Avaya Agile Communication Environment™ Message Drop and Message Blast Administration

Release 6.2
NN10850-025
Issue 05.01
July 2013
© 2013 Avaya Inc.
All Rights Reserved.

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 additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees 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.

Documentation disclaimer
“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees 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.

Warranty
Avaya provides a limited warranty on its hardware and Software (“Product(s)”). 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 website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

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 CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA CHANNEL PARTNER. 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 AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, 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”).

Avaya grants you a license within the scope of the license types described below, with the rights, restrictions, and limitations set forth below, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The number of licenses and units of capacity for which the license is granted will be on (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License types
CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Heritage Nortel Software
“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright
Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product 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 unless expressly authorized by Avaya. 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.

Virtualization
Each vAppliance will have its own ordering code. Note that each instance of a vAppliance must be separately ordered. If the end user customer or Avaya channel partner would like to install two of the same type of vAppliances, then two vAppliances of that type must be ordered.
Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation 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 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. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.
Contents

Chapter 1: Introduction........................................................................................................... 7
  Purpose................................................................................................................................. 7
  Intended audience................................................................................................................ 7
  Document changes since last issue.................................................................................. 7
  Related resources................................................................................................................ 7
    Documentation................................................................................................................ 7
    Training............................................................................................................................ 10
    Avaya Mentor videos....................................................................................................... 10
  Support............................................................................................................................... 11

Chapter 2: Message Drop and Message Blast overview..................................................... 13
  Click-to-Dial....................................................................................................................... 14
  Message Drop.................................................................................................................... 14
  Message Drop and Leave.................................................................................................. 14
  Message Record................................................................................................................ 15
  Message Review.................................................................................................................. 16
  Message Blast.................................................................................................................... 16
  Message Drop and Blast LDAP lookup service............................................................... 16
  Message Drop and Message Blast logs........................................................................... 18

Chapter 3: Message Drop and Message Blast service deployment...................................... 21

Chapter 4: Avaya ACE configuration.................................................................................. 23
  Configuring a user profile for Message Drop and Message Blast service....................... 29
  Configuring the route address.......................................................................................... 28
  Configuring translation rules............................................................................................ 29
  Message Drop and Message Blast provisioning considerations........................................ 29

Chapter 5: Message Drop and Message Blast configuration.............................................. 33
  Configuring Message Drop and Message Blast authorization........................................ 35
  Configuring the Message Drop and Message Blast service............................................ 36
  Configuring a Message Blast schedule............................................................................. 38
  Downloading the LDAP Provisioning Tool......................................................................... 39
  Loading an LDAP server configuration file........................................................................ 39
  Adding a new LDAP server entry...................................................................................... 40
  Cloning an LDAP server entry......................................................................................... 44
  Adding an LDAP server address rule............................................................................... 44
  Validating LDAP server configuration............................................................................ 46
  Applying the LDAP server configuration file................................................................. 47

Chapter 6: Managing the Message Drop and Message Blast ACE user password............... 49

Chapter 7: Troubleshooting the Avaya Media Server.......................................................... 51
  Disabling the media security policy.................................................................................. 51
  Monitoring active calls on the Avaya Media Server....................................................... 52
  Enabling debug logging on the Avaya Media Server...................................................... 52
  Verifying the Avaya Media Server media configuration.................................................. 53
Chapter 1: Introduction

Purpose

This document contains information on configuration and administration of Message Drop and Message Blast service on Avaya Agile Communication Environment™.

Intended audience

The primary audience for this document is anyone who must configure, administer, troubleshoot Message Drop and Message Blast service on Avaya ACE™. The audience includes implementation engineers, field technicians, and customers.

Document changes since last issue

The following are the changes to Avaya Agile Communication Environment™ Message Drop and Message Blast Administration (NN10850–025) for Avaya ACE Release 6.2.1:

• Added purpose, audience, help resources, and support information to the Introduction chapter.

Related resources

Documentation

This document is a part of the Avaya ACE documentation suite. Avaya ACE documents provide information on Avaya ACE fundamentals and planning, ordering ACE software, and ACE installation and administration. The documents also contain information on Avaya and third-
party system solution integration, Web service application programming interfaces (APIs), security, fault, and performance management, and troubleshooting.

You can also find information on core applications or APIs delivered with the base software, for example, Message Drop, and Message Blast API.

**Avaya ACE Release 6.2.1 documents**

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overview</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avaya Agile Communication Environment™ Overview and Specification</td>
<td>Provides a description of ACE including solution architecture, services, features, hardware, and software.</td>
<td>Sales engineers, Solution architects, Implementation engineers, and Support personnel</td>
</tr>
<tr>
<td>Avaya Agile Communication Environment™ Documentation Roadmap (NN10850–002)</td>
<td>Provides a list of documents in the Avaya ACE documentation suite for the release.</td>
<td>Sales engineers, Solution architects, Implementation engineers, and Support personnel</td>
</tr>
<tr>
<td><strong>Installation, upgrades, migrations, and configurations</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avaya Agile Communication Environment™ Planning and Installation (NN10850–004)</td>
<td>Describes network planning when integrating Avaya ACE with other applications. The document also contains information and procedures for installing and upgrading Avaya ACE software components.</td>
<td>Sales engineers, Solution architects, Implementation engineers, and Support personnel</td>
</tr>
<tr>
<td>Avaya Agile Communication Environment™ using VMware in the Virtualized Environment Deployment Guide (NN10850-065)</td>
<td>Describes the procedures for deploying the Avaya ACE vAppliance on VMware.</td>
<td>Sales engineers, Solution architects, Implementation engineers, Support personnel</td>
</tr>
<tr>
<td><strong>Maintenance and Troubleshooting</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avaya Agile Communication Environment™ Troubleshooting</td>
<td>Contains troubleshooting information and procedures for Avaya ACE.</td>
<td>Solution architects, Implementation engineers, Support personnel</td>
</tr>
<tr>
<td>Avaya Agile Communication Environment™ Fault and Performance Management</td>
<td>Describes how the fault and performance management system collects alarms and events generated by Avaya ACE. The document also describes how to monitor Avaya ACE.</td>
<td>Solution architects, Implementation engineers, Support personnel</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>Audience</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>Administration and system programming</td>
<td>Provides information about the initial configuration, administration, and ongoing management of Avaya ACE service providers. The Avaya ACE host supports a Web-based GUI that administrators can use to perform the tasks.</td>
<td>Implementation engineers, Support personnel</td>
</tr>
<tr>
<td>Avaya Agile Communication Environment™ Service Provider Administration</td>
<td>Provides information on how Avaya ACE uses certificates for secure communication. The document also contains procedures that describe how to manage certificates using OpenSSL, IBM certificate management tools, and Avaya Aura® System Manager.</td>
<td>Implementation engineers, Support personnel</td>
</tr>
<tr>
<td>Avaya Agile Communication Environment™ User and Security Administration</td>
<td>Provides information about user management on Avaya ACE. The Avaya ACE host supports a Web-based GUI that administrators can use to perform system administration, configuration, fault management, performance management, and user management.</td>
<td>Implementation engineers, Support personnel</td>
</tr>
<tr>
<td>Avaya Agile Communication Environment™ Message Drop and Message Blast Administration</td>
<td>Provides information about the administration of the Avaya ACE Message Drop and Message Blast service.</td>
<td>Implementation engineers, Support personnel</td>
</tr>
<tr>
<td>Administering Avaya WebLM (stand-alone)</td>
<td>Provides administration, configuration, and troubleshooting information for the Web-based license manager (WebLM).</td>
<td>Implementation engineers, Support personnel</td>
</tr>
<tr>
<td>Application developer</td>
<td>Describes the Web services supported by Avaya ACE.</td>
<td>Solution architects, Implementation engineers, Support personnel, Application developer</td>
</tr>
</tbody>
</table>
Title | Description | Audience
--- | --- | ---
Avaya Agile Communication Environment™ Foundation Toolkit Overview | Provides a general overview of Avaya ACE Foundation Toolkit. | Solution architects, Implementation engineers, Support personnel, Application developer
Avaya Agile Communication Environment™ Foundation Toolkit Developer Guide | Describes the administration and maintenance of Foundation Toolkit. | Solution architects, Implementation engineers, Support personnel, Application developer
Avaya Agile Communication Environment™ Foundation Toolkit Sample Java SE Application Guide | Describes the sample Java SE application delivered with Foundation SDK. | Solution architects, Implementation engineers, Support personnel, Application developer
Avaya Agile Communication Environment™ Foundation Toolkit Sample Web Application Guide | Describes the sample Web application delivered with Foundation SDK. | Solution architects, Implementation engineers, Support personnel, Application developer
Avaya Agile Communication Environment™ Foundation Toolkit Sample Basic Java SE Application Guide | Describes the Basic Java SE sample applications delivered with Foundation SDK. | Solution architects, Implementation engineers, Support personnel, Application developer
Avaya Agile Communication Environment™ Foundation Toolkit Sample Web Application Guide Addendum Implicit Sequencing | Describes how to run sample Web applications in an implicit sequencing scenario. | Solution architects, Implementation engineers, Support personnel, Application developer

### Training

<table>
<thead>
<tr>
<th>Course code</th>
<th>Course title</th>
<th>Activity type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10U00010E</td>
<td>Avaya Agile Communication Environment(TM) (ACE) Core Implementation Virtual Campus Offering</td>
<td>On demand</td>
</tr>
</tbody>
</table>

### Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.
Go to http://www.youtube.com/AvayaMentor and perform one of the following actions:

- Enter a key word or key words in the Search Channel to search for a specific product or topic.
- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.
Introduction
Chapter 2: Message Drop and Message Blast overview

The Avaya Agile Communication Environment™ Message Drop and Message Blast service provides orchestration of audio recording and call control web services provided by Avaya ACE™ to enable automation of voice recording and broadcasting of audio messages to specified recipients. Message Drop and Message Blast is a service residing on the Avaya ACE server that provides the high level web service-based interfaces for the various telecommunication capabilities.

In a typical deployment, the Message Drop and Message Blast service interfaces with a Customer Relationship Management (CRM) system to provide click-to-dial and automated audio recording and broadcast capabilities.

The Message Drop and Message Blast service consists of the following functional areas:

- Click-to-Dial on page 14
- Message Drop on page 14
- Message Blast on page 15
- Message Record on page 16
- Message Review on page 16
- Message Drop and Blast LDAP lookup service on page 16

The log files for the Message Drop and Message Blast service are described in Message Drop and Message Blast logs on page 18.

Prerequisites

- Avaya ACE must be installed and functional. For more information, see Avaya Agile Communication Environment™ Planning and Installation (NN10850–004).
- The Avaya Media Server (MS) must be installed and functional.
- The Avaya ACE media processing support software must be installed on the Avaya MS. For more information, see Avaya Agile Communication Environment™ Service Provider Administration (NN10850–005).
- You must be familiar with Avaya ACE service provider configuration and user management. For more information, see Avaya Agile Communication Environment™ Service Provider Administration (NN10850–005).

⚠ Important:
Click-to-Dial

Click-to-Dial functionality allows users to initiate calls to clients from directly within the CRM system, regardless of their device type; for example, soft client, desktop phone, or Turret system.

With Click-to-Dial, a user can select a party in the directory and initiate a call. The Message Drop and Message Blast service automatically connects the user device to the called party, without need for the device to ring or the user to answer it, as with other third party call control applications.

At the end of the call, the Message Drop and Message Blast service makes various call statistics available so that the call log for the selected called party can be updated. These details include the time and date of the call and its duration. The user can also modify or expand these events to include further details such as the topics discussed with the called party and any actions or next steps arising from the discussion.

Message Drop

With the Message Drop functionality, you can insert audio messages into an ongoing call. The audio message can be played directly to the called party, or inserted when the call goes to the called party’s voice mail system. Once a call has been setup, you can leave the call even while the message is playing and proceed to make other calls.

When the announcement is finished playing, the Message Drop and Message Blast service makes call statistics available so that the call log for the selected called party can be updated. These details include the time and date of the call and its duration, whether the message was played, and how much of the message was played.

Message Drop and Leave

Message Drop and Leave is similar to Message Drop; however, in Message Drop and Leave, once a call has been setup, the application automatically drops you from the call without any manual intervention from you. Using additional parameters of the Message Drop and Leave feature, you can configure Answering Machine Detection.
Message Blast

Using Message Blast you can schedule the playing of a prerecorded message to a number of participants. You do not need to manually originate a call to each participant and initiate a Message Drop.

For a Message Blast, you can select:

- Many destination parties
- The message to play to each party
- The time at which the Blast must begin

The Message Drop and Message Blast application will originate the call at the scheduled time, calling each party sequentially. When the destination party answers, the Message Drop and Message Blast service connects the party to an Avaya Media Server. The Avaya Media Server can optionally play the called party a short message indicating that this call is a Message Blast and prompt the called party to press the star key to hear the message.

Alternatively, if the called party forwards to Voice Mail then the Message Blast application will perform Answer Machine Detection and play the message when the voice mail greeting completes, leaving the scheduled message in the voice mailbox of the called party.

The Message Drop and Message Blast application usually schedules the delivery of the Message Blasts to the destination party out of hours, however, within a multinational environment scheduling a Message Blast to be originated out of one time zone to another can result in a need for Message Drop and Message Blast resources to be occupied during peak hours. Message Blast uses the same Avaya Media Server resources and licenses as the other Message Drop and Message Blast operations such as Message Drop, Message Drop and Leave, Telset Record and Telset Review so the means to manage the allocation of Message Blast resources during peak office hours is provided.

By default there is a maximum capacity for the number of concurrent Message Blast participants that can listen to a message at the same time, this is defined by the global setting ‘Max Concurrent Voice Blasts’. This parameter can be modified using the Message Drop and Blast Configuration GUI.

In addition, the system administrator can use the Blast Scheduler to increase or decrease the available number of resources allocated to the Message Blast operation at various times of day. This provides the ability to avoid potential exhaustion of the available Avaya Media Server and telephony resources during peak working hours.
Message Record

Using the Message Record functionality you can record announcements from your telephony device and store the announcements on the network for retrieval in a Message Drop or Message Blast action.

When you initiate a Message Record feature, your telephony device is automatically connected to a media server. Follow the voice prompts to record a custom message in a way similar to voice mail. This audio message is stored on the network and made available for Message Drop and Message Blast actions.

Message Review

Message Review functionality allows users to review any announcement available to them from the network message store. In this way, the user can confirm the contents of a message prior to using it in a Message Drop or Message Blast operation.

The user can consult the list of available messages and request one of them for review. On initiating the Message Review feature, the user’s device is automatically connected to a media server which will retrieve the message from the network message store and play it back to the user.

Message Drop and Blast LDAP lookup service

The Message Drop and Blast LDAP Lookup Service provides clients of the Message Drop and Blast ClickToDial API the option of retrieving calling party URIs from an external, third-party LDAP Directory. Retrieval of calling party URIs from an LDAP directory is supported for the following ClickToDial service operations — ClickToDial, RecordAnnouncement, ReviewAnnouncement. When one of these operations is invoked, the client is required to provide a callingParty element in the service request. This callingParty element may either be an Explicit Calling Party URI or a Directory Lookup URI.

Explicit calling party URI

Explicit Calling Party URIs are provided in the form:

```
<tel | sip | trid>:<calling party>
```

When an Explicit Calling Party URI is provided, the URI is used directly as the calling party for the operation. No LDAP lookup is carried out.
**Directory lookup URI**

Directory Lookup URIs are provided in the form

\[\text{<prefix>:<LDAP lookup value}>\]

Any callingParty element with a prefix other than tel, sip or trid, is considered to be a Directory Lookup URI. When a Directory Lookup URI is received as the calling party, the Message Drop and Blast will consult its Directory Lookup Service in order to resolve the Directory Lookup URI into an Explicit Calling Party URI. The Directory Lookup Service is configured via the Message Drop and Blast LDAP Provisioning Tool.

**Calling party resolution**

Starting with the Server with the lowest index, the Directory Lookup Service will iterate through each configured Server, comparing the Server Prefix against the Prefix received in the Directory Lookup URI. For each server with a matching prefix, the Directory Lookup Service will connect to the LDAP Server using the configured LDAP Endpoint, Bind Distinguished Name and Bind Password. Once connected, the Directory Lookup Service will search the LDAP Server under the configured Search Base for an entry in which the configured Filter attribute value matches the \(<\text{LDAP lookup value}>\) provided in the Directory Lookup URI.

If an entry is found, the Directory Lookup Service will iterate through each configured Rule associated with the Server, starting with the Rule with the lowest index until it is able to match and transform the configured attribute into a valid Explicit Calling Party URI. Once a valid Explicit Calling Party URI is obtained, it is then used as the calling party for the original operation.

**Caching**

If an explicit Calling Party URI is obtained via an LDAP Server lookup it is cached for a period defined by the Cache Timeout value for that server. A Cache Timeout value of zero disables caching. Future Directory Lookup Service requests for the same Directory Lookup URI will return the cached value, instead of performing an LDAP lookup, until the cached entry expires. Cached entries can be cleared using the clearDirectoryCache operation in the clickToDial WSDL. The clearDirectoryCache supports wildcards (*) to clear multiple cache entries.

<table>
<thead>
<tr>
<th>dbdir:fred</th>
<th>Clears cache entry for the Lookup URI dbdir:fred.</th>
</tr>
</thead>
<tbody>
<tr>
<td>*:fred</td>
<td>Clears all cache entries with a lookup value of fred for all servers.</td>
</tr>
<tr>
<td>dbdir:*</td>
<td>Clears all cache entries from all Servers with Prefix dbdir.</td>
</tr>
<tr>
<td><em>:</em></td>
<td>Clears all cache entries from all servers.</td>
</tr>
</tbody>
</table>

**Blacklisting**

When connecting to an LDAP server, the Directory Lookup Service will wait for a period defined by the Connection Timeout before giving up and trying the next Server with the specified Prefix. Once connected to an LDAP server, the Directory Lookup Service will wait for a period defined by the Read Timeout to actually perform the lookup before giving up and trying the next Server with the specified prefix. If an LDAP Server connection timeout or read timeout occurs, the Server will be blacklisted for a number of minutes defined by the Blacklist Timeout value for that server. Any future Directory Lookup Service requests will skip the blacklisted Server until the Blacklist Timeout expires.
Message Drop and Message Blast logs

Log files contain a historical record of system activity. Log files store information so that it can be analyzed later. Message Drop and Message Blast logs are stored on the Avaya ACE host at /var/avaya/ace/log/AppSrv01/msgdropblast. The Message Drop and Message Blast logs are:

- **MsgDropBlast.log**
  
The **MsgDropBlast.log** captures the logs for all incoming service requests.

- **blast.log**
  
The **blast.log** captures all logs for the voice blasts that have run. This includes the launch order, the number of concurrent blasts, and errors.
  
This log does not capture the scheduling, cancelling or monitoring of blasts. These events are service requests and service request logs are written to **MsgDropBlast.log**.

- **worker.log**
  
Message Drop and Message Blast uses four work managers that perform the following functions:
  
- handle incoming call notifications from Avaya ACE
- handle asynchronous calls to Avaya ACE
- handle incoming announcement notifications from the Avaya Media Server
- handle outgoing notifications

The work managers log events to **worker.log**.

- **poll.log**
  
Message Drop and Message Blast runs an audit every 3-4 seconds that checks all calls in progress. The audit identifies calls that require maintenance. Maintenance activities could include calls being torn down, cleaned up, manipulated in some way, or checked on because they have been up for a long period with no notifications received from Avaya ACE. It is also responsible for performing some maintenance tasks. The more intensive tasks are passed to a work manager.

The **poll.log** captures the work of the audit timer, including when it passes on jobs to the work managers.

- **configure_MsgDropBlast.log**
The `configure_MsgDropBlast.log` records changes made to the Message Drop and Message Blast configuration.

- `MsgDropBlastConf.log` records setAuthentication events.
Message Drop and Message Blast overview
Chapter 3: Message Drop and Message Blast service deployment

Use the Message Drop and Message Blast service to include click-to-dial, automated audio recording, and broadcast capabilities in your applications.

Message Drop and Message Blast service deployment tasks

The following diagram shows the sequence of steps to deploy the Message Drop and Message Blast service.
Navigation

• For information and procedures on adding and configuring supporting software for media processing on the Avaya Media Server, see “Installation of media processing support software on Avaya Media Server” in *Avaya Agile Communication Environment™ Administration* (NN10850–005).

• [Avaya ACE configuration](#) on page 23

• [Message Drop and Message Blast configuration](#) on page 33
Chapter 4: Avaya ACE configuration

You must configure service providers on the Avaya Agile Communication Environment™ host to support third-party call control services on the call servers in the network.

In addition, you must configure an Avaya ACE user profile for the Message Drop and Message Blast service to fire Web services for the client application.

Prerequisites

Install and commission the Avaya ACE host, as described in Avaya Agile Communication Environment™ Planning and Installation (NN10850-004).

Avaya ACE configuration procedures

The following task flow shows the sequence of procedures to configure Avaya ACE.
Avaya ACE configuration

- Adding a service provider on page 25
- Adding a media terminal on page 26
- Adding media addresses on page 27
- Configuring the route address on page 28

Navigation
Adding a service provider

Before you begin
For TR/87 providers:

- Configure a call back trunk on the PBX. A call back trunk is a SIP trunk between the PBX and Avaya ACE. Use the following guidelines while entering the parameter values for the call back trunk.

- Configure the dial patterns and routing policies on the PBX for the SIP trunk. This will enable the PBX to route a call back to Avaya ACE based on the policies configured. While adding a service provider, you must provide this information in the PBX related fields.

About this task
Avaya ACE™ provides service provider interfaces (also known as adapters) to enable communications with the network communication layer. You must add and configure a service provider on Avaya ACE to enable Message Drop and Message Blast services. For information and procedures on adding and configuring Avaya ACE service providers, see Avaya Agile Communication Environment™ Service Provider Administration (NN10850-005).

The table below lists the service providers that support Message Drop and Message Blast services.

<table>
<thead>
<tr>
<th>Capability</th>
<th>CS 1000 (TR/87 with Advanced Services)</th>
<th>CS 1000 SIP</th>
<th>Turret</th>
<th>Avaya Aura (TR/87 with Advanced Services)</th>
<th>Avaya Aura SIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click to dial</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Message Review</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Message Record</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Message Blast</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Message Drop</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Message Drop and Leave</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
Adding a media terminal

Add the Avaya Media Server (MS) to a service provider on the Avaya ACE™ for call treatment. A media server anchors call sessions and hosts media services added to a call.

After adding an MS as a media terminal, you must add the media addresses associated with the MS.

**Before you begin**

- You have added a service provider requiring a media terminal.
- The MS server is installed and configured.
- You have registered ACE as a trusted node on the MS server.
- You have the IP address of the MS server.
- You have the port number used for the SIP signaling to the MS server.
- An Avaya ACE GUI session is open.

**Procedure**

1. Make sure that the Service Providers - Terminals window is open.
2. In the **Terminal Details** dialog box, enter a name for this MS server in the **Name** field to internally identify the MS server within Avaya ACE.
3. In the **IP Address** field, enter the IP address for this MS server.
4. In the **Port** field, enter the port used for SIP signaling on this MS server.
5. Select the **Enable** check box to put the MS server in service and have the MS server support the associated services.
   You can keep the check box clear to have the MS server defined, but disabled.
6. Click **Add** to add the MS server terminal.
   The MS server is added to the Terminals dialog box.
7. If additional MS servers are needed, repeat **1** on page 26 through **6** on page 26.
8. Click **Next**.
   The ACE GUI takes you to the next task in the service provider configuration.
Adding media addresses

After you add Avaya Media Server (MS) to a service provider, you must define the services or media addresses associated with the Avaya MS.

Before you begin

Ensure that:

• You have added Avaya MS to Avaya ACE as a media terminal.
• You have a viable domain name in the Avaya MS server.
• An Avaya ACE GUI session is open.

About this task

Two pre configured services are mandatory for Avaya MS. These services are SIP addresses configured on Avaya ACE. You must add the following two services:

• ANNC to provide announcements used for ringback tone and recorded announcements
• CONF to provide the media path for all third-party call or TPCv3 and audio call scenarios

You must also add the following media addresses specific to the Message Drop and Message Blast service:

• REC to provide the endpoint used to initiate recording of announcements
• REV to provide the endpoint used to initiate a review of a recorded announcement
• DROP to provide the endpoint used to initiate a voice drop action
• DROPLEAVE to provide the endpoint used to initiate a message drop action when the calling party leaves the call
• BLAST to provide the endpoint used to initiate a message blast action

Procedure

1. Ensure that the Service Providers - Addresses window is open.
2. In the Address Details pane:
   a. In the Name field, enter ANNC.
   b. In the URI field, enter a valid SIP URI for the media address in the format sip:annc@<domain_name>.
   c. In the Terminals field, select the media terminal at which this media address is available. For more information about adding media terminals, see Adding a media terminal on page 26.
      You can select one or more media terminals from the list if you want to load-share across multiple Avaya MS nodes. To select multiple media terminals, press and hold the Shift key and highlight more than one terminal in the list.
   d. Click Add to add the media address.
The media address is added to the Addresses dialog box.

3. Repeat step 2 for the **CONF** media address, specifying SIP URI as sip:conf@<domain_name>.

4. Repeat step 2 for the RFC4240 media address, specifying SIP URI as sip:annc@<domain_name>.

5. Repeat step 2 for the following media addresses. These addresses are specific to the Message Drop and Message Blast service:
   - sip:DropBlast-Record@<domain_name>
   - sip:DropBlast-Review@<domain_name>
   - sip:DropBlast-Drop@<domain_name>
   - sip:DropBlast-DropAndLeave@<domain_name>
   - sip:DropBlast-Blast@<domain_name>

! Important:

Ensure that you edit the default route address after you add the media addresses and before you click **Next** in the Addresses window.

6. Edit the route address. Go to **Configuring the route address** on page 28.

---

**Configuring the route address**

Configure the route address to indicate from where a call is originating.

A route address represents the third party in a third party call control call. When you add a service provider that supports third party call control, the system automatically adds a default route address (sip:AppCore@Avaya.com). You can keep the default value or configure a valid SIP URI for the route address.

**Before you begin**

- You have added a service provider for this route address.
- You have the SIP URI to identify the route address.
- An Avaya ACE™ GUI session is open.

**Procedure**

1. Make sure that the Service Providers - Addresses window is open.
2. In the Addresses dialog box, select the route entry.
   - The details of the route address appear in the Address Details dialog box.
3. In the **URI** field, enter a valid URI to identify the route address.

4. Click **Modify** to configure the route address.
   The route address is updated in the Addresses dialog box.

5. Click **Next**.
   The Avaya ACE GUI takes you to the next task in the service provider configuration.

### Configuring translation rules

As part of the service provider configuration on Avaya ACE, you must add translation rules for each service provider as required.

Translation involves applying a translation rule to a URI coming in with a selected Web service request before being passed to the service provider of a network element. Translation rules manipulate the URI so that Avaya ACE can route it to the appropriate service provider.

For Click-To-Dial, Voice Drop, Message Record, and Message Review, valid and consistent number ranges are required for each provider you plan to use for Message Drop and Message Blast. Please consult provisioning and administration information of each provider type for provisioning specifics. For more information on configuring translation rules, see *Avaya Agile Communication Environment™ Service Provider Administration* (NN10850-005).

### Message Drop and Message Blast provisioning considerations

The following job aids provide examples of translation rules specific to the Message Drop and Message Blast service.

#### Translation rule example for Message Blast

A rule must be added for service providers to support Message Blast. Supported adapters require an advanced rule to transform a URI from `sip:<dn>` to `sip:<dn>@<domain>`. Given CS 1000 or an Avaya service provider domain provisioned as `SP_Domain` and two DNs of `9191`, a transformation rule similar to the example below is required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling URIs</td>
<td>sip:9191</td>
</tr>
<tr>
<td>Matching Pattern</td>
<td><code>^(?sip:)?(\d+)$</code></td>
</tr>
</tbody>
</table>
### Translation rule example for the Turret service provider

When using the Turret service provider, where called parties begin with a “+” as a dialing prefix, an additional provider rule is required to ensure that supported operations function properly. This rule needs to take the `tel:+<dial prefix><DN>` and convert it to `<prefix><DN>`, as in the example below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>URIs</td>
<td><code>tel:+445551234</code></td>
</tr>
<tr>
<td>Matching Pattern</td>
<td><code>^(?:tel:)?(\+)?(\d+)$</code></td>
</tr>
<tr>
<td>Transform URI Rule</td>
<td><code>$2</code></td>
</tr>
<tr>
<td>Transformed URI</td>
<td><code>445551234</code></td>
</tr>
</tbody>
</table>

### Configuring a user profile for Message Drop and Message Blast service

Create a user profile for the Message Drop and Message Blast service on Avaya ACE™. You must then assign the appropriate privileges to the user account to enable the Message Drop and Message Blast service to invoke Web services.

You can gain access to Avaya ACE Web services through HTTP basic authentication. All HTTP request messages from the Message Drop and Message Blast service must include a valid user name and password in the HTTP header.

**Before you begin**

You must have administrator privileges on the Avaya ACE server.

**Procedure**

1. Open a Web browser and log in to the Avaya ACE GUI as administrator.
   
   [https://<ACE_host_IP>:9449/oamp](https://<ACE_host_IP>:9449/oamp)

2. On the menu bar, choose **Security > User Management > Create User**. The Create User window appears.

3. On the User tab:
a. In the **User ID** field, enter a name for the Message Drop and Message Blast service account.
b. In the **User Password** field, enter a password for the account.
c. In the **Confirm User Password** field, enter the password again to confirm.

4. Create a new role with API Integration Suite license assigned to it. Turn **ON** the access control for **CallNotificationService**, **ThirdPartyCallService**, and **TurretService**. If such a role already exists, go to the next step.

5. Assign the user created in the previous step to this role. To assign a role, perform the following:
   - On the Role Membership tab, select a role from the Available Roles window and move it to the Member Roles window.

6. On the Role Membership tab, from the Available Roles window, select a role that has API Integration Suite license assigned to it. Ensure that the access control for **CallNotificationService**, **ThirdPartyCallService**, and **TurretService** is **turned ON**.

7. Click **Submit** to save the changes.
   - The system displays the User Creation Success window with the settings you have created for the user.
Chapter 5: Message Drop and Message Blast configuration

Message Drop and Message Blast configuration procedures
The following task flow shows you the sequence of procedures you perform to configure Message Drop and Message Blast.
Message Drop and Message Blast configuration

1. Configure MsgDropBlast Authorization
2. Configure Message Blast Settings
3. Configure Message Blast Schedule
4. Download the LDAP Provisioning Tool
5. Existing LDAP configuration file?
   - Yes: Load an LDAP configuration file
   - No: Add LDAP server entry
6. Add LDAP server entry
7. Clone LDAP server entry?
   - Yes: Clone LDAP server entry
   - No: Add LDAP server address rule
8. Add LDAP server address rule?
   - Yes: Add LDAP server address rule
   - No: Validate LDAP server configuration
9. End
Configuring Message Drop and Message Blast authorization

You must configure the user ID and password to enable the Message Drop and Message Blast service. The user ID and password values in the Message Drop and Message Blast Configuration window must be the same as the values configured for the Avaya Agile Communication Environment™ user profile for the Message Drop and Message Blast service.

⚠️ Important:

You must set the user ID and password in the Avaya ACE™ user profile before you set the values in the Message Drop and Message Blast Configuration window.

Procedure

1. Log in to the Avaya ACE™ GUI.
2. On the menu bar, click Configuration and select Services.
3. In the list of services on the left, click Message Drop and Blast.
4. In the Message Drop and Message Blast Configuration window, click the Third Party Call Authorization tab.
5. Enter the User Name and Password for the Message Drop and Message Blast service account on ACE.
6. Click Save.
7. You receive a message that the update succeeded. Click OK.

---

**Configuring the Message Drop and Message Blast service**

You can configure the Message Drop and Message Blast service in the Message Drop and Blast Configuration window.

**Before you begin**

Ensure that:

- Avaya ACE is installed and configured on the server.
- The necessary service providers are configured with the appropriate media terminal and media addresses.
- The Message Drop and Message Blast service is installed with Avaya ACE and all the configuration variables are assigned default values during Avaya ACE installation. The default values are acceptable for most deployments. If you are going to change the defaults, you must be familiar with the following variables:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya MS</td>
<td></td>
</tr>
<tr>
<td>Max Record Length</td>
<td>Maximum length in seconds of a recorded announcement. The default is 300 seconds. The valid range is 0 to 3600.</td>
</tr>
<tr>
<td>Drop-and-Leave Wait</td>
<td>The silence detection interval for message drop and leave. The default is 1. The valid range is 0 to 10.</td>
</tr>
<tr>
<td>Blast Wait</td>
<td>The silence detection interval for message blast. The default is 3. The valid range is 0 to 10.</td>
</tr>
<tr>
<td>Blast Preamble</td>
<td>Check the check box to play the preamble before the message blast. Clear the check box to turn off the preamble.</td>
</tr>
<tr>
<td><strong>makeCall Options</strong></td>
<td></td>
</tr>
<tr>
<td>Media Treatment Suffix</td>
<td>Media terminal (Avaya MS) treatment suffix for load balancing</td>
</tr>
<tr>
<td>Call Transaction Histories</td>
<td>Enabling this option will allow the transaction history event logging to be generated for each message drop operation, excluding message blast.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>The default setting is off.</td>
<td></td>
</tr>
<tr>
<td><strong>Message Blast Options</strong></td>
<td></td>
</tr>
<tr>
<td>Transaction Histories</td>
<td>Enabling this option will allow the transaction history event logging to be generated for each message blast operation. The default setting is off.</td>
</tr>
<tr>
<td>Calling Party Name</td>
<td>The name sent as the callingParticipantName for all TPC V3 requests to Avaya ACE from the Message Drop and Message Blast service.</td>
</tr>
<tr>
<td>Max Concurrent Blasts</td>
<td>Number of concurrent blasts participants. The higher the number, the faster the blast completes for all participants. The default is 20. The valid range is 10 to 180.</td>
</tr>
<tr>
<td>Scheduler Interval</td>
<td>The frequency (in milliseconds) at which the Message Drop and Message Blast service initiates message blasts if the maximum permitted number of concurrent blasts has not been reached. The default value is 10000 ms. The valid range is 1000 to 10000. The lower the number, the faster blast participants ramp and the faster the overall blast will complete.</td>
</tr>
<tr>
<td><strong>Database Audit Options</strong></td>
<td></td>
</tr>
<tr>
<td>Interval</td>
<td>The frequency in days that the database audit is run. The default is 7 days. The valid range is 1 to 14.</td>
</tr>
<tr>
<td>Retention Period</td>
<td>The number of events, measured in days, to retain in the database after archiving. The default is 3 days. The valid range is 1 to 30.</td>
</tr>
<tr>
<td>Start Hour</td>
<td>Hour of the day to run the archiver. The default is 4. The valid range is 0 to 23.</td>
</tr>
<tr>
<td>First Audit Delay</td>
<td>How long, in minutes, to wait after a restart before running an audit. The default is 10 minutes. The valid range is 1 to 10.</td>
</tr>
</tbody>
</table>
Procedure

1. Log in to the Avaya ACE GUI.
2. On the menu bar, click Configuration > Services.
3. From the list of services on the left, select Message Drop and Blast.
4. In the Message Drop and Blast Configuration window, review the current configuration settings and make the required changes.
5. Enter the password and click Save.
6. You receive a message that the update succeeded. Click OK. Changes are applied immediately to any new operations. Operations in progress continue based on the previous configuration settings.

Configuring a Message Blast schedule

You can create a Message Blast schedule that allows you to vary the number of resources allocated to the Message Blast operation.

About this task

Without entering any details into the scheduler the default number of concurrent voice blast participants is defined by the Maximum Blasts setting. To configure the number of blast participants allowed at any given time, specify a starting day, time, and amount. The setting remains in effect until a subsequent time slot is encountered.

Procedure

1. Log in to the Avaya ACE GUI.
2. Open the Message Drop and Blast configuration page. Click Configuration and select Services.
3. In the list of services on the left, click Message Drop and Blast.
4. In the Message Drop and Blast windows, click the Message Blast Preferences tab.
5. In the Blast Schedule area, select a Day of Week and Starting Time.
6. Under Maximum Blasts, select the maximum number of concurrent blasts allowed.
7. Click Add.
8. Continue to define time slots as required. New entries are listed in chronological order.
9. When you have completed the Message Blast schedule, click **Save**. When the configuration is applied, the schedule details are verified and any unnecessary entries condensed. For example, if two adjacent time slots have the save concurrent Blasts value, they are condensed into one entry. Changes are applied immediately to any new operations. Operations in progress continue based on the previous configuration settings.

---

**Downloading the LDAP Provisioning Tool**

The LDAP Provisioning Tool allows you to create a configuration file to define the LDAP server for Message Drop and Message Blast service. Use this procedure to download the LDAP Provisioning Tool from the ACE server.

**Before you begin**

You must run the LDAP Provisioning Tool on a Windows based machine.

**Procedure**

1. Log in to the Avaya ACE GUI.
2. Open the Message Drop and Message Blast configuration page. On the menu bar, navigate to **Configuration > Services**.
3. In the list of services on the left, click **Message Drop and Blast**.
4. In the Message Drop and Blast windows, click the **Message Blast Preferences** tab.
5. Click **Configure** and save the file `Avaya_ACE_MsgDB_Directory_Configurator.exe` to your local machine.
6. Navigate to the location of the configuration utility and double-click on the file `Avaya_ACE_MsgDB_Directory_Configurator.exe`.

---

**Loading an LDAP server configuration file**

If an LDAP server configuration file already exists, you can start the LDAP provisioning task by loading the existing file.
Procedure

1. In the MSGDB LDAP Provisioning Tool Window, click **Load Config**.
2. In the Load Configuration window, select one of the following options from the list:

<table>
<thead>
<tr>
<th>Load configuration option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrieve from Remote MSGDB Server</td>
<td>Load an existing LDAP server configuration file from a Message Drop and Message Blast server. In the Fetch Configuration window, you must enter the IP address and Port of the Message Drop and Message Blast server.</td>
</tr>
<tr>
<td>Load config from local machine</td>
<td>Load a existing LDAP server configuration file from your local machine. You are prompted for the location of the file.</td>
</tr>
<tr>
<td>Backup and Load from Remote Server</td>
<td>Save the current configuration information in the MSGDB LDAP Provisioning Tool to a local file and then load an LDAP server configuration file from a Message Drop and Message Blast server. You are prompted for a save location for the current configuration information. In the Fetch Configuration window, you must enter the IP address and Port of the Message Drop and Message Blast server.</td>
</tr>
<tr>
<td>Backup and Load from Local Machine</td>
<td>Save the current configuration information in the MSGDB LDAP Provisioning Tool to a local file and load an alternate LDAP server configuration file from your local machine. You are prompted for a save location for the current configuration information. Then you are prompted to specify the new file to load.</td>
</tr>
</tbody>
</table>

---

Adding a new LDAP server entry

Use this procedure to add a new LDAP server entry for the Message Drop and Message Blast service.

**Before you begin**

You must get the values for the following configuration parameters.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix</td>
<td>used as the identifier for which LDAP servers to use for the lookup of the calling party. For example, If</td>
<td></td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>a click to dial request originating in to the Message Drop and Message Blast application is prefixed with a specific identifier, in this case dbdir:&lt;unique_id&gt;, the LDAP servers with the prefix dbdir is used by the Message Drop and Message Blast application to find the calling party number.</td>
<td></td>
</tr>
<tr>
<td>Search Base</td>
<td>The search base is the distinguished name of the search base object and defines the location in the directory at which the LDAP search will be executed.</td>
<td></td>
</tr>
<tr>
<td>Server URL</td>
<td>The address of the LDAP server. LDAP Server URLs have the following syntax: ldap[s]://hostname:port.</td>
<td></td>
</tr>
<tr>
<td>bindDN</td>
<td>Required if anonymous binds are not possible on the LDAP server to obtain user and group information. Can be left blank if the LDAP server is set up to use anonymous binds. If the LDAP server is not set up to use anonymous binds then enter the bindDN. When the server details are saved, the value is encrypted.</td>
<td></td>
</tr>
<tr>
<td>bindPW</td>
<td>Required if anonymous binds are not possible on the LDAP server to obtain user and group information. Can be left blank if the LDAP server is set up to use anonymous binds. If the LDAP server is not set up to use anonymous binds then enter the bindPW. When the server details are saved, the value is encrypted.</td>
<td></td>
</tr>
<tr>
<td>Filter</td>
<td>Defines which attribute in the LDAP to search against to retrieve the LDAP entry containing the calling party. For example, if the user provided a calling party of dbdir:&lt;unique_id&gt;, the Message Drop and Message Blast service would search LDAP under the search base (ou=people,</td>
<td></td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>ou=group, dc=dbgroup, dc=com)</td>
<td>for an entry where the attribute dbdirid=&lt;unique_id&gt;.</td>
<td></td>
</tr>
<tr>
<td>Cache Entry Timeout (minutes)</td>
<td>The length of time a specific entries lookup result will remain in cache. Subsequent attempts to retrieve the same information from the LDAP server will firstly retrieve the information from the cache stores in the Message Drop and Message Blast application. Attempts after the Cache Entry Timeout has expired will perform a new lookup and store the result in cache, resetting the cache timeout for that specific lookup. Valid values are 0 (caching disabled) to 10080.</td>
<td></td>
</tr>
<tr>
<td>Read Timeout (milliseconds)</td>
<td>Applies to the LDAP response from the server after the initial connection is established with the server. Timeouts under these circumstances will result in the server being blacklisted. The Message Drop and Message Blast Directory Service will then try the next LDAP server that matches the prefix. Valid values are 1000 to 20000.</td>
<td></td>
</tr>
<tr>
<td>Connection Timeout (milliseconds)</td>
<td>The timeout associated with the original connection to the LDAP server. Failure to respond to the connection results in the LDAP server being blacklisted for subsequent lookups. The Message Drop and Message Blast Directory Service will move and try the next LDAP server that matches the prefix. Valid values are 1000 to 20000.</td>
<td></td>
</tr>
<tr>
<td>Blacklist Timeout (minutes)</td>
<td>The length of time that a specific server is blacklisted after an unsuccessful connection attempt. During the blacklist time the server will not be sent LDAP lookups. Valid values are 0 (blacklisting disabled) to 1440.</td>
<td></td>
</tr>
</tbody>
</table>
Cached Entry Allowed | When enabled, every call attempt that queries this LDAP server will first check the cache for previously obtained results. When this option is disabled every call attempt will perform an LDAP lookup to retrieve the latest results directly from the LDAP server – it will not consult the cache. Note that results received via lookups when this option is disabled may still be cached in accordance with the Cache Entry Timeout settings above.

**About this task**

The MSGDB LDAP Provisioning Tool Window consists of a list of the configured LDAP servers. The LDAP servers are listed in the order in which the servers will be consulted. When a calling party URI is received with a non-reserved prefix, a prefix other than `tel:`, `sip:` or `trid:`, the Message Drop and Message Blast service will traverse this list in order, consulting each LDAP server with a matching prefix until a valid calling party URI is returned. Servers can be added multiple times with different prefixes; also the same prefix can be used on multiple servers. However, each server/prefix combination should only appear in the list once. A maximum of 20 LDAP servers can be provisioned.

**Procedure**

1. In the MSGDB LDAP Provisioning Tool Window, click **Add New LDAP Server**.
2. In the window that opens, configure the following values.

<table>
<thead>
<tr>
<th>Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix</td>
</tr>
<tr>
<td>Search Base</td>
</tr>
<tr>
<td>Server URL</td>
</tr>
<tr>
<td>bindDN</td>
</tr>
<tr>
<td>bindPW</td>
</tr>
<tr>
<td>Filter</td>
</tr>
<tr>
<td>Cache Entry Timeout (minutes)</td>
</tr>
<tr>
<td>Read Timeout (milliseconds)</td>
</tr>
<tr>
<td>Connection Timeout (milliseconds)</td>
</tr>
<tr>
<td>Blacklist Timeout (milliseconds)</td>
</tr>
<tr>
<td>Cached Entry Allowed</td>
</tr>
</tbody>
</table>
3. Click **Save**.

---

**Cloning an LDAP server entry**

To create a new LDAP server entry, you can clone an existing entry and then modify the configuration as required.

**Procedure**

1. In the MSGDB LDAP Provisioning Tool Window, click **Edit** next to the server you want to clone.
2. Click **Clone**.
   - The new server entry is added to the list with a new **Index** number.
3. Click **Edit** to edit the new server entry.

---

**Adding an LDAP server address rule**

An address rule defines which attributes in the returned search entry contain the real calling party identity, and the matching pattern and transform required to extract the calling party identity, if it is embedded in other data in the contents of the attribute.

Use this procedure to define an address rule. You can add the following address rule types:

- Trader address
- SIP address
- Tel address

**Before you begin**

You must get the values for the configuration parameters described in the following table.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute</td>
<td>Indicates which attribute, located within the returned search entry, contains the Trader ID, or SIP/Tel address.</td>
<td></td>
</tr>
<tr>
<td>Match</td>
<td>Indicates what regular expression pattern match, the system must</td>
<td></td>
</tr>
</tbody>
</table>
### Variable Description | Value
--- | ---
apply to the Trader ID Attribute to determine whether it contains a valid Trader ID or SIP/Tel address. | **Transform**
Indicates how the system must transform the Attribute, based on the results of the pattern match above, to return the real calling party match. |  

If the returned search entry contains multiple values against the defined Attribute, the Message Drop and Message Blast service will iterate through the list and use the first attribute value that pattern matches against the Match. When the Message Drop and Message Blast service finds, matches and transforms the Trader ID or sip or tel address, the service will add the appropriate prefix (`trid:`, `sip:` or `tel:`) to the result and use it as the calling party.

For a Trader address, the Trader ID information is mandatory. The Site ID information is optional. However, you can define a Site ID Attribute for a Trader address rule, if a Site ID must be appended to make a fully qualified Trader ID.

### Variable Description | Value
--- | ---
Site ID Attribute | Indicates which attribute, located within the returned search entry, contains the Site ID. This attribute might be different or the same as the attribute provided as the Trader ID attribute. If the Site ID attribute is the same as the Trader ID attribute, and the attribute has multiple values, then Message Drop and Message Blast will use the same value to determine the Trader ID and Site ID.

Site ID Match | Indicates what regular expression pattern match must be applied to the Site ID Attribute to determine whether it contains a valid Site ID.

Site ID Transform | Indicates how the Site ID Attribute must be transformed, based on the results of the pattern match above, to return the real calling party match.

### Procedure

1. In the MSGDB LDAP Provisioning Tool Window, click **Edit** for the LDAP server where you want to add the rule.
2. Under **Transform Rules**, click **Add New Rule**.
3. In the Attribute Type window, select the type of rule to add.
4. In the Address window, enter the **Attribute**, **Match**, and **Transform** configuration parameters.
5. For a Trader address rule, enter the **Site ID** configuration parameters.
6. Click **Add**.

As each rule is added to the LDAP server, the list of configured rules on the server edit screen increases. A brief description of the rule type is shown alongside the **Index**, as well as the ability to **Edit**, **Delete** or shift the order. The order in which the rules are accessed is determined by the **Index** associated with the rule.

To view a rule without having to edit the rule, click on the index number next to the rule. The rule is displayed in the **XML view of the transform rules** box.

---

**Validating LDAP server configuration**

**About this task**

Use this procedure to perform a lookup in order to validate the configuration settings of an LDAP server.

**Procedure**

1. In the MSGDB LDAP Provisioning Tool window, click **Validate On**.
2. In the LDAP Verification Tool area at the bottom of the window, select the server from the **Select Server** list.
3. Select the prefix required for the lookup in the **Select Prefix** field.
4. Enter a unique identifier for the lookup in the **Test String** field and click **Return**.
5. Click **Validate**.

If the LDAP query is successful, then the **Test Result** field displays the return result from the LDAP server.

If the query doesn’t find a entry in the LDAP server then the **Test Result** field displays a message indicating that the lookup was unsuccessful.
Applying the LDAP server configuration file

Once you have finished defining the LDAP server in the LDAP Provisioning tool, you must apply the configuration file to the Message Drop and Message Blast server.

Procedure

1. In the MSGDB LDAP Provisioning Tool window, click **Save Config**.
2. In the Save Configuration Window, select one of the following options:

<table>
<thead>
<tr>
<th>Save Configuration Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save to Remote MSGDB Server</td>
<td>Apply the configuration file to a Message Drop and Message Blast server. You are prompted to save a local copy of the configuration file. In the Post Configuration window, you must enter the IP address and Port of the Message Drop and Message Blast server and a <strong>Username</strong> and <strong>Password</strong>.</td>
</tr>
<tr>
<td>Save to Local Machine Only</td>
<td>Select the option if you are not ready to apply the file but want to save a local copy. You are prompted for a save location for the directory.xml file.</td>
</tr>
<tr>
<td>Save to Multiple MSGDB Servers</td>
<td>Apply the configuration file to up to five Message Drop and Message Blast servers. You are prompted to save a local copy of the configuration file. In the Post Configuration window, you must enter the IP address and Port for each of the Message Drop and Message Blast servers and a <strong>Username</strong> and <strong>Password</strong>. When applying to multiple servers, if an error occurs, the provisioning is abandoned and any servers listed after the error will not have been provisioned. The success or failure states of those servers who could be contacted will be displayed in a pop up window.</td>
</tr>
</tbody>
</table>
Chapter 6: Managing the Message Drop and Message Blast ACE user password

About this task
Use this procedure to change the Message Drop and Message Blast user password.

⚠️ Important:
When changing the password for the Message Drop and Message Blast user, change the password in the Avaya ACE user profile first.

Procedure

1. Log in to the Avaya ACE GUI.
2. On the menu bar, click Configuration and select Services.
3. In the list of services on the left, select Message Drop and Blast.
4. In the Message Drop and Blast Configuration window, click the Third Party Call Authorization tab.
5. Enter a new password in the Password box.
6. Click Save.
7. You receive a message that the update succeeded. Click OK.
Managing the Message Drop and Message Blast ACE user password
Chapter 7: Troubleshooting the Avaya Media Server

Use these procedures to troubleshoot issues with the Avaya Media Server.

Navigation

- Disabling the media security policy on page 51
- Monitoring active calls on the Avaya Media Server on page 52
- Enabling debug logging on the Avaya Media Server on page 52
- Verifying the Avaya Media Server media configuration on page 53
- Logging in to the primary security server on page 54
- Adding a license key on page 54
- Adding SIP nodes and routes on page 55
- License requirements on Avaya Media Server on page 56
- Restart the Avaya ACE application on page 57

Disabling the media security policy

About this task

By default after an install of the Avaya Media Server (MS), the media security policy is set to BEST EFFORT. If announcements are not playing, disable the media security policy.

Procedure

1. Open the Element Manager in a web browser (http://<AMS_server>). The system opens the Element Manager window.
2. In the Navigation pane, click System Configuration > Media > Media Security. The system displays the Media Security window in the right pane.
4. Click Save.
Monitoring active calls on the Avaya Media Server

About this task
View the current active sessions on the Avaya Media Server (MS) to help troubleshoot issues.

Procedure

1. Open the Element Manager in a web browser (http://<AMS_server>).
   The system opens the Element Manager window.
2. In the Navigation pane, click System Status > Monitoring > Active Sessions.
   The system displays the Active Sessions window in the right pane.

Enabling debug logging on the Avaya Media Server

About this task
Enable debug logging on the Avaya Media Server (MS) to help troubleshoot issues.

Procedure

1. Open the Element Manager in a web browser (http://<AMS_server>.
2. In the Navigation pane on the left, select System Configuration > Debug tracing.
5. Click Save.
6. To view the Avaya MS logs, go to <drive_letter>:\Program Files\Avaya \Multimedia_Applications\MAS\common\log
   The logs of interest to the MsgDropBlast vxml service are vxmlidebug.txt and vxmliAppDebug.txt.
7. You can also collect all relevant logs using the Log Capture tool. In the Navigation pane on the left, select Tools > Log Capture.
Verifying the Avaya Media Server media configuration

About this task
In the event that a media issue is experienced, check the Avaya Media Server (MS) media configuration.

Procedure

1. Open the Element Manager in a web browser. The system opens the Element Manager window.
2. In the Navigation pane, click System Configuration, Media, and then Audio Codecs. The system displays the Audio Codecs window in the right pane.
3. Make sure that the following audio codecs are enabled:
   - G711-Ulaw
   - G711-Alaw
   - G729
   By default, all PTimes (10, 20, 30, and 60) are enabled.
4. In the Navigation pane, click System Configuration, Media, and then Digit Relay (DTMF). The system displays the Digit Relay (DTMF) window in the right pane.
5. Make sure that RFC2833 and INFO Digits are enabled on the Avaya MS to allow DTMF key presses to be detected during Message Record, Message Review, and Message Blast operations.

⚠️ Note:
If In-band DTMF is required then you must ensure that the RCS2833 and INFO digits are not enabled in the Digit Relay (DTMF) setting.
Logging in to the primary security server

About this task
Log in to the primary security server.

Procedure

1. Open Internet Explorer with the Element Manager (EM) link (http://localhost:8080/em or https://<server_name>:8443) and go to the login page.
2. On the primary security server login page, log in with the User ID admin and the password you selected during the configuration of the primary security server. Click Log In to log directly into the Element Manager.

The Element Manager interface appears.

Adding a license key

Add a license key to enable the Avaya Media Server (MS) to create active sessions of software applications using a floating license server.

Floating licensing enables the Avaya MS system to share licenses across all Avaya MS nodes in the same cluster. In this configuration, the Avaya MS system installs the license key on the primary server.

Before you begin

- You have a license key.
- You are logged into the primary security server

Procedure

1. In the Navigation pane on the left, click Licensing > Licensing Configuration.
2. On the Licensing page, click General Settings.
3. Click Use License Server.
4. In the Add License Keys box, copy and paste the content of the license file.
5. Click Validate.
Important:
If the keys are not valid, an error message appears. If the keys are valid, details appear in the License Details area.

6. Click **Save**.
7. On the **General Settings Confirmation** page, read the warning and click **Confirm**.
8. Restart the system to implement your changes.
9. In the Navigation pane on the left, click **Licensing**.
10. On the Licensing page, click **Server Status**.
11. The server must be in the started state. If the server is started, the **Start** button is greyed out.

---

### Adding SIP nodes and routes

Configure trusted nodes for each proxy server. The Avaya MS only processes SIP traffic from trusted nodes, for example, proxies and gateways. Requests from nodes that are not trusted are rejected. Trusted nodes are required for all proxy servers that interact with the Avaya MS.

Configure SIP routes for all proxy servers. SIP routes define all proxy servers that communicate with this Avaya MS node. You can configure up to 32 routes for each domain. Routes are selected based on matching domain. If no domain is configured, the wildcard domain, represented by an asterisk (*), is used.

Include the following trusted nodes in the SIP nodes and routes:

- Avaya ACE™ host IP address
- Message Drop and Message Blast IP addresses if hosted off of a separate Web server to the ACE
- Avaya MS IP address

**Before you begin**

You have the IP addresses for the trusted nodes.

**Procedure**

1. Log on to Element Manager for the primary server.
2. In the navigation pane on the left, click **System Configuration**.
4. On the Signaling Protocols page, click SIP.
5. On the SIP page, click Nodes and Routes.
6. On the SIP Nodes and Routes page, in the Trusted Nodes section, click Add.
7. On the Add SIP Trusted Node page, enter the host name or server IP address and click Save.
8. Repeat step 7 for each proxy server.
9. In the bread crumb trail at the top of the page, click Nodes and Routes.
10. In the Routes section, click Add.
11. On the Add SIP Route page, select the Enabled check box to enable the route.
12. From the Trusted Node list, select the trusted node to associate with the route.
13. From the Transport list, select the transport protocol that the route uses.

⚠️ Important:
If you select a transport type of TLS, ensure that a certificate is configured for the SIP TLS service profile.

14. In the Remote Port field, enter the port number of the remote port.
15. In the Priority field, set the priority of the route by entering a value.
16. In the Weight field, set the weight of the route by entering a value.
17. Under Roles, the Proxy check box is checked and the Registrar check box is cleared.
18. Click Save.
19. If you do not want to restrict traffic to trusted nodes, in the navigation pane on the left, click System Configuration.
20. Select Signaling Protocols, then SIP, and then General Settings.
22. Restart the server for the SIP route additions to take effect.

---

License requirements on Avaya Media Server

MSGDB license requirements on the Avaya Media Server (MS).

The following are the licenses required on the Avaya MS:
### License

<table>
<thead>
<tr>
<th>License</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>interp:sess</td>
<td>Individual session licenses. The number is based on customer requirements.</td>
</tr>
<tr>
<td>inst:auth</td>
<td>1 per server.</td>
</tr>
<tr>
<td>cpd::auth</td>
<td>1 per server (To enable answering machine detection).</td>
</tr>
<tr>
<td>plicd</td>
<td>1 per server.</td>
</tr>
</tbody>
</table>

---

## Restart the Avaya ACE application

This section contains procedures for restarting the Avaya Agile Communication Environment™ (ACE) application.

- [Restarting the Avaya ACE application](#) on page 57
- [Restarting the application (HA)](#) on page 58

**Related topics:**
- [Restarting the Avaya ACE application](#) on page 57
- [Restarting the Avaya ACE application (HA)](#) on page 58

### Restarting the Avaya ACE application

Use this procedure to restart a standalone deployment of the Avaya ACE™ application.

**Important:**
This procedure is for standalone deployments only.

To restart Avaya ACE in a HA deployment, see [Restarting the application (HA)](#) on page 58.

**Before you begin**
You must be able to log in as the root user ID.

**Important:**
If direct root login has been disabled, you must log in and change to the root user ID.

When changing to the root user ID, always use the command syntax `su - root`. Using a dash ensures that you have the correct environment when entering commands as the root user.
About this task

Restart the Avaya ACE application by rebooting the Avaya ACE machine from the command prompt.

⚠️ Important:

After you restart the application server, you must open a new browser session to view the Avaya ACE GUI. This ensures that the data displayed on the GUI is refreshed and up-to-date.

It is important to note that session information is not maintained through an application restart. As a result, the following behavior can be expected:

- Any calls set up using the ThirdPartyCall v3 web service are terminated at the next long call audit. The long call audit can be disabled on the Avaya Media Server or the audit period may be customized up to a maximum of one hour. For more information, see the section "Configuring SIP general server settings" in *Avaya Media Application Server and Interactive Communications Portal Commissioning* (NN44471-301). Any changes to settings must be done on all Avaya Media Servers used by the system.
- Calls set up using a SIP service provider remain active until the next long call audit, if the SIP service provider implements long call auditing.
- Calls set up using a non-SIP service provider before restart remain active.
- If the SIP terminal sends a re-INVITE, the call is terminated.
- Calls in the process of being setup during the restart do not complete successfully.
- Call events such as notifications and status messages related to calls setup prior to the restart, are not successful.
- Presence notification and status must be re-subscribed.
- Calls initiated during the restart are not successful.

Procedure

1. Log in to the Avaya ACE host as the *root* user ID.
2. At the prompt, enter `reboot`.

---

Restarting the Avaya ACE application (HA)

Before you begin

- Perform this procedure on either the active or idle server.
Important:
If direct root login has been disabled, you must log in and change to the root user ID.

When changing to the root user ID, always use the command syntax `su - root`. Using a dash ensures that you have the correct environment when entering commands as the root user.

About this task
For ACE servers deployed in high availability (HA) configuration, perform administrative tasks using the `aceadmin.sh` tool.

Important:
After you restart the application server, ensure that you close all existing browser sessions. You must open a new browser session to view the Avaya ACE GUI. This ensures that the data displayed on the GUI is refreshed and up-to-date.

Procedure

1. Log in to one of the Avaya ACE hosts as the root user.
2. Change directories. Enter
   ```
   cd /opt/avaya/ace/bin
   ```
3. Disable the cluster service and stop the application server. Enter
   ```
   ./aceadmin.sh disable
   ```
4. Verify that the cluster service is disabled. Enter
   ```
   crm status
   ```
5. Enable the cluster service and start the application server. Enter
   ```
   ./aceadmin.sh enable
   ```
6. Verify that the cluster suite is enabled. Enter
   ```
   crm status
   ```