Dialogic

Making Innovation Thrive™

Dialogic® PowerMedia™IP Media Server

Release 3.0.0

Installation and Operations Guide

March 2010 64-0530-01

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 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, Diva, Diva ISDN, Making Innovation Thrive, Video is the New Voice, Diastar, Cantata, TruFax, SwitchKit, SnowShore, Eicon, Eicon Networks, NMS Communications, NMS (stylized), Eiconcard, SIPcontrol, TrustedVideo, Exnet, EXS, Connecting to Growth, Fusion, Vision, PacketMedia, NaturalAccess, NaturalCallControl, NaturalConference, NaturalFax and Shiva, among others as well as related logos, are either registered trademarks or trademarks of Dialogic Corporation or its subsidiaries. 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.

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

Please refer to the following Dialogic web site for information on hardware warranty information, which applies unless different terms have been agreed to in a signed agreement between yourself and Dialogic Corporation or its subsidiaries. The listed hardware warranty periods and terms are subject to change without notice. For purchases not made directly from Dialogic please contact your direct vendor in connection with the warranty period and terms that they offer.

http://www.dialogic.com/warranties

Contents

List of Figures

List of Tables

About this Publication

The Dialogic® PowerMedia™ IP Media Server (which is also referred to herein as "IP Media Server", "IPMS", or "Media Server") is a standards-based SIP, VoiceXML, and MSCML server that performs a wide variety of media processing functions.

The IP Media Server is also an economical and scalable IP media option, as it can power a broad range of voice and video services for next generation wireline, wireless, and broadband services.

This section covers the following topics:

- Using this Publication
- Documentation Set
- Contacting Dialogic Technical Services and Support

Using this Publication

Audience and Purpose

This manual is for network or system administrators responsible for installing and configuring the Dialogic® IP Media Server.

Organization and Content

Chapter 1, “Introduction”, provides an overview of the structure and operation of the Dialogic® IP Media Server.

Chapter 2, “Installing the Dialogic® IP Media Server”, explains how to install and configure the IP Media Server.

Chapter 3, “Using the Web User Interface (Web UI)”, explains how to use the Web User Interface.

Chapter 4, “Configuring the Dialogic® IP Media Server”, describes procedures for configuring the IP Media Server for operation.

Chapter 5, “Operations, Administration, and Maintenance”, describes procedures for operating, administering, and maintaining the IP Media Server.

Appendix A, “Compliance and Standards Information”, describes the IP Media Server’s compliance with standards.

Appendix B, “Troubleshooting”, provides troubleshooting procedures for the IP Media Server.

Appendix C, “Required Red Hat Enterprise Linux Packages” lists the software packages that are required for the IP Media Server.

Documentation Set

Dialogic provides the following publications for the Dialogic® IP Media Server:

- The *Software Quick Start Guide* describes how to install and configure Red Hat Enterprise Linux and IP Media Server software, configure a softphone, and run a demo.
- The *Installation and Operations Guide* provides instructions for configuring, administering, and maintaining the IP Media Server.
- The *Application Developer's Guide* provides information for application developers who choose to use the IP Media Server to deploy network announcements, conferences, and Interactive Voice Response (IVR) in a voice over IP (VoIP) environment.
- The *Command Line Interface Reference Guide* describes the CLI utility which can be used to configure and troubleshoot the IP Media Server.
- *Installing Red Hat Enterprise Linux 5.0 for the IP Media Server* describes how to install and configure Red Hat Enterprise Linux 5 if you are installing the licensed software version of the IP Media Server.
- The *License Activation Guide* describes how to activate the license for your IP Media Server.
- *Upgrading from Release 2.6.0 to 3.0.0 on Red Hat Enterprise Linux Platform* provides information and instructions for upgrading from IP Media Server Release 2.6.0 to IP Media Server Release 3.0.0 on platforms running Red Hat Enterprise Linux Platform. It also includes instructions for downgrading in the event that you need to restore your previous configuration.

These publications, as well as Release Notes, are available in PDF format at http://www.dialogic.com/manuals.

Document Conventions

Conventions used in this document are described here.

Notes, Cautions, and Warnings

Notes contain information of general interest.

Cautions and warnings appear when appropriate throughout the manual.

Cautions alert you to situations that can make system administration less effective or compromise system performance or security. For example:

⚠ **Before changing the configuration of a running system, always back up the current configuration using the System→Config command.**

Warnings alert you to situations that could cause physical harm to an operator or damage to the IP Media Server. For example:

If an interface is deactivated, all traffic on that interface will be dropped.

Links in PDF

Hypertext links in the PDF version of this manual are in blue. You can click on a cross-reference link to move to the information it references.

Index entries and Table of Contents listings are also clickable links in the PDF format. After you jump to a link, use the Back button on the Acrobat Reader toolbar to return to your prior location.

Contacting Dialogic Technical Services and Support

For more information, refer to the Dialogic Technical Services and Support site:

http://www.dialogic.com/support/

When reporting an issue to Technical Services and Support, be prepared to provide the following information:

- Full description of the issue.
- Version of the IP Media Server software you are using.
- IP Media Server log files.
- Whether the issue is reproducible; the steps that you took.

Please note that the latest software update and release notes are available from the Dialogic support page.

Ordering Licenses

You must have a software license to use the Dialogic® IP Media Server. For directions on how to acquire licenses, see the Dialogic® IP Media Server *License Activation Guide.*

1 - Introduction

This chapter provides an overview of the Dialogic® PowerMedia™ IP Media Server (which is referred to in this document as the “IP Media Server” or “Media Server” or IPMS” or “MS”).

This chapter includes the following sections:

- Overview of the IP Media Server
- IP Media Server Components
- Supported Applications

Overview of the IP Media Server

The Dialogic® IP Media Server is capable of handling processing tasks associated with next generation voice, video, and data applications. The IP Media Server processes, manages, and delivers media resources for IP-based services when one or more third-party application servers, softswitches, or telephony applications provide direction to do so.

The IP Media Server is capable of handling media in various forms. Streaming media, such as real-time voice, most often takes the form of Real Time Protocol (RTP) streams encapsulated in UDP/IP packets. Other media, such as recorded announcement files, are stored locally or on remote servers and retrieved using the HTTP, NFS, or RTSP protocol.

Figure 1 illustrates the role of the Dialogic® IP Media Server in a network and how it communicates with other network resources and devices.

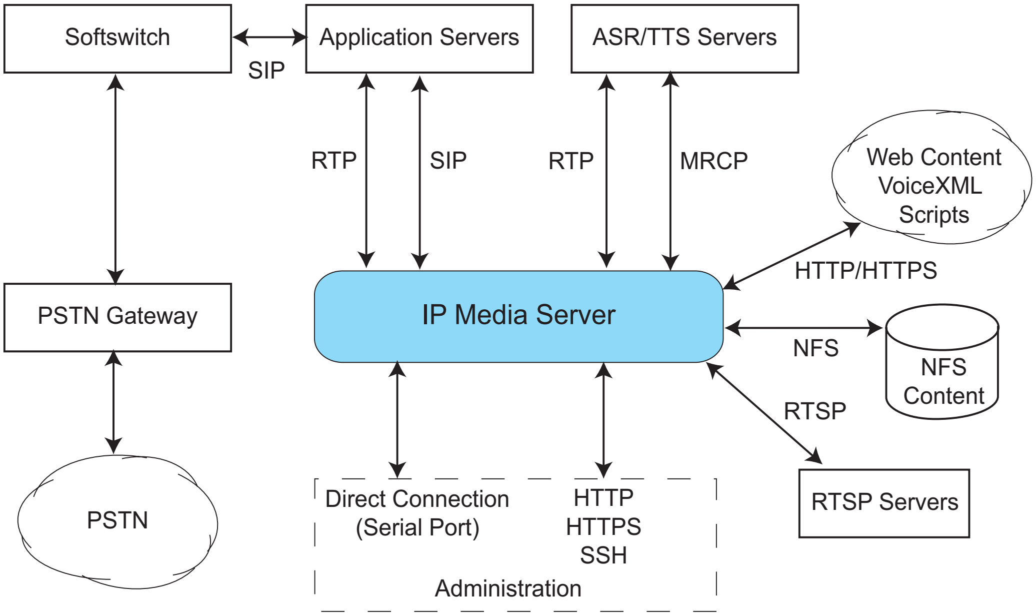


Figure 1. The IP Media Server in a Network

IP Media Server Components

The IP Media Server consists of several stand-alone processes and integrations with standard Linux applications such as Apache. Figure 2 illustrates these major components.

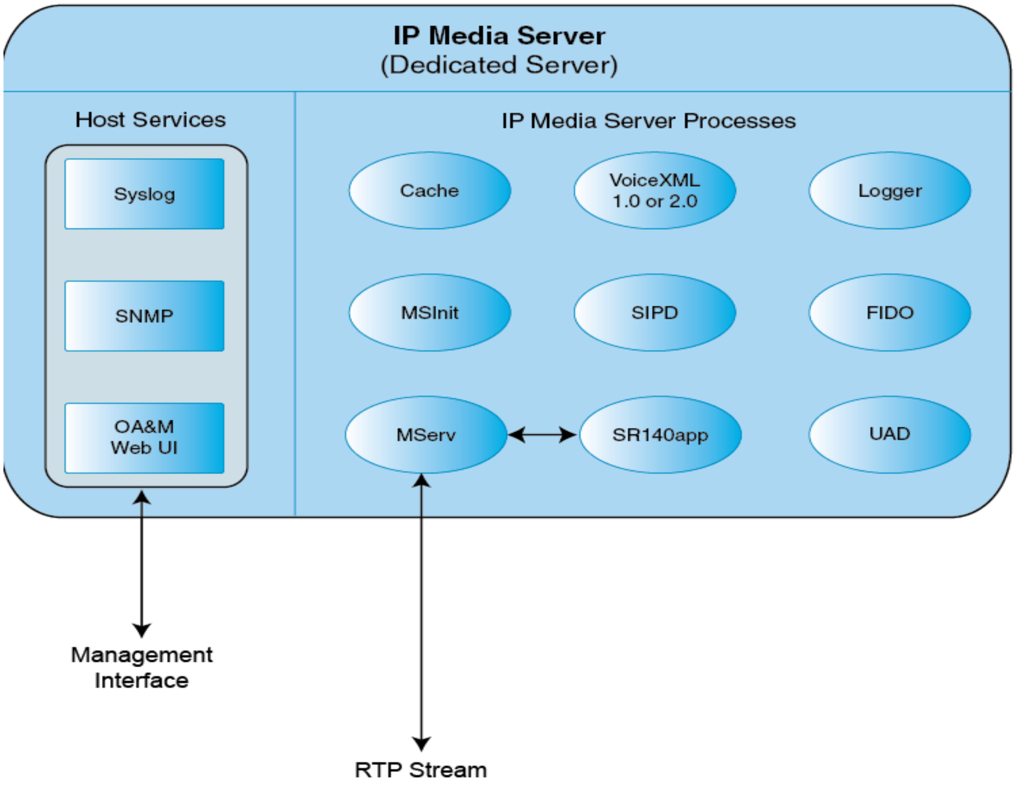


Figure 2. IP Media Server Components

The IP Media Server components are described in the following sections. Components have associated log files which may be useful in troubleshooting. For more information, see “Checking Log Files” (page 138).

FIDO

FIDO (Fetcher of Internet Domain Objects) is an HTTP/HTTPS client used to retrieve prompts and VoiceXML scripts and to post recordings and VoiceXML results.

Cache

The cache component is an HTTP caching proxy server used by other processes that retrieve content using the HTTP and HTTPS protocols.

MRCP

MRCP is the component responsible for ASR and TTS communication with a MRCP server. MRCP is responsible for managing MRCP IP Media Server licenses. The IP Media Server supports MRCPv1 and MRCPv2.

MServ

The MServ process is responsible for all RTP processing and the handling of audio and video media (e.g., conference mixing, playing prompts, etc.).

MSInit

This component tracks and logs initialization of other IP Media Server components.

MSProvider

This process handles licensing services on the IP Media Server.

RTSPC

The RTSPC (Real Time Streaming Protocol Client) component handles RTSP client functions on the IP Media Server.

SIPD

SIPD processes SIP requests received by the IP Media Server.

SNMPDaemon

The SNMPDaemon process handles SNMP traps and activities on the IP Media Server.

SR140app

The SR140app process handles fax communication.

UAD

The User Agent Daemon (UAD) generates outbound SIP requests and is used in conjunction with the VoiceXML <transfer> tag.

VoiceXML 1.0 and VoiceXML 2.0

The IP Media Server provides VoiceXML 1.0- and VoiceXML 2.0-compliant browsers. VoiceXML browsers interpret and execute VoiceXML scripts generated by applications.

When VXML 1.0 is enabled on the IP Media Server, the VXMLD process runs. When VXML 2.0 is enabled on the IP Media Server, multiple processes are invoked.

Supported Applications

The Dialogic® IP Media Server supports various application services including the following:

- Network Announcements
- Conferencing
- IVR
- VoiceXML

All application services are implemented through the Session Initiation Protocol (SIP) protocol and optional XML-based directives. The SIP Request-URI indicates the service to receive a request. See the *Application Developer's Guide* for more information about application services and functionality supported by the IP Media Server.

2 - Installing the Dialogic® IP Media Server

The Dialogic® IP Media Server is distributed in two forms:

- An integrated server, including a hardware platform and pre-installed IP Media Server software.
- A software-only release for installation on an existing hardware platform.

This chapter covers the following topics:

- Installing the Integrated IP Media Server
- Installing the IP Media Server Software
- Configuring a Management Interface
- License Activation

Note: The Dialogic® IP Media Server is suitable for use as a dedicated telephony media server. Other software applications installed on the IP Media Server may adversely affect its performance.

Installing the Integrated IP Media Server

The integrated IP Media Server is delivered as a 1U system either based on the Kontron TIGW1U chassis or the Dell PowerEdge R410 chassis with the IP Media Server software already installed. The operating system supported is Red Hat Enterprise Linux 5.2 Server.

For more information about installing the product, including requirements and specifications, see the *Quick Install Guide* that came with your IP Media Server.

The IP Media Server Release Notes list other supported hardware platforms.

Warning: Although your IP Media Server may have open disk drive bays, these must not be upgraded with field-installed drives.

Installing the IP Media Server Software

This section provides instructions for installing the IP Media Server software on a server that will act as a dedicated IP Media Server platform. The server hardware must meet the minimum system requirements defined below.

Operating System Requirements

IP Media Server software can be installed on systems running Red Hat Enterprise Linux 5.2 Server.

Server Hardware Requirements

The server on which you install the IP Media Server software must meet the minimum requirements listed in Table 1.

Table 1. Minimum Server Hardware Requirements

Item	Requirement
Processor	Two 64-bit Intel Xeon Processors running at no less than 2.8 GHz, 800 MHz front side bus, 2 MB L2 cache
Memory	2 GB ECC DDR-2 SDRAM
Ethernet	Dual 1000baseT Gigabit Ethernet
Disk	At least 30 GB Ultra320 SCSI 10000 RPM hard drive

Note: The Dialogic® IP Media Server is suitable for use as a dedicated telephony media server. Other software applications installed on the same physical device that is configured as the IP Media Server may adversely affect the performance of the IP Media Server.

Installing the IP Media Server 3.0.0 Software

This section provides instructions for installing the IP Media Server 3.0.0 software on a system that has Red Hat Enterprise Linux installed.

Note: For information on installing and configuring Red Hat, see *Installing Red Hat Enterprise Linux 5.0 for the Dialogic® IP Media Server* and the Red Hat documentation.

Before installing the IP Media Server software on the Red Hat operating system, you must disable SELinux. This is done automatically by the kickstart script described in *Installing Red Hat Enterprise Linux 5.0 for the Dialogic® IP Media Server*. You can also disable SELinux by editing the file `/etc/sysconfig/selinux`**, changing the selinux line to** `SELINUX=disabled` **and rebooting the system.**

After installing Red Hat Enterprise Linux on your system, insert the IP Media Server CD-ROM (IP Media Server software only for Red Hat Server 5.0 CD) into the drive.

1 Mount the CD-ROM on your system:

```
mount  /dev/hda  /media/cdrom
```

Note: This command may vary depending on the device names in your system.

2 Make a temporary installation directory on your system:

```
mkdir /tmp/install_1
```

3 Copy the contents of the CD-ROM to your temporary installation directory:

```
cp /media/cdrom/* /tmp/install_1
```

4 Change directory to install_1:

```
cd /tmp/install_1
```

5 Unzip the tar.gz file:

```
gunzip -d SNOW*.gz
```

6 Untar the compressed tar file:

```
tar -xvf SNOW*.tar
```

7 Install the Snowshore RPMs:

```
rpm -ivh SNOW*.rpm
```

8 When the installation script ends, unmount the CD drive:

```
unmount /media/cdrom
```

9 Remove the temporary installation directory:

```
cd /tmp
rm -rf /tmp/install_1
```

10 Reboot the system (this should take approximately 5 minutes):

```
reboot
```

Refer to “Configuring a Management Interface” (page 28) for information about configuring a management interface on the IP Media Server. You use the management interface to configure and administer the system.

Running the G2Check Utility to Check the Installation

The IP Media Server CD-ROM contains the G2Check utility that you can run to ensure that the Media Server Installation was successful.

1 Copy the G2Check utility to the install_1 directory.

2 Run the G2Check utility:

```
root@snow-sip snowshore]# perl G2Check
```

3 Respond to the prompts.

4 When the utility is done, it prints the results to STDOUT and the details to G2Install.log.

Configuring a Management Interface

The system is configured by default to run DHCP on the Ethernet interfaces (eth0, eth1, and optional eth2). If you use DHCP to set the IP address of an interface and you know the IP address, then you can use the Web User Interface (Web UI) immediately.

If you do not know the IP address configured on the system, or to set an IP address for the first time, access the system with a monitor and keyboard or over the serial port. Connect to the serial port using any standard terminal interface.

The serial port on the IP Media Server is configured as:

- Rate: autosense 9600 baud (press enter several times to autosense)
- Bits: 8
- Parity: None
- Stop Bits: 1
- Flow Control: None

Logging In

When a connection to the IP Media Server is established, the login prompt appears. The IP Media Server is delivered with a single Administrator access level user defined in the system. The login prompt appears as follows:

```
{hostname} login:
```

Use “admin” as the user name to log in through the serial port or through the console.

For more information, see Chapter 3, “Using the Web User Interface (Web UI)”.

Changing the Interface Configuration

To view the interface configuration, select the Network Interface Configuration command.

To change the IP address of an interface:

1. Select the interface to be configured.
2. Tab or mouse over to the IP address field.
3. Enter an IP address.
4. Enter network mask.
5. Note the IP address and apply the change.

Note: Specify an IP address for each interface.

The next page displayed is the original page you saw when you logged in.

Tab to the **REBOOT** option and press **ENTER**. The host reboots and the interface comes up with the specified address.

All further configuration is done through the Web User Interface.

The Web User Interface arrives configured to use HTTP. If HTTPS is preferred, you can install a security certificate and key on the system using the Web User Interface. You can also install a certificate and key using the command options provided over the serial port or monitor/keyboard.

The Web User Interface can create a self-signed certificate. You are prompted to create one if you have not done so yet.

Refer to “Managing Certificates” (page 120) for information on how to install a certificate.

License Activation

The IP Media Server has limited functionality unless you activate licenses. The primary method of activation is interactive through use of the Web. To activate your license, you must have the following:

- Access to the license key from the License Certificate or via an email from Dialogic.
- Access to the IP Media Server Web User Interface to obtain your Node ID.
- Access to the Dialogic Web site from a system with a Web browser and Internet access.
- Secure access over HTTPS or HTTP.
- External WWW access.

For detailed information and instructions on activating the license, refer to the *License Activation Guide*.

3 - Using the Web User Interface (Web UI)

This chapter explains how to use the Web User Interface (Web UI). It includes the following sections:

Overview

The Dialogic® IP Media Server is configured using a standard Web browser. Internet Explorer 7.0 or Netscape 7 or higher is recommended.

Web UI Access Levels

The IP Media Server supports two access levels:

- Administrator—Can change the configuration of the system and execute administrative tasks.
- Operator—Can monitor the system, but cannot change configurations or execute administrative tasks.

Commands that are only available to Administrators are noted as such. All other commands are usable by both operators and administrators.

Note: You must be an Administrator to configure the system.

These two levels and the privileges associated with each are described in detail in Chapter 5, “Operations, Administration, and Maintenance”. The IP Media Server comes with a default Administrator user account. The user name and password of this account are:

User Name: admin

Password: <blank>

User names and passwords are case sensitive.

Note: You should immediately change your password after initial login; see “Changing Administrator Password” (page 115).

Logging In

To open the Web User Interface (Web UI):

1 Start your Web browser.

2 Enter the fully qualified domain name or IP address (for either eth0 or eth1) of the system in the address field of your browser; for example:

```
https://<your IP address>
```

A message related to the website’s security certificate is displayed. Click Continue or Proceed Anyway to continue to the Login page.

3 The Login page is displayed.

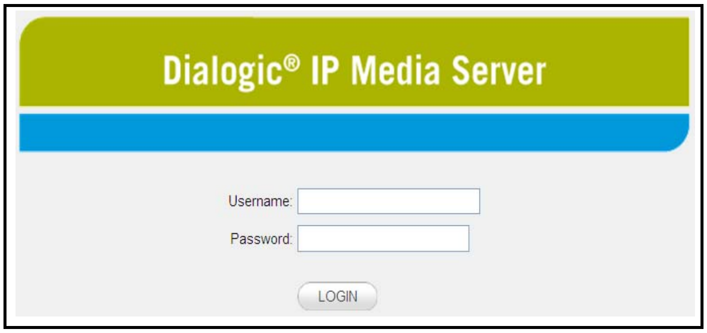
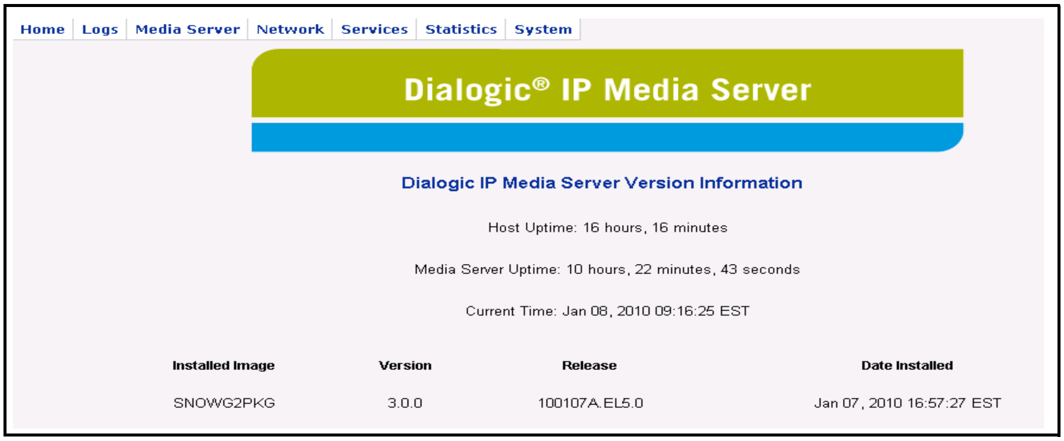


Figure 3. Login page

4 To log in, enter your user name and password, then click LOGIN. The Web UI home page is displayed.

Web User Interface Home Page

A sample Web User Interface (Web UI) home page is shown below.



Dialogic IP Media Server Version Information

Host Uptime: 16 hours, 16 minutes

Media Server Uptime: 10 hours, 22 minutes, 43 seconds

Current Time: Jan 08, 2010 09:16:25 EST

Installed Image	Version	Release	Date Installed
SNOWG2PKG	3.0.0	100107A.EL5.0	Jan 07, 2010 16:57:27 EST

Figure 4. Web User Interface Home Page

The Web UI page has three sections:

- The page title at the top.
- A tabbed menu at the top for navigation.
- A display area for viewing and changing data.

The display area of the home page contains the following information about the IP Media Server you have logged into:

Item	Description
Host Uptime	How long the IP Media Server host has been running.

Item	Description
Media Server Uptime	How long the IP Media Server software has been running.
Current Time	The current time.

Navigating the Web User Interface (UI)

This section describes how to use the Web UI to view and change data and perform commands. The Web UI has a menu at the top for navigation and a display area for viewing and changing data.

The tabs at the top contain a hierarchical menu system. If a menu item has submenu items, an arrow appears to the right. If a menu item does not have an arrow, the item is a command. Select the menu item to execute the command. An example of the Media Server menu and menu items is shown in Figure 5.

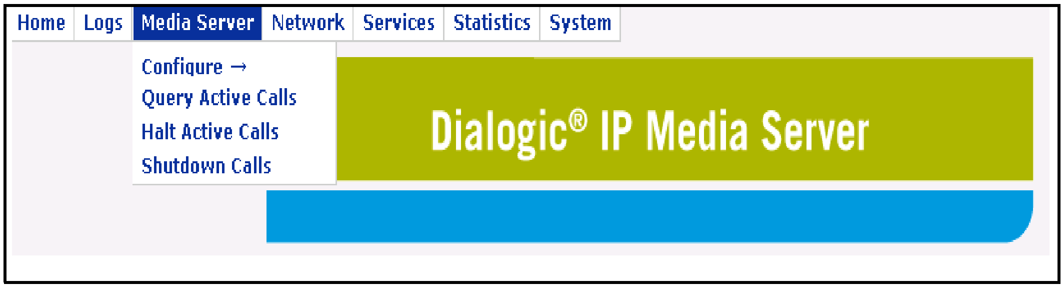


Figure 5. Menu and Display Area in the Web User Interface

Use the keyboard to navigate through the interface. The navigation keys are:

Table 2. Navigation Keys

Navigation Key	Description
Tab, up and down arrows	Navigate through the fields on a page.
Right arrow	Select an option in the menu item.
Enter	To apply, cancel, or reboot.
H	To access help.

4 - Configuring the Dialogic® IP Media Server

This chapter describes procedures for configuring the Dialogic® IP Media Server for operation, and includes the following sections:

Configuration Checklist

⚠ **Note:** Before changing the configuration of a running system, always back up the current configuration using the System→Config→Create Backup command.

The following checklist summarizes the minimum configuration steps required to get the IP Media Server up and running.

1. Configure the Network Interfaces (Network→Configure→Interface):
   - Assign IP addresses.
   - Select an interface to be used for RTP traffic.
   - Select an interface to be used as the SIP contact address.
   - Add routes to the interfaces (Network and Routes).
2. Check the IP Media Server default parameter settings:
   - Check SIP and SDP settings (Media Server→Configure→SIP).
   - Check audio codec settings (Media Server→Configure→Codec→Audio).
   - Check video codec settings (Media Server→Configure→Codec→Video).
   - Check VoiceXML settings (Media Server→Configure→VoiceXML).
   - Check CPU monitoring settings (Media Server→Configure→Media Engine).
3. Reboot the host to ensure all configuration changes take effect:
   - Select System→Reboot Host.
4. Test the interfaces:
   - From another system, ping the IP address of each interface.
   - From the IP Media Server, use the Network→Utilities→Ping command to verify that the IP Media Server can access the network.

After these configuration steps have been done, the IP Media Server can accept calls.

The following sections give details on IP Media Server configuration menus and commands.

System Files Updated

Dialogic recommends using the Web UI (administrator access level) to configure the IP Media Server. The following system files are updated during configuration.

- `/etc/hosts` (snow-sip, snow-rtp and snow-mrcp get added)
- `/etc/resolve.conf` (DNS servers)
- `/etc/ntp.conf` and `/etc/ntp/step-tickers` (NTP servers)
- `/etc/sysconfig/network-scripts/ifcfg-eth(x)` (interface configuration settings)

If you create routes on the Media Server:

- `/etc/sysconfig/network-scripts/route-eth(x)`
- `/opt/snowshore/etc/snmp.conf` and `/etc/snmp/snmp.conf` (snmp)

⚠ **You can manually update these files, but be careful because if you manually update a parameter and later change the parameter using the Web UI, you can create a conflict.**

Network Configuration

The Ethernet interfaces and routing table in the IP Media Server must be configured to enable the operation of the IP Media Server. The IP Media Server requires an interface to be designated for RTP traffic and one for SIP traffic. When IP addresses, routes and designated interfaces for SIP and RTP have been established, the IP Media Server is ready to be brought up in its default configuration and to process calls.

The Network menu provides commands for configuring and activating the Ethernet interfaces on the IP Media Server and for configuring routing and DNS information.

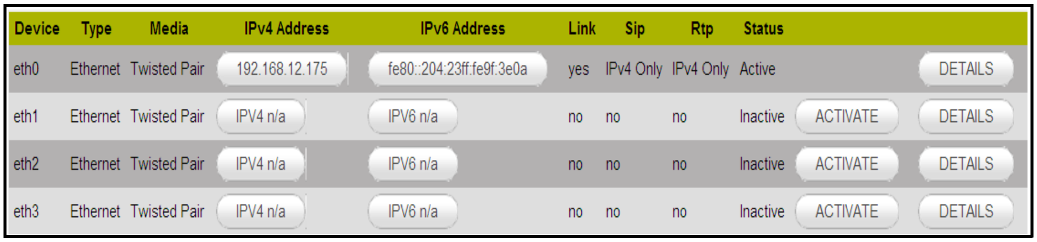
IP Media Server Ethernet Interfaces

The IP Media Server has two Ethernet interfaces by default, eth0 and eth1.

- eth0 is typically connected to a DHCP server and acquires its address via DHCP. This port is used for management and configuration access via the Web UI.
- eth1 is typically configured with a static address dedicated to SIP and RTP traffic.

Configuring Interfaces

There are two default interfaces on the IP Media Server, eth0 and eth1. To configure an interface, select Network→Configure→Interfaces. The Interfaces page appears:



Device	Type	Media	IPv4 Address	IPv6 Address	Link	Sip	Rtp	Status		
eth0	Ethernet	Twisted Pair	192.168.12.175	fe80::204:23ff:fe9f:3e0a	yes	IPv4 Only	IPv4 Only	Active		DETAILS
eth1	Ethernet	Twisted Pair	IPV4 n/a	IPV6 n/a	no	no	no	Inactive	ACTIVATE	DETAILS
eth2	Ethernet	Twisted Pair	IPV4 n/a	IPV6 n/a	no	no	no	Inactive	ACTIVATE	DETAILS
eth3	Ethernet	Twisted Pair	IPV4 n/a	IPV6 n/a	no	no	no	Inactive	ACTIVATE	DETAILS

Figure 6. Interfaces Page

The Interfaces page shows the following information:

Item	Description
Device	Device name
Type	Type of the interface: Ethernet
Media	Type of media: normally twisted pair
IPv4 Address	Current IPv4 address of the IP Media Server host

Item	Description
IPv6 Address	Current IPv6 address of the IP Media Server host
Link	Describes the physical link connection. “Yes” indicates cable is connected and a link to the connected device is established.
Sip	Indicates that Sip signaling is on this interface.
Rtp	Indicates that Rtp traffic is on this interface.
Status	Describes the administrative status of the interface. “Yes” indicates that the interface is configured.

The Interfaces page enables you to perform several actions on each interface:

- Changing the Status of an Interface (toggle between Active and Inactive)
- Viewing Interface Details
- Configuring the Interface

Changing the Status of an Interface

Note: Only Administrators can change the status of an interface.

Each interface except eth0 has a DEACTIVATE button next to it, which enables you to change its status.

- To activate an inactive interface, click ACTIVATE.

  The interface comes up with the configuration stored in the configuration file.

- To deactivate an active interface, click DEACTIVE.

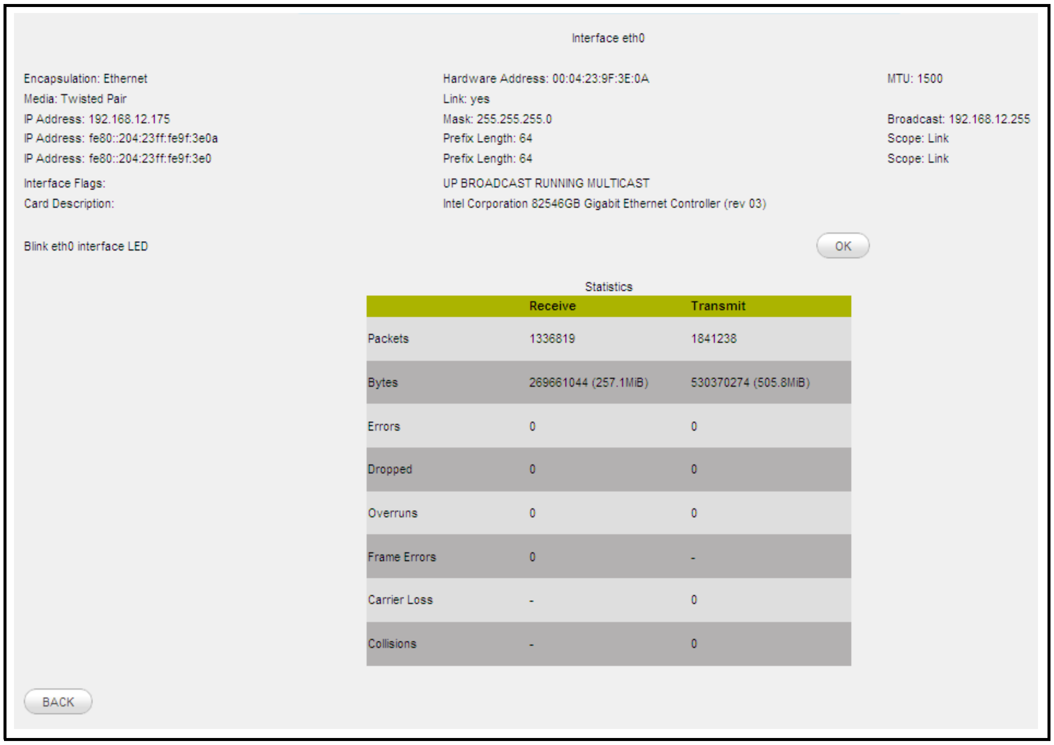
  This action stops all traffic using that interface.

  Note: You cannot deactivate the interface eth0, because there must always be an interface available for the Web User Interface.

  When you click Deactivate from the Configure Network Interfaces page, a warning page appears.

Viewing Interface Details

The DETAILS button for an interface displays the Interface Details page (Figure 7), which contains information about the running configuration of the interface and interface statistics.



Interface eth0

Encapsulation: Ethernet
Media: Twisted Pair
IP Address: 192.168.12.175
IP Address: fe80::204:23ff:fe9f:3e0a
IP Address: fe80::204:23ff:fe9f:3e0

Hardware Address: 00:04:23:9F:3E:0A
Link: yes
Mask: 255.255.255.0
Prefix Length: 64
Prefix Length: 64

MTU: 1500
Broadcast: 192.168.12.255
Scope: Link
Scope: Link

Interface Flags: UP BROADCAST RUNNING MULTICAST
Card Description: Intel Corporation 82546GB Gigabit Ethernet Controller (rev 03)

Blink eth0 interface LED

Statistics

	Receive	Transmit
Packets	1336819	1841238
Bytes	269661044 (257.1MiB)	530370274 (505.8MiB)
Errors	0	0
Dropped	0	0
Overruns	0	0
Frame Errors	0	-
Carrier Loss	-	0
Collisions	-	0

Figure 7. Interface Details Page

The configuration includes the following information:

Table 3. Interface Configuration Items

Item	Description
Encapsulation	Type of network connection (such as Ethernet).
Hardware Address	MAC address of the IP Media Server host.
MTU	Maximum Transmission Unit, the largest physical packet size, measured in bytes, that a network can carry. Ethernet has a fixed MTU of 1500 bytes.
Media	Type of media: normally twisted pair.
Link	Whether the interface is linked.
IP Address	Current IP address of the IP Media Server host.
Mask	Network mask associated with this interface.
Broadcast	Default route.
Interface Flags	Linux flags showing the current status of the interface.
Card Description	Type of hardware card for the interface.

Below the configuration parameters is a button Blink eth0 interface LED. Clicking this button lights the system LED (front and back) on the IP Media Server, so that you can identify it in a rack of equipment.

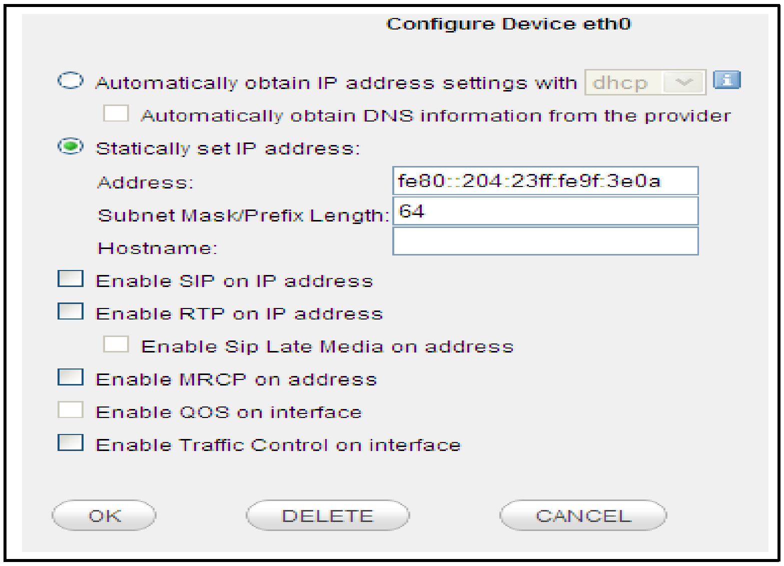
The interface statistics include statistics for all packets received at or sent from the host through the selected interface, including the numbers for Packets, Bytes, Errors, Dropped packets, Overruns, Frame errors, Carrier losses, and Collisions.

Configuring the Interface

Note: Only Administrators can configure interfaces. All users can view the configuration.

Note: If you configure a bonded interface, such as bond1, to enable/disable STP and RTP on the interface, the settings apply only to the bonded interface. They do not change any existing settings on the physical interfaces that are combined in the bonded interface.

1 Click the IP Address of the interface that you want to configure to display the Configure Network Interfaces page:



Configure Device eth0

○ Automatically obtain IP address settings with dhcp

□ Automatically obtain DNS information from the provider

● Statically set IP address:

Address: fe80::204:23ff:fe9f:3e0a

Subnet Mask/Prefix Length: 64

Hostname:

□ Enable SIP on IP address

□ Enable RTP on IP address

□ Enable Sip Late Media on address

□ Enable MRCP on address

□ Enable QOS on interface

□ Enable Traffic Control on interface

Figure 8. Configure Network Interfaces Page

When the page above appears, it shows the current information stored in the configuration file. For an active interface, this information can be different from the running configuration shown in the Interfaces display.

The IP Media Server can be configured to use a particular interface for RTP traffic and for the SIP contact address. Only interfaces configured with static IP addresses can be enabled for RTP and SIP. If DHCP is used to set the IP address for an interface, that interface cannot be enabled for RTP and SIP. You can enter a single, or multiple hostnames separated by spaces, associated with a single IP Address.

If no interface has been enabled for RTP and SIP, the system tries to use the interface associated with the local hostname. If a host name has not been assigned, this attempt fails and the IP Media Server cannot accept calls.

Note: A typical configuration uses DHCP to set the address for eth0 to be used for the Web UI. The second Ethernet interface, eth1, should have a static IP address and be used for RTP and SIP traffic.

The Enable Sip Late Media on Address field determines which interface to dictate where the late media will originate.

The Enable MRCP on address field allows you to enable MRCP on the IPv4 interface only.

2 To store the changes made, click OK. To cancel the changes, click CANCEL.

Accepting the configuration change updates the configuration file, but does not change the running configuration of an active interface:

- When you go back and display the interfaces, the running configuration is shown.
- When you return to the Configure page, the stored configuration is shown.

3 To apply a configuration change to an interface, reboot the IP Media Server.

Setting an IP Address for an Interface

Note: Only Administrators can set the IP address of an interface.

By default, the system has DHCP configured on eth0 and eth1. This allows the IP Media Server to automatically receive an IP address from a DHCP server (or from bootp). If the system is automatically obtaining an IP address, it can also obtain other DNS information, such as the network mask and hostname.

Note: If DHCP (or bootp) is used to set the IP address for an interface, you cannot enable that interface for RTP and SIP.

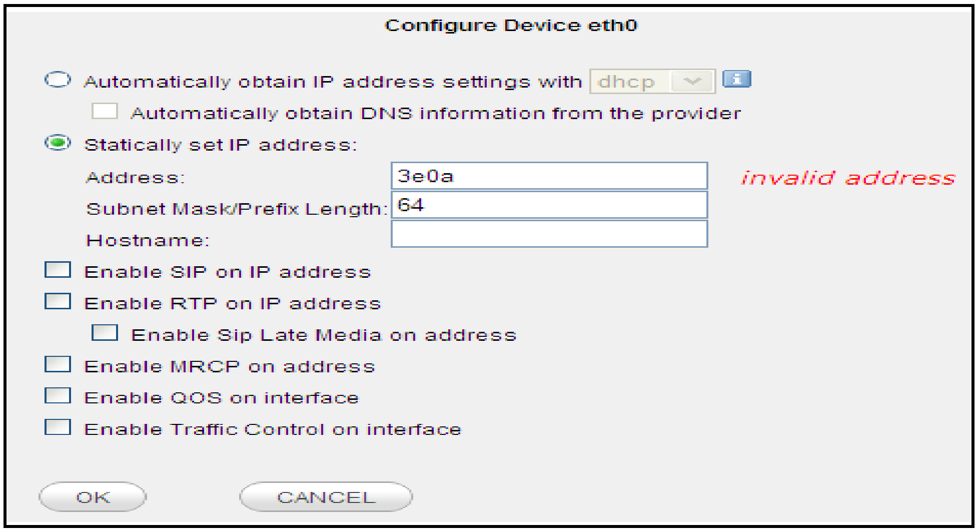
You can also set IP addresses and subnet masks statically. To do this:

1 Select Statically set IP addresses.

2 Enter an IP address and subnet mask in the Configure Network Interfaces page.

The system checks to ensure that the addresses entered are valid. If an invalid address is entered (for example, five octets instead of four), the system flags the error and does not accept the changes. The error appears in red beside the text field that has the violation. For example, in the case of a wrong IP address, the invalid address error appears in red beside the IP textbox.

3 After setting the static IP address, the Web UI will prompt you to reboot. After the reboot, you must then go into the DNS configuration and set the DNS settings since they are no longer receiving the data from DHCP. For more information, see “Configuring DNS” (page 49).



Configure Device eth0

○ Automatically obtain IP address settings with dhcp

□ Automatically obtain DNS information from the provider

● Statically set IP address:

Address: 3e0a *invalid address*

Subnet Mask/Prefix Length: 64

Hostname:

□ Enable SIP on IP address

□ Enable RTP on IP address

□ Enable Sip Late Media on address

□ Enable MRCP on address

□ Enable QOS on interface

□ Enable Traffic Control on interface

Figure 9. Setting IP Address: Error Page

Enabling SIP and RTP on an Interface

You can configure the IP Media Server to use a particular interface for RTP traffic and for the SIP contact address. Only interfaces configured with static IP addresses can be enabled for RTP and SIP. You must enable both SIP and RTP on the same interface. Typically, eth0 is configured with DHCP for the management address, and eth1 is configured with a static address and with SIP and RTP enabled.

Enabling QOS and Traffic Control on an Interface

The IP Media Server supports Differentiated Services (DiffServ) as follows:

If you select Enable QOS on interface, the IP Media Server prioritizes outgoing traffic by injecting a QOS stamp in each UDP and HTTP packet. This way, other network devices know how to prioritize the packet for delivery.

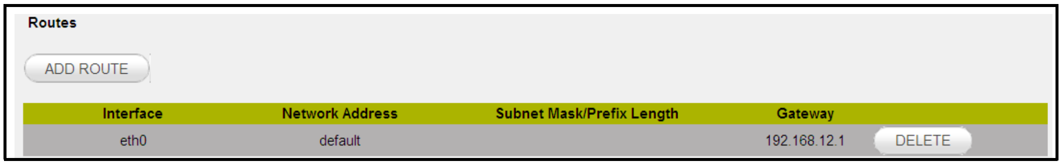
If you select Enable Traffic Control on interface, the IP Media Server filters incoming traffic. Incoming traffic that matches SIP, RTP, RTCP, and HTTP get priority over all other types of incoming traffic.

Note: Traffic Control is a system parameter and enabling/disabling it on an interface applies to all system interfaces.

Configuring Routes

Note: Only Administrators can add and delete routes. All users can display the routes.

The Network→Configure→Routes menu displays the Routes page containing the routing table for eth0 and eth1.



Interface	Network Address	Subnet Mask/Prefix Length	Gateway	
eth0	default		192.168.12.1	DELETE

Figure 10. Routes Page

The routing table displays the following information for each route:

- Interface name
- Network address
- Subnet mask
- Gateway IP address

Routes that have been automatically added to the table are displayed, but they cannot be deleted. Only routes that have been added by users have a DELETE button and can be deleted. For example, in Figure 10, one route was added automatically by the system, and the other two routes were added by a user.

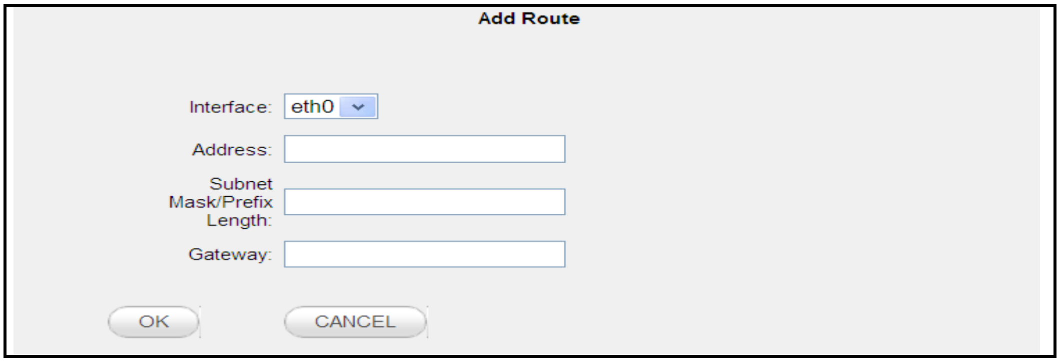
Note: Routes created by DHCP do not persist if the system is rebooted. To make a route persistent, when assigning a static IP address to the primary interface eth0, you must add it statically, even if it already appears in the list on the Routes page.
This is especially important for default routes. If you are accessing the IP Media Server from a different subnet, you must statically create a default route in order to be able to manage the system following a reboot.

Adding Routes

Note: Only Administrators can add routes.

To add a route to the system:

1 Click ADD ROUTE to display the Add Route page.



Interface: eth0

Figure 11. Add Route Page

2 Select the interface from the drop-down menu.

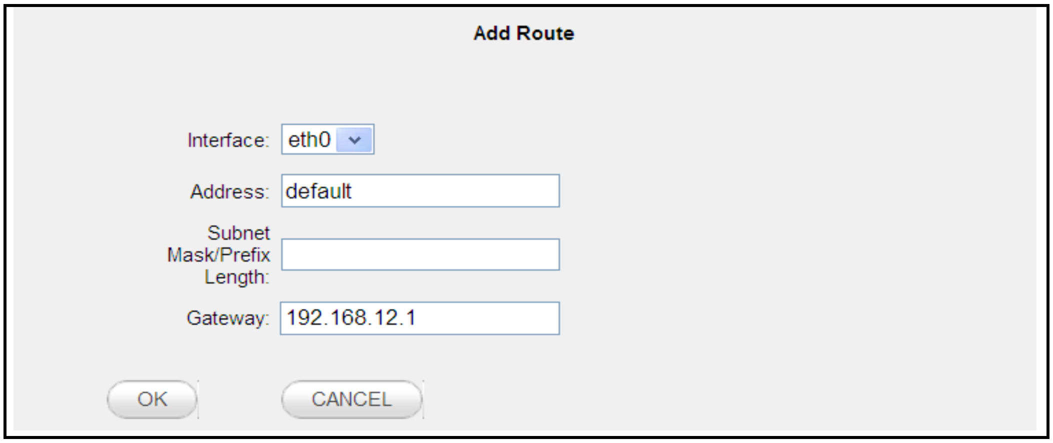
3 Enter the IP address and subnet mask; leave the Gateway field empty.

If this is a default route:

a. Type default in the Address field.

b. Leave the Subnet Mask field empty.

c. Enter a gateway IP address.



Interface: eth0

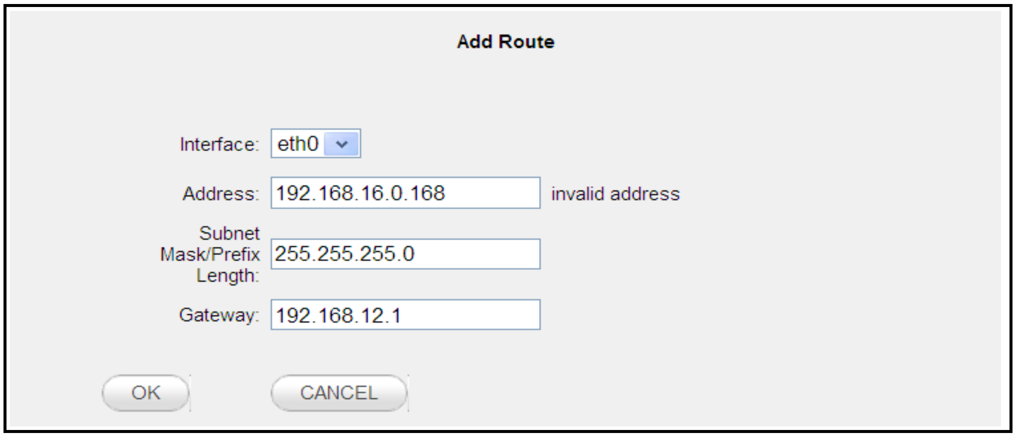
Address: default

Gateway: 192.168.12.1

Figure 12. Add Default Route Page

4 If you do not want to add the route, click CANCEL. When you are satisfied that your entries are correct, click OK.

When the OK button is selected, the route entry is checked and added to the current routing table and to the configuration file. If the route entry has an error in it, an error message appears in red next to the text field where the error occurred (for example, Figure 13).



Add Route

Interface: eth0

Address: 192.168.16.0.168 invalid address

Subnet Mask/Prefix Length: 255.255.255.0

Gateway: 192.168.12.1

Figure 13. Add Route Error Page

A confirmation page is displayed.

5 Click CONTINUE to return to the routing table display.

Note: The system displays results of the route table update immediately after OK is selected.

Deleting Routes

Note: Only Administrators can delete routes. Also, only routes that have been manually added can be deleted.

To delete a route from the system:

1. Click DELETE next to the route that is to be deleted. A confirmation page is displayed.
2. Click OK to delete the route.
3. Click CONTINUE to return to the Routes page.

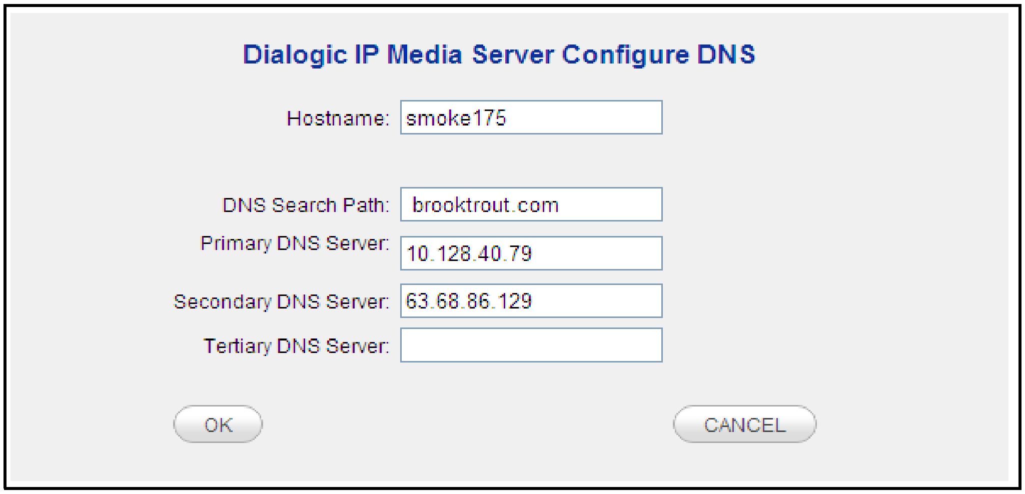
Configuring DNS

Note: Only Administrators can configure DNS. Both Administrators and Operators can display the DNS configuration.

You can configure up to three DNS servers by selecting Network→Configure →DNS. The existing configuration appears and can be changed.

To configure DNS:

1 Select Network→Configure→DNS Configuration to display the DNS Configuration page.



Dialogic IP Media Server Configure DNS

Hostname: smoke175

DNS Search Path: brooktrout.com

Primary DNS Server: 10.128.40.79

Secondary DNS Server: 63.68.86.129

Tertiary DNS Server:

Figure 14. DNS Configuration Page

2 You can change the fields on this page. To set the hostname for the Device, enter a new hostname.

3 Click **OK** to save the changes. To cancel the changes without writing them to the configuration file, click CANCEL.

Note: The IP Media Server must be reset for these changes to take place.

Network Utilities

Use the Network Utilities to determine if access to the network exists.

Ping Utility

The Ping utility is a standard ICMP ping request. It sends out twelve 64-byte packets to the specified IP address.

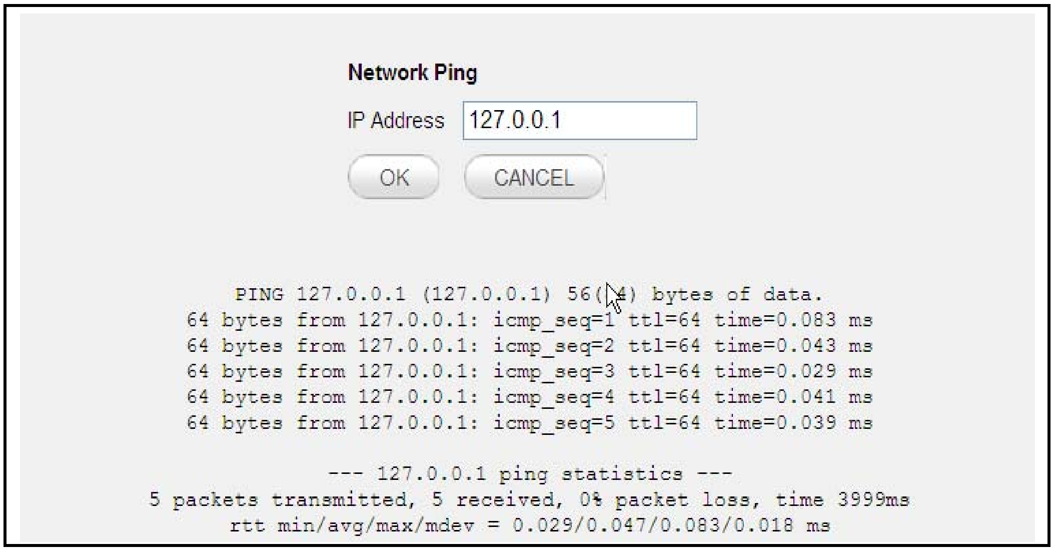
To use the Ping Utility:

1 Select Network→Utilities→Ping to display the Network Ping page.

2 Enter the IP address you want to test.

3 Click OK.

The Display Network Ping page appears with the results of the ping command.



IP Address 127.0.0.1

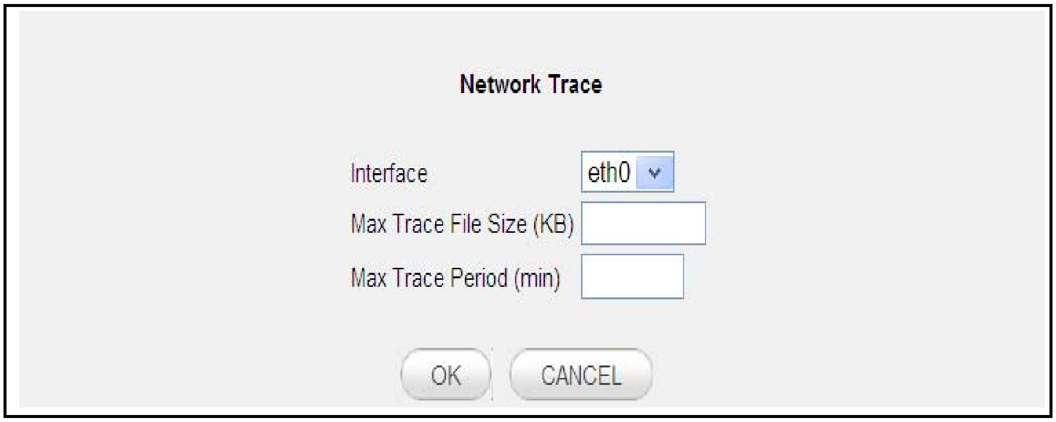
```
      PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
  64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.083 ms
  64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.043 ms
  64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.029 ms
  64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.041 ms
  64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.039 ms

          --- 127.0.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
      rtt min/avg/max/mdev = 0.029/0.047/0.083/0.018 ms
```

Figure 15. Display Network Ping Page

Trace Utility

The Trace Utility enables you to capture a network trace of all incoming and outgoing IP traffic. You can access the trace output from the Logs→Trace page. All of the traces are named by a date/timestamp.

1 Select Network→Utilities→Trace to display the Network Trace page:



Interface eth0

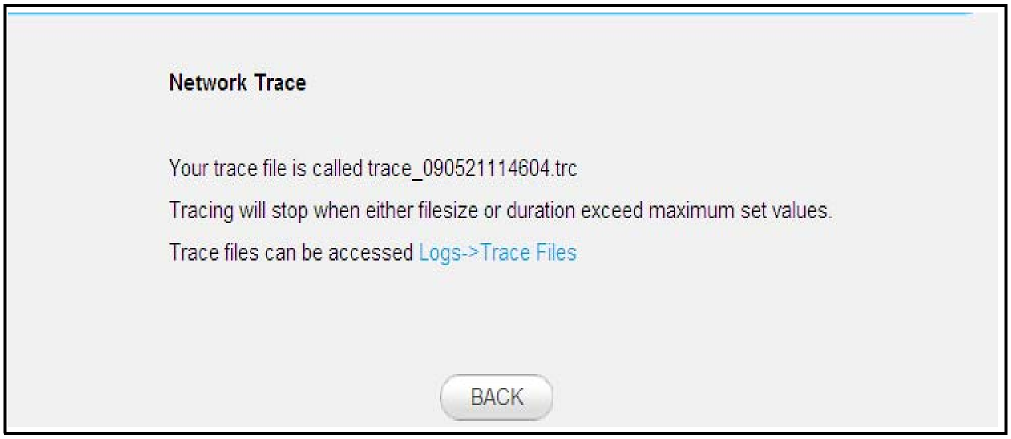
Figure 16. Network Trace Page

2 Enter the Ethernet interface you want to monitor.

3 Enter the maximum trace file size in kilobytes.

4 Enter the maximum trace time period in minutes.

5 Click OK to start the trace. The following page appears, providing status information about the trace:



Network Trace

Your trace file is called trace_090521114604.trc

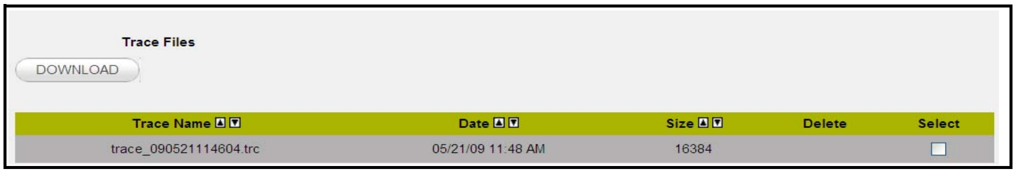
Tracing will stop when either filesize or duration exceed maximum set values.

Trace files can be accessed Logs->Trace Files

Figure 17. Network Trace Status Page

6 Click BACK to return to the Network Trace page.

7 To view a trace file, select the Logs→Trace Files menu to display the Trace Files page:



Trace Files

Trace Name ▲▼	Date ▲▼	Size ▲▼	Delete	Select
trace_090521114604.trc	05/21/09 11:48 AM	16384		□

Figure 18. Trace Files Page

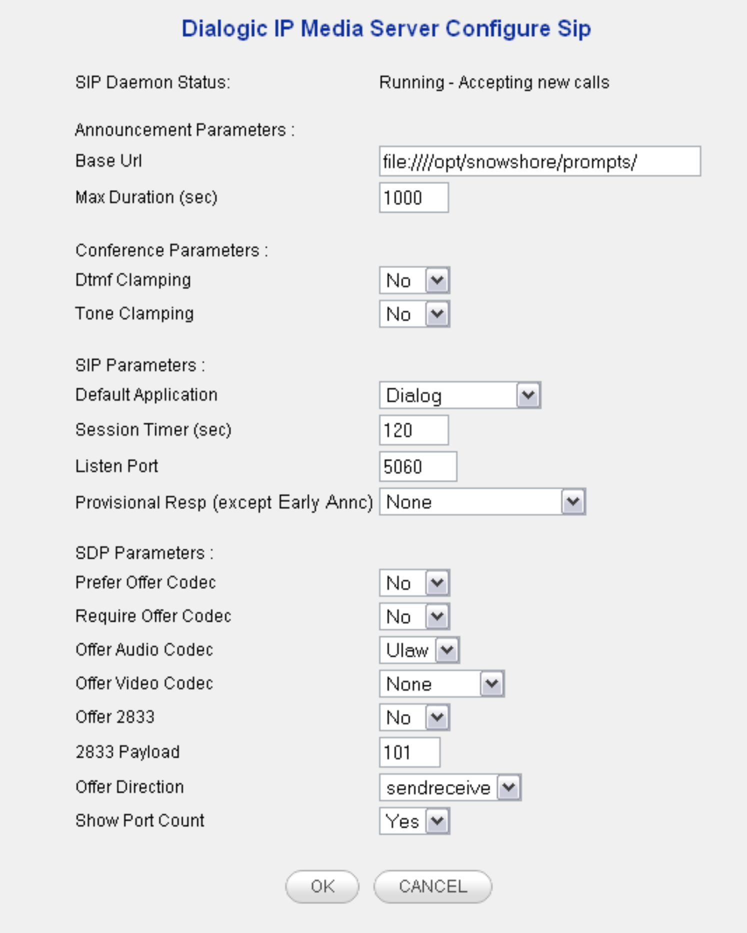
8 To view the trace file, click DOWNLOAD. The trace file is a text file you can view with any network analyzer software.

Configuring SIP and SDP

Select Media Server→Configure→SIP to configure SIP and SDP parameters.

All user access levels can view the configuration, but only Administrators can change the configuration.

⚠ **The commands in this configuration section manipulate the configuration file. To apply a new configuration, reboot the IP Media Server.**



Dialogic IP Media Server Configure Sip

SIP Daemon Status:	Running - Accepting new calls
Announcement Parameters :	
Base Url	file:///opt/snowshore/prompts/
Max Duration (sec)	1000
Conference Parameters :	
Dtmf Clamping	No
Tone Clamping	No
SIP Parameters :	
Default Application	Dialog
Session Timer (sec)	120
Listen Port	5060
Provisional Resp (except Early Annc)	None
SDP Parameters :	
Prefer Offer Codec	No
Require Offer Codec	No
Offer Audio Codec	Ulaw
Offer Video Codec	None
Offer 2833	No
2833 Payload	101
Offer Direction	sendreceive
Show Port Count	Yes

Figure 19. Configure SIP Page

Table 4 describes the SIP and SDP parameters.

Table 4. Configure SIP and SDP Parameters

Parameter	Values	Description
SIP Daemon Status	- Running - Accepting calls - Running - Not accepting calls - Not running	Current status of the SIP Daemon (SIPD).
Announcement Parameters		

Base URL	<string>	String that is prepended to non-rooted audio URLs. If an INVITE arrives with just a file name, the file name is assumed to be in the location specified in the base URL. For example, if the base URL is:
		`file:////net/IP_of_nfs_server/path_of_file_storage/`
		an invite such as:
		`INVITE sip:annc@172.17.100.157;play=circuit_busy.ulaw`
		rewrites the URL by prepending the Base URL as:
		`file:////net/IP_of_nfs_server/path_of_file_storage/circuit_busy_.ulaw`

Max Duration	- 0 - 1-10000 (Default: 0)	System-wide default announcement duration in seconds to be used if no per-call duration parameter is specified in the SIP URI. This parameter is used for both early and normal media announcements. Once the limit is reached, the IP Media Server terminates the call. A setting of 0 indicates no announcement duration limit.

Table 4. Configure SIP and SDP Parameters (Continued)

Parameter	Values	Description
Conference Parameters		
DTMF Clamping	- Yes - No (Default: No)	Simple conferences do not support DTMF clamping. Enhanced conferences use this parameter as the default when each leg is created in a conference. It can be changed later with an INFO with a new value.
Tone Clamping	- Yes - No (Default: No)	Simple conferences do not support tone clamping. Enhanced conferences use this parameter as the default when each leg is created in a conference. It can be changed later with an INFO with a new value.
SIP Parameters		
Default Application	- Announcement - Conference - Dialog - IVR (Default: Dialog)	Application (SIP service) used if the INVITE message does not specify an application.
Session Timer	Integer: - 0 - 10 - 6000 (Default: 120)	SIP Session Timer interval in seconds. A setting of 0 turns session timers off. The IP Media Server issues a session timer refresh every t/2 seconds, where t is the value set by this command. Setting this timer to a small value can significantly increase the volume of SIP message traffic over the network and can negatively impact overall service delivery and performance.
Listen Port	Integer: 1025 - 65535 (Default: 5060)	UDP port used for SIP.

Table 4. Configure SIP and SDP Parameters (Continued)

Parameter	Values	Description
Provisional Response (except Early Annc)	- None - Send 180 (ringing) - Send 183 (progress).	This parameter only applies to dialog, conference, and announce services. The provisional responses sent for these services never contain SDP information. Early announce always sends 183 Session Progress. The 183 sent for early announce is not affected by this value and always contains SDP information. This feature is normally used when interacting with other protocols that require resource reservation (e.g., PacketCable, NCS) when establishing a session.
SDP Parameters		
Prefer Offer Codec	- Yes - No (Default: No)	If Yes, the Offer Codec is used as the highest preference codec in the offer. If the Offer codec is not present, another codec can be used.
Require Offer Codec	- Yes - No (Default: No)	The policy for the SDP offer. Yes –The offer SDP must match the parameters Offer Codec, Offer 2833, 2833 Payload, and Offer Direction. If the offer does not match, the call is rejected. No – The standard offer/answer rules are used, taking into account the setting of the Prefer Offer Codec parameter.
Offer Codec	- Ulaw - Alaw - G726 - G729 - AMR (Default: Ulaw)	Codec offered by the IP Media Server in the SDP m= audio line. This setting applies when the inbound initial INVITE does not contain an SDP body, forcing the IP Media Server response to make the initial SDP offer.

Table 4. Configure SIP and SDP Parameters (Continued)

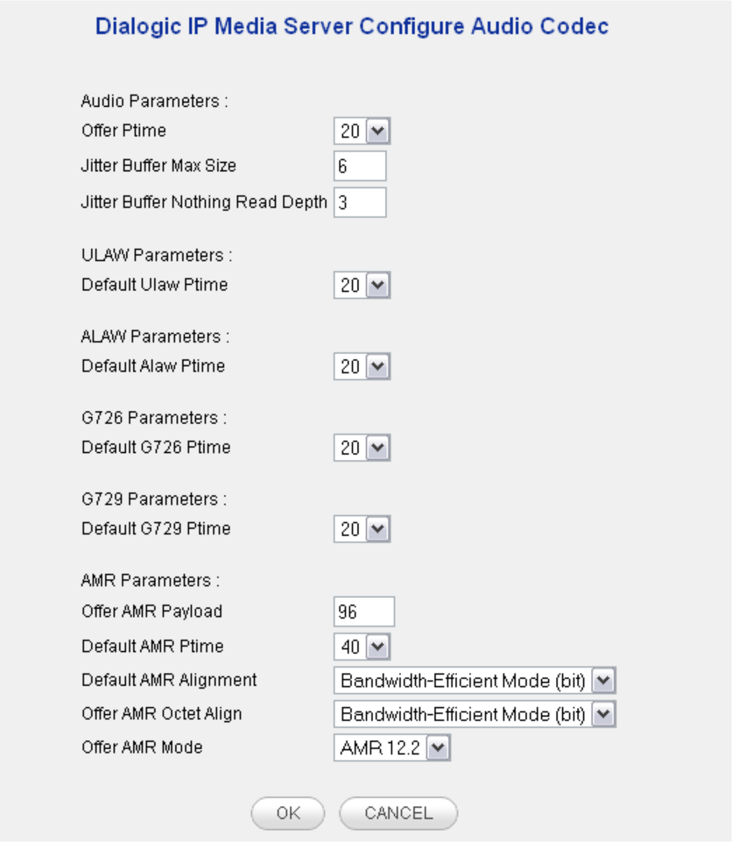
Parameter	Values	Description
Offer Ptime	◆ 10 ◆ 20 ◆ 30 (Default: 20)	Length of time in milliseconds represented by the media in a packet offered by the IP Media Server in the SDP attribute (a=). This setting applies when the inbound initial INVITE does not contain an SDP body, forcing the IP Media Server response to make the initial SDP offer.
Offer 2833	◆ Yes ◆ No (Default: Yes)	Whether 2833 is offered.
2833 Payload	integer: 96–127 (Default: 101)	Dynamic payload type to be used when 2833 is offered.
Offer Direction	◆ sendonly ◆ recvonly ◆ sendrecv (Default:sendrecv)	Direction of the media stream offered by the IP Media Server in the SDP attribute (a=). This setting applies when the inbound initial INVITE does not contain an SDP body, forcing the IP Media Server response to make the initial SDP offer.
Show Port Count	◆ Yes ◆ No (Default: Yes)	Whether "/1" is appended to the port number in the SDP attribute (m=).
Offer Video Codec	◆ None ◆ H263 ◆ H263-1998 ◆ H263-2000 ◆ H264	Default video codec for the IP Media Server.

Configuring Audio Codecs

Select Media Server→Configure→Codec→Audio to configure audio codec parameters.

All user access levels can view the configuration, but only Administrators can change the configuration.

The commands in this configuration section manipulate the configuration file. To apply a new configuration, reboot the IP Media Server.



Dialogic IP Media Server Configure Audio Codec

Audio Parameters :	
Offer Ptime	20
Jitter Buffer Max Size	6
Jitter Buffer Nothing Read Depth	3
ULAW Parameters :	
Default Ulaw Ptime	20
ALAW Parameters :	
Default Alaw Ptime	20
G726 Parameters :	
Default G726 Ptime	20
G729 Parameters :	
Default G729 Ptime	20
AMR Parameters :	
Offer AMR Payload	96
Default AMR Ptime	40
Default AMR Alignment	Bandwidth-Efficient Mode (bit)
Offer AMR Octet Align	Bandwidth-Efficient Mode (bit)
Offer AMR Mode	AMR 12.2

Figure 20. Configure Audio Codec Page

Table 5 describes the audio codec parameters.

Table 5. Configure Audio Codec Parameters

Parameter	Values	Description
Offer Ptime	◆ 10 ◆ 20 ◆ 30 (Default: 20)	Length of time in milliseconds represented by the media in a packet offered by the IP Media Server in the SDP attribute (a=). This setting applies when the inbound initial INVITE does not contain an SDP body, forcing the IP Media Server response to make the initial SDP offer.
Jitter Buffer Max Size	Integer: 6 to 10 (Default: 6)	Maximum size of jitter buffer.
Jitter Buffer Nothing Read Depth	Integer: 3 to 20 (Default: 3)	Value used to insert silence in the packet stream. If no packets are read from the line, then audio silence is inserted in the RTP stream.
Default Ulaw Ptime	◆ 10 ◆ 20 ◆ 30 (Default: 20)	Value to use when the SDP offer is received, but the PTIME attribute is not specified. This value appears in the SDP answer sent by the IP Media Server.
Default Alaw Ptime	◆ 10 ◆ 20 ◆ 30 (Default: 20)	Value to use when the SDP offer is received, but the PTIME attribute is not specified. This value appears in the SDP answer sent by the IP Media Server.
Default G726 Ptime	◆ 10 ◆ 20 ◆ 30 (Default: 20)	Value to use when the SDP offer is received, but the PTIME attribute is not specified. This value appears in the SDP answer sent by the IP Media Server.
Default G729 Ptime	◆ 10 ◆ 20 ◆ 40 (Default: 20)	Value to use when the SDP offer is received, but the PTIME attribute is not specified. This value appears in the SDP answer sent by the IP Media Server.
Offer AMR Payload	Integer: 96–127 (Default: 96)	Dynamic payload type to be used when AMR is offered.

Table 5. Configure Audio Codec Parameters (Continued)

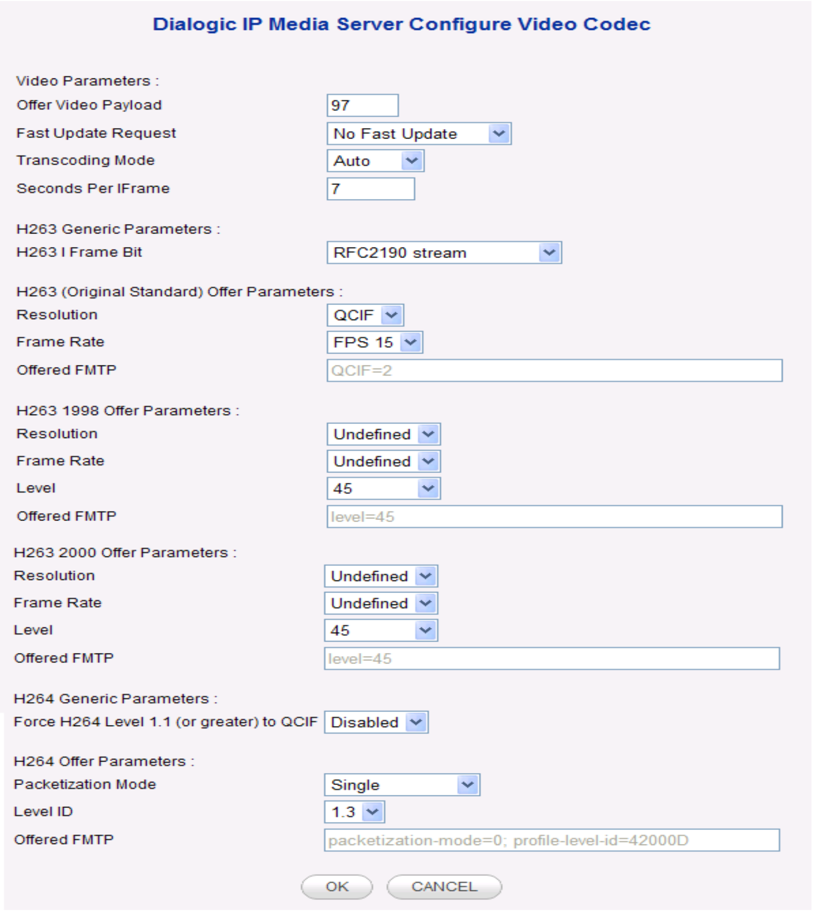
Parameter	Values	Description
Default AMR Ptime	◆ 20 ◆ 40 (Default: 20)	Value to use when the SDP offer is received, but the PTIME attribute is not specified. This value appears in the SDP answer sent by the IP Media Server.
Default AMR Alignment	◆ Bandwidth-Efficient Mode (bit) ◆ Octet-Aligned Mode (byte)	Default alignment mode to be used when INVITE SDP specifies AMR encoding, but does not specify the alignment mode.
Offer AMR Octet Align	◆ Bandwidth-Efficient Mode (bit) ◆ Octet-Aligned Mode (byte)	Alignment mode to be used when AMR is offered.
Offer AMR Mode	◆ AMR 4.75 ◆ AMR 5.15 ◆ AMR 5.9 ◆ AMR 6.7 ◆ AMR 7.4 ◆ AMR 7.95 ◆ AMR 10.2 ◆ AMR 12.2	Default AMR-NB encoding mode (bit rate).

Configuring Video Codecs

Select Media Server→Configure→Codec→Video to configure video codec parameters.

All user access levels can view the configuration, but only Administrators can change the configuration.

The commands in this configuration section manipulate the configuration file. To apply a new configuration, reboot the IP Media Server.



Dialogic IP Media Server Configure Video Codec

Video Parameters :	
Offer Video Payload	97
Fast Update Request	No Fast Update
Transcoding Mode	Auto
Seconds Per IFrame	7
H263 Generic Parameters :	
H263 I Frame Bit	RFC2190 stream
H263 (Original Standard) Offer Parameters :	
Resolution	QCIF
Frame Rate	FPS 15
Offered FMTP	QCIF=2
H263 1998 Offer Parameters :	
Resolution	Undefined
Frame Rate	Undefined
Level	45
Offered FMTP	level=45
H263 2000 Offer Parameters :	
Resolution	Undefined
Frame Rate	Undefined
Level	45
Offered FMTP	level=45
H264 Generic Parameters :	
Force H264 Level 1.1 (or greater) to QCIF	Disabled
H264 Offer Parameters :	
Packetization Mode	Single
Level ID	1.3
Offered FMTP	packetization-mode=0; profile-level-id=42000D

Figure 21. Configure Video Codec Page

Table 6 describes the video codec parameters.

Table 6. Configure Video Codec Parameters

Parameter	Values	Description
Video Parameters		
Offer Video Payload	Integer: 96–127 (Default: 97)	Dynamic payload type to be used when video is offered.
Fast Update Request	- No Fast Update - Media XML Update	Sets the fast update request field.
Transcoding Mode	- Auto - Force - Turn off (Default: Auto)	Sets the video transcoding field. Auto – Automatically determines when video transcoding is required on a video connection and enables it as needed. Force – Enables video transcoding for each video connection. Turn off – Disables video transcoding for each video connection.
Seconds per IFrame	Integer: 0–65535 (Default: 7)	Determines the maximum time interval between I-frames regardless of video content.
H.263 Generic Parameters		
H263 I Frame Bit	- Inverted RFC2190 Stream - RFC2190 Stream - Inverted H263 Location - H263 Location	Sets the I-frame bit.
H.263 (Original Standard) Offer Parameters		
Resolution	- QCIF - CIF - Undefined (Default: QCIF)	Resolution to be used when video is offered. If Undefined is selected, the default value is used.

Table 6. Configure Video Codec Parameters (Continued)

Parameter	Values	Description
Frame Rate	- FPS 6 - FPS 10 - FPS 15 - FPS 30 - Undefined (Default: FPS 15)	Frame rate to be used when video is offered. If Undefined is selected, the default value is used.
Offered FMTP		Write-protected. Contains the string used for the FMTP line in the offered message.
H.263 1998 Offer Parameters		
Resolution	- QCIF - CIF - Undefined (Default: QCIF)	Resolution to be used when video is offered. If Undefined is selected, the default value is used. If Offer Level parameter is specified, this parameter is set to Undefined.
Frame Rate	- FPS 6 - FPS 10 - FPS 15 - FPS 30 - Undefined (Default: FPS 15)	Frame rate to be used when video is offered. If Undefined is selected, the default value is used. If Offer Level parameter is specified, this parameter is set to Undefined.
Level	- 10 - 20 - 30 - 40 - 45 - Undefined (Default: 45)	Level to be used when video is offered. If Undefined is selected, the default value is used. If Offer Resolution and Offer Frame Rate are specified, this parameter is set to Undefined.
Offered FMTP		Write-protected. Contains the string used for the FMTP line in the offered message.
H.263 2000 Offer Parameters		

Table 6. Configure Video Codec Parameters (Continued)

Parameter	Values	Description
Resolution	- QCIF - CIF - Undefined (Default: QCIF)	Resolution to be used when video is offered. If Undefined is selected, the default value is used. If Offer Level parameter is specified, this parameter is set to Undefined.
Frame Rate	- FPS 6 - FPS 10 - FPS 15 - FPS 30 - Undefined (Default: FPS 15)	Frame rate to be used when video is offered. If Undefined is selected, the default value is used. If Offer Level parameter is specified, this parameter is set to Undefined.
Level	- 10 - 20 - 30 - 40 - 45 - Undefined (Default: 45)	Level to be used when video is offered. If Undefined is selected, the default value is used. If Offer Resolution and Offer Frame Rate are selected, this parameter is set to Undefined.
Offered FMTP		Write-protected. Contains the string used for the FMTP line in the offered message.
H.264 Generic Parameters		
Force H264 Level 1.1 (or greater) to QCIF	- Enabled - Disabled (Default: Disabled)	When enabled, forces H.264 video output to default to QCIF. When disabled, forces H.264 video output to default to CIF.
H.264 Offer Parameters		
Packetization Mode	- Single - Non-Interleaved - Interleaved (Default: Single)	Packetization to be used when video is offered.

Table 6. Configure Video Codec Parameters (Continued)

Parameter	Values	Description
Level ID	◆ 1 ◆ 1B ◆ 1.1 ◆ 1.2 ◆ 1.3 (Default: 1.3)	Level ID to be used when video is offered.
Offered FMTP		Write-protected. Contains the string used for the FMTP line in the offered message.

Configuring VoiceXML

Select Media Server→Configure→VoiceXML to configure VoiceXML support on the IP Media Server. The Configure VoiceXML page is displayed (see Figure 22 and Figure 23).

⚠ **The commands in this configuration section manipulate the configuration file. To apply a new configuration, reboot the IP Media Server.**

VoiceXML Version

The IP Media Server supports two versions of VoiceXML:

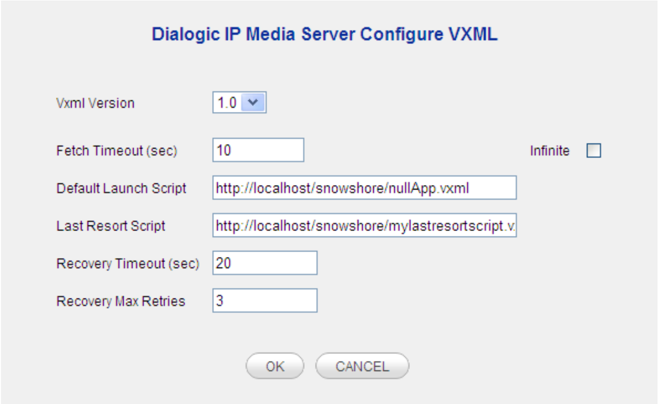
- VoiceXML 1.0
- VoiceXML 2.0 (default browser)

Use the Vxml Version drop-down list box to select the version of VoiceXML that you want to enable on the IP Media Server. The default is VoiceXML version 2.0.

Each version has its own configuration parameters. The parameters associated with VoiceXML 1.0 and 2.0 configurations are described below.

VoiceXML 1.0 Configuration Parameters

If you select VXML Version 1.0, the Configure VoiceXML page appears as follows:



Dialogic IP Media Server Configure VXML

Vxml Version	1.0		
Fetch Timeout (sec)	10	Infinite	□
Default Launch Script	http://localhost/snowshore/nullApp.vxml		
Last Resort Script	http://localhost/snowshore/mylastresortscript.v		
Recovery Timeout (sec)	20		
Recovery Max Retries	3		

Figure 22. Configure VoiceXML 1.0 Page

Table 7 describes the parameters you can set for VoiceXML Version 1.0.

Table 7. VoiceXML 1.0 Parameters

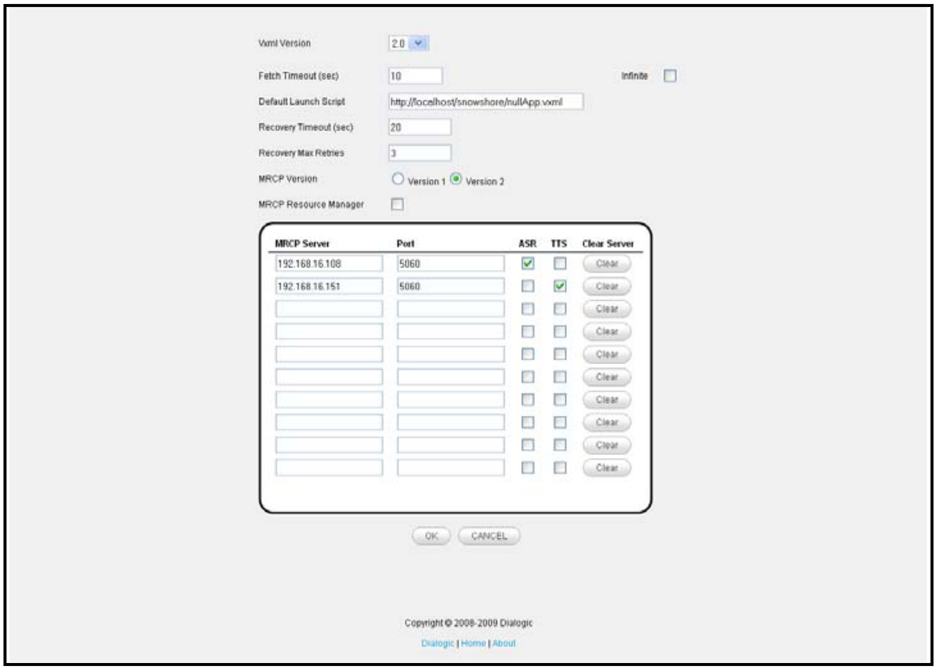
Parameter	Values	Description
Fetch Timeout	integer: 1–65, infinite (Default: 10)	Time (in seconds) the IP Media Server waits when trying to fetch a VoiceXML script from the network. A value of infinite means that a fetch timeout is not applied.
Default Launch Script	<string>	VXML script that is fetched if a dialog request is received and it does not contain a voicexml= parameter. This parameter allows a call to be accepted and for a VoiceXML script to be launched as a result of the initial SIP invite. A Launch Script is required regardless of the browser.
Last Resort Script	<string>	VXML script that is fetched and executed if the VoiceXML browser cannot retrieve the initial VoiceXML script due to a network, server, or other system issue.
Recovery Timeout	integer (Default: 20)	Time (in seconds) after which an attempt to recover media content files will fail. This setting and the Recovery Max Retries setting apply to VXML applications that use the Media Content Recovery extensions in VXML 1.0.

Table 7. VoiceXML 1.0 Parameters

Parameter	Values	Description
Recovery Max Retries	integer (Default: 3)	Number of times to retry the recovery of media content files. If a particular file cannot be delivered within the configured number of retry attempts, a "final failure" state is reached. If this occurs, the recovery daemon writes an error-level log message specifying the file name and associated recovery information. The recovery daemon generates an SNMP trap to inform the operator of this condition.

VoiceXML 2.0 Configuration Parameters

If you select VXML Version 2.0, the Configure VoiceXML page appears as follows:



Vxml Version: 2.0

Fetch Timeout (sec): 10 Infinite □

Default Launch Script: http://localhost/snowshore/nullApp.vxml

Recovery Timeout (sec): 20

Recovery Max Retries: 3

MRCP Version: ○ Version 1 ● Version 2

MRCP Resource Manager □

MRCP Server	Port	ASR	TTS	Clear Server
192.168.16.108	5060	☑	□	Clear
192.168.16.151	5060	□	☑	Clear
		□	□	Clear
		□	□	Clear
		□	□	Clear
		□	□	Clear
		□	□	Clear
		□	□	Clear
		□	□	Clear
		□	□	Clear

Figure 23. Configure VoiceXML 2.0 Page

Note: MRCP servers can be configured for both ASR and TTS as well as just ASR and just TTS. If you check both ASR and TTS buttons then both are configured.

Table 8 describes the parameters you can set for VoiceXML Version 2.0. MRCP server entries should be contiguous (no blank lines).

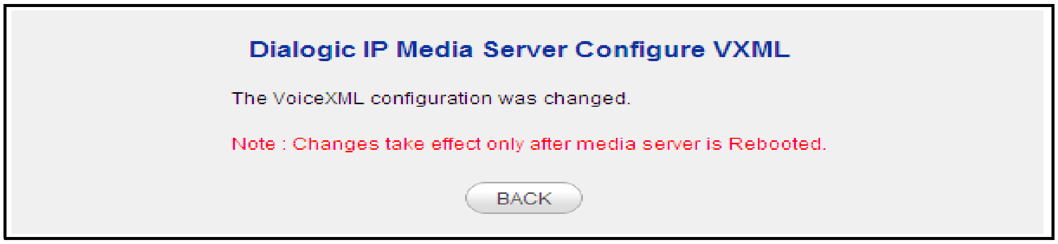
Table 8. VoiceXML 2.0 Parameters

Parameter	Values	Description
Fetch Timeout	integer: 1–65, infinite (Default: 10)	Time (in seconds) the IP Media Server waits when trying to fetch a VoiceXML script from the network. A value of infinite means that a fetch timeout is not applied.
Default Launch Script	<string>	VXML script that is fetched if a dialog request is received and it does not contain a voicexml= parameter. This parameter allows a call to be accepted and for a VoiceXML script to be launched as a result of the initial SIP invite. A Launch Script is required.
Recovery Timeout	integer (Default: 20)	Time (in seconds) after which an attempt to recover media content files will fail. This setting and the Recovery Max Retries setting apply to VXML applications that use the Media Content Recovery extensions.
Recovery Max Retries	integer (Default: 3)	Number of times to retry the recovery of media content files. If a particular file cannot be delivered within the configured number of retry attempts, a "final failure" state is reached. If this occurs, the recovery daemon writes an error-level log message specifying the file name and associated recovery information. The recovery daemon generates an SNMP trap to inform the operator of this condition.

Table 8. VoiceXML 2.0 Parameters

Parameter	Values	Description
MRCP Resource Manager	Checkbox	If unchecked and multiple servers are configured offering the same service (ASR or TTS or both), the IP Media Server software performs load balancing automatically. If checked, the ASR or TTS server performs the load balancing, if provided by the manufacturer.
MRCP Server	IP Address (associated with a port)	Enter the IP address of the MRCP server.
Port	Integer	Indicates the TCP port that is used to send SIP signaling to establish MRCP sessions. The ports are based on what is configured on the MRCP server and are outside IP Media Server Control.
ASR	Checkbox	Select if this MRCP server is for ASR.
TTS	Checkbox	Select if this MRCP server is for TTS. MRCP servers can be configured for ASR and TTS as well as configured for just ASR or just TTS.

You must reboot the IP Media Server for changes to any of the VoiceXML parameters to take effect.



Dialogic IP Media Server Configure VXML

The VoiceXML configuration was changed.

Note : Changes take effect only after media server is Rebooted.

Figure 24. Configure VoiceXML Confirmation Page

Configuring CPU Monitoring Parameters

Select Media Server→Configure→Media Engine to configure CPU monitoring parameters.

All user access levels can view the configuration, but only Administrators can change the configuration.

⚠ **The commands in this configuration section manipulate the configuration file. To apply a new configuration, reboot the IP Media Server.**

Follow these steps to configure CPU monitoring parameters:

1 Select Media Server→Configure→Media Engine to display the Configure Media Engine page.

2 Click the Enable CPU Monitoring checkbox. CPU Load parameters are displayed:

% CPU Load to Reject New Calls (default value 85%)
% CPU Load to Accept New Calls (default value 80%)

Note: The value for % CPU Load to Accept New Calls must be less than or equal to the value for % CPU Load to Reject New Calls. If it is higher, the system will reset it to equal the value for % CPU Load to Reject New Calls.

3 Modify the value as needed for % CPU Load to Reject New Calls. When this CPU threshold value is exceeded, IP Media Server rejects any new calls and sends a SIP response, 480 Temporarily Unavailable, to the client.

4 Modify the value as needed for % CPU Load to Accept New Calls. After the Reject New Calls threshold is exceeded, the CPU load must fall below the Accept New Calls threshold in order for calls to be accepted by IP Media Server.

5 Click **OK**.

6 Reboot the IP Media Server to apply the changes.

Configuring Fax

The fax software in the IP Media Server comes preconfigured. If you want to change any of the default values of the attributes, follow the procedures below to update the following configuration files:

- btcall
- Call Control

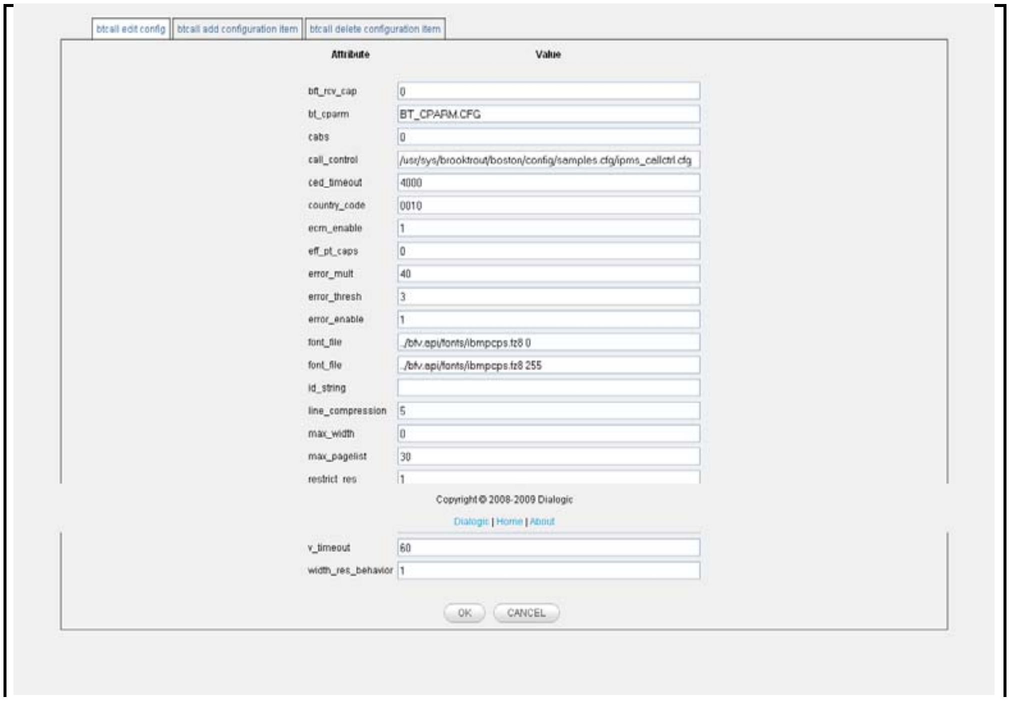
btcall

Follow the procedure below to edit, add, and/or delete attributes for the btcall configuration file.

Editing btcall Attributes

Follow the steps below to edit BTCALL attributes.

1 Select Media Server→Configure→ Fax → Btcall and click the btcall edit config tab. The following page appears.



btcall edit config
btcall add configuration item
btcall delete configuration item

Attribute	Value
bft_rcv_cap	0
bt_cparm	BT_CPARM.CFG
cabs	0
call_control	/usr/sys/brooktrout/boston/config/samples.cfg/ipms_callctrl.cfg
ced_timeout	4000
country_code	0010
ecm_enable	1
eff_pt_caps	0
error_mult	40
error_thresh	3
error_enable	1
font_file	./bfv.api/fonts/ibmpcps.fz8 0
font_file	./bfv.api/fonts/ibmpcps.fz8 255
id_string	
line_compression	5
max_width	0
max_pagelist	30
restrict_res	1
v_timeout	60
width_res_behavior	1

Figure 25. Edit btcall Configuration Page

2 Complete the page as indicated in Table 9 below. Click OK when complete.

Table 9. btcall Attributes

Attribute	Values	Description
bft_rcv_cap		Not used
bt_cparm	String Default: BT_CPARM.CFG	Specifies the path and name of the country telephony parameter file to use.
call_control	<User defined>	Specifies the name of the call control configuration file to use.
cabs		Not used
ced_timeout	Country dependent: 4000 (40 sec) in USA	Specifies the length of time, in 10 ms units, to wait for a fax answer tone (CED tone) from a remote fax machine. This parameter can only be set if the host country permits changing the wait_for_ced_high and wait_for_ced_low
country_code	<Hexadecimal> Default: 0010 (USA)	Specifies the international country code with modifiers. Initial digits (up to 3) identify the host country; the last digit supplies a modifier for properties such as the phone system attached to the board. The ccode.h header file contains the available country codes.
ecm_enable	0 - Turns off ECM 1 - Turns on ECM (256-byte frames) (default) 2 - Turns on ECM (64-byte frames)	Turns ECM (error correction mode) on or off. If disabled, MMR fax compression on the line is unavailable. The normal ECM frame size is 256 bytes. You can enable a frame size of 64 bytes, but the channel uses that frame size on transmit only. On receive, it always uses the frame size the transmitter selects.

Attribute	Values	Description
eff_pt_caps	Values are formed by logically ORing together the base values: 0 - Enhanced fax format reception disabled. 1 - JPEG. 2 - Full color mode (JPEG). 4 - Reserved for Huffman tables, do not use. 8 - 12 bits/pel, otherwise 8 bits/pel (JPEG). 10 - No subsampling (JPEG). 20 - Custom illuminant (JPEG). 40 - Custom Gamut (JPEG). 100 - JBIG. 200 - L0 Mode (JBIG).	Specifies the enhanced fax format page types that the channel is permitted to receive. If EFF page reception is enabled, then ECM is automatically enabled for receive faxes regardless of the setting of ecm_enable.
error_mult	<Decimal> Default: 40 (for 5% error rate)	Specifies an error multiplication value used to determine if the error percentage on a received page is too high. The number of errors per page is multiplied by this number and the product is divided by 2. If this result exceeds the number of lines on the page, the error percentage per page is too high and an RTN signal is returned to the transmitting station. The value set for this parameter should normally be less than that of the error_mult_rtp parameter (corresponding to a larger percentage). The RTN threshold takes precedence over the RTP threshold.
error_thresh	<Decimal> Default: 3	Specifies an error threshold value of n (2n for fine resolution) number of consecutive bad G3 lines on a received page. A page with errors in this number of consecutive lines is considered bad, regardless of the results from error_mult. An RTN is returned when a “bad” page occurs.

Attribute	Values	Description
error_enable	0 - Off 1 - On (default)	Turns error detection on (1) or off (0) during fax reception in non-ECM mode.
font_file	<String or Decimal> 0 - 6, 255 Default: ibmpcps.fz8 (no path) and 0	Specifies the name of the file that contains the transmit/convert font for ASCII. An optional font number, indicating the downloadable font to use, can be specified (if no font number is specified, 0 is assumed). The font file must be located in the current directory, or the correct path must be included with its name. The file is opened, and the contents downloaded to the module when BfvLineReset is called using the mill_load_fonts option. Multiple occurrences of font file parameters with different font numbers are permitted in the configuration file. When a font number that is specified for ASCII conversion has not been downloaded, a default font is used. This is font 255. Font 255 may be specified using the font_file keyword. If not, it defaults to ibmpcps.fz8 (no path). When font downloads are done as described above, font 255 is always downloaded regardless of whether other font numbers are listed using this keyword. Some font numbers may be reserved for preloaded fonts.
id_string	<String> Default: 20 spaces	Sets the default ID string (up to 20 characters long) for fax machines. The parameter can be overridden by the BfvFaxSetLocalId function if the host country permits changing the ID string.
line_compression	0 - MH only 1 - MR or MH 5 - MMR, MR, or MH (default)	Specifies the permitted compression types for fax transmission or reception on the phone line. This specification is independent of the file format specified for transmission or reception. If ECM is disabled, then MMR fax compression on the line is unavailable.

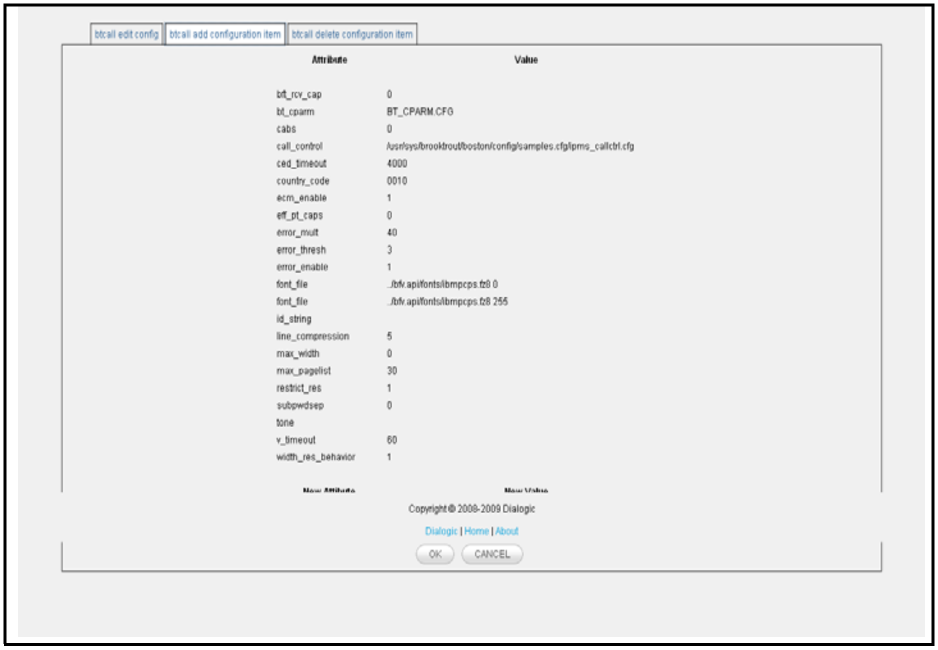
Attribute	Values	Description
max_width	0 - 215 mm A4 1728 Normal resolution pixels. (default) 1 - 255 mm B4 2048 Normal resolution pixels. 2 - 303 mm A3 2432 Normal resolution pixels.	Sets the maximum page width permitted for fax reception.
max_pagelist	<Decimal> Default: 30	Specifies the maximum number of pages allowed for storing results during a call. The last max_pagelist PAGE_RES structures are accessible via the FAX_RES structure if this feature has been enabled.
restrict_res	0 - 200H x 100V (normal) and 100H x 100V (for JPEG only) 1 - 200H x 200V (fine) 2 - 200H x 400V 4 - 300H x 300V 8 - 400H x 400V 10 - 300H x 600V 20 - 400H x 800V 40 - 600H x 600V 80 - 600H x 1200V 100 - 1200H x 1200V	Specifies allowable resolutions for fax reception. Regardless of the value chosen, 200H x 100V (normal) and 100H x 100V (for JPEG only) is always allowed.
subpwdsep	To form values, OR together the following base values: 0 - SUB, PWD, and SEP reception disabled. 1 - SEP reception enabled. 2 - PWD reception enabled. 4 - SUB reception enabled.	Enables reception of the SUB, PWD, and SEP FSK signals. Applications typically use these signals to direct or validate incoming calls.
Tone	Tone	Channel used DTMF tone dialing as the default mode

Attribute	Values	Description
v_timeout	<Decimal> Default: 60	Specifies the maximum time (in seconds) to wait after the last dialed digit for a final call progress result. Use only when you select CALL_PROTOCOL_VOICE mode. This parameter only applies to the use of BfvLineOriginateCall and BfvLineOrigCallDB.
width_res_behavior	<Decimal> Default: 1	Specifies the action taken as a result of page width or resolution mismatches on fax transmission. Does not affect fax reception. Scaling the fax is not available for all combinations of resolution mismatches.

Adding btcall Attributes

Follow the steps below to add new btcall attributes.

1 Select Media Server →Configure→ Fax → Btcall and click the btcall add configuration item tab. The following page appears.



btcall edit config
btcall add configuration item
btcall delete configuration item

Attribute	Value
bft_rcv_cap	0
bt_cparm	BT_CPARM.CFG
cabs	0
call_control	/usr/sys/brooktrout/boston/config/samples.cfg/ipms_callctrl.cfg
ced_timeout	4000
country_code	0010
ecm_enable	1
eff_pt_caps	0
error_mult	40
error_thresh	3
error_enable	1
font_file	../bfv.api/fonts/ibmpcps.f28 0
font_file	../bfv.api/fonts/ibmpcps.f28 255
id_string	
line_compression	5
max_width	0
max_pagelist	30
restrict_res	1
subpwdsep	0
tone	
v_timeout	60
width_res_behavior	1

Figure 26. Add btcall Configuration Item Page

2 Enter the attribute in the New Attribute field.

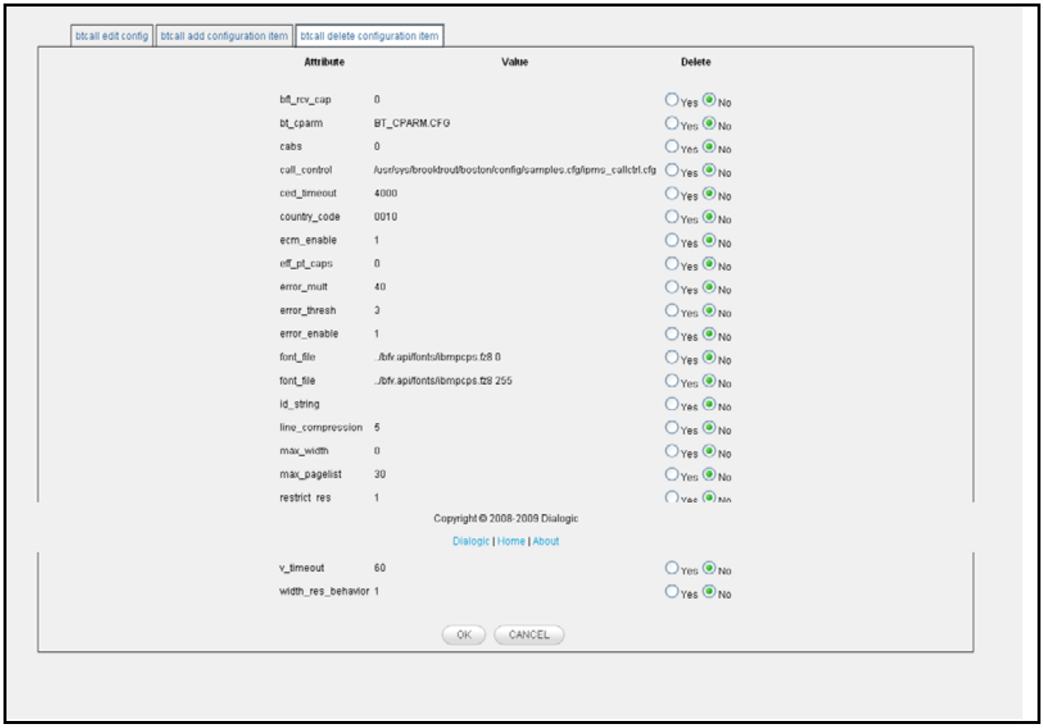
3 Enter the value in the New Value field.

4 Repeat the steps above for additional attributes.

5 Click OK when complete.

Deleting btcall Attributes

1 Select Media Server→Configure→Fax→ Btcall and click the btcall delete configuration tab. The following page appears.



btcall edit config
btcall add configuration item
btcall delete configuration item

Attribute	Value	Delete
bfl_rcv_cap	0	○ Yes ● No
bt_cparm	BT_CPARM.CFG	○ Yes ● No
cabs	0	○ Yes ● No
call_control	/usr/sys/brooktrout/boston/config/samples.cfg/ipms_callctrl.cfg	○ Yes ● No
ced_timeout	4000	○ Yes ● No
country_code	0010	○ Yes ● No
ecm_enable	1	○ Yes ● No
eff_pt_caps	0	○ Yes ● No
error_mult	40	○ Yes ● No
error_thresh	3	○ Yes ● No
error_enable	1	○ Yes ● No
font_file	../bfv.api/fonts/ibmpcps.f28 0	○ Yes ● No
font_file	../bfv.api/fonts/ibmpcps.f28 255	○ Yes ● No
id_string		○ Yes ● No
line_compression	5	○ Yes ● No
max_width	0	○ Yes ● No
max_pagelist	30	○ Yes ● No
restrict_res	1	○ Yes ● No
v_timeout	60	○ Yes ● No
width_res_behavior	1	○ Yes ● No

Copyright © 2008-2009 Dialogic

Dialogic | Home | About

Figure 27. Delete btcall Configuration Item Page

2 Select Yes next to the attributes that you want to delete.

3 Click OK.

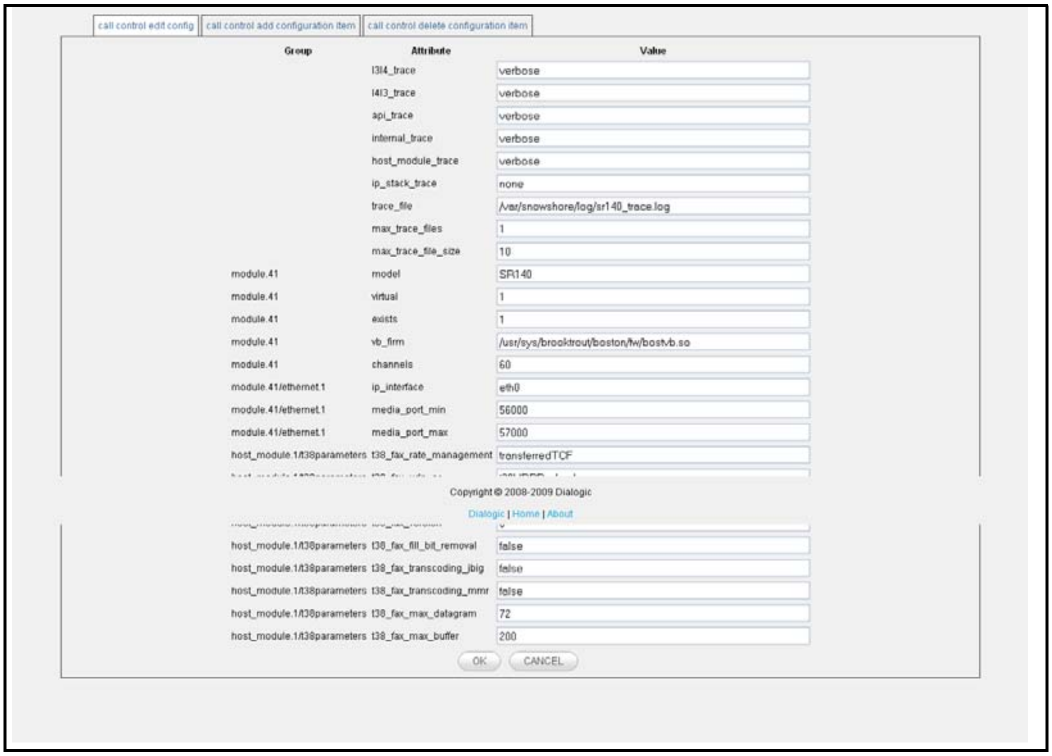
Call Control

Follow the procedures below to edit, add, and/or delete attributes in the Call Control configuration file.

Editing Call Control Attributes

Follow the steps below to edit BTCALL attributes.

1 Select Media Server→ Configure→ Fax → Call Control. The following page appears.


call control edit config
call control add configuration item
call control delete configuration item
Copyright © 2008-2009 Dialogic
Dialogic | Home | About
OK
CANCEL

Group	Attribute	Value
	l3l4_trace	verbose
	l4l3_trace	verbose
	api_trace	verbose
	internal_trace	verbose
	host_module_trace	verbose
	ip_stack_trace	none
	trace_file	/var/snowshore/log/sr140_trace.log
	max_trace_files	1
	max_trace_file_size	10
module.41	model	SR140
module.41	virtual	1
module.41	exists	1
module.41	vb_firm	/usr/sys/brooktrout/boston/fw/bostvb.so
module.41	channels	60
module.41/ethernet.1	ip_interface	eth0
module.41/ethernet.1	media_port_min	56000
module.41/ethernet.1	media_port_max	57000
host_module.1/t38parameters	t38_fax_rate_management	transferredTCF
host_module.1/t38parameters	t38_fax_fill_bit_removal	false
host_module.1/t38parameters	t38_fax_transcoding_jbig	false
host_module.1/t38parameters	t38_fax_transcoding_mmr	false
host_module.1/t38parameters	t38_fax_max_datagram	72
host_module.1/t38parameters	t38_fax_max_buffer	200

Figure 28. Edit Call Control Configuration Page

2 Complete the page as indicated in Table 10 below. Click OK when complete.

Table 10. Call Control Attributes

Attribute	Values	Description
1314_trace	none - Does not perform a trace operation (default value). error - Detects errors and stores them in the specified trace_file. warning - Detects warnings and stores them in the specified trace_file. basic - Stores a simplified trace in the specified trace_file. verbose - Stores a complete trace of operations in the specified trace_file.	Traces BSMI messages between layers 3 and 4.

Attribute	Values	Description
1413_trace	Same as 1314_trace above.	Traces BSMI messages between layers 4 and 3.
api_trace	Same as 1314_trace above.	Traces call control activity to and from the Bfv API functions.
internal_trace	Same as 1314_trace above.	Traces call control activity in areas not otherwise covered. Dialogic's engineering personnel use this tracing. Application developers are not advised to select this type of tracing.
host_module_trace	Same as 1314_trace above.	Traces call control activity to and from all host modules defined in your call control configuration file.
ip_stack_trace	Same as 1314_trace above.	Traces call control activity to and from all IP stack module libraries defined in your call control configuration file.
trace_file	<user defined>	Turns on tracing and reports results to the filename specified for this parameter.
max_trace_files	1 - 999 Default: 1	Specifies the maximum number of trace files for the API to retain on the system's file system. When set to a value greater than 1, the API appends a sequence number extension to the file name, starting at 1. If the number of created trace files exceeds the value set for this parameter, the API starts deleting files from the lowest numbered trace log until it frees sufficient disk space to store the last created file. To prevent deleting older files, set the maximum number of trace files to a large number.
max_trace_file_size	0 - Sets the trace file to an unlimited size Default: 10	Specifies the maximum size, in megabytes, allowed for the trace file. If the trace of operations reaches this size, tracing loops back to the start of the file and the continued trace starts overwriting the older trace.

Attribute	Values	Description
model	<user defined>	Indicates a value that identifies the name of a module. The configuration tool uses the value in this parameter as the cached information that identifies the module when in offline mode.
virtual	1	If present in the file, this parameter indicates that the module is a virtual module. When the parameter is absent, configuration applies to a hardware module.
exists	0 - Module does not exist 1 - Module exists	Indicates the state of a module.
vb_firm	Default: No default. Absence of the parameter indicates that the module is not a virtual module.	Indicates that the module is a virtual module and specifies the filename of the shared library that contains the loadable firmware for the virtual module

Attribute	Values	Description
channels	0 - Specifies downloading the firmware to the default value of the number of channels on the module (default). 1 – 1024 - Specifies a value defining the number of channels on the module configured to receive a firmware download.	Specifies the number of channels on either a hardware or virtual module configured to receive a firmware download. When the firmware is downloaded to a module for the first time, the assigned ordinal channel numbers start wherever the assignment left off on the previous module. As the system initializes the modules, this numbering process creates a continuous ordering of the channel assignments across all the modules in the system. On later downloads, each module's ordinals begin at the same location, regardless of any decrease or increase in the channel count of a lower-numbered module. Therefore, if you decrease the channel count for a lower numbered module, the process creates gaps in the channel numbering assignments, possibly affecting your application. If you attempt to increase the channel count above any module's initial channel count, the system ignores the added channels. For the following situations, restart the driver whenever you want to: 1. Get a continuous assignment of channel numbers after decreasing the channel count on any module. 2. Increase the number of channels above a module's initial channel count.

Attribute	Values	Description
IP_interface	<string> Default: <blank>. The virtual module uses the first interface in the PC for sending IP messages.	Specifies the identity of the device on the PC with the IP interface that the virtual module can use for sending IP messages. Note: This parameter only applies to host-based fax applications using a virtual module. Set the value of this parameter to the name of any device in the PC with an IP interface. If you do not provide a value (blank string), the virtual module chooses the first interface in the PC to send its messages.
media_port_min	1024 - 64535 Default: 56000	Specifies the lowest IP port number that the module can use for media transmissions. Set this value to a value 1000 below the value specified for the media_port_max parameter.
media_port_max	2024 - 65535 Default: 57000	Specifies the highest IP port number that the module can use. Set this value to a value 1000 above the value specified for the media_port_min parameter.
t38_fax_rate_management	localTCF - Indicates that the transport uses the local training check frame (TCF) data rate management type (not supported). transferredTCF - Indicates that the transport uses the transferred training check frame (TCF) data rate management type. (Default)	Specifies a value that identifies the data rate management method of the transport.
t38_fax_udp_ec	t38UDPFEC - The transport uses the T.38 user datagram protocol (UDP) forward error correction (FEC) method (not supported). t38UDPRedundancy - The transport uses the T.38 UDP redundancy error correction method. (Default)	Specifies a value that identifies the error correction method of the T.38 fax transport.

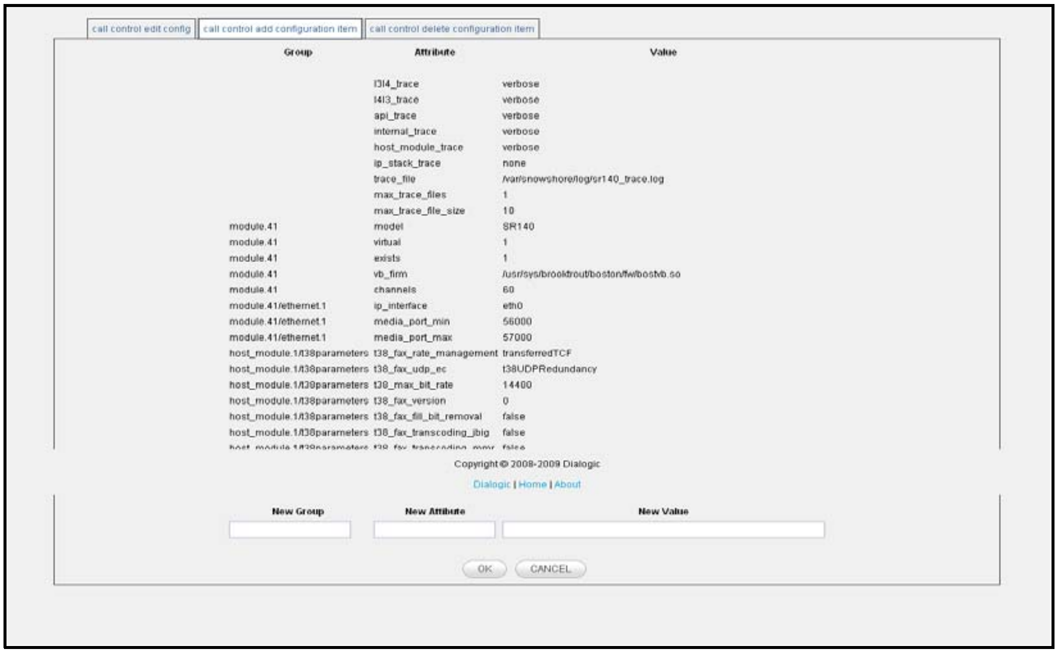
Attribute	Values	Description
T38_max_bit_rate	The following values represent the maximum bit rate that can be negotiated for fax packetization. 2400 4800 7200 9600 12000 14400 - default if T38 Fax Version is 0 or1 16800 19200 21600 24000 26400 28800 31200 33600 - default if T38 Fax Version is 2 or 3	Specifies a value that defines the maximum bit rate for fax packetization onto the network.
t38_fax_version	0, 1, 2, 3 Default: 3	Controls the maximum T.38 ASN.1 version the IP Call Control offers or accepts from a remote party. Versions 0, 1, 2 support a maximum bit rate of 14,400 bps. Version 3 supports V.34 and the following are the possible bit rates: 33,600 (default), 31,200, 28,800, 26,400, 24,000, 21,600, 16,800
t38_fax_fill_bit_removal	FALSE Indicates that the API does not support the capability. TRUE Indicates that the API can remove or insert fill bits.	Specifies whether the API can remove or insert fill bits to reduce the bandwidth of the transport mechanism. Note: This parameter does not affect the normal T.30-level capability to remove or insert fill bits.
t38_fax_transcoding_jbig	FALSE - Indicates that the API does not support the capability. (Default) TRUE - Indicates that the API can convert JBIG fax images.	Specifies whether the API can convert to and from JBIG fax images to reduce the bandwidth of the transport mechanism when using a reliable transport (for example, TCP).

Attribute	Values	Description
t38_fax_transcoding_MMR	FALSE Indicates that the API does not support the capability. (Default) TRUE Indicates that the API can convert MMR compression.	Specifies whether the API can convert to and from MMR fax compression to reduce the bandwidth of the transport mechanism when using a reliable transport (for example, TCP). Note: This parameter does not affect the normal T.30-level capability to use MMR if the two endpoints select MMR as a line compression format.
t38_fax_max_datagram	72	Maximum datagram for receive
t38_fax_max_buffer	200	Maximum fax buffer

Adding Call Control Attributes

Follow the steps below to add new Call Control attributes.

1 Select Fax→ Call Control and click the call control add configuration item tab. The following page appears.



call control edit config
call control add configuration item
call control delete configuration item

Group	Attribute	Value
	l3l4_trace	verbose
	l4l3_trace	verbose
	api_trace	verbose
	internal_trace	verbose
	host_module_trace	verbose
	ip_stack_trace	none
	trace_file	/var/snowshore/log/sr140_trace.log
	max_trace_files	1
	max_trace_file_size	10
module.41	model	SR140
module.41	virtual	1
module.41	exists	1
module.41	vb_firm	/usr/sys/brooktrout/boston/fw/bostvb.so
module.41	channels	60
module.41/ethernet.1	ip_interface	eth0
module.41/ethernet.1	media_port_min	56000
module.41/ethernet.1	media_port_max	57000
host_module.1/t38parameters	t38_fax_rate_management	transferredTCF
host_module.1/t38parameters	t38_fax_udp_ec	t38UDPRedundancy
host_module.1/t38parameters	t38_max_bit_rate	14400
host_module.1/t38parameters	t38_fax_version	0
host_module.1/t38parameters	t38_fax_fill_bit_removal	false
host_module.1/t38parameters	t38_fax_transcoding_jbig	false
host_module.1/t38parameters	t38_fax_transcoding_mmr	false

Copyright © 2008-2009 Dialogic

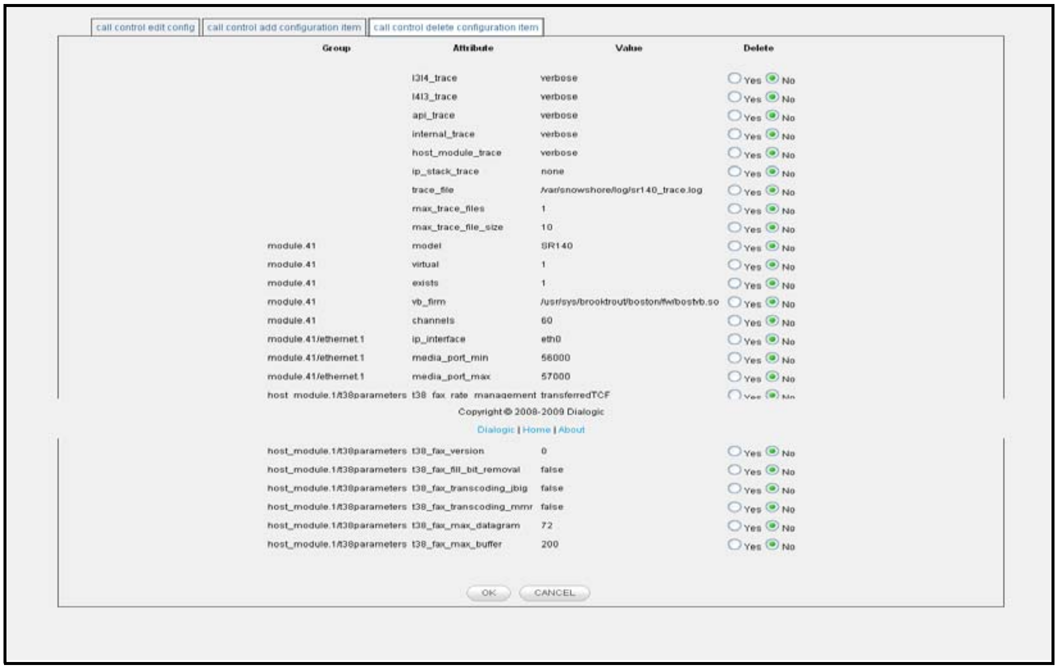
Figure 29. Add Call Control Configuration Item Page

2 At the bottom of the page, complete the New Group, New Attribute, and New Value fields and click OK.

3 Repeat the step above until complete.

Deleting Call Control Attributes

1 Select Fax→ Call Control and click the call control delete configuration item tab. The following page appears.


call control edit config
call control add configuration item
call control delete configuration item
OK
CANCEL

Group	Attribute	Value	Delete
	l3l4_trace	verbose	○ Yes ● No
	l4l3_trace	verbose	○ Yes ● No
	api_trace	verbose	○ Yes ● No
	internal_trace	verbose	○ Yes ● No
	host_module_trace	verbose	○ Yes ● No
	ip_stack_trace	none	○ Yes ● No
	trace_file	/var/snowshore/log/sr140_trace.log	○ Yes ● No
	max_trace_files	1	○ Yes ● No
	max_trace_file_size	10	○ Yes ● No
module.41	model	SR140	○ Yes ● No
module.41	virtual	1	○ Yes ● No
module.41	exists	1	○ Yes ● No
module.41	vb_firm	/usr/sys/brooktrout/boston/fw/bostvb.so	○ Yes ● No
module.41	channels	60	○ Yes ● No
module.41/ethernet.1	ip_interface	eth0	○ Yes ● No
module.41/ethernet.1	media_port_min	56000	○ Yes ● No
module.41/ethernet.1	media_port_max	57000	○ Yes ● No
host_module.1/t38parameters	t38_fax_rate_management	transferredTCF	○ Yes ● No
host_module.1/t38parameters	t38_fax_version	0	○ Yes ● No
host_module.1/t38parameters	t38_fax_fill_bit_removal	false	○ Yes ● No
host_module.1/t38parameters	t38_fax_transcoding_jbig	false	○ Yes ● No
host_module.1/t38parameters	t38_fax_transcoding_mmr	false	○ Yes ● No
host_module.1/t38parameters	t38_fax_max_datagram	72	○ Yes ● No
host_module.1/t38parameters	t38_fax_max_buffer	200	○ Yes ● No

Copyright © 2008-2009 Dialogic

Dialogic | Home | About

Figure 30. Delete Call Control Configuration Item Page

2 Select Yes next to the attributes that you want to delete.

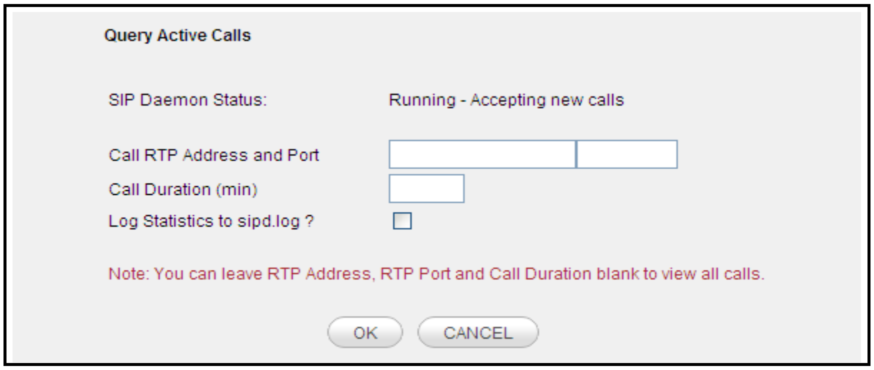
3 Click OK.

Query Active Calls

You can query for currently active calls on the IP Media Server. This enables you to determine if it is safe to change configuration settings.

1 Select Media Server→Query Active Calls from the menu.

The Query Active Calls page is displayed:



Query Active Calls

SIP Daemon Status: Running - Accepting new calls

Call RTP Address and Port

Call Duration (min)

Log Statistics to sipd.log ? □

Note: You can leave RTP Address, RTP Port and Call Duration blank to view all calls.

Figure 31. Query Active Calls Page

2 Enter the call RTP address and RTP port.

3 Enter the call duration. The IP Media Server returns all calls that have existed at least as long as the duration value (that is, all calls with times equal to or greater than the specified Duration).

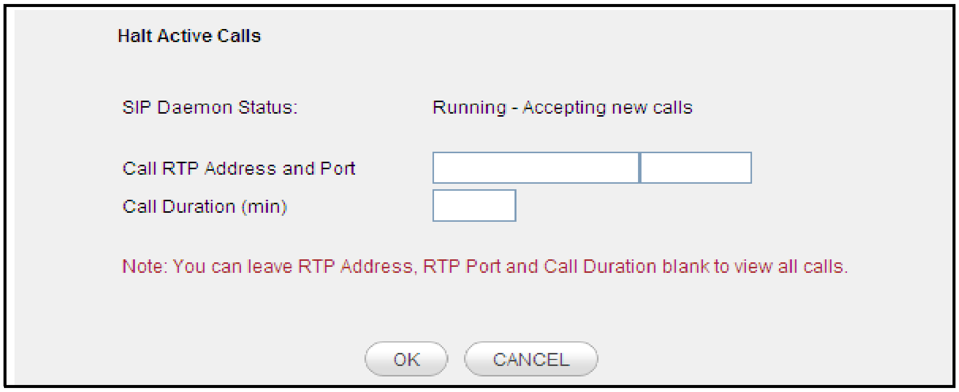
Note: To view all calls, leave the RTP Address, RTP Port, and Call Duration fields blank.

4 Click OK to get the results of the query.

Halt Active Calls

You can selectively stop currently active calls on the IP Media Server at any time. To halt active calls on the IP Media Server:

1 Select Media Server→Halt Active Calls from the menu to display the Halt Active Calls page:



Halt Active Calls

SIP Daemon Status: Running - Accepting new calls

Call RTP Address and Port

Call Duration (min)

Note: You can leave RTP Address, RTP Port and Call Duration blank to view all calls.

Figure 32. Halt Active Calls Page

2 Enter the call RTP address and RTP port.

3 Enter the call duration.

Note: To view all calls, leave the RTP Address, RTP Port, and Call Duration fields blank.

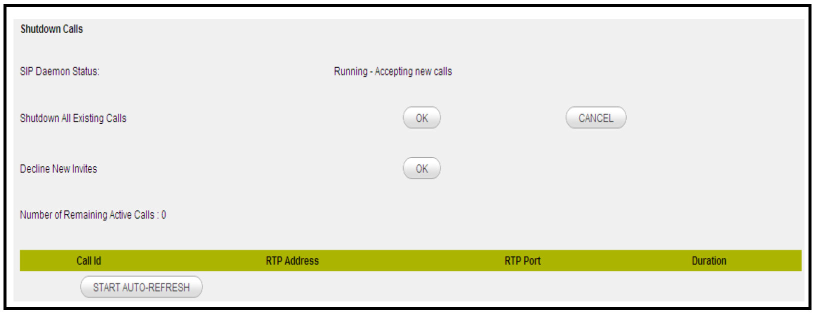
4 Click OK to get the results of the query.

5 Check the Select box for each call you want to halt and click OK to force the halt. The page re-displays, minus the halted calls.

Shutdown Calls

The Shutdown Calls feature blocks incoming call requests to the IP Media Server. This allows an administrator to reboot the server without losing any incoming calls. The Shutdown Calls page also enables an administrator to shutdown all existing calls.

Select Media Server→Shutdown Calls.



Shutdown Calls

SIP Daemon Status: Running - Accepting new calls

Shutdown All Existing Calls

Decline New Invites

Number of Remaining Active Calls : 0

Call Id	RTP Address	RTP Port	Duration

Figure 33. Shutdown Calls Page

To block new incoming calls, click OK adjacent to Decline New Invites. This causes the IP Media Server to stop accepting new calls. Active calls are not affected by this setting. After the page is refreshed, the option then changes to Accept New Invites, letting you re-enable the server to accept calls.

This page also enables you to shutdown all active calls.

- To selectively shut down calls, use the Halt Active Calls menu option.
- To shut down all calls, click the OK button adjacent to Shutdown All Existing Calls. The IP Media Server sends SIP BYE requests to terminate any existing calls.

5 - Operations, Administration, and Maintenance

This chapter describes procedures for operating, administering, and maintaining the Dialogic® IP Media Server using the Web User Interface (Web UI).

This chapter includes the following sections:

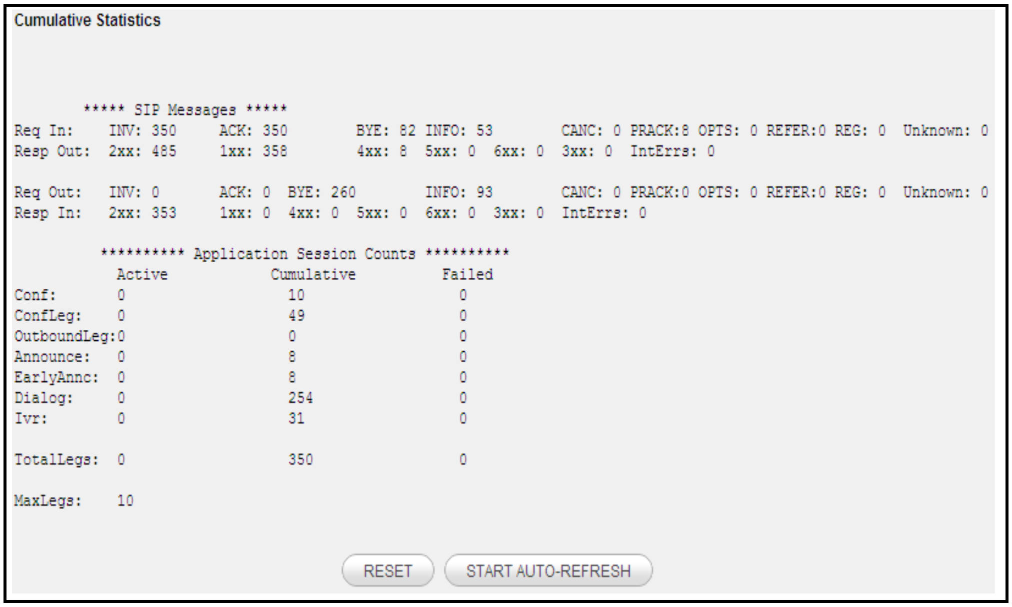
Dialogic® IP Media Server Statistics

The IP Media Server collects statistics associated with SIP messages and call attempts. It also gathers statistics on the server hardware.

Cumulative Statistics

To access the SIP message statistics:

1 Select **Statistics→Cumulative**. The number of SIP messages received and sent is shown.



Cumulative Statistics

```
        ***** SIP Messages *****
Req In:    INV: 350     ACK: 350        BYE: 82 INFO: 53        CANC: 0 PRACK:8 OPTS: 0 REFER:0 REG: 0  Unknown: 0
Resp Out:  2xx: 485     1xx: 358        4xx: 8  5xx: 0  6xx: 0  3xx: 0  IntErrs: 0

Req Out:   INV: 0       ACK: 0  BYE: 260        INFO: 93        CANC: 0 PRACK:0 OPTS: 0 REFER:0 REG: 0  Unknown: 0
Resp In:   2xx: 353     1xx: 0  4xx: 0  5xx: 0  6xx: 0  3xx: 0  IntErrs: 0

          ********** Application Session Counts **********
            Active            Cumulative          Failed
Conf:       0                   10                  0
ConfLeg:    0                   49                  0
OutboundLeg:0                   0                   0
Announce:   0                   8                   0
EarlyAnnc:  0                   8                   0
Dialog:     0                   254                 0
Ivr:        0                   31                  0

TotalLegs:  0                   350                 0

MaxLegs:    10
```

Figure 34. Cumulative Statistics Page

The IP Media Server also keeps statistics of call attempts for the supported application services. For each application service type, the statistics show:

- Active Calls – The number of currently active calls for each application service type.
- Cumulative Calls – The total number of call attempts for each application service type since the last reset of the statistics.
- Failed Calls – The total number of failed call attempts for each application service type since the last reset of the statistics.

The screen displays the total number of calls (Active, Cumulative, Failed) since the last reset of the statistics. This is shown at the bottom of the statistics screen and is labeled **TotalLegs**.

Note: The total does not include the **Conf** row, but does include the **ConfLeg** row. The **Conf** number is the number of unique conferences, not the number of calls in the conference.

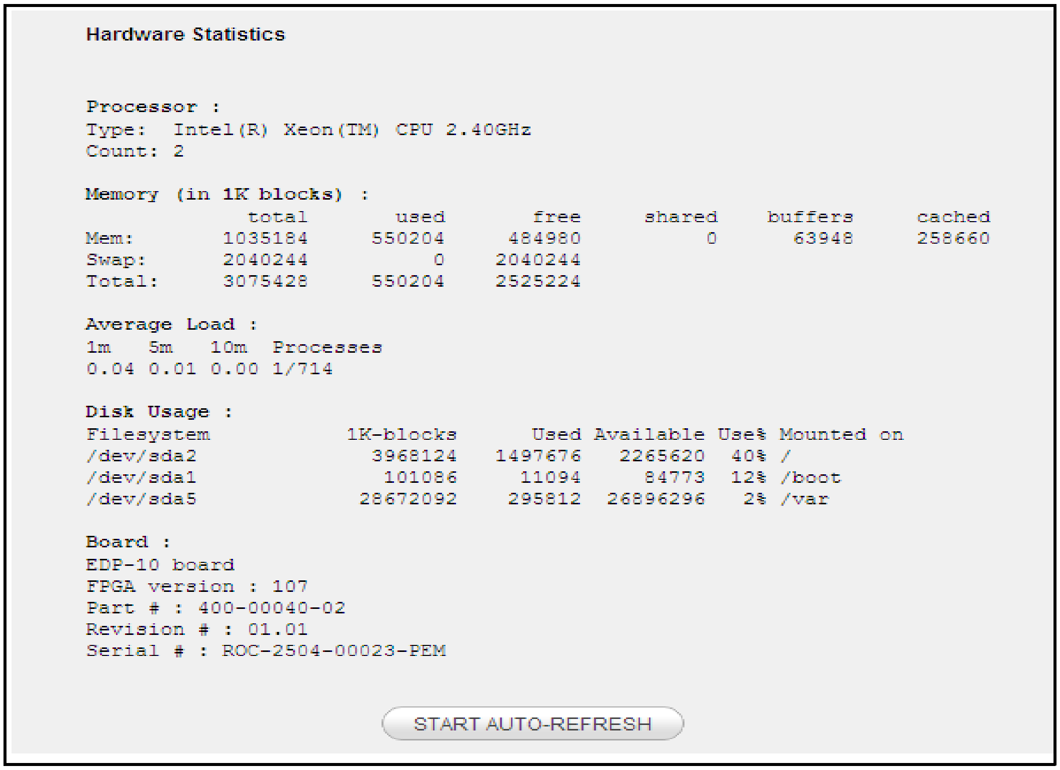
A high-water mark counter is found under the **TotalLegs** line and is called **MaxLegs**. This shows the highest number of simultaneously active calls on the IP Media Server since the last reset of the statistics.

2 To set the statistics to 0, click **RESET**.

Hardware Statistics

To access the hardware statistics, select **Statistics →Hardware** to display the Hardware Statistics page. This page reflects the current status of the IP Media Server hardware. The hardware statistics include processor information, memory, average load of the system, and disk usage of the system.

The only option on this page is to stop/start the auto refresh. To use this feature, click **Stop Auto-Refresh** to stop the page from automatically refreshing. To restart auto-refresh, click **Start Auto-Refresh**.



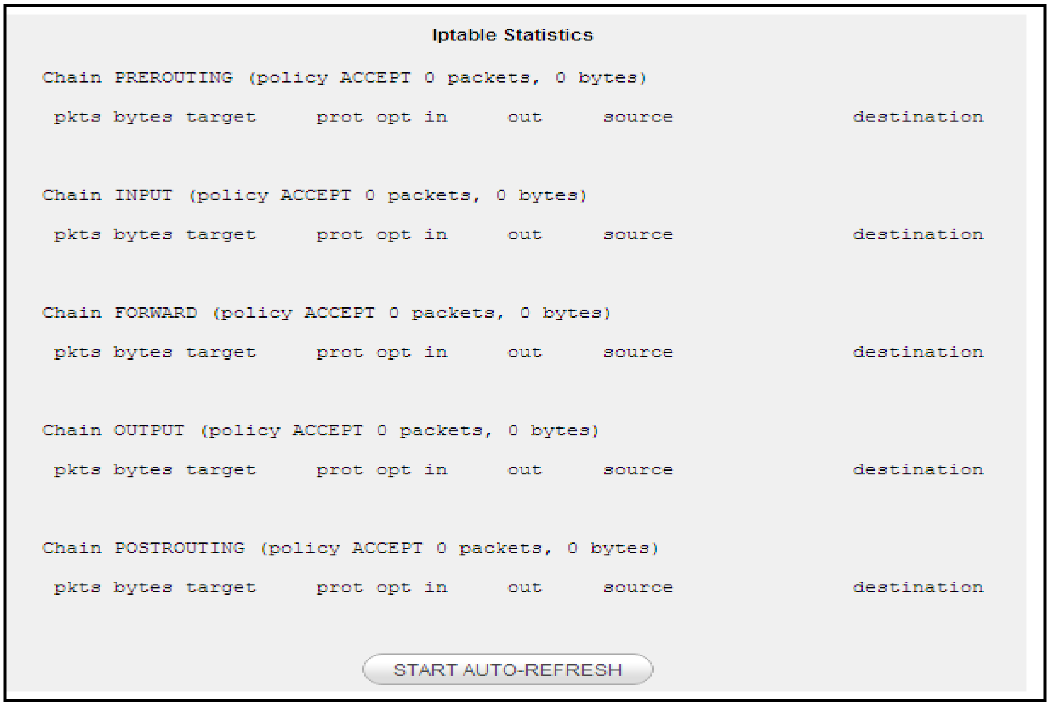
Hardware Statistics

```
Processor :
Type:  Intel(R) Xeon(TM) CPU 2.40GHz
Count: 2

Memory (in 1K blocks) :
             total       used       free     shared    buffers     cached
Mem:       1035184     550204     484980          0      63948     258660
Swap:      2040244          0    2040244
Total:     3075428     550204    2525224

Average Load :
1m   5m   10m  Processes
0.04 0.01 0.00 1/714

Disk Usage :
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/sda2              3968124   1497676   2265620  40% /
/dev/sda1               101086     11094     84773  12% /boot
/dev/sda5             28672092    295812  26896296   2% /var

Board :
EDP-10 board
FPGA version : 107
Part # : 400-00040-02
Revision # : 01.01
Serial # : ROC-2504-00023-PEM
```

Figure 35. Hardware Statistics Page

IP Tables Statistics

To displays statistics for the IP Tables, select **Statistics → Ip tables**. IP Tables are used to tag specific outgoing VoIP traffic.



```
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Figure 36. IP Table Statistics Page

The following are key points from these statistics:

- The line below indicates to set the TOS (Type of Service) bit for all UDP traffic on eth0 where the destination port is 5060 (SIP) to be Minimum delay.

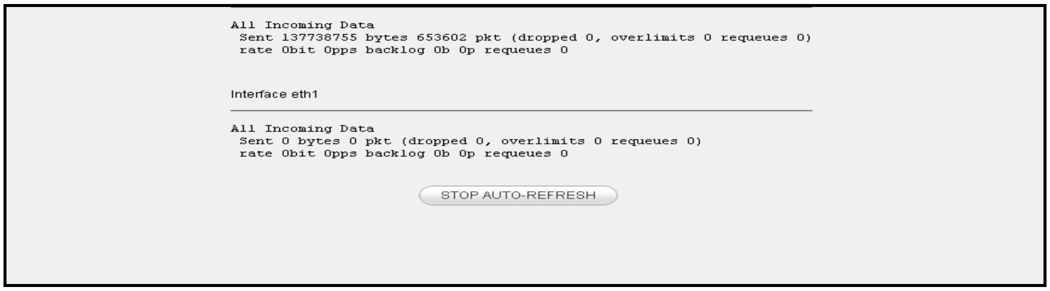
```
0 0 TOS udp -- any eth0 anywhere anywhere udp dpt:5060 TOS set Minimize-Delay
```

- The next line indicates to log this information.

```
0 0 LOG udp -- any eth0 anywhere anywhere udp dpt:5060 LOG level warning prefix
```

Traffic Control Statistics

To display statistics for the Traffic Control, select **Statistics → Traffic Control**. Traffic Control application allows the IP Media Server to prioritize incoming traffic.



```
All Incoming Data
 Sent 137738755 bytes 653602 pkt (dropped 0, overlimits 0 requeues 0)
 rate 0bit 0pps backlog 0b 0p requeues 0

Interface eth1

All Incoming Data
 Sent 0 bytes 0 pkt (dropped 0, overlimits 0 requeues 0)
 rate 0bit 0pps backlog 0b 0p requeues 0
```

Figure 37. Traffic Control Statistics Page

The following are key points from these statistics:

- This line is all the traffic seen on eth0:

```
qdisc prio 1: bands 2 priomap 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
```

- “Sent” means allowed or passed or seen:

```
Sent 5578871 bytes 27740 pkts (dropped 0, overlimits 0 requeues 0)
```

- This line is the filter for VOIP traffic incoming:

```
qdisc pfifo 11: parent 1:1 limit 1000p
```

- All traffic in this case was VOIP and was passed on up:

```
Sent 5533101 bytes 27477 pkts (dropped 0, overlimits 0 requeues 0)
```

- The following line is all non-VOIP traffic:

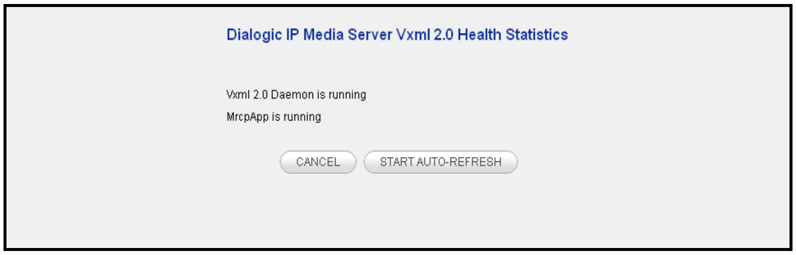
```
qdisc pfifo 12: parent 1:2 limit 1000p
```

- This traffic took the slow path in the IP Media Server as it is not as important

```
Sent 45770 bytes 263 pkts (dropped 0, overlimits 0 requeues 0)
```

VXML 2.0 Health Statistics

To display system health information for VXML 2.0, select **Statistics →VXML Health**. This information can be useful for troubleshooting a VXML 2.0 configuration or application issue.



Dialogic IP Media Server Vxml 2.0 Health Statistics

Vxml 2.0 Daemon is running

MrcpApp is running

Figure 38. VXML 2.0 Health Statistics Page

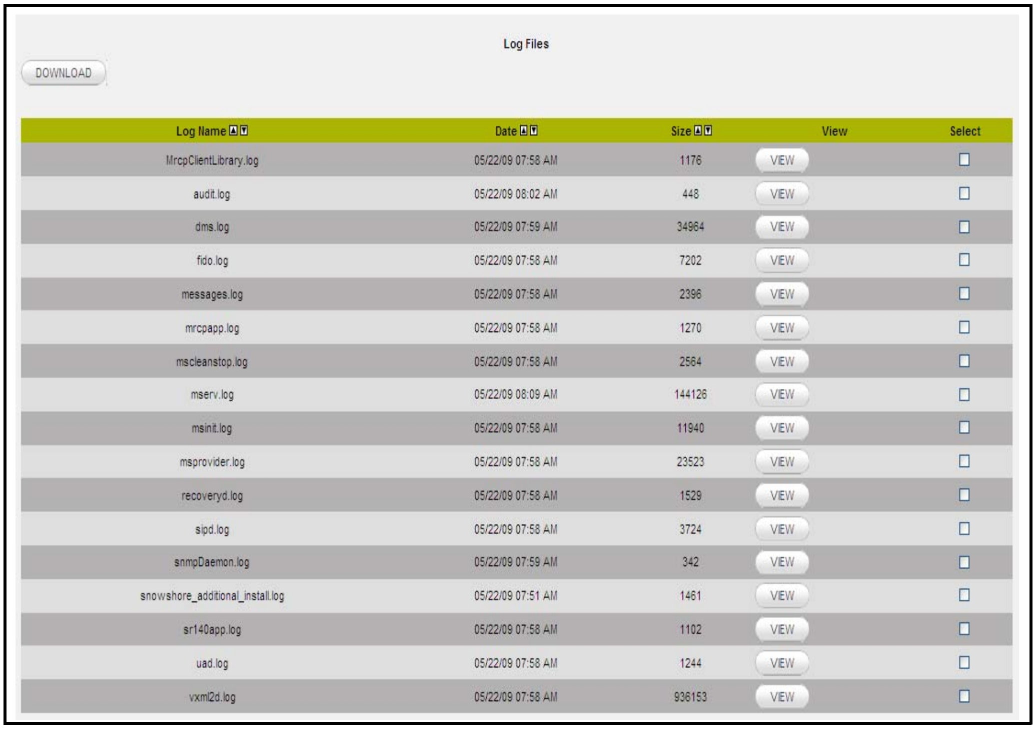
Logs Menu

The Logs menu provides commands for configuring logs, and viewing log files, core files, and trace files.

Log Files

The IP Media Server produces several log files.

To view or download log files generated by the IP Media Server, select **Logs→Log Files**. The Log Files page displays the available log files and the date/time they were last modified. For a list and description of log files, see "Checking Log Files" (page 138).



Log Files

Log Name ▲▼	Date ▲▼	Size ▲▼	View	Select
MrcpClientLibrary.log	05/22/09 07:58 AM	1176	VIEW	□
audit.log	05/22/09 08:02 AM	448	VIEW	□
dms.log	05/22/09 07:59 AM	34964	VIEW	□
fido.log	05/22/09 07:58 AM	7202	VIEW	□
messages.log	05/22/09 07:58 AM	2396	VIEW	□
mrcpapp.log	05/22/09 07:58 AM	1270	VIEW	□
mscleanstop.log	05/22/09 07:58 AM	2564	VIEW	□
mserv.log	05/22/09 08:09 AM	144126	VIEW	□
msinit.log	05/22/09 07:58 AM	11940	VIEW	□
msprovider.log	05/22/09 07:58 AM	23523	VIEW	□
recoveryd.log	05/22/09 07:58 AM	1529	VIEW	□
sipd.log	05/22/09 07:58 AM	3724	VIEW	□
snmpDaemon.log	05/22/09 07:59 AM	342	VIEW	□
snowshore_additional_install.log	05/22/09 07:51 AM	1461	VIEW	□
sr140app.log	05/22/09 07:58 AM	1102	VIEW	□
uad.log	05/22/09 07:58 AM	1244	VIEW	□
vxml2d.log	05/22/09 07:58 AM	936153	VIEW	□

Figure 39. Log Files Page

Downloading a Log File

To **download** a file from the Log Files page:

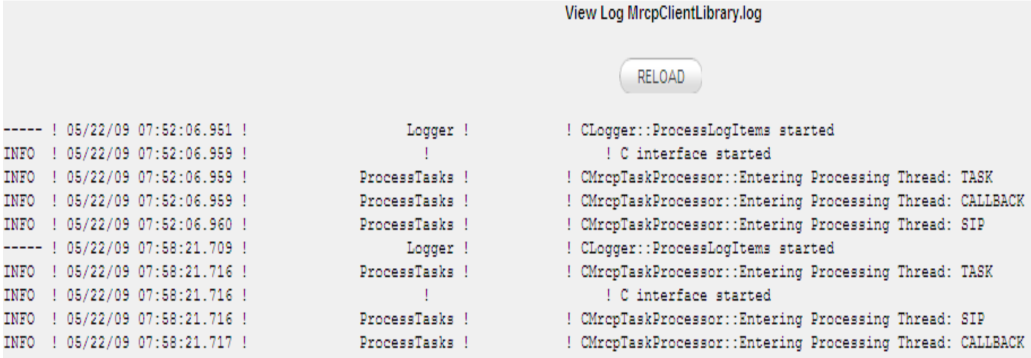
1. Select **Logs→Log Files** from the Web UI.
2. Click the checkbox for each file you want to download.
3. Click **DOWNLOAD** at the top of the page. The selected files are compressed into a ZIP file and the **File Download** dialog appears with the name of the ZIP file.
4. Select the preferred action from the **File Download** dialog:
   - Open – Displays a window to enable you to manipulate the log files.

- Save – Displays a window to enable you to select a location to save the log file.

Viewing a Log File

To **view** a log file from the Log Files page:

1. Select **Logs→Log Files** from the Web UI.
2. Click the **VIEW** button for the file you want to view. The log file is displayed.



View Log MrcpClientLibrary.log

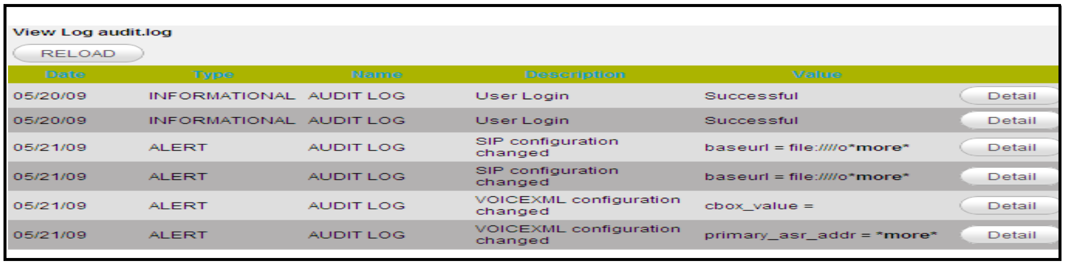
```
----- ! 05/22/09 07:52:06.951 !             Logger !        ! CLogger::ProcessLogItems started
INFO  ! 05/22/09 07:52:06.959 !                    !            ! C interface started
INFO  ! 05/22/09 07:52:06.959 !       ProcessTasks !        ! CMrcpTaskProcessor::Entering Processing Thread: TASK
INFO  ! 05/22/09 07:52:06.959 !       ProcessTasks !        ! CMrcpTaskProcessor::Entering Processing Thread: CALLBACK
INFO  ! 05/22/09 07:52:06.960 !       ProcessTasks !        ! CMrcpTaskProcessor::Entering Processing Thread: SIP
----- ! 05/22/09 07:58:21.709 !             Logger !        ! CLogger::ProcessLogItems started
INFO  ! 05/22/09 07:58:21.716 !       ProcessTasks !        ! CMrcpTaskProcessor::Entering Processing Thread: TASK
INFO  ! 05/22/09 07:58:21.716 !                    !            ! C interface started
INFO  ! 05/22/09 07:58:21.716 !       ProcessTasks !        ! CMrcpTaskProcessor::Entering Processing Thread: SIP
INFO  ! 05/22/09 07:58:21.717 !       ProcessTasks !        ! CMrcpTaskProcessor::Entering Processing Thread: CALLBACK
```

Figure 40. View Log File Page

Viewing an Audit Log File

To **view** an audit log from the Log Files page:

1. Select **Logs→Log Files** from the Web UI.
2. Click the **VIEW** button for audit.log file. This file has a special table view.

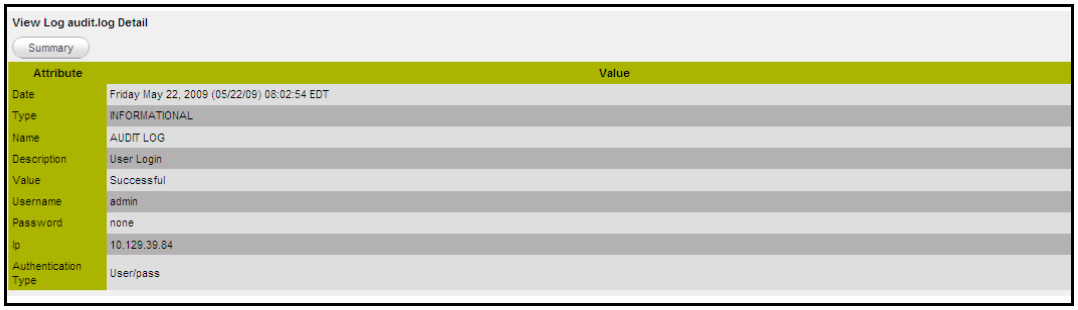


View Log audit.log

Date	Type	Name	Description	Value	
05/20/09	INFORMATIONAL	AUDIT LOG	User Login	Successful	Detail
05/20/09	INFORMATIONAL	AUDIT LOG	User Login	Successful	Detail
05/21/09	ALERT	AUDIT LOG	SIP configuration changed	baseurl = file:////o*more*	Detail
05/21/09	ALERT	AUDIT LOG	SIP configuration changed	baseurl = file:////o*more*	Detail
05/21/09	ALERT	AUDIT LOG	VOICEXML configuration changed	cbox_value =	Detail
05/21/09	ALERT	AUDIT LOG	VOICEXML configuration changed	primary_asr_addr = *more*	Detail

Figure 41. View Audit Log Page

3. To view the details of an entry, click the **DETAIL** button for that entry.



View Log audit.log Detail

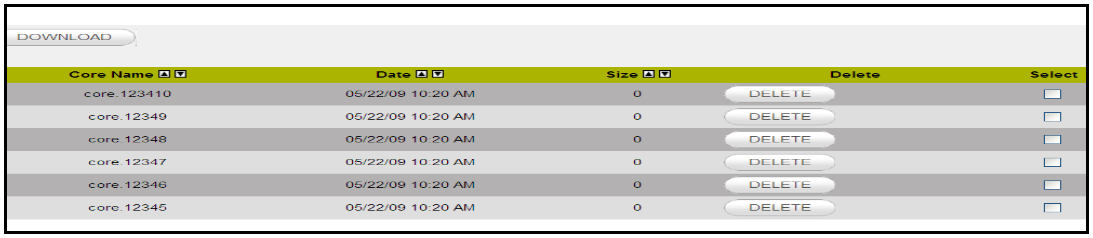
Attribute	Value
Date	Friday May 22, 2009 (05/22/09) 08:02:54 EDT
Type	INFORMATIONAL
Name	AUDIT LOG
Description	User Login
Value	Successful
Username	admin
Password	none
Ip	10.129.39.84
Authentication Type	User/pass

Figure 42. Audit Log Detail Page

4 To search for a particular word or character string, use the browser Find command.

Core Files

To download core files generated by the IP Media Server, select **Logs→Core Files**. Core files appear in this view when a failure has occurred. The core files contain a memory image of the terminated process. These files are useful in debugging.

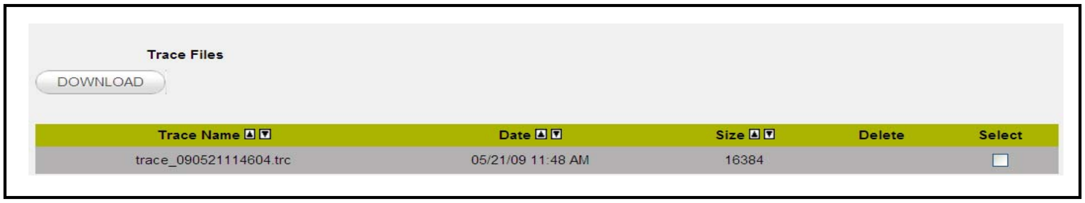


Core Name ▲▼	Date ▲▼	Size ▲▼	Delete	Select
core.123410	05/22/09 10:20 AM	0	DELETE	□
core.12349	05/22/09 10:20 AM	0	DELETE	□
core.12348	05/22/09 10:20 AM	0	DELETE	□
core.12347	05/22/09 10:20 AM	0	DELETE	□
core.12346	05/22/09 10:20 AM	0	DELETE	□
core.12345	05/22/09 10:20 AM	0	DELETE	□

Figure 43. Core Files Page

Trace Files

To download trace files generated by the IP Media Server, select **Logs→Trace Files**. This page lists the output files from the trace feature on the IP Media Server (**Networks → Utilities → Trace**). These files can be opened using network analyzer software.



Trace Files

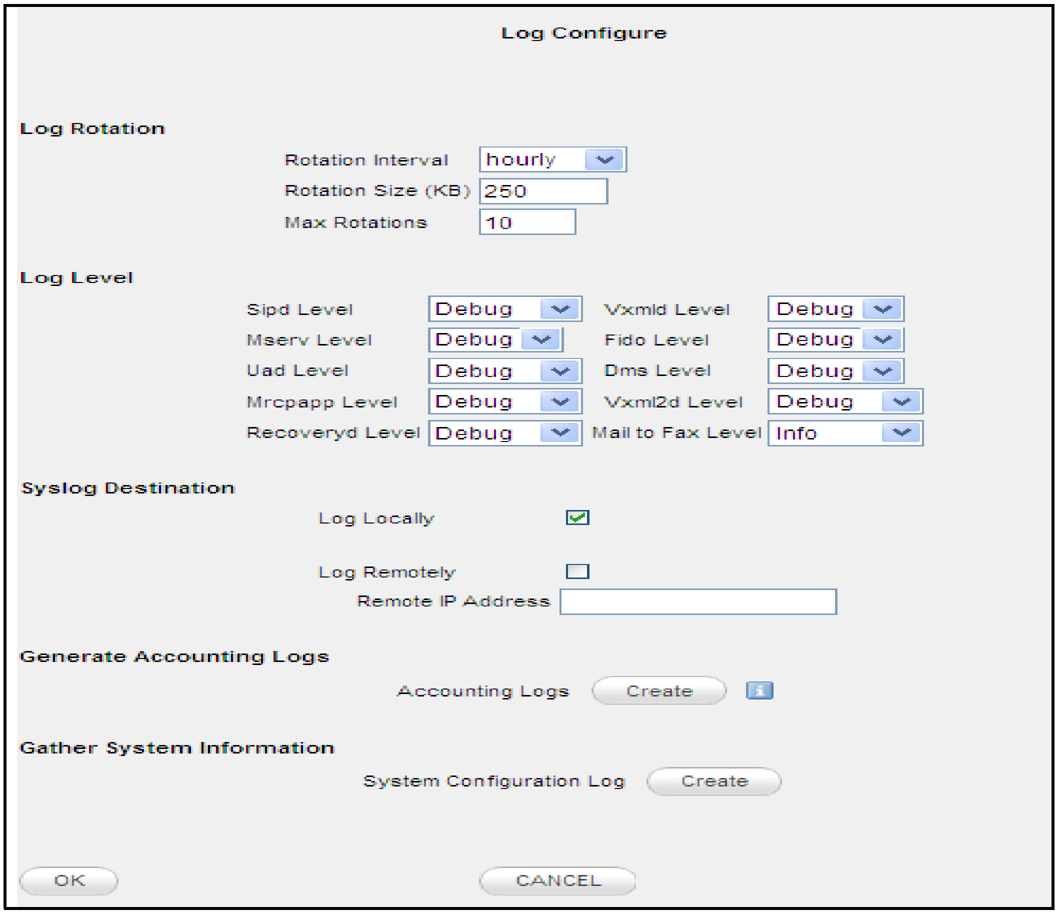
Trace Name ▲▼	Date ▲▼	Size ▲▼	Delete	Select
trace_090521114604.trc	05/21/09 11:48 AM	16384		□

Figure 44. Trace Files Page

Configure Logs

The log system is controlled by a set of parameters you configure from the **Logs→Configure** menu.

Note: Only Administrators can configure the log system.



Log Configure

Log Rotation

Rotation Interval: hourly

Rotation Size (KB): 250

Max Rotations: 10

Log Level

Sipd Level	Debug	Vxmld Level	Debug
Mserv Level	Debug	Fido Level	Debug
Uad Level	Debug	Dms Level	Debug
Mrcpapp Level	Debug	Vxml2d Level	Debug
Recoveryd Level	Debug	Mail to Fax Level	Info

Syslog Destination

Log Locally ☑

Log Remotely □

Remote IP Address

Generate Accounting Logs

Accounting Logs

Gather System Information

System Configuration Log

Figure 45. Configure Logs Page

Log Rotation

The Log Rotation section of the Configure Logs page enables you to configure parameters related to log rotation intervals, size, and maximum rotation.

Note: If you change the log rotation values from the defaults, do not exceed file sizes of 2GB or available disk storage space.

Table 11. Log Rotation Parameters

Parameter	Values	Description
Rotation Interval	◆ Monthly ◆ Weekly ◆ Daily ◆ Hourly ◆ 30 minutes ◆ 15 minutes (Default: Hourly)	Interval at which the log files are checked for rotation. The interval can be: ◆ Monthly (at 4:42 AM, the first day of the month) ◆ Weekly (at 4:22 AM, first day of the week) ◆ Daily (at 4:02 AM) ◆ Hourly (at the top of the hour) ◆ 30 minutes ◆ 15 minutes
Rotation Size	integer: 1–250,000 (Default: 250)	Minimum size (in kilobytes) that a log file must be to be rotated at the next rotation interval. **Note:** Logs are rotated based on their size when they are checked. If you want the logs to be rotated at the interval chosen, make the rotation size small. **Caution:** Specifying a large rotation size creates very large log files which take longer to view and download. For maximum system efficiency, set rotation sizes to less than 50,000 KB.
Max Rotations	integer: 1–240 (Default: 10)	Number of rotations allowed for each log file. This determines how many log files are kept on the system before they are deleted.

Note: The log configuration parameters do not apply to the VXML 2.0 logs. These logs are preconfigured to have a maximum rotation size of 10MB and a maximum of 5 rotations.

Log Level

The Log Level section of the Configure Logs page enables you to configure the level of detail to be included in each log. Select the level of detail to record for each log from the drop-down list.

Table 12. Log Level Parameters

Level	Log Contents
Debug	All messages associated with a process. A log event that denotes information that is only required for component-level debugging.
Info	Informative messages regarding a process.
Warning	All warning messages about normal events associated with a process.
Error	All errors encountered by a process.
Critical	All critical messages generated by a process.
Fatal	Fatal messages associated with a process that denote an error condition that should never happen and that results in the loss of functionality.
None	No information is logged.

Syslog Destination

The Syslog Destination section of the Configure Logs page determines where syslog information will be saved.

Table 13. Syslog Destination Parameters

Parameter	Description
Log Locally	Logs the syslog information to the message.log file on the IP Media Server.
Log Remotely	Logs the syslog information to a remote system. Enter the IP address of the remote system in the **Remote IP Address** field.

Generate Accounting Logs

In the Generate Accounting Logs section of the Configure Logs page, the **Create** button creates the accounting.log and the msaccounting.log files.

The accounting.log is the clear xml formatted ascii text file that stores the IP Media Server's Accounting Statistics over time.

The msaccounting.log is the encrypted xml formatted Log file used for debug purposes.

Note: When you upgrade to a new version of IP Media Server, accounting data is removed from your system. If you want to save the accounting data, you can generate accounting logs from the Configure Logs page before upgrading. Select **Logs→Configure** and click **Create** next to Accounting Logs.

Gather System Information

In the Gather System Information section of the Configure Logs page, the **Create** button creates the System Configuration Log for the current system. This information includes system and IP Media Server configuration information. Once you click **Create**, the log file is generated and the Web page is redirected to the log files page. This new log file can be downloaded to aid in debugging software issues.

Log Naming Convention

Logs are configured to rotate based on a size parameter that is set in the **Logs→Configure** command.

The convention for naming log files is <log file name>.log.n where *n* is changed every time a new log file is started. The current log file being used does not have an *n* extension. For example, the following logs might be found on the system:

- sipd.log – the current sip log.
- sipd.log.1 – the most recent sip log that was rotated.
- sipd.log.2 – the next most recent sip log that was rotated.
- sipd.log.*n* – the sip log from *n* rotations ago, where *n* is the number of rotations.

Services Menu

The Services menu provides commands for configuring the SNMP functionality. Under the IP Media Server implementation of SNMP, users can add traps, communities, and users.

Note: Only Administrators have the permissions to configure the SNMP utility.

SNMP Trap Hosts

On the SNMP Trap Hosts page, administrators can add and delete trap hosts for the IP Media Server.

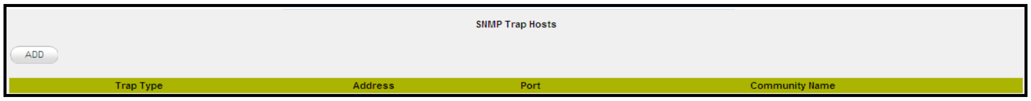


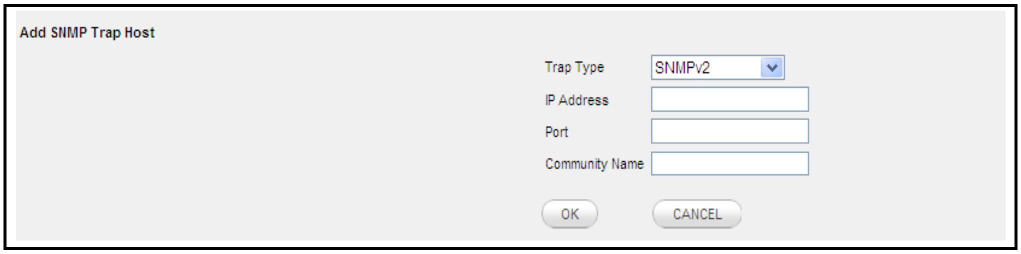
Figure 46. SNMP Trap Hosts Page

To add a new trap host:

1 Select **Services→SNMP Trap Hosts** from the Web UI.

2 Click **ADD**.

The **Add SNMP Trap Host** page appears.


Add SNMP Trap Host

Trap Type: SNMPv2

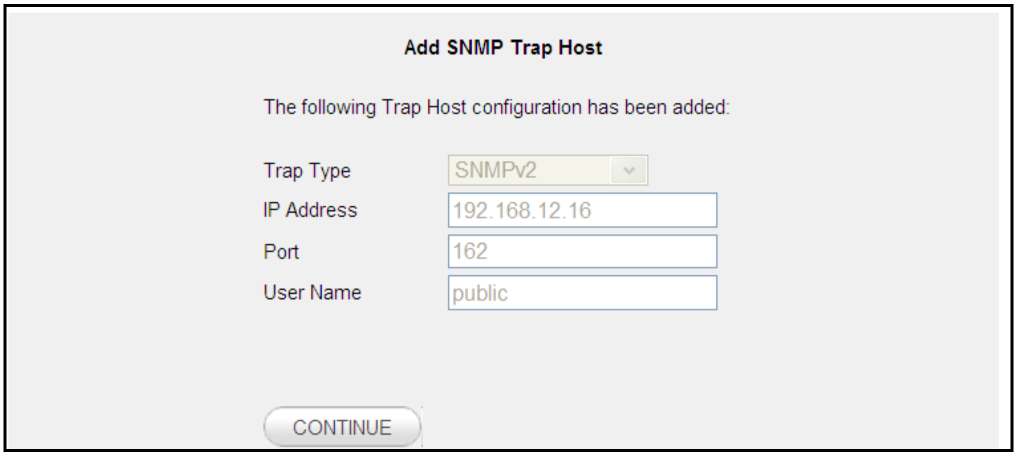
Figure 47. Add SNMP Trap Host Page

3 Select the trap type from the pull-down menu.

4 Enter the IP address.

5 Enter the Port and Community Name. These are optional. If not specified, the Port defaults to 162 and the Community defaults to Public.

6 Click **OK**. The next screen shows the new trap.



Add SNMP Trap Host

The following Trap Host configuration has been added:

Trap Type	SNMPv2
IP Address	192.168.12.16
Port	162
User Name	public

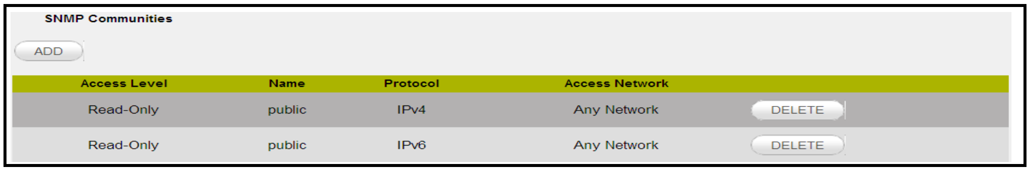
Figure 48. Add SNMP Trap Host Confirmation Page

SNMP Communities

In this page, administrators can add and delete SNMP Communities for the IP Media Server. You can use the SNMP Community Names to manage the System from either an SNMPv1 or SNMPv2c management level.

To add a read/write community:

1 Select **Services→SNMP→Communities** from the Web UI. The SNMP Communities page is displayed.

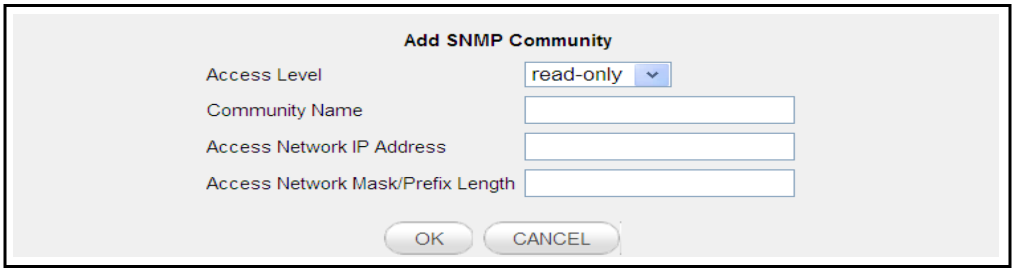


SNMP Communities

Access Level	Name	Protocol	Access Network
Read-Only	public	IPv4	Any Network
Read-Only	public	IPv6	Any Network

Figure 49. SNMP Communities Page

2 Click **ADD** to display the **Add SNMP Community** page.



Add SNMP Community

Access Level: read-only
Community Name:
Access Network IP Address:
Access Network Mask/Prefix Length:

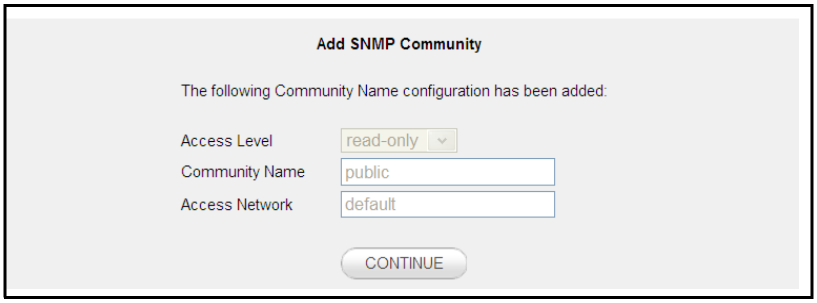
Figure 50. Add SNMP Community Page

3 Choose the access level as read-write.

4 Fill in the Community Name.

5 Leave the Access Network IP address and Access Network Mask fields blank.

6 Click **OK** when you are done. The following confirmation screen appears.



Add SNMP Community

The following Community Name configuration has been added:

Access Level: read-only
Community Name: public
Access Network: default

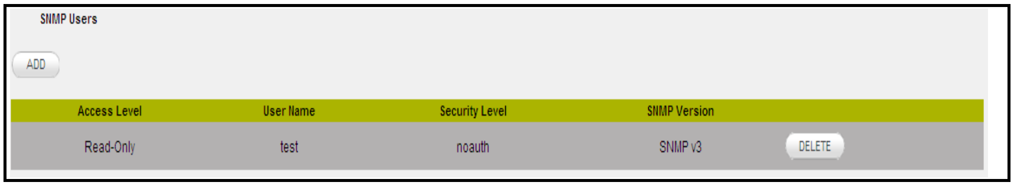
Figure 51. Add SNMP Community Confirmation Page

7 Click **CONTINUE** to return to the SNMP Communities page.

SNMP Users

To add a read/write user:

1 Select the menu option **Services→SNMP→Users** to display the SNMP Users page.

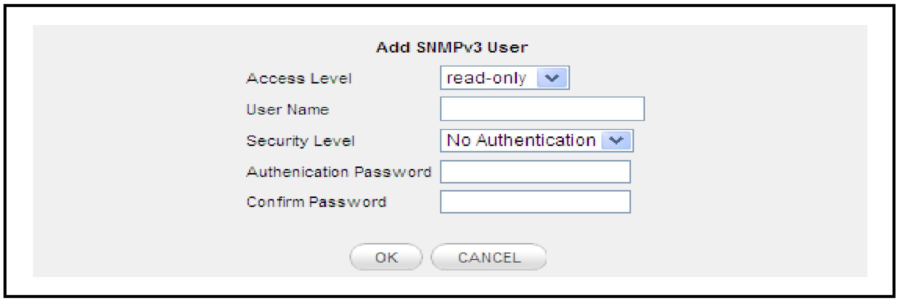


SNMP Users

Access Level	User Name	Security Level	SNMP Version	
Read-Only	test	noauth	SNMP v3	DELETE

Figure 52. SNMP Users Page

2 Click **ADD** to display the ADD SNMP User page.



Add SNMPv3 User

Access Level	read-only
User Name	
Security Level	No Authentication
Authenication Password	
Confirm Password	

Figure 53. Add SNMP User Page

3 Select the access level from the pull-down menu.

The choices are: read-only [default] and read-write.

4 Enter the new user name.

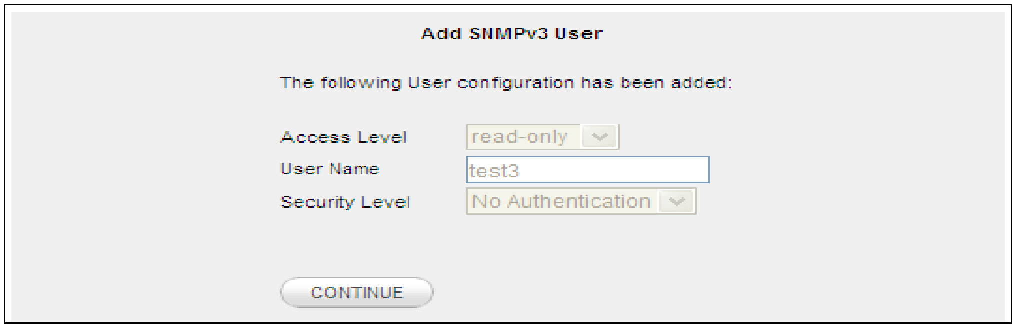
5 Select the security level from the pull-down menu.

The choices are: No Authentication [default] and Authenticated.

6 If the user is authenticated, enter the password and confirm. Leave the password blank if the user is not authenticated.

7 Click **OK** to continue.

The following screen appears to confirm the user changes.



Add SNMPv3 User

The following User configuration has been added:

Access Level read-only

User Name test3

Security Level No Authentication

Figure 54. Add SNMP User Confirmation Page

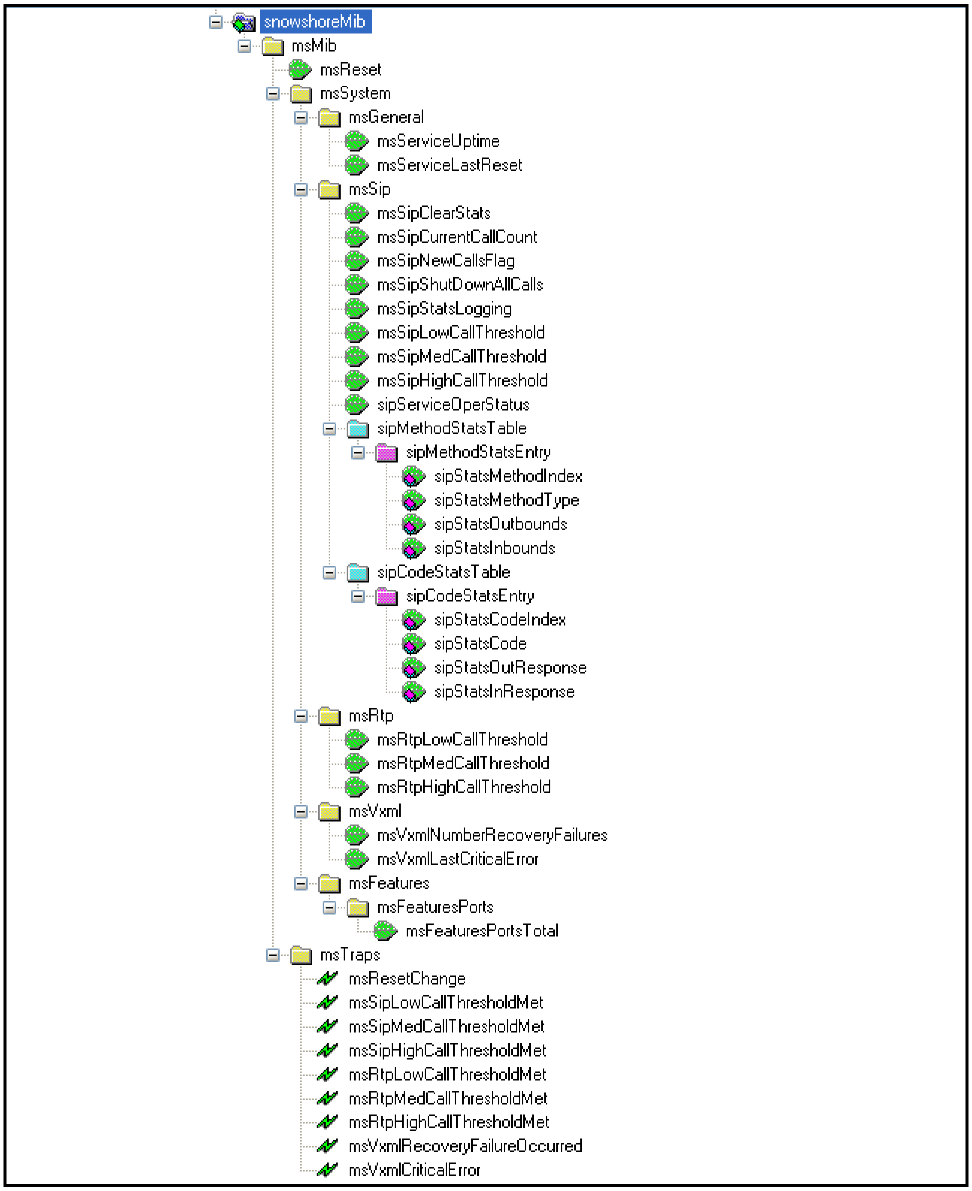
8 Click **CONTINUE** to return to the SNMP Users page.

The Dialogic® IP Media Server Private MIB

The MIB Structure

The MIB (Management Information Base) structure in the IP Media Server is based on Net-SNMP. A private MIB gathers information about the IP Media Server and controls some of the functionality through SNMP. The IP Media Server supports SNMPv1, SNMPv2, and SNMPv3. Note that invalid values used in a set operation will result in an SNMP error.

Figure 55 shows the Dialogic® IP Media Server MIB tree structure.



```
snowshoreMib
  msMib
    msReset
    msSystem
      msGeneral
        msServiceUptime
        msServiceLastReset
      msSip
        msSipClearStats
        msSipCurrentCallCount
        msSipNewCallsFlag
        msSipShutDownAllCalls
        msSipStatsLogging
        msSipLowCallThreshold
        msSipMedCallThreshold
        msSipHighCallThreshold
        sipServiceOperStatus
        sipMethodStatsTable
          sipMethodStatsEntry
            sipStatsMethodIndex
            sipStatsMethodType
            sipStatsOutbounds
            sipStatsInbounds
        sipCodeStatsTable
          sipCodeStatsEntry
            sipStatsCodeIndex
            sipStatsCode
            sipStatsOutResponse
            sipStatsInResponse
      msRtp
        msRtpLowCallThreshold
        msRtpMedCallThreshold
        msRtpHighCallThreshold
      msVxml
        msVxmlNumberRecoveryFailures
        msVxmlLastCriticalError
      msFeatures
        msFeaturesPorts
          msFeaturesPortsTotal
    msTraps
      msResetChange
      msSipLowCallThresholdMet
      msSipMedCallThresholdMet
      msSipHighCallThresholdMet
      msRtpLowCallThresholdMet
      msRtpMedCallThresholdMet
      msRtpHighCallThresholdMet
      msVxmlRecoveryFailureOccurred
      msVxmlCriticalError
```

Figure 55. MIB Tree Structure

MIB Definitions

The MIB Tree Structure Object IDs (OIDs) are described in Table 14:

Table 14. MIB OIDs

MIB	OID	Description
msReset	1.3.6.1.4.1.9234.5.1	Resets the IP Media Server. It supports the get and set operations. The valid set option is 1 (to reset the MS). The subagent resets the IP Media Server by performing an init 3 followed by an init 4, when set to 1. Upon reset, the value is reset to 0. When a get is performed, it always returns a 0.
msServiceUptime	1.3.6.1.4.1.9234.5.2.1.1.0	Time since the IP Media Server services was last re-initialized. It supports the get operation. The time is displayed in the following format: "0 day, 14 hours, 17 minutes". This value is the time the 'get' occurred, minus the time the system was initialized. This is the uptime of the IP Media Server.
msServiceLastReset	1.3.6.1.4.1.9234.5.2.1.2.0	Time since the IP Media Server was last restarted or reset. It supports the get operation. The time is displayed in the following format: “Thu May 12 12:19:23 2005”.
msLastFetchFailureURL	1.3.6.1.4.1.9234.5.2.1.3	The URL of the last file that fails to be fetched.
msLastFetchFailureErrorCode	1.3.6.1.4.1.9234.5.2.1.4	Error code of the last fetch failure.
msLastFetchFailureErrorSting	1.3.6.1.4.1.9234.5.2.1.5	Error description of the last fetch failure.
msSipClearStats	1.3.6.1.4.1.9234.5.2.2.1.0	Clears the SIP statistics. It supports the get and set operations. The possible value for this to be set to is 1.
msSipCurrentCallCount	1.3.6.1.4.1.9234.5.2.2.2.0	Number of active calls. It only supports the get operation.
msSipNewCallsFlag	1.3.6.1.4.1.9234.5.2.2.3.0	Stops or enables calls on the IP Media Server. It supports the get and set operations. The possible values for this to be set to are 1 and 0.
msSipShutdownAllCalls	1.3.6.1.4.1.9234.5.2.2.4.0	Stops all calls on the IP Media Server. It supports the get and set actions. The possible value for this to be set to is 1.
msSipStatsLogging	1.3.6.1.4.1.9234.5.2.2.5.0	Stops or starts SIP stats logging on the IP Media Server. It supports the get and set operations. The possible values for this to be set to are 1 or 0. When this is set to 1, it turns on logging. If this is set to 0, this turns off logging.

Table 14. MIB OIDs (Continued)

MIB	OID	Description
msSipLowCallThreshold	1.3.6.1.4.1.9234.5.2.2.6.0	Number of calls versus the maximum number of calls allowed. It supports the get and set operations. Its value is a percentage, and specifies the lower boundary. Valid values for the set operation range from 1 to 100. When the current call percentage exceeds this threshold, the msSipLowCallThreshold trap is sent. The current call volume (as a percent of the current call load verses the total licenses available) is compared to this threshold. This comparison is made every 30 seconds. When setting this value, use the following format: LowThreshold < MedThreshold < HighThreshold
msSipMedCallThreshold	1.3.6.1.4.1.9234.5.2.2.7.0	Number of calls versus the maximum number of calls allowed. It supports the get and set operations. Its value is a percentage, and specifies the medium boundary. Valid values for the set operation range from 1 to 100. When the current call percentage exceeds this threshold, the msSipMedCallThreshold trap is sent. The current call volume (as a percent of the current call load verses the total licenses available) is compared to this threshold. This comparison is made every 30 seconds. When setting this value use the following format: LowThreshold < MedThreshold < HighThreshold
msSipHighCallThreshold	1.3.6.1.4.1.9234.5.2.2.8.0	Number of calls versus the maximum number of calls allowed. It supports the get and set operations. Its value is a percentage, and specifies the upper boundary. Valid values for the set operation range from 1 to 100. When the current call percentage exceeds this threshold, the msSipHighCallThreshold trap is sent. The current call volume (as a percent of the current call load verses the total licenses available) is compared to this threshold. This comparison is made every 30 seconds. When setting this value use the following format: LowThreshold < MedThreshold < HighThreshold

Table 14. MIB OIDs (Continued)

MIB	OID	Description
sipServiceOperStatus	1.3.6.1.4.1.9234.5.2.2.9.0	Current health status of the sipd process. The possible values for this OID are: ◆ up The application is operating normally, and is processing (receiving and possibly issuing) SIP requests and responses. ◆ down The application is currently unable to process SIP messages. ◆ quiescing The application is currently operational, but has been administratively put into quiescent mode. Additional inbound transactions are rejected. This data is updated every 30 seconds.
sipMethodStatsTable sipMethodStatsEntry sipStatsMethodIndex sipStatsMethodType sipStatsOutbounds sipStatsInbounds	1.3.6.1.4.1.9234.5.2.2.10 1.3.6.1.4.1.9234.5.2.2.10.1.1 1.3.6.1.4.1.9234.5.2.2.10.1.1.0 1.3.6.1.4.1.9234.5.2.2.10.1.2.0 1.3.6.1.4.1.9234.5.2.2.10.1.3.0 1.3.6.1.4.1.9234.5.2.2.10.1.4.0	This table is indexed by sipStatsMethodIndex and sipStatsMethodType. This supports the get operation. This table is updated every 30 seconds.
"Req in" and "Req out" statistics for the following methods (INV, ACK, BYE, INFO, CANC, PRACK, OPTS, REFER, REG, Unknown) are packed in a table. For example: sipStatsMethodIndexsipStatsMethodTypesipOutResponsesipInResponse 1INV20 2ACK02		
sipCodeStatsTable sipCodeStatsEntry sipStatsCodeIndex sipStatsCode sipStatsOutResponse sipStatsInResponse	1.3.6.1.4.1.9234.5.2.2.11 1.3.6.1.4.1.9234.5.2.2.11.1.1 1.3.6.1.4.1.9234.5.2.2.11.1.1.0 1.3.6.1.4.1.9234.5.2.2.11.1.2.0 1.3.6.1.4.1.9234.5.2.2.11.1.3.0 1.3.6.1.4.1.9234.5.2.2.11.1.4.0	This table is indexed by sipStatsCodeIndex and sipStatsCode. This supports the get operation. This table is updated every 30 seconds.
"Req in" and "Req out" statistics for the following methods (1xx, 2xx, 3xx, 5xx, 6xx, IntErrs) are packed in a table. For example: sipCodeStatsTable sipStatsCodeIndexsipStatsCodesipOutResponsesipInResponse 11xx20 22xx02		

Table 14. MIB OIDs (Continued)

MIB	OID	Description
msRtpLowCallThreshold	1.3.6.1.4.1.9234.5.2.3.1.0	Number of calls versus the maximum number of calls allowed. It supports the get and set operations. Its value is a percentage, and specifies the lower boundary. Valid values for the set operation range from 1 to 100. When the current call percentage exceeds this threshold, the msRtpLowCallThreshold trap is sent. The current call volume (as a percent of the current call load verses the total licenses available) is compared to this threshold. This comparison is made every 30 seconds. When setting this value use the following format: LowThreshold < MedThreshold < HighThreshold
msRtpMedCallThreshold	1.3.6.1.4.1.9234.5.2.3.2.0	Number of calls versus the maximum number of calls allowed. It supports the get and set operations. Its value is a percentage, and specifies the medium boundary. Valid values for the set operation range from 1 to 100. When the current call percentage exceeds this threshold, the msRtpMedCallThreshold trap is sent. The current call volume (as a percent of the current call load verses the total licenses available) is compared to this threshold. This comparison is made every 30 seconds. When setting this value use the following format: LowThreshold < MedThreshold < HighThreshold
msRtpHighCallThreshold	1.3.6.1.4.1.9234.5.2.3.3.0	Number of calls versus the maximum number of calls allowed. It supports the get and set operations. Its value is a percentage, and specifies the upper boundary. Valid values for the set operation range from 1 to 100. When the current call percentage exceeds this threshold, the msRtpHighCallThreshold trap is sent. The current call volume (as a percent of the current call load verses the total licenses available) is compared to this threshold. This comparison is made every 30 seconds. When setting this value, use the following format: LowThreshold < MedThreshold < HighThreshold
msVxmlNumberRecoveryFailures	1.3.6.1.4.1.9234.5.2.4.1.0	Number of failures that have occurred while attempting to recover Media Content files. Setting to 0 clears it.
msVxmlLastCriticalError	1.3.6.1.4.1.9234.5.2.4.2.0	Last Critical level error received.
msFeaturesPortsTotal	1.3.6.1.4.1.9234.5.2.5.1.1.0	Number of licensed ports available on the IP Media Server.

TRAP Definitions

Table 15. Trap OIDs and Descriptions

Trap	OID	Description
msResetChange	1.3.6.1.4.1.9234.5.3.1	The IP Media Server has been reset by SNMP. The following string is included in the trap message: “The IP Media Server Has Been Reset”.
msSipLowCallThresholdMet	1.3.6.1.4.1.9234.5.3.2	The IP Media Server call percentage has exceeded the low threshold value. The following string is included in the trap message: “Low Call Threshold is Met, Call Volume at %d” (where %d is the current percent call volume).
msSipMedCallThresholdMet	1.3.6.1.4.1.9234.5.3.3	The IP Media Server call percentage has exceeded the medium threshold value. The following string is included in the trap message: “Med Call Threshold is Met, Call Volume at %d” (where %d is the current percent call volume).
msSipHighCallThresholdMet	1.3.6.1.4.1.9234.5.3.4	The IP Media Server call percentage has exceeded the high threshold value. The following string is included in the trap message: “High Call Threshold is Met, Call Volume at %d” (where %d is the current percent call volume).
msRtpLowCallThresholdMet	1.3.6.1.4.1.9234.5.3.5	The IP Media Server call percentage has exceeded the low threshold value. The following string is included in the trap message: "Low Call RTP Threshold is Met, Call Volume at %d” (where %d is the current percent call volume).
msRtpMedCallThresholdMet	1.3.6.1.4.1.9234.5.3.6	The IP Media Server call percentage has exceeded the medium threshold value. The following string is included in the trap message: "Med Call RTP Threshold is Met, Call Volume at %d” (where %d is the current percent call volume).
msRtpHighCallThresholdMet	1.3.6.1.4.1.9234.5.3.7	The IP Media Server call percentage has exceeded the high threshold value. The following string is included in the trap message: "High Call RTP Threshold is Met, Call Volume at %d” (where %d is the current percent call volume).
msVxmlRecoveryFailureOccurred	1.3.6.1.4.1.9234.5.3.8	An attempt to recover a recorded media content file has failed.
msVxmlCriticalError	1.3.6.1.4.1.9234.5.3.9	A critical level error has occurred in a VXML application. Contains the text of msVxmlLastCriticalError.
msVxmlScriptAsLastResortOccurred	1.3.6.1.4.1.9234.5.3.10	The default script is used.
msVxmlScriptFileAsLastResort	1.3.6.1.4.1.9234.5.2.4.3	The filename and location of the default script.

Table 15. Trap OIDs and Descriptions

Trap	OID	Description
msFetchFailureOccurred	1.3.6.1.4.1.9234.5.3.11	An HTTP fetch failure occurred. The following string is included in the trap message: “The URL of the last file that fails to be fetched <error code of the last fetch failure> <error description of the last fetch failure>

SNMP MIB-II

The IP Media Server supports SNMPv2 and SNMPv3 agent operation and includes the following Management Information Bases (MIBs) and all their specified managed objects:

RFC 1213 MIB-II

- system
- interface
- ip
- icmp
- tcp
- udp
- snmp

RFC 1907 SNMPv2

snmpTRAP-coldStart, authenticationFailure

Unsupported OIDs

The following OIDs are not supported on the IP Media Server as part of the SNMP MIB-II specification.

System Group

- sysServices

Interfaces Group

- ifInUnknownProtos
- ifOutNUcastPkts

IP Group

- ipRouteMetric2

- ipRouteMetric3
- ipRouteMetric4
- ipRouteAge
- ipRouteMetric5

System Menu

The **System** menu contains commands for:

- Changing Administrator Password
- Configuring the Clock
- Backing Up and Restoring Configurations
- Managing Licenses
- Managing Certificates
- Rebooting the Host
- Resetting the Dialogic® IP Media Server
- Shutting Down the Host
- Updating Software
- Administering Users

These menu items are described in the following sections.

System Home Page

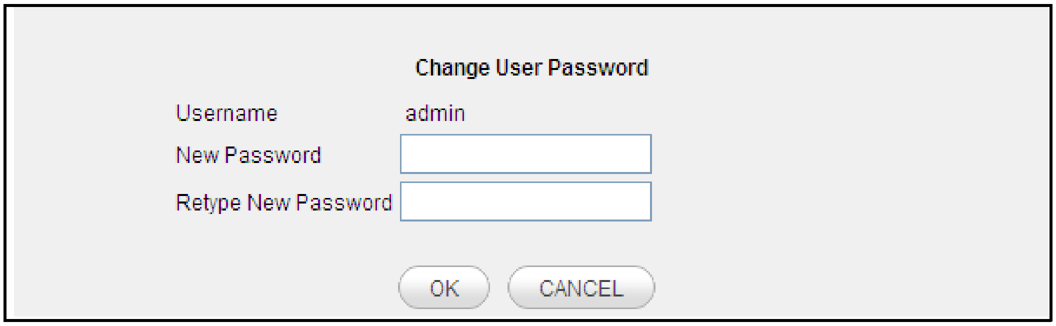
When you select the **System** menu, the IP Media Server home page appears with updated status information (see "Web User Interface Home Page" (page 33)).

Changing Administrator Password

Note: Passwords are case sensitive.

To change the password of the account you are currently logged in on:

1 Select the **System→Change Password** command to display the Change Password page:



Change User Password

Username admin

New Password

Retype New Password

Figure 56. Change Password Page

2 Enter your current password.

3 Enter a new password.

4 Confirm your new password.

5 Click OK to make the change.

Configuring the Clock

Note: Only Administrators have access to the **CLOCK** command.

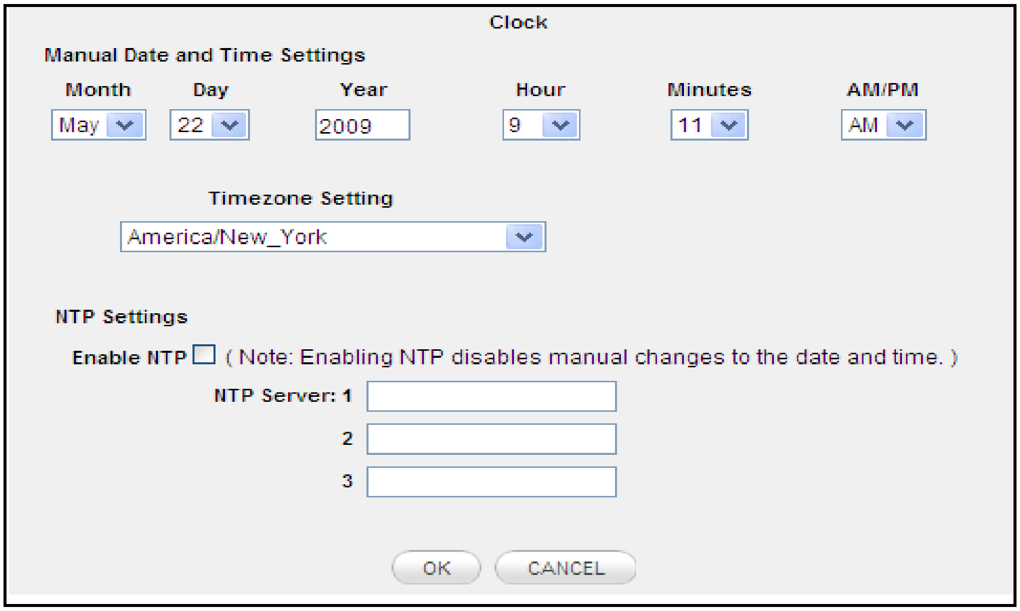
The system has an internal clock, but it can also be configured to source its clock from a network time protocol (NTP) server.

- If NTP is enabled, the system immediately starts using the NTP server.
- If NTP is not enabled, you can set the current system time, date, and time zone.

Note: The use of an NTP server across all servers in your network is strongly recommended, as it ensures that time and date stamps will be consistent and comparable across the network. This helps considerably when troubleshooting the IP Media Server.

To configure an NTP server:

1 Select **CLOCK** from the **System** menu to display the Clock page.



Clock

Manual Date and Time Settings

Month	Day	Year	Hour	Minutes	AM/PM
May	22	2009	9	11	AM

Timezone Setting: America/New_York

NTP Settings

Enable NTP □ (Note: Enabling NTP disables manual changes to the date and time.)

NTP Server: 1

2

3

Figure 57. Clock Page

2 Check **Enable NTP**.

3 Enter the IP address of one or more NTP servers.

Note: You can configure up to three NTP servers.

4 Click **OK** to apply any changes. To cancel changes, click **CANCEL**.

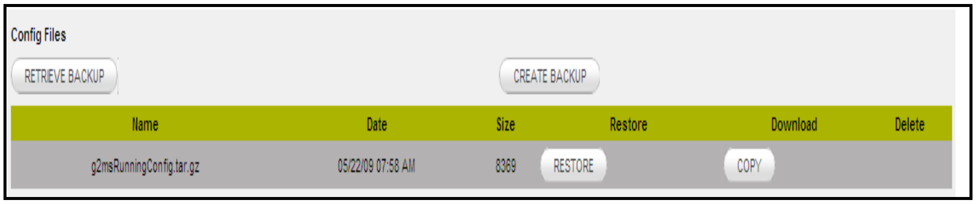
Backing Up and Restoring Configurations

The system provides the ability to back up all the configuration parameters. The backup files are stored together in a tar file and can be downloaded to another location on the network. The configuration can also be restored from a previously saved backup of the system.

Note: Only Administrators can create and delete backup configurations. All users can download a configuration.

To access the configuration backup services:

1 Select **System→Config** to display the **Config Files** page.



Name	Date	Size	Restore	Download	Delete
g2msRunningConfig.tar.gz	05/22/09 07:58 AM	8369	RESTORE	COPY	

Figure 58. Config Files Page

The Config Files page contains a list of currently backed-up configurations, as well as the currently running configuration.

Note: The running configuration is saved each time the host reboots or the IP Media Server is reset. It is called `g2mRunningConfig.tar.gz`.

From the **Config Files** page you can perform several configuration file actions:

- Back up configurations
- Delete a stored backup
- Download a stored backup configuration
- Restore a backed-up configuration.

Backup Current Configurations

To back up the current set of configuration files:

1 Click **CREATE BACKUP**.

This action makes a copy the current configuration files (which are not necessarily identical to the running configuration) and creates a backup copy. The name of the backup is based on the date and time the backup was created. It is similar to:

```
g2msbackup.20050701114510.tar.gz
```

which is a backup file created on July 01, 2005 at 11:45:10.

Delete a Stored Backup

To delete a stored backup configuration:

1 Click the **DELETE** button beside the file name.

This action must be confirmed or cancelled. The backup of the running configuration cannot be deleted.

Download a Stored Backup Configuration

To download a stored backup configuration to another location:

1 Click the **DOWNLOAD** button beside the file name.

A standard file dialog appears, giving you the option of opening or saving the file.

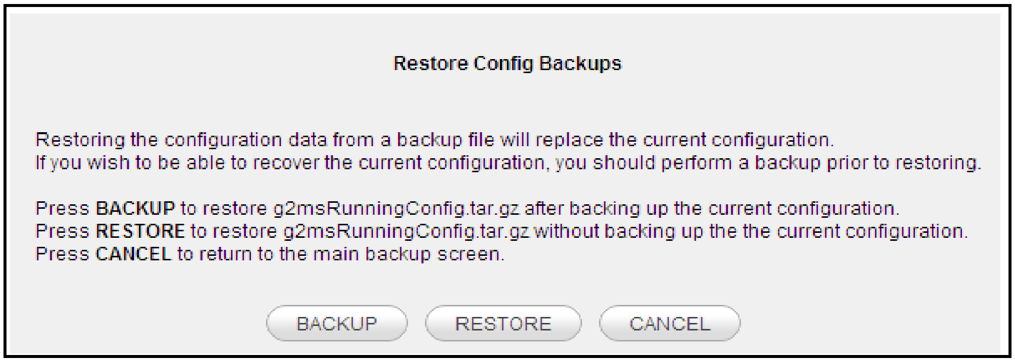
2 Click **SAVE** and select the directory where the configuration file is saved.

Restore a Backed-up Configuration

Note: Only Administrators can restore a configuration.

To restore a previously backed up configuration:

1 Click the **RESTORE** button beside the backup file name to display the Restore Config Backups page:



Restore Config Backups

Restoring the configuration data from a backup file will replace the current configuration.
If you wish to be able to recover the current configuration, you should perform a backup prior to restoring.

Press **BACKUP** to restore g2msRunningConfig.tar.gz after backing up the current configuration.
Press **RESTORE** to restore g2msRunningConfig.tar.gz without backing up the the current configuration.
Press **CANCEL** to return to the main backup screen.

Figure 59. Restore Config Backups Page

There are two types of restorations available:

- Backup–Creates a copy of the current configuration files and then replaces them with the selected backup configuration.
- Restore–Overwrites the current configuration files with the selected backup configuration, but does not create a copy of the current configuration.

You can also cancel the restore action by clicking **CANCEL**.

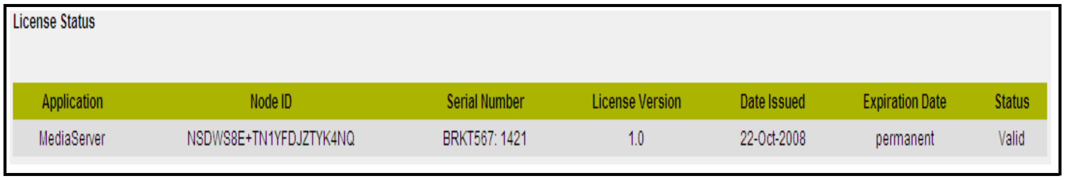
Restoring the configuration data from a backup file can replace the current configuration. If you wish to be able to recover the current configuration, you should perform a backup prior to restoring.

Restoring a configuration updates the configuration files, but does not affect the currently running configuration. The host must be rebooted for the restored configuration to take effect.

Managing Licenses

You use the IP Media Server Web UI to install and activate IP Media Server licenses, and to view the current status of licenses on your system. For detailed information on managing licenses, see the *Dialogic IP Media Server License Activation Guide*.

To manage licenses, select the **System→License→ Status** menu item. This displays the License Status page, which contains information about the currently active license.

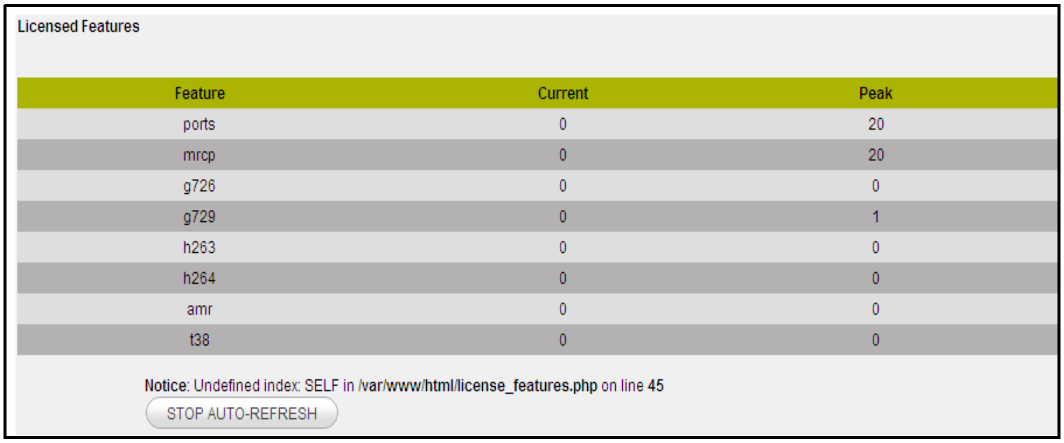


License Status

Application	Node ID	Serial Number	License Version	Date Issued	Expiration Date	Status
MediaServer	NSDWS8E+TN1YFDJZTYK4NQ	BRKT567: 1421	1.0	22-Oct-2008	permanent	Valid

Figure 60. License Status Page

To view the features currently licensed on your system and statistics about their usage, select the **System→License→ Features** menu item. The License Features page is displayed:



Licensed Features

Feature	Current	Peak
ports	0	20
mrcp	0	20
g726	0	0
g729	0	1
h263	0	0
h264	0	0
amr	0	0
t38	0	0

Notice: Undefined index: SELF in **/var/www/html/license_features.php** on line **45**

Figure 61. Licensed Features Page

To activate and install a license, use the NODE ID and INSTALL menus. For more information, see the *License Activation Guide*.

Managing Certificates

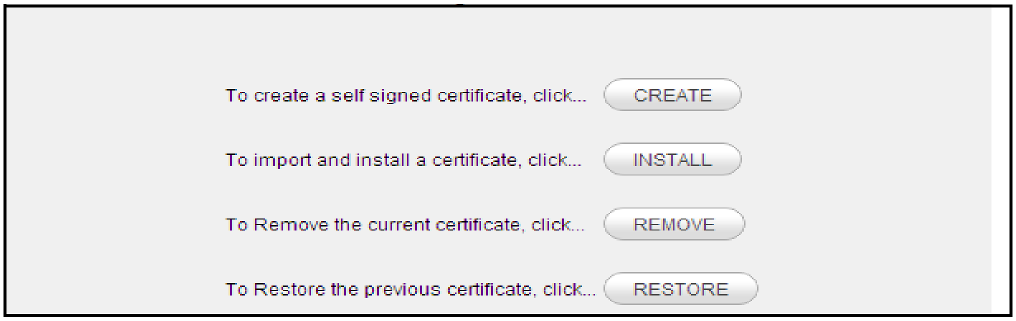
The Dialogic® IP Media Server Web User Interface can operate with HTTP or HTTPS. If HTTPS is being used, a padlock appears at the bottom right in the browser display. If HTTP is being used, a padlock does not appear.

To use HTTPS, the Dialogic® IP Media Server must have a server certificate and key, and the browser must have the matching client certificate.

A user-generated security certificate and key can be installed on the Dialogic® IP Media Server. The Web UI uses this certificate/key for HTTPS authentication.

To retrieve a certificate/key:

1 Select **System→Manage Certificates** to display the manage **Certificates** page:



To create a self signed certificate, click...

To import and install a certificate, click...

To Remove the current certificate, click...

To Restore the previous certificate, click...

Figure 62. Manage Certificates Page

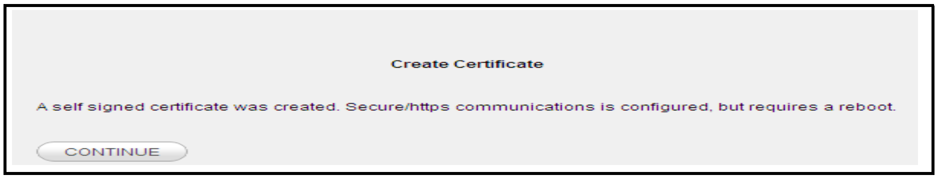
This page provides the following options:

- **CREATE**: Creates a self signed certificate and automatically installs it.

- **INSTALL**: Imports a certificate and key from a remote server and installs it on the Dialogic® IP Media Server.
- **REMOVE**: Removes the current certificate from the Dialogic® IP Media Server.
- **RESTORE**: Restores the previous certificate to the Dialogic® IP Media Server.

Creating a Certificate

When you click **CREATE**, a certificate is created and automatically installed. The following page appears.



Create Certificate

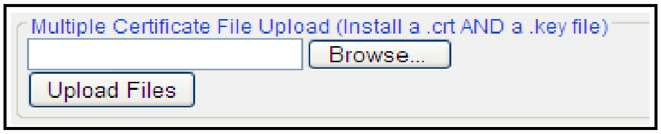
A self signed certificate was created. Secure/https communications is configured, but requires a reboot.

Installing a Certificate

When you click **INSTALL**, a certificate and key can be retrieved from a remote server using Secure access over HTTPS or HTTP. Enter the parameters for the Secure access over HTTPS or HTTP server that holds the certificates and keys. The Dialogic® IP Media Server attempts to access the server, and then displays the available certificates (.crt files) for retrieval. Only certificate files (<filename>.crt) are shown, but there must also be a matching valid key (<filename>.key) present for the certificate in order for the certificate to be displayed in the Web UI. The certificate and the key must have the same name with the appropriate file extension (xx.crt and xx.key). You can navigate through the directory structure, but the window only displays directories and certificates.

To install a certificate:

1 On the Manage Certificates page, click **INSTALL** to display the Install Certificates page:



Multiple Certificate File Upload (Install a .crt AND a .key file)

Figure 63. Install Certificate Page

2 Browse to the certificate file and click **Upload Files** to install the certificate and display the results of the installation.

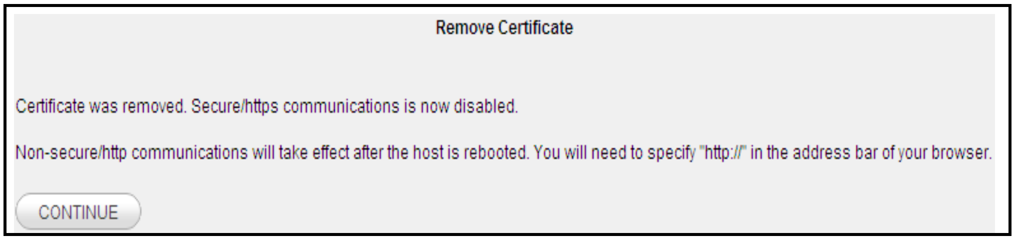
- If the installation is successful, the previous certificate (if there is one) is saved and the Web UI begins using the new certificate as soon as you click Continue.
- If the installation is not successful an error appears and the update of the certificate does not take place. The certificate is not kept for installation in the future.

Removing a Certificate

To remove the current certificate:

1 On the Manage Certificates page, click **REMOVE** to remove the current certificate and key from the system and save them.

The Remove Certificate page is displayed to confirm the removal:



Remove Certificate

Certificate was removed. Secure/https communications is now disabled.

Non-secure/http communications will take effect after the host is rebooted. You will need to specify "http://" in the address bar of your browser.

Figure 64. Remove Certificate Page

The Web User Interface uses HTTP when the **CONTINUE** button is clicked. The padlock icon at the bottom of the browser display disappears when the screen is next refreshed.

Restoring a Certificate

On the Manage Certificates page, click the **RESTORE** button to put the previous certificate (if there is one that has been removed or overwritten) back on the system. The Web User Interface uses HTTPS when the **CONTINUE** button is clicked. The padlock icon at the bottom of the browser display appears when the screen is refreshed.

Rebooting the Host

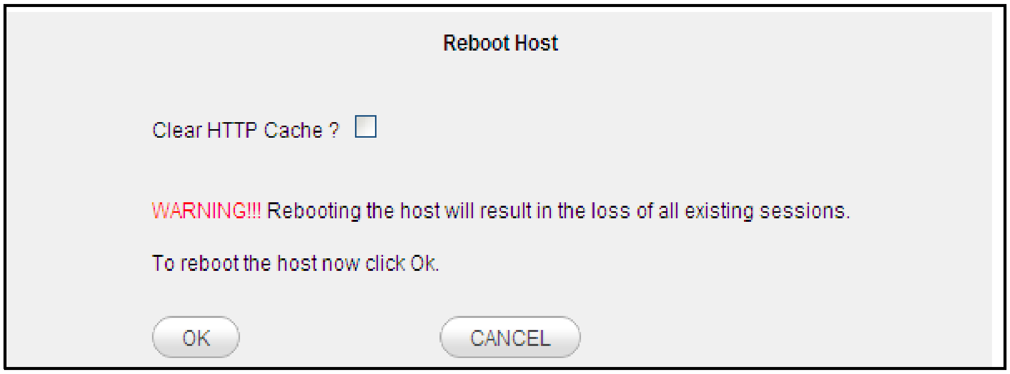
Rebooting the host causes all applications to stop and the operating system to reboot. After rebooting, the system reads and uses the configuration files for all services and interfaces. This action causes all traffic to be dropped and all existing sessions to be disconnected.

Note: Only Administrators can reset the Dialogic® IP Media Server.

Rebooting the host results in the loss of all existing sessions.

To reset the Dialogic® IP Media Server:

1 Select **Reboot Host** from the **System** menu to display the **Reboot Host** page.



Reboot Host

Clear HTTP Cache ? □

WARNING!!! Rebooting the host will result in the loss of all existing sessions.

To reboot the host now click Ok.

Figure 65. Reboot Host Page

2 Select **Clear HTTP Cache** if you wish to delete all stored IP Media Server pages.

3 Click **OK** to reboot the IP Media Server host. Click **CANCEL** to continue without rebooting.

When the action is complete, you are returned to the IP Media Server home page.

Resetting the Dialogic® IP Media Server

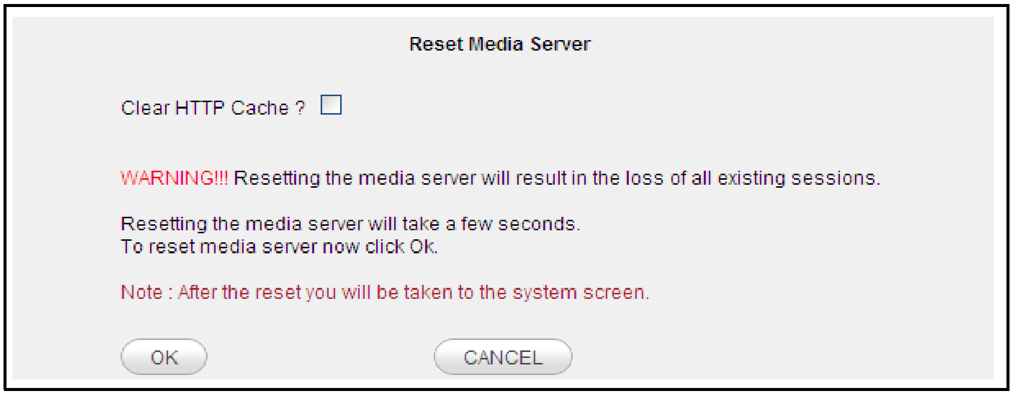
This command causes the Dialogic® IP Media Server application to reset and restart itself, but does not reboot the host.

Note: Only Administrators can reset the Dialogic® IP Media Server.

Resetting the IP Media Server results in the loss of all existing sessions.

To reset the IP Media Server:

1 Select **Reset Media Server** from the **System** menu to display the **Reset Media Server** page.



Reset Media Server

Clear HTTP Cache ? □

WARNING!!! Resetting the media server will result in the loss of all existing sessions.

Resetting the media server will take a few seconds.
To reset media server now click Ok.

Note : After the reset you will be taken to the system screen.

Figure 66. Reset Media Server Page

2 Select **Clear HTTP Cache** if you wish to delete all stored IP Media Server pages.

3 Click **OK** to reset the IP Media Server. Click Cancel to continue without resetting the IP Media Server.

When the action is complete, you are returned to the IP Media Server home page.

Shutting Down the Host

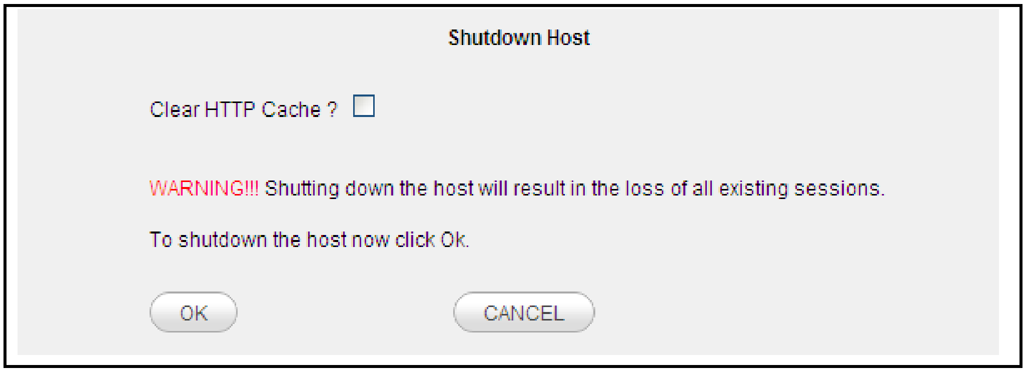
Shutting down the host stops all applications and the operating system. This action causes all traffic to be dropped and all existing sessions to be disconnected.

Note: Only Administrators can shut down the Dialogic® IP Media Server.

Shutting down the host results in the loss of all existing sessions.

To shut down the Dialogic® IP Media Server:

1 Select **Shutdown Host** from the **System** menu to display the Shutdown Host page.



Shutdown Host

Clear HTTP Cache ? □

WARNING!!! Shutting down the host will result in the loss of all existing sessions.

To shutdown the host now click Ok.

Figure 67. Shutdown Host Page

2 Select **Clear HTTP Cache** if you wish to delete all stored IP Media Server pages.

3 Click **OK** to shut down the IP Media Server host. Click **CANCEL** to continue without shutting down.

Updating Software

You can download and upgrade the IP Media Server software from a remote location. The software releases are digitally signed by Dialogic and contain checksums to ensure the files are not corrupted during the download process.

Note: Only Administrators have access to the software updates menu.

Releases can be downloaded from secure access over HTTPS or HTTP. Releases can be obtained from the Dialogic Technical Support web site. This requires a user name, password, and directory, which can be obtained from Dialogic Technical Support.

To download a release and upgrade a system:

1 Download the desired release to the system using the Retrieve command.

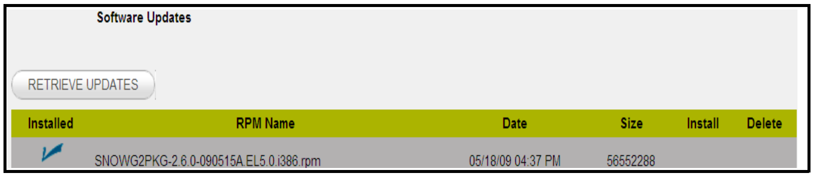
Performs download and the Retrieve command checks to ensure the software release was downloaded successfully.

2 Using the Install command, select the release you want to install.

Saves the existing release, and installs the new release. Installing a new release of software causes the host to reboot.

Displaying the Releases Available on the System

1 Select **Software Updates** from the **System** menu to display the **Software Updates** page:

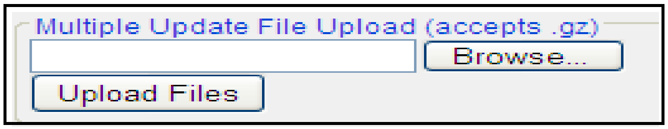


Software Updates

Installed	RPM Name	Date	Size	Install	Delete
✓	SNOWG2PKG-2.6.0-090515A.EL5.0.i386.rpm	05/18/09 04:37 PM	56552288		

Figure 68. Software Updates Page

2 Click **RETRIEVE UPDATES** to display the **Retrieve Updates** page.



Multiple Update File Upload (accepts .gz)

Figure 69. Retrieve Updates Page

3 Enter the location of updates for the IP Media Server and your login name and password. The Results page displays.

If you leave the Directory Path blank, the Results page includes all accessible directories on the RTP server. Updates that are currently on your computer are indicated with a checkmark in the folder icon on the left.

If necessary, navigate to the appropriate subdirectory to display the list of available updates.

4 Click **RETRIEVE** to download the update to your computer. The display returns to the Software Updates page, with the new update included in the list.

5 To install a new software update, click Install. This displays the **Confirm Software Update** page.

6 Click **OK** to complete the installation of the new software. The **Software Update** page is again displayed with a checkmark next to the newly installed software.

Viewing the Running Release

To display information about the current release, click **SYSTEM** to display the system home page; see “Web User Interface Home Page” (page 33).

Retrieving a Software Release

You access software releases via secure access over HTTPS or HTTP.A list of valid software releases appears and a **RETRIEVE** button appears for each release. The Installed column to the left of the release name contains a check mark if the release has already been downloaded to the system. If the Installed column is blank, the release has not been downloaded.

The window directories are also displayed and have a file folder icon to their left. You can navigate through the directory structure, but only other directories and IP Media Server releases are shown.

Click **RETRIEVE UPDATES** to download the selected software release to the IP Media Server. The standard transfer progress dialog appears and gives information about the success and failure of the download.

To retrieve a software release and download it (without installing it):

1. On the Software Updates page, click **RETRIEVE UPDATES** to display the **Retrieve Updates** page:

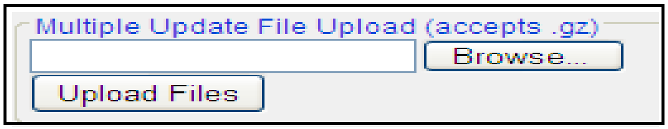


Figure 70. Retrieving Software

2. Browse to the file to upload and click **Upload Files**.

Installing a New Software Release

To install a new software release on the system, click the **INSTALL** button beside the release.

The screen displays the currently running release and asks you to confirm that you want to install the selected release. Click Confirm to install the new release and reboot the system.

⚠ **Installing a new release reboots the host.**

To remove a software release from the system, click the **DELETE** button beside the release to be deleted. Click confirm to confirm the deletion, or click Cancel to stop.

Note: Deleting a software release does not affect the currently running system. It continues to operate and use the same release when reset.

Administering Users

The IP Media Server supports two access levels:

- Administrator—Can change the configuration of the system and execute administrative tasks.
- Operator—Can monitor the system, but cannot change configurations or execute administrative tasks.

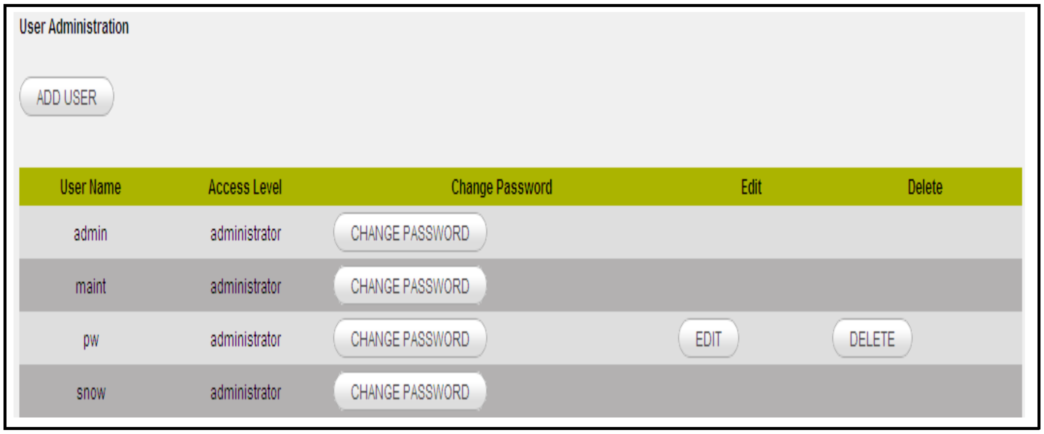
Commands that are only available to Administrators are noted as such. All other commands are usable by both operators and administrators.

Note: Only Administrators can perform user administration.

Use the **System→User Administration** command to display the User Administration page, which contains the currently configured users on the system. Administrators can add, delete, and change the attributes of other users.

The attributes are:

- password
- access level



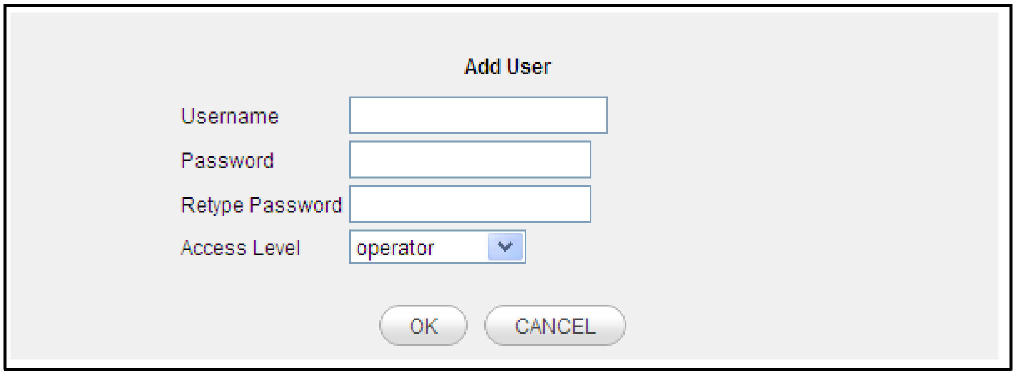
User Name	Access Level	Change Password	Edit	Delete
admin	administrator	CHANGE PASSWORD		
maint	administrator	CHANGE PASSWORD		
pw	administrator	CHANGE PASSWORD	EDIT	DELETE
snow	administrator	CHANGE PASSWORD		

Figure 71. User Administration Page

Adding a User

To add a new user:

1 Click **ADD USER** to display the **Add User** page.



Username

Password

Retype Password

Access Level operator

Figure 72. Add User Page

2 Fill in the following:

- Username
- Password
- Access level

Note: User names and passwords are case sensitive.

3 To complete the action, click **OK**.

To cancel the action, click **CANCEL**.

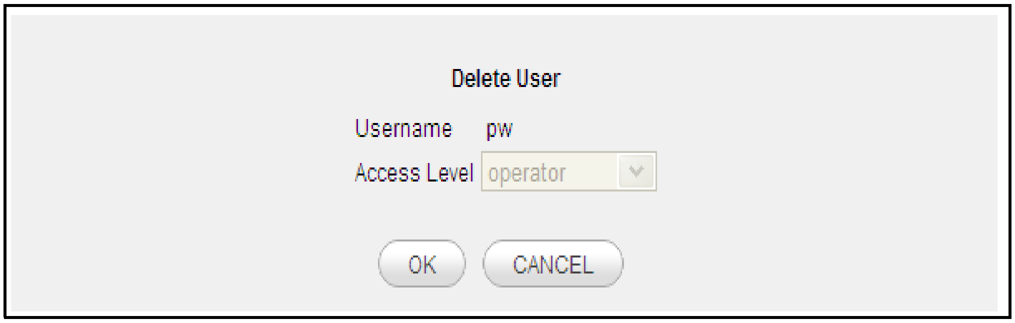
Deleting a User

To delete a user (Administrator only):

1 Click the **DELETE** button beside the user name.

A new screen appears to verify the change.

2 Click **OK** to delete the user. Click **CANCEL** to cancel.



Delete User

Username pw

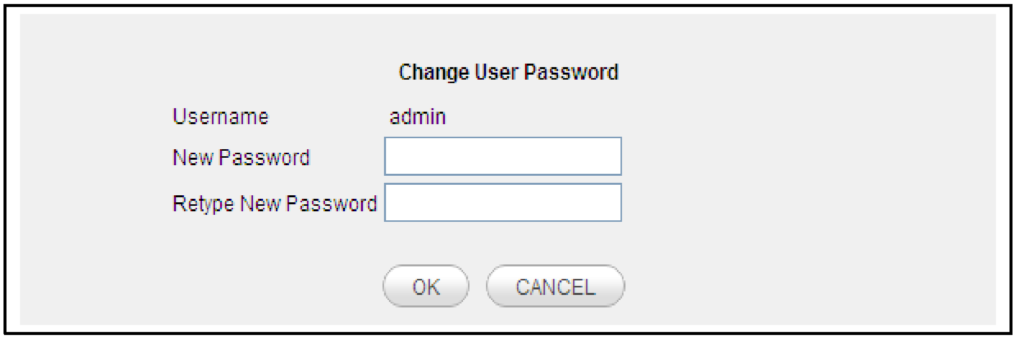
Access Level operator

Figure 73. Delete User Page

Resetting a Password

To reset the password of any other user, do the following:

1 Click the **CHANGE PASSWORD** button beside the user name to display the Change User Password page.



Change User Password

Username admin

New Password

Retype New Password

Figure 74. Change User Password Page

2. Enter a new password.
3. Confirm the new password.
4. Click **OK** to accept.

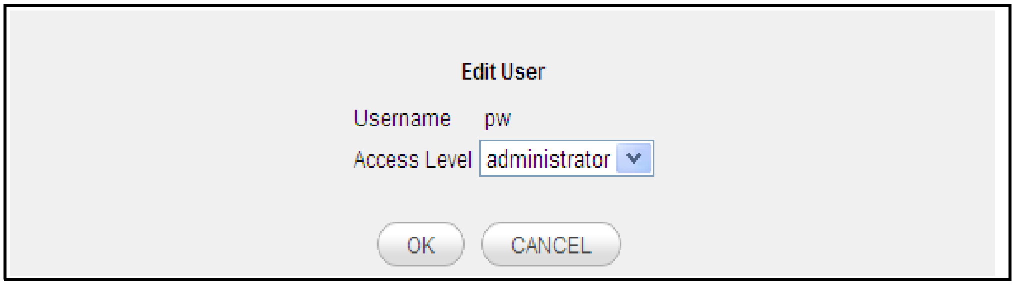
   Click CANCEL to cancel the change.

Note: As Administrator, you cannot change your own password or delete your own username in USER ADMINISTRATION. You can change your password using the **SYSTEM→CHANGE PASSWORD** command.

Changing User Access Level

To change the access level of a user (administrator only), do the following:

1. Click the **EDIT** button beside the user name to display the Edit User page:



Username pw

Access Level administrator

Figure 75. Edit User Page

2. Choose the access level **ADMINISTRATOR** or **OPERATOR**.
3. To accept the change, click **OK**.

   To cancel the change, click **CANCEL**.

Accounting Mechanism

Monitoring Call Volume

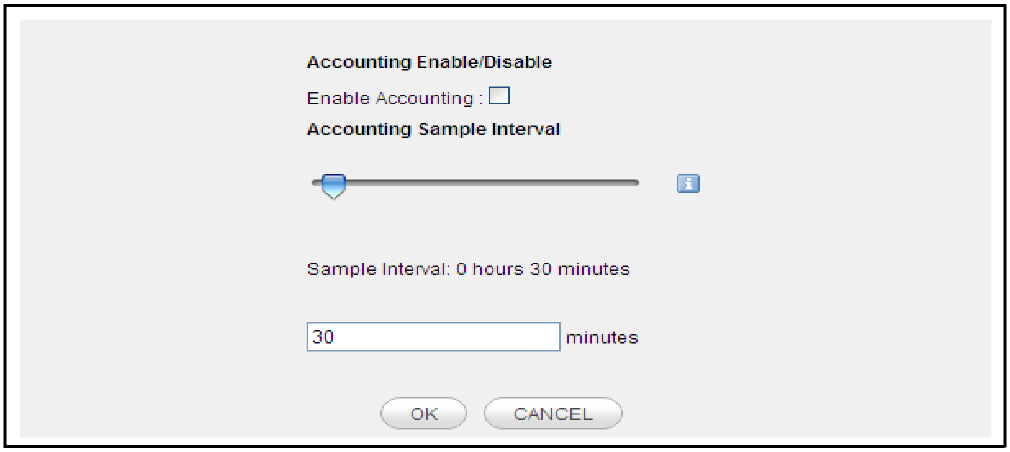
The IP Media Server has an accounting mechanism that provides details on what licensed resources a customer is using during a given time interval. The Web UI allows you to configure this time interval.

The accounting mechanism in the IP Media Server stores the data in two parts:

- xml format text log file
- secure private database

Follow the steps below to configure the time interval.

1 Select **Media Server→ Configure→ Accounting** from the Web UI. The following screen appears.



Accounting Enable/Disable

Enable Accounting : □

Accounting Sample Interval

Sample Interval: 0 hours 30 minutes

30 minutes

2 Accounting is disabled by default. Select the Enable Accounting checkbox to enable.

3 There are three ways to enter the sample interval:

- Slide the tab on the bar.
- Click on the bar and use the mouse scroll wheel.
- Type the sample interval in the box.

4 Click **OK**.

5 Changes require you to reset or reboot the IP Media Server.

A - Compliance and Standards Information

This chapter describes the IP Media Server's compliance with standards and provides regulatory compliance notices.

Supported Protocols and Standards

The following is a list of currently supported protocols and RFC standards.

Table 16. Supported Protocols and Standards

Protocols	RFC #
ARP	RFC 826
DNS	RFC 1034, RFC 1035, RFC 2181
Ethernet v2	RFC 894
	Gigabit Ethernet specification IEEE 802.3z. 802.3x.
	RFC 2665, General Ethernet statistics
HTTP/1.0	RFC 1945
HTTP/1.1	RFC 2068, 2616
ICMP	RFC 792, 950
Internet Host-Apps	RFC 1123
Internet Host-Comm.	RFC 1122
IP	RFC 791
MIME	RFC 2045, 2046
NTPv3	RFC 1305
RTP	RFC 1889, 1890, 2833
RTSP	RFC 2326
SIP	RFC 2543 draft-ietf-sip-rfc2543bis-03 RFC 2976, “The SIP Info Method” RFC 4028 RFC 2976 RFC 3261 RFC 4240 RFC 5022
SDP	RFC 2327
TELNET	RFC 854
TFTPv2	RFC 1350
URI	RFC 2396

Table 16. Supported Protocols and Standards (Continued)

Protocols	RFC #
URL	RFC 1738
VXML	V1.0, V2.0 W3C
MRCP v1	RFC 4463
MRCP v2	draft-ietf-speechsc-mrcpv2-16

Product Safety and Emissions - Regulatory Compliance Notices

The IP Media Server complies with industry safety and emissions requirements, as indicated below.

Safety	UL 60950-1, First Edition CAN/CSA-C22.2 No. 60950-1-03 EN 60950-1:2001 IEC 60950-1:2001	USA Canada Europe Global (CB)
EMC Emissions	FCC 47 CFR Part 15 Class A ICES-003 Issue 3 Class A EN 55022:1998/A1:2000/A2:2003 Class A VCCI Class A ITE AS/NZS CISPR22:2002 Class A	USA Canada Europe Japan Australia
EMC Immunity	EN 55024:1998/A1:2001/A2:2003 EN 61000-3-2:2000 EN 61000-3-3:1995/A1:2001	Europe Europe Europe

EN 550022 Class A Required Warning

Warning: This is a Class A product. In a domestic environment, this product can cause radio interference, in which case the user might be required to take adequate measures.

United States: FCC CFR 47 Part 15 Required Instructions

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this manual, can cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user is required to correct the interference at his own expense.

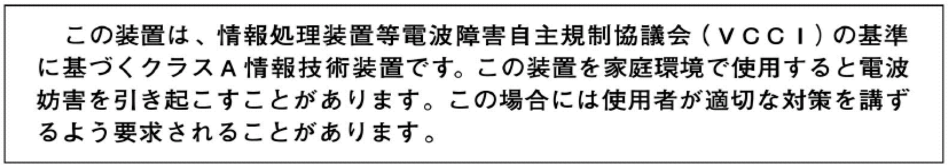
Canada

This Class A digital apparatus complies with Canadian Standard ICES-003.

Cet appareil numérique de la class A est conforme à la norme NMB-003 du Canada.

VCCI Japan

ITE Class A Statement (For Class A Products).



この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Translation: This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

B - Troubleshooting

This appendix describes some basic troubleshooting techniques you can use when working with the Dialogic® IP Media Server. It includes the following topics:

- Checking Log Files
- Checking Network Connectivity
- Checking Current Calls
- Recovering after a Power Failure

Checking Log Files

Log files contain detailed information about the operation of the IP Media Server. This information may be useful in troubleshooting issues that may arise during application development and deployment. Tracing a call through the log files also can help one to become familiar with the operation of the IP Media Server.

Log files are stored in the directory `/var/snowshore/logs`. The log files and their description (including IP Media Server component if applicable) are provided in Table 17. See also "Log Naming Convention" (page 101) for information on the naming convention for log files.

Table 17. IP Media Server Log Files

File	Contents	IP Media Server Component
accounting.log	Clear text log created from Generate Accounting Logs option in Configure Logs page of Web User Interface (Web UI).	
audit.log	All SNMP sets and user configuration changes made through the Web UI. (IP Media Server persisted settings.)	Web UI
cache.log	Squid cache processes.	HTTP
cache_access.log	Squid cache accesses.	Cache
dms.log	Log for DMS component.	DMS
email_to_fax	Information about email to fax traffic.	
fido.log	Messages associated with fetching Internet domain objects (files, VXML pages over HTTP).	FIDO
messages.log	SIPD and UAD messages written when the Syslog option is enabled.	Syslog
MrcpClientLibrary.log	Information about MRCP activity.	MRCP
mrcpapp.log	Information about the interaction between the mrcpapp and VoiceXML layers (MRCP activity at the IP Media Server level).	MRCP
msaccounting.log	Encrypted log created from Generate Accounting Logs option in Configure Logs page of Web UI.	
mserv.log	Details of creating and managing RTP streams on the IP Media Server.	MServ
msinit.log	Log entries of the IP Media Server initialization.	MSInit
msprovider.log	License information.	MSProvider

Table 17. IP Media Server Log Files

File	Contents	IP Media Server Component
recoveryd.log	VoiceXML 1.0 messages on the IP Media Server.	VoiceXML 1.0
rtspc.log	RTSP information.	RTSPC
sipd.log	SIP messages received and sent by the IP Media Server.	SIPD
snmpdaemon.log	Log for SNMPDaemon component.	SNMPDaemon
sr140app.log	Details of creating and managing fax on the IP Media Server.	SR140app
uad.log	Internal messages associated with VoiceXML transfer functions.	UAD
vxmld.log	VoiceXML 1.0 messages on the IP Media Server.	VoiceXML 1.0
vxml2d.log	VoiceXML 2.0 messages on the IP Media Server.	VoiceXML 2.0
<hostname>_system_info.log	System information log file created from Gather System Information option in Configure Logs page of Web UI.	
snowshore_additional_install.log	Used to verify installation or upgrade.	

The primary log file for troubleshooting call setup issues is the sipd.log. This log file can be viewed and processed to look for all the messages for a particular call. Each message carries a time stamp. Useful tags to search for in the log file are:

- ◆ By Call-ID

  For example, use *Call-ID: 12995-7@172.17.100.245* to find all the SIP messages associated with a particular call.

- ◆ By 400 and 500 type messages

  For example, use *SIP/2.0 400* or *SIP/2.0 500* to find all error messages in the file. These messages can be related to a particular call, and often lead to the reason the call failed.

In addition to these log files, you can generate the system information log file at the time the issue occurs. To generate this log file:

1. Log in to the IP Media Server Web UI.
2. Select **Logs→Configure** to display the Configure Logs page.
3. Click the **Create** button next to System Configuration Log.
4. Click **OK**. The Log Files page is displayed and the log file called <hostname>_system_info.log is created.

Note: Be aware that logging affects system performance. Increasing the number of logs enabled and the level of detail requested may adversely affect system performance.

For more information about logging, see “Logs Menu” (page 95).

Checking Network Connectivity

If a call cannot be successfully placed, check that there is connectivity to the required networks.

1. Ping the devices used in the call. Using **Network→Utilities→Ping** from the Web UI, try pinging the application server IP address and the IP address of the RTP device.
2. If either ping command fails, select **Network→Configure→Interfaces**. Check to ensure that the interfaces are active and that one of the interfaces is designated as supporting SIP and RTP.
3. Check the routing table for routes, network masks, and default gateways using **Network→Configure→Interfaces**.

Checking Current Calls

To determine how many calls are currently active on the system, use the Statistics menu on the Web UI. Select **Statistics→Cumulative** to display the current number of calls on the IP Media Server for a given application service type. For more information, see "Dialogic® IP Media Server Statistics" (page 90).

Recovering after a Power Failure

When a system reboots, it does a file system check. Under most circumstances, the system recovers automatically and reboots. In rare circumstances, the system can have issues and be unable to recover the file system. In this case, use the following procedure.

1. Connect to the serial port of the IP Media Server.
2. Power up the system and watch the terminal page. As the file check happens, it can find bad files that need to be repaired.
3. When asked to repair a file, type y.

   At the end of this process, the system should reboot and recover.

If the system does not recover, contact Dialogic Technical Support for repair and return procedures.

Note: It is recommended that a UPS be used to power the system to avoid issues from power fluctuations.

C - Required Red Hat Enterprise Linux Packages

The following details the inclusive list of Red Hat Enterprise Linux 5.2 Server packages required for IP Media Server Release 3.0.0 operation.

```
acl-2.2.39-3.el5.i386.rpm
acpid-1.0.4-5.i386.rpm
amtu-1.0.6-1.el5.i386.rpm
anacron-2.3-45.el5.i386.rpm
apmd-3.2.2-5.i386.rpm
apr-1.2.7-11.i386.rpm
apr-util-1.2.7-7.el5.i386.rpm
aspell-0.60.3-7.1.i386.rpm
aspell-en-6.0-2.1.i386.rpm
at-3.1.8-82.fc6.i386.rpm
atk-1.12.2-1.fc6.i386.rpm
atk-devel-1.12.2-1.fc6.i386.rpm
attr-2.4.32-1.1.i386.rpm
audit-1.6.5-9.el5.i386.rpm
audit-libs-1.6.5-9.el5.i386.rpm
audit-libs-python-1.6.5-9.el5.i386.rpm
authconfig-5.3.21-3.el5.i386.rpm
autofs-5.0.1-0.rc2.88.i386.rpm
basesystem-8.0-5.1.1.noarch.rpm
bash-3.2-21.el5.i386.rpm
bc-1.06-21.i386.rpm
beecrypt-4.1.2-10.1.1.i386.rpm
bind-libs-9.3.4-6.P1.el5.i386.rpm
bind-utils-9.3.4-6.P1.el5.i386.rpm
binutils-2.17.50.0.6-6.el5.i386.rpm
bluez-gnome-0.5-5.fc6.i386.rpm
bluez-hcidump-1.32-1.i386.rpm
```

```
bluez-libs-3.7-1.i386.rpm
bluez-utils-3.7-2.i386.rpm
bzip2-1.0.3-3.i386.rpm
bzip2-libs-1.0.3-3.i386.rpm
cairo-1.2.4-5.el5.i386.rpm
ccid-1.0.1-6.el5.i386.rpm
checkpolicy-1.33.1-4.el5.i386.rpm
chkconfig-1.3.30.1-2.i386.rpm
chkfontpath-1.10.1-1.1.i386.rpm
compat-libstdc296-2.96-138.i386.rpm
compat-libstdc33-3.2.3-61.i386.rpm
comps-extras-11.1-1.1.noarch.rpm
conman-0.1.9.2-8.el5.i386.rpm
coolkey-1.1.0-6.el5.i386.rpm
coreutils-5.97-14.el5.i386.rpm
cpio-2.6-20.i386.rpm
cpp-4.1.2-42.el5.i386.rpm
cpuspeed-1.2.1-3.el5.i386.rpm
cracklib-2.8.9-3.3.i386.rpm
cracklib-dicts-2.8.9-3.3.i386.rpm
crash-4.0-5.0.3.i386.rpm
crontabs-1.10-8.noarch.rpm
cryptsetup-luks-1.0.3-2.2.el5.i386.rpm
cups-1.2.4-11.18.el5.i386.rpm
cups-libs-1.2.4-11.18.el5.i386.rpm
curl-7.15.5-2.el5.i386.rpm
cyrus-sasl-2.1.22-4.i386.rpm
cyrus-sasl-lib-2.1.22-4.i386.rpm
cyrus-sasl-plain-2.1.22-4.i386.rpm
db4-4.3.29-9.fc6.i386.rpm
dbus-1.0.0-7.el5.i386.rpm
dbus-glib-0.70-5.i386.rpm
dbus-python-0.70-7.el5.i386.rpm
Deployment_Guide-en-US-5.2-9.noarch.rpm
desktop-file-utils-0.10-7.i386.rpm
device-mapper-1.02.24-1.el5.i386.rpm
device-mapper-multipath-0.4.7-17.el5.i386.rpm
dhcdbd-2.2-1.el5.i386.rpm
dhclient-3.0.5-13.el5.i386.rpm
dhcpv6-client-1.0.10-4.el5.i386.rpm
diffutils-2.8.1-15.2.3.el5.i386.rpm
distcache-1.4.5-14.1.i386.rpm
dmidecode-2.7-1.28.2.el5.i386.rpm
dmraid-1.0.0.rc13-9.el5.i386.rpm
dos2unix-3.1-27.1.i386.rpm
dosfstools-2.11-6.2.el5.i386.rpm
dump-0.4b41-2.fc6.i386.rpm
e2fsprogs-1.39-15.el5.i386.rpm
e2fsprogs-libs-1.39-15.el5.i386.rpm
ed-0.2-38.2.2.i386.rpm
eject-2.1.5-4.2.el5.i386.rpm
ElectricFence-2.2.2-20.2.2.i386.rpm
```

```
elfutils-0.125-3.el5.i386.rpm
elfutils-libelf-0.125-3.el5.i386.rpm
elfutils-libelf-devel-0.125-3.el5.i386.rpm
emacs-common-21.4-20.el5.i386.rpm
emacs-leim-21.4-20.el5.i386.rpm
enscript-1.6.4-4.1.el5.i386.rpm
ethtool-5-1.el5.i386.rpm
expat-1.95.8-8.2.1.i386.rpm
expect-5.43.0-5.1.i386.rpm
fbset-2.1-22.i386.rpm
file-4.17-13.i386.rpm
filesystem-2.4.0-1.i386.rpm
findutils-4.2.27-4.1.i386.rpm
finger-0.17-32.2.1.1.i386.rpm
firstboot-tui-1.4.27.3-1.el5.noarch.rpm
fontconfig-2.4.1-7.el5.i386.rpm
fontconfig-devel-2.4.1-7.el5.i386.rpm
freetype-2.2.1-19.el5.i386.rpm
freetype-devel-2.2.1-19.el5.i386.rpm
ftp-0.17-33.fc6.i386.rpm
gawk-3.1.5-14.el5.i386.rpm
gcc-4.1.2-42.el5.i386.rpm
GConf2-2.14.0-9.el5.i386.rpm
gd-2.0.33-9.4.el5_1.1.i386.rpm
gdb-6.5-37.el5.i386.rpm
gdbm-1.8.0-26.2.1.i386.rpm
gettext-0.14.6-4.el5.i386.rpm
ghostscript-8.15.2-9.1.el5_1.1.i386.rpm
ghostscript-fonts-5.50-13.1.1.noarch.rpm
giflib-4.1.3-7.1.el5.1.i386.rpm
giflib-utils-4.1.3-7.1.el5.1.i386.rpm
glib2-2.12.3-2.fc6.i386.rpm
glib2-devel-2.12.3-2.fc6.i386.rpm
glibc-2.5-24.i386.rpm
glibc-common-2.5-24.i386.rpm
glibc-devel-2.5-24.i386.rpm
glibc-headers-2.5-24.i386.rpm
gmp-4.1.4-10.el5.i386.rpm
gnome-python2-gconf-2.16.0-1.fc6.i386.rpm
gnu-efi-3.0c-1.1.i386.rpm
gnupg-1.4.5-13.i386.rpm
gnutls-1.4.1-2.i386.rpm
gpm-1.20.1-74.1.i386.rpm
grep-2.5.1-54.2.el5.i386.rpm
groff-1.18.1.1-11.1.i386.rpm
grub-0.97-13.2.i386.rpm
gtk2-2.10.4-20.el5.i386.rpm
gtk2-devel-2.10.4-20.el5.i386.rpm
gzip-1.3.5-10.el5.i386.rpm
hal-0.5.8.1-35.el5.i386.rpm
hdparm-6.6-2.i386.rpm
hesiod-3.1.0-8.i386.rpm
```

```
htmlview-4.0.0-2.el5.noarch.rpm
httpd-2.2.3-11.el5_1.3.i386.rpm
hwdata-0.213.6-1.el5.noarch.rpm
ifd-egate-0.05-15.i386.rpm
ImageMagick-6.2.8.0-4.el5_1.1.i386.rpm
info-4.8-14.el5.i386.rpm
initscripts-8.45.19.EL-1.i386.rpm
iproute-2.6.18-7.el5.i386.rpm
ipsec-tools-0.6.5-9.el5.i386.rpm
iptables-1.3.5-4.el5.i386.rpm
iptables-ipv6-1.3.5-4.el5.i386.rpm
iptstate-1.4-1.1.2.2.i386.rpm
iputils-20020927-43.el5.i386.rpm
irda-utils-0.9.17-2.fc6.i386.rpm
irqbalance-0.55-10.el5.i386.rpm
isdn4k-utils-3.2-51.el5.i386.rpm
jpackage-utils-1.7.3-1jpp.2.el5.noarch.rpm
jwhois-3.2.3-8.el5.i386.rpm
kbd-1.12-20.el5.i386.rpm
kernel-2.6.18-92.el5.i686.rpm
kernel-devel-2.6.18-92.el5.i686.rpm
kernel-headers-2.6.18-92.el5.i386.rpm
kexec-tools-1.102pre-21.el5.i386.rpm
keyutils-libs-1.2-1.el5.i386.rpm
kpartx-0.4.7-17.el5.i386.rpm
krb5-libs-1.6.1-25.el5.i386.rpm
krb5-workstation-1.6.1-25.el5.i386.rpm
ksh-20060214-1.7.i386.rpm
kudzu-1.2.57.1.17-1.i386.rpm
lcms-1.15-1.2.2.i386.rpm
less-394-5.el5.i386.rpm
lftp-3.5.1-2.fc6.i386.rpm
libacl-2.2.39-3.el5.i386.rpm
libaio-0.3.106-3.2.i386.rpm
libattr-2.4.32-1.1.i386.rpm
libcap-1.10-26.i386.rpm
libdrm-2.0.2-1.1.i386.rpm
liberation-fonts-1.0-1.el5.noarch.rpm
libevent-1.1a-3.2.1.i386.rpm
libFS-1.0.0-3.1.i386.rpm
libgcc-4.1.2-42.el5.i386.rpm
libgcrypt-1.2.3-1.i386.rpm
libgpg-error-1.4-2.i386.rpm
libgssapi-0.10-2.i386.rpm
libhugetlbfs-1.2-5.el5.i386.rpm
libICE-1.0.1-2.1.i386.rpm
libicu-3.6-5.11.1.i386.rpm
libicu-devel-3.6-5.11.1.i386.rpm
libIDL-0.8.7-1.fc6.i386.rpm
libidn-0.6.5-1.1.i386.rpm
libjpeg-6b-37.i386.rpm
libjpeg-devel-6b-37.i386.rpm
```

```
libmng-1.0.9-5.1.i386.rpm
libmng-devel-1.0.9-5.1.i386.rpm
libnl-1.0-0.10.pre5.5.i386.rpm
libnotify-0.4.2-6.el5.i386.rpm
libpcap-0.9.4-12.el5.i386.rpm
libpng-1.2.10-7.1.el5_0.1.i386.rpm
libpng-devel-1.2.10-7.1.el5_0.1.i386.rpm
libselinux-1.33.4-5.el5.i386.rpm
libselinux-python-1.33.4-5.el5.i386.rpm
libsemanage-1.9.1-3.el5.i386.rpm
libsepol-1.15.2-1.el5.i386.rpm
libSM-1.0.1-3.1.i386.rpm
libsmi-0.4.5-2.el5.i386.rpm
libstdc4.1.2-42.el5.i386.rpm
libsysfs-2.0.0-6.i386.rpm
libtermcap-2.0.8-46.1.i386.rpm
libtermcap-devel-2.0.8-46.1.i386.rpm
libtiff-3.8.2-7.el5.i386.rpm
libtool-ltdl-1.5.22-6.1.i386.rpm
libusb-0.1.12-5.1.i386.rpm
libuser-0.54.7-2.el5.5.i386.rpm
libutempter-1.1.4-3.fc6.i386.rpm
libvolume_id-095-14.16.el5.i386.rpm
libwnck-2.16.0-4.fc6.i386.rpm
libwvstreams-4.2.2-2.1.i386.rpm
libX11-1.0.3-9.el5.i386.rpm
libXau-1.0.1-3.1.i386.rpm
libXcursor-1.1.7-1.1.i386.rpm
libXdmcp-1.0.1-2.1.i386.rpm
libXext-1.0.1-2.1.i386.rpm
libXfixes-4.0.1-2.1.i386.rpm
libXft-2.1.10-1.1.i386.rpm
libXi-1.0.1-3.1.i386.rpm
libXinerama-1.0.1-2.1.i386.rpm
libxml2-2.6.26-2.1.2.1.i386.rpm
libxml2-python-2.6.26-2.1.2.1.i386.rpm
libXrandr-1.1.1-3.1.i386.rpm
libXrender-0.9.1-3.1.i386.rpm
libXres-1.0.1-3.1.i386.rpm
libxslt-1.1.17-2.i386.rpm
libXt-1.0.2-3.1.fc6.i386.rpm
libXxf86vm-1.0.1-3.1.i386.rpm
lm_sensors-2.10.0-3.1.i386.rpm
lockdev-1.0.1-10.i386.rpm
logrotate-3.7.4-8.i386.rpm
logwatch-7.3-6.el5.noarch.rpm
lrzsz-0.12.20-22.1.i386.rpm
lsof-4.78-3.i386.rpm
lvm2-2.02.32-4.el5.i386.rpm
lynx-2.8.5-28.1.i386.rpm
m2crypto-0.16-6.el5.2.i386.rpm
m4-1.4.5-3.el5.1.i386.rpm
```

```
mailcap-2.1.23-1.fc6.noarch.rpm
mailx-8.1.1-44.2.2.i386.rpm
make-3.81-3.el5.i386.rpm
MAKEDEV-3.23-1.2.i386.rpm
man-1.6d-1.1.i386.rpm
man-pages-2.39-10.el5.noarch.rpm
mcstrans-0.2.7-1.el5.i386.rpm
mdadm-2.6.4-1.el5.i386.rpm
mesa-libGL-6.5.1-7.5.el5.i386.rpm
mgetty-1.1.33-9.fc6.i386.rpm
microcode_ctl-1.17-1.47.el5.i386.rpm
mingetty-1.07-5.2.2.i386.rpm
minicom-2.1-3.i386.rpm
mkbootdisk-1.5.3-2.1.i386.rpm
mkinitrd-5.1.19.6-28.i386.rpm
mktemp-1.5-23.2.2.i386.rpm
mlocate-0.15-1.el5.i386.rpm
mod_perl-2.0.2-6.3.el5.i386.rpm
mod_ssl-2.2.3-11.el5_1.3.i386.rpm
module-init-tools-3.3-0.pre3.1.37.el5.i386.rpm
mozldap-6.0.5-1.el5.i386.rpm
mtools-3.9.10-2.fc6.i386.rpm
mtr-0.71-3.1.i386.rpm
nano-1.3.12-1.1.i386.rpm
nash-5.1.19.6-28.i386.rpm
nc-1.84-10.fc6.i386.rpm
ncurses-5.5-24.20060715.i386.rpm
ncurses-devel-5.5-24.20060715.i386.rpm
net-snmp-5.3.1-24.el5.i386.rpm
net-snmp-libs-5.3.1-24.el5.i386.rpm
net-tools-1.60-78.el5.i386.rpm
NetworkManager-0.6.4-8.el5.i386.rpm
newt-0.52.2-10.el5.i386.rpm
nfs-utils-1.0.9-33.el5.i386.rpm
nfs-utils-lib-1.0.8-7.2.z2.i386.rpm
notification-daemon-0.3.5-9.el5.i386.rpm
nscd-2.5-24.i386.rpm
nspr-4.7.0.99.2-1.el5.i386.rpm
nss-3.11.99.5-2.el5.i386.rpm
nss_db-2.2-35.3.i386.rpm
nss_ldap-253-12.el5.i386.rpm
nss-tools-3.11.99.5-2.el5.i386.rpm
ntp-4.2.2p1-8.el5.i386.rpm
ntsysv-1.3.30.1-2.i386.rpm
numactl-0.9.8-2.el5.i386.rpm
OpenIPMI-2.0.6-6.el5.i386.rpm
OpenIPMI-libs-2.0.6-6.el5.i386.rpm
openldap-2.3.27-8.el5_1.3.i386.rpm
openssh-4.3p2-26.el5.i386.rpm
openssh-clients-4.3p2-26.el5.i386.rpm
openssh-server-4.3p2-26.el5.i386.rpm
openssl-0.9.8b-10.el5.i386.rpm
```

```
ORBit2-2.14.3-4.el5.i386.rpm
pam-0.99.6.2-3.27.el5.i386.rpm
pam_ccreds-3-5.i386.rpm
pam_krb5-2.2.14-1.i386.rpm
pam_passwdqc-1.0.2-1.2.2.i386.rpm
pam_pkcs11-0.5.3-23.i386.rpm
pam_smb-1.1.7-7.2.1.i386.rpm
pango-1.14.9-3.el5.i386.rpm
pango-devel-1.14.9-3.el5.i386.rpm
paps-0.6.6-17.el5.i386.rpm
parted-1.8.1-17.el5.i386.rpm
passwd-0.73-1.i386.rpm
patch-2.5.4-29.2.2.i386.rpm
pax-3.4-1.2.2.i386.rpm
pciutils-2.2.3-5.i386.rpm
pcmciautils-014-5.i386.rpm
pcre-6.6-2.el5_1.7.i386.rpm
pcsc-lite-1.4.4-0.1.el5.i386.rpm
pcsc-lite-libs-1.4.4-0.1.el5.i386.rpm
perl-5.8.8-10.el5_0.2.i386.rpm
perl-String-CRC32-1.4-2.fc6.i386.rpm
perl-URI-1.35-3.noarch.rpm
php-5.1.6-20.el5.i386.rpm
php-cli-5.1.6-20.el5.i386.rpm
php-common-5.1.6-20.el5.i386.rpm
php-pdo-5.1.6-20.el5.i386.rpm
php-pgsql-5.1.6-20.el5.i386.rpm
pinfo-0.6.9-1.fc6.i386.rpm
pkgconfig-0.21-2.el5.i386.rpm
pkinit-nss-0.7.3-1.el5.i386.rpm
pm-utils-0.99.3-6.el5.19.i386.rpm
policycoreutils-1.33.12-14.el5.i386.rpm
popt-1.10.2-48.el5.i386.rpm
portmap-4.0-65.2.2.1.i386.rpm
postgresql-8.1.11-1.el5_1.1.i386.rpm
postgresql-docs-8.1.11-1.el5_1.1.i386.rpm
postgresql-libs-8.1.11-1.el5_1.1.i386.rpm
postgresql-server-8.1.11-1.el5_1.1.i386.rpm
ppp-2.4.4-1.el5.i386.rpm
prelink-0.3.9-2.1.i386.rpm
procmail-3.22-17.1.i386.rpm
procps-3.2.7-9.el5.i386.rpm
psacct-6.3.2-41.1.i386.rpm
psmisc-22.2-6.i386.rpm
pygobject2-2.12.1-5.el5.i386.rpm
pyOpenSSL-0.6-1.p24.7.2.2.i386.rpm
python-2.4.3-21.el5.i386.rpm
python-elementtree-1.2.6-5.i386.rpm
python-sqlite-1.1.7-1.2.1.i386.rpm
python-urlgrabber-3.1.0-2.noarch.rpm
pyxf86config-0.3.31-2.fc6.i386.rpm
PyXML-0.8.4-4.i386.rpm
```

```
qt-3.3.6-23.el5.i386.rpm
quota-3.13-1.2.3.2.el5.i386.rpm
rdate-1.4-6.i386.rpm
rdist-6.1.5-44.i386.rpm
readahead-1.3-7.el5.i386.rpm
readline-5.1-1.1.i386.rpm
readline-devel-5.1-1.1.i386.rpm
redhat-logos-4.9.16-1.noarch.rpm
redhat-lsb-3.1-12.3.EL.i386.rpm
redhat-menus-6.7.8-2.el5.noarch.rpm
redhat-release-5Server-5.2.0.4.i386.rpm
redhat-release-notes-5Server-12.i386.rpm
rhel-instnum-1.0.8-1.el5.noarch.rpm
rhn-check-0.4.17-8.el5.noarch.rpm
rhn-client-tools-0.4.17-8.el5.noarch.rpm
rhnlib-2.2.5-1.el5.noarch.rpm
rhnsd-4.6.1-1.el5.i386.rpm
rhn-setup-0.4.17-8.el5.noarch.rpm
rhpl-0.194.1-1.i386.rpm
rmt-0.4b41-2.fc6.i386.rpm
rng-utils-2.0-1.14.1.fc6.i386.rpm
rootfiles-8.1-1.1.1.noarch.rpm
rpm-4.4.2-48.el5.i386.rpm
rpm-libs-4.4.2-48.el5.i386.rpm
rpm-python-4.4.2-48.el5.i386.rpm
rp-pppoe-3.5-32.1.i386.rpm
rsh-0.17-38.el5.i386.rpm
rsync-2.6.8-3.1.i386.rpm
sed-4.1.5-5.fc6.i386.rpm
selinux-policy-2.4.6-137.el5.noarch.rpm
selinux-policy-targeted-2.4.6-137.el5.noarch.rpm
sendmail-8.13.8-2.el5.i386.rpm
sendmail-cf-8.13.8-2.el5.i386.rpm
setarch-2.0-1.1.i386.rpm
setools-3.0-3.el5.i386.rpm
setserial-2.17-19.2.2.i386.rpm
setup-2.5.58-1.el5.noarch.rpm
setuptool-1.19.2-1.i386.rpm
shadow-utils-4.0.17-13.el5.i386.rpm
slang-2.0.6-4.el5.i386.rpm
smartmontools-5.36-4.el5.i386.rpm
sos-1.7-9.2.el5.noarch.rpm
specspo-13-1.el5.noarch.rpm
sqlite-3.3.6-2.i386.rpm
squid-2.6.STABLE6-5.el5_1.3.i386.rpm
startup-notification-0.8-4.1.i386.rpm
strace-4.5.16-1.el5.1.i386.rpm
stunnel-4.15-2.i386.rpm
sudo-1.6.8p12-12.el5.i386.rpm
svrcore-4.0.4-3.el5.i386.rpm
symlinks-1.2-24.2.2.i386.rpm
sysfsutils-2.0.0-6.i386.rpm
```

```
sysklogd-1.4.1-44.el5.i386.rpm
syslinux-3.11-4.i386.rpm
system-config-network-tui-1.3.99.10-2.el5.noarch.rpm
system-config-securitylevel-tui-1.6.29.1-
   2.1.el5.i386.rpm
SysVinit-2.86-14.i386.rpm
talk-0.17-29.2.2.i386.rpm
tar-1.15.1-23.0.1.el5.i386.rpm
tcl-8.4.13-3.fc6.i386.rpm
tcpdump-3.9.4-12.el5.i386.rpm
tcp_wrappers-7.6-40.4.el5.i386.rpm
tcsh-6.14-12.el5.i386.rpm
telnet-0.17-39.el5.i386.rpm
termcap-5.5-1.20060701.1.noarch.rpm
time-1.7-27.2.2.i386.rpm
tmpwatch-2.9.7-1.1.el5.1.i386.rpm
traceroute-2.0.1-3.el5.i386.rpm
tree-1.5.0-4.i386.rpm
ttmkfdir-3.0.9-23.el5.i386.rpm
tzdata-2007k-2.el5.noarch.rpm
udev-095-14.16.el5.i386.rpm
unix2dos-2.2-26.2.2.i386.rpm
unixODBC-2.2.11-7.1.i386.rpm
unzip-5.52-2.2.1.i386.rpm
urw-fonts-2.3-6.1.1.noarch.rpm
usbutils-0.71-2.1.i386.rpm
usermode-1.88-3.el5.1.i386.rpm
util-linux-2.13-0.47.el5.i386.rpm
valgrind-3.2.1-6.el5.i386.rpm
vconfig-1.9-2.1.i386.rpm
vim-common-7.0.109-3.el5.3.i386.rpm
vim-enhanced-7.0.109-3.el5.3.i386.rpm
vim-minimal-7.0.109-3.el5.3.i386.rpm
vixie-cron-4.1-72.el5.i386.rpm
vsftpd-2.0.5-12.el5.i386.rpm
wget-1.10.2-7.el5.i386.rpm
which-2.16-7.i386.rpm
wireless-tools-28-2.el5.i386.rpm
wireshark-0.99.7-1.el5.i386.rpm
words-3.0-9.noarch.rpm
wpa_supplicant-0.4.8-10.2.el5.i386.rpm
wvdial-1.54.0-5.2.2.1.i386.rpm
Xaw3d-1.5E-10.1.i386.rpm
xmlsec1-1.2.9-8.1.i386.rpm
xorg-x11-filesystem-7.1-2.fc6.noarch.rpm
xorg-x11-fonts-ISO8859-1-75dpi-7.1-2.1.el5.noarch.rpm
xorg-x11-font-utils-7.1-2.i386.rpm
xorg-x11-proto-devel-7.1-9.fc6.i386.rpm
xorg-x11-xfs-1.0.2-4.i386.rpm
ypbind-1.19-8.el5.i386.rpm
yp-tools-2.9-0.1.i386.rpm
yum-3.2.8-9.el5.noarch.rpm
```

```
yum-metadata-parser-1.1.2-2.el5.i386.rpm
yum-rhn-plugin-0.5.3-6.el5.noarch.rpm
yum-security-1.1.10-9.el5.noarch.rpm
yum-updatesd-0.9-2.el5.noarch.rpm
zip-2.31-1.2.2.i386.rpm
zlib-1.2.3-3.i386.rpm
zlib-devel-1.2.3-3.i386.rpm
```

Index