Videoscape Control Suite Alert Manager Service

Configuration 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.

Open Source GNU GPL Statement

Cisco *Alert Manager* and *Videoscape Control Suite* contain(s), in part, certain free/open source software ("Free Software") under licenses which generally make the source code available for free copy, modification, and redistribution. Examples of such licenses include all the licenses sponsored by the Free Software Foundation (e.g. GNU General Public License (GPL), GNU Lesser General Public License (LGPL), Berkeley Software Distribution (BSD), the MIT licenses and different versions of the Mozilla and Apache licenses). To find additional information regarding the Free Software, including a copy of the applicable license and related information, please refer to the product Licensing Information on **www.cisco.com**. If you have any questions or problems accessing any of the links, please contact: **spvtg-external-opensource-requests@cisco.com**.

Copyright

Contents

About This Guide

Introduction

This document contains configuration information for the Cisco Videoscape Control Suite (VCS) Alert Manager service for versions 2.1/2.5/3.0 of the VCS.

The Federal Communications Commission (FCC), the National Weather Service, and national and local authorities send emergency alert messages (EAMs) to service providers who broadcast these messages to television subscribers. These messages include regular tests of the Emergency Alert System (EAS), as well as messages that warn of dangerous conditions such as thunderstorms, floods, tornadoes, hurricanes, and earthquakes.

The FCC requires that service providers receive and send EAMs. In addition, the FCC requires that service providers conduct weekly and monthly tests of the EAS. By conducting weekly and monthly tests of the EAS, service providers ensure the reliability of their EAS equipment so that subscribers can receive national, state, and local warning messages about emergency situations.

Important: The parameter values displayed in this document are for example only; your specific setup might be different based on your database cluster.

Purpose

The Alert Manager is a service that runs on the Videoscape™ Conductor™, and is managed using the Conductor Management Console (CMC). After reading this guide, you will be able to configure, operate, maintain, and test EAS components on the Videoscape Control Suite using the Alert Manager.

Properly configuring, maintaining, and testing your system lets you follow FCC regulations by receiving and then sending EAMs to subscribers through a correctly configured and fully automatic EAS process. If your system does not perform as expected, this guide also includes a troubleshooting section so that you can quickly restore your system to full operation.

Terminology

There are two types of Emergency Alert Controllers (EACs) that you need to configure for EAS:

- The first is the physical unit that actually receives and processes the EAS messages from the issuing authority (federal government, state government, NOAA, etc) then forwards the messages to the Alert Manager. In this document, this EAC is referred to as the *physical EAC*. These are the external units manufactured by various companies, such as Trilithic and Monroe.
- The second is the logical entity within the CMC/Alert Manager that allows the Alert Manager to filter messages it receives from the physical EAC. In this document, this EAC is referred to as the *Alert Manager EAC*.

Audience

This document is written for operators of systems that use the VCS and EAS. System operators, field service engineers, and Cisco® Services engineers may also find the information in this document helpful.

Document Version

This is the third formal release of this document, which was revised for Videoscape Control Suite 3.0.

1

Alert Manager Configuration

Introduction

This section details the steps you need to take to configure the Alert Manager.

In This Chapter

Overview AM Configuration

This section describes the steps you need to take to configure the Alert Manager for EAS. You should perform these steps in the order presented:

1. ***Configure Your Physical EAC*** (on page 9)
2. ***Log Into the Management Console UI*** (on page 10)
3. ***Create the PubSub Nodes*** (on page 11)
4. ***Create the Alert Manager EAC*** (on page 13)
5. ***Create the Listeners*** (on page 15)
6. ***Configure the Common Alerting Protocol Parameters*** (on page 20)
7. ***Verify the End-to-End Alert Manager Configuration*** (on page 23)

Configure Your Physical EAC

You need to configure your physical EAC so it can communicate with the Alert Manager. The physical EAC is the external controller manufactured by companies, such as Trilithic and Monroe.

Use the documentation that came with your EAC to configure a port and IP address to be used to send EAS messages to the Alert Manager.

Notes:

- The port that you use for EAS must be between 1024 and 4097, or between 4099 and 65535. Port 4098 is reserved for DVS/168 messages.
- Before configuring the Alert Manager, set your log to **TRACE**. See ***Changing Logging Levels*** (on page 47) for information on how to set logging levels.

Log Into the Management Console UI

1. Open a supported browser (Internet Explorer 8 or 9, or Firefox 5).
2. Type the following command in the address bar and press **Enter**:
   `https://[CMC IP address]/webacs`
   Example: `https://10.90.180.241/webacs`
   Result: The Control Suite Management login page opens.

3. Type the administrator **User Name** and **Password** and click **Login** to log into the management console.

Create the PubSub Nodes

The PubSub nodes define the geographic restrictions (similar to FIPS codes) that filter and send EAS messages only to targeted states, counties, or subdivisions. The clients receive the EAS messages appropriate for their location when those clients are registered to a PubSub node, either directly or through the Alert Manager.

Before You Begin

Before you begin to create the PubSub nodes, you need the following information:

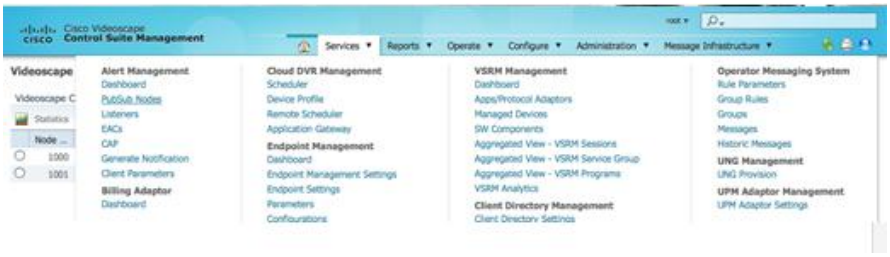
- The name of the PubSub node
- Whether this is a national node or not

  Note: You can only have one national node in your system.
- The location that this node will service (state/major, county/minor, subdivision), if applicable

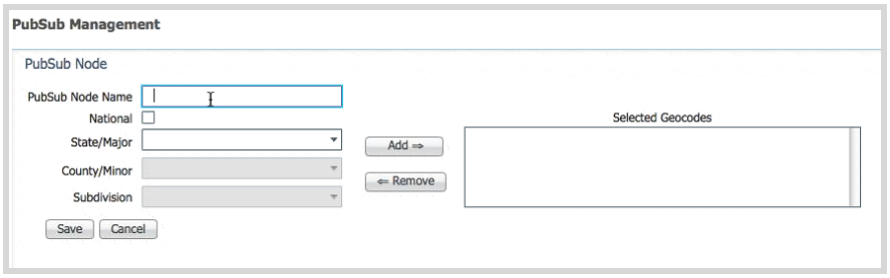
If you make an error by entering an unsupported value in any field, saving the PubSub will fail and a message will display on the screen.

Creating the PubSub Nodes

1 In the CMC, click **Services > Alert Management > PubSub Nodes**.



2 Click **Create**.



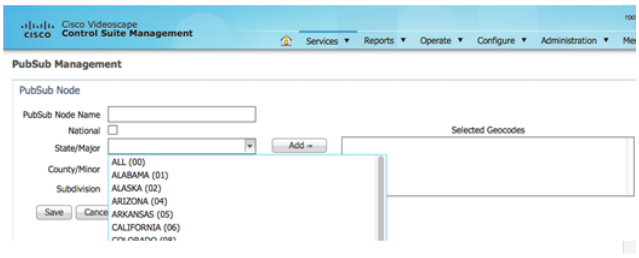
3 Enter and select the information specific to this node depending upon whether the Location Code Type is SGC (Canadian) or FIPS (US).

- **PubSub Node Name**

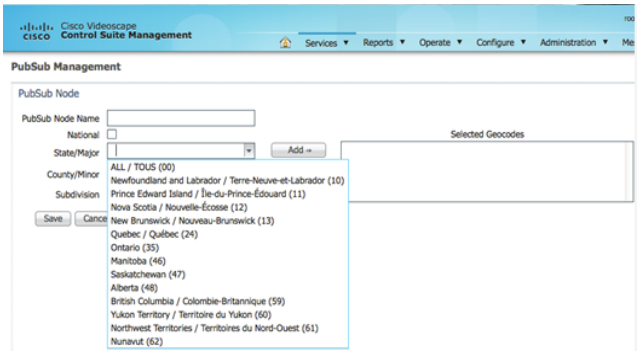
  Note: Names are case-sensitive. Be sure to use a name that corresponds to your site's naming conventions.
- **National** (you can only have one National PubSub node in your system)
- **State/Major**
- **County/Minor**
- **Subdivision**

Examples:

FIPS



SGC

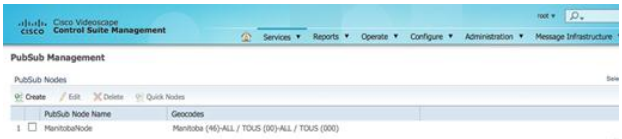


4 When you are finished, click **Add** to move the node to the **Selected Geocodes** list.

5 Click **Save**. The new node appears in the PubSub Nodes list.

- FIPS

- SGC



6 Continue to create other nodes as required.

Create the Alert Manager EAC

The Emergency Alert Controller (EAC) on the Alert Manager allows the Alert Manager to filter messages it receives for EAS messages.

Before You Begin

Before you begin to create the Alert Manager EAC, you need the following information:

- The incoming Alert Protocol (SCTE-18, DVS-168 or CAP)
- The name of the Alert Manager EAC
- The physical EAC IP address
- The URL of the content passed to the client if the client must be force tuned
- The name of the CDN server that holds the audio and/or image file (if applicable)

  Note: The Alert Manager is able to support both overlay and force-tune messages. In the overlay case, audio files (wav, mp3, wma) and image files (jpeg, png) will be delivered to clients via HTTP download over the customers' CDN. The Alert Manager serves as the origin server of these audio and image files.
- The Delivery Protocol (if applicable – HTTP or HTTPS for CAP, only)

If you make an error by entering an unsupported value in any field, saving the EAC will fail and a message will display on the screen.

Creating the Alert Manager EAC

1 In the CMC, click **Services > Alert Management > EACs**.

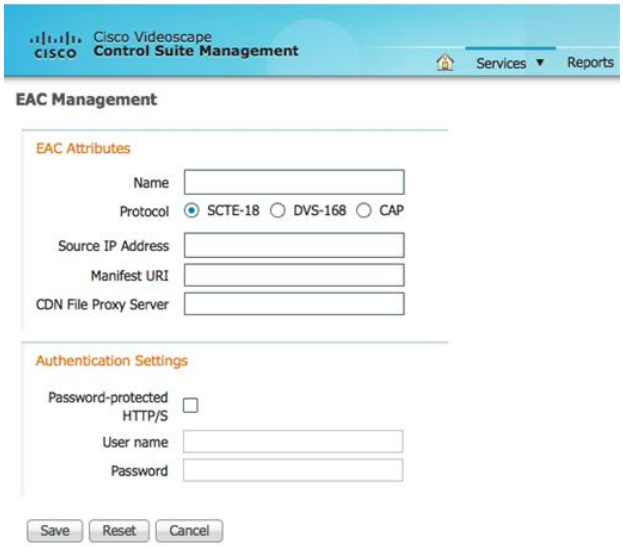
2 Click **Create**. The EAC Management window opens.

3 Enter and select the information specific to this EAC:

- **Name**

  Note: Names are case-sensitive. Be sure to use a name that corresponds to your site's naming conventions.
- **Source IP Address** — The physical EAC IP address
- **Manifest URI** — The URL passed to the client when force-tuned
- **Protocol** — The Alert Message protocol (SCTE-18, DVS/168 or CAP)
- **Audio File Proxy Server Name** — For systems using a CDN, the name of the CDN server (optional)
- **Authentication Settings** — Applicable only to CAP ingest, and not SCTE-18 or DVS-168. This allows the Alert Manager to authenticate the EAC device and is required for HTTP, but is optional for HTTPS.

  Example: In this example, the SCTE-18 protocol has been selected.



4 Click **Save**. The new EAC appears in the EAC Nodes list.

Create the Listeners

The function of the listener is to monitor the EAC for EAS messages and make sure that the Alert Manager is aware of these messages. You need to create a listener for each of the available protocols. This is only applicable to SCTE-18 and DVS-168. Listener creation is not required for CAP ingest. Therefore, this section does not pertain to CAP ingest scenarios.

Before You Begin

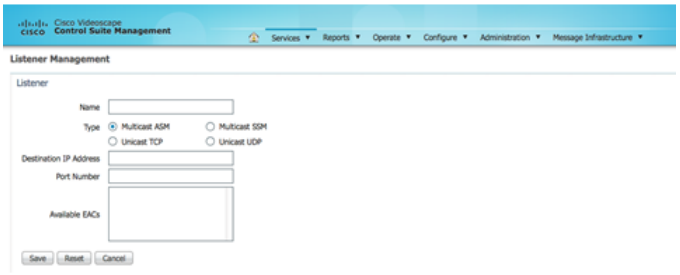
Before you begin to create the listener, you need the following information:

- The name of the listener for each of the following listener types:
  - **Multicast ASM** — Multicast any-source multicast; multiple senders on the same channel
  - **Unicast TCP** — Unicast transmission control protocol; reliable unicast messaging
  - **Multicast SSM** — Multicast source-specific multicast; the multicast source is specified
  - **Unicast UDP** — Unicast user datagram protocol; point-to-point messaging over the UDP protocol
- The IP address of the physical EAC
- The port number of the physical EAC
- The name of the Alert Manager EAC you created in the previous procedure (optional for ASM)

If you make an error by entering an unsupported value in any field, saving the listener will fail and a message will display on the screen.

Creating the Listeners

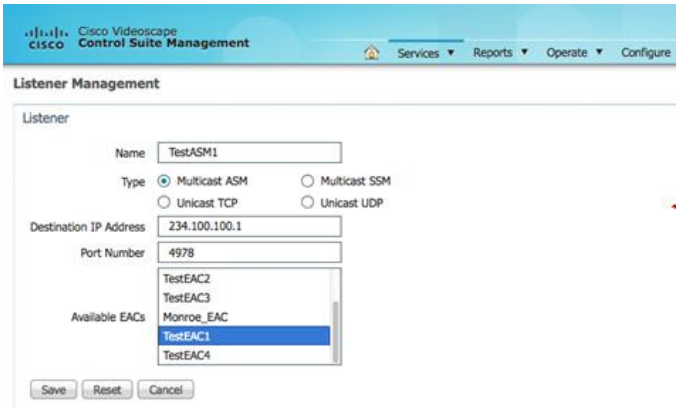
1. In the CMC, click **Services > Listeners**.
   Result: The Listener Management Listener List window opens.
2. Click **Create**. The Listener Management window opens.



3. Create the specific listener you desire by referencing one of the following sections.

Multicast ASM Listener Option

1. In order to create a Multicast ASM Listener, enter the following information specific to this listener:
   - **Name**
     Note: Names are case-sensitive. Be sure to use a name that corresponds to your site's naming conventions.
   - **Type** — Select the **Multicast ASM** option
   - **Destination IP Address** — The IP address of the Alert Manager
   - **Port Number** — The port number of the Alert Manager
   - **Available EACs** — Select the Alert Manager EAC you created previously (optional)

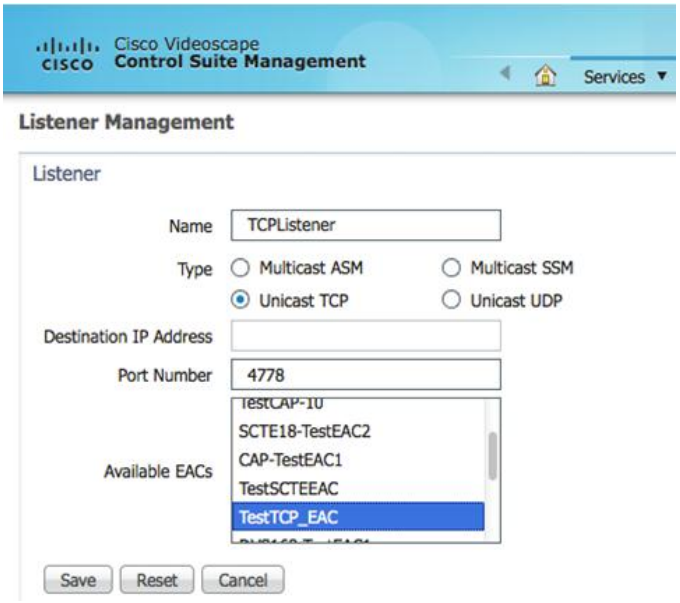


2. Click **Save**.

Unicast TCP Listener Option

1 In order to create a Unicast TCP Listener, enter the following information specific to this listener:

- **Name**
- **Type** — Select the **Unicast TCP** option
- **Destination IP Address** — The IP address of the Alert Manager
- **Port Number** — The port number of the Alert Manager
- **Available EACs** — Select the Alert Manager EAC you created earlier



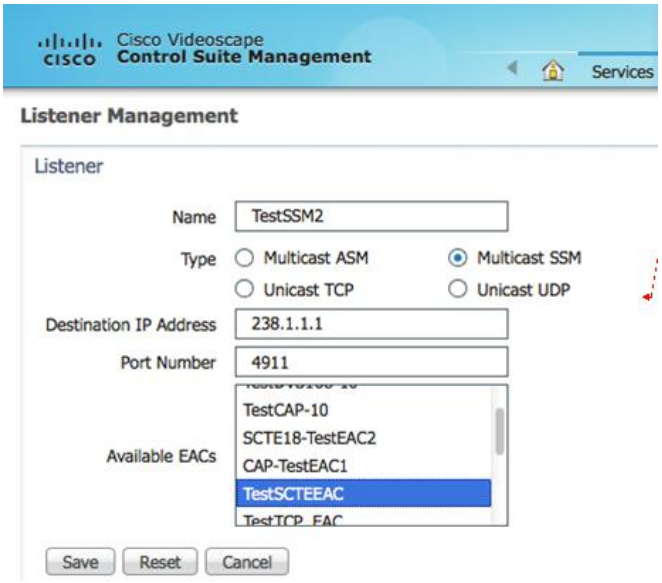
2 Click **Save**.

Multicast SSM Listener Option

1 In order to create a Multicast SSM Listener, enter the following information specific to this listener:

- **Name**

  Note: Names are case-sensitive. Be sure to use a name that corresponds to your site's naming conventions.
- **Type** — Select the **Multicast SSM** option
- **Destination IP Address** — The IP address of the Alert Manager
- **Port Number** — The port number of the Alert Manager
- **Available EACs** — Select the Alert Manager EAC you created earlier



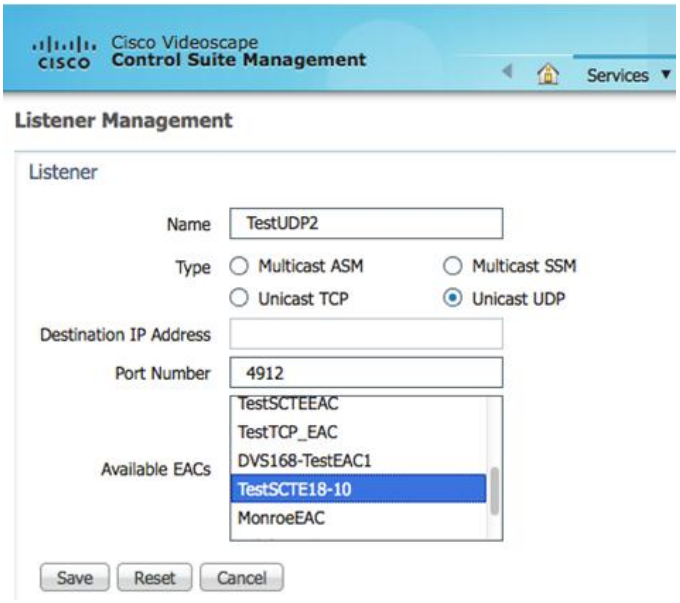
2 Click **Save**.

Unicast UDP Listener Option

1 In order to create a Unicast UDP Listener, enter the following information specific to this listener:

- **Name**

  Note: Names are case-sensitive. Be sure to use a name that corresponds to your site's naming conventions.
- **Type** — Select the **Unicast UDP** option
- **Port Number** — The port number of the Alert Manager
- **Available EACs** — Select the Alert Manager EAC you created earlier



2 Click **Save**.

Configure the Common Alerting Protocol Parameters

The Common Alerting Protocol (CAP) provides an open, non-proprietary, digital message format for all types of alerts and notifications. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task.

Alert Manager converts the SCTE-18 and DVS/168 EAS messages that it receives into the CAP 1.2 XML format for distribution.

The CAP window allows you to customize certain CAP parameters that might not be contained in the EAMs when they arrive from the physical EAC. The CAP configuration is not required for alerts that are ingested when already in CAP or CAP-CP format. This is because the required parameters are already present, unless some of the CAP parameter values may need to be changed for the CAP XML message going to the client. For example, a resource field may need to be changed by Alert Manager.

In a deployment where the ECS is downstream of Alert Manager, there exists an install flag to indicate the presence of an ECS. When this is the case, a dedicated Pubsub node (ECSnode) is hard-coded for ECS and Alert Manager publishes all CAP-CP messages to the ECS PSN over XMPP.

In addition, CAP-CP messages may also be published to any additional UI-configured PSN(s).

Before You Begin

Before you begin to create a CAP customization, you need the following information:

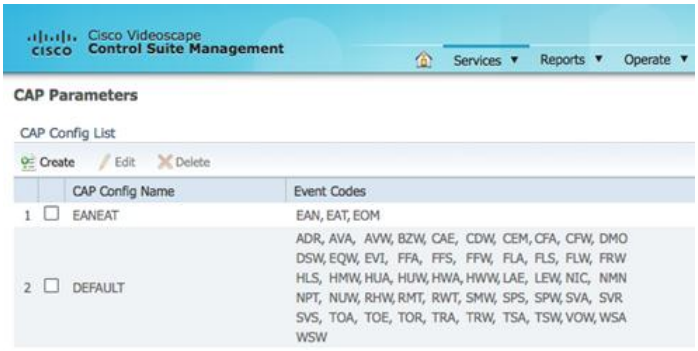
- CAP configuration name
- Alert Remaining Time
- Scope
- Restrictions
  Note: Required only if Scope is set to Restricted, and a list of exceptions exists.
- Addresses
  Note: Required only if Scope is set to Private.
- Resource description
- Alert priority

- Force tune (determines whether this event code will force the client to tune to a different channel)
- Category
- Urgency
- Severity
- Certainty
- Event codes related to this CAP customization

Configure the CAP Parameters

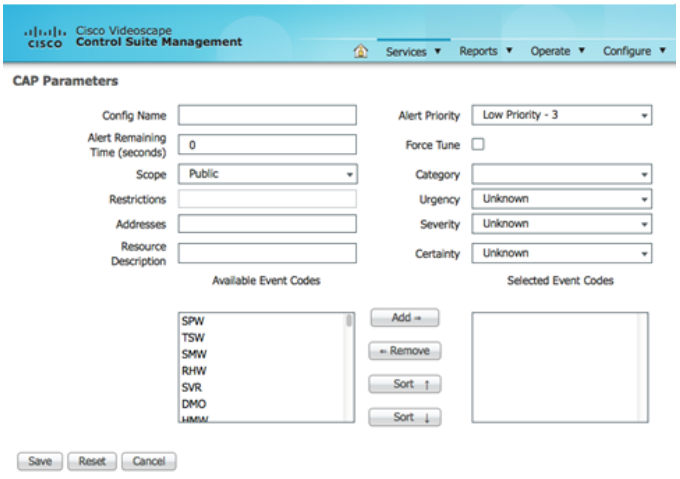
1 On the CMC, click **Services > CAP**.

Result: The CAP Parameters window opens.



Note: You cannot edit the DEFAULT and EANEAT CAP configurations because they are created during installation to make sure the system has data with which to start, even if there is no human intervention. Also, the EANEAT configuration represents the national alerts that are mandatory and should not be modified.

2 Click **Create**.



3 Configure the following CAP parameters for the CAP XML message going to the client.

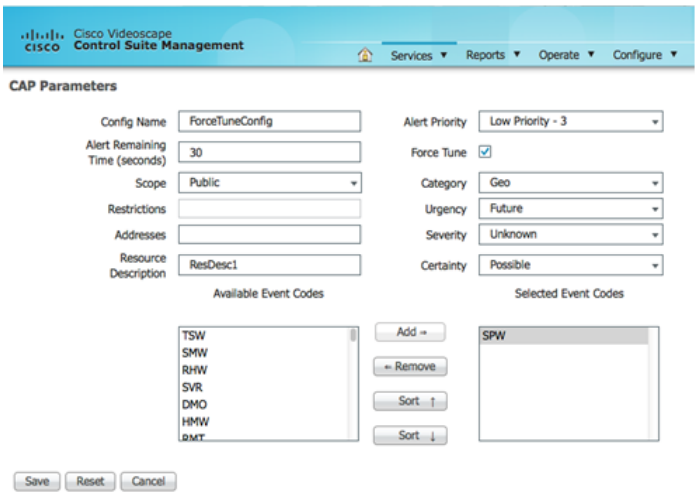
- **Config Name**
- **Alert Remaining Time (seconds)**
- **Scope**
- **Restrictions**
- **Addresses**
- **Resource Description**
- **Alert Priority**
- **Force Tune** (optional; select only if you want the event code to force tune the client)
- **Category**
- **Urgency**
- **Severity**
- **Certainty**

4 Select the **Event Codes** for this customization in the **Available Event Codes** list. Press and hold the **Ctrl** button on your keyboard to select multiple codes.

5 Click **Add** to move the codes into the **Selected Event Codes** list.

6 Click **Save**.

Example: The following example has **Force Tune** selected.



Verify the End-to-End Alert Manager Configuration

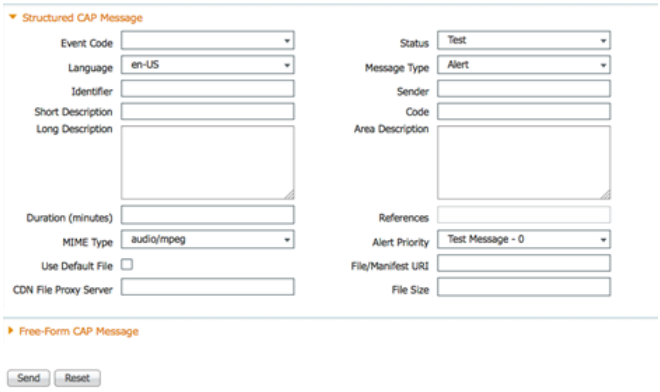
You can verify the Alert Manager configuration by creating a user notification using either the Structured CAP Message template or Free-Form CAP Message template in which you enter your own CAP parameters.

Verifying the Configuration by Sending a User Notification

You can verify the Alert Manager configuration by creating a user notification.

1. On the CMC, click **Services > Alert Management > Generate Notification**.
2. Select a PubSub Node.

3. Enter the other required data using the Structured CAP Message template.



4. Click **Send** and verify that the operation is successful by checking the alertManager.log file. If the log level is set to TRACE, you should see an entry similar to the following:

```
2012-08-20 14:09:27,474 DEBUG  AlertManagerUserNotification.sendNote:
Published to node GeorgiaNode
```

Note: For information on setting logging levels, see ***Changing Logging Levels*** (on page 47).

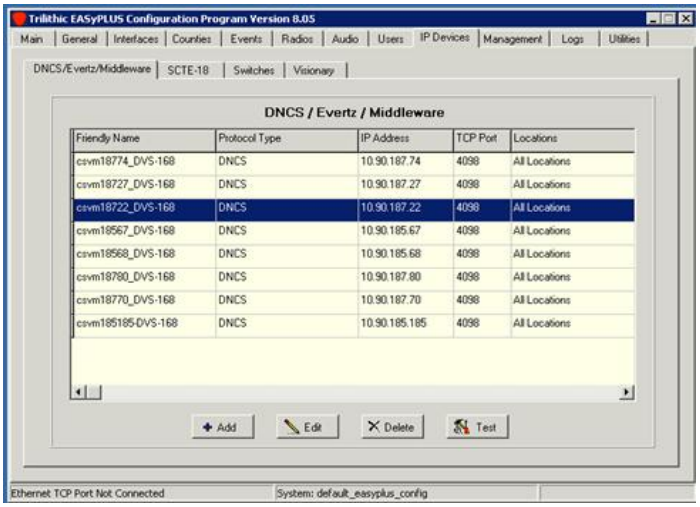
Verifying the Configuration by Sending a Message from the Physical EAC

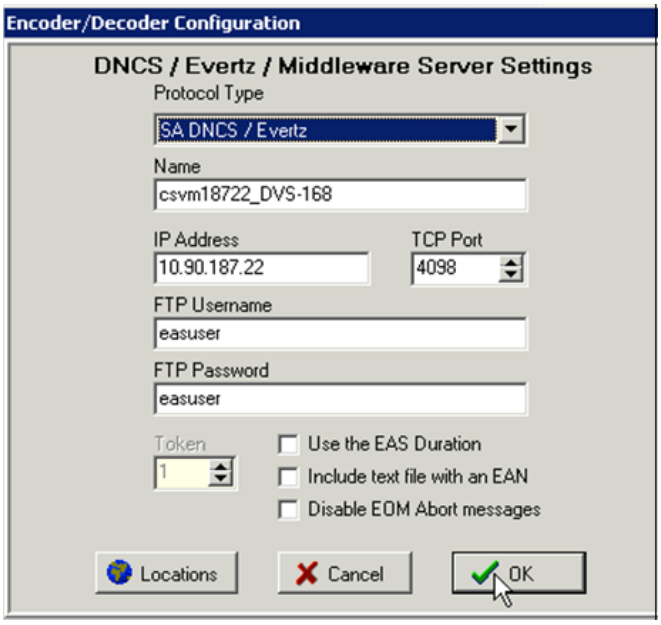
For a complete end-to-end test, you need to send a message from your physical EAC and confirm the following:

- That the message published to the appropriate PubSub nodes
- That the **Long Description** is displayed on the client machines that are subscribed to those PubSub nodes

DVS-168

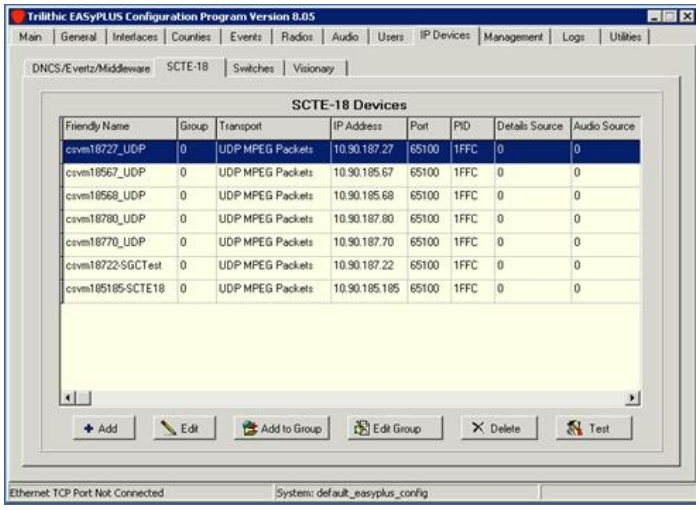
The DVS-168 screenshots that follow provide an example of the Trilithic configuration.

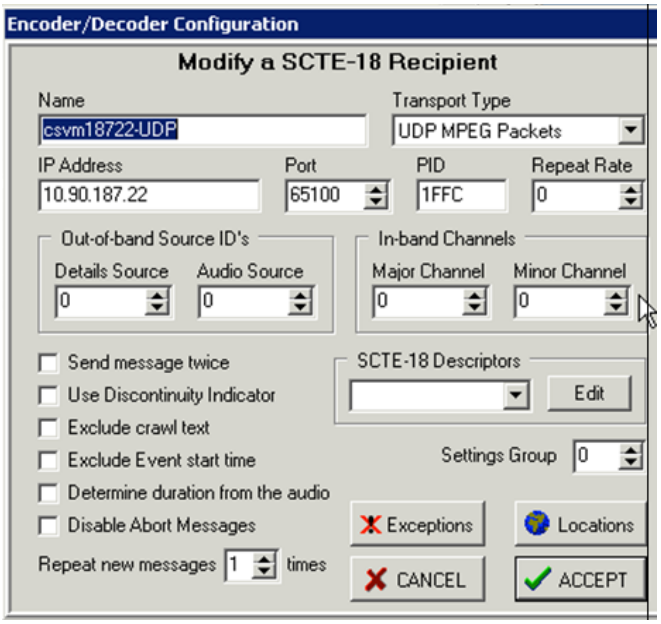




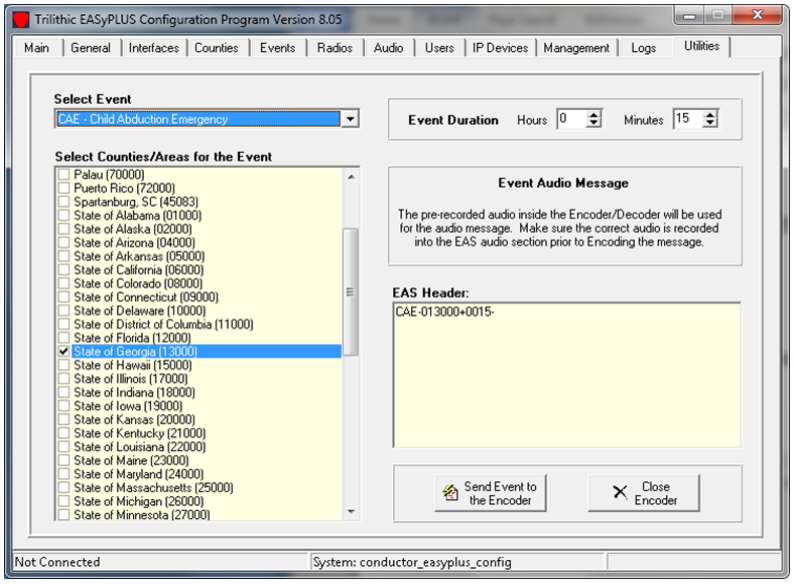
SCTE-18

The SCTE-18 screenshots that follow provide an example of the Trilithic configuration.



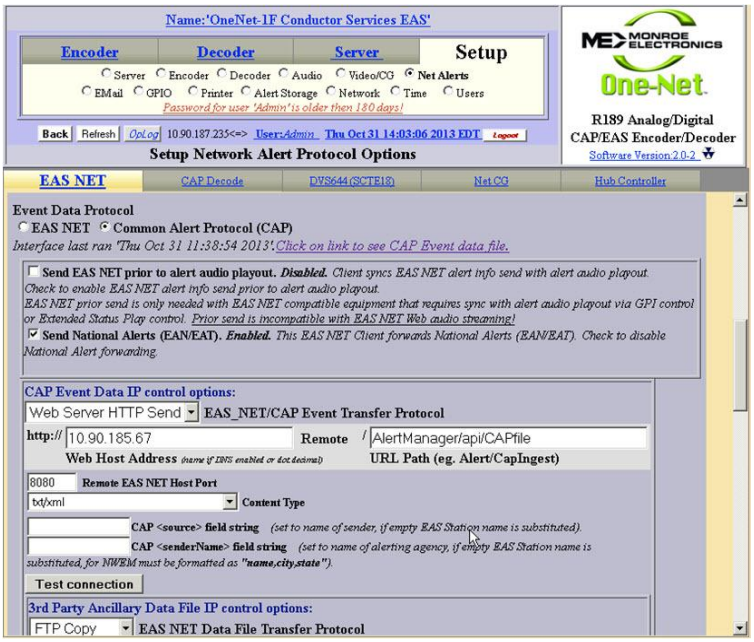


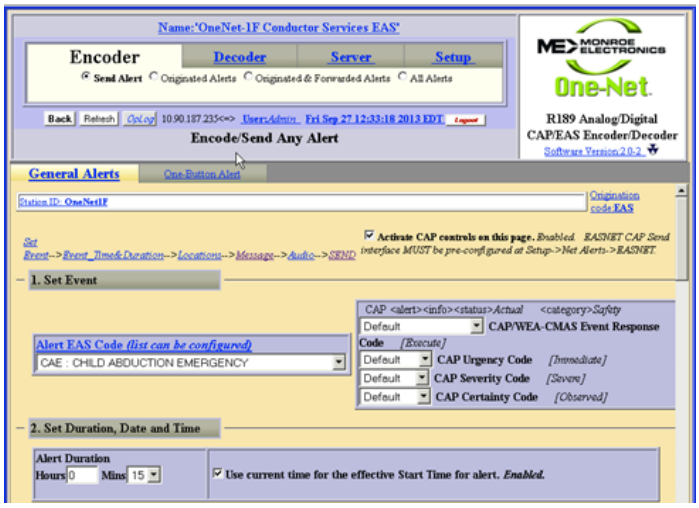
The following screen allows the operator to select the FIPS code(s) that need to be included in the outgoing EAS message.

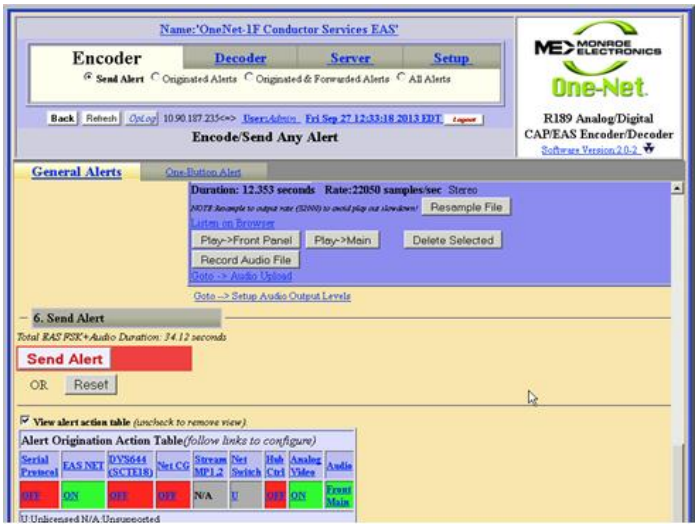


CAP

The CAP screenshots that follow provide an example of the Monroe configuration.







To learn how to change logging levels in the Alert Manager, see ***Changing Logging Levels*** (on page 47).

Verifying the Configuration Using the Psi Client

Psi is a client used to connect to the Jabber Instant Messaging network. You can use Psi to test the end-to-end EAS functionality in your system.

1. Download and install the Psi client from www.psi-im.org.
2. If you haven't already, create a PubSub on the Alert Manager for testing.
3. Create a user in the Psi client:
   a. Add an account (for example, **easuser**).
   b. Edit the account properties:
      i. Add the **Jabber ID** (JID): **easuser@[CMC Host Name].com**
      ii. Add the CMC **Password**.
      iii. Click the **Connection** tab.
      iv. Select the **send keep alive** option.
      v. Select the **manual specify host server ip/port** option.
      vi. Enter the CMC host IP address; make sure that you use port **5222**.
4. On the Psi client, open the user and enable it.

5 Open the XML console and create the following message:

```
<iq type='set'
  to='pubsub.features'
  id='sub1'>
  <pubsub xmlns="http://jabber.org/protocol/pubsub'>
  <subscribe
    node='[PubSub name that you created for this test]'
    jid='easuser@[CMC Host Name].com'/>
  </pubsub>
</iq>
```

6 Transmit the message. You should see a **success** response from the CMC. If you do not receive this message, verify the Psi client settings.

7 On the CMC, select **Service > Alert Management** and click **Generate Notification**.

8 Select the **PubSub** you created for this test.

9 Send a notification. You should see the results in the Psi XML console.

Note: See *Perform an Adhoc Test* (on page 32) for more information on sending a notification.

2

Perform Tests

Introduction

This chapter contains the procedures specific to creating and performing tests of the EAS.

In This Chapter

Perform an Adhoc Test

An adhoc test allows you to test connectivity in your EAS system.

Performing an Adhoc Test

1. In the Conductor Manager, click **Services > Alert Managment > Generate Notification**.
2. Select the **PubSub Node** that you want to send the message to.
3. In the **Event Code** field, select **DMO - Practice/Demo Warning**.
4. In the **Short Description** field, type a few words to describe the test.
5. In the **Long Description** field, type the text of the message.
6. In the **Duration** field, type how long you want the message to display. You can enter from 1 to 1440 minutes.
7. When you have finished configuring the message, click **Send**. You should see the text you entered in the **Long Description** field appear on the client screens.

Perform a Required Weekly Test

The FCC requires system operators to conduct weekly and monthly tests of their EAS. These tests ensure the reliability of the EAS equipment so that subscribers will receive national, state, and local warning messages about emergency situations.

The procedures in this section provide you with instructions for configuring your VCS to perform regular tests of your EAS.

Note: The VCS and FCC use the following acronyms to refer to the mandated tests of the EAS:

- **RWT:** Required Weekly Test
- **RMT:** Required Monthly Test

Weekly tests consist of transmitting the EAS digital header codes and end of message (EOM) codes once per week. Weekly tests must be conducted by EAS participants on different days and at different times.

No weekly test is necessary during the week that a monthly test is conducted or when there is an EAS activation for a state or local emergency.

Performing a Required Weekly Test

1. In the CMC, click **Services > Alert Management > Generate Notification**.
2. Select the national **PubSub Node** so that the message goes to all nodes in your network.
3. In the **Event Code** field, select **RWT - Required Weekly Test**.
4. In the **Short Description** field, type a few words to describe the test.
5. In the **Long Description** field, type the text of the message.
6. In the **Duration** field, type how long you want the message to display. You can enter from 1 to 1440 minutes.
7. When you have finished configuring the message, click **Send**. You should see the text you entered in the Long Description field appear on the client screens.

Perform a Required Monthly Test

The FCC requires system operators to conduct weekly and monthly tests of their EAS. These tests ensure the reliability of the EAS equipment so that subscribers will receive national, state, and local warning messages about emergency situations.

The procedures in this section provide you with instructions for configuring your VCS to perform regular tests of your EAS.

Note: The VCS and FCC use the following acronyms to refer to the mandated tests of the EAS:

- **RWT:** Required Weekly Test
- **RMT:** Required Monthly Test

Weekly tests consist of transmitting the EAS digital header codes and end of message (EOM) codes once per week. Weekly tests must be conducted by EAS participants on different days and at different times.

No weekly test is necessary during the week that a monthly test is conducted or when there is an EAS activation for a state or local emergency.

Performing a Required Monthly Test

1. In the CMC, click **Services > Alert Management > Generate Notification**.
2. Select the national **PubSub Node** so that the message goes to all nodes in your network.
3. In the **Event Code** field, select **RMT - Required Monthly Test**.
4. In the **Short Description** field, type a few words to describe the test.
5. In the **Long Description** field, type the text of the message.
6. In the **Duration** field, type how long you want the message to display. You can enter from 1 to 1440 minutes.
7. When you have finished configuring the message, click **Send**. You should see the text you entered in the **Long Description** field appear on the client screens.

Message Validation

This section describes how the Alert Manager validates emergency alert messages.

Message Validation for SCTE-18 Messages

The following checks are specified in the SCTE-18 message specification, which you can view at www.scte.org.

Step 1: Examine the Buffer Content

The Alert Manager first examines the content of the buffer from the socket read.

If byte 0, 4, or 5 is 0xD8, Alert Manager tries to parse the SCTE-18 message.

Step 2: Examine the Message Header

The Alert Manager then examines the message header.

- No header: The message came in on a TCP socket
- DSG/BT header or an MPEG header(s): Multiple headers indicate that the message spans multiple MPEG packets

Step 3: Isolate the Data

The Alert Manager then isolates the transmitted data and performs a CRC check.

If the CRC transmitted in the message does not match the computed CRC, the record fails and the message is not processed.

Step 4: Verify the Table ID

The Alert Manager then tries to verify that the table ID is 0xD8.

If the table match fails, the record fails and the message is not processed.

Step 5: Verify the Protocol Version

The Alert Manager then verifies that the protocol version is 0 (zero).

If the protocol version check fails, the record fails, and the message is not processed.

Step 6: Check the Alert Event ID

For Conductor 2.5/3.0

The Alert Manager then checks the combination of Event ID and sequence_number values.

If the two alerts have the same Event ID, but different sequence_number values, they are both processed and published.

If the two alerts have identical Event IDs and sequence_number values, the second alert is dropped as a redundant message.

For Conductor 2.1

The Alert Manager then checks the alert event ID.

If a record with the same event ID has already been processed, the record is dropped as a redundant message.

If the record has a unique event ID, the Alert Manager continues processing the record.

Step 7: Check the Message Priority

The Alert Manager then checks to see whether the alert has a priority of 0 (zero).

An alert with a priority of zero is not processed.

Message Validation for DVS/168 Messages

The following checks are specified in the DVS/168 message specification, which you can view at www.scte.org.

Field	Type	Range	Length (bytes)	Comments
EventType Descriptor				
MsgName	char<8>	n/a	8	Unique ASCII name that identifies the EAM. If more than one message is used to create the EAM, this field links the messages.
CountyType Descriptor				
NumCounties	char<2>	0 - 32	2	Specifies the number of the destination counties in the EAM. A value of 00 (two zeros) indicates all counties.
FIPSCode	char<6>	n/a	n/a	Specifies the destination county codes of the EAM as determined by the FCC FIPS codes.
MessageTime Descriptor				

Field	Type	Range	Length (bytes)	Comments
OriginationTime	char<7>	n/a	7	Specifies the origination time of the EAM in GMT (JJJHHMM), where JJJ indicates the Julian calendar days.
Duration	char<4>	n/a	4	Specifies the length of the EAM in minutes. For an open-ended message, this value is always 0 (zero). If the message is to be repeated only once, the value is 0 (zero).
MessageType Descriptor				
EventCode	char<3>	n/a	3	Specifies the FCC-defined event code for the EAM.
DisplayFlag	char<1>	0 - 3	1	ASCII character that specifies the type of content in the DisplayContent field. ■ 0 - No text message, the content in the field is not valid ■ 1 - The content is ASCII characters ■ 2 - The content is HTML formatted characters ■ 3 - The content is a relative directory and file name
AudioFlag	char(1)	0 - 5	1	Character that specifies the content of the AudioContent field. ■ 0 - No audio content, the content in the field is not valid ■ 1 - The content is AIF formatted audio ■ 2 - The content is WAV formatted audio ■ 3 - The content is a relative directory and file name ■ 4 - The content is VOC formatted sample ■ 5 - The content is open-formatted (to be determined)
DisplayLength	char<4>	0000 - FFFF	4	Specifies the length of the DisplayContent field in hexadecimal format.

Field	Type	Range	Length (bytes)	Comments
AudioLength	char<4>	0000 - FFFF	4	Specifies the length of the AudioContent field in hexadecimal format.
DisplayContent	char<n>	n/a	Display Length	Specifies the text part of the EAM, the format of which is based on the value in the DisplayFlag field.
AudioContent	char<n>	n/a	AudioLength	Specifies the audio part of the EAM, the format of which is based on the value in the AudioFlag field.

EAM Errors

EAM requests can result in the following error codes:

- No error (0)
- Missing required descriptor (1)
- Invalid descriptor (2)
- Discarded the message (3)
- No file exists (4)
- Unspecified error (99)

Message Validation for CAP v1.2 IPAWS1.0 and CAP-CP Ingest Messages

The Alert Manager validates the CAP ingest message based upon CAPv1.2 or CAP-CP, depending upon the type of incoming message. The specifications are found here:

- Canadian Profile of the Common Alerting Protocol (CAP-CP): http://cap-cp.ca/index.php/en/#CAP-CP%20Specifications
- Common Alerting Protocol, v. 1.2 USA Integrated Public Alert and Warning System Profile Version 1.0 (IPAWS1.0): http://docs.oasis-open.org/emergency/cap/v1.2/ipaws-profile/v1.0/cap-v1.2-ipaws-profile-v1.0.pdf

3

Troubleshooting the EAS

Introduction

This chapter provides troubleshooting information that will help you verify the proper configuration and performance of the EAS, so that you can achieve optimum system performance in receiving and sending EAS messages.

In This Chapter

The Dashboard

The Alert Manager dashboard lets you view metrics and error messages at a glance, without having to go through log files. The types of information you can view on the dashboard include:

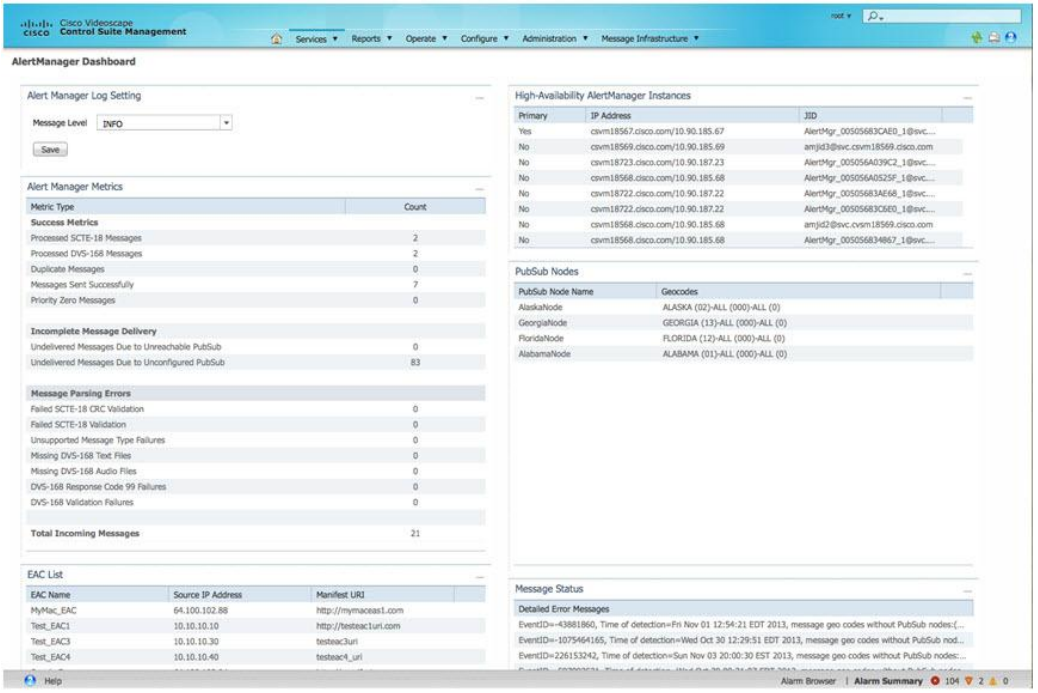
- Alert Manager metrics
- Message status (error messages)
- A list of the EACs defined in the Alert Manager
- A list of the PubSub nodes defined in the Alert Manager

Launching the Alert Manager Dashboard

On the CMC, click **Services > Dashboard**.

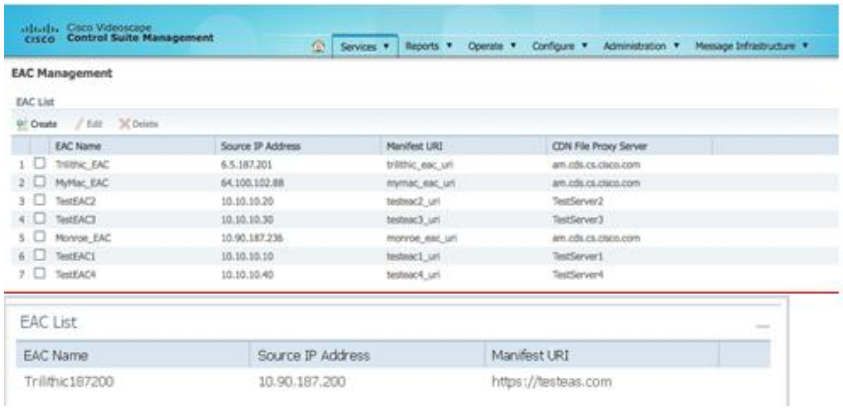
Note: This example is from the initial screen when you first log onto the Cisco Videoscape CSM. It defaults to the Home screen that displays the VCS nodes on the system, as seen on the left.

Result: The Alert Manager Dashboard window opens.



Note: If no information displays in the dashboard, click **Refresh** . The lists should populate.

EAC List



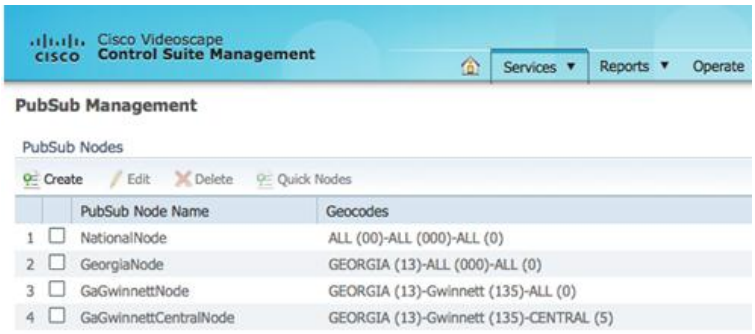
The EAC list displays the Alert Manager EACs currently configured in the system.

Information on this screen includes:

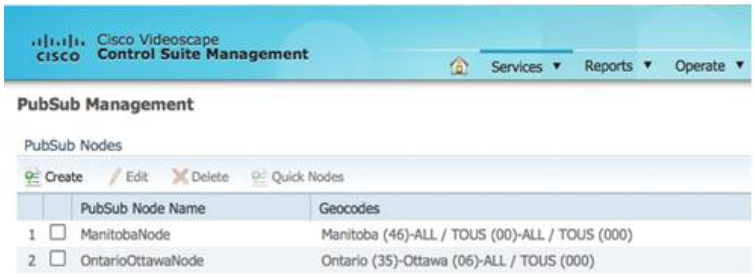
- **EAC Name**
- **Source IP Address** (the physical EAC)
- **Manifest URI**

PubSub Nodes

US (FIPS) Location Code Type



Canadian (SGC) Location Code Type

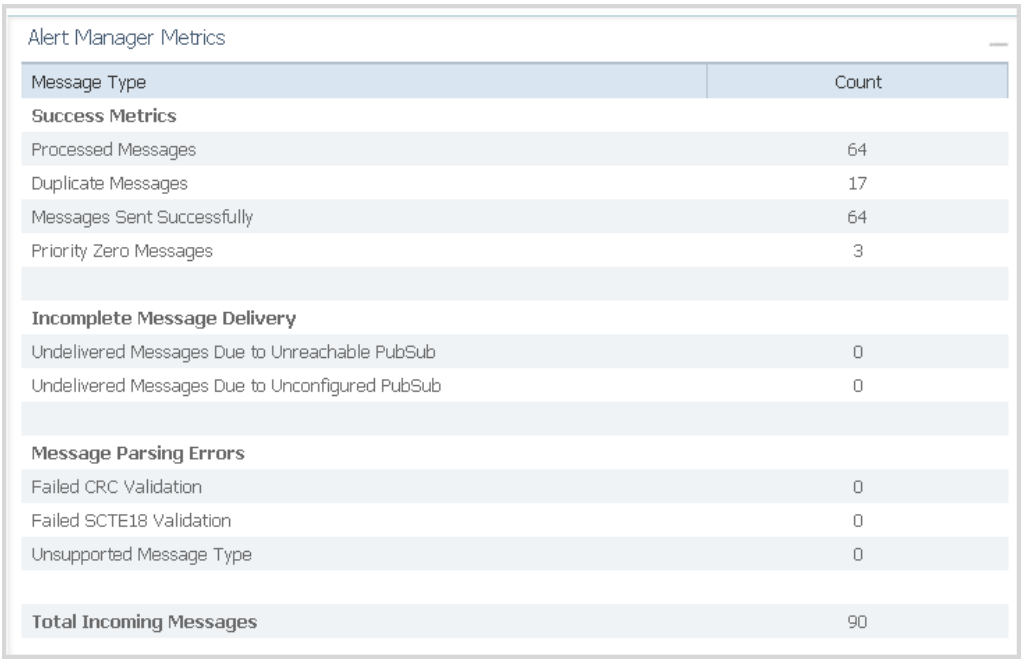


The PubSub Nodes list displays the Alert Manager PubSub Nodes currently configured in the system.

Information on this screen includes:

- **PubSub Node Name**
- **Geocodes** assigned to the PubSubs

Alert Manager Metrics



Alert Manager Metrics

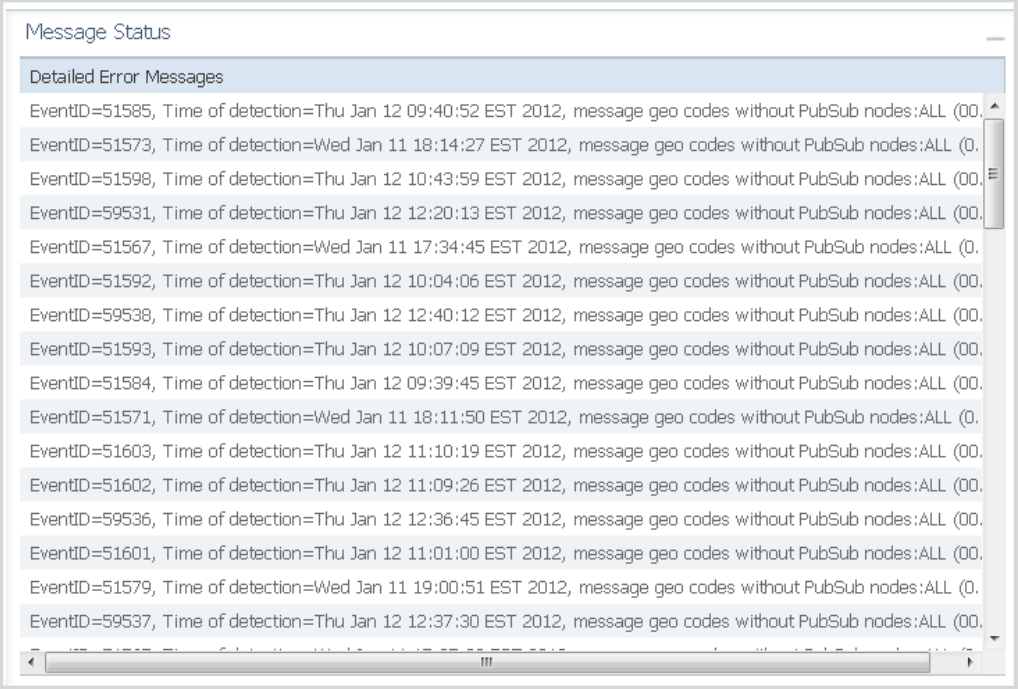
Message Type	Count
Success Metrics	
Processed Messages	64
Duplicate Messages	17
Messages Sent Successfully	64
Priority Zero Messages	3
Incomplete Message Delivery	
Undelivered Messages Due to Unreachable PubSub	0
Undelivered Messages Due to Unconfigured PubSub	0
Message Parsing Errors	
Failed CRC Validation	0
Failed SCTE18 Validation	0
Unsupported Message Type	0
Total Incoming Messages	90

The metrics section of the screen allows you to view the number of messages that have passed through the system, and whether any messages failed to be delivered.

Information displayed on this screen includes:

- Number of processed messages
- Number of duplicate messages
- Number of messages sent successfully
- Number of priority zero messages
- Number of undelivered messages due to unreachable or unconfigured PubSubs
- Number of message parsing errors
- Total number of incoming messages

Message Status

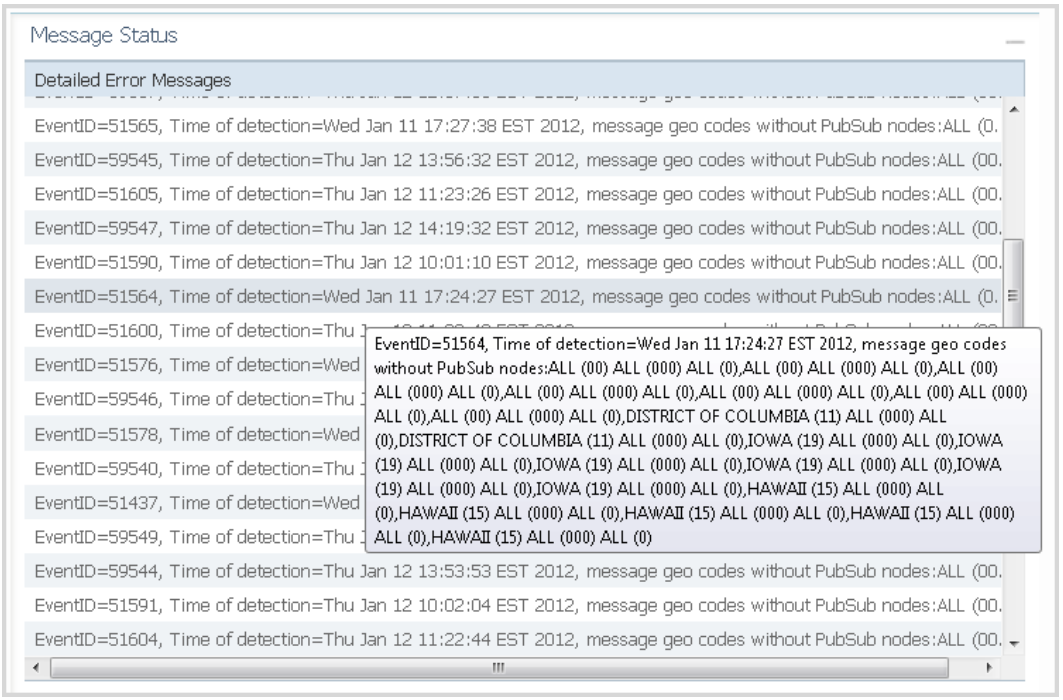


The Message Status section of the screen allows you to view the error message log from the Alert Manager UI.

Information displayed on this screen includes:

- Event ID
- Time of detection
- Message geocode

To view further details of an error message, hover your mouse over the error message. A pop-up window opens with further details.



Alert Manager Log Files

Viewing Log Files

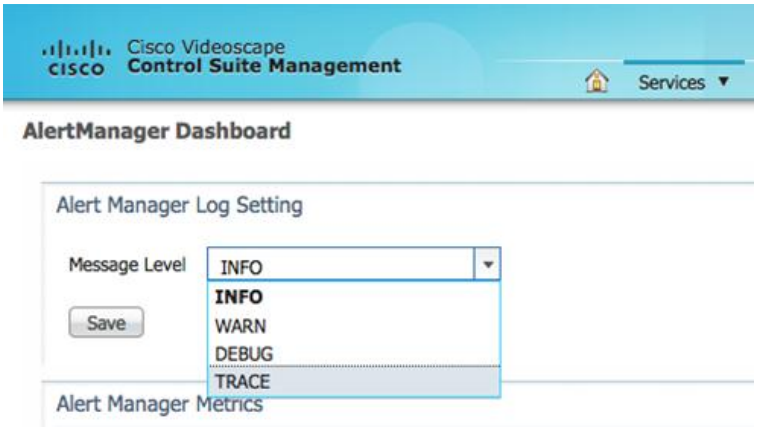
1. Open an xterm window on the Alert Manager.
2. Log in as an administrator.
3. To view the names of all the Alert Manager logs, type the following and press **Enter**:
   `file list activelog /jboss/*`
4. To view the log messages in a specific Alert Manager log file, type the following and press **Enter**:
   `file view activelog /jboss/AlertManager.log`

Example: As an example, the following AlertManager.log file (set to **INFO**) confirms that the message has been published to the PubSub nodes associated with previously configured geocodes.

```
2012-08-20 14:25:03,746 INFO   AMListener.run: processing key
AlertManagerSocketBufferHashKey [theSocket=DbSocket [oid=ffb562ff-a836-4e2a-
ab41-0f47dece5b30, ipAddress=0.0.0.0, port=65100, socketType=1,
socketName=UDPListener1, userOid=3014d09b-be2f-41a1-9c08-a65a0ff806d0],
theFd=416, messageOid=, inIp=10.90.184.75]

2012-08-20 14:25:03,986 INFO   AlertManagerCapServer.call: Published to node
GeorgiaNode

2012-08-20 14:25:04,082 INFO   AlertManagerCapServer.call: Published to node
GaGwinnettNode

2012-08-20 14:25:04,280 INFO   AlertManagerCapServer.call: Published to node
GaGwinnettCentralNode

2012-08-20 14:25:36,058 INFO   AMListener.run: processing key
AlertManagerSocketBufferHashKey [theSocket=DbSocket [oid=DVS168-SOCKET-OID,
ipAddress=0.0.0.0, port=4098, socketType=0, socketName=DVS168SOCKET,
userOid=DVS168-USER-OID], theFd=378, messageOid=, inIp=10.90.184.75]

2012-08-20 14:25:36,087 INFO   AMSocketManager.writeTcpSocket: 1 bytes to fd
378

2012-08-20 14:25:36,264 INFO   AlertManagerCapServer.call: Published to node
GeorgiaNode

2012-08-20 14:25:36,342 INFO   AlertManagerCapServer.call: Published to node
GaGwinnettNode

2012-08-20 14:25:36,414 INFO   AlertManagerCapServer.call: Published to node
GaGwinnettCentralNode
```

Changing Logging Levels

1. On the CMC, open the Alert Manager Dashboard: **Services > Alert Management > Dashboard > Alert Manager Dashboard**.
2. From the pull-down **Message Level** menu, select **TRACE**.



Logging levels:

- **TRACE** - Logs events directly associated with request activity
- **DEBUG** - Logs more information about INFO-level events
- **INFO** - Logs service lifecycle events and other related information
- **WARN** - Logs non-critical service errors

4

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.

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

November 2013

Part Number OL-25915-03