Dialogic® IMG 1010/1004 Integrated Media Gateways

Radius
Release 10.3.x / 10.5.x

September 2008
www.dialogic.com

Copyright and Legal Notice

All contents of this document are furnished for informational use only and are subject to change without notice and do not represent a commitment on the part of Dialogic Corporation or its subsidiaries ("Dialogic"). Reasonable effort is made to ensure the accuracy of the information contained in the document. However, Dialogic does not warrant the accuracy of this information and cannot accept responsibility for errors, inaccuracies or omissions that may be contained in this document.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH DIALOGIC® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications.

Due to differing national regulations and approval requirements, certain Dialogic products may be suitable for use only in specific countries, and thus may not function properly in other countries. You are responsible for ensuring that your use of such products occurs only in the countries where such use is suitable. For information on specific products, contact Dialogic Corporation at the address indicated below or on the web at http://www.dialogic.com/.

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic does not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic and no such licenses are provided except pursuant to a signed agreement with Dialogic. More detailed information about such intellectual property is available from Dialogic's legal department at 9800 Cavendish Blvd., 5th Floor, Montreal, Quebec, Canada H4M 2V9.

Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements.

Any use case(s) shown and/or described herein represent one or more examples of the various ways, scenarios or environments in which Dialogic® products can be used. Such use case(s) are non-limiting and do not represent recommendations of Dialogic as to whether or how to use Dialogic products.

Dialogic, Dialogic Pro, Brooktrout, Cantata, SnowShore, Eicon, Eicon Networks, Eiconcard, Diva, SIPcontrol, Diva ISDN, TruFax, Realblocs, Realcomm 100, NetAccess, Instant ISDN, TRXStream, Exnet, Exnet Connect, EXS, ExchangePlus VSE, Switchkit, N20, Powering The Service-Ready Network, Vantage, Making Innovation Thrive, Connecting People to Information, Connecting to Growth and Shiva, among others as well as related logos, are either registered trademarks or trademarks of Dialogic. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at 9800 Cavendish Blvd., 5th Floor, Montreal, Quebec, Canada H4M 2V9. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic's trademarks requires proper acknowledgement.

Windows is a registered trademark of Microsoft Corporation in the United States and/or other countries. Other names of actual companies and products mentioned herein are the trademarks of their respective owners.

This document discusses one or more open source products, systems and/or releases. Dialogic is not responsible for your decision to use open source in connection with Dialogic products (including without limitation those referred to herein), nor is Dialogic responsible for any present or future effects such usage might have, including without limitation effects on your products, your business, or your intellectual property rights.

Hardware Limited Warranty

Warranty for Hardware Products: Dialogic Corporation or its subsidiary that originally sold the hardware product ("Dialogic") warrants to the original purchaser of this hardware product, that at the time of delivery the hardware product supplied hereunder will be free from defects in material and workmanship. This warranty is for the standard period set out on Dialogic's website at http://www.dialogic.com/warranties and is subject to all of the terms and limitations set out on the Dialogic website at http://www.dialogic.com/warranties.

Additional Exclusions: Dialogic will have no obligation to make repairs or replacements necessitated by your fault or negligence, improper or unauthorized use of the product, repairs or modifications made without Dialogic's prior written approval or by causes beyond the control of Dialogic, including, but not limited to, power or air conditioning failure, acts of God, improper interface with other units, or malfunction of any equipment or software used with the Dialogic product(s). If Dialogic is requested and agrees to make repairs or replacements necessitated by any such causes, you will pay for such service or replacement at Dialogic's then prevailing rates.

No Other Warranties: DIALOGIC DISCLAIMS AND YOU WAIVE ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY AGAINST LATENT DEFECTS, WITH RESPECT TO ANY DIALOGIC PRODUCT.

No Liability for Damages: IN NO EVENT SHALL DIALOGIC OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, INTERRUPTION OF ACTIVITIES, LOSS OF INFORMATION OR OTHER PECUNIARY LOSS AND DIRECT OR INDIRECT, CONSEQUENTIAL, INCIDENTAL, ECONOMIC OR PUNITIVE DAMAGES) ARISING OUT OF THE USE OF OR INABILITY TO USE ANY DIALOGIC PRODUCT.

Limitation of Liability: DIALOGIC'S MAXIMUM CUMULATIVE LIABILITY SHALL BE LIMITED TO THE AMOUNTS ACTUALLY PAID BY YOU TO DIALOGIC FOR THE SPECIFIC PRODUCT BEING THE OBJECT OF THE CLAIM. YOU RELEASE DIALOGIC FROM ALL AMOUNTS IN EXCESS OF THE LIMITATION. YOU ACKNOWLEDGE THAT THIS CONDITION IS ESSENTIAL AND THAT DIALOGIC WOULD NOT SUPPLY TO YOU IF IT WERE NOT INCLUDED.

IMPORTANT NOTE:

Please be aware that the following terminology and abbreviations are used throughout this document. Please also be sure to consult the legal notice for other important details.

When used herein, the term "IMG 1010" refers to the "Dialogic® IMG 1010 Integrated Media Gateway" product.

When used herein, the term "IMG 1004" refers to the "Dialogic® IMG 1004 Integrated Media Gateway" product.

When used herein, the general term "IMG" refers collectively or alternatively to the Dialogic® IMG 1010 and the Dialogic® IMG 1004 Integrated Media Gateway products

When used herein, the term "GCEMS" refers to the "Dialogic® Gate Control Element Management System"

Technical Support

Technical Support Number: 781-433-9600
Technical Support Fax: 781-449-9520
http://www.dialogic.com/

Table Of Contents

An Overview of RADIUS on the IMG

Topic Location: *Product Description > RADIUS*

Overview
The IMG uses Remote Authentication Dial In User Service (RADIUS) for streaming the Call Detail Records (CDR). The implementation is compliant with RFC 2865 and RFC 2866. The RADIUS messages are sent to external RADIUS servers. The IMG RADIUS interface generates an ACCESS, a START & a STOP Request for the inbound leg and a START & STOP Request for the outbound leg of the call, as well as data associated with the INVITE, the 200 OK, the BYE and the CANCEL methods for those legs utilizing a SIP protocol.

Specifications
The IMG implementation of RADIUS is based on the following RADIUS RFCs:
RFC 2865 - Remote Authentication Dial-In User Service (RADIUS)
RFC 2866 - RADIUS Accounting

Formats
The IMG supports the Dialogic RADIUS formats, which Includes some attributes defined by RFC 2865 and RFC 2866, as well as Dialogic Vendor Specific Attributes (VSA).

Scenarios
The IMG supports RADIUS Authentication and Accounting. Users have the option of using one of the following scenarios:

Authentication and Accounting
In this case an Authentication Server and an Accounting Server are both assigned to the RADIUS client on the IMG.
Accounting only
In this case only an Accounting Server is assigned to the RADIUS client on the IMG.
Authentication only
In this case only an Authentication Server is assigned to the RADIUS client on the IMG.

See RADIUS Scenarios for more details.

As per RFC 2865 and RFC 2866, the IMG by default uses port 1812 for Authentication and port 1813 for Accounting. However, these ports are also configurable through the ClientView GUI. When implementing Authentication and Accounting, both processes can be either on the same or separate servers.

The RADIUS attributes and VSA's included in the messages will vary based on the following:

- Protocol Used
- What leg of the call the protocol is used
- Whether it is a TDM protocol (SS7 or ISDN) or IP protocol (SIP or H.323).

The User name and Password values configured for the Authentication Server used will be included in the user name and password attributes in the Access Request message sent from the IMG.

RADIUS Server Redundancy

The IMG supports an Active/Standby redundancy scheme. Redundancy logic is independent for Authentication and Accounting Servers. When configuring RADIUS servers they may get created with an initial priority preference. The IMG will begin using the Active Server(s) and switchover to a Standby server after detecting a communication failure to the currently Active server. Once the switchover occurs all future Radius messages will flow to the new Active server until a failure occurs on this server. If an error is detected in trying to send a Radius message to this new Active server, the IMG will attempt to switch back to the initial Active server. This behaviour is repeated, until a working server is detected. If the IMG fails to connect to a RADIUS Server an alarm will be sent. You can monitor alarms using EventView.

Typically when a RADIUS message needs to be sent to a server it is assembled and passed to the OS for transport to the active server. These servers are configured to send the message wait 2 seconds and then retry sending the message an additional 3 times. Therefor a RADIUS message will be sent a total of 4 times at 2 second intervals. Once the message has been sent 4 times with no success a switchover to the next server will occur. The switchover behaviour is coupled to the message type. Therefore an Accounting Server switchover is independent of an Authentication Server switchover.

Under typical call load it will take a while for the switchover to complete since the IMG may have many RADIUS messages queued up to the failed server. Each of these messages must fail and be retried on the newly active server following notification of the send failure.

NOTE: A negative response does not constitute a server failure.

Supported Packet Types

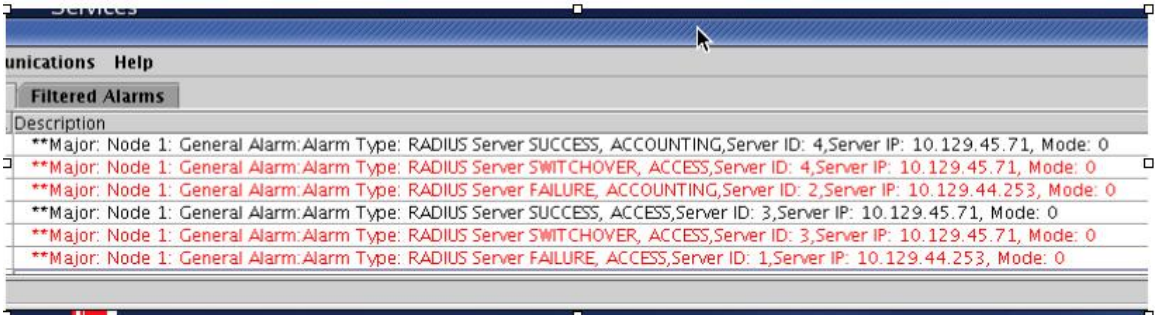
Access-Request
Sent to a RADIUS server - conveys information used to determine whether a user is allowed access to a specific NAS, and any special services requested for that user.
Access-Accept
Sent by the RADIUS server - provides specific configuration information necessary to begin delivery of service to the user.
Access-Reject
Sent by the RADIUS Server if any value of the received Attributes is not acceptable
Accounting-start
Describes the type of service being delivered and the user to whom it is being delivered at the start of service delivery
Accounting-stop
Describes the type of service that was delivered and some optional statistics, such as elapsed time, input and output octets, and input and output packets.

RADIUS Server Debug Mode

You can configure your RADIUS Client in Debug Mode so that calls will be completed whether the RADIUS server is active or not. The IMG will not require authentication for the RADIUS server to complete a call and no billing information will be logged. You enable RADIUS Debug Mode using the RADIUS Client screen.

RADIUS Server Failure Alarm

The IMG provides automatic alarming notification to IMG users when a Radius Server has changed states and can no longer be accessed. The alarm, reported in EventView, will include the RADIUS Server Type (Access, Accounting), the Server ID, the mode of the Radius Server (normal, debug), the state of the Radius Server and the IP address.



Related Topics
Basic RADIUS Call Flow
Generic RADIUS Attributes
Cantata RADIUS VSAs
RADIUS Call Flow: SS7 to H.323
RADIUS CDR Example: SIP-to-ISDN
Configuring Billing and Authentication

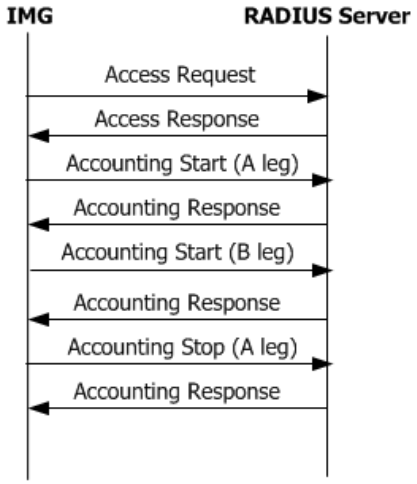
RADIUS Scenarios

Topic Location: *Product Description > RADIUS*

The IMG supports RADIUS Authentication and Accounting. IMG customer has the option of using one of the following scenarios:

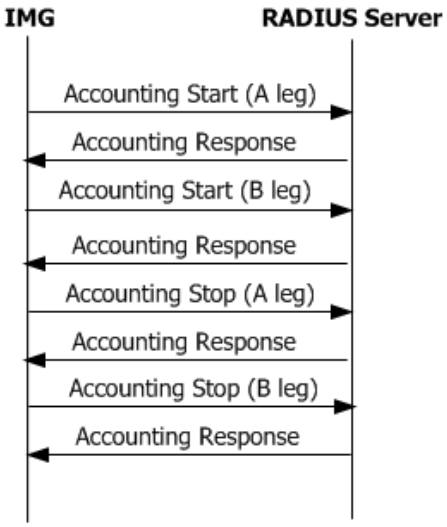
Authentication and Accounting

In this case an Authentication Server and an Accounting Server are both assigned to the RADIUS client on the IMG.



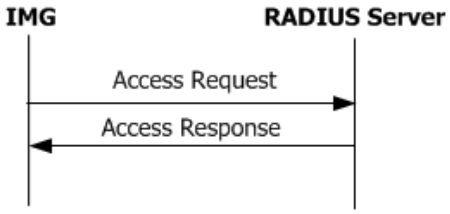
Accounting only

In this case only an Accounting Server is assigned to the RADIUS client on the IMG.



Authentication only

In this case only an Authentication Server is assigned to the RADIUS client on the IMG.



Generic RADIUS Attributes

Topic Location: *Product Description > RADIUS*

RADIUS Attributes carry the specific authentication, authorization, information and configuration details for the request and reply. Some Attributes may be included more than once.

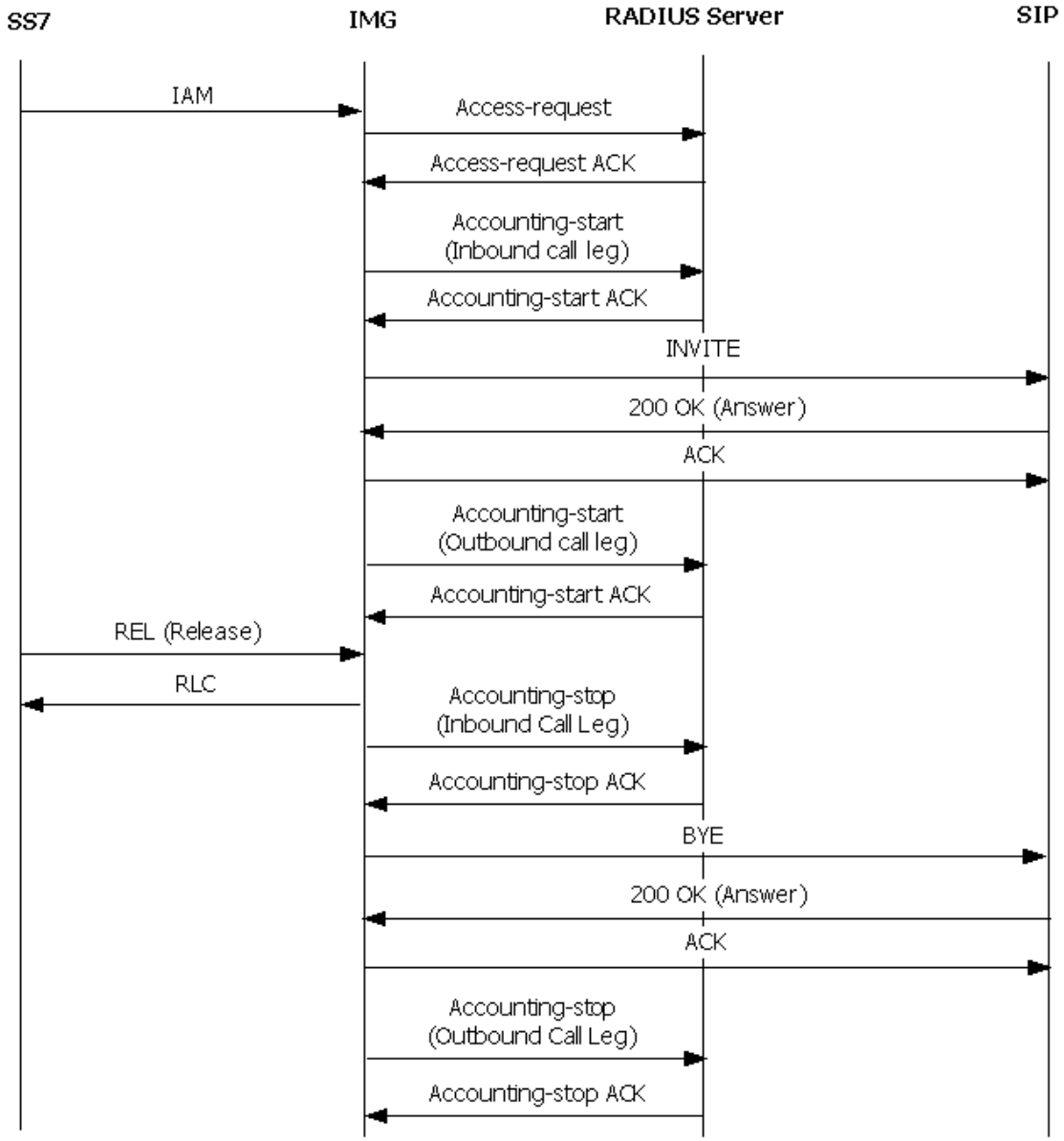
IETF Attribute #	Attribute Name	Values	Example	Description
1	User-Name	String	50886230002	Account number or calling party number
2	User-Password	String	dialogic	16 octets user password
4	NAS-IP-Address	String	192.168.0.100	IP Address of the requesting IMG
5	NAS-Port	Numeric (4 octets)	1812	The Physical Port Number of the NAS (Network Access Server) that is authenticating the user.
6	Service-Type	Numeric (4 octets)	Login-User	The Type of Service the user has requested, or the type of service to be provided
14	Login-IP-Host	Numeric Values	192.168.0.100	
29	Termination-Action	Numeric (4 octets Values	RADIUS-Request	0 Default 1 RADIUS-Request
30	Called-Station-Id	String The String field is one or more octets, containing the phone number that the user's call came in on.	50886230002	This Attribute allows the NAS to send in the Access-Request packet the phone number that the user called, using Dialed Number Identification (DNIS) or similar technology. Note that this may be different from the phone number the call comes in on. It is only used in Access-Request packets.
31	Calling-Station-Id	String The String field is one or more octets, containing the phone number that the user placed the call from.	50886230002	This Attribute allows the NAS to send in the Access-Request packet the phone number that the call came from, using Automatic Number Identification (ANI) or similar technology. It is only used in Access-Request packets.
32	NAS-Identifier	String The String field is one or more octets, and should be unique to the NAS within the scope of the		This Attribute contains a string identifying the NAS originating the Access-Request. It is only used in Access-Request packets.

		RADIUS server. For example, a fully qualified domain name would be suitable as a NAS-Identifier.		
40	Acct-Status-Type	Numeric (4 octets) Values	Start	Indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop).
41	Acct-Delay-Time	Numeric (4 octets)	0	This attribute indicates how many seconds the client has been trying to send this record for, and can be subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request. (Network transit time is ignored.)
42	Acct-Input-Octets	Numeric (4 octets)	1	Indicates how many octets have been received from the port over the course of this service being provided, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
43	Acct-Output-Octets	Numeric (4 octets)	1	indicates how many octets have been sent to the port in the course of delivering this service, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
44	Acct-Session-ID	String The String field SHOULD be a string of UTF-8 encoded 10646 [7] characters.	00201c0405b9009000 3500001000129e48b99e	This attribute is a unique Accounting ID to make it easy to match start and stop records in a log file.
46	Acct-Output-Octets	Numeric (4 octets)	10	This attribute indicates how many seconds the user has received service for, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
47	Acct-Input-Packets	Numeric (4 octets)	1	This attribute indicates how many packets have been received from the port over the course of this service being provided to a Framed User, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.

48	Acct-Output-Packets	Numeric (4 octets)	0	This attribute indicates how many packets have been sent to the port in the course of delivering this service to a Framed User, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
49	Acct-Terminate-Cause	Values	NAS-Request	This attribute indicates how the session was terminated, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
60	Chap-Challenge	String The String field contains the CHAP Challenge.		This Attribute contains the CHAP Challenge sent by the NAS to a PPP Challenge-Handshake Authentication Protocol (CHAP) user. It is only used in Access-Request packets.
61	NAS-Port-Type	Values	Ethernet	This Attribute indicates the type of the physical port of the NAS which is authenticating the user.

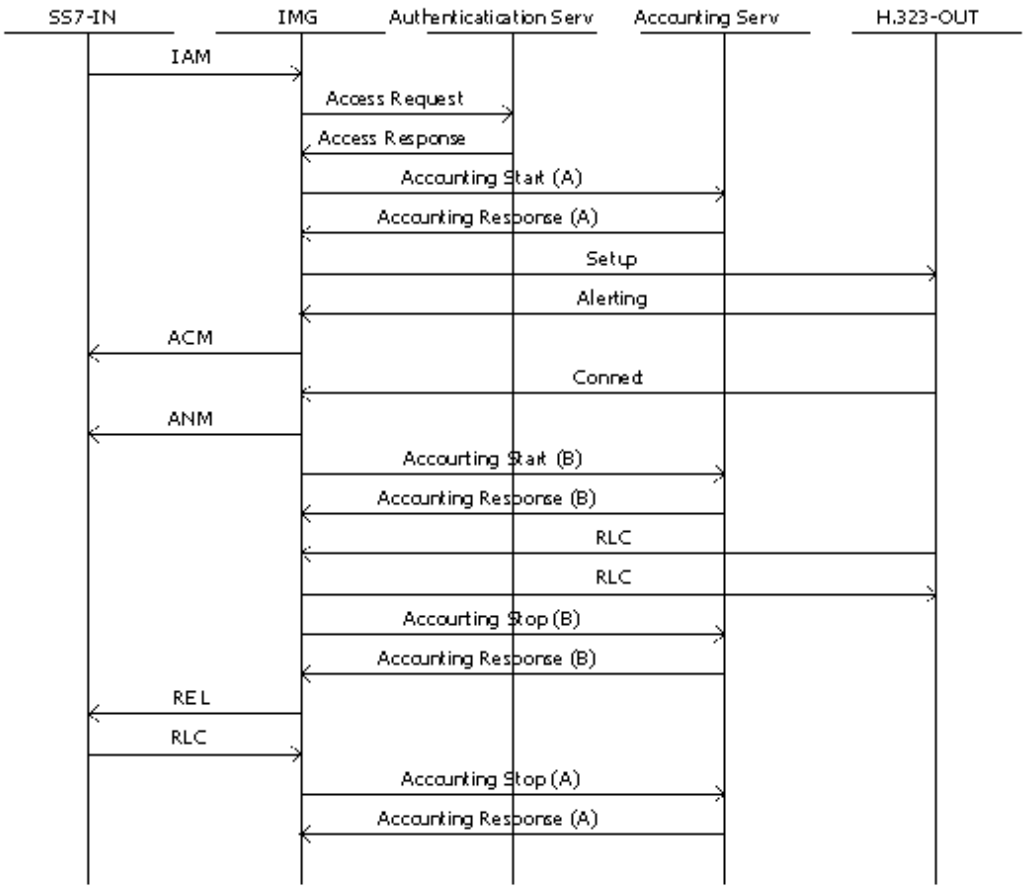
RADIUS Call Flow: SS7 to SIP

Topic Location: *Product Description > RADIUS*



RADIUS Call Flow: SS7 to H.323 - Release from SS7

Topic Location: *Product Description > RADIUS*



Incomplete Call Behavior

Topic Location: *Product Description > RADIUS*

This section outlines the behavior of the IMG gateway in case of the most common incomplete calls.

- User Busy
- No Answer from User
- No Circuit/Channel Available
- Unallocated Number
- H.323 Release Reason
- H.323 non-Fast-Start

Configuring RADIUS

Topic Location: *Configuration > RADIUS*

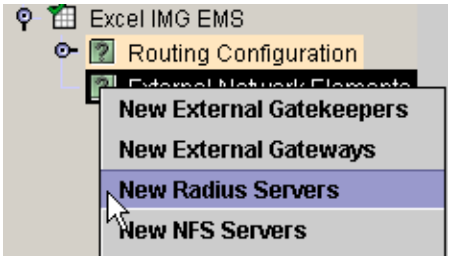
You can configure a total of 256 RADIUS servers.
Before You Begin
Make sure you have moved the RADIUS dictionary files (*dictionary* and *dictionary.cantata)* to your RADIUS installation folder. The files are located in the following directory: /opt/cantata (dialogic)/common/Radius

Task Summary

1. Configuring a RADIUS Authentication Server
2. Configuring a RADIUS Accounting Server
3. Configuring a RADIUS Client

Configuring a RADIUS Authentication Server (Optional)
The IMG only verifies if authentication is accepted or rejected by the RADIUS Server; it does not act on any other information returned by the server.

1. Right-click **External Network Elements** and select **New Radius Servers**.



2. Right-click **Radius Servers** and select **New Radius Server**.

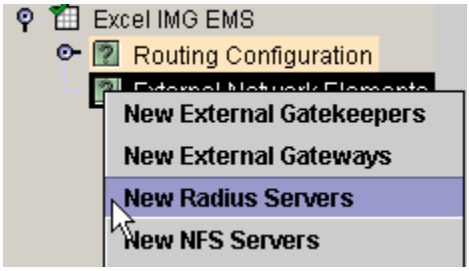
   The Radius Server pane appears.

3. The following fields are automatically populated:
   Radius ID - the next number in sequence
   Radius Server Type - Authentication
   Radius Server Port - field is automatically populated with 1812.
4. Enter the IP address of the Radius Server in the **Radius Server IP Address** field.
5. Enter the User Name and Password as configured on the Radius Server in the **Radius Server UserName** and **Radius Server Password** fields.
6. Select the desired Authentication Type in the **Radius Server Authentication Type** field.
7. Enter the Radius Server Secret configured on the Radius Server in the **Radius Server Server Secret** field.

   See the Radius Server pane reference for field details.

Configuring a RADIUS Accounting Server

1. Right-click **External Network Elements** and select **New Radius Servers**.



2. Right-click **Radius Servers** and select **New Radius Server**.

   The Radius Server pane appears.

The following fields are automatically populated:

Radius Server ID - the next number in sequence

3. Select *Accounting* in the **Radius Server Type** field.
4. In the **Radius Server IP Address** field, enter the IP address of the Radius Server.

The **Radius Server Port** field is automatically populated with 1813.

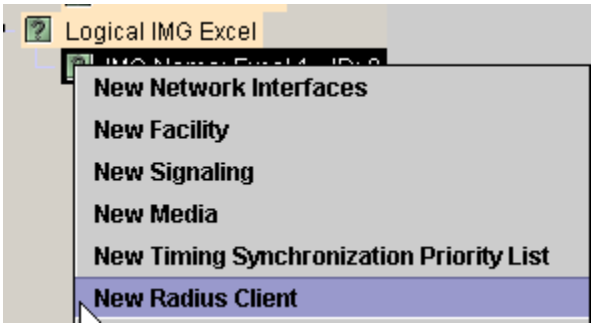
The following fields do not apply for an Accounting Server:

Radius Server UserName
Radius Server Password
Radius Server Authentication Type
Radius Server Server Secret

See the Radius Server pane reference for field details.

Configuring a RADIUS Client

1. Right-click the desired Physical IMG and select **New Radius Client**.



   The Radius Client pane appears.

2. The following fields are automatically populated. Change any default values, if required.
   Radius Client Network Interface - IP Address of the Physical IMG.
   Authentication Port - 1812
   Accounting Port - 1813
   Primary Authentication Server - First Authentication Server Configured
   Primary Accounting Server - First Accounting Server Configured

3. Select a Secondary Authentication Server from the **Secondary Authentication Server** field, if required.
4. Select a Secondary Accounting Server from the **Secondary Accounting Server** field, if required.
5. To enable RADIUS Client Debug Mode, select On in the RADIUS Client Debug Mode field. When Debug Mode is On, calls will be completed whether the RADIUS server is active or not. The IMG will not require authentication from the RADIUS server to complete a call and no billing information will be logged.

See the Radius Client pane reference for field details.

Configuring Free RADIUS using GCEMS as a RADIUS Server

Topic Location: *Configuration > RADIUS*

The IMG runs a RADIUS client that is configured to send CDR start & stop events to the RADIUS server, which can be the GCEMS Linux server or another RADIUS server.

Requirements

- GCEMS server running Linux Redhat ES 3.0, 4.0 or 5.0 with freeradius installed, or another server running Radius.
- For RADIUS authentication, the username and password specified in ClientView for the Radius server authentication either needs to be in the /etc/raddb/users configuration or if using the Linux server for authentication should be added as a Linux user.

Steps

- To add a RADIUS user using the users file start with step 1.
- If using a Linux username for authentication skip to step 2.
- If not using RADIUS authentication (accounting only) skip to step 3.

1. In the freeRADIUS users file (/etc/raddb/users), replace <your_username> and <your_password> with the RADIUS username and password.

   <your_username> Auth-Type:=Local, User-Password==<"your_password">
   Fall-Through = No

2. Verify the DEFAULT Authorization Type is REJECT. Edit the freeRadius users file (/etc/raddb/users)

   Add the following line at the end of the file, if missing

   ```
   # IF NOTHING ELSE MATCHES, REJECT USER DEFAULT Auth-Type:=
   Reject
   ```

3. Modify the Detail File Rollover Interval (/etc/raddb/radiusd.conf). This is required for users doing load testing with high call rates. The detail files will could reach the max file size in less than 24 hours depending on the call rate and then calls will stop being processed.

   a. Look for the following line around line 1030:

   ```
   # Write a detailed log of all accounting records received
   ```

   b. Look for the following line around line 1056:

   ```
   detailfile =",
   ```

   c. at the end of this line add the %H to have the log files roll over every hour.

4. Add access for each IMG
   Edit the freeRadius clients.conf file (/etc/raddb/clients.conf)
   If you have multiple IMG's, the Username should be different for each IMG.
   Shortname = Your username configured in the RADIUS users file and ClientView A unique username is recommended for each IMG.username
   Secret = a password that you choose for each IMG that is used in the ClientView RadiusServer Authentication & Accounting configuration.Key used to encrypt sensitive account information transmitted between the IMG and the RADIUS server.
   Password = Your RADIUS password configured in the RADIUS users file and ClientView

```
client 10.129.44.240 { # IMG IP
    secret = server_secret
 shortname   = your_username
password = your_password
    }
```

5. Copy the Cantata VSA Dictionary file.
.a. Copy the dictionary.cantata file from /opt/cantata/common/radius to /usr/share/freeradius.
a.b. In the /usr/share/freeradius/ folder, edit the dictionary file and add the following include line.
$INCLUDE dictionary.cantata

6. Start the Radius service:
service radiusd restart

7. Set the Radius service to restart when the system restarts:
chkconfig radiusd on

8. In ClientView, Configure a Radius Client and Servers on the IMG.
See Configuring Billing and Authentication.

9. Verify CDR's are being generated
By default the files will roll over once a day. Follow the instructions in step 3 to roll the log files over once an hour.
CDR's stored at: /var/log/radius/radacct/<IMG_IP>/
file names are: detail-YYYYMMDDHH
detail-2005081801

10. Archive & delete CDR detail files.
A copy of the following files can be found at /opt/cantata/IMG/radius .
a. In the /var/log/radius/radacct folder create a script to archive files. Name the file "CDR"

```
#!/bin/sh
#  CDR
#       Sample script to archive CDR's.
#       Files are archived if more than 1 days old
#       Files are deleted if more than 31 days old
find /var/log/radius/radacct/*/detail* -mtime +1 -exec gzip {} \;
find /var/log/radius/radacct/*/detail* -mtime +31 -exec rm -f {} \;
```

b. Create a cron task to run this script. This cron task can be run hourly or daily. The example below will run it hourly. After creating this script restart the cron service or restart the server.
In the /etc/cron.hourly folder create a file to run the script created in the previous step.

```
#!/bin/bash
  crontab<<EOF
# cron.dat-cdr - cron file for CDR's
#
# This script restarts the CDR log files each hour.
0 * * * * /var/log/radius/radacct/CDR
#
EOF
```

To e-mail this topic, click here

Radius Client

Topic Location: *ClientView Pane Reference*

Overview

Description

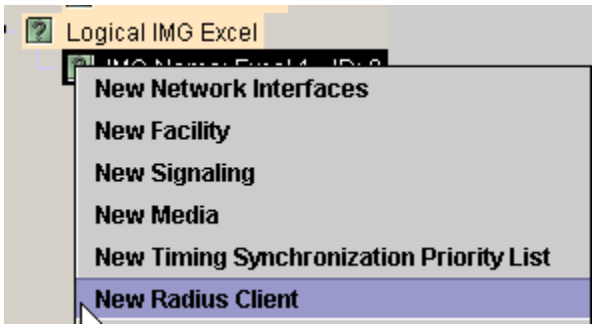
This pane configures a Radius Client for a single Physical IMG. Before configuring a client, at least one Radius Server must be configured.

Related Topics

An Overview of RADIUS
Configuring a RADIUS Client

Accessing this Pane

IMG EMS-> Logical IMG-> Physical IMG-> Radius Client



Maximum Objects: 1 per Physical IMG

Technical Notes

Pane

Radius Client 0d:10.129.38.221

Property	As-Configured	User-Specified
Radius Client Network Interface		0d:10.129.38.221
Authentication Port		1812
Accounting Port		1813
Radius Server Debug Mode		Off
Pre-Paid Support		Disabled
Radius Time Format		Legacy Format
Primary Authentication Server		Primary Server Not Used
Secondary Authentication Server		Secondary Server Not Used
Primary Accounting Server		Primary Server Not Used
Secondary Accounting Server		Secondary Server Not Used

Field Descriptions

Radius Client Network Interface

This drop-down list is populated with all of the Network Interfaces configured on this particular IMG. It is the responsibility of the user to make sure the interface may reach the particular server. If you are

Authentication Port

The port on the physical IMG that will be used to talk to the Authentication server.

Accounting Port

The port on the physical IMG that will be used to talk to the Accounting server.

RADIUS Server Debug Mode

- Off (Default)
  If Radius is configured and the RADIUS server becomes unavailable, the IMG will not process incoming calls. This is most typically found when the IMG is used to create CDRs. Since the absence of a RADIUS server results in un-billable calls, the IMG has been designed to not process calls when RADIUS is enabled. If this occurs the IMG will reject calls to the network with the following cause values:
  ISDN - Cause 41 - Temporary failure
  SS7 - Cause 41 - Temporary failure
  H.323 - Cause 41 - Temporary failure
  SIP - 503 - Service Unavailable
- On
  When Debug Mode is On, calls will be completed whether the RADIUS server is active or not. The IMG will not require authentication from the RADIUS server to complete a call and no billing information will be logged.
  This is most typically used when using RADIUS for debugging purposes (tracking call failures, cause codes, etc). You can also choose this mode if you wish the IMG to continue to process calls in an un-billed fashion if you prefer to provide free service rather than no service.

Prepaid Support

- Enable
  The IMG will act on data received in RADIUS Authentication Response messages that the Radius Server may send pertaining to prepaid application. This will allow the IMG1010 to be used in a prepaid application environment.
- Disable (default)

NOTE: Radius Prepaid Support Mode will be disabled if Radius Debug Mode is enabled. The two modes cannot be enabled at the same time.

RADIUS Time Format

This setting determines the format that will be used in CDR in attributes that include time.

- Legacy Format
  This is the format used before the availability of the Time Zone feature (10.3.2 ER6). Use this for backward compatibility if you are not using local time.
  Example: `Cantata-setup-time = "TUE FEB 20 22:24:45:270 2007"`

- Legacy Format with timezone
  Use this format to represent local time in CDRs.
  Example: `Cantata-setup-time = "WED FEB 14 12:05:54:740 2007 -0500"`

- RFC-2822 with optional day of week
  Use this format to represent local time with optional day of week in CDRs.
  Example: `Cantata-setup-time = "Tue, 20 Feb 2007 23:31:36.553 +0000"`

Primary Authentication Radius Server

The Server ID that is used as the primary Authentication Server. Drop-down list populated with all Radius Authentication Servers that have been configured. Automatically populated with the first Authentication Server configured.

Secondary Authentication Radius Server

The Server ID that is used as the secondary Authentication Server. Drop-down list populated with all Radius Authentication Servers that have been configured.

Primary Accounting Radius Server

The Server ID that is used as the primary Accounting Server. Drop-down list populated with all Radius Accounting Servers that have been configured. Automatically populated with the first Accounting Server configured.

Secondary Accounting Radius Server

The Server ID that is used as the secondary Authentication Server. Drop-down list populated with all Radius Accounting Servers that have been configured.

Radius Server

Topic Location: *ClientView Pane Reference*

Overview

Description

Use this pane to configure information about the Radius Servers that are in the network. There are two types of Radius Servers, accounting and authorization; each type may have a primary and secondary server. The same server may also do both accounting and authorization. The Servers are configured at the network level. Radius Client must be configured for every Physical IMG.

Related Topics

An Overview of RADIUS
Configuring a RADIUS Accounting Server
Configuring a RADIUS Authentication Server
RADIUS Client

Accessing this Pane

IMG EMS->External Network Elements->Radius Servers->Radius Server

Maximum Objects: 256 per EMS

Technical Notes

Pane

Authentication - ID: 1

Property	As-Configured	User-Specified
Radius Server Id	1	1
Radius Server Type	Authentication	Authentication
Radius Server Data Format	Cantata	Cantata
Radius Server IP Address	0d:5.5.5.5	0d:5.5.5.5
Radius Server Port	1812	1812
Radius Server UserName	a	a
Radius Server Password	a	a
Radius Server Authentication Type	PAP	PAP
Radius Server Secret	a	a

Field Descriptions

Radius Server Id

Allows a unique reference to address this particular server.

- 1-255

Radius Server Type

This describes the type of server, whether it is used for authentication or for accounting.

- Authentication
  This server is used to give permission for the call to continue.
- Accounting
  This server is used for tracking billing information for the call.

Radius Server Data Format
- Cantata Format

Radius Server IP Address
The IP Address of the Radius Server.

Radius Server Port
The port on the server which will accept the Radius connection.

Radius Server UserName
A Username to access this server.

Radius Server Password
The password to access this server.

Radius Server Authentication Type
This is the type of authentication the client server will use.
- PAP: Password Authentication Protocol
- CHAP: Challenge Handshake Authentication Protocol

Radius Server Secret
This must match the shared secret configured on the RADIUS server, otherwise authentication will fail.

Display Table

The table will show all the Radius Clients that have been configured.

Radius Servers

Topic Location: *ClientView Pane Reference*

Overview

Description

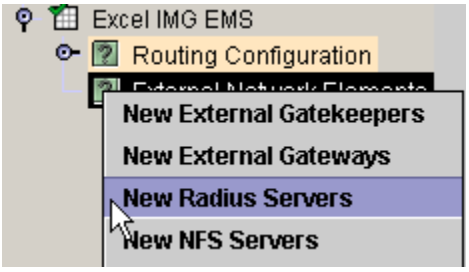
To create a Radius Server, right-click Radius Server and select New Radius Servers.

Related Topics

An Overview of RADIUS
Configuring a RADIUS Accounting Server
Configuring a RADIUS Authentication Server

Accessing this Pane

IMG EMS -> New External Network Elements -> New Radius Servers



Maximum Objects: 1

Pane

This pane shows the number of each type of Radius Server that have been configured.

Radius Servers

Property	As-Configured	User-Specified
Authentication Servers Configured	1	
Accounting Servers Configured	0	