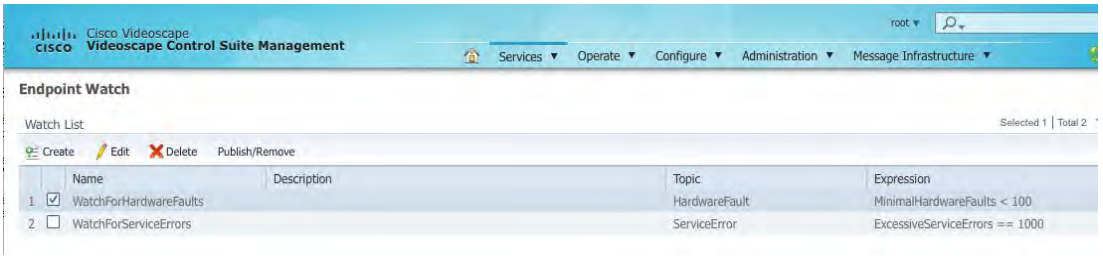
To remove a Watch from an Endpoint, from the Deployed Watch List, click **Remove**. The Watch is removed from the Endpoint and is no longer visible in the Deployed Watch List.

Deploying a Watch to a Group

EPM permits the transmission of Watches to all Endpoints assigned to a Group.

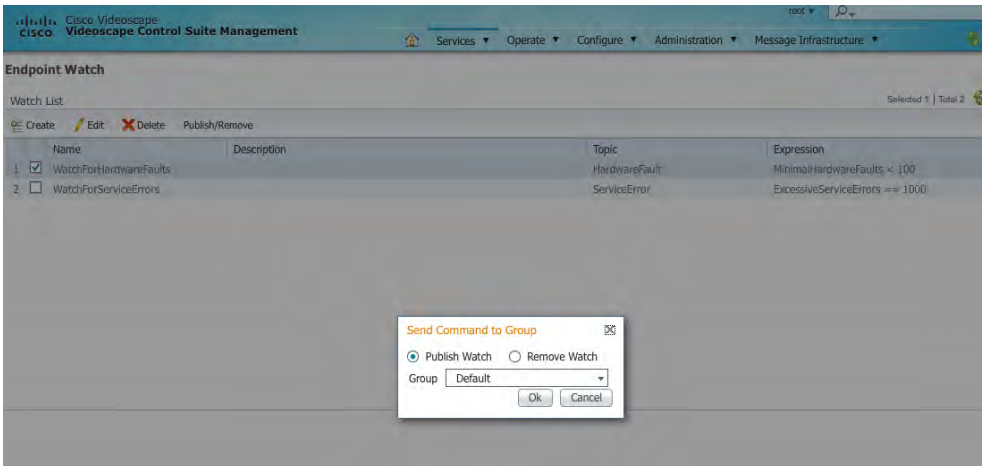
1 Choose **Services > Endpoint Management > Watches**.

2 Choose a Watch from the Watch List window.



3 Click **Publish/Remove**.

4 Click **Publish Watch**, choose the **Group** to which the Watch is to be published, and click **OK**.



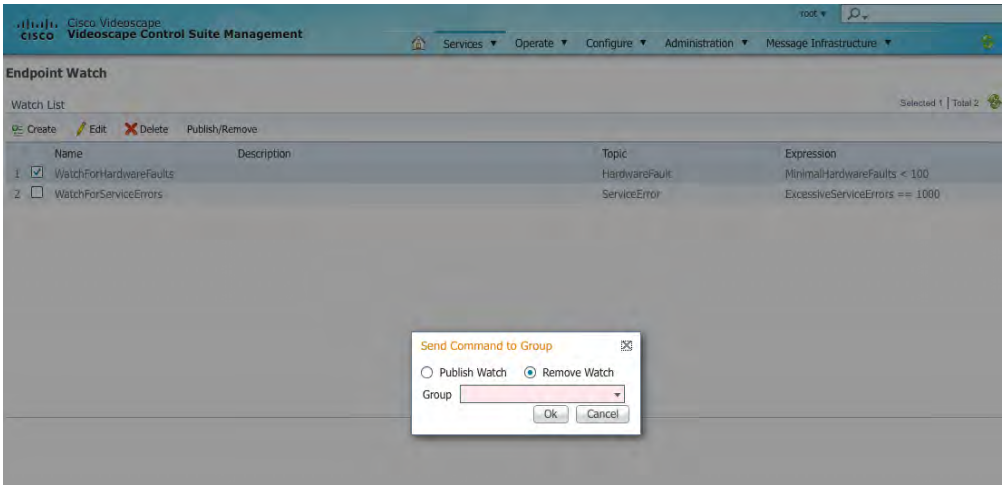
Note: When the Watch is successfully deployed, the system displays a message that indicates a successful deployment.

Removing a Watch from a Group

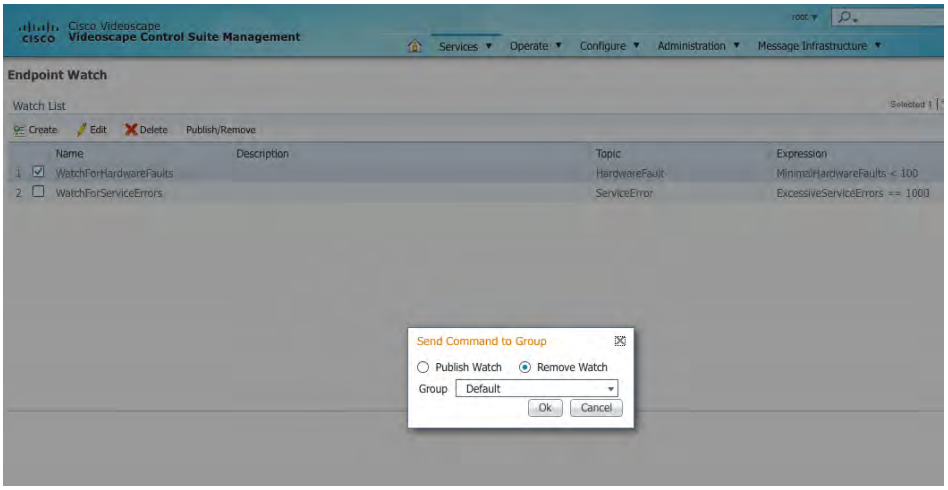
1 Choose **Services > Endpoint Management > Watches**.

2 Choose a Watch from the Watch List window.

3 Click **Publish/Remove**.



4 Click **Remove Watch**, choose the **Group**, and click **OK**.



Note: When the Watch is successfully removed, the system displays a message that indicates the successful removal.

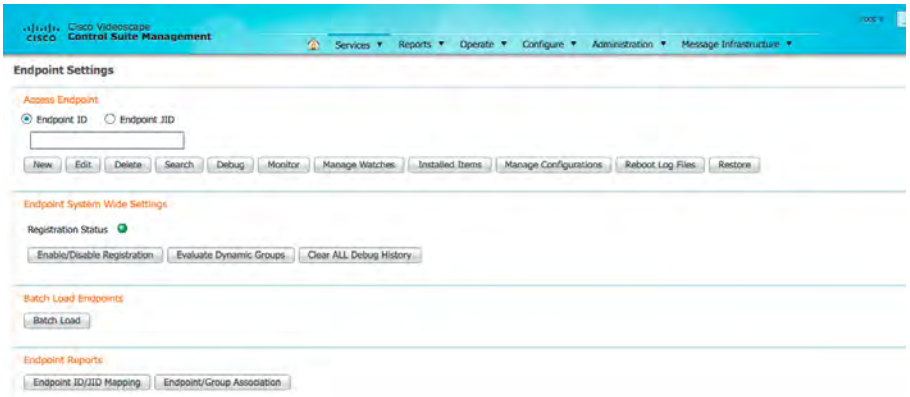
Endpoint Performance Parameters

Information on the state of an Endpoint is available using the Performance Parameter function. EPM specifies what Parameter the Endpoint should monitor and how often. Then, the Endpoint performs the actions to monitor the status and returns the information to the associated Topic PubSub.

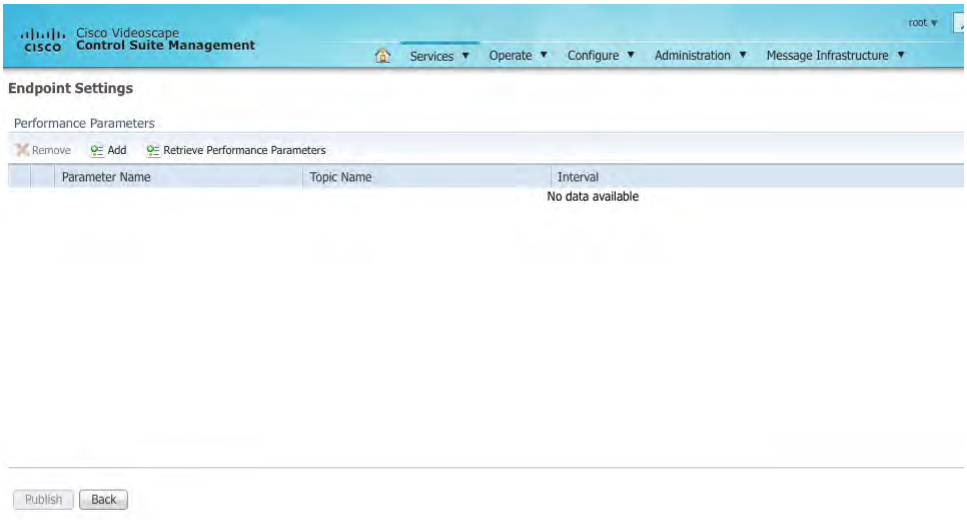
Note: To deploy a Performance Parameter to an Endpoint, a Parameter and Topic must be previously set up. See ***Creating an Endpoint Topic*** (on page 27).

Deploying a Performance Parameter to an Endpoint

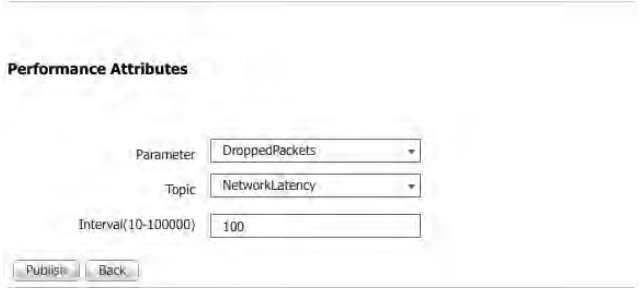
1 Choose **Services > Endpoint Management > Endpoint Settings**. The Endpoint Settings window opens.



2 Type an **Endpoint ID** and click **Monitor**. The Performance Parameter window opens.



3 Click **Add**. The Performance Attributes window opens.

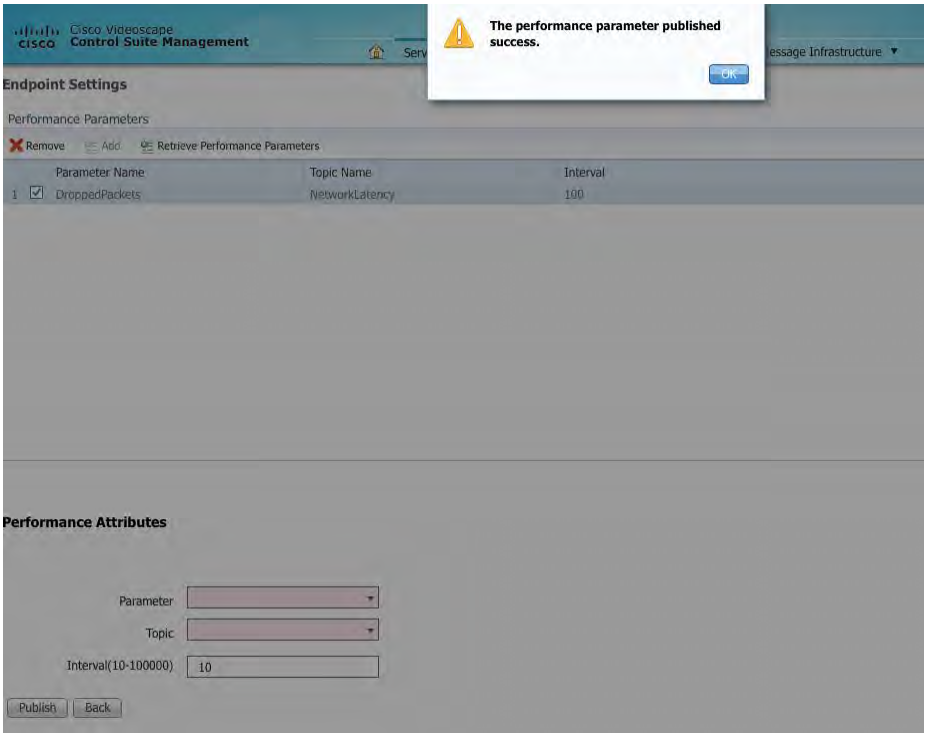


Note: The **Interval** is measured in seconds.

4 Click to select the **Parameter** and **Topic** for the Performance Parameter.

5 Type the **Interval** for the Performance Parameter.

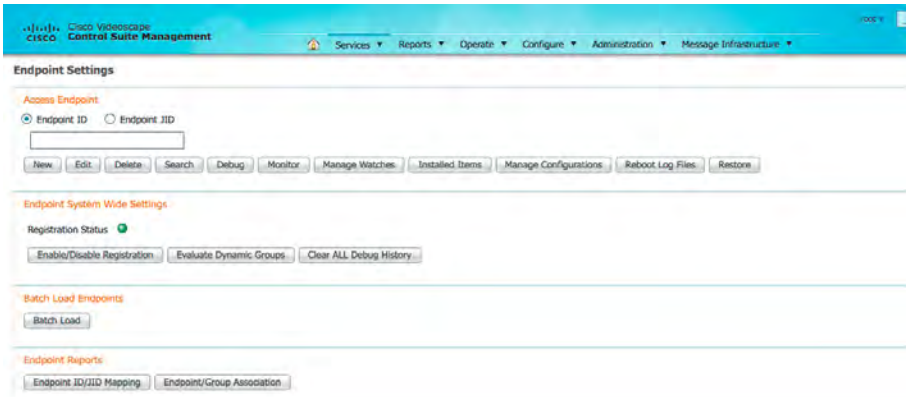
6 Click **Publish**. The Performance Parameter is published to the Endpoint and is now visible in the Performance Parameters list.



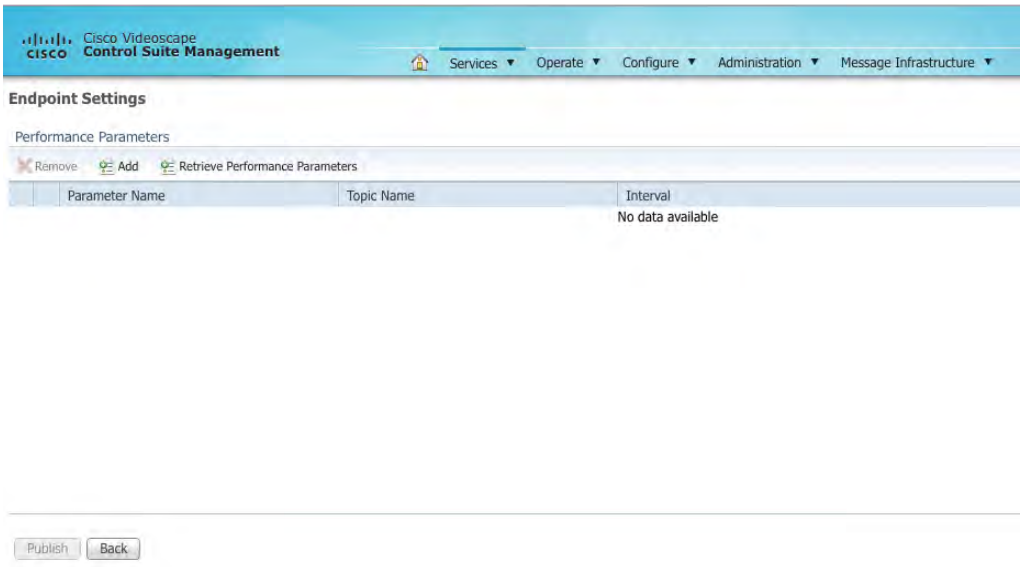
7 Click **OK** to close the **The performance parameter published success** message.

Retrieving a Performance Parameter from an Endpoint

1 Choose **Services > Endpoint Management > Endpoint Settings**. The Endpoint Settings window opens.

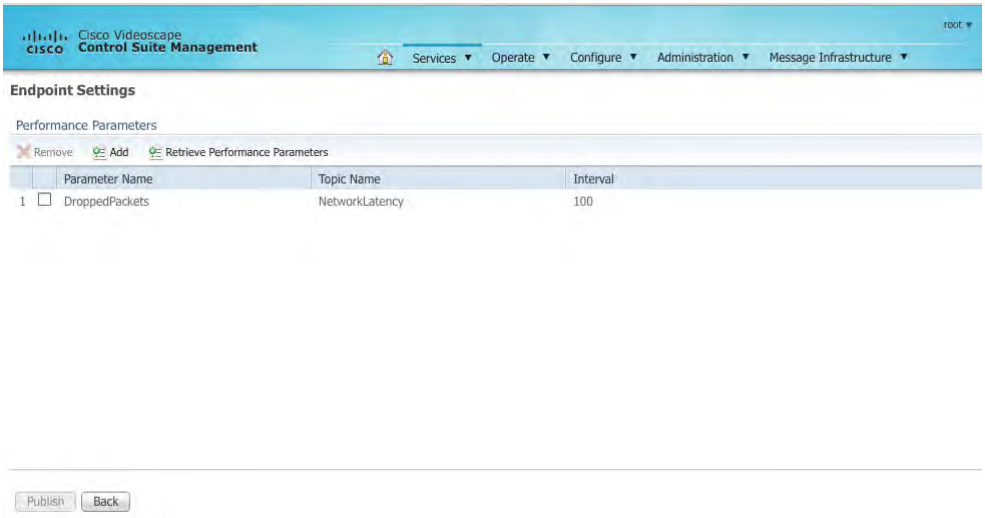


2 Type an **Endpoint ID** and click **Monitor**. The Performance Parameter window opens.



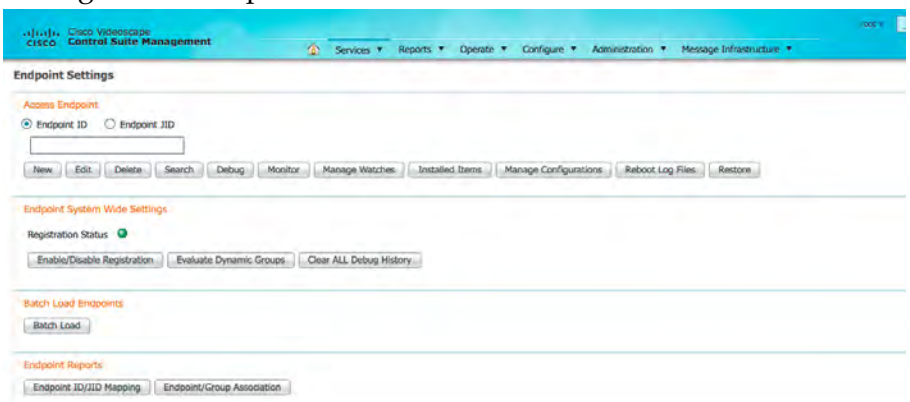
3 On the top, right portion of the window, click **monitor**. The Performance Parameters window opens.

4 Click **Retrieve Performance Parameters**. The Performance Parameters of the Endpoint are displayed.

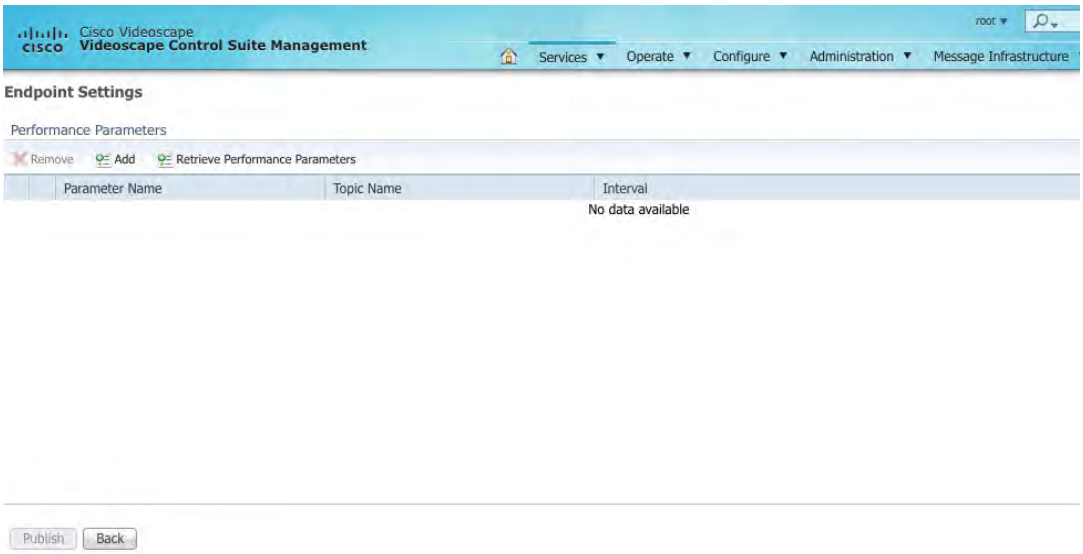


Removing a Performance Parameter from an Endpoint

1 Choose **Services > Endpoint Management > Endpoint Settings**. The Endpoint Settings window opens.

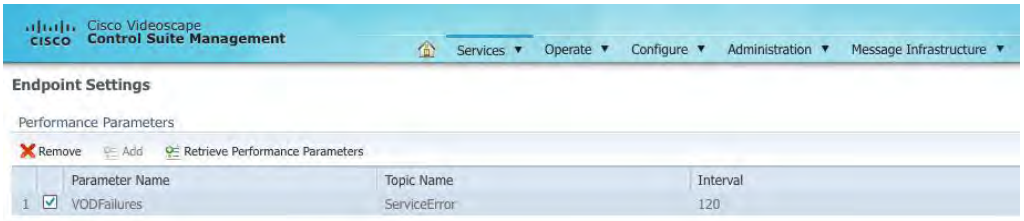


2 Type an **Endpoint ID** and click **Monitor.** The Performance Parameters window opens.



3 Click **Retrieve Performance Parameters**. The Performance Parameters of the Endpoint are displayed.

4 Choose the Performance Parameter to delete by clicking on the check-box next to the Parameter.

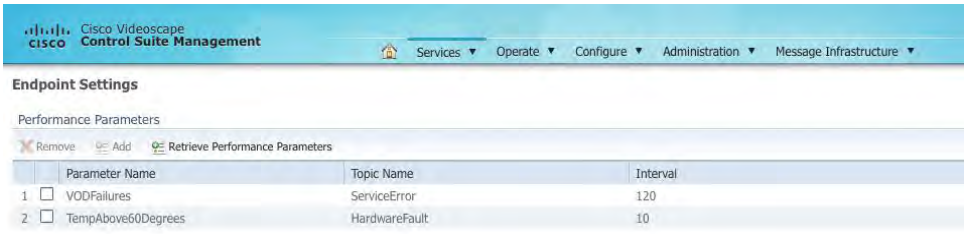


5 Click **Remove**. The Performance Parameter is removed from the Endpoint and is no longer visible in the Performance Parameter List.

Displaying the Active Performance Parameter List

The Active Performance Parameter List displays a listing of active Performance Parameters set on Endpoints.

- Choose **Services > Endpoint Management > Performance Parameters**. The Performance Parameters List window opens.

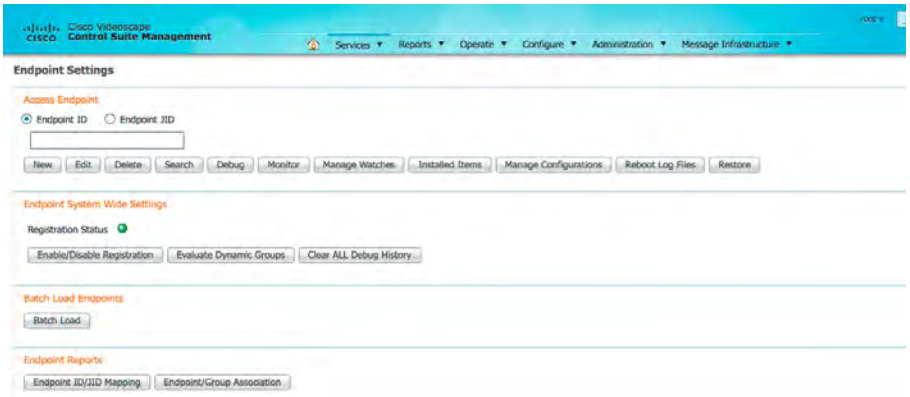


Endpoint Debug Commands

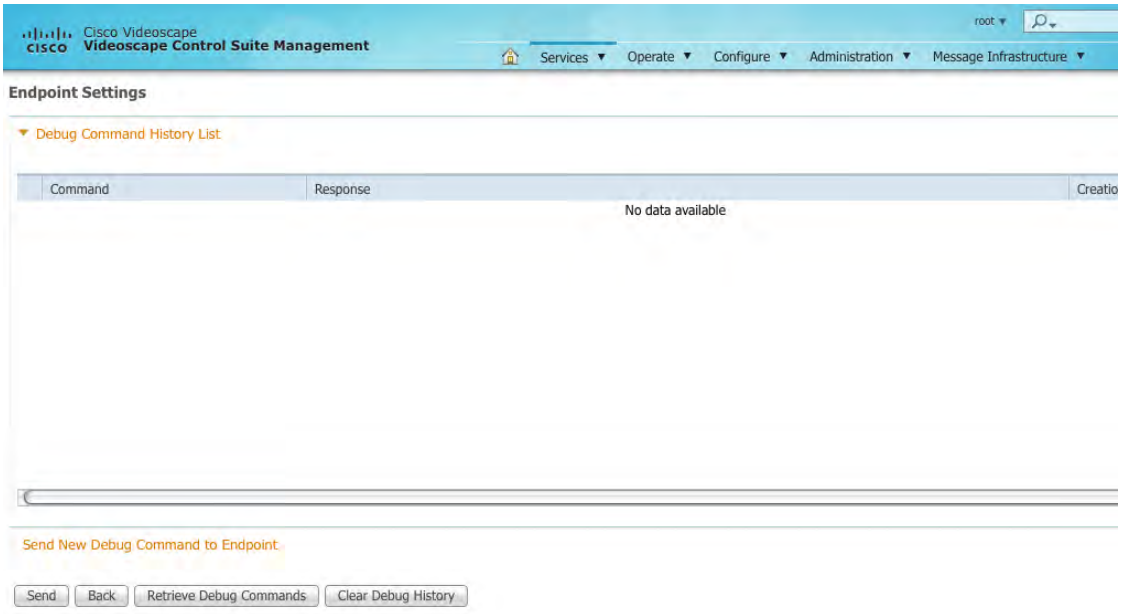
Debug commands are used by the EPM in order to assist in troubleshooting issues on an Endpoint. The Videoscape Control Suite server does not know what the debug commands are for each Endpoint device, so it has to query each Endpoint in order to discover the supported debug commands. Once the commands are discovered, they can be selected for execution.

Retrieving Debug Commands from an Endpoint

1 Choose **Services > Endpoint Management > Endpoint Settings**. The Endpoint Settings window opens.



2 Type an **Endpoint ID** and click **Debug**. The Debug Command History List opens.

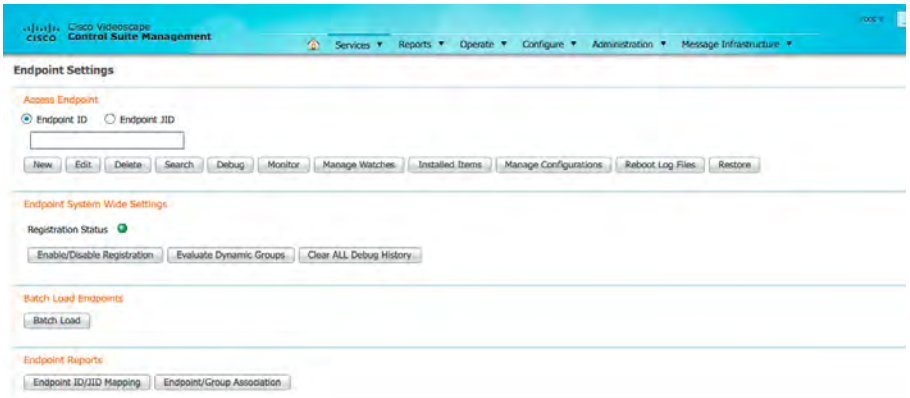


3 Click **Retrieve Debug Commands**. The Endpoint displays a list of available debug commands.

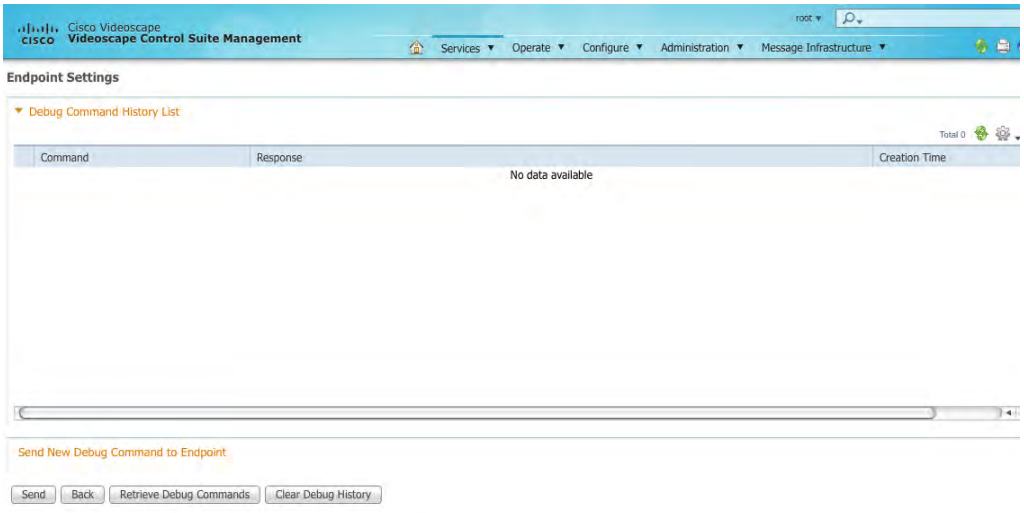
4 Click the drop-down arrow to the right of the **Available Commands** field to see a list of all available debug commands.

Sending Debug Commands to an Endpoint

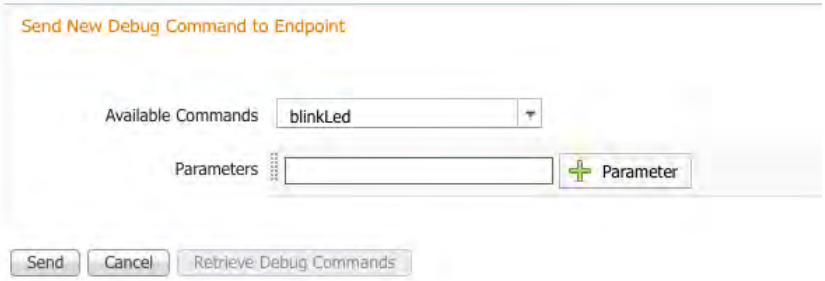
1 Choose **Services > Endpoint Management > Endpoint Settings**. The Endpoint Settings window opens.



2 Type an **Endpoint ID** and click **Debug**. The Debug Command History List opens.



3 From the **Send New Debug Command to Endpoint** section, select the required command from the **Available Commands** drop-down list.



4 Enter any required parameters and click **Send**.

Clear Debug History from an Endpoint

1 Navigate to **Services > Endpoint Settings**.
2 Enter the **Endpoint ID** and click **Debug**.
3 Click **Clear Debug History**.

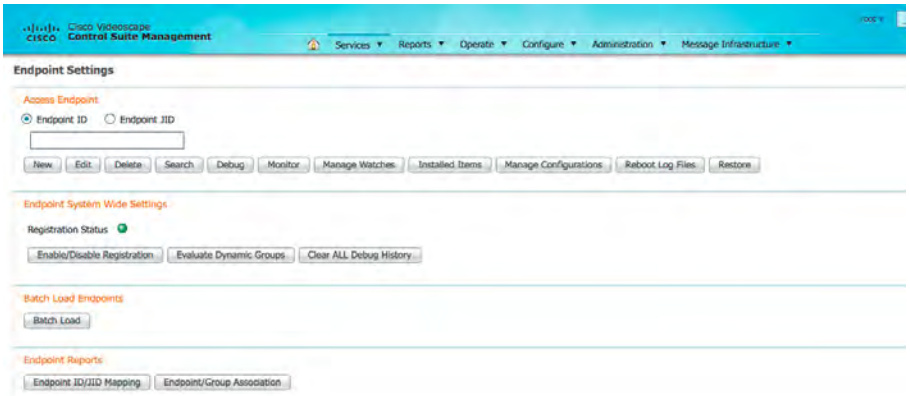
Results: All Debug responses to a previous command are deleted for the Endpoint.

Manage Installed Items

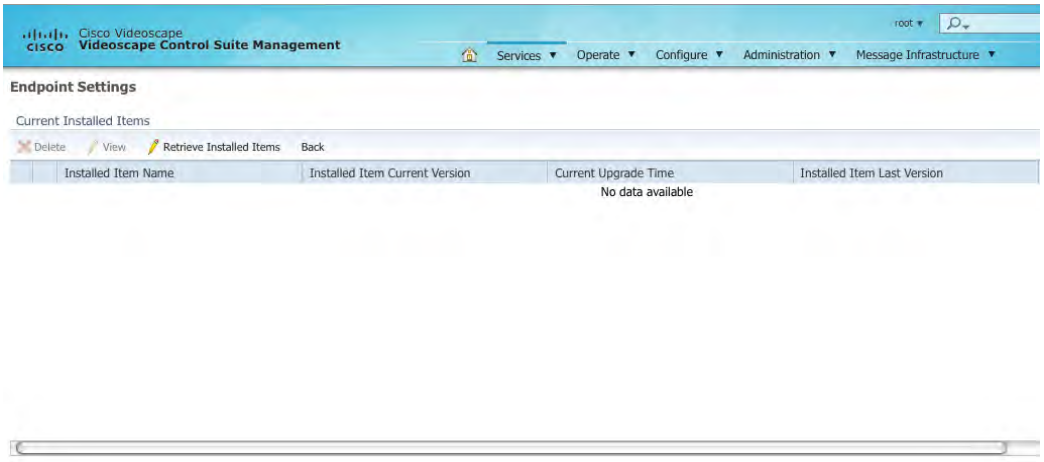
EPM provides support for lifecycle management of binary data on Endpoints. Through EPM, the operator can access information for installed items that are resident on an Endpoint. Additionally, the operator can delete installed items.

Retrieve an Installed Item

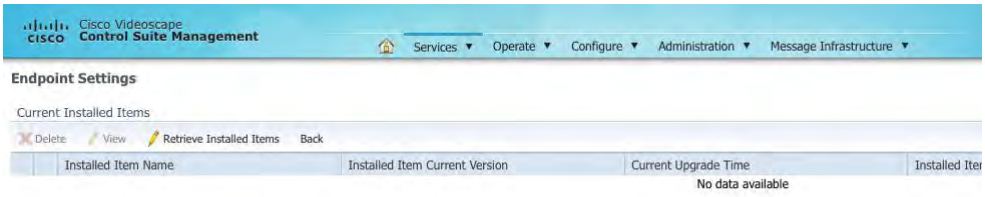
1 Choose **Services > Endpoint Management > Endpoint Settings**.



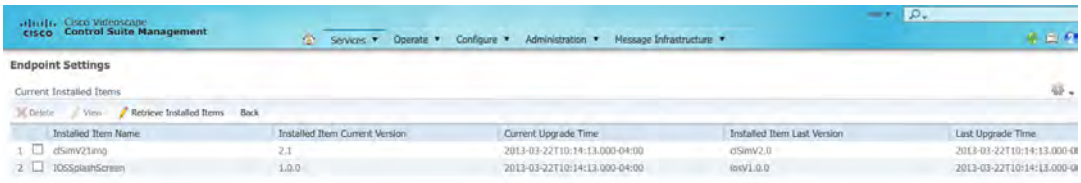
2 Enter an **Endpoint ID** and click **Installed Items**. The Current Installed Items list is displayed.



3 Click **Retrieve Installed Items**.



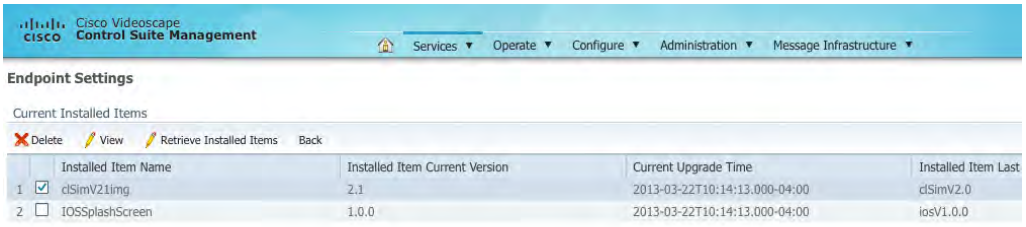
Result: The system displays a list of installed items.



Delete an Installed Item

1 Choose the item that you want to delete from the list of installed items.

2 Click **Delete**. The system deletes the item.

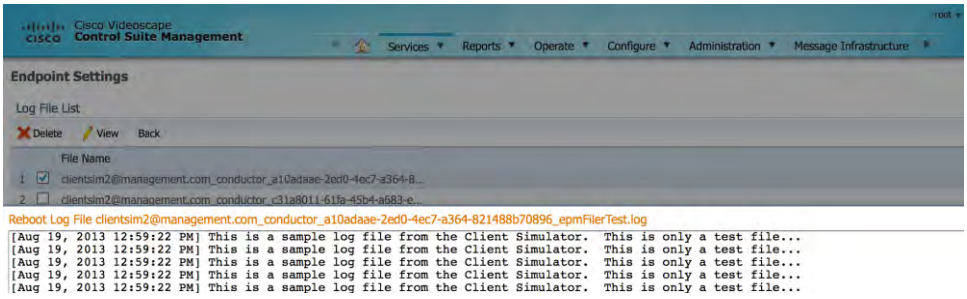


Manage Reboot Log Files

EPM allows for the storing of reboot logs generated when the Endpoint receives a trap, and then reboots. The user can view or delete these logs by accessing the Endpoint.

Note: See *Installing COP Files for the Videoscape Control Suite* (part number OL-27753) for instructions on installing the EPMFiler service. For EPM to store Reboot files from Endpoints, the EPM Filer COP file needs to have been previously installed.

1. Choose **Services > Endpoint Settings**.
2. Enter the **Endpoint ID** and then click **Reboot Log Files**.
3. Click an entry in the Log Files List and then click **View**. The user can now browse the contents of the log file for the cause of the reboot.



4. If you want to delete a Reboot Log File, select the log file and click **Delete**.

Manage Endpoint Restore

EPM allows an Endpoint to be restored with the configurations it received from the group of which it is a member so long as the group still contains the configuration. The Endpoint will also be restored with its original configurations as long as those configurations have not been canceled from the Endpoint.

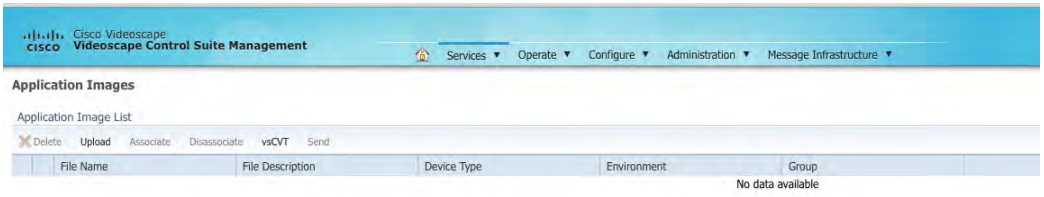
1. Click **Services** and then click **Endpoint Settings**.
2. Enter the **Endpoint ID**.
3. Click **Restore**.

Endpoint Application Images

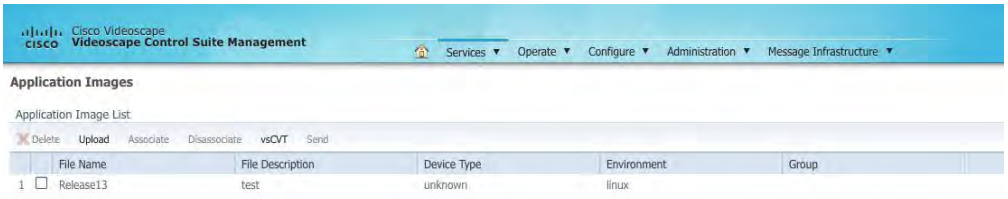
The addition of a new file to EPM requires that the manifest, which is prepended, be read and used to populate the Videoscape Code Version Table (vsCVT). The vsCVT will be published to one or more group PubSubs in order to signal the client that this image is available for download. Currently, the file with the associated manifest data, is generated outside of the Videoscape system by the software creation process of the Endpoint manufacturer.

Uploading an Image File

1. Choose **Services > Endpoint Management > Application Images**. The Application Image List opens.

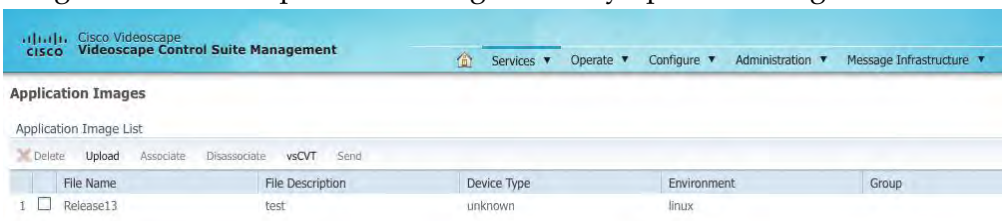


2. Click **Upload**. The Select Image pop-up window opens.
3. Browse the Select Image window and choose the image that you want to upload.
4. Click **Upload**. A security warning appears.
5. Click **Continue**. The image uploads and is displayed on the Application Image List.



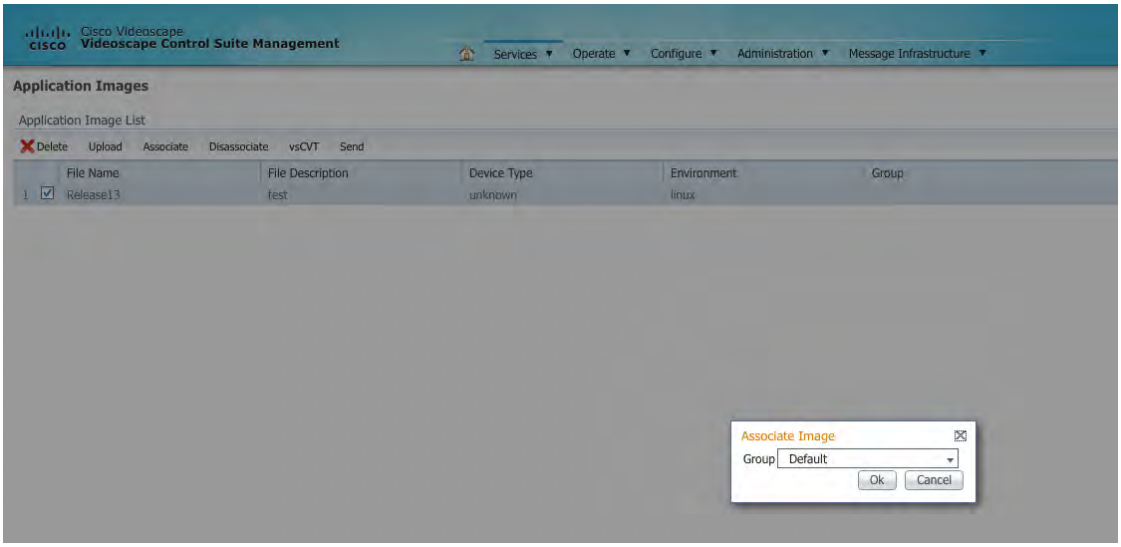
Associating an Image with a Group

1. Choose **Services > Endpoint Manager > Application Images**. The Application Image List window opens containing the newly uploaded image.



2. Choose the image that you want to associate with a group and click **Associate**. The Associate Image pop-up window opens.

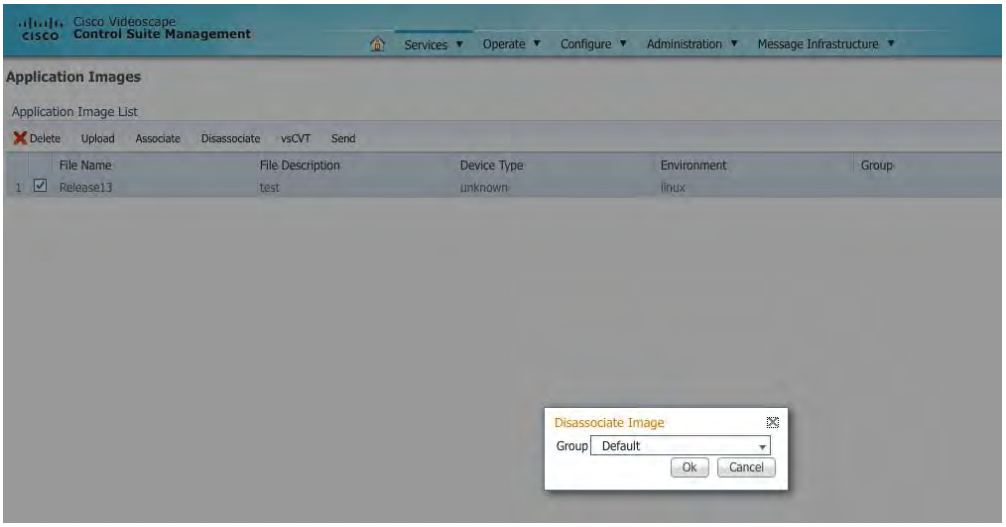
3 Click the arrow to choose the desired group from the drop-down list and click **OK**.



Disassociating an Image From a Group

1 Choose **Services > Endpoint Management > Application Images**. The Application Image List window opens containing a list of uploaded images.

2 Choose the image that you want to disassociate from a group and click **Disassociate**. The Disassociate Image pop-up window opens.

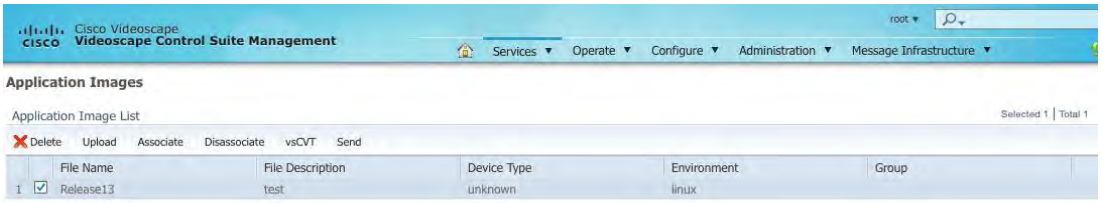


3 Click the arrow to select the Group from which the image is to be disassociated and click **OK**.

Deleting an Image From the Image List

Note: You cannot delete an image if it is associated with a group. The image needs to be first disassociated from the group if it is to be deleted.

1. Choose **Services > Endpoint Management > Application Images**. The Application Image List appears.
2. Choose the image that you want to delete and click **Delete**. The system deletes the image.



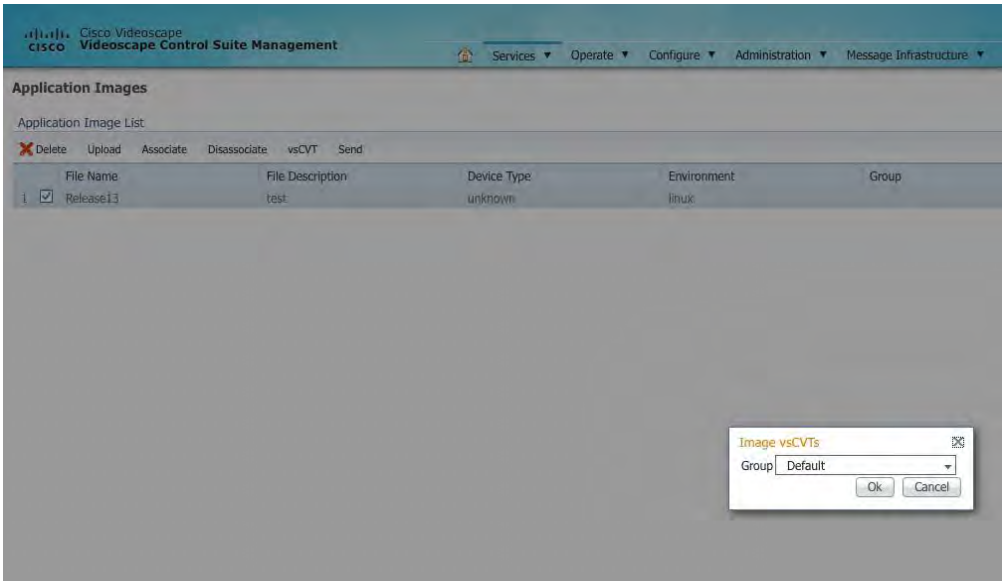
Manage vsCVTs

The term vsCVT refers to the process whereby software is made available to Endpoints to download. When an application file is made available to one or more Endpoint clients, the EPM updates the vsCVT to include the information on the application file and notifies the clients of one or more groups via a PubSub. The clients will be subscribed to the PubSub by the EPM and receive notification messages with the attached vsCVT.

Adding an Image to the vsCVT List

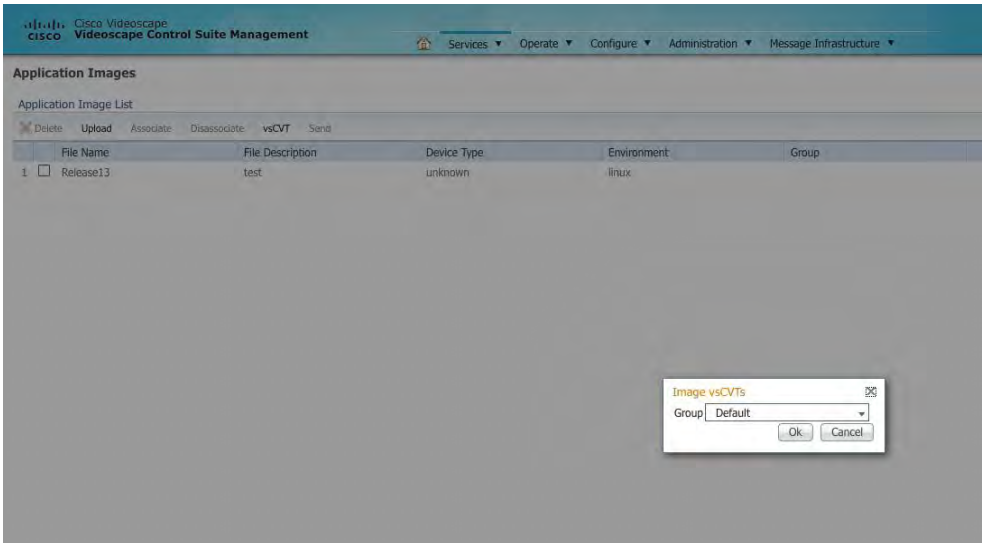
Important: Prior to adding an image to the vsCVT list, the image must be associated with a group. See ***Associating an Image with a Group*** (on page 45) for details.

1. Choose **Services > Endpoint Management > Application Images**. The Application Image List opens.
2. Choose the image you require and click **vsCVT**. The Image vsCVTs pop-up window opens.
3. Click the drop-down menu to select the group for which you intend to build the vsCVT and then click **OK**.

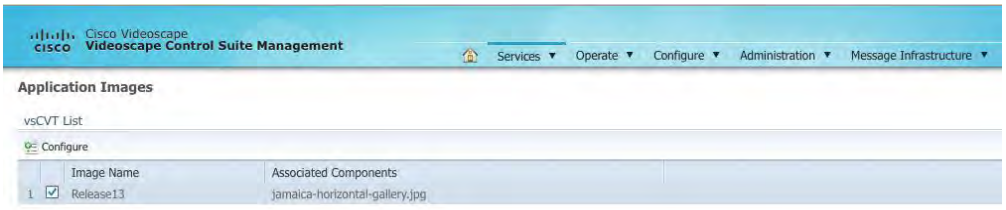


Publishing a vsCVT to a Group

1. Choose **Services > Endpoint Management > Application Images**. The Application Image List opens.
2. Click **vsCVT**. The Image vsCVTs pop-up window opens.



3. Choose the Group that you want to publish the vsCVT, and click **OK**. The vsCVT List appears.



4. Choose the vsCVT and click **Configure** (at the top of the window).
5. Enter or select the desired **Type** of download.

   Notes:

   - Select one of the following download Types:
     - **Emergency** — The client starts the download immediately.
     - **Immediate** — The client should start the download as soon as possible.
     - **Normal** — Download occurs when the client determines that there is no impact to any video service the subscriber has requested, such as scheduled DVR events.
     - **Forced** — The clients are required to download the specified application/component immediately even if this application is identical to the installed application.
     - **Delete** — The client removes the indicated application/component from the installed set.

- The **Download Start Time** field (in the next step) specifies the start time, in UTC, of the window when the client should download the application/image.
- The **Download Stop Time** field (in the next step) specifies the stop time, in UTC, of the window when the client should download the application/image.

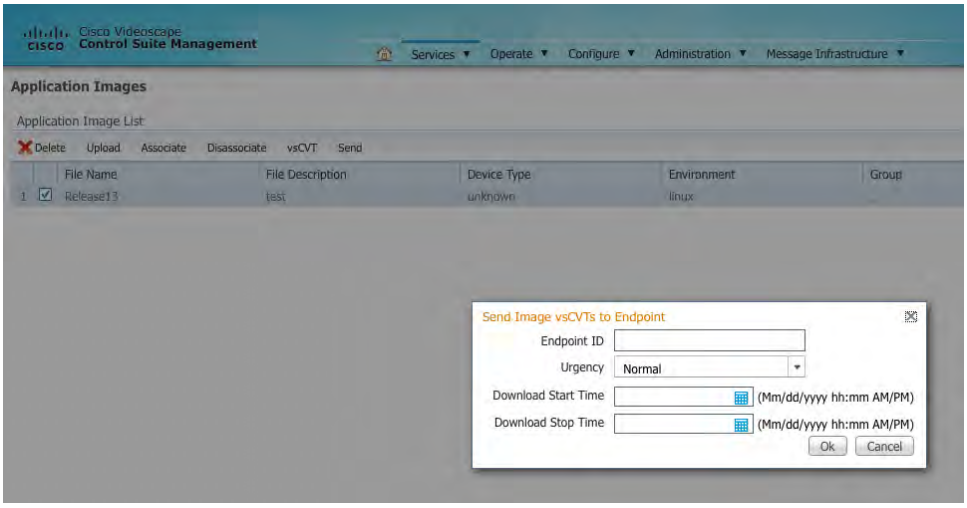
6 Click to select the **Download Start Time** and the **Download Stop Time**.

7 Click **Publish**. The vsCVT publishes to the Group.

Sending a vsCVT to an Endpoint

1 Click **Services**.

2 Under **Endpoint Management Settings**, choose **Application Images**. The Send Image vsCVTs to Endpoint dialog window opens.



3 Enter the **Endpoint ID**, **Urgency**, **Download Start Time**, and **Download Stop Time**.

4 Click **Ok**. The vsCVT is sent to the Endpoint.

Note: A vsCVT cannot be directly sent to an Endpoint. **CSCuj66170** addresses this issue.

Endpoint Notification Access

EPM provides the capability to query a specific notification for information that occurred within a start and stop time. It also provides access to the entire contents of any notification.

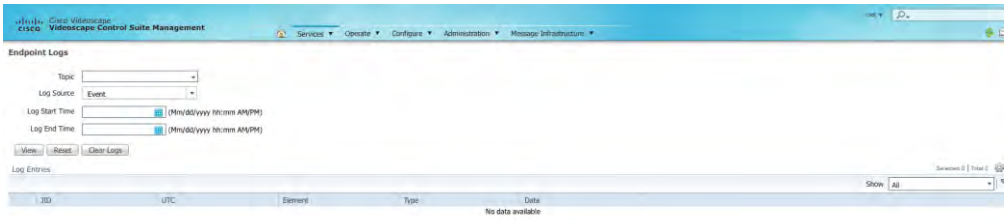
Notification information includes the Endpoint JID value, a time stamp, and the type of notification for each entry.

Notes:

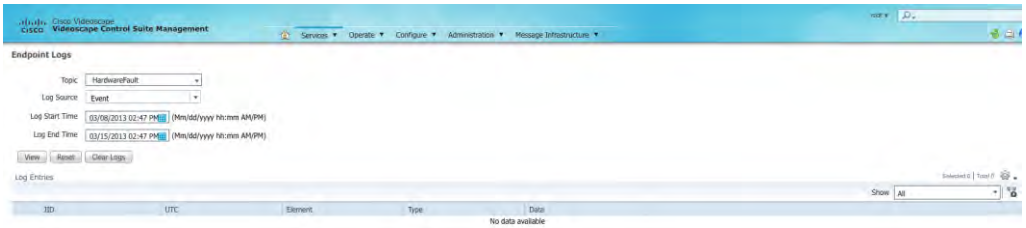
- A notification is tied to a Topic.
- The notification source consists of an Event, a Performance, or a Watch.

  Note: In the case of the Event notification source, the service provider provides this information in the client code. The operator needs to know the events supported by the clients in advance, and then create Topics for those events. Once the Topics have been created, EPM receives the Event notifications from the Endpoints.

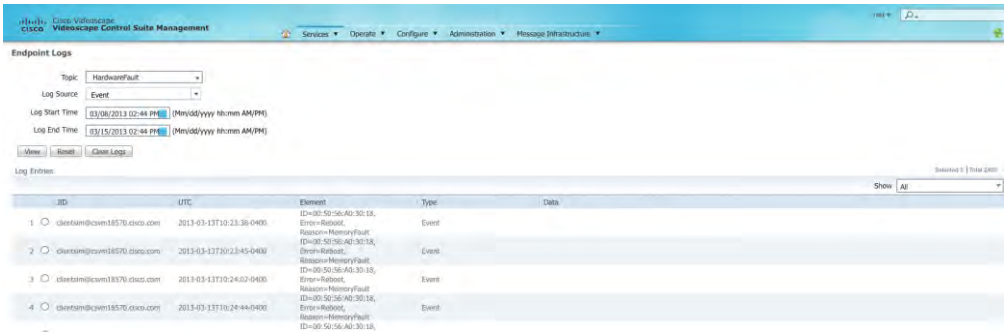
1 Choose **Services > Endpoint Management > Notifications**. The Endpoint Notifications window opens.



2 Select the **Topic**, **Notification Source**, **Notification Start Time**, and **Notification End Time**.



3 Click **View**. The EPM displays the notification entries.



Note: The notification includes the Endpoint JID, the time the notification was sent, and element/reason for the notification, as well as the Notification Source Type.

4 Click **Clear Logs** to clear all notifications.

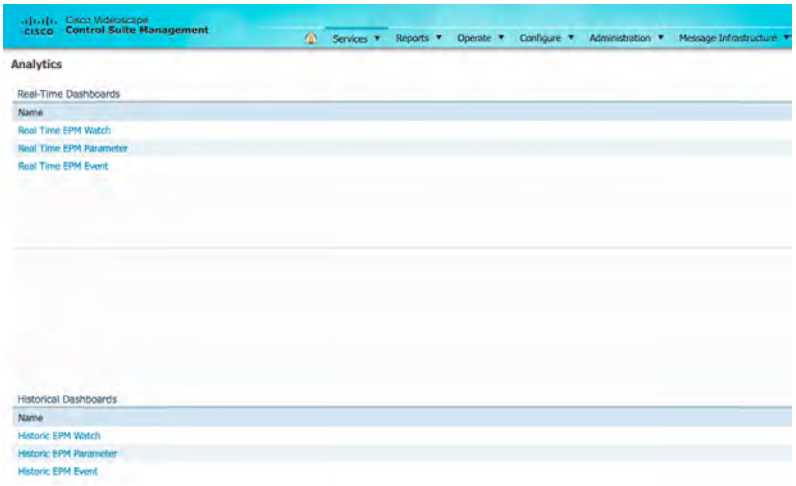
Endpoint Analytics

Prime Analytics reports real and historical data for Events, Performance, and Watch notifications. Refer to the **Install the Data Analytics** chapter of *Installing COP Files for the Videoscape Control Suite* (part number OL-27753) for more information on installing and configuring Prime Analytics.

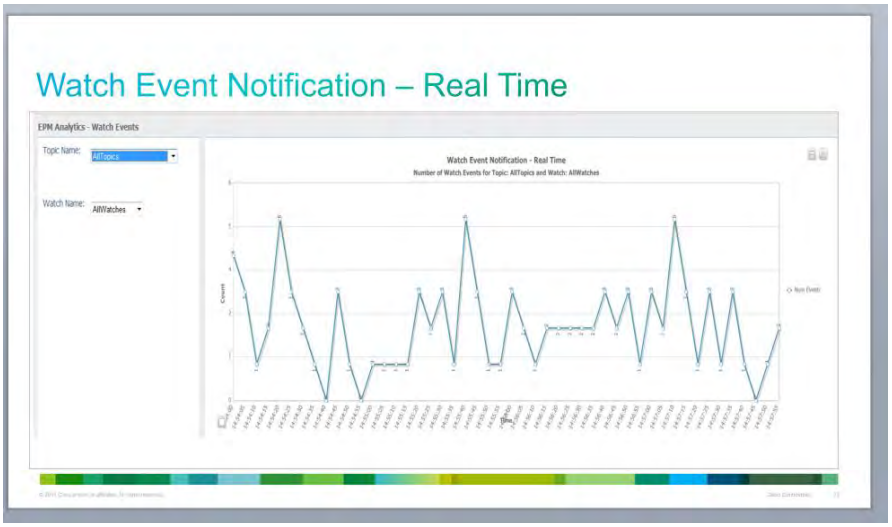
Query Type	Dashboard	Feature	Notes
Real Time Graph	EPM Event – Real Time	Show total number of Events by Topic and Error Name.	Data point every 5s. Drop-down selections for Topic, Error Name.
	EPM Parameter – Real Time	Show Performance Parameters received by Topic, Parameter Name, Device Type, Function Type (Total or Min/Max/Avg).	Data point every 5s. Drop-down selections for Topic, Parameter Name, Device Type, Function Type.
	EPM Watch – Real Time	Show total number of Watch events by Topic and Watch Name.	Data point every 5s. Drop-down selections for Topic, Watch Name.
Historical Graph	EPM Event – Last Day	Show total number of Events by Topic and Error Name for selected time ranges in the last 24 hours.	Drop-down Selections for Time Range, Topic, Error Name.
	EPM Parameter – Last Day	Show Performance Parameters received by Topic, Parameter Name, Device Type, Function Type (Total or Min/Max/Avg) for selected time ranges in the last 24 hours.	Drop-down selections for Time Range, Topic, Parameter Name, Device Type, Function Type.
	EPM Watch – Last Day	Show total number of Watch events by Topic and Watch Name for selected time ranges in the last 24 hours.	Drop-down selections for Time Range, Topic, Watch Name.

To view data in the Real Time or Historical Dashboard, Endpoints have to be currently sending notifications to view the real-time data, or have previously sent notifications to view the historical data.

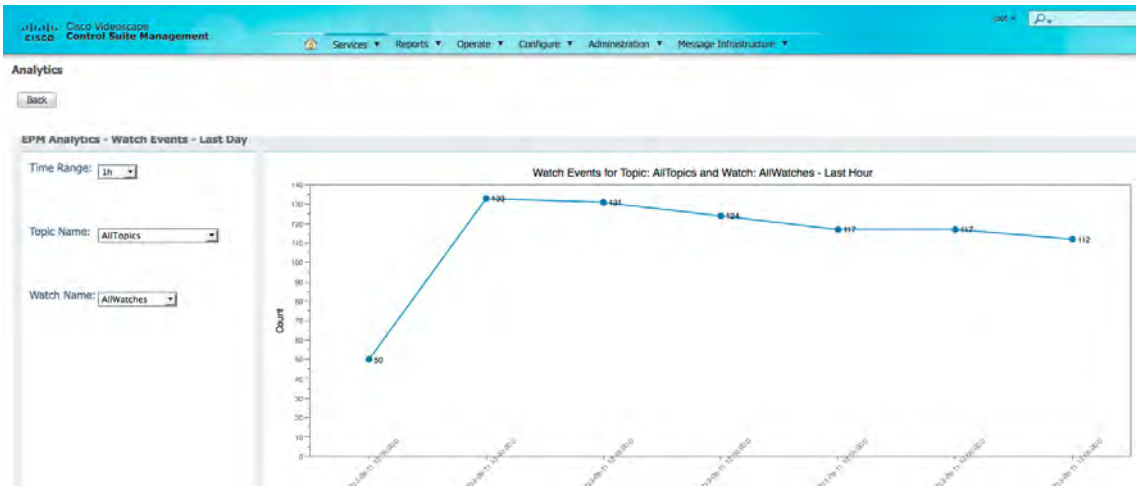
From the **Services** menu, navigate to the **Endpoint Management** section and click **Analytics**.



- To view real-time data for Watch notifications, click **Real Time EPM Watch**.



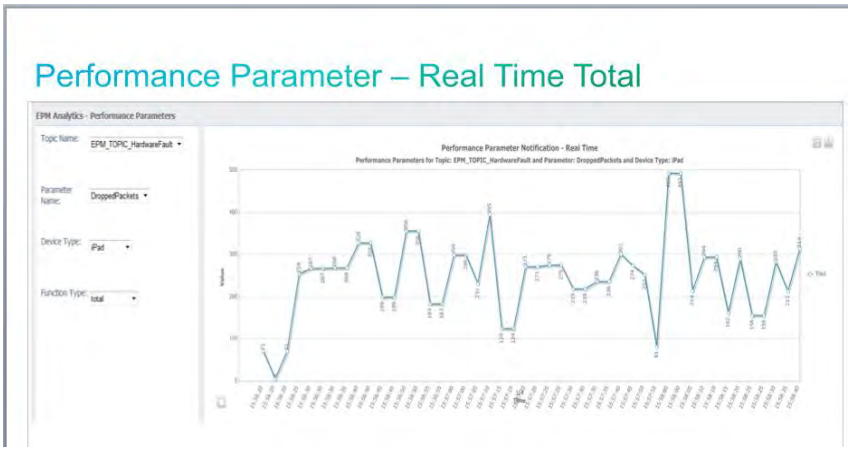
- To view Historic EPM Watch notifications, click **Historic EPM Watch**.



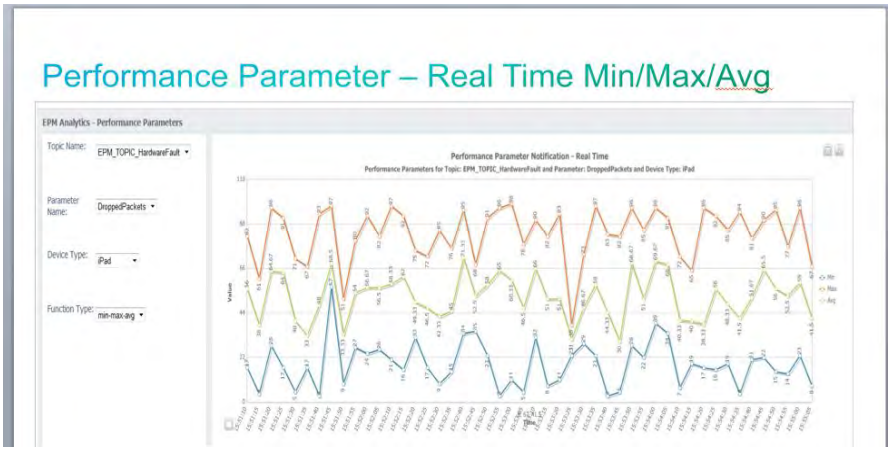
Notes:

- Filter on **Time Range**, **Topic Name**, or **Watch Name**.
- The user can see real-time performance parameters by specific **Topic Name**, **Parameter Name**, **Device Type**, and function type of "total" or "min-max-avg".

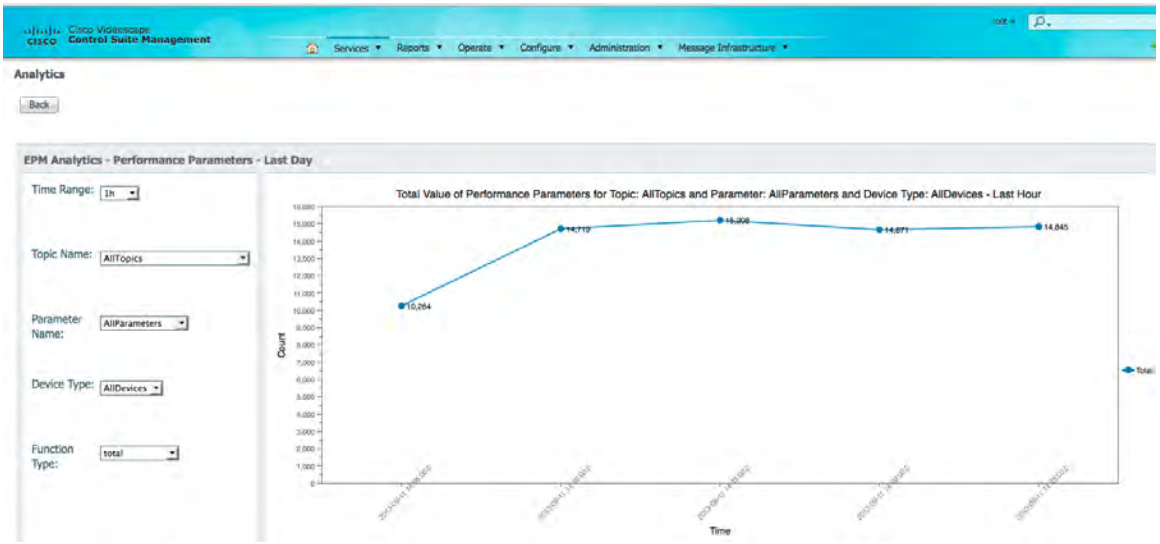
- To view real-time data for Parameter notifications by "total", click **Real Time EPM Parameter**. Then, filter on **Topic Name**, **Parameter Name**, and **Device Type**. Select **Function Type** "total".



- To view real-time data for Parameter notifications by "min-max-avg", click **Real Time EPM Parameter**. Then, filter on **Topic Name**, **Parameter Name**, and **Device Type**. Select **Function Type** min-max-avg.

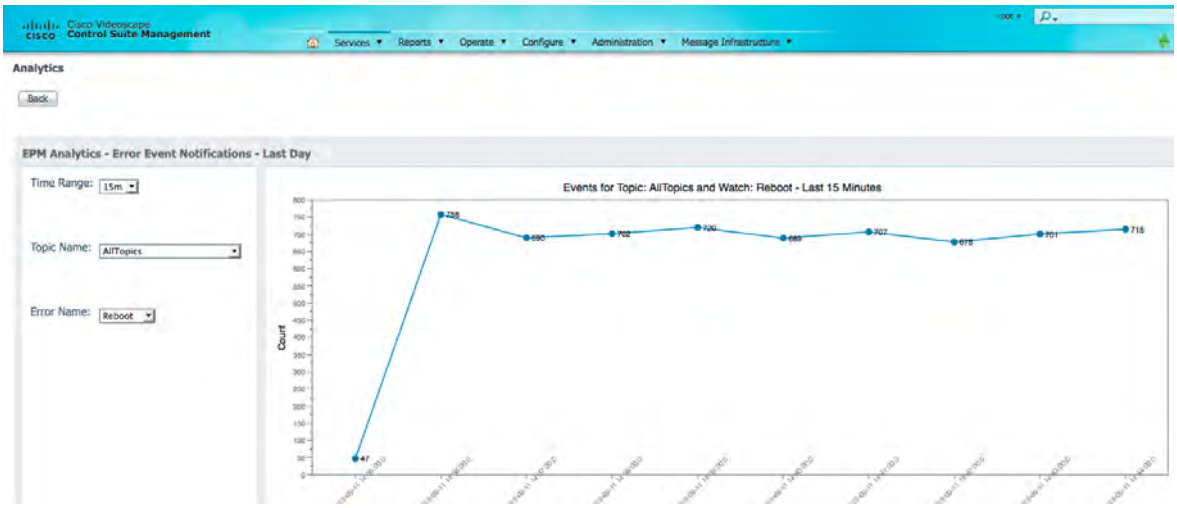


- To view Historic data for Parameter notifications, click **Historic EPM Parameter**.



- To view real-time data for Event notifications, click **Real Time EPM Event**.

- To view Historic data for Event notifications, click **Historic EPM Event**. Filter on **TIme Range**, **Topic Name**, or **Error Name** to see specific data.

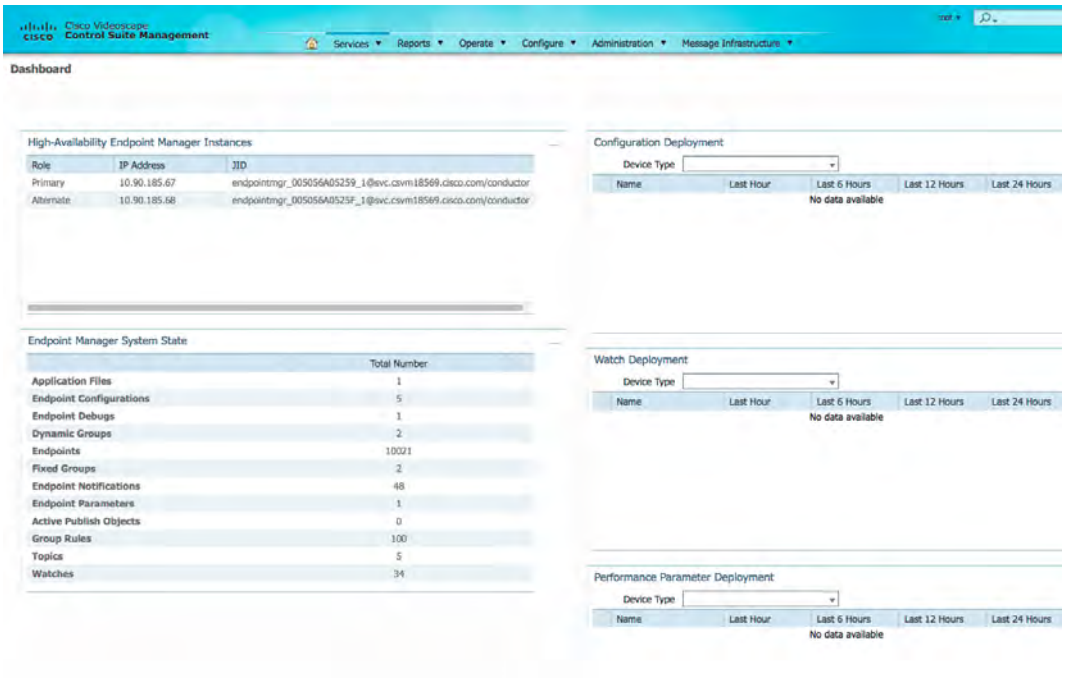


Endpoint Diagnostics

The EPM Dashboard window provides configuration and key resource utilization information for the following items:

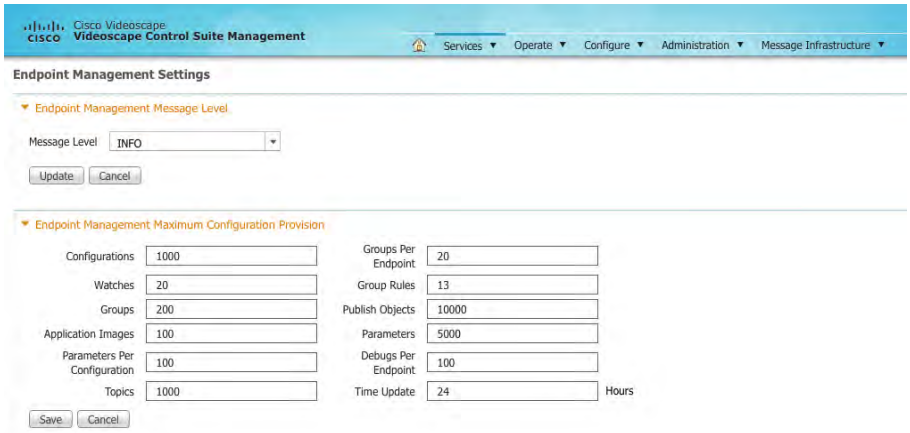
- vsCVT
- Application Files
- Endpoint Configurations
- Endpoint Debugs
- Dynamic Groups
- Endpoints
- Fixed Groups
- Endpoint Logs
- Endpoint Parameters
- Active Publish Records
- Group Rules
- Topics
- Watches
- Configuration Deployment (to a device within the last 1, 6, 12, or 24 hours)
- Watch Deployment (to a device within the last 1, 6, 12, or 24 hours)
- Performance Parameter Deployment (to a device within the last 1, 6, 12, or 24 hours)

To access the Dashboard, choose **Services > Endpoint Management > Dashboard**.



Endpoint Management Settings

The Endpoint Management Settings window allows the user to set the **Message Level** in the EndpointManager and server logs. Message levels are INFO, WARN, DEBUG, ERROR, and TRACE.



- **INFO —** The INFO level identifies informational messages that highlight the progress of the application at a coarse-grained level.
- **WARN —** The WARN level identifies potentially harmful situations.
- **DEBUG —** The DEBUG Level shows fine-grained informational events that are most useful to debug an application.
- **ERROR —** The ERROR level identifies error events that might still allow the application to continue running.
- **TRACE —** The TRACE Level shows finer-grained informational events than the DEBUG level.

To change the levels, click the arrow to the right of the **Message Level** tab and choose the desired level. Then, click **Update**.

Endpoint Management Maximum Configuration Provision

The Endpoint Management Maximum Configuration Provision section displays the default configuration of Endpoint Manager.

To change the configuration values, enter the new value and select **Save**.

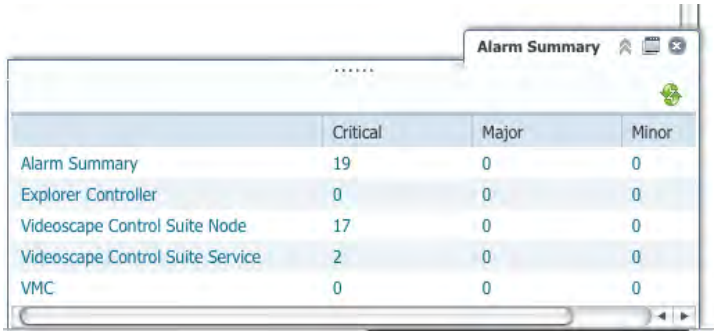
Note: The current default value and maximum settings are as follows:

Variable Name	Default Value	Maximum Setting	Type
BatchLoadRecordMaximum	10,000	100,000	Integer
GroupMaximumPerEndpoint	20	200	Integer
WatchCountMaximum	20	200	Integer
GroupRuleMaximum	13	100	Integer
GroupMaximum	100	1000	Integer
ApplicationStoredMaximum	100	200	Integer
ParameterPerConfigurationMaximum	100	500	Integer
PublishObjectsMaximum	10,000	100,000	Integer
TimeUpdateValue	24 hours	N/A	Integer
DebugEntryMaximum (per Endpoint)	100	500	Integer
TopicMaximum	500	1000	Integer
ParameterMaximum	5,000	10,000	Integer
ConfigurationMaximum	1,000	1,000	Integer

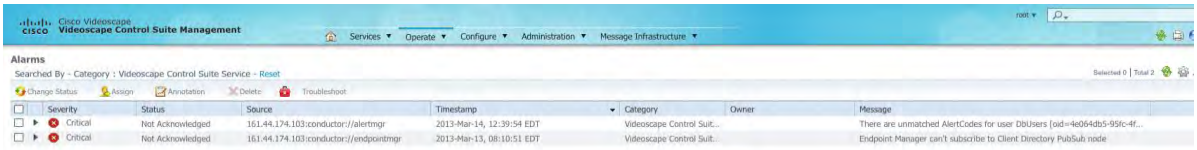
SNMP Alarms

EPM currently implements two alarms: communication errors with the database and errors encountered when subscribing to the ClientDirectory. Alarms are displayed using the Alarm Summary icons at the bottom right corner of the CMC UI.

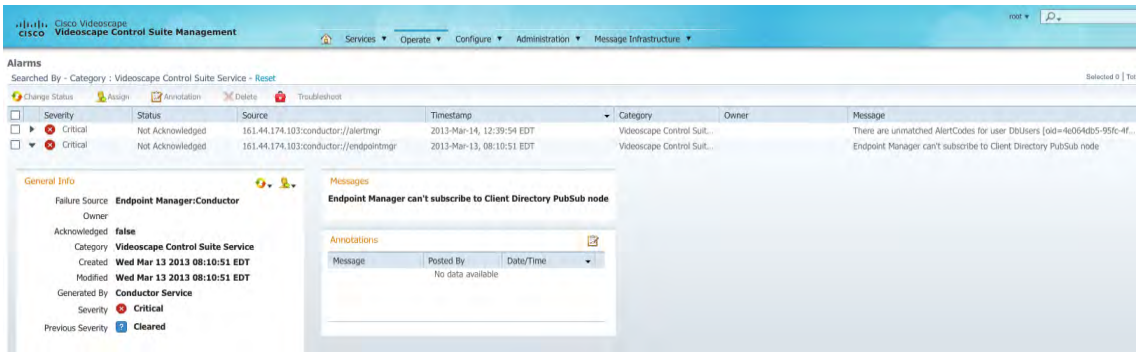
1 In the main Videoscape Control Suite window, click **Alarm Summary** (at the bottom of the window). The Alarm Summary window opens.



2 Click **Videoscape Control Suite Service**. The window updates to show alarms associated with the Videoscape Control Suite service.



3 Click the arrow to the left of an alarm to see the details for that alarm.



Notes:

- To acknowledge, unacknowledge, or clear an alarm, choose the alarm and click **Change Status**.
- To assign an alarm, choose the alarm and click **Assign**.
- To annotate an alarm, choose the alarm and click **Annotation**.
- To delete an alarm, choose the alarm and click **Delete**.
- To ping or perform a traceroute operation upon an alarm, choose the alarm and click **Troubleshoot**.

Manage Endpoint Manager Logs

Endpoint Manager writes to two logs: EndpointManager.log and server.log.

1 To see a listing of available logs, type the following command at the **admin** prompt and then press **Enter**.

```
file list activelog jboss
```

Result: The system returns a list of available logs.

Example:

```
EndpointManager.log.1                EndpointManager.log.10
EndpointManager.log.2                EndpointManager.log.3
EndpointManager.log.4                EndpointManager.log.5
EndpointManager.log.6                EndpointManager.log.7
EndpointManager.log.8                EndpointManager.log.9
boot.log
 server.log
server.log.2013-03-29.log.1.gz       server.log.2013-03-30.log.1.gz
server.log.2013-03-31.log.1          server.log.2013-04-01.log.1
server.log.2013-04-01.log.2          server.log.2013-04-02.log.1.gz
server.log.2013-04-02.log.2          server.log.2013-04-03.log.1
server.log.2013-04-04                server.log.2013-04-04.log.1
dir count = 2, file count = 34
```

Notes:

- Files with a .log extension are the most recent.
- Files with a .log.1 extension are the next most recent, and so on.
- Files that have been compressed (.gz extension) cannot be uncompressed from the CLI. They need to be transferred to a desktop server, uncompressed, and viewed from there.

2 To view a log file, type the following command and press **Enter**.

```
file view activelog jboss/[server.log]
```

Note: Replace [server.log] with the name of any log file from the output of step 1.

3 To tail a log, type the following command and press **Enter**.

```
file tail activelog jboss/EndpointManager.log
```

4 To search through a log, type the following command and press **Enter**.

```
file search activelog jboss/EndpointManager.log jid
```

Note: In this example, **jid** is the string you are looking for in the EndpointManager.log file.

5 To transfer a log file to another server, type the following command and press **Enter**.

```
file transfer secure-export [local-src-file-path]
[user@host:file_path]
```

Example:

```
file transfer secure-export jboss/EndpointManager.log
ftpuser@10.90.187.251:/home/ftpuser
```

3

Troubleshooting the Endpoint Manager Service

Introduction

Refer to this chapter for information that can help you troubleshoot the Endpoint Manager service.

In This Chapter

- Endpoint Manager Troubleshooting..... 66

Endpoint Manager Troubleshooting

EPM HTTP Error Codes

The standard HTTP error codes that EPM returns are as follows:

- 200 Ok
- 201 Created
- 400 Bad Request
- 401 Unauthorized
- 404 Not Found
- 405 Method Not Allowed
- 500 Internal Error; a status object is returned and the error message is populated upon error.

Registration Flag Red, Service Instance Green, Unable to Create Endpoints (1)

Possible Cause: Incorrect IP addresses entered for NOSQLCB during EndpointManager COP file install

1 View the server.log file for NOSQLCB connection errors.

```
admin:file dump activelog jboss/server.log
```

Sample output:

```
14:28:27,083 INFO  [stdout] (pool-1160-thread-1) 2012-11-09
14:28:27,083 ERROR [root]
CouchbaseConnection.openConnection() Exception while trying to
connect to Couchbase Cluster null
14:28:27,083 INFO  [stdout] (pool-1160-thread-1) 2012-11-09
14:28:27,083 WARN  [root]
ConductorAlarmMgrSingleton.raisePersistenceAlarm(): Conductor
SNMP framework not intialized
14:28:27,083 INFO  [stdout] (pool-1160-thread-1) 2012-11-09
14:28:27,083 ERROR [root]  EPMInstancePoolDAO.getAndLock()
Couldn't establish a connection with Couchbase Server
14:28:27,083 INFO  [stdout] (pool-1160-thread-1) 2012-11-09
14:28:27,083 ERROR [root]  CheckLeadershipTask.run(): Unknow
execption while trying to read instance pool object: Couldn't
establish a connection with Couchbase Server
14:28:32,087 ERROR [stderr] (pool-1160-thread-1) 2012-11-09
14:28:32.087 WARN
com.couchbase.client.vbucket.ConfigurationProviderHTTP:
Connection problems with URI http://10.90.187.30:8091/pools
...skipping
14:28:32,088 ERROR [stderr] (pool-1160-thread-1)
java.net.ConnectException: Connection refused
```

2 Enter the correct NOSQLCB IP address(es) in the Endpoint Manager configuration file.
3 Uninstall and then reinstall the Endpoint Manager service, using the correct NOSQLCB IP address(es).

Registration Flag Red, Service Instance Green, Unable to Create Endpoints (2)

Possible Cause: NOSQLCB password mismatch

1 View the server.log file for HTTP response 401 errors.

```
admin:file dump activelog jboss/server.log
```

Sample output:

```
15:14:18,893 ERROR [stderr] (pool-1344-thread-1) 2012-11-09
15:14:18.893 WARN
com.couchbase.client.vbucket.ConfigurationProviderHTTP:
Connection problems with URI http://10.90.187.31:8091/pools
...skipping
15:14:18,894 ERROR [stderr] (pool-1344-thread-1)
java.io.IOException: Server returned HTTP response code: 401
for URL: http://10.90.187.31:8091/pools
```

2 Check to ensure that the NOSQLCB password entered during the Endpoint Manager COP file installation matches the password used when creating the bucket in NOSQLCB.
3 View the Endpoint Manager configuration file and compare the password in the file to the password used in creating the NOSQLCB bucket.

Sample output:

```
<?xml version="1.0" encoding="UTF-8"?><configuration><node-
attributes><serviceJID>epmjid@svc.csvm18725.cisco.com</service
JID><clientDirVSNS>clientdirectort</clientDirVSNS><clientDirJI
D>client@cisco.com</clientDirJID><couchbasePrimaryIP>10.90.187
.31</couchbasePrimaryIP><couchbaseSecondaryIP>10.90.187.32</co
uchbaseSecondaryIP><couchbasePort>8092</couchbasePort><binding
Jsm>jsm-1.rtr-svc25-
2</bindingJsm><password>cisco123</password><userID>endpoint</u
serID><servicePassword>epmpasswd</servicePassword><pubsubDomai
n>pubsub.features</pubsubDomain><mccHost>10.90.187.26</mccHost
><fileProxyServer>10.90.187.251</fileProxyServer><jsmHost>10.9
0.187.26</jsmHost></node-attributes></configuration>
```

4 If there is a password mismatch, edit the Endpoint Manager configuration file. Then, uninstall and reinstall Endpoint Manager.

Endpoint Manager Fails to Start, Registration Flag is red, Service Instance is Red

Possible Cause: The SVC password was changed for the SVC JID in the Endpoint Manager Configuration file.

1. Check the server.log file.

   ```
   file dump activelog jboss/server.log
   ```

   Sample output:

   ```
   12:36:53,039 INFO  [stdout] (MSC service thread 1-5) 2012-07-
   23 12:36:53,039 INFO  [root]  EndpointManagerMBean.start()
   Starting EndpointMgr Conductor Service thread under virtual
   service ns: conductor://endpointmgr
   12:36:53,269 INFO
   [com.cisco.conductor.servicesdk.backend.ConductorService] (MSC
   service thread 1-5) EndpointManagerConductorService service is
   initialized successfully
   12:36:53,281 INFO  [stdout] (MSC service thread 1-5) 2012-07-
   23 12:36:53,281 ERROR [root]  EndpointManagerMBean.start()
   Exception while trying to start Endpoint Conductor Service:
   SASL authentication DIGEST-MD5 failed: not-authorized:
   12:36:53,281 ERROR [stderr] (MSC service thread 1-5)
   java.lang.Exception: SASL authentication DIGEST-MD5 failed:
   not-authorized
   ```

2. Edit the Endpoint Manager configuration file and change the password back to the correct password.
3. Uninstall and then reinstall Endpoint Manager.

The Default Group is Missing When an Endpoint is Created

1. Check the management console UI to determine whether the DefaultGroupPubSub is present.
   a. Log into the management console UI and navigate to the PubSub list:
      Message Infrastruture > PubSub Management > pubsub.features
   b. If the DefaultGroupPubSub is present, delete it along with the following pubsubs:
      - DownloadApplicationFinish
      - DownloadApplicationStart
      - EndpointProvison
2. Uninstall and then reinstall Endpoint Manager.

No Endpoint Log Information Stored for Endpoints

Possible causes:

- Logging is not enabled on the relevant Endpoint(s).
  Solution: Enable logging on the Endpoint(s).
- There is no PubSub created for the desired Topic Log Source.
  Solution: Create the appropriate Topic for Events, Watches, or Performances.

4

Troubleshooting EPM Analytics

Introduction

Refer to this chapter for information that can help you troubleshoot EPM Analytics.

In This Chapter

- EPM Analytics Troubleshooting..... 70

EPM Analytics Troubleshooting

- Start the EPM analytics application
  `cd /opt/cisco/vcs/analytics/connectors/epm/epm && ./start.sh`
- Stop the EPM analytics application
  `cd /opt/cisco/vcs/analytics/connectors/epm/epm && ./stop.sh`
- EPM install log
  `/opt/cisco/vcs/analytics/logs/epm/da_install.log`
- Uninstall log
  `/var/da_uninstall.log`

Database Purge

The database has tables that are purged each day. To keep the database from growing too large, a script removes data older than 24 hours from all tables that belong to EPM. A notice is sent to the root email account (smtp).

- Script location: /etc/cron.d/epm_purge_archives.cron
- Cron entry: **`00 01 * * * root /opt/cisco/vcs/analytics/scripts/epm/epm_purge_archives.sh epm all 1`**
- To review events in the database
  `psql -C -U epm`
- To review the primary stream
  `cqdb=> select date, Cmd from endpoint_events;` (Ctrl-C to end)

```
cqdb=> select date, Cmd from endpoint_events;
            date              |     cmd
------------------------------+-------------
 2013-08-31 10:35:02.54-04    | TimeMarker
 2013-08-31 10:35:07.543-04   | TimeMarker
 2013-08-31 10:35:12.546-04   | TimeMarker
 2013-08-31 10:35:17.55-04    | TimeMarker
 2013-08-31 10:35:18.661-04   | EndpointEventNotification
 2013-08-31 10:35:22.551-04   | TimeMarker
 2013-08-31 10:35:25.685-04   | EndpointEventNotification
 2013-08-31 10:35:27.612-04   | TimeMarker
 2013-08-31 10:35:32.615-04   | TimeMarker
```

Notes:

- Heartbeat (TimeMarker): Database commit every 10 records
- Events: Database commit every 500 records

Review Derived Streams and Archive Tables

Derived stream tables for 5 s, 1 m, 5 m, 15 m, 30 m, 60 m

Example:

1 m Derived Stream — `endpoint_events_1m`

1 m Archive — `endpoint_events_1m_archive`

```
cqdb=> select * from endpoint_events_1m_archive;
      _time       | count | topicname |    cmd     | parametername | parametermin | parametermax | parametersum | eventerror | eventreason | watchname | watchcount | devicetype
------------------+-------+-----------+------------+---------------+--------------+--------------+--------------+------------+-------------+-----------+------------+------------
2013-08-30 09:53:00-04 |    12 |           | TimeMarker |               |              |              |              |            |             |           |          0 |
2013-08-30 09:54:00-04 |    12 |           | TimeMarker |               |              |              |              |            |             |           |          0 |
2013-08-22 16:45:00-04 |    12 |           | TimeMarker |               |              |              |              |            |             |           |          0 |
2013-08-22 16:45:00-04 |     3 | EPM_TOPIC_HardwareFault | EndpointEventNotification |              |              |              |            | HDDFault   | BadSector   |           |          0 |
2013-08-22 16:45:00-04 |     3 | EPM_TOPIC_ServiceError | EndpointEventNotification |              |              |              |            | ServiceURLError | N/A    |           |          0 |
2013-08-22 16:46:00-04 |     3 | EPM_TOPIC_HardwareFault | EndpointEventNotification |              |              |              |            | Reboot     | MemoryFault |           |          0 |
```

5

Customer Information

If You Have Questions

If you have technical questions, contact Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.

A

Endpoint Manager Operational Scenarios

Introduction

This appendix defines a typical set of operational scenarios that employ the Endpoint Manager.

In This Appendix

- Endpoint Manager Overview 76
- Typical Endpoint Scenarios 78

Endpoint Manager Overview

The EPM software is intended to operate on the Videoscape Control Suite platform interconnected to the other system components with XMPP. EPM provides the system configuration and lifecycle management of the software on the attached clients. In addition, EPM provides the capability to monitor the status of Endpoints and log this information for reference by an external system.

This appendix defines a number of typical scenarios that an operator will perform to manage a normal EPM system. Included in this is the monitoring of Endpoint performance, software lifecycle operations, and the set-up of groups of Endpoints to standard configurations.

Endpoint Manager Features

Endpoint Groups — Endpoint Groups allow the division of the entire population of Endpoints into subsets. This provides the capability to apply configurations to geographic areas, Endpoint types, or to specially defined test groups, i.e. "friendlies". Groups may be cascaded, one under another, to provide flexible configurations of Endpoints. Dynamic Groups use Rules to determine which Endpoint is part of a Group.

Topics — A Topic is defined as part of a data collection system where Endpoints send data that requires monitoring. Each Topic has a corresponding PubSub node to which Events, Watches, or Logs on Endpoints can publish. The associated data is recorded and handled by components of the EPM Videoscape system for access by external systems.

Endpoint Parameters — A Parameter is defined as a value in an Endpoint that needs to be monitored or configured. An example is the amount of RAM in use. Endpoint Parameters are assigned to Endpoints based upon the software resident in the Endpoint.

Endpoint Watches — A Watch is defined as a trigger that occurs when one or more conditions have been met. When a trigger occurs, the Endpoint will publish data matching the conditions to the specified PubSub. A condition is composed of a Parameter value, an operation, and a value. Conditions may be concatenated using logical operators.

Endpoint Configurations — An Endpoint Configuration is composed of one-to-N Parameters. A Configuration can be used to configure a single Endpoint or a Group of Endpoints. In addition, the capability to publish a Configuration to the PubSub associated with a Group is defined. The Configuration may be composed of the merger of high to low-level sets of Parameters.

Monitor Endpoint Performance — Endpoint Performance monitoring is used to provide data on a Parameter at a selected rate. A Parameter is selected for monitoring with an operator-defined interval, and the Endpoint will publish the data at the specified rate to a Topic PubSub. The Endpoint is responsible for the actions required to monitor the parameter and returns the information to the EPM after each interval has elapsed.

Debug — EPM provides the capability to query an Endpoint for a list of commands that are applicable to it. EPM performs the transmission of debug commands to Endpoints and receives the associated responses.

Image/Application Download — The process for distributing applications or images to the population of clients within the Videoscape system is divided into three major areas:

- Conversion of an image file into the format used by the EPM subsystem
- Loading of the file into Videoscape storage for later distribution to clients
- Signaling to the client population that images are available for download using the Videoscape Code Version Table (vsCVT)

Rule — A Rule is an expression that is composed of a Parameter, an operation, and a value, which evaluates to either True or False. Currently the Parameter list is composed of:

- TypeID
- JID
- TimeZone
- LocationCode
- BillingID
- MetadataID.

The set of operations that may be included is:

- GreaterThan
- LessThan
- EqualTo
- NotEqualTo
- StartsWith
- Contains

Typical Endpoint Scenarios

During the normal operation of the Endpoint Manager, there are sets of typical operations that will be required to be executed by an operator. This section describes these scenarios using the operations defined earlier in this guide.

Watch Creation/Deployment

These are the steps required to create and deploy a Watch to an Endpoint, and then to gather any data that is generated by the Endpoint.

1 **Create Parameter**

Reference the ***Endpoint Parameters*** (on page 16) section to perform a create operation for a new Parameter. This Parameter should correspond to a value that is defined by the vendor of the Endpoint software and must be specified by a unique name. Enter the unique name and type of the value, either integer or string.

2 **Create Topic**

Reference the ***Endpoint Topics*** (on page 27) section to perform a create operation for a new Topic. Specify the name and description.

3 **Create Watch**

Reference the ***Endpoint Watches*** (on page 28) section to perform a create operation for a new Watch. Specify a unique name for the Watch and optionally enter a description. Using the drop-down list, select the Topic created in the last step. Define a logical operation using the Parameter created in the first step. For example, this operation can include equality/inequality with respect to a value.

4 **Deploy Watch to Endpoint**

Reference the ***Endpoint Settings*** (on page 29) section to perform a deploy operation for the Watch that was created in the previous step. Select the Endpoint that is to receive the Watch by entering the Endpoint ID. Select from the list of available Watches the Watch created in the last step and have the EPM deploy it to the Endpoint.

5 **Alternate Deploy Watch to a Group**

Reference the ***Endpoint Watches*** (on page 28) section to perform a deploy operation for the Watch that was created. Select the Publish Watch and then from the drop-down list, select the Group that is to receive the Watch.

6 **Access Watch Data**

Reference the ***Endpoint Notification Access*** (on page 51) section to see any data that may have been generated by the Watch. Select an existing Topic, and for the log source, select “Watch”. Select a time interval to examine for entries by entering a start and stop time. Because a Watch only generates data when the condition is true, there may be no data present.

Event Data Collection

These are the steps required to create the Topic used to gather data that is generated by an Endpoint Event. Events are defined by the vendor of the Endpoint software and include a predefined, well-known Topic value.

1 **Create Topic**

Reference the ***Endpoint Topics*** (on page 27) section to perform a create operation for a new Topic. Specify the Name value that is part of the software embedded in the Endpoint, and, if needed, a Description.

Note: The Event will be active as soon as an Endpoint is part of the system, but data will only be collected when a corresponding Topic is created.

2 **Access Event Data**

Reference the ***Endpoint Log Access*** (on page 51) section to see any data that may have been generated by the Event. Select an existing Topic, and for the log source select "Event." Select a time interval to examine for entries by entering a start and stop time. Because an Event only generates data when the condition is true, there may be no data present.

Log Performance Creation/Deployment

These are the steps required to create and deploy a Log Performance data monitor to an Endpoint, and then to examine any data that is generated by the Endpoint.

1 **Create Parameter**

Reference the ***Endpoint Parameters*** (on page 16) section to perform a create operation for a new Parameter. This Parameter should correspond to a value that is defined by the vendor of the Endpoint software, and must be specified by a unique name. Enter the unique name and type of the value, either integer or string.

2 **Create Topic**

Reference the ***Endpoint Topics*** (on page 27) section to perform a create operation for a new Topic. Specify the name and description.

3 **Deploy Log Performance to Endpoint**

Reference the ***Endpoint Settings*** (on page 29) section to perform an edit operation for an existing Endpoint. Select the Endpoint that is to have a Performance Parameter monitored by entering the Endpoint ID. Select the Parameter created in the first step from the drop-down list. Select the Topic created in the previous step from the drop-down list. Enter an interval between samples, in milliseconds.

Important: If the update interval is very short and/or a large number of Endpoints are selected, then a very large amount of data will be generated.

4 **Access Log Performance Data**

Reference the ***Endpoint Log Access*** (on page 51) section to see any data that may have been generated by the Log Performance. Select an existing Topic, and for the log source, select "Log Performance." Select a time interval to examine for entries by entering a start and stop time. If no data is present, then either the interval selected is prior to the start of the Log Performance, or the update rate is very slow.

Dynamic Group Creation

These are the steps required to create a Dynamic Group, and to allocate Endpoints to it.

1 **Create Group Rule(s)**

Reference the ***Endpoint Group Rules*** (on page 21) section to perform a create operation for each new Rule required to define a Group. Select a parameter from the drop-down list, then an operation, and finally a value to complete the Rule expression. Give each Rule a unique name with an optional description.

2 **Create Group**

Reference the ***Endpoint Groups*** (on page 23) section to perform a create operation for a new Dynamic Group. Select one or more of the Rules defined in the previous step and add them to the Select Rules area. Give each Group a unique name, with an optional description.

Note: The Dynamic group created will be the product of the Rules selected. Each Rule that is added will narrow the number of Endpoints contained in the Dynamic Group.

3 **Activate Dynamic Group**

Reference the ***Endpoint Groups*** (on page 23) section to perform an activate operation for an existing Dynamic Group. Select the Dynamic Group created in the last step. Click on the **Activate/Deactivate** button for this Group. The EPM will begin determining which Endpoints from the entire population are a member of the Dynamic Group.

Simple Configuration

These are the steps required to create and deploy a Configuration to an Endpoint.

1 **Create Parameter**

Reference the ***Endpoint Parameters*** (on page 16) section to perform a create operation for a new Parameter. This Parameter should correspond to a value that is defined by the vendor of the Endpoint software, and be specified by a unique name. Enter the value to which to set the Parameter. Enter the unique name and type of the value, either integer or string.

2 **Create Configuration**

Reference the ***Endpoint Configurations*** (on page 17) section to perform a create operation for a new Configuration. This Parameter should correspond to a value that is defined by the vendor of the Endpoint software, and must be specified by a unique name. Enter the unique name and type of the value, either integer or string.

3 **Associate Configuration with Endpoint**

Reference the ***Endpoint Settings*** (on page 29) section to perform an edit operation for an existing Endpoint. Add the Configuration created in the previous step to the Endpoint.

4 **Configure Endpoint**

Reference the ***Endpoint Settings*** (on page 29) section to transmit the Configuration to the Endpoint selected in the previous step. The Endpoint will receive a message with the Configuration value and perform the indicated Setting.

Simple Configuration -- Published

These are the steps required to create and deploy a Configuration to a group of Endpoints.

1 **Create Parameter**

Reference the ***Endpoint Parameters*** (on page 16) section and perform a create operation for a new Parameter. This Parameter should correspond to a value that is defined by the vendor of the Endpoint software and be specified by a unique name. Enter the value to which to set the Parameter. Enter the unique name and type of the value, either integer or string.

2 **Create Configuration**

Reference the ***Endpoint Configurations*** (on page 17) section and perform a create operation for a new Configuration. Enter the unique name and type of the value, either integer or string.

3 **Select Configuration**

Reference the ***Endpoint Groups*** (on page 23) section and select a Group from the list of those available. Then, click on the Edit icon. From the Available Configurations window, select the one created in the previous step and click on Add. Then **save** the Group information.

4 **Publish Configuration**

Reference the ***Endpoint Groups*** (on page 23) section and select the Group that has the Configuration associated with it. Click on the **Publish Configuration** icon. This will send the Configuration to the PubSub associated with the Group and distribute it to all the Endpoints in the Group.

5 **Unpublished Configurations**

In the ***Endpoint Groups*** (on page 23) section there is a list of unpublished Configurations. These correspond to Configurations that have been associated with a Group, but not pushed down to the PubSub for distribution to the Endpoints.

Cancel Configuration

These are the steps that are required to remove a Configuration that has been published to a group of Endpoints.

1 **Cancel Configuration**

Using the ***Endpoint Groups*** (on page 23) section, select the Group from the previous ***Simple Configuration - Published*** (on page 81). Click on the **Cancel Configuration** icon. This will send a Cancel message to the PubSub associated with the Group and distribute it to all the Endpoints in the Group.

2 **Endpoints**

The Endpoints will receive the Cancel message and delete all references to the Configuration and its associated Parameter settings.

Complex Configuration

These are the steps required to configure a group of Endpoints using more than one Configuration. This example will apply them to the Endpoints associated with multiple Groups.

1 **Create Group Rules**

Reference the ***Endpoint Group Rules*** (on page 21) section to perform a create operation for a Rule that defines TypeID equal to "X." Give this Rule a unique name, with an optional description.

2 **Create Groups**

Reference the ***Endpoint Groups*** (on page 23) section to perform a create operation for a new Dynamic Group. Select the first Rule defined in the previous step and add it to the Select Rules area. Give the Group a unique name, with an optional description.

3 **Create Parameter**

Reference the ***Endpoint Parameters*** (on page 16) section and perform a create operation for a new Parameter. This Parameter should correspond to a value that is defined by the vendor of the Endpoint software and be specified by a unique name. Enter the value to which to set the Parameter. Enter the unique name and type of the value, either integer or string.

4 **Create Configuration**

Reference the ***Endpoint Configurations*** (on page 17) section and perform a create operation for a new Configuration. Enter the unique name and type of the value, either integer or string.

5 **Select Configuration**

Reference the ***Endpoint Groups*** (on page 23) section and select the Dynamic Group from step 2. Then click on the **Edit** icon. From the **Available Configurations**, select the one created in the previous step and click **Add**. Then, **Save** the Group information.

6 **Create Second Configuration**

Repeat steps 3 through 5 with a different Parameter name.

7 **Activate Dynamic Groups**

Reference the ***Endpoint Groups*** (on page 23) section to perform an activate operation for both Dynamic Groups. Select the Dynamic Groups created in the previous step. Click on the **Activate/Deactivate** button for each Group. The EPM will begin determining which Endpoints from the entire population are a member of each Dynamic Group.

8 **Publish Configuration**

Reference the ***Endpoint Groups*** (on page 23) section and select the Group that has the Configurations associated with it. Click on the **Publish Configuration** icon. This will send the Configurations to the PubSub associated with the Group and distribute it to all the Endpoints in the Group.

Image Download

These are the steps required to load an image into the Endpoint Manager and to signal its availability to a set of Endpoints.

1 **Load Image**

Reference the ***Endpoint Application Images*** (on page 45) section to perform an upload operation. If the Image is correctly formatted with the proper manifest then it will be successfully loaded into the application image list.

2 **Create Group Rule(s)**

Reference the ***Endpoint Group Rules*** (on page 21) section to perform a create operation for each new Rule required to define a Group. Select a parameter from the drop-down list, then an operation, and finally a value to complete the Rule expression. Give each Rule a unique name, with an optional description.

3 **Create Group**

Reference the ***Endpoint Groups*** (on page 23) section to perform a create operation for a new Dynamic Group. Select one or more of the Rules defined in the previous step and add them to the Select Rules area. Give each Group a unique name, with an optional description.

Note: The Dynamic group created will be the product of the Rules selected. Each Rule that is added will narrow the number of Endpoints contained in the Dynamic Group.

4 **Activate Dynamic Group**

Reference the ***Endpoint Groups*** (on page 23) section to perform an activate operation for an existing Dynamic Group. Select the Dynamic Group created in the previous step. Click on the Activate/Deactivate button for this Group. The EPM will begin determining which Endpoints from the entire population are a member of the Dynamic Group.

5 **Associate Image to Group**

Reference the ***Endpoint Application Images*** (on page 45) section to select the image loaded in the first step. Perform the association operation for the Group defined in the third step. The EPM will update (or, if needed, create) the vsCVT associated with the Group.

6 **Publish vsCVT to Group**

Reference the ***Endpoint Application Images*** (on page 45) section to select the image loaded in the first step. Select the vsCVT created in the previous step and associated with the Group from the second step. Enter the download Type and a download time window for the Endpoints in the Group to attempt to retrieve the Image. This vsCVT will be published to the PubSub that is part of the Group.

7 **Image Retrieval**

As specified in the vsCVT, the Endpoints will retrieve the Image from the EPM.

Endpoint Restore

These are the steps that are used to trigger an Endpoint to match the Configuration data that EPM has for it.

1 **Select Endpoint**

Reference the ***Endpoint Settings*** (on page 29) section and enter either an Endpoint ID or an Endpoint JID value.

2 **Command Restore**

On the Endpoint Settings page, select the **Restore** button.

3 **Endpoints**

The Endpoints will receive the Restore message;= and delete all references to all Configurations. Then, the Endpoint will receive the Configurations associated with any Group that the Endpoint is part of and the Configurations assigned specifically to it.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

http://www.cisco.com
Tel: 408 526-4000
800 553-6387
Fax: 408 527-0883

January 2014

Part Number OL-27000-04