AVAYA

Avaya Media Application Server

Troubleshooting and Fault Management

Release: 6.6
Document Revision: 01.02

NN44474-700

Avaya Media Application Server
Release: 6.6
Publication: NN44474-700
Document release date: 21 May 2010

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support

Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Copyright

Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

New in this release

The following sections detail what’s new in *Avaya Media Application Server Troubleshooting and Fault Management* (NN44474-700) for Avaya Media Application Server Release 6.6.

Features

For information about feature-related changes, see the following section:

- "Media Application Server on Linux" (page 9)

For information about all MAS Release 6.6 features, see *Avaya Aura™ Application Server 5300 Release Delta* (NN42040-201).

Media Application Server on Linux

Avaya no longer supports Windows for MAS releases. Removed content about Windows Operating System (OS) and replaced with content about Linux OS. Changes affect procedures in the following sections:

- "Unified Communications Management" (page 25)
- "Reporting" (page 39)
- "SNMP" (page 49)

Other changes

This document contains the following other changes:

- Moved the Emergency security chapter from *Avaya Media Application Server Administration and Security* (NN44474-600) to *Avaya Media Application Server Troubleshooting and Fault Management* (NN44474-700).
- Moved the Disaster recovery for the primary server chapter from *Avaya Media Application Server Administration and Security* (NN44474-600) to *Avaya Media Application Server Troubleshooting and Fault Management* (NN44474-700).

Revision history

May 2010	Standard 01.02. Editorial changes were made.
April 2010	Standard 01.01. This document is issued to support Avaya Media Application Server Release 6.6 for Avaya Aura™ Application Server Release 2.0. This document contains information previously contained in the following document, now retired: *Nortel Media Application Server Troubleshooting* (NN44471-703)

Introduction

The *Avaya Media Application Server Troubleshooting and Fault Management* (NN44474-700) document provides information about troubleshooting for the Media Application Server (MAS).

Not all the sections in this book are applicable to all systems. For more information about supported systems, see *Avaya Media Application Server Planning and Engineering* (NN44474-200).

Prerequisites

- For detailed information about fault management, logs, and alarms, see *Avaya Media Application Server Alarms and Logs Reference* (NN44474-702).
- For detailed information about performance management, operational measurements, and reports, see *Avaya Media Application Server Operational Measurements Reference* (NN44474-701).

Navigation

- "SNMP" (page 49)
- "Common procedures" (page 51)
- "Appendix: SIP response messages" (page 59)

Call completion failure

This section provides descriptions, possible causes, and solutions for common issues and error messages that relate to call completion failures.

Navigation

- "An in-service MAS rejects calls" (page 13)

An in-service MAS rejects calls

The Media Application Server (MAS) rejects incoming SIP calls for one or more service types. Consult the Log Viewer to identify attempts to launch an uninstalled or unlicensed service.

Possible causes

Any of the following reasons can cause this problem:

- Calls to services on MAS that are not licensed; you receive a SIP final response indicating that the service is unavailable.
- The proxy configuration is incomplete.
- The target service application is not installed.
- The MAS is in the Pending Lock state.

Solutions

Each solution relates to a possible cause.

Licensing

1. In Element Manager, navigate to **Licensing**, **Licensing Configuration** to view the number and variety of installed licenses.
2. Ensure that the required licenses are installed and available.
3. Restart the MAS to activate any newly installed license. See "Restarting the MAS" (page 54).

Proxy configuration

1. In Element Manager, navigate to **System Configuration**, **Signaling**, **SIP**, **Nodes and Routes** and ensure that all required trusted nodes are configured.
2. On the SIP Nodes and Routes page, ensure that all SIP routes are configured.

Application installation

1. In Element Manager, navigate to **Products and Applications** and ensure that the target service is installed.
2. If necessary, install the application by launching it in the application installer.

Pending Lock MAS

1. Check the operational state of the MAS. In Element Manager, navigate to **System Status**, **Element Status**.
   A MAS in the Pending Lock state rejects new service requests.
2. Configure the MAS state to the Unlocked state to accept calls. On the Element Status page, in the **More Actions** list, select **Unlock**.

Data

This section provides details, possible causes, and solutions for common issues and error messages that relate to data.

Navigation

- "Backup and restore is not allowed" (page 15)
- "Data Synchronization in Progress alarm is raised" (page 16)

Backup and restore is not allowed

After a Media Application Server (MAS) platform software upgrade, you receive a BackupRestore error when attempting to restore an older backup file to the MAS.

Possible causes

The Restore operation prevents the system from restoring old configurations with outdated schemas to a newer, incompatible MAS software load. Restorations of service data are not as restrictive.

Solutions

You can restore a data backup file of an older configuration as follows.

1. Uninstall the current MAS software. For more information, see *102.1.6 AS5300 MAS Platform and Application Installation*.
2. Reinstall the MAS software version that is compatible with the backup file you want to restore.
3. Restore the backup file to the MAS software version you installed in Step 2.
4. Upgrade the MAS to the latest software version. The upgrade process automatically converts the data for the upgraded load.

Data Synchronization in Progress alarm is raised

The MAS raises the Data Synchronization in Progress alarm to indicate an ongoing data synchronization audit between the Primary and Secondary nodes in a cluster. The duration of the synchronization is directly proportional to the amount of subscriber data on the system.

Possible causes

The synchronization occurs any time the Primary and Secondary servers in a cluster establish a connection to each other. Typically, the cause is a restart of one of the nodes or a reestablishment of a lost network connection between the peers.

Solutions

Typically, no action is required. Data synchronization does not put the MAS into a state that blocks any processing. If both MAS servers are synchronizing due to a restart, in most cases, they have the data required for application functionality. In general, when there is the potential that one machine was out of service while the other was in service, a data delta can exist. In this case, the synchronization audit addresses this issue.

If an application data request occurs on a MAS that has not received new data from its peer due to an in-progress synchronization, that request will fail. The system raises an alarm to bring this potential issue to the attention of the administrators controlling traffic on the MAS. The alarm indicates a potential data mismatch between the nodes until the system completes the audit and clears the alarm.

Any data changes received during a synchronization are reflected immediately on both nodes. (This condition also occurs when the synchronization is not running.) In most cases, synchronization is considered a background audit. You can ignore this condition, unless one machine is known to be missing data, or complete data integrity is required and there were known changes while the peers were isolated from each other.

The only potential action is to temporarily reroute calls away from a newly installed MAS, which lacks a full data set, to another MAS until the synchronization is complete.

E-mail Delivery

This section provides details, possible causes, and solutions for common issues and error messages that relate to e-mail delivery.

Navigation

- "Simple Mail Transport Protocol (SMTP) mail delivery is not working" (page 17)

Simple Mail Transport Protocol (SMTP) mail delivery is not working

The system does not deliver recorded conferences or e-mail messages as expected.

Possible causes

Typical causes of this problem include SMTP server configuration, provisioning, or availability.

Network security settings can prevent the MAS from accessing the SMTP server.

Solutions

Each of the following solutions relates to a possible cause.

- Ensure that an SMTP server address is configured for the service in question. You can configure these settings on the provisioning system connected to the MAS. In some cases, you must provision and save a destination e-mail address for each user on the MAS.
- Ensure that the network settings allow the MAS access to the SMTP server configured as the e-mail server. Check for firewalls and other security settings.
- Ensure that the configured SMTP server address refers to a valid in-service mail server.

Emergency recovery trees

This section provides the procedures to recover from field outages as quickly as possible.

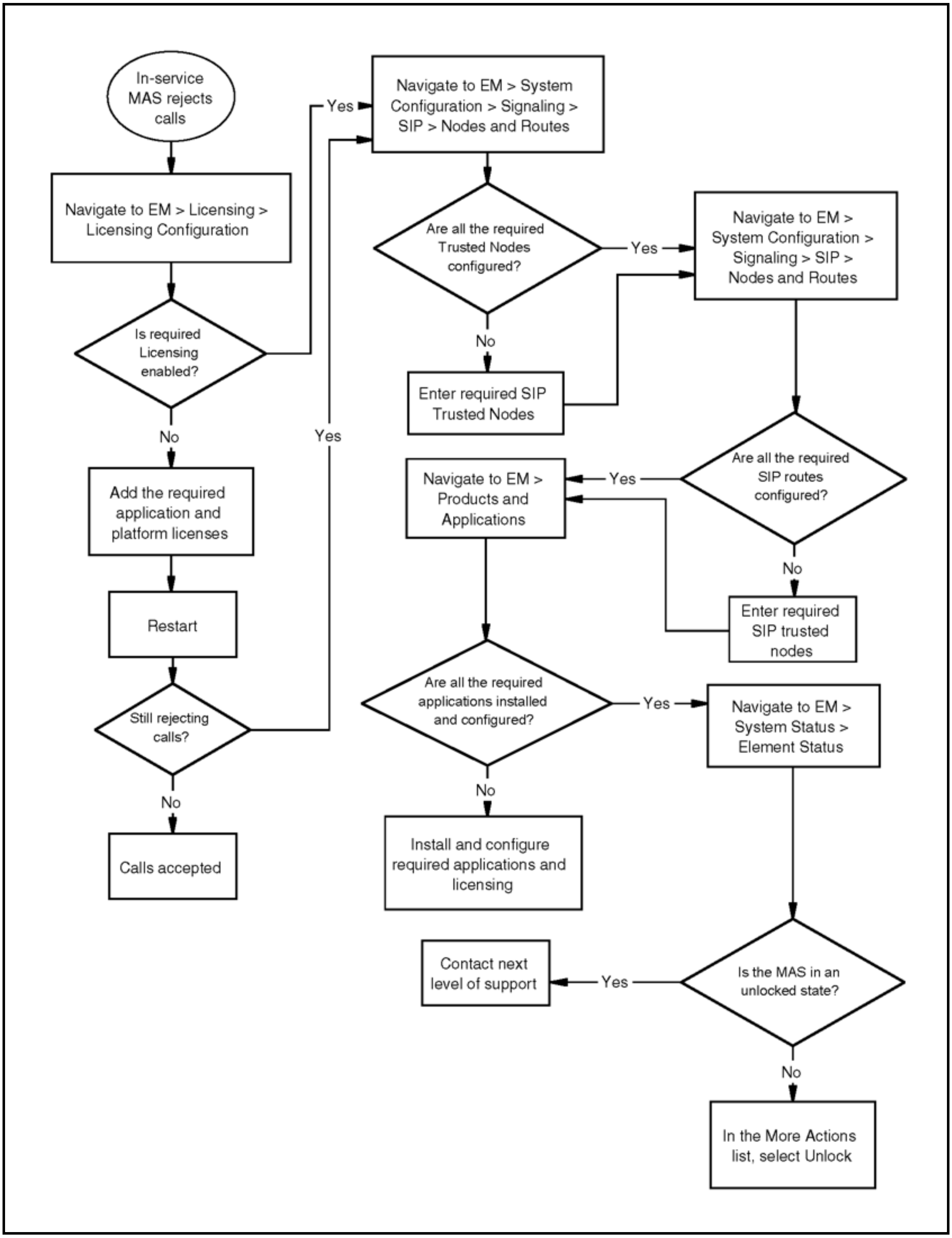
Navigation

- "In-service MAS rejects calls recovery tree" (page 19)
- "Nodal license is not working recovery tree" (page 21)

In-service MAS rejects calls recovery tree

Use the following recovery tree when an in-service MAS rejects calls.

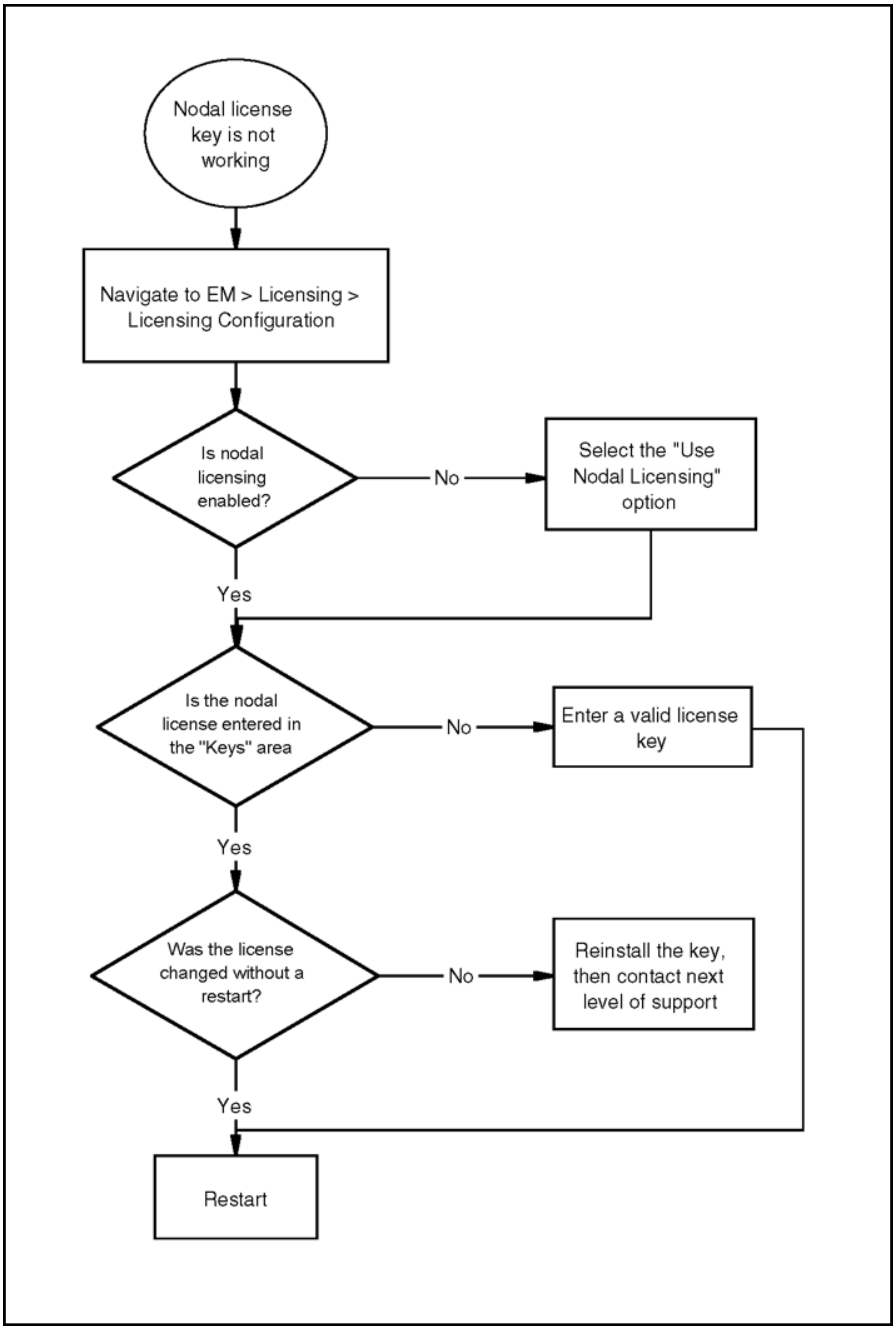
Figure 1
In-service MAS rejects calls recovery tree


In-service MAS rejects calls
Navigate to EM > Licensing > Licensing Configuration
Is required Licensing enabled?
Yes
No
Add the required application and platform licenses
Restart
Still rejecting calls?
Yes
No
Calls accepted
Navigate to EM > System Configuration > Signaling > SIP > Nodes and Routes
Are all the required Trusted Nodes configured?
Yes
No
Enter required SIP Trusted Nodes
Navigate to EM > System Configuration > Signaling > SIP > Nodes and Routes
Are all the required SIP routes configured?
Yes
No
Enter required SIP trusted nodes
Navigate to EM > Products and Applications
Are all the required applications installed and configured?
Yes
No
Install and configure required applications and licensing
Navigate to EM > System Status > Element Status
Is the MAS in an unlocked state?
Yes
No
Contact next level of support
In the More Actions list, select Unlock

Nodal license is not working recovery tree

Use the following recovery tree when the nodal license is not working.

Figure 2
Nodal license is not working recovery tree


Nodal license key is not working
Navigate to EM > Licensing > Licensing Configuration
Is nodal licensing enabled?
No
Select the "Use Nodal Licensing" option
Yes
Is the nodal license entered in the "Keys" area
No
Enter a valid license key
Yes
Was the license changed without a restart?
No
Reinstall the key, then contact next level of support
Yes
Restart

Emergency security

Perform emergency security procedures to access Element Manager (EM) if the security servers are down.

Navigation

- "Local authentication on the MAS in emergencies" (page 23)

Local authentication on the MAS in emergencies

Authenticate locally on the Media Application Server (MAS) during an emergency to log on to Element Manager if your security servers are down.

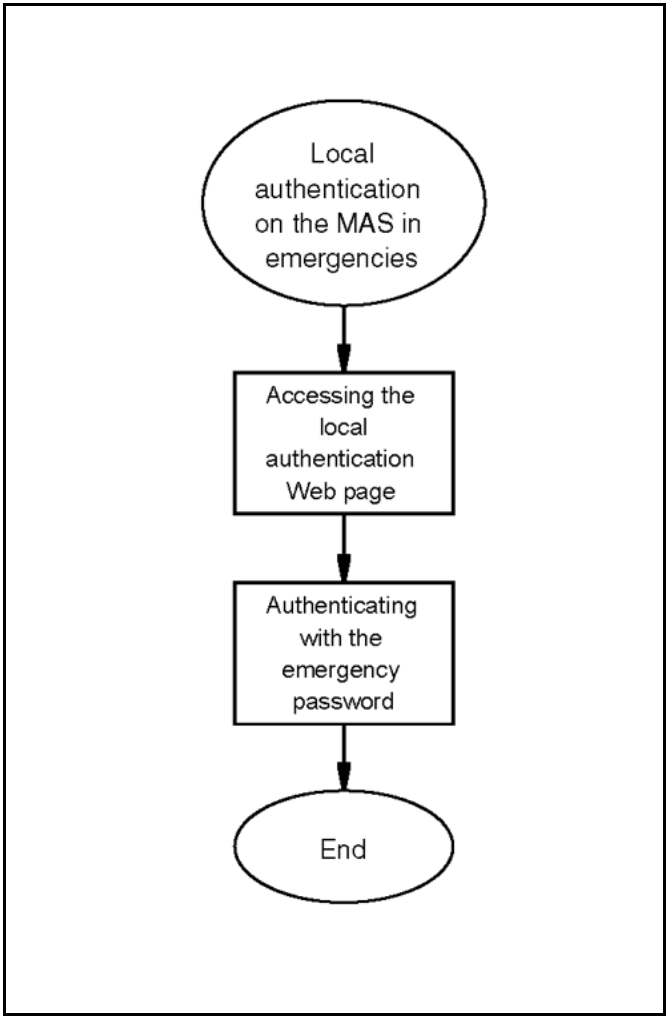
Prerequisites to local authentication on the MAS in emergencies

- Create an emergency account and password.

Local authentication on the MAS in emergencies procedures

This task flow shows you the sequence of procedures you perform to authenticate locally on the MAS during an emergency. To link to any procedure, go to "Local authentication on the MAS in emergencies navigation" (page 24).

Figure 3
Local authentication on the MAS in emergencies procedures


Local authentication on the MAS in emergencies
Accessing the local authentication Web page
Authenticating with the emergency password
End

Local authentication on the MAS in emergencies navigation

- "Accessing the local authentication Web page" (page 58)
- "Authenticating with the emergency password" (page 58)

Unified Communications Management

This section provides details, possible causes, and solutions for common issues and error messages that relate to Unified Communications Management (UCM).

Navigation

Server error on UCM pages when using 3-tier domains in FQDN

After you install and configure the Unified Communications Management (UCM) security server, UCM pages such as the policy page do not open but give a Server Error. In addition, the Logout link does not work; it redirects you back to the Element List in the Navigator.

Possible causes

UCM incorrectly configures the single sign-on (SSO) cookie domain because the configured FQDN is a 3-tier domain ending in a country code. For example, if the FQDN is hostname.avaya.com.uk, UCM incorrectly configures the SSO cookie domain to .com.uk, which most browsers reject.

Solutions

To resolve this problem, do the following:

1. Open a Firefox 2.x web browser.
2. In the Firefox 2.x web browser, log on to UCM as normal.

   UCM works correctly because Firefox 2.x does not block the cookie.
3. On the navigation menu, click **Security**, **Policies**.
4. In the **Single Sign-on Cookie Domain** pane, click **Edit**.
5. On the **Edit Domain Name** page, in the **Single Sign-on Cookie Domain** list, select the proper domain.

For example, if the FQDN is avaya.com.uk, UCM selects com.uk by default. However, you must select avaya.com.uk in the Single Sign-on Cookie Domain list instead.

6. Click **Save**.

   All browsers types such as IE 6.0, IE 7.0, and Firefox 3.x now work correctly.

An item CND appears as Failed at the last step of UCM initial security configuration

After installation, during the last step of Unified Communications Manager (UCM) initial security configuration, the system displays the Common Network Directory (CND) as Failed.

Potential Causes

Something goes wrong in the related certificate or Lightweight Directory Access Protocol (LDAP) on the local server.

Solutions

To resolve this problem, perform a Clean Install of the software, as follows:

1. Optionally, back up your service data. For information about the backup and restore procedure, see *Avaya Media Application Server Administration and Security* (NN44474-600).
2. Take note of your MAS configuration data on Element Manager.
3. Uninstall the MAS platform, ensuring that you do not select the option to preserve data during the uninstall. For information about the uninstall procedure, see *102.1.6 AS5300 MAS Platform and Application Installation*.
4. Install the new MAS load.
5. Optionally, restore the backed-up service data.
6. Configure settings as required on Element Manager.

Other issues

You experience issues other than those described in this document.

Possible causes

Not Available.

Solutions

To resolve other issues, review the UCM security configuration procedure described in *Avaya Media Application Server Administration and Security* (NN44474-600) first. If the solution is not available, contact Avaya Support personnel.

MAS General Issues

This module provides details, possible causes, and solutions for common issues and error messages that relate to general Media Application Server (MAS) issues when you use the MAS with Avaya Aura™ Application Server 5300 systems.

Navigation

Nodal license key is not working

The existing nodal license key is not working.

Possible causes

The Use License Server scheme is enabled, instead of the Use Nodal License scheme.

Solutions

Enable the Use Nodal License scheme, as follows:

1. In Element Manager, navigate to **Licensing**, **Licensing Configuration**.
2. To enable nodal licensing, select the **Use Nodal Licensing** option.
3. In the **Keys** area, enter the nodal license keys.
4. Click **Save**.
5. Restart the node.

Unified Communications

This module provides details, possible causes, and solutions for common issues and error messages that relate to Unified Communications issues when you use MAS with Avaya Aura™ Application Server 5300 systems.

Navigation

MWI does not light for new voice mail messages

New messages left for a Unified Communications subscriber do not cause the subscriber’s Message Waiting Indicator (MWI) lamp to light. However, the message is actually present and can be retrieved.

Possible causes

A Session Initiation Protocol (SIP) route to the proxy is not defined on the Media Application Server (MAS).

Solutions

To resolve this problem, do the following:

1. In Element Manager, navigate to **System Configuration**, **Signaling**, **SIP**, **Nodes and Routes**.
2. Ensure that a route to the proxy exists for the subscriber’s domain.
3. If a route to the proxy does not exist, add the proxy to the trusted nodes list. For information about adding SIP trusted nodes and routes, see *Avaya Media Application Server Commissioning* (NN44474-301).

Calls do not rollover automatically to voice mail

Calls to a user who is either not logged on or does not answer the call, do not rollover automatically to voice mail. However, calls to Express Messaging and Message Retrieval can still be completed.

Possible causes

The VMS Host configuration on the Avaya Aura™ Application Server 5300 provisioning system is incorrect.

Solutions

This is not a MAS issue. However, you can resolve the issue on the Avaya Aura™ Application Server 5300 provisioning system.

1. From the Application Server 5300 Provisioning Client menu, select **Services, Call Termination, Voicemail**.
2. On the **VMS Host** tab, in the table, click the name of the voice mail host.
3. Verify that the Host Address is a Host URL and not a preconfigured Address Name.
4. Verify that the URL appears in the following format: **sip:ucmsgrtv@<yourDomain>;trusted**
5. Replace **<yourDomain>** with the name of the domain for the VMS Host.

Media

This module provides details, possible causes, and solutions for common issues and error messages that relate to Media issues.

Navigation

Digit collection issues and login failures

Users are unable to log on to Media Application Server (MAS) services because of problems occurring with digit collection.

Possible causes

If the client is connecting to the MAS through a Public Switched Telephone Network (PSTN) or other form of internet gateway device; then that device must be configured to properly translate digits to the format it negotiates with the MAS. You can use three digit signaling formats: Inband Dual-Tone Multi-Frequency (DTMF) tones, RFC 2833 telephone events, and SIP INFO digits. Both the client and the gateway device must communicate digits according to the methodology that they signal to the MAS and they must use only that methodology. If necessary, collect SIP messaging to resolve the nature of digit communication between the client, gateway, and MAS.

In some cases (as with conferencing), users can feed digits into the conference through their microphone. These digits carry into the conference and are detected as conference controls. For example, during a conference a user dials a number on a nearby speakerphone, which is not involved in the conference, and those digits carry into the conference. When users report digit collection issues, ask about their client type and surroundings to identify the cause of any unexpected conference behaviors. Similarly, some gateways that translate inband digits into events (such as telephone-event or INFO digits) fail to completely clamp the received tones. These tones are heard by the MAS and can trigger unexpected behavior.

Solutions

Configure the appropriate mode of digit transport from the clients and/or gateways for your installation.

Adjust any digit translating gateway device to fully clamp inband DTMF tones.

Unsupported CODEC when calling MAS

The MAS rejects incoming calls and indicates there is no supported CODEC.

Possible causes

When the MAS is configured for **SECURITY ENFORCED** mode, it does not accept calls from clients offering unsecure media.

Solutions

If the intent is to allow these calls, use the **BEST EFFORT** security policy.

1. In Element Manager, navigate to **System Configuration**, **Media**, **Media Security**.
2. In the Security Policy list, select **BEST EFFORT**.
3. Click **Save**.

If the security settings are not the cause, then the session incoming to the MAS is not offering a supported audio CODEC.

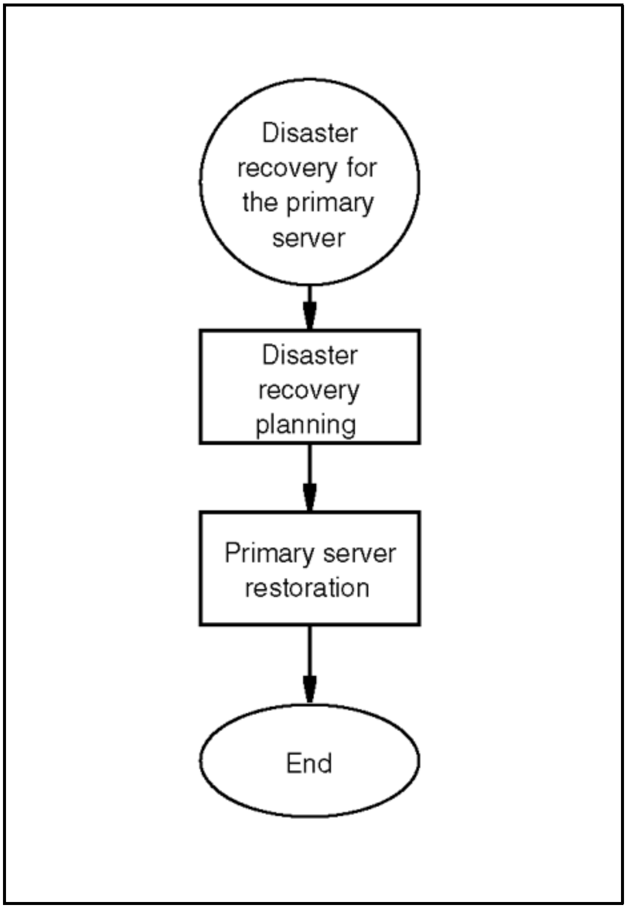
Disaster recovery for the primary server

Recover the primary server to restore critical operations if you experience a disaster situation. To ensure successful recovery, you must implement a disaster recovery plan when you configure a Media Application Server (MAS). For information about disaster recovery planning, see *Avaya Media Application Server Administration and Security* (NN44474-600).

Disaster recovery for the primary server tasks

This work flow shows you the tasks you perform to recover the primary server. To link to any task, go to "Disaster recovery for the primary server navigation" (page 36).

Figure 4
Disaster recovery for the primary server tasks


Disaster recovery for the primary server
Disaster recovery planning
Primary server restoration
End

Disaster recovery for the primary server navigation

- For information about disaster recovery planning, see *Avaya Media Application Server Administration and Security* (NN44474-600).
- "Primary server restoration" (page 36)

Primary server restoration

Restore the primary server to reestablish critical operations after you experience a disaster situation.

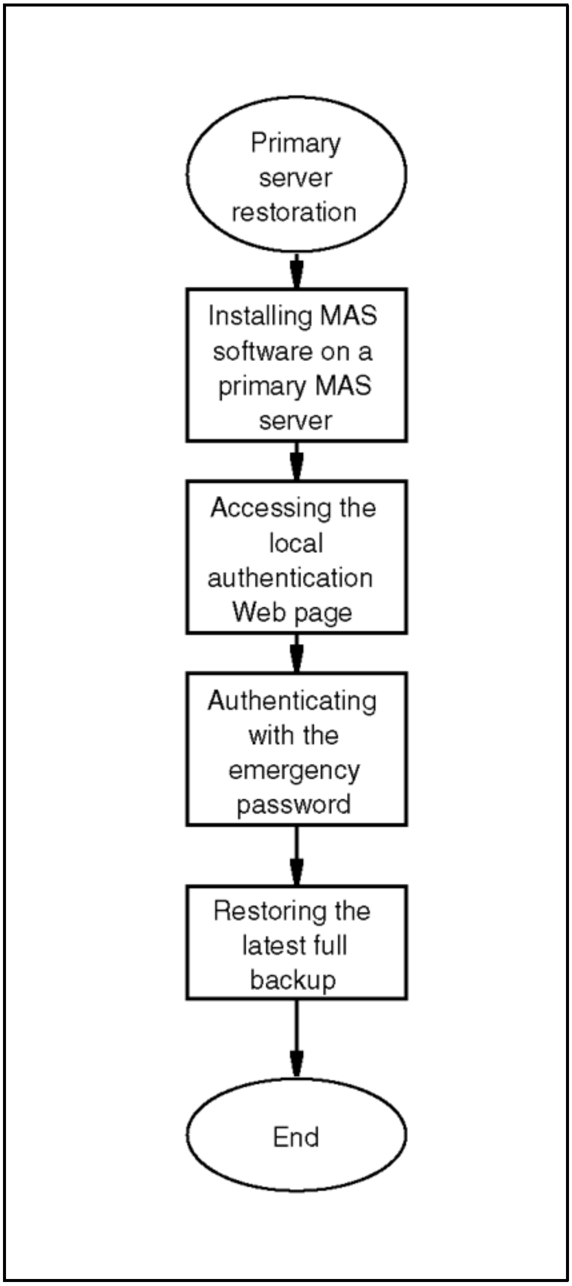
Prerequisites to primary server restoration

- Ensure that you use the same fully qualified domain name (FQDN) and IP address for the new primary as you did for the primary that you are restoring.

Primary server restoration procedures

This task flow shows you the sequence of procedures you perform to restore the primary server. To link to any procedure, go to "Primary server restoration navigation" (page 38).

Figure 5
Primary restoration procedures


Primary server restoration
Installing MAS software on a primary MAS server
Accessing the local authentication Web page
Authenticating with the emergency password
Restoring the latest full backup
End

Primary server restoration navigation

- "Installing Media Application Server software on a primary MAS server" (page 38)
- "Accessing the local authentication Web page" (page 58)
- "Authenticating with the emergency password" (page 58)
- "Restoring the latest full backup" (page 38)

Installing Media Application Server software on a primary MAS server

Install Media Application Server (MAS) software on a primary MAS server to establish both the application server/media server platform and the framework for running standards-based multimedia applications.

For information about installing MAS platform software, see *102.1.6 AS5300 MAS Platform and Application Installation*.

Restoring the latest full backup

Restore the latest full backup to recover your original data. For information about restoring the latest full backup, see *Avaya Media Application Server Administration and Security* (NN44474-600).

Reporting

This module provides details, possible causes, and solutions for common issues and error messages that relate to reporting. Use the information in the following table to interpret terms that are used in some solutions.

Terms	Interpretation
`<jboss>`	Directory where JBoss is installed. Example: `D:\Program Files\SelfService\jboss-4.2.1.GA`
`<mysql>`	Directory where MySQL is installed. Example: `D:\Program Files\SelfService\MySQL`
`default`	The JBoss server may be configured to use a server other than the default server. In this case, replace `default` with the name of the JBoss server.

Navigation

- "Immediate execution of report times out" (page 39)
- "E-mail not sent after report is configured" (page 40)
- "Java Out of Memory error" (page 41)
- "Recurring scheduled job does not create report or report is empty" (page 41)
- "Report shows Start as 00:00:00 and not as the default Start value" (page 42)
- "Scheduled job fails to execute" (page 42)
- "Report e-mailed only to first address in recipient list" (page 43)

Immediate execution of report times out

You select an SDR report, specify parameters, and run the report. However, the report is not visible after a period of time has elapsed.

Possible causes

The amount of data to process takes longer than a preconfigured JasperServer connection timeout period.

Solutions

Specify a smaller set of parameters or submit the report to run in the background.

E-mail not sent after report is configured

The report is configured with e-mail notification or was sent as an attachment to an e-mail, but the e-mail is not sent.

Possible causes

There can be two possible causes for this problem.

E-mail not configured

The e-mail configuration file is configured incorrectly.

System cannot connect to mail server

The Mail Exchange server and port number are incorrect.

Solutions

Each solution addresses a possible cause.

Configure e-mail

Edit the following file and specify the `host`, `username`, `password`, `from`, `protocol`, and `port`. The text entry is modified to encrypt the password using a Java Bean mechanism.

```
<jboss>\server\default\deploy\jasperserver-pro.war\WEB-INF\js.mail.properties
```

Connect to mail server

Use Telnet to verify that the Mail Exchange server and port number are correct. These values must be correct to establish a successful connection between the client and the server.

Two sample Telnet sessions follow. The sessions demonstrate both a successful and an unsuccessful connection between the client and server. In each sample Telnet session, `<C>` represents the client and `<S>` represents the server.

- Successful connection Telnet session sample

```
<C> telnet mymailserver 25
<S>220 mymailserver.corp.nortel.com Microsoft ESMTP
MAIL Service, Version:  6.0.3790.183 0 ready at Thu, 17
Apr 2008 08:53:56 -0400
<C>helo
<S>250 mymailserver.corp.nortel.com Hello
[47.102.169.62]
<C>quit
```

```
<S>221 2.0.0 mymailserver.corp.nortel.com Service
closing transmission channel Connection to host lost.
```

- Unsuccessful connection Telnet session sample

```
<C> telnet mymailserver 25
Connecting To mymailserver...Could not open connection
to the host, on port 25:  Connect failed
```

Invalid delivery e-mail address to the JasperServer

Reporter subsystem generates no error for invalid delivery e-mail address to the JasperServer.

Possible causes

Reporter subsystem does not generate error at run time if the administrator configures an invalid return e-mail address for e-mail messages sent by the JasperServer. The recipient of an e-mail message sent by the JasperServer attempts to reply, but no valid return e-mail address exists.

Solutions

If the customer system administrator requires the recipient of the e-mail sent by JasperServer to reply to the e-mail, you must specify a valid source e-mail address. This source e-mail address receives the replies from the recipients of the JasperServer e-mail messages.

Java Out of Memory error

Java Out of Memory errors display or are logged during report execution.

Possible causes

The amount of data exceeds Java memory settings.

Solutions

Modify the report parameters to select a smaller set of data.

Recurring scheduled job does not create report or report is empty

At the time of the scheduled report execution, the JasperServer log shows the message:

```
ERROR ReportExecutionJob, JasperServerScheduler_Worker-0
:208 - org.acegisecurity.AccessDeniedException:  Access
is denied.
```

Possible causes

Possible causes for this problem are:

- The folder specified as Content Repository has improper access rights.
- A report with same name in the Content Repository exists and no option is selected to Overwrite or use Sequential File Names when scheduling the job.

Solutions

Use the following actions to resolve this problem.

- Modify the access rights to the Content Repository folder.
- In the parameters for the scheduled job, select the check box in the Content Repository options to specify either Sequential File Names and/or Overwrite Files. For more information about scheduling jobs, see *Avaya Media Application Server Administration and Security* (NN44474-600).

Report shows Start as 00:00:00 and not as the default Start value

When you choose a report, the Start parameter is configured to 01-24-2008 05:00:00. The default setting is 00:00:00. When you run the report, the Start value shows 01-24-2008 00:00:00.

Possible causes

The JasperServer was started with a Time Zone different from the system's Time Zone configuration.

Solutions

During the logon operation, change the JasperServer Time Zone setting to match the system's Time Zone.

Scheduled job fails to execute

A scheduled job is created and executes the first time without error. However, for every subsequent execution of the scheduled job, they system displays an error message (The job failed to execute) and the job fails to execute.

Possible causes

Parameters for creating and storing recurring or subsequent report files are configured incorrectly. When you create a scheduled job, the system displays two check boxes in the **Content Repository** section of the **Output** pane: **Sequential File Names** and **Overwrite Files**. Every time a recurring scheduled job executes, a report is generated; these check boxes indicate how the system should create and store report files.

Leaving both of these two check boxes unchecked allows the first report to generate successfully after the first execution of the job. Subsequent job executions fail because you must specify how the system generates and stores a recurring scheduled task report.

Solutions

To resolve this problem, specify scheduled job report handling by selecting either **Sequential File Names** or **Overwrite Files**.

Report e-mailed only to first address in recipient list

An e-mailed report is sent to the first address in the recipient list, and is not sent to any other addresses in the list.

Possible causes

E-mail addresses in the recipient list are specified using semicolons as separators.

Solutions

Specify the e-mail addresses in the recipient list using commas as separators.

Security

This module provides details, possible causes, and solutions for common issues and error messages that relate to security. For additional information about security, see *Avaya Media Application Server Administration and Security* (NN44474-600).

Navigation

- "TLS connection issues" (page 45)

TLS connection issues

This topic describes various errors or problems that relate to establishing Transport Layer Security (TLS) connections.

Possible causes

Any of the following items can cause TLS connection issues.

- Certificates on either side of the attempted connection are expired.
- Trust Anchor configuration incomplete.
- TLS change made that requires a MAS Restart to take effect.
- All nodes in a cluster are not TLS enabled.
- IP address of the server was changed.
- Configuration is incomplete.
- A backup file containing expired certificates or improper TLS configuration settings was restored.

Solutions

Many configuration items are required for proper TLS configuration in a MAS cluster. Refer to the proper Security configuration documents and ensure that all settings are implemented correctly. Some common solutions follow:

- Ensure certificates on either side of the attempted connection are not expired.
- Ensure the Trust Anchor is in the Trust Store on all cluster nodes.

- Some TLS changes require a MAS Restart to take effect. In these cases, a message appears indicating a restart is required. In these cases, restarting the MAS enables the desired configuration.
- Ensure that all nodes in a cluster are TLS enabled for every interface.
- When the IP address of a server changes, new certificates may be required if you select **Subject Alt Name** to use an alternate name for the server. For information about configuring TLS, see *Avaya Media Application Server Administration and Security* (NN44474-600).
- If a restored backup file contains expired certificates or improper TLS configuration settings, update the certificates or TLS configurations. For more information about certificates and TLS configuration settings, see *Avaya Media Application Server Administration and Security* (NN44474-600).

SIP

This module provides details, possible causes, and solutions for common issues and error messages that relate to Session Initiation Protocol (SIP).

For more information about SIP response messages, see "Appendix: SIP response messages" (page 59).

Navigation

- "Calls rejected with reason 403 Use Proxy" (page 47)
- "Calls redirected with reason 305 Use Proxy" (page 47)

Calls rejected with reason 403 Use Proxy

Calls to the MAS do not complete and are rejected with reason code 403 Use Proxy. MAS generates an event titled Default proxy not provisioned. Reject call from 47.101.23.30 with 403.

Possible causes

SIP trusted nodes are not defined.

Solutions

Ensure that the node is configured as trusted.

1. In Element Manager, navigate to **System Configuration**, **Signaling**, **SIP**, **Nodes and Routes**.
2. Under **Trusted Nodes**, ensure that the proxy IP address the client uses is configured as trusted.
3. If the proxy IP address is not configured as trusted, add the proxy to the trusted nodes list.

Calls redirected with reason 305 Use Proxy

Calls to the MAS do not complete and are redirected to the configured default outgoing proxy with reason code 305 Use Proxy.

Possible causes

Calls can be rejected with the 305 Use Proxy reason code because SIP trusted nodes are not defined.

Solutions

To resolve the 305 Use Proxy error, do the following:

1. In Element Manager, navigate to **System Configuration**, **Signaling**, **SIP**, **Nodes and Routes**.
2. In the **Trusted Nodes** section, ensure that the proxy IP address used by the client is configured as trusted.
3. If the proxy IP address used by the client is not configured as trusted, click **Add**. For more information about adding SIP Trusted Nodes and SIP routes, see *102.1.6 AS5300 MAS Platform and Application Installation*.

SNMP

This module provides details, possible causes, and solutions for common issues and error messages that relate to Simple Network Management Protocol (SNMP).

Navigation

- "MAS alarms do not appear on Element Manager" (page 49)

MAS alarms do not appear on Element Manager

SNMP Traps are not posting to the monitoring system management servers.

Possible cause

Network problems

Network problems can cause alarms not to appear in Element Manager.

Solution

1. Verify that the monitoring system can ping the MAS.
2. If the ping fails, troubleshoot the network connection between the monitoring system and the MAS

Common procedures

The following chapter describes common procedures that you use while troubleshooting the Media Application Server (MAS).

Navigation

Logging on to the UCM

Log on to the UCM interface to configure central authentication, authorization, and auditing for the MAS servers, or to access the Element Managers for MAS servers.

Prerequisites

- UCM must be configured on all application servers.
- You must be an administrator with a valid user ID and password to access UCM. (A local user can also log on to UCM but has less permission.)
- When you access Element Manager from a Web browser, Host name to IP translation solution is required.

Procedure steps

Step	Action
1	From the local console, double-click the **Element Manager** icon on the desktop.
2	Click the link that appears on the browser window. The link is the Fully Qualified Domain Name (FQDN) of the UCM server. If you want to access Element Manager from a Web browser, use the following Uniform Resource Locator (URL): https://<FQDN of MAS>:8443
3	Click **OK** or **Yes** in the security dialog boxes that appear.
4	On the **UCM Login** page, in the **User ID** field, enter the user ID.
5	On the **UCM Login** page, in the **Password** field, enter the password.
6	Click **Log In**.
7	To access an Element Manager for a server , on the **Unified Communications Management** page, under the **Element Name** column, click the name of the server.

--End--

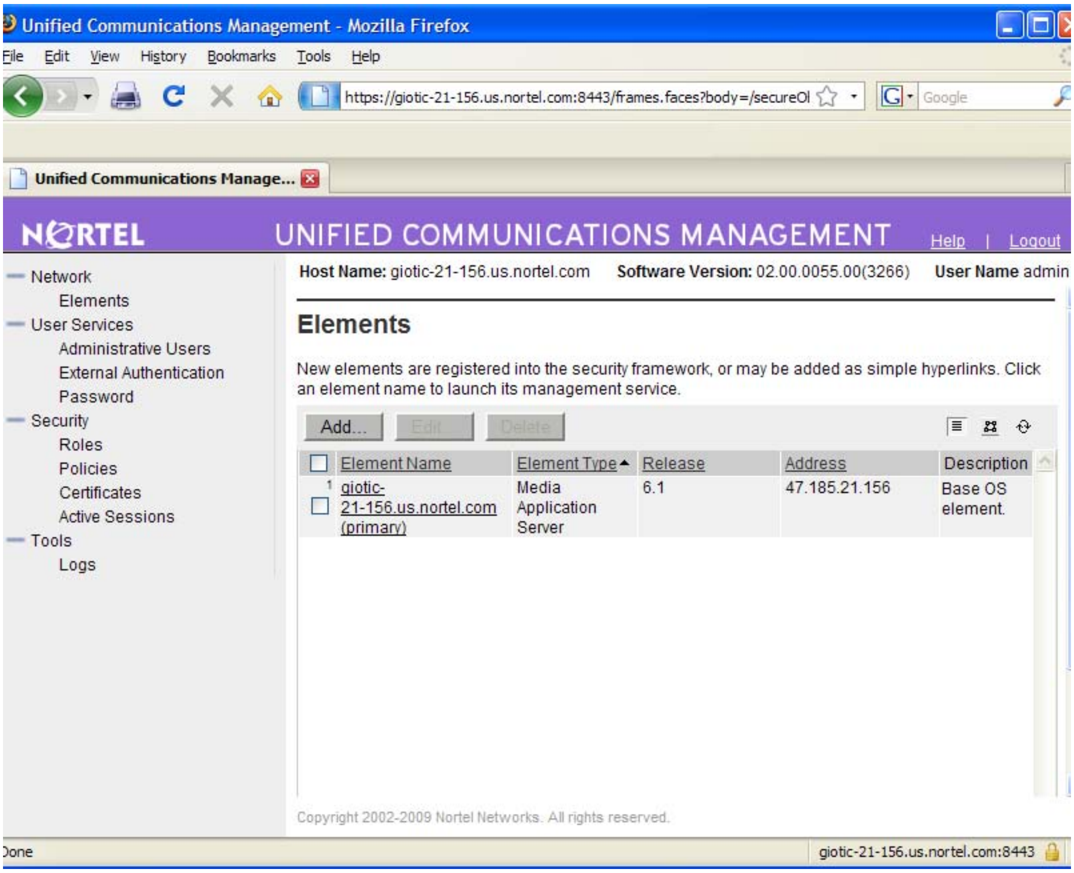
Variable definitions

Variable	Value
Password	The password used to log on to UCM.
User ID	The user ID for UCM.

Logging on to the UCM job aid

The following graphics show the main page of the Unified Communications Management (UCM) and the welcome page in Element Manager.

Figure 6
UCM main page



https://giotic-21-156.us.nortel.com:8443/frames.faces?body=/secureOl

Host Name: giotic-21-156.us.nortel.com **Software Version:** 02.00.0055.00(3266) **User Name** admin

Elements

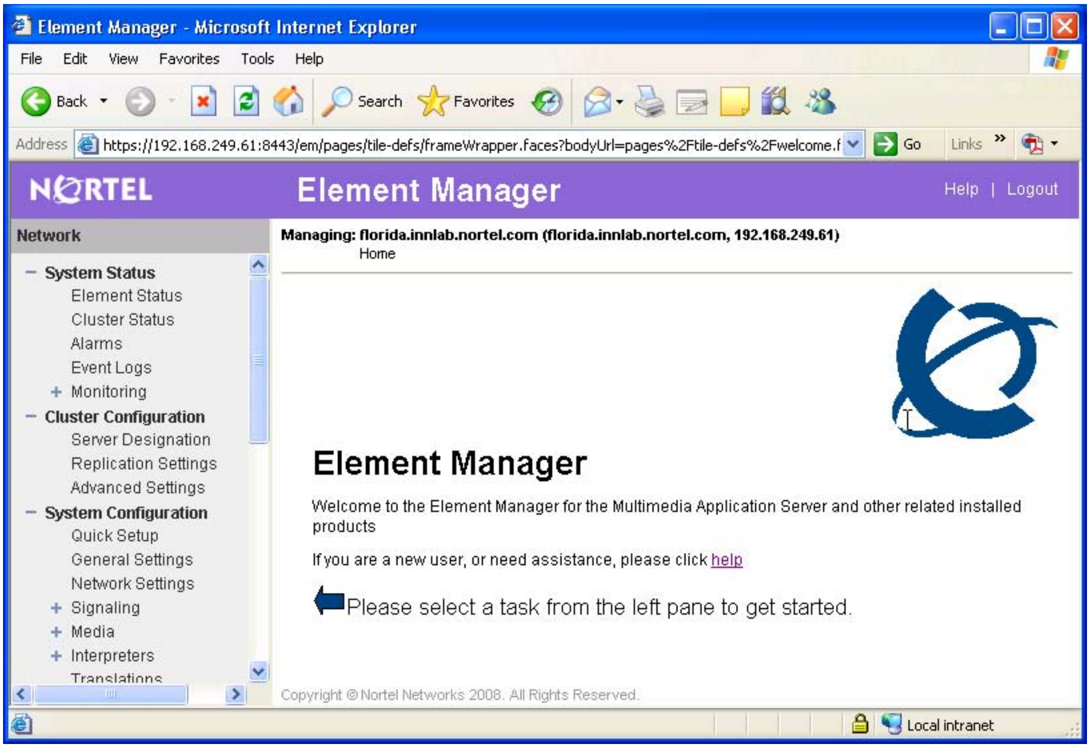
New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service.

□	Element Name	Element Type	Release	Address	Description
1 □	giotic-21-156.us.nortel.com (primary)	Media Application Server	6.1	47.185.21.156	Base OS element.

Copyright 2002-2009 Nortel Networks. All rights reserved.

giotic-21-156.us.nortel.com:8443

Figure 7
Element Manager welcome page



Managing: florida.innlab.nortel.com (florida.innlab.nortel.com, 192.168.249.61)
Home

Element Manager

Welcome to the Element Manager for the Multimedia Application Server and other related installed products

If you are a new user, or need assistance, please click help

Please select a task from the left pane to get started.

Copyright © Nortel Networks 2008. All Rights Reserved.

Restarting the MAS

Use the following procedure to restart the MAS.

Attention: Some configuration procedures require that you restart the MAS before configuration changes take effect. You can perform multiple procedures that require a restart of the MAS service, and then restart the MAS once.

Prerequisites

- Log on to UCM and navigate to Element Manager. For more information, see "Logging on to the UCM" (page 51).
- The Service Status of the MAS must be configured to Started before you can restart the MAS.

Procedure steps

Step	Action
1	In the navigation pane, click **System Status, Element Status**.
2	Click **Restart**.
3	Read the warning that appears and click **Confirm** to restart the system.

--End--

Starting the MAS

Use the following procedure to start the MAS.

Prerequisites

- Log on to UCM and navigate to Element Manager. For more information, see "Logging on to the UCM" (page 51).
- The Service Status of the MAS must be configured to Stopped before you can start the MAS.

Procedure steps

Step	Action
1	In the navigation pane, click **System Status, Element Status**.
2	Click **Start**. If the MAS is already active, the Start button appears dimmed.
3	Read the warning that appears and click **Confirm** to start the system.

--End--

Stopping the MAS

Use the following procedure to stop the MAS.

Prerequisites

- Log on to UCM and navigate to Element Manager. For more information, see "Logging on to the UCM" (page 51).
- The Service Status of the MAS must be configured to Started before you can stop the MAS.

Procedure steps

Step	Action
1	In the navigation pane, click **System Status, Element Status**.
2	Click **Stop**. If the MAS is already stopped, the Stop button appears dimmed.
3	Read the warning that appears and click **Confirm** to stop the system.

--End--

Locking the MAS

Use this procedure to lock the MAS. If you lock the MAS, the system terminates all active sessions (existing calls) and redirects new traffic.

You typically place the system into a Locked state when performing maintenance.

Prerequisites

- Log on to UCM and navigate to Element Manager. For more information, see "Logging on to the UCM" (page 51).

Procedure steps

Step	Action
1	In the navigation pane, click **System Status, Element Status**.
2	From the **More Actions** list, select **Lock** to lock the MAS. If the MAS is already locked, the Lock option does not appear.
3	Read the warning that appears and click **Confirm** to lock the system.

--End--

Locking the MAS with a pending lock

Use the Pending Lock option to lock the MAS. You use this procedure to transition call processing to a locked state. Using this method, the system allows all active sessions (existing calls) to finish and redirects new traffic. The MAS locks after all active sessions complete.

Prerequisites

- Log on to UCM and navigate to Element Manager. For more information, see "Logging on to the UCM" (page 51).

Procedure steps

Step	Action
1	In the navigation pane, click **System Status, Element Status**.
2	From the **More Actions** list, select **Pending Lock** to lock the MAS after all processes finish. If a pending lock is already requested, the Pending Lock option does not appear.
3	Read the warning that appears and click **Confirm** to lock the system with a pending lock.

--End--

Unlocking the MAS

Use this procedure to unlock the MAS. If the MAS is locked, no applications or services can function.

After the system is unlocked, the MAS can perform normal call processing.

Prerequisites

- Log on to UCM and navigate to Element Manager. For more information, see "Logging on to the UCM" (page 51).
- The MAS server must be locked or pending locked before you can unlock the MAS.

Procedure steps

Step	Action
1	In the navigation pane, click **System Status, Element Status**.
2	From the **More Actions** list, select **Unlock** to unlock the MAS. If the MAS is already unlocked, the Unlock option does not appear.
3	Read the warning that appears and click **Confirm** to unlock the system.

--End--

Accessing the local authentication Web page

Access the local authentication Web page to navigate to Element Manager if the security servers are down.

Procedure steps

Step	Action
1	On your local system, open an Internet browser window.
2	In the address bar, enter the Uniform Resource Locator (URL) of the local logon page: **http://<server FQDN>/local-login**.

--End--

Variable definitions

Variable	Value
server FQDN	The fully qualified domain name (FQDN) of the server.

Authenticating with the emergency password

Authenticate with the emergency password to log on to Element Manager if the security servers are down.

Prerequisites

- Preconfigure the emergency account using the Linux User Management Configuration tool. For information about configuring the emergency account, see *Avaya Media Application Server Administration and Security* (NN44474-600).

Procedure steps

Step	Action
1	On the local logon page, type your emergency account credentials.
2	Click **Log In**.
3	Click **Local Administration**.

--End--

Appendix: SIP response messages

This section describes the SIP response messages that are supported in the current release of the Announcements service.

- "Request failure 4xx" (page 59)
- "Server failure 5xx" (page 60)
- "Global failure 6xx" (page 60)

Request failure 4xx

4xx responses indicate that the user should not retry the same request without modification (for example, adding appropriate authorization). However, the same request to a different server might be successful.

Table 1
Treatment (cause) group reasons

Treatment (cause) reason	Message number
BAD_REQUEST	400
UNAUTHORIZED	401
PAYMENT_REQUIRED	402
FORBIDDEN	403
NOT_FOUND	404
METHOD_NOT_ALLOWED	405
NOT_ACCEPTABLE	406
PROXY_AUTHENTICATION_REQUIRED	407
REQUEST_TIMEOUT	408
CONFLICT	409
GONE	410
LENGTH_REQUIRED	411
PRECONDITION_FAILED	412
REQUEST_ENTITY_TOO_LARGE	413
REQUEST_URI_TOO_LONG	414

Table 1
Treatment (cause) group reasons (cont'd.)

Treatment (cause) reason	Message number
UNSUPPORTED_MEDIA_TYPE	415
BAD_EXTENSION	420
TEMPORARILY_UNAVAILABLE	480
CALL_LEG_TRANSACTION_DOES_NOT_EXIST	481
LOOP_DETECTED	482
TOO_MANY_HOPS	483
ADDRESS_INCOMPLETE	484
AMBIGUOUS	485
BUSY_HERE	486
REQUEST_TERMINATED	487
NOT_ACCEPTATBLE_HERE	488
EVENT_NOT_SUPPORTED	489
REQUEST_PENDING	491

Server failure 5xx

5xx responses are failure responses given when a server has erred.

Table 2
Treatment (cause) group reasons

Treatment (cause) reason	Message number
SERVER_INTERNAL_ERROR	500
NOT_IMPLEMENTED	501
BAD_GATEWAY	502
SERVICE_UNAVAILABLE	503
GATEWAY_TIMEOUT	504
VERSION_NOT_SUPPORTED	505

Global failure 6xx

6xx responses indicate that a server has definitive information about a particular user, not just the particular instance indicated in the Request-URI.

Table 3
Treatment (cause) group reasons

Treatment (cause) reason	Message number
BUSY_EVERYWHERE	600

Table 3
Treatment (cause) group reasons (cont'd.)

Treatment (cause) reason	Message number
DECLINE	603
DOES_NOT_EXIST_ANYWHERE	604
NOT_ACCEPTABLE	606