Avaya Video Communications Systems Administrator Guide

Avaya 1050, Avaya 1040, Avaya 1030

Issue 1

June 2010

Notices

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

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

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Shrinkwrap License (SR). Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License"). (see "Third Party Components" for more information).

Copyright

Third Party Components

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

Preventing toll fraud

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

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States

and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com

Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya and Aura are trademarks of Avaya, Inc.

Avaya is a registered trademark of Avaya Inc.

Avaya Aura is a trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

Downloading documents

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

Contact Avaya Support

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

Patent Notice

For patents covering LifeSize® products, refer to http://www.lifesize.com/support/legal.

Welcome to Avaya Video Communications Systems

This guide explains how to administer and locally configure the Avaya video conferencing systems:

- Avaya 1030
- Avaya 1040
- Avaya 1050

For information about administering Avaya 1010 and Avaya 1020 video conferencing systems, refer to the *Avaya 1020 and 1020 Video Conferencing Systems Administrator Guide*.

For information about how to install and physically connect an Avaya video conferencing system, refer to the installation guide for your Avaya video conferencing system model.

Avaya 1030, 1040, and 1050 video conferencing systems connect to Avaya Aura™ Session Manager. Please refer to Administering Avaya Aura Communication Manager for Avaya Aura Session Manager for details about how to administer these video systems on Avaya Aura Session Manager.

Related documentation is available from the documentation CD included with the product and from support.avaya.com. Release Notes, technical notes and technical reference publications are available from support.avaya.com.

Note: Avaya 1030, 1040, and 1050 video conferencing systems are not administrable on H.323 video gatekeepers.

Accessing Administrative Features

You can manage your Avaya video communications system using the remote control or remotely using a web browser, telnet session, or secure shell (SSH) session.

Administration Using the Remote Control

To access administrator preferences for configuring the system using the remote control, follow these steps:

1. From the main screen of the user interface, press the ◉ button on the remote control to access the **System Menu**.

2. Select **Administrator Preferences** and press **OK**.

3. Enter the administrator password and press **OK**.

   Note: The default administrator password is 1 2 3 4. To change the administrator password, refer to "Changing the Administrator Password" on page 6. If you enter an incorrect password, press the ↶ button on the remote control to clear the **Login Attempt Failed** message.

Administration from a Web Browser

To configure your Avaya system from a web browser, you must have Adobe Flash Player installed and configured on your web browser. You can download the Flash Player from **www.adobe.com**.

By default, remote access to an Avaya system through a web browser is enabled. To disable remote access through a web browser, select *Disabled* for the **HTTP** preference in **Administrator Preferences : Security : General**.

To access the web administration interface, follow these steps.

1. Open a web browser and enter the IP address of the Avaya system in the web address field. The IP address of the system appears at the top of the main screen in the user interface.

   A login screen appears.

   Note: This is a secure Internet connection, and you may receive an unknown certificate warning.

2. In the login screen, do the following:

   a. Choose the language in which to display the interface.

   b. Enter the administrator password.

   c. Click **Submit**.

3. When you are finished administering the system, click the **Log out** button at the bottom of the screen, and then close your web browser.

Configuring Security Preferences

You can set preferences in **Administrator Preferences : Security** to control remote access to the system through the web, telnet, SSH sessions, and SNMP.

Controlling Remote Administration

By default, remote access to an Avaya system through the web (HTTP), SSH, and SNMP is enabled; remote access through a telnet session is disabled. To enable or disable remote access through any of these mechanisms, configure the **HTTP**, **SSH**, **Telnet**, and **SNMP** preferences in **Administrator Preferences : Security : General**.

Changing the Administrator Password

Avaya recommends that you protect the administrator preferences with a secure password to prevent occasional users from changing them. To change the administrator password, follow these steps:

1. From the **System Menu**, access **Administrator Preferences : Security : Passwords**.
2. Enter a new password in the **New Password** field below **Administrator Password** and press **OK**.

   Note: If you did not change the administrator password during initial configuration, the default password is 1 2 3 4.

3. Re-enter the new password in the **Confirm Password** field and press **OK**.
4. Select the **Set New Password** button and press **OK**.

Setting the User Password

You can set a user password to control access to **User Preferences** screens. By default, the user password is not set.

Note: If you set a user password, you can also access the **User Preferences** screens with the administrator password.

To set the user password, follow these steps:

1. From the **System Menu**, access **Administrator Preferences** : **Security** : **Passwords**.
2. Enter a new password in the **New Password** field below **User Password** and press **OK**.
3. Re-enter the new password in the **Confirm Password** field and press **OK**.
4. Select the **Set New Password** button and press **OK**.

Specifying a Locally Configured IP Address

Dynamic Host Configuration Protocol (DHCP) is used to dynamically allocate and assign IP addresses. DHCP allows you to move network devices from one subnet to another without administrative attention. You can choose to enable DHCP if a DHCP server is present. If you disable DHCP, you must enter an IP address (the locally configured IP address if not assigned by a DHCP server), subnet mask (used to partition the IP address into a network and host identifier), and gateway (IP address of the default gateway the system uses).

Configuring Avaya Systems Using DHCP

If an Avaya video communications system obtains its IP address using DHCP (the default), it can accept an option from the DHCP server that specifies a location and file from which the system can obtain configuration information. The file can be located on a web server, trivial file transfer protocol (TFTP) server, or file transfer protocol (FTP) server. Each time the system boots, it attempts to fetch the configuration file specified by the option. If the configuration file has changed since the last time it was applied, the system applies the configuration file before the boot process continues. The following prerequisites must be met to enable this feature:

- The **DHCP** preference in **Administrator Preferences : Network : General** on the Avaya system must be set to *Enabled*.
- An Avaya system accepts site-specific option 157 for this feature. You must configure this option on the DHCP server.

  Note: If you configure a system using DHCP option 157 and specify a TFTP server as the source from which to obtain the configuration file, the system accepts the download through port 5351. Ensure that firewalls between the system and the TFTP server are configured to allow the download through this port.

Configuring the DHCP Option

Specific configuration details of DHCP servers for use with this feature vary depending on the DHCP server used and your environment. The scope of this section is limited to describing the format of site-specific option 157, which Avaya video communications systems can accept from a DHCP server to obtain a configuration file.

An Avaya system can accept site-specific option 157 from the DHCP server if you configure the option as a string with the following format:

```
“Avaya: server=<path>”
```

where *<path>* is a one or more URLs separated by a semicolon and that specifies the location to a configuration file. Supported protocols include TFTP, FTP, and HTTP. If the path contains more than one URL, the Avaya system tries the URLs in the order listed and uses the first file that exists.

Example:

If the path is:

```
http://example/config/fishtank.cfg;ftp://example/other/fishtank.cfg
```

the system attempts to obtain the configuration file `fishtank.cfg` from the web server at http://example/config/fishtank.cfg. If the file does not exist at that location, the system attempts to obtain the configuration from the FTP server at ftp://example/other/fishtank.cfg.

Note: If the server requires a username and password to access the file, for example to log into an FTP server, you can include the user name and password in the URL. For example:

```
ftp://<username>:<password>@example/other/fishtank.cfg
```

where <*username*> is the user name and <*password*> is the password required for the login. The user name and password must not contain a semicolon.

Each URL can also contain the following escapes to make the configuration unique to the system:

Escape	**Replacement Value**
#M	Replaced with the MAC address using the underscore character to replace the colon between bytes. The MAC address resolves to a hexadecimal number with lower-case letters.
#S	Replaced by the system model as follows: 1050 1040 1030
#I	Replaced by the assigned IP address.

If a machine name or IP address is used alone as a path element, then the following path is substituted:

```
tftp://<name>/#M.cfg;tftp://<name>/#S.cfg
```

where <*name*> is the IP address or DNS name in the path.

Example:

For a system with a MAC address of 00:13:FA:00:12:33 and an IP address of 10.10.22.77, the path:

```
http://example/configs/fishtank.cfg;example;ftp://example/#I.cfg
```

resolves to search for a configuration file at the following locations:

1. `http://example/configs/fishtank.cfg`
2. `tftp://example/00_13_fa_00_12_33.cfg`
3. `tftp://example/room.cfg`
4. `ftp://example/10.10.22.77.cfg`

Note: The MAC address resolves to a hexadecimal number with lower-case letters. In the previous example, the MAC address 00:13:FA:00:12:33 is replaced with 00_13_fa_00_12_33. If you specify a path that uses the #M escape, ensure that the file name of the configuration file contains lower-case letters.

The first file found is used. If the checksum of the file is different from the last configuration file loaded into the system, then the new file is used.

Note: Setting preferences that result in a system reboot, for example port ranges or SIP preferences, may cause the system to reboot once the configuration file is loaded into the system. Because the checksum for the configuration file in this case is the same, the file is not loaded again. The actual configuration changes are applied when the system is fully booted. This may cause previous configuration preferences to appear in the user interface, for example a previous system name, before the configuration takes effect.

Specifying the Hostname and Domain Name Service (DNS) Servers

You can enter the hostname of the system and the IP addresses to configure DNS servers. You can also enter the domain names to search when resolving hostnames. Domain Name System (DNS) translates names of network nodes into addresses; specify this preference to use DNS to resolve the hostnames of devices to IP addresses.

Specifying Network Speed

If you choose an option other than *Auto* for the **Administrator Preferences : Network : Network Speed** preference, ensure that it matches the speed and duplex configured on your network switch.

Note: If your Ethernet switch is configured for half duplex, you may experience poor quality video when placing calls greater than 512 Kb/s.

Specifying a VLAN Tag

If you have static virtual local area networks (VLANs) configured in your environment, you can configure your Avaya system to apply a VLAN tag to outgoing packets and only accept incoming tagged packets that have the same VLAN identifier. To enable this feature, navigate to **Administrator Preferences : Network : General : VLAN Tag** and specify the VLAN identifier of the VLAN to which the system is assigned. The value is a number in the range 1 through 4094.

Note: If you set or modify the **VLAN Tag** preference, the system reboots when you navigate to another screen.

Specifying an NTP Server

The system date and time appear in the user interface and are automatically set if one of the following conditions exists:

- The **Administrator Preferences : Network : General : DHCP** preference is set to *Enabled*, and the DHCP server can pass an NTP server address to your system.

  - or -

- The hostname or IP address of an NTP server is specified in **Administrator Preferences : Network : General : NTP Server Hostname**.

  Note: An NTP server address that a DHCP server passes to your system overrides an NTP server hostname or address specified in the **NTP Server Hostname** preference.

The **System Information** page displays the IP address of the NTP server that the system uses.

Note: The time zone is not set automatically. If you did not specify the time zone for your system during the initial configuration, the time that appears in the user interface may not be correct. To specify the time zone manually, refer to "Manually Setting System Date and Time" on page 16.

Restricting Reserved Ports

By default, Avaya systems communicate through TCP and UDP ports in the range 60000 - 64999 for video, voice, presentations, and camera control. Avaya systems use only a small number of these ports during a call. The exact number depends on the number of participants in the call, the protocol used, and the number of ports required for the type (video or voice) of call.

To minimize the number of UDP and TCP ports that are available for communication, you can restrict the range by entering values in **Administrator Preferences : Network : Reserved Ports**. Avaya recommends that the range you choose, if other than a subset of the default range, begins with a port number greater than 10000.

Note: Changing the TCP range causes an automatic reboot of the system.

SIP two-way call required ports:

Call Type	Number of Required UDP Ports
Video[a]	6 UDP ports
Voice[b]	2 UDP ports

[a] Each additional video participant requires 6 UDP ports.

[b] Each additional voice participant requires 2 UDP ports.

Configuring Quality of Service

You can specify network Quality of Service (QoS) settings in the **Administrator Preferences : Network : Network QoS** preferences. Set these preferences according to the settings used in your network.

Note: Network QoS preferences are supported with IPv4 addressing only.

You can specify DiffServ (differentiated services) or IntServ (integrated services) values for audio, video, and data packets. You can also set the IntServ Type of Service (ToS) preference. By default, **Network QoS** and **IntServ ToS** are set to *None*.

Configuring Communications Preferences

You can specify options that control which protocols the system uses during calls by configuring preferences in **Administrator Preferences : Communications**.

Disabling Multiway Calling

You can disable multiway calling on Avaya systems by choosing *Disabled* for the **Multiway Calls** preference in **Administrator Preferences : Communications : General**. The default, *Enabled*, allows users to place multiway calls up to the maximum number supported by the system. You can configure this preference only when the system is not in a call. Choosing *Disabled* allows only one call, voice or video, to connect to the system.

If the system includes an embedded multipoint bridge, the *One Video + One Voice* option also appears for this preference. This option allows the system to connect to both a video and a voice call as the maximum number of connected callers.

Configuring Dialing Options

You can choose voice and video dialing options during the initial configuration, when performing a system reset, or at any other time by accessing **Administrator Preferences : Communications : General**. Refer to the Installation Guide for your Avaya system model for more information about these preferences.

Enabling Presentations

Users can share data during a call through a secondary H.239 media channel, typically from a laptop or personal computer that is connected to the appropriate input on the Avaya codec. By default, the presentation function is enabled on an Avaya system. To disable presentations access **Administrator Preferences : Communications : General : Presentations**. Consider disabling the presentation function if your system experiences interoperability issues with third party systems that do not support presentations.

Note: When presentations are disabled for all participants during a call, the user interface offers the user the option to send video from the presentation input as the primary video stream. Refer to the *Avaya Video Communications Systems User Guide* for more information about presentations and selecting primary and presentation inputs.

Manually Starting a Presentation

If the **Presentations** preference is set to *Enabled* (the default), a presentation starts automatically during a call if a user connects a video input device other than an Avaya Video Camera 150, Avaya Video Camera 200, or Avaya Video Camera 100 to the codec and the video input device is not selected as the primary input. The user interface switches the presentation input to this video input and starts the presentation. The presentation stops automatically if the video input device is disconnected during the call. You can choose *Manual* for the **Auto Start Presentation** preference in **Administrator Preferences : Communications : General** to allow users to start a presentation manually.

Supported VGA and DVI-I Input Resolutions

Avaya systems support native 16:9 and 4:3 VGA and DVI-I inputs. The **System Information** screen shows the actual VGA or DVI-I input size for **VGA Input** or **DVI-I Input**. The input selector shows a 16:9 or 4:3 window for the input depending on the aspect ratio.

The resolutions are sent natively to the far end for the primary or secondary video streams. These resolutions are supported only with a screen refresh rate set to 60 Hertz on the device connected to the VGA or DVI-I input.

Following are the supported input resolutions and frame rates for video sent to the DVI-I input from an HDMI source:

- 480p60
- 576p50
- 720p60
- 1080p30 (available only on Avaya systems that support 1080p30 output)

If audio is sent to the DVI-I input from an HDMI source, the audio is sent to the near end speakers and to the far end when the DVI-I input is selected as the primary or presentation video input.

For more information about configuring the DVI-I input, refer to "Configuring HD In and DVI-I In" on page 27.

Configuring SIP Settings

By default, support for Session Initiation Protocol (SIP) is enabled on Avaya systems. To configure SIP as the protocol to use for placing calls, configure SIP preferences in **Administrator Preferences : Communications : SIP**. You can also disable support for SIP by choosing *Disabled* for the **SIP** preference when the system is not in a call. If you choose *Disabled* for the **SIP** preference, the system cannot place or receive calls with the SIP protocol.

For the server, enter the username, SIP server authorization name, and password for the device, if required.

When you select the **Register** button and press **OK**, icons appear in the status bar to indicate the status of the registration process with the SIP server. The yellow SIP icon SIP appears when your Avaya system is trying to register with the SIP server. If the registration fails, the red SIP icon SIP appears.

To navigate to the second page of SIP preferences, press ● on the remote control.

You can change the SIP UDP signaling port. You can also enable TCP signaling and change the TCP signaling port.

Note: The system reboots if you change the UDP signaling port, enable or disable TCP or TLS signaling, or change the TCP or TLS signaling ports.

Configuring System Settings

You can change settings that identify the system to users in the user interface, set the system date and time, check for updates to license keys, and reset the system to its factory default settings by accessing **Administrator Preferences : System**.

Identifying the System

To change the system name, dialing numbers, and geographic location specified for the system, access **Administrator Preferences : System : Identification**.

Manually Setting System Date and Time

You can set the system date and time manually as follows:

1. From the **System Menu**, access **Administrator Preferences : System : Date and Time**.
2. Set the time zone.
3. Set the month, day, and year for the date.
4. Set the hour, minute, and second for the time.
5. Select the **Set Date and Time** button and press **OK** to save your changes.

Restoring Default Settings

Administrator preferences contain the configuration of the entire system. You may need to reset the system to its default state to correct unknown problems you may be experiencing or to return to a known configuration. You can reset the system from the user interface or manually with the **Reset** button on the back of the codec.

Resetting a System from the User Interface

To reset the system from the user interface, follow these steps:

1. From the **System Menu**, access **Administrator Preferences : System : System Reset**.
2. Enter the administrator password.

The system automatically reboots and the administrator password is reset to the default value (1 2 3 4). The user password also resets to a blank password, enabling users to access **User Preferences** without a password. The **Initial Configuration** screen appears. You must complete the initial configuration screens to complete the reset.

Note: If you reset the system using a remote access method, you must complete the reset from the user interface by navigating the initial configuration screens and pressing **OK** on the remote control when prompted to save the configuration.

Resetting a System Using the Reset Button

If this reset fails or if you do not have access to the user interface, you can manually reset the system using the **Reset** button on the back of the codec.

Using the Reset Button on Avaya 1030, Avaya 1050, and Avaya 1040:

If you are using an Avaya 1030, Avaya 1050, or Avaya 1040, you can use the reset button without removing power to the system. Press and hold the reset button. The blue LED on the front of the codec changes color or behavior approximately every five seconds until the LED turns solid blue. The following table indicates the sequence of color and behavior changes that the LED exhibits and the corresponding effect on the system when you release the reset button.

When the LED is This Color:	Release the Reset Button to Get This Result:
blue and red **Note**: The LED may remain in this state for more than 5 seconds. Depending on your viewing angle, the LED may appear purple.	The system reboots without changes to the configuration.
solid red	The system reboots without changes to the configuration.
flashing blue (longer duration on than off)	The system reboots and resets preferences to their default settings.
flashing blue (shorter duration on than off)	The system reboots at the initial configuration using the alternate software image installed on the system and resets values to default settings.
solid blue	If you release the reset button when the LED turns solid blue the system stops and does not reboot. Continue to hold the reset button until the system reboots (approximately 5 to 10 seconds after the LED turns solid blue). The system reboots without changes to the configuration.

Configuring Call Preferences

All users can set auto answer options for calls and specify the maximum number of entries to appear in the **Redial** list. Refer to the *Avaya Video Communications Systems User Guide* for more information.

Administrators can configure the maximum call time and bandwidth in **Administrator Preferences : Calls**.

Managing Bandwidth

You can specify the maximum bandwidth that an outgoing or incoming call uses by setting the **Outgoing Maximum Bandwidth** and **Incoming Maximum Bandwidth** preferences in **Administrator Preferences : Calls**. The value that you choose for the **Outgoing Maximum Bandwidth** becomes the maximum value that users can choose in the user interface when placing a call by dialing a number manually or when specifying a bandwidth in a directory entry. If a user specifies *Auto* for the bandwidth when placing a call, the maximum outgoing bandwidth becomes the starting point for negotiating bandwidth when the call connects.

If you choose *Auto* as the value for the **Outgoing Maximum Bandwidth** and **Incoming Maximum Bandwidth** preferences and the user chooses *Auto* for the bandwidth when placing the call, the system places the call at 1152 kb/s. An exception occurs when you set the display resolution to a 1080i or 1080p resolution in **Administrator Preferences : Appearance : Displays** on Avaya systems that support these resolutions with Avaya Video Camera 200. In this case, the system places the call at 1728 kb/s.

The **Auto Bandwidth** preference addresses how the system responds to packet loss during a call. When set to *Enabled*, the default, the system attempts to use the best available bandwidth after the call connects.

Selecting a Maximum Call Time

You can control the amount of time that a call stays connected by selecting an option for the **Maximum Call Time** preference in **Administrator Preferences : Calls**.

Controlling REDIAL List Entries and Auto Answer Options

Users and administrators can control the number of entries that appear in the **REDIAL** list and how the system answers calls in **User Preferences** and **Administrator Preferences : Calls**. Refer to the *Avaya Video Communications Systems User Guide* for more information.

Enabling Telepresence

You can configure an Avaya system for use in telepresence rooms in which a conference administrator controls calls from a control panel (such as Avaya System Manager or the Call Manager in the web administration interface) and users interact with the system using an attached phone.

Enabling telepresence removes the user interface from view. When the system is idle, only the background image appears in the display. An administrator can access the user interface by pressing **OK** and entering the administrator password.

During a call, users see the video from the call and the mute indicators. The navigation bar, PIP windows, caller ID information, and call status messages do not appear on the screen.

Users can invoke the **Call Manager** dialog and call statistics and choose video inputs with the remote control. The numeric keys on the remote control play touch tones. Users can change this behavior from the **Call Manager**.

To enable or disable telepresence and lock or unlock cameras, configure preferences in **Administrator Preferences : Telepresence**.

Configuring Audio Behaviors

You can adjust audio behaviors by configuring preferences in **Administrator Preferences : Audio**.

Configuring Audio Codec Order

To change the order of available audio codecs for the system to use to place calls, select the **Audio Codec Order** preference, select a codec, and press the right arrow to move the entry up in the list or press the left arrow to move the entry down in the list.

Selecting the Active Microphone

Avaya video communications systems can connect to more than one microphone device for audio input during calls (for example, an Avaya Video Conference Phone 1000, Avaya Video Camera 100, and on codecs with a microphone in connector, an Avaya Video MicPod 1000). Only one of these devices can function as the active microphone during a call.

To select a device to serve as the active microphone, navigate to **Administrator Preferences : Audio** and select a device in the **Active Microphone** preference. The options that are available for the **Active Microphone** preference depend on the Avaya system model as follows:

Active Microphone Options	Avaya Model
Auto (default)	All models
Phone	All models
Microphone In	All models
Microphone In (no AEC)	All models
Line In	Avaya 1030
Line In (no AEC)	Avaya 1030
Line In 1	Avaya 1050 Avaya 1040
Line In 1 (no AEC)	Avaya 1050 Avaya 1040
Line In 2	Avaya 1050 Avaya 1040
Line In 2 (no AEC)	Avaya 1050 Avaya 1040
Camera 1	Avaya 1050 Avaya 1040

The *Microphone In (no AEC)* and *Line In (no AEC)* options are for connecting microphones that have their own acoustic echo canceller.

Camera options are for specifying Avaya Video Camera 100 as the active microphone.

When the **Active Microphone** preference is set to *Auto* (the default), or if the option selected is not connected to the codec, the system automatically attempts to select a device based on the following priority order:

Avaya Model	Default Order for Active Microphone Selection
Avaya 1030	1. Phone 2. Microphone In
Avaya 1050 Avaya 1040	1. Phone 2. Microphone In 3. Camera 1

When the **Active Microphone** preference is set to *Auto* the following conditions apply:

- An Avaya system ignores audio input from an Avaya Video MicPod 1000 connected to the microphone input if an Avaya Video Conference Phone 1000 is also connected to the system. The Avaya Video Conference Phone 1000 becomes the active microphone and the LEDs on the Avaya Video MicPod 1000 flash red to indicate an invalid configuration. To stop the LEDs from flashing red, either disconnect the Avaya Video MicPod 1000 or enable audio input from the Avaya Video MicPod 1000 by setting **Administrator Preferences : Audio : Active Microphone** to *Microphone In.*
- The system does not automatically choose Line In.

Adjusting the Active Microphone Volume

You can adjust the audio level for the active microphone by selecting **Active Microphone Volume** and pressing **OK** on the Avaya remote control.

Note: If you choose Avaya Video Conference Phone 1000 as the active microphone, the **Active Microphone Volume** preference is not available. The Avaya Video Conference Phone 1000 microphones adjust volume automatically.

An audio meter appears below **Active Microphone Volume** when you access the preference. The audio meter shows the level of the transmitted voice in decibels (dB) root mean square (RMS) below digital full scale (DFS). The meter is accurate to ± 1 dB. The maximum level is 0 dB. Levels below –50 dB are not displayed, and indicate a very quiet or inactive input. Typical levels during a call peak around –28 to –22 dB DFS. A detailed explanation of how the audio meter functions on an Avaya system and recommended settings for the **Active Microphone Volume** preference appear in the installation guide for your Avaya system model.

Checking Microphone Status in the System Information Page

The **Active Microphone** field in the **System Information** page shows which device is functioning as the active microphone. When the value is **None**, the No Active Microphone indicator appears in the status bar of the user interface indicating that no active microphone is available.

Note: If you choose a line in option as the active microphone, and a device is not connected to line in on the codec, the No Active Microphone indicator does not appear in the user interface and the **System Information** page shows line in as the status for **Active Microphone**.

The **Microphone In** field appears in the **System Information** page for systems that have a microphone in connector on the codec and indicates the connection status of a device for the input (*None*, *Ready*, or *Error*).

Configuring Audio In (Line In)

An Avaya system automatically sends audio from a device connected to line in on the codec to line out, except when line in is selected for the **Active Microphone** preference. Line in is mono when selected as the active microphone for the **Active Microphone** preference.

Users and administrators can set the volume of line in using the **Line In Volume** preference in **User Preferences** or **Administrator Preferences : Audio**.

Note: The **Line In Volume** preference is not available for selection if the **Active Microphone** preference is set to a line in option.

Two line in connectors are available on Avaya 1050, and Avaya 1040. Use the **Line In 1 Association** and **Line In 2 Association** preferences in **Administrator Preferences : Audio** to select the video input to associate with these inputs. If you choose *Any Input*, the device attached to the line input is always audible. If you choose a specific video input from the preference options, the device attached to the line input is only audible when the video image from the selected video input appears in the display. If you select line in as the active microphone, its associated video input is automatically set to *Any Input* and you must use the *Active Microphone Volume* preference to adjust the volume for the line input.

Testing Primary Audio Output

You can send an audio test tone to speakers that are connected to the codec as the primary audio output device. Navigate to **Administrator Preferences : Audio : Primary Audio Output Test**. Select a channel to test, or select *Auto*. The *Auto* option cycles through all available channels, playing the test tone for 5 seconds before moving to the next available channel. To end the test, choose *Off* or navigate to another preference or screen.

On Avaya 1030, Avaya 1050, and Avaya 1040, primary audio test tones output through line out and HD video out of Display 1.

Muting Audio Inputs

By default, when you press the mute button on the remote control or on an Avaya audio input device, all audio inputs to the system are muted, including audio from the active microphone, a PC connected to the codec for a presentation, or a device connected to auxiliary inputs if available on the codec. You can configure the system to mute only the active microphone by selecting *Active Microphone Only* for the **Audio Mute** preference in **Administrator Preferences : Audio**. The default is *All Inputs*. Users can discover which option is selected for this preference by viewing the **Audio Mute** field in the **System Information** page.

Selecting Audio Output

By default, audio in a voice call is sent to the Avaya Video Conference Phone 1000 attached to the Avaya codec. If you want the audio in a voice call to be sent to the line out, set the preference in **Administrator Preferences : Audio : Voice Call Audio Output.** If Avaya Video Conference Phone 1000 is not connected to the Avaya codec, audio in a voice call is sent to the line out regardless of the preference selected.

By default, audio in a video call is sent to the line out (typically, your display). If you want audio in a video call to be sent to the attached phone, set the preference in **Administrator Preferences : Audio : Video Call Audio Output**.

Adjusting Audio Levels

In addition to adjusting the audio volume for line in and the active microphone, you can adjust levels associated with the following preferences:

- **Line Out Treble** (dB)—Select to adjust the higher frequencies in the sound range for the audio line output.
- **Line Out Bass** (dB)—Select to adjust the lower frequencies in the sound range for the audio line output.
- **Ring Tone Volume**—Select the volume level of the ring and busy tones.
- **DTMF Tone Volume—**Select the volume level of the DTMF and key click tones.
- **Status Tone Volume**—Select the volume level of status tones.

Configuring Video Behaviors

Administrators can adjust video behaviors to control cameras and video quality by configuring preferences in **Administrator Preferences : Video**.

Controlling Camera Use by Far End Users

To prevent far end users from controlling your near end camera, including configuring and controlling camera presets, choose *Disabled* for the **Administrator Preferences : Video : Video Control : Far Control of Near Camera** preference. If you choose *Enabled*, you can still prevent far end users from configuring and using near end camera presets by choosing *Disabled* for the **Far Set of Camera Presets** and **Far Move to Camera Presets** preferences.

Locking Camera Presets

By default, all users can configure pan, tilt, and zoom camera presets. To prevent all users (near and far end) from configuring camera presets, select *Locked* for the **Administrator Preferences : Video : Video Control : Camera Presets Lock** preference. To prevent only far end users from configuring camera presets, choose *Disabled* for the **Far Control of Near Camera** or **Far Set of Camera Presets** preferences.

Controlling Camera Pan Direction

You can define the pan direction of the camera relative to the physical arrangement of the camera by setting **Administrator Preferences : Video : Video Control : Camera Pan Direction**. Select *Perceived* for the camera to pan left or right from the user’s perspective, when facing the camera. Select *Reversed* for the camera to pan to the camera’s actual left or right.

Controlling Digital Zoom

Digital zoom electronically crops an area of the video image that appears in the display using the same aspect ratio as the original image and then scales the cropped image to the dimensions of the original image. Digital zoom is available with Avaya Video Camera 100 and Avaya Video Camera 150 connected to Avaya 1050 and Avaya 1040.

Digital zoom is available with Avaya Video Camera 150 only after the camera’s longest focal length with optical zoom has been reached. Camera presets are not supported with Avaya Video Camera 150 while using digital zoom. Using a camera preset while in digital zoom returns the camera to optical zoom.

Note: Image quality may degrade when using digital zoom.

By default, digital zoom is disabled. You can enable this feature by choosing *Enabled* for the **Digital Zoom** preference in **Administrator Preferences : Video : Video Control**.

For information about using digital zoom, refer to the *Avaya Video Communications System User Guide*.

Controlling Video Snapshots in the Web Administration Interface

You can save video snapshots in .jpg format of video from the near and far cameras only from the **Call Manager** in the web administration interface. By default, video snapshots are enabled. To disable video snapshots select *Disabled* for the **Video Snapshot** preference in **Administrator Preferences : Video : Video Control**. You can also disable or enable video snapshots in the **Call Manager** in the web administration interface. For more information about video snapshots, refer to "Saving Video Snapshots" on page 37.

Specifying Primary and Presentation Input Defaults

You can specify a default input for the primary input and the presentation input using the **Default Primary Input** and **Default Presentation Input** preferences in **Administrator Preferences : Video : Video Control**. The user interface resets to show the selected default input when a call is answered after the system was idle and when the call terminates. This ensures that the default input is always selected when a call starts. Users can change the inputs before or during a call. If you choose *Manual* for these preferences, the user interface shows the last input selected by the user and does not automatically change the inputs.

If you choose *Auto* (the default) for the **Default Presentation Input** preference, the system chooses the device connected to the VGA or DVI-I input on the codec.

If you choose *Auto* (the default) for the **Default Primary Input** preference, the system chooses a default input device in the following order:

Avaya Model	Input Priority
Avaya 1030	HD Input 1
Avaya 1040	1. HD Input 1 (if connected to Avaya Video Camera 200) 2. HD Camera 1 (Avaya Video Camera 150 or Avaya Video Camera 100 connected to the port labeled **Avaya Camera Only** or **System Camera Only**) 3. HD Input 1 (connected to a device other than an Avaya Video Camera 200)
Avaya 1050	1. HD Input 1 (if connected to Avaya Video Camera 200) 2. HD Input 2 (if connected to Avaya Video Camera 200) 3. HD Camera 1 (Avaya Video Camera 150 or Avaya Video Camera 100 connected to the port labeled **System Camera Only**) 4. HD Input 1 (connected to a device other than an Avaya Video Camera 200)

Customizing Input Device Names

You can define custom input names by changing the default values for the following preferences in **Administrator Preferences : Video : Video Control**. Customized names for inputs are limited to 16 characters.

Preference	Support	Default
HD Camera 1 Name	Avaya 1050 Avaya 1040	HD Camera 1
HD Input 1 Name	Avaya 1030 Avaya 1050 Avaya 1040	HD 1
HD Input 2 Name	Avaya 1050	HD 2
Auxiliary Video Input Name	Avaya 1050	DVD
DVI-I Input Name	Avaya 1030 Avaya 1040 Avaya 1030	PC

Configuring HD In and DVI-I In

If your Avaya system has one or more HD inputs or a DVI-I input on the codec, you may need to adjust the **HD Input Type** and **DVI-I Input Type** preferences in **Administrator Preferences : Video : Video Control**. The default option *Auto* works with most devices. If no video image or a solid colored image appears from the HD device attached to the HD input on the codec, choose the *DVI* option for this preference.

Note: Choosing the DVI option forces the Avaya system to only use DVI video and ignore any audio input. To work around this issue, connect the audio from the attached HD device to the line in port on the back of the codec.

Controlling Video Stretch

You can ensure that users always see 4:3 aspect ratio presentation input or received presentation video in 16:9 aspect ratio by selecting *Enabled* for the **Stretch Video** preference in **Administrator Preferences : Video : Video Control**. The default is *Disabled*.

Note: Setting this preference to *Enabled* has no effect if the resolution of either display connected to the system is set to 1920x1080 on Avaya systems that support this resolution.

The **System Information** screen shows the actual input size for the **VGA Input** status (or **DVI-I Input** status on models that include a DVI-I input on the codec). The input selector shows a 16:9 or 4:3 window for the input depending on the aspect ratio.

Choosing a VISCA Input with Supported Third Party Cameras

Avaya 1050 includes the **VISCA Input** preference in **Administrator Preferences : Video : Video Control** for selecting the input on the codec to which a supported VISCA controlled camera is connected. The default is *SDI Adapter*. If you are using the RS-232 serial port on Avaya 1050 to control the system through the command line interface with a third party device, *None* appears as the setting for this preference.

Balancing Primary and Presentation Video Bandwidth

For video images sent to the far side during a presentation, you can allocate bandwidth to the primary and presentation video input streams as percentages of the total available bit rate for the video streams. Select the percentage to allocate in **Administrator Preferences : Video : Video Quality : Video Bandwidth Balance**.

Note: Adjust this preference before placing a call. Adjusting this preference during a call has no effect.

The first percentage in each option applies to the primary video input stream, typically the high definition camera. The second percentage applies to the presentation video input stream, typically a laptop or personal computer connected to the codec. The system allocates the bandwidth based on the selected option when only the system sends video images during a presentation. Consider adjusting this preference when the video stream from the presentation video input includes motion, for example a slide show that includes several animations or video input from a DVD player.

Selecting Priority of Quality Metrics for Source Video

You can favor sharpness or motion as a priority for the quality of primary and presentation video that the Avaya system sends to the far end during a call. If you favor sharpness by selecting a smaller number for the **Administrator Preferences : Video : Video Quality : Primary Video Motion** preference, in lower bandwidth calls the system sends the primary video at a lower frame rate and a higher resolution. The default value (10) favors motion. Consider adjusting this preference if bandwidth is limited.

If you are sending a presentation, select the priority for the quality of the presentation video in **Administrator Preferences : Video : Video Quality : Presentation Video Sharpness**. The default value (10) favors sharpness. Typically, presentation data does not include motion (for example, a spread sheet or slide show). When you favor motion for presentation video by selecting a smaller number for this preference, the system sends the video at a higher frame rate and a lower resolution.

Adjusting Video Encoder Quality

You can adjust the quality of the video image sent to the far end during a call by specifying a relative lower or higher resolution in the **Administrator Preferences : Video : Video Quality : Video Encoder Quality** preference. Moving the slider to the right decreases the resolution of the video sent to the far end and improves the quality of the video image. Consider using this preference to make minor adjustments to the quality of the video image sent to the far end.

Disabling Access to the Local Directory

By default, users can place calls using entries in the local directory and add, remove, or modify these entries. For more information about the local directory, refer to the *Avaya Video Communications System User Guide*.

You can disable user access to the local directory by setting **Local Directory** to *Disabled* in **Administrator Preferences : Directory : General**. Disabling access to the local directory also disables the following:

- saving entries from the **REDIAL** list to the local directory
- copying corporate directory entries to the local directory
- selecting entries from the local directory when creating a meeting entry in the meetings directory

Administrators maintain access to the local directory on the web administration interface **Directory** page when the **Local Directory** preference is set to *Disabled*. For more information about managing the local directory from the web administration interface, refer to "Using Advanced Directory Features" on page 37.

Populating the Corporate Directory

Users can place calls from the directory by selecting a number to dial from a list of stored numbers. The corporate directory is H.350 compliant and can store up to 1000 entries in both an alphabetical and hierarchical format. All users can manage entries in the local and meetings directories. Only administrators can manage entries in the corporate directory.

You can populate the corporate directory by configuring **Auto Discovery** preferences or Lightweight Directory Access Protocol (**LDAP**) preferences in **Administrator Preferences : Directory**. By default, auto discovery is enabled and LDAP is disabled. You can enable only one of these methods. The system automatically disables the other method to prevent duplicate entries from appearing in the corporate directory. The status of these methods, either enabled or disabled, appears on the **Administrator Preferences : Directory** screen in the user interface. The connection status of the LDAP installation also appears on this page and on the **System Information** page. The values that can appear for the connection status include the following:

LDAP Connection Status	Description
Unregistered	LDAP preferences are not configured.
Registered	LDAP preferences are configured. The last attempt by the Avaya system to contact the LDAP server and receive data was successful.
Unreachable	LDAP preferences are configured, but the LDAP hostname is invalid or the service does not exist.
Unauthorized	LDAP preferences are configured, but the username or password is invalid.
Invalid Syntax	LDAP preferences are configured, but the base Distinguished Name (DN) is invalid.
Failed	LDAP preferences are configured, but an unexpected failure occurred.

Configuring Auto Discovery

Auto discovery enables Avaya systems on your network to pass address information to other Avaya systems automatically. Configure the **Auto Discovery Subnets** and **Auto Discovery Ignored Subnets** preferences to enable the system to discover other Avaya systems outside the local subnet and share that information with other Avaya systems. Specify subnet filters (separated by spaces) in the **Auto Discovery Subnets** preference to identify the subnets to which the Avaya system can send queries and replies. By default, the preference is empty; the system sends queries and replies to other Avaya systems on the local subnet only. To exclude subnets from auto discovery, specify subnet filters in the **Auto Discovery Ignored Subnets** preference. If a destination address does not match one of the filters in the **Auto Discovery Subnets** preference, or if it matches one of the filters in the **Auto Discovery Ignored Subnets** preference, then the Avaya system does not query or reply to the Avaya system at that address.

For example, you can configure the **Auto Discovery Subnets** preference to include a large subnet and the **Auto Discovery Ignored Subnets** preference to exclude a subset of the subnet. Consider a network that has several subnets with the IP address 10.* and a slow network connection to devices that have a 10.85.* address. If you enter 10.* in the **Auto Discovery Subnets** and 10.85.* in the **Auto Discovery Ignored Subnets** preference, the Avaya system queries and replies to all Avaya systems that have a 10.* address, except those that have a 10.85.* address.

If you set **Auto Discovery** to *Disabled*, the Avaya system does not send a broadcast message to the local subnet and cannot discover or be discovered by other Avaya systems.

Reading from an LDAP Server

When you enable and configure **LDAP** preferences to populate the corporate directory, you specify the hostname, login and query parameters, and the refresh interval for reading data from a preconfigured LDAP server. Avaya recommends that you use an LDAP server configured with an H.350 compliant schema.

Configuring Appearance Preferences

Users can configure preferences in **User Preferences : Appearance** and **Backgrounds** that affect the appearance or behavior of the following:

- screen saver that appears when the system is idle and the screen saver timeout
- system sleep timeout
- timeout interval for the appearance of the user interface after a call connects
- language that appears in the user interface
- LCD contrast on the display of a connected phone
- background image or color that appears in the user interface

Help text appears at the bottom of the screen to assist users in selecting an option for each preference. Administrators can also access these preferences in **Administrator Preferences : General**, **Backgrounds**, and **Layout**.

Only administrators can hide or show Avaya branding in the user interface and screen saver logo and add or remove custom background images. To hide or show Avaya branding, access **Administrator Preferences : Appearance : General : Company Logo**. Choose *None* to hide the branding. The *Default* option shows the branding. To add or remove custom background images, refer to "Adding or Removing Custom Background Images and Colors" on page 36.

Video Layout Preferences

All users can configure the **Picture In Picture** video layout preference in **User Preferences: Appearance**. Refer to the *Avaya Video Communications Systems User Guide* for more information about setting this preference.

On Avaya systems that support dual displays, voice-activated switching of video, and auxiliary video outputs, only administrators can configure the following video layout preferences in **Administrator Preferences : Appearance : Layout**:

- **Display 2 Layout**
- Auxiliary video output preferences

Display 2 Layout

By default, when you connect a second display to an Avaya system that supports dual displays, a message appears in the display instructing you to select a configuration option. Navigate to **Administrator Preferences : Appearance : Layout : Display 2 Layout** and select an option. Options for this preference vary depending on the Avaya system model. For information about configuring this preference, refer to the Installation Guide for your Avaya system model.

Configuring Display Preferences

Only administrators can configure preferences that affect display types, resolutions, and energy management options. Display preferences appear in **Administrator Preferences : Appearance : Displays**. Typically, you configure display types and resolutions when you install your system or change a display and to troubleshoot display issues. Refer to the Installation Guide for your system model for more information.

Note: If a video input device other than an Avaya camera is connected to an HD input or component input on an Avaya system, ensure that the display resolution selected in **Administrator Preferences : Appearance : Displays** matches the resolution on the input device. Mismatched resolutions can result in video transmitted to the far side at 720p30.

You can set the **Display Energy Saver** preference to *Enabled* for connected displays to turn off the signal that the Avaya system sends to the display when the system goes to sleep. Avaya recommends that you test this feature for compatibility with your displays before using it in your environment. Some displays may appear black when the signal from the system is no longer received, but not enter an energy saving state. Other displays may recognize the loss of the signal and show text indicating this state. This may result in the text image burning into the screen. Some displays may recognize the loss of the signal and power off, but then not wake up when the Avaya system wakes up.

Viewing Recent Configuration Changes

As an aid to troubleshooting issues that you may encounter with your Avaya system or to quickly access a preference that has been recently changed, view the preferences in **Administrator Preferences : Recent**. Preferences that have dependencies on other preference settings may not appear in **Recent**.

Note: Upgrading the system software removes all preferences from the **Recent** screen.

Using Diagnostics Preferences and Tools

Diagnostic preferences and tools that are available to all users include high-definition camera preferences, input preferences for devices connected to the codec, and a system reboot option. For information about using these preferences and tools, refer to the *Avaya Video Communications Systems User Guide*. Administrators can access these preferences and tools through **User Preferences** or **Administrator Preferences : Diagnostics**.

Note: In the web administration interface, to view the effect of changes made to camera diagnostic preferences on the **Diagnostics : Cameras** page, click **Save Changes** and then **Refresh**.

Diagnostic preferences and tools available only to administrators in **Administrator Preferences : Diagnostics** include call counter statistics, color bar settings, and network utilities.

Using Network Utilities

You can troubleshoot network connection issues with your system using the ping and traceroute utilities in **Administrator Preferences : Diagnostics: Network Utilities**. The **ping** command tests responsiveness between two devices. The **traceroute** command tests responsiveness and traces the path of a packet from one device to the other.

Rebooting the System

The system reboots when you do any of the following:

- Reboot the system (**Administrator Preferences** or **User Preferences : Diagnostics : System Reboot**).
- Reset the system to its default state (**Administrator Preferences : System : System Reset**).
- Restore a system configuration using **System Restore** in the web administration interface (**Preferences : System : System Reset : System Restore**).
- Change the **VLAN Tag** preference (**Administrator Preferences : Network : General**).
- Change TCP reserved ports (**Administrator Preferences : Network : Reserved Ports**).
- Change the UDP signaling port, enable or disable TCP or TLS signaling, or change the TCP or TLS signaling ports (**Administrator Preferences : Communications : SIP**.)

- Repeatedly change the language that appears in the user interface or the display connected to an Avaya system to a resolution that requires the user interface to be reloaded into memory, for example from 720 to 1080. In this case, memory can become fragmented and not all of the user interface can be reloaded.
- Upgrade the system software from the web administration interface (**Maintenance : System Upgrade**).

All users can reboot the system by accessing **User Preferences : Diagnostics : System Reboot** from the main screen. Administrators can also reboot the system by accessing **Administrator Preferences : Diagnostics : System Reboot**. Select **Yes** when prompted to confirm the reboot.

To reset the system to its default state, refer to "Restoring Default Settings" on page 16.

Note: If the user interface is not responding and you are unable to reboot the system by following these instructions, you can reboot the system by pressing the reset button on the back of the codec as described in "Restoring Default Settings" on page 16. Avaya recommends you do not unplug power from the codec to reboot it.

Exclusive Web Administration Features

You can perform the same administrative configuration from the web administration interface that is available from the user interface. The web administration interface contains the following additional features that are not available in the user interface.

Note: Ensure that you are using a supported version of Adobe Flash Player and a supported browser when administering an Avaya system in the web administration interface. Some features such as file uploads may fail to function properly with an unsupported web browser or version of the Flash Player. Refer to the *Release Notes* for your Avaya system model on the Support page of support.avaya.com for supported web browsers and Flash Player versions.

Adding or Removing Custom Background Images and Colors

You can add or remove custom background images only from the web administration interface. Access **Preferences : Appearance : Backgrounds** and click **Add** at the bottom of the screen to add a new background image. To apply the new image, select it and then click the display to which to apply it. Images must be 1280 x 720, .jpg file type, and have unique display names.

Users and administrators can specify a background color instead of a background image to appear in the display. Choose *None* for the **Display Background Image** preference in **Administrator Preferences : Appearance : Backgrounds** or in **User Preferences : Backgrounds** and then select a color for the **Display Background Color** preference.

Only administrators can specify a custom background color in the web administration interface in **Preferences : Appearance : Backgrounds**. A color swatch appears next to the current background for each display. Click the color swatch. An eye dropper icon and a color wheel icon appear. Use these icons to do the following:

Choose a Background Color from the Interface

1. Click the eye dropper to choose a color from the web administration interface.
2. Click the color you wish to apply from the interface.
3. Click the display to apply the color.

Specify a Custom Color

1. Click the color wheel to access the color editor.
2. Specify a custom color by supplying RGB values or a hexadecimal value. You can also choose a predefined color by clicking one of the color swatches that appears in the color editor.
3. Click **Save Changes** to save the selection.
4. Click the display to apply the color.

Saving Video Snapshots

You can save video snapshots in .jpg format of video from the near and far cameras only from the web administration interface. From the **Call Manager** in the web administration interface, click the **Save Snapshot** button to capture a video image from the near or far camera. By default, video snapshots are enabled. To disable video snapshots, navigate to **Preferences : Video : Video Control** and select *Disabled* for the **Video Snapshot** preference. You can also use the button in the **Call Manager** to disable or enable video snapshots.

Note: A system does not generate video snapshots when it is asleep. If the web administration interface is showing the **Call Manager** screen, the system awakens if asleep and does not go to sleep. If you leave the **Call Manager** screen, or the web administration interface times out to the login screen, the system goes to sleep after the interval specified by the **Screen Saver Timeout** plus the **Sleep Timeout** preferences.

Video snapshots of the primary input camera are also available on the **Diagnostics : Cameras** page in the web administration interface.

Using Advanced Directory Features

Advanced usage of the directory is available only from the web administration interface. On the **Directory** tab, click the name of the directory you wish to access. **List All** retrieves the current directory data. Use **Search** to locate a specific entry in the directory.

When viewing the local or meetings directory, you can click **Clear All** to delete all entries; **Import** to add multiple entries; **Export** to export the entries in CSV format; and **Add New** to add a single entry.

When viewing the corporate directory, you can click **Export** to export the entries in CSV format.

Note: When importing and exporting directory entries from the web administration interface, use a text editor that supports UTF-8 encoding to view or edit the data. Double-byte characters are not supported in directory entries imported using the web administration interface.

Saving and Restoring a System Configuration

You can save and restore a system configuration only from the web administration interface.

The **System Save** feature creates a text file that contains command line interface commands to restore a saved configuration. The saved configuration includes all the preferences that can be set through the command line interface, except the command line interface password and the password for the default SNMP user. You can edit the file manually to customize the configuration. The **System Restore** feature restores a system configuration using the saved configuration file.

Note: Configuration preferences and options vary across Avaya system models and software releases. Restoring a system configuration using a file saved from a different model or software release may produce unexpected results. Avaya recommends that you restore a configuration that was saved from the same system or the same system model and software release.

To save a system configuration from the web administration interface, follow these steps:

1. In the web administration interface, navigate to **Preferences : System : System Reset**. If you wish to save system passwords in the file, select **Save passwords**. Passwords saved with this option are not encrypted.

2. Click **System Save**.

3. In the **Download file** dialog box, click **Yes**.

4. When prompted, choose a location in which to save the configuration file and then click **Save**.

To restore the system configuration from the web administration interface, follow these steps:

1. Ensure that a saved configuration file exists before performing a restore.

2. If you chose not to save passwords when you saved the configuration file, passwords appear in the file as tokens surrounded by ### characters and **FIX:** precedes the command in the configuration file, for example:

   ```
   FIX: set admin password ###Password###
   ```

   If you wish to replace these tokens with passwords before using the file to restore a system, delete **FIX:** and replace ###*token*### with the password. If you do not edit these lines, error 09 (invalid command) appears in the command output when you restore the system; the **FIX:** lines are ignored; and values previously set for the passwords remain unchanged.

3. Hang up all calls connected to the system. If calls are connected when you perform a restore, a dialog appears prompting you to continue or cancel the restore. If you continue, the system restore process terminates the calls.
4. In the web administration interface, navigate to **Preferences : System : System Reset**.
5. Click **System Restore**.
6. Click **Continue**. The Avaya system reboots and a dialog appears indicating that the restore succeeded.

Copying Screen Text to the Clipboard

The web administration interface supports copying data from most screens to the operating system clipboard. This feature facilitates troubleshooting by enabling you to paste configuration information into an email or text editing application. If a screen supports this feature, a **Copy** button appears in the lower right corner of the screen. Click the **Copy** button to copy the data on the screen to the clipboard.

Downloading Call History

You can download call history as a comma separated value file (.csv file extension) from the **Diagnostics** page in the web administration interface. Click **Call History** and then click **Download Call History**. When prompted, choose a location to save the file.

Managing Calls from the Web Administration Interface

You can place calls from the **Directory** tab by selecting an entry and clicking **Dial**. Dialing an entry from the directory invokes the **Call Manager**. The **Call Manager** tab includes all call management features that are available to users in the user interface. When you move the pointer over an interface element, a tool tip appears to assist you in identifying the call management feature associated with that element. Data that appears in the Call Manager refreshes every five seconds.

Upgrading your System Software

Before you upgrade your Avaya system software, ensure that the system meets the following prerequisites:

- All cameras that you intend to use with the system are connected to the codec properly.

  Note: Cameras not connected to an Avaya system before an upgrade may not function properly after an upgrade.

To upgrade the software for your system, follow these steps:

1. Access support.avaya.com
2. Click the **Download Software** button.
3. Enter your serial number (located on the bottom or back of your Avaya system codec and on the **System Information** page).
4. Click the link for the software version you wish to download.
5. Download it to a local directory on your system.
6. Access the web administration interface for your system. Refer to "Administration from a Web Browser" on page 5.
7. Click the **Maintenance** tab.
8. Click **System Upgrade**.
9. If your upgrade requires you to reset the system to the original default settings, select the **Reset to Default State** checkbox.
10. Browse for the upgrade file you downloaded in step 5.
11. Click **Upgrade**.

    Note: If calls are connected to the system, a dialog appears prompting you to continue or cancel the upgrade. Click **Yes**, to continue with the upgrade and disconnect the active calls. The upgrade may take several minutes; do not disrupt the upgrade process. During an upgrade, a status screen appears in the display connected to the system. Users cannot cancel the screen, and the system rejects incoming calls.

12. A system upgrade status message displays when the upgrade is complete. Close the status window and close the administrator configuration window.

13. Your system is ready to use. If you selected the **Reset to Default State** checkbox in step 9, you must first reconfigure your system. Refer to the Installation Guide for your Avaya system model.

Troubleshooting Upgrade Failures

If attempts to upgrade software for your Avaya system fail, follow these steps:

1. Ensure you have a valid upgrade image.
2. Reboot the system.
3. Attempt the upgrade again.
4. If a second attempt fails, note the error code returned.
5. If problems persist, contact Avaya Customer Support.

Upgrade Error Codes

Following are the error codes you may receive when an upgrade fails.

Code	Problem	Description
1	Internal error	The system is missing critical files.
2	Switch to upgrade failed	The command to set the active partition failed.
3	Write failed	A write failure occurred during copying of the image to the upgrade partition. This typically occurs when using an upgrade image for another Avaya product.
4	Read failed	Reading incoming data failed during the uploading of the image. This typically occurs if the connection is broken during the upload.
5	Upgrade script failed	After the image has been successfully uploaded the system runs an upgrade script for final processing. This error indicates a failure in that script. This typically occurs when using an upgrade image for another Avaya product.
6	Unable to run upgrade script	The system was unable to run the upgrade script. This typically occurs when using an upgrade image for another Avaya product.

Code	Problem	Description
7	Unable to mount upgrade partition	After the image has been copied to the system, the system failed to mount the image. This typically occurs if the upgrade image is corrupt or when using an upgrade image for another Avaya product.
8	No permission	The system failed to read the upgrade partition.
9	Corrupt image	The upgrade image is corrupt and unusable. This typically occurs due to a bad image or errors during upload to the device.
10	Bad argument	An invalid argument was submitted to the upgrade process. This typically occurs when using an upgrade image for another Avaya product.
11	Invalid signature	The encryption signature is invalid. This typically occurs if the image is corrupt or compromised.
12	Decrypt failed	The system was unable to decrypt the upgrade image. This typically occurs if the image is corrupt or compromised.
13	Developer system	The system is configured for development and can only be upgraded by an Avaya representative.
14	Upgrade in progress	An upgrade is already in progress. The system only supports one upgrade at a time.