# Cisco Conductor EAS 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 *Conductor* 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 go to **ftp://ftpeng.cisco.com/pub/opensource/scientificatlanta/**. Once at the site, search for the product listing and click on the related items identified. 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

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 Conductor 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 Videoscape Conductor 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 second formal release of this document. In addition to minor text and graphic changes, the following table provides the technical changes to this document.

| Description | See Topic |
|---|---|
| Removed installation steps and procedures | ■ Installation steps are now included in a comprehensive services installation guide, xref |
| Updated configuration procedures | ■ ***Alert Manager Configuration*** (on page 1) |
| Added CAP configuration | ■ ***Set Up the Common Alerting Protocol*** (on page 12) |
| Updated troubleshooting section to include CAP messages | ■ ***Troubleshooting the EAS*** (on page 27) |
| Added validation section for CAP messages | ■ ***Message Validation for CAP Messages*** (on page 24) |
| Added a section on the Alert Manager log files | ■ ***Alert Manager Log Files*** (on page 32) |

# 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 3).
2. ***Log Into the CMC UI*** (on page 4).
3. ***Create the PubSub Nodes*** (on page 5).
4. ***Create the Alert Manager EAC*** (on page 7).
5. ***Create the Listeners*** (on page 9).
6. ***Set Up the Common Alerting Protocol*** (on page 12).
7. ***Verify the End-to-End Alert Manager Configuration*** (on page 15).

# Configure Your Physical EAC

You need to configure your physical EAC so it can talk to 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 physical EAC to configure a port and IP address to be used to send EAS messages to the Alert Manager.

**Note:** 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.

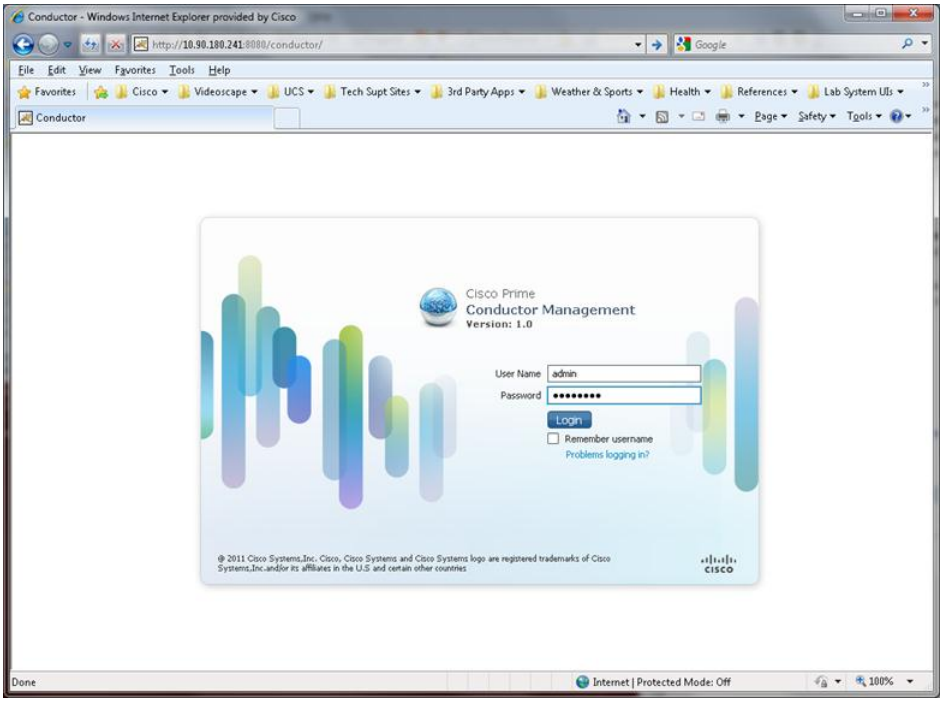
# Log Into the CMC UI

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 CMC login page opens.




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

# 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 register to the PubSub node and receive the EAS messages appropriate for their location.

## Before You Begin

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

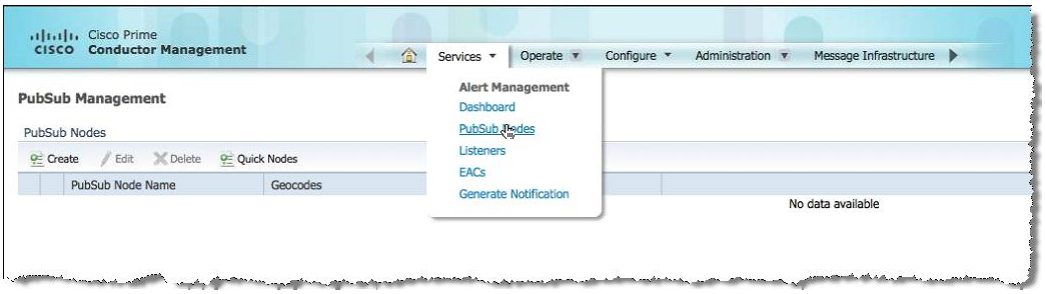
- The name of the PubSub node.
- Whether this is a national node or not.

  **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.

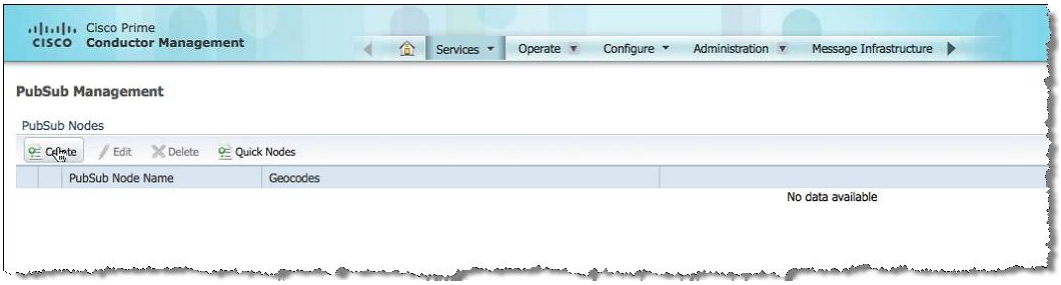
If you make an error by entering an unsupported value in any field, saving the PubSub will fail and a message will display on the screen.

## Creating the PubSub Nodes

1 In the Conductor Manager, click the **Services > PubSub Nodes**.




2 Click **Create**.

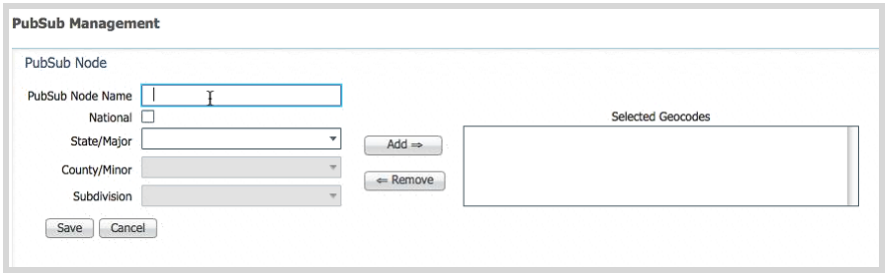


3 Enter and select the information specific to this node:

- PubSub Node Name

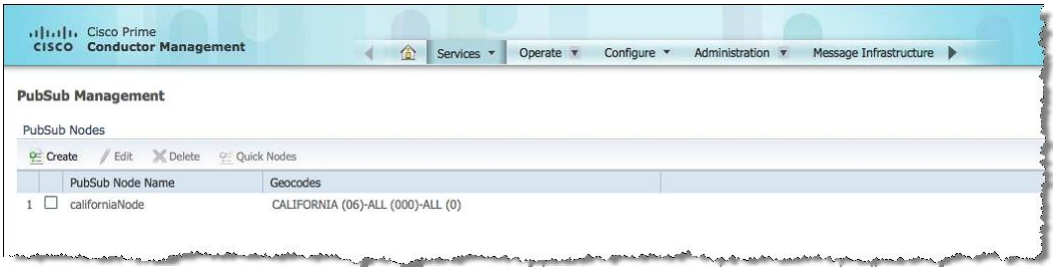
  **Note:** Names are case-sensitive. Be sure to use a name that corresponds to your site's naming conventions.

- National (you can only have one National PubSub node in your system)
- State/Major
- County/Minor
- Subdivision




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.




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

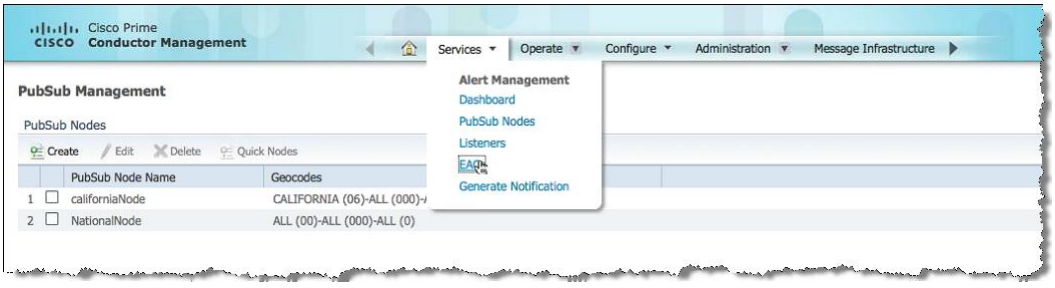
Before you begin to create the Alert Manager EAC, you need the following information:

- The 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 (if applicable)

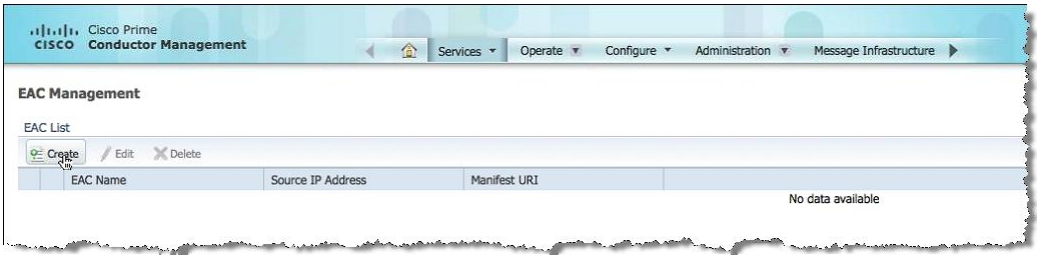
If you make an error by entering an unsupported value in any field, saving the EAC will fail and a message will display on the screen.

## Creating the Alert Manager EAC

1 In the Conductor Manager, click **Services > EACs**.




2 Click **Create**.



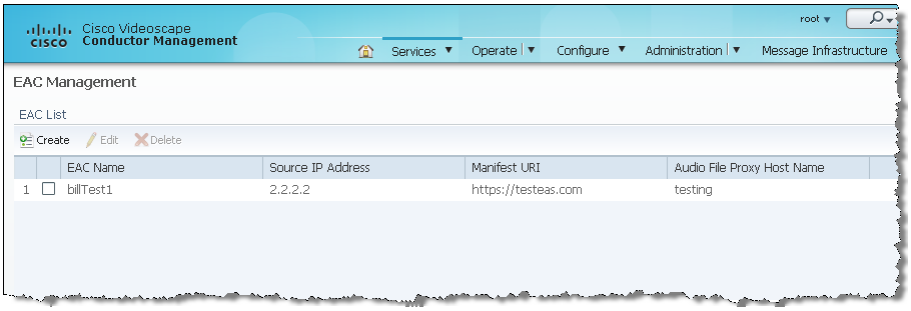
3 Enter and select the information specific to this EAC:

- 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
- Audio File Proxy Server Name: For systems using a CDN, the name of the CDN server


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.

## Before You Begin

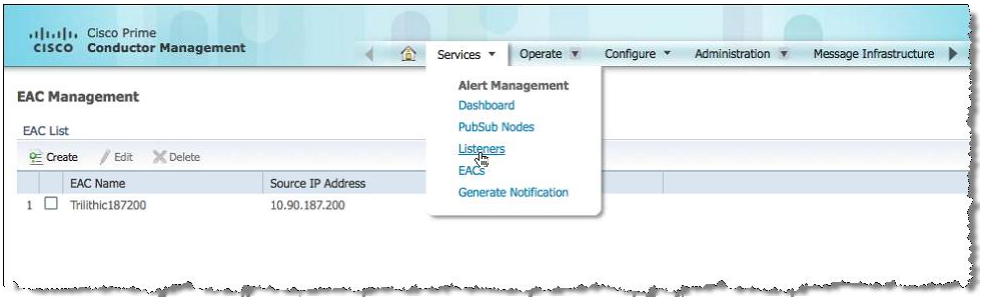
Before you begin to create the listener, you need the following information:

- 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; receiver-specified source
  - Unicast UDP: Unicast user datagram protocol; point-to-point messaging over the UDP protocol
- The IP address of the Alert Manager
- The port number of the Alert Manager
- The name of the Alert Manager EAC you created in the previous step

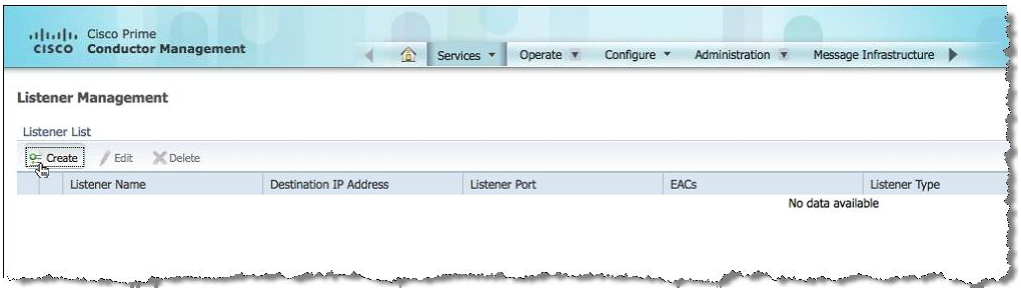
If you make an error by entering an unsupported value in any field, saving the listener will fail and a message will display on the screen.

## Creating the Listeners

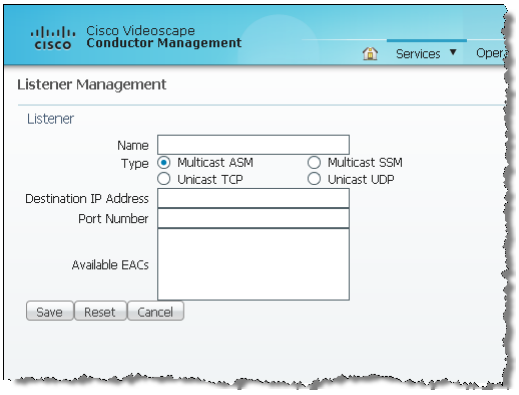
1 In the Conductor Manager, click **Services > Listeners**.



**Result:** The Listener Management Listener List window opens.




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




3 Create a multicast ASM listener by entering the 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

4 Click **Save**.

5 Create a unicast TCP listener by entering the 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

6 Click **Save**.

7 Create a multicast SSM listener by entering the information specific to this listener:
   - Name
   - 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

8 Click **Save**.

9 Create a unicast UDP listener by entering the information specific to this listener:
   - Name
   - 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

10 Click **Save**.

# Set Up the Common Alerting Protocol

The Common Alerting Protocol (CAP) is a protocol for EAS messages (EAMs) that converts the SCTE-18 and DVS/168 EAS messages the Alert Manager 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.

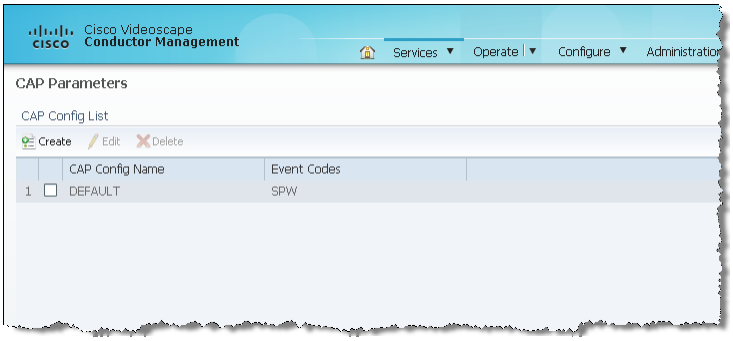
## Before You Begin

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

- CAP configuration name
- Alert Remaining Time
- Scope
- Restrictions
- Addresses
- Resource description
- Alert priority
- Force tune
- Category
- Urgency
- Severity
- Certainty
- Event codes related to this CAP customization

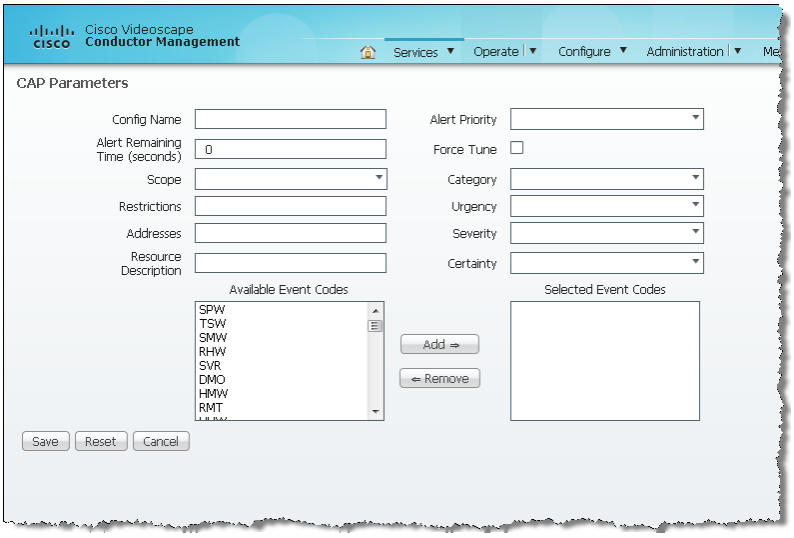
## Setting Up the CAP

1 On the Conductor Manager, click **Services > CAP**.




**Note:** You cannot edit the DEFAULT CAP.

2 Click **Create**.




3 Create a CAP by entering the information specific to this CAP:

- Config Name
- Alert Remaining Time (seconds)
- Scope
- Restrictions
- Resource Description
- Alert Priority
- Force Tune
- 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**.

# Verify the End-to-End Alert Manager Configuration

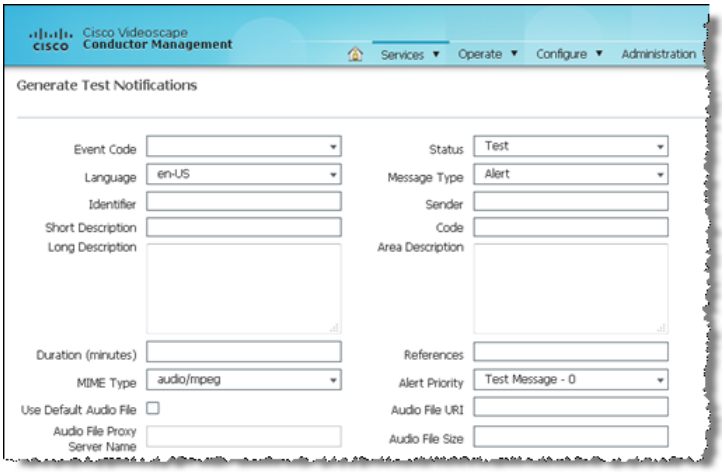
## Verifying the Configuration by Sending a User Notification

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

1 On the Conductor Manager, click **Services > Alert Manager > Generate Notification**.

2 Select a PubSub Node.

3 Enter the other required data.




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
```

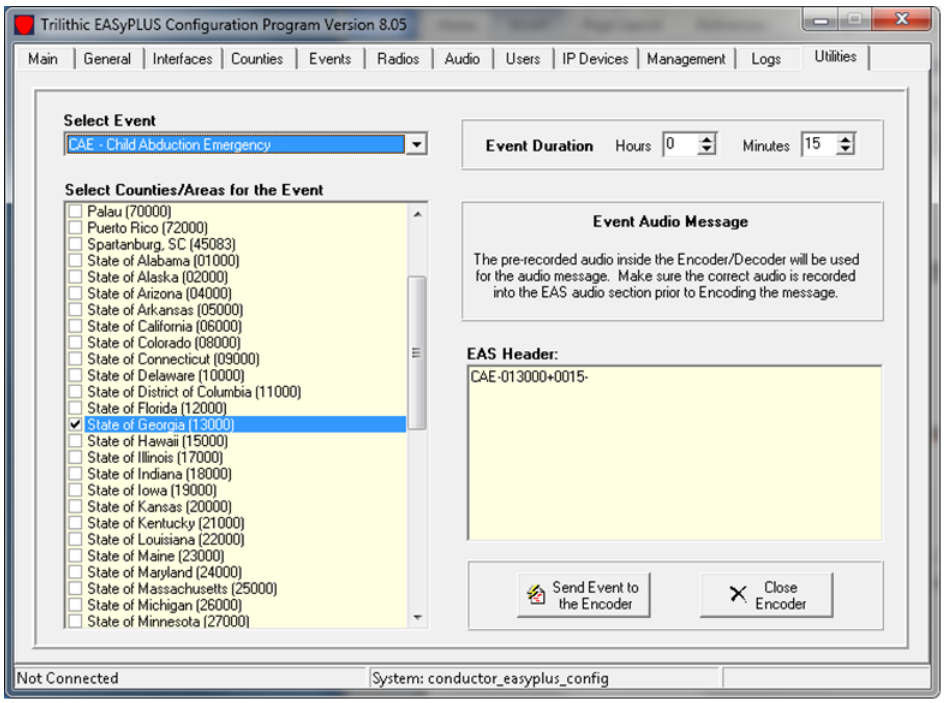
**Note:** For information on setting logging levels, see ***Changing Logging Levels*** (on page 32).

## 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

The following is an example of a message set up in the Trilithic EAC:




This corresponds to the following alertManager.log file entries (set to TRACE):

```
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
```

To learn how to change logging levels in the Alert Manager, see ***Changing Logging Levels*** (on page 32).

## 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. See ***Create the PubSub Nodes*** (on page 5) for the procedure.
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 Manager** and click **General Notification**.
8. Select the **PubSub** you created for this test.
9. Send a general notification. You should see the results in the Psi XML console.

   **Note:** See ***Perform an Adhoc Test*** (on page 20) for more information on sending a general 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 > 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 Alert Manager to perform regular tests of your EAS.

**Note:** The Alert Manager 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 Conductor Manager, click **Services > 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 Alert Manager to perform regular tests of your EAS.

**Note:** The Alert Manager 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 Conductor Manager, click **Services > 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 passed 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

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 CAP Messages

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

### CAP Message Format

The following message format is specified in the CAP protocol.

| 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* | | | | |
| 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 (zer0). |
| *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.<br>■ 0 - No text message, the content in the field is not valid<br>■ 1 - The content is ASCII characters<br>■ 2 - The content is HTML formatted characters<br>■ 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.<br>■ 0 - No audio content, the content in the field is not valid<br>■ 1 - The content is AIF formatted audio<br>■ 2 - The content is WAV formatted audio<br>■ 3 - The content is a relative directory and file name<br>■ 4 - The content is VOC formatted sample<br>■ 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. |
| AudioLength | char<4> | 0000 - FFFF | 4 | Specifies the length of the AudioContent field in hexadecimal format. |
| DisplayContent | char<n> | N/A | DisplayLength | 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 product the following result codes:

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

# 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 the receiving and sending of 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:

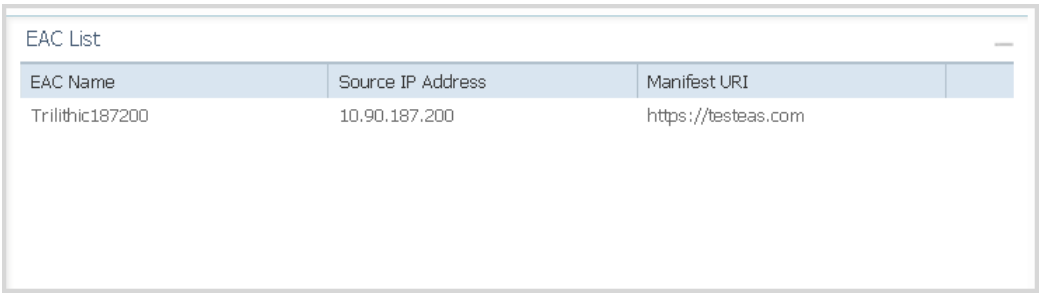
- Alert Manager metrics
- Message status (error messages)
- A list of the EACs defined in the Alert Manager
- A list of the PubSub nodes defined in the Alert Manager

## Launching the Alert Manager Dashboard

On the Conductor Manager, click **Services > Dashboard**. The Alert Manager Dashboard window opens.

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

## EAC List

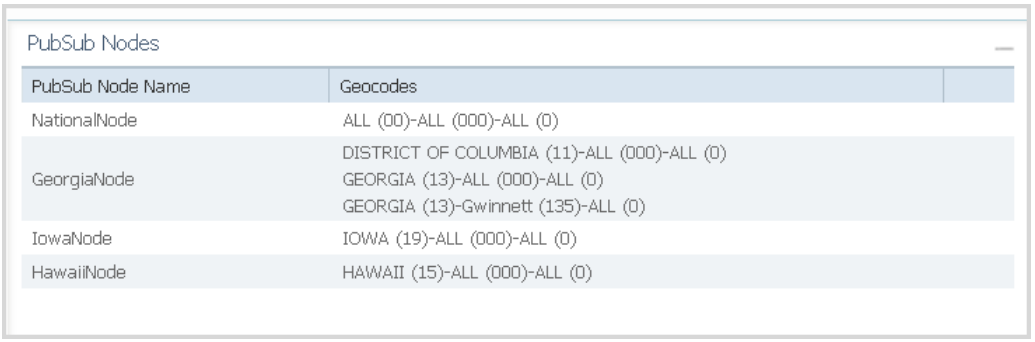



The EAC list displays the Alert Manager EACs currently configured in the system.

Information on this screen includes:

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

## PubSub Nodes



PubSub Nodes

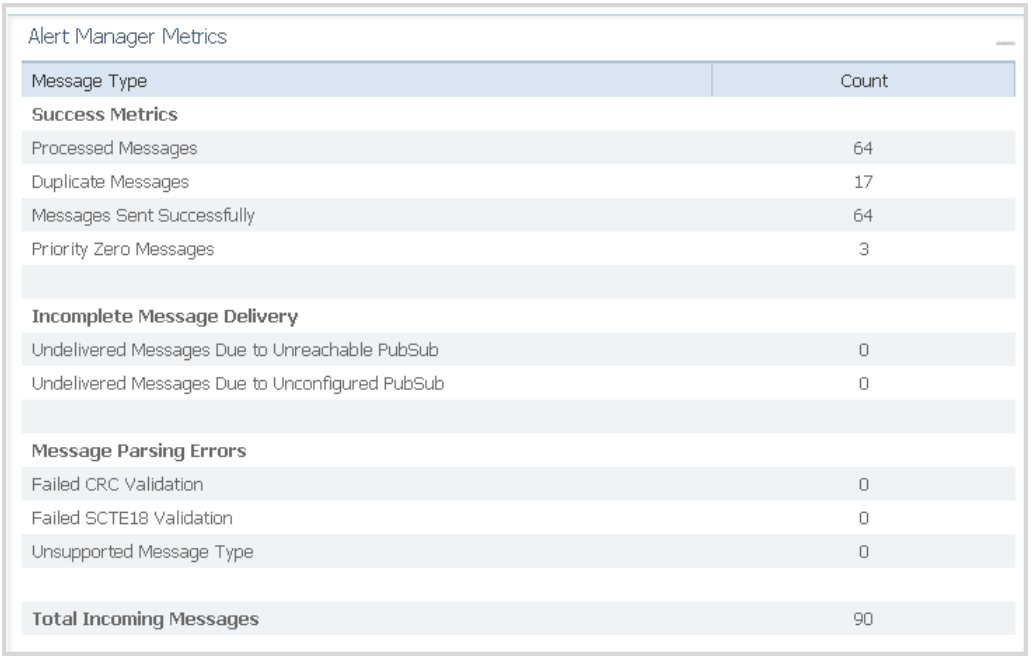
| PubSub Node Name | Geocodes |
|---|---|
| NationalNode | ALL (00)-ALL (000)-ALL (0) |
| GeorgiaNode | DISTRICT OF COLUMBIA (11)-ALL (000)-ALL (0)<br>GEORGIA (13)-ALL (000)-ALL (0)<br>GEORGIA (13)-Gwinnett (135)-ALL (0) |
| IowaNode | IOWA (19)-ALL (000)-ALL (0) |
| HawaiiNode | HAWAII (15)-ALL (000)-ALL (0) |

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

Information on this screen includes:

- PubSub Node Name
- Geocodes assigned to the PubSubs

## Alert Manager Metrics



Alert Manager Metrics

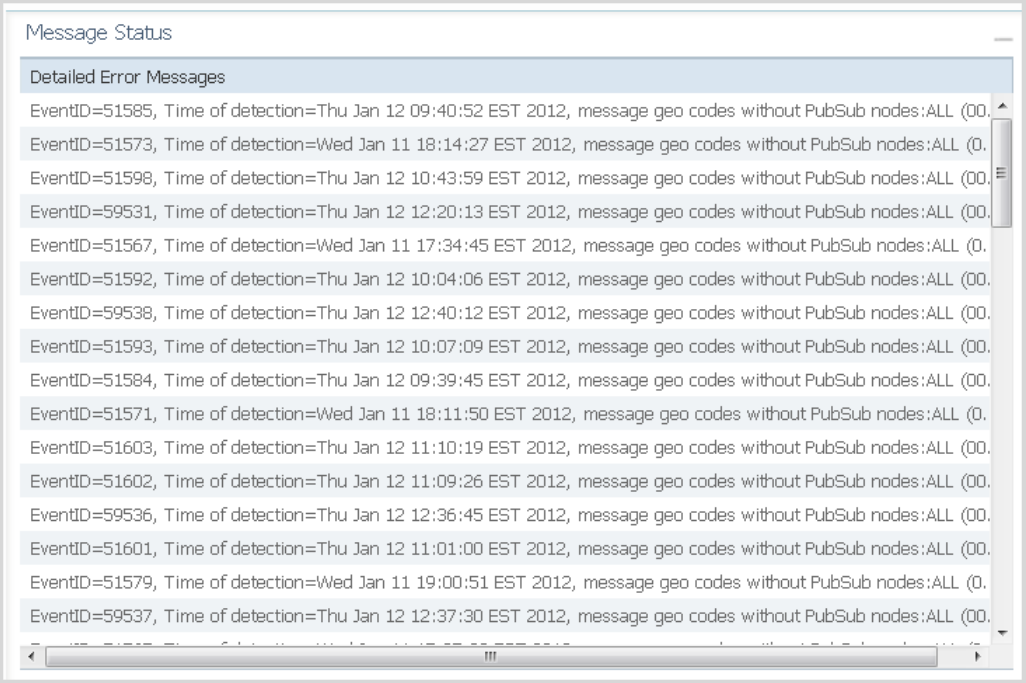
| Message Type | Count |
|---|---|
| **Success Metrics** | |
| Processed Messages | 64 |
| Duplicate Messages | 17 |
| Messages Sent Successfully | 64 |
| Priority Zero Messages | 3 |
| | |
| **Incomplete Message Delivery** | |
| Undelivered Messages Due to Unreachable PubSub | 0 |
| Undelivered Messages 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 message 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

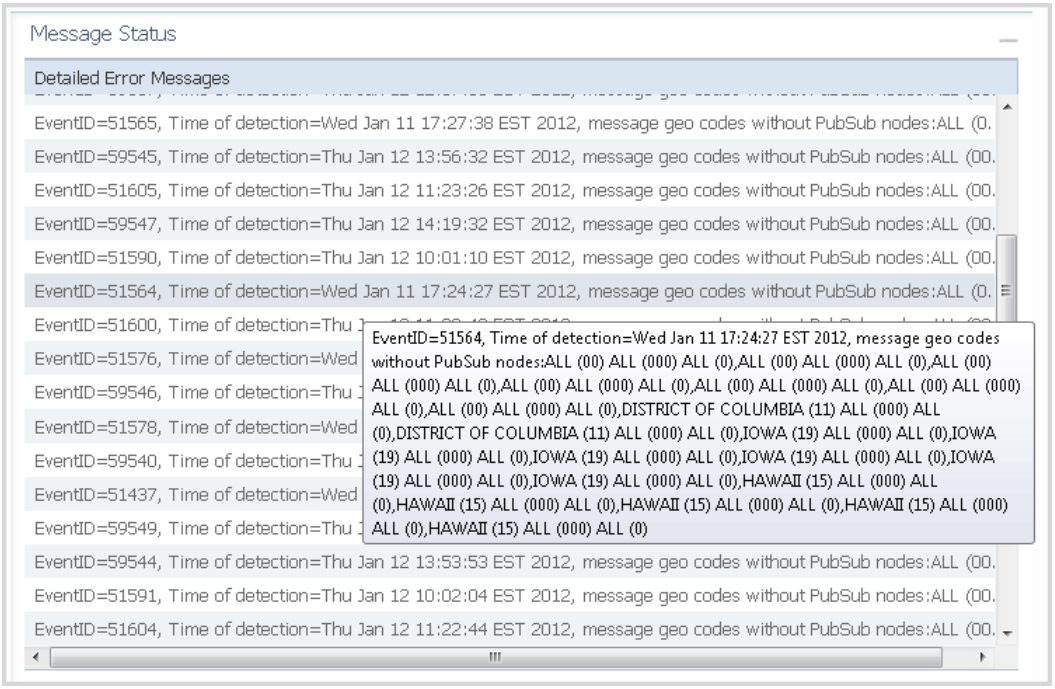



The Message Status section of the screen allows you to view the error message log from the Alert Manager UI.

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 a command line 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
   ```

## Changing Logging Levels

1. Open a web browser.
2. Type the following URL in the address line of the browser:

   ```
   http://[AMbladeIpAddress]:8080/AlertManager/api/log/[level]
   ```

   where:

   - `AMbladeIpAddress` is the IP address of the blade where the Alert Manager is installed
   - `level` is one of the following 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, call 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.

# Index

Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678 277-1120
800 722-2009
www.cisco.com



October 2012 Printed in USA

Part Number OL-25915-02