



**Avaya 1010/1020
User Guide**

Issue 1
June 2010

© 2010 Avaya Inc.
All Rights Reserved.

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

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

Third Party Components

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

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>.

Using Avaya 1010/1020

This guide explains how to administer, locally configure, and use the Avaya 1010 and 1020 video conferencing systems.

For information about administering Avaya 1030, 1040, and Avaya 1050 video conferencing systems, refer to the *Avaya Video Conferencing Systems Administrator Guide* for those systems.

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 1010 and 1020 video conferencing systems connect to Avaya Aura™ Session Manager. 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 1010 and 1020 video conferencing systems are not administrable on H.323 video gatekeepers.

System Components

Before using Avaya 1010/1020, familiarize yourself with its components.

Camera and Microphone

An Avaya 1010/1020 system includes a high-definition video camera and a device with one or more microphones for audio input during a call. Avaya Video Camera 100 is a fixed-focus camera that includes two omni-directional microphones, providing audio and video input from the same device.



Avaya Video Camera 100

Optionally, you can use a combination of an Avaya Video Camera 150 and Avaya Video MicPod 1000 for video input and audio input during a call. Avaya Video Camera 150 is a pan, tilt, zoom camera and Avaya Video MicPod 1000 includes a single omni-directional microphone, mute button and mute status LEDs.



Avaya Video Camera 150



Avaya Video MicPod 1000

Codec

The Avaya 1010/1020 codec compresses outgoing video and audio, transmits this information to the far end of a call, and decompresses incoming information. You should not need to interact with the codec once it has been properly installed in your environment.



Avaya 1010/1020

Third Party Display

A third party display connected to the Avaya codec enables you to access the user interface and view video images during a video call.

Remote Control

The Avaya remote control provides wireless control of all Avaya 1010/1020 functions and enables you to navigate the user interface, place and receive calls, and control cameras connected to the system. The remote control is shown in the following illustration:



Navigating the User Interface




When your Avaya system is idle, a screen saver appears on the display, or the screen is black. An incoming call or pressing any button on the remote control automatically invokes the system.










The Main Screen

Use the arrow keys on the remote control to navigate the main screen. As you navigate to different parts of the screen, the icons and their descriptions that appear in the navigation bar change to indicate what actions are available for a selected object or screen.

The main screen includes the following features:


- The top right corner of the screen displays system information such as the system name, and video number. This information is hidden during a call.
- Video from the primary input, typically a camera connected to the system, appears in a small window below the system information.
- The center of the screen contains the **REDIAL** list and the **Voice Call** and **Video Call** buttons. From the **REDIAL** list you can place a call by selecting a number from a list of recently dialed numbers. Use the **Voice Call** and **Video Call** buttons to dial a number manually.
- The system status bar is a white bar that appears immediately below the **REDIAL** list. The system status bar indicates system and network status, including the number of voice and video calls, the time and date, or the duration of a call when a call is in progress. When the system is booting, status also appears at the top of the **REDIAL** list to indicate the current state of the system. The following table identifies the icons that can appear in the system status bar.



Icon	Condition
Video 	Indicates a video call in progress. An orange circle appears to the right of the video icon to indicate a video call in progress.
Voice 	Indicates a voice call in progress. An orange circle appears to the right of the voice icon to indicate a voice call in progress.
	Indicates that the communication subsystem is initializing. If this icon reappears after the system has booted, a problem has occurred and rebooting the system is necessary.

Icon	Condition
	Indicates that the system is initializing. When the system is initializing, functionality on the main screen is disabled and no entries appear in the REDIAL list. This icon also appears when a new device is connected to the system after the system boots and disappears when the device is ready. If the icon persists, a problem has occurred and rebooting the system is necessary.
	Indicates that the system does not have an active microphone. Contact your administrator.
Network Status	Identifies the network status, as follows: connected  (green indicator) in progress  (yellow indicator) disconnected  (red indicator)
System Overheating	This yellow indicator warns you when the system temperature is above normal operating temperature. The codec adjusts fan speed automatically to cool itself.  This red indicator warns that the system is overheated and approaching the maximum allowed operating temperature and will automatically reboot after reaching it.  <hr/> Warning: Temperatures that require the codec to reboot can permanently damage codec components. Ensure the room that houses the codec is properly ventilated and temperature controlled.
SIP server registration status	When SIP is configured as the protocol for placing calls, this indicator identifies the registration status of the Avaya system with the SIP server as follows: in progress  (yellow indicator) registration failed  (red indicator) Contact your administrator.

- The navigation bar is a grey bar that appears below the system status bar. The navigation bar contains icons that correspond to buttons on the remote control and text that describes the action a button performs. The icons and text change depending on how you use the system. The quick reference card *Getting Started with your Avaya Video System* shows you how to perform common tasks with the remote control.
Note: Pressing and holding any button except the **OK** button on the remote control may cause the command associated with the button to repeat.

The System Menu

To access the **System Menu** from the main screen, press the  button on the remote control. From the **System Menu** you can do the following:

- View selected configuration and status information about your Avaya system in the **System Information** pages. Use the  and  buttons on the remote control to navigate the pages.
- Access **User Preferences** from which you can do the following:
 - Change the appearance of the user interface, including the language, screen saver and screen saver timeout, system sleep timeout, and the duration of time that the user interface appears after a call connects.
 - Change the background image or color.
 - Choose the method the system uses for answering calls. For more information, refer to “Answering or Rejecting a Call” on page 16.
 - Adjust settings for audio input and output devices connected to the system. For more information, refer to “Managing Audio” on page 18.
 - Access diagnostic tools to adjust camera settings and reboot the system. For more information, refer to “Troubleshooting” on page 30.


When you select a preference, help text appears at the bottom of the screen to assist you in selecting an option for the preference.

Note: Your administrator may require a password to access these preferences.



- **Administrator Preferences** is password protected and contains preferences for administrators only. Refer to “Accessing Administrative Features” on page 33.
- Activate the system **Do Not Disturb** feature. For more information, refer to “Answering or Rejecting a Call” on page 16.

Controlling Avaya Video Camera 150s

Before placing a video call, become familiar with how to control your Avaya Video Camera 150 using the remote control. To prevent far end users from controlling your near end camera during a call, contact your administrator. Avaya Video Camera 100 does not support camera control.

To adjust Avaya Video Camera 150 at the near end when the system is idle, select the camera. Press the **near/far**  camera button on the remote control.

Use the following buttons on the remote control to adjust the camera angle:

Remote Control Button	Function
	Left and right arrows pan the camera. Up and down arrows tilt the camera.
	Zoom in and zoom out keys make objects appear closer or farther away.

Configuring Avaya Video Camera 150 Presets

A camera preset is a predefined camera position that is associated with a numeric key on the remote control. Camera presets enable you to quickly change the position of the near end PTZ camera during a call by pressing a single key on the remote control instead of using the arrow and zoom keys. Far end participants see the video image without the delay that is associated with using more than one key to position the camera.

You can configure and use presets in the **Primary Input** and **Presentation Input** screens before placing a call and from any video screen during a call. To configure and use presets during a call, you must first select **Presets** from the **Call Manager** screen. For more information about using presets during a call, refer to “Using Avaya Video Camera 150 Presets During a Call” on page 24.

You can save nine presets. When presets are available for use, icons for the numeric keys (0 through 9) followed by the word **Presets** appear in the navigation bar.

Configuring presets before placing a call ensures that you can quickly change the near end camera position during the call. To configure a preset for the near end camera before placing a call, follow these steps:

1. Select the near end camera and adjust its position. Refer to “Controlling Avaya Video Camera 150s” on page 10.
2. Press and hold a numeric key (1 through 9) on the remote control until you hear a beep. The current position of the camera is associated with the key. **Preset x saved**, where **x** is the numeric key associated with the preset, appears above the status bar.

If you choose a numeric key that already has a preset configured, it is overwritten. An administrator can lock existing presets to prevent them from being overwritten. If an existing preset associated with the key is locked, **Preset x locked** appears on the screen. The 0 key, when used as a preset, always moves the selected camera to the default position and cannot be overwritten.

3. To test the preset, use the arrow keys to move the camera to a different position, and press the numeric key associated with the preset to move the camera to the preset position. **Preset x**, where **x** is the numeric key associated with the preset, appears above the status bar.

Managing Near End Video Quality

Before you place a call, examine the near end video image from the camera connected to your Avaya system. If the image flickers, colors appear unbalanced, or the image appears too dark, you may need to adjust the room lighting or camera settings. For more information, refer to “Adjusting Room Lighting” on page 30 and “Camera Issues” on page 31.




Placing a Call

You can place a video or voice call with your Avaya system in the following ways:

- Select a stored number from the **REDIAL** list on the main screen or from the directory.
- Manually dial a number using the **Video Call** or **Voice Call** buttons on the main screen

Placing a Call from the REDIAL List

The **REDIAL** list on the main screen stores up to 15 recently dialed numbers. A scroll bar appears when more than five entries are available for selection. The oldest entry in the list is automatically removed when the system receives a call after the maximum number of entries has been reached.

The last call placed always appears at the top of the list. The entry includes the name of the system called and an icon that indicates whether the call was a voice  or video  call. The entry's number (and bandwidth if the entry is a video call) appears below the list when the entry is selected. If the system receives a call, but does not answer it, the call appears in the **REDIAL** list as a missed call. The  symbol appears next to the name in the entry. Select the entry to display the date and time of the missed call below the **REDIAL** list.

To place a call from the **REDIAL** list, use the arrow keys on the remote control to select an entry and press **OK**.

To change the bandwidth for a video call on the **REDIAL** list before placing the call, select **Video Call** on the main screen, press **OK** twice, and use the right arrow key to select the desired bandwidth from the list.

Note: Selecting *Auto* from the **Video Call** selection before placing a call does not change the bandwidth selection for an entry on the **REDIAL** list that does not have *Auto* as its last called bandwidth.

You can adjust the maximum number of entries that appear in the **REDIAL** list by adjusting the **Maximum Redial Entries** preference in **User Preferences : Calls**.


The *None* option for the **Maximum Redial Entries** preference removes existing entries from the **REDIAL** list and prevents new entries from appearing on the list.




You can also add entries from the **REDIAL** list to the local directory and manually remove entries or lock them to prevent them from being automatically removed when the maximum number of entries is reached. For more information, refer to "Managing the REDIAL List" on page 26.

Placing a Call from the Directory


The directory stores a list of names and numbers from which you can place calls. The directory includes two subdirectories: the local and corporate directories. The corporate directory is read only and managed by your administrator.

To place a call from the directory, follow these steps:

1. From the main screen, press the  button on the remote control to access the directory.
2. Use the arrow keys to select either the **Local** (if available) or **Corporate** directory, and press **OK**.
3. Use the arrow keys on the remote control to select the entry that you wish to dial.

You can browse the directory using either the alphabetical or hierarchical method. When you use the alphabetical method, the entries appear in alphabetical order and you can select an alphabet group in the **Browse** column to quickly navigate to an entry. Hierarchies are predefined organizational units similar to folders or directories on a computer system. You can place an entry into a hierarchy when you create the entry or at any time by editing the **Hierarchy** field when editing the entry. For more information about creating hierarchies, refer to “Managing the Directory” on page 28. Using the hierarchical method, you can select a hierarchy in the **Browse** column to locate an entry. To move down one level in **Browse**, press **OK**. To move up one level, press the  button. You can also use the  and  keys on the remote control to move up or down a page of entries when an entry is selected.

4. Press **OK** on the remote control to place the call.

Note: If an entry in the local or corporate directory has more than one number, the  symbol appears in the **NUMBERS** column. Press **OK** and select the number you wish to call. Press **OK** to place the call.




You can also add, remove, or edit entries in the directory. For more information, refer to “Managing the Directory” on page 28.

Manually Dialing a Number from the Main Screen


Use the **Video Call** and **Voice Call** selections on the main screen to dial a video or voice number manually, using the remote control.

Manually Dialing a Video Number

To dial a video number manually from the main screen, follow these steps:





1. Use the arrow keys on the remote control to select **Video Call** and press **OK**.
2. Enter the number you wish to call. The last manually entered number appears by default. To edit the number, use the following keys:
 - The  button changes the text entry method (indicated at the bottom of the screen).
 - The  button behaves as backspace.
 - The  button displays the keyboard from which you can enter alphanumeric characters. Use the arrow keys to navigate to the character you wish to enter and press **OK**.

Press **OK** to exit the field.

3. *Optional:* Navigate to the list that appears next to the entry box for numbers and choose a value for the maximum bandwidth for the call. Press **OK** to access the list, use the arrow keys to select a value, and press **OK** again to save your selection.
4. Press the **call**  button to dial the number.

Manually Dialing a Voice Number

To dial a voice number manually from the main screen, follow these steps:

1. Use the arrow keys on the remote control to select **Voice Call** and press **OK**.
2. Enter the number you wish to call. The last manually entered number appears in this field by default. To edit the number, use the following keys:
 - The  button changes the text entry method (indicated at the bottom of the screen).
 - The  button behaves as backspace.
 - The  button displays the keyboard from which you can enter alphanumeric characters. Use the arrow keys to navigate to the character you wish to enter and press **OK**.
3. Press **call**  to place the call.

Answering or Rejecting a Call


You can configure your system to automatically answer incoming calls by setting preferences in **User Preferences : Calls** as follows:

- **Auto Answer**—If set to *Enabled*, the system automatically answers the first incoming call. If set to *Disabled* (the default), you must manually answer incoming calls.
If your system is configured for answering calls manually, choose one of the following options when an incoming call arrives:
 - Select **Answer** and press **OK** to accept the call.
 - Select **Ignore** and press **OK** to reject the call.
- **Auto Answer Mute**—If set to *Enabled* (the default), and the **Auto Answer** preference is set to *Enabled*, the system is muted when a call connects.

Using System Do Not Disturb

You can enable the system **Do Not Disturb** feature to show only the background image of the main screen with the status and navigation bars and a system **Do Not Disturb** message. When the system **Do Not Disturb** feature is enabled, the system responds only to the volume control buttons and the **OK** button on the remote control. Callers hear a busy signal and missed calls appear in the **REDIAL** list. Consider using this feature, for example, if you are using the meeting room for a purpose other than a video conference and do not wish to be disturbed by incoming calls.

To enable this feature, follow these steps:

1. From the main screen, access the system menu by pressing the  button on the remote control.
2. Use the down arrow key to select **Do Not Disturb**.
3. Click **OK**. A dialog box appears indicating that the system **Do Not Disturb** feature is enabled. Press **OK** to return the system to normal operation.

Managing a Call






During a call, you can view information about the status of the call and the identity of the connected caller. You can also manage audio output and video images, and control the PTZ camera.

Call Status


When you place a call with your Avaya system, a **Call Status** dialog appears. The **Call Status** dialog shows the number or IP address that you are attempting to call and the status of the call (for example, dialing, ringing, connecting, answered, or unavailable).

Caller ID

When your video call is answered, video from the far end appears in your display. In the upper-left corner of the far video image, the caller ID (phone number or IP address) of the far end system appears. One or more of the following icons may appear next to the caller ID to represent information about the call.

Icon	Description
	Video call.
	Voice call.
	Microphones are muted on the far end system.
	A voice call that is encrypted. Note: The  icon appears in the Call Status, Call Manager list, and Call Statistics list.

Hiding or Showing User Interface Elements


By default, the system information, status bar, and navigation bar fade from the screen after a call has been connected for 10 seconds. This interval resets after any interaction with the system. You can adjust the duration of the fade out interval by adjusting the **Fade Out Timeout** preference in **User Preferences : Appearance**. To hide or show these user interface elements at any time during a call, press the  button.

Note: The user interface does not hide if the system is overheating. System overheating icons appear in the status bar. Refer to “The Main Screen” on page 8 for more information about the system overheating icons.

Managing Audio


You can identify the video caller who is speaking in the call, adjust the volume of the audio, and mute the active microphone.

Identifying the Dominant Speaker

When a video participant in a call is speaking, the dominant speaker icon  appears in the display in the video image from that participant.

Adjusting Volume



To adjust the volume in a call, use the  button on the remote control. You can also adjust the active microphone volume, or the treble and bass levels for audio out by adjusting preferences in **User Preferences : Audio**.

Volume preferences for audio inputs appear with a bar graph audio meter next to the slider. The audio meter expands below the slider when you select the slider and press **OK** on the remote control.



The audio meter displays the level of the transmitted voice. The meter is calibrated in decibels (dB) RMS below digital full scale (DFS). The meter is accurate to ± 1 dB.



- A level of 0 dB is the maximum.
- 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. The AEC (Acoustic Echo Canceller) and AGC (Automatic Gain Control) In Avaya 1010/1020 attempt to keep the RMS transmit level below -20 dB DFS.

To set the level for your audio input, position someone the same distance from the microphone as participants would be in the room during a video conference and have them speak at a normal volume. Green bars indicate an acceptable setting at normal speaking volume. Yellow bars are acceptable if you are shouting or speaking loudly. Avoid settings that produce red bars in the audio meter.

Avaya recommends a volume setting of 5 to 8 for most Avaya Video MicPod 1000 applications. Avaya recommends a volume setting of 5 to 10 for most Avaya Video Camera 100 applications. Use the meter to visually verify that the transmit level peaks in the desired -28 to -22 dB range.

When the user interface is visible during a call, a volume meter for the active microphone appears in the near video image next to the dominant speaker icon.

Muting the Active Microphone

Pressing the mute  button on the remote control or Avaya Video MicPod 1000 mutes the active microphone. When the near side active microphone is muted in a call, the  symbol appears.

Managing PIP

Your display shows the far-end and near-end video conferencing sites in addition to the menus and video images from connected video sources.

Picture-In-Picture (PIP) is a smaller window placed in one of the corners of the call screen. This second image is placed on top of the main image and always displays the primary (near) input by default. You can change the default setting so that PIP never appears or always appears by adjusting the **User Preferences : Appearance : Picture in Picture** preference.


Managing Video Layout

During a call, video from the connected caller appears in your display. You can change the screen layout of near and far end video that appear in the display.


Understanding Screen Layouts

Screen layouts appear as one of the following types:

- A far end participant or a presentation, when in progress, appears as the largest video image.
- Your site (the near end participant) appears as the largest video image.
- Both video images are the same size.

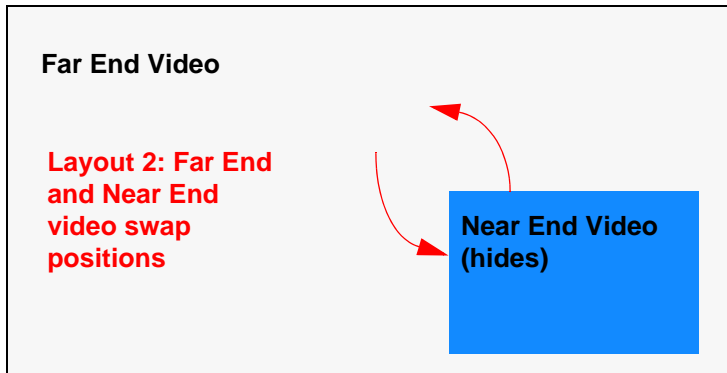
If you choose a screen layout that shows both video images as the same size, only the dominant speaker icon  moves to indicate which participant is currently speaking.

Changing the Screen Layout of Video Images (No Presentation)

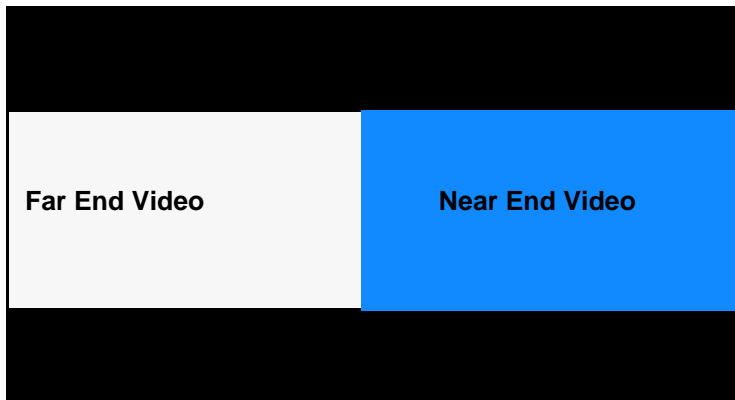
To change the screen layout, press the screen layout  button.

The number of the selected screen layout (x) and the total number of screen layouts that are available (y) appear in the center of the screen above the status bar as x/y . Continue to press the screen layout button to show all available screen layouts.

Layouts 1/3 and 2/3 (No Presentation)



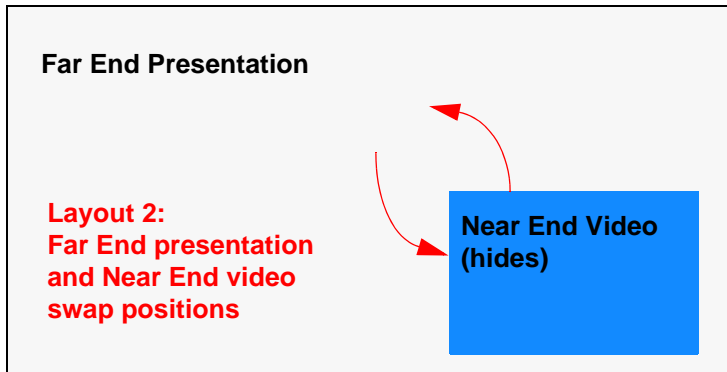
Layout 3/3 (No Presentation)



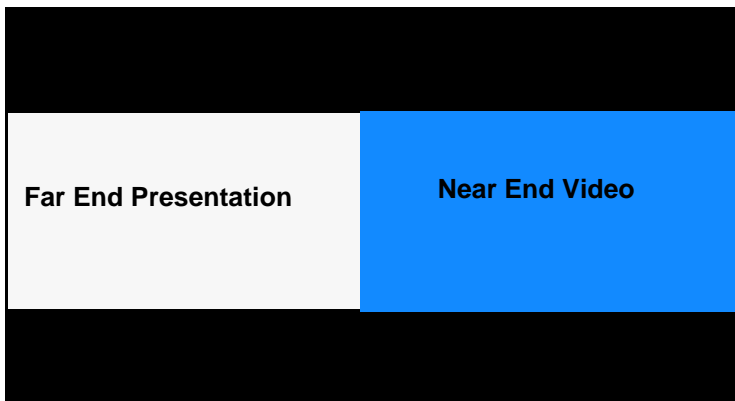
Changing the Screen Layout of Video Images while Receiving a Presentation

When you are receiving a presentation, you can choose from the following layouts:

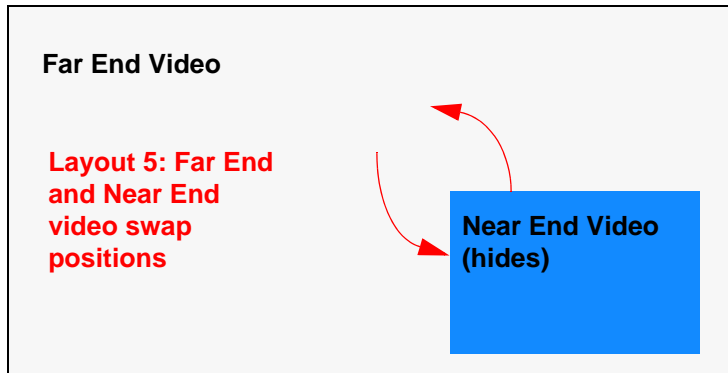
Layouts 1/6 and 2/6



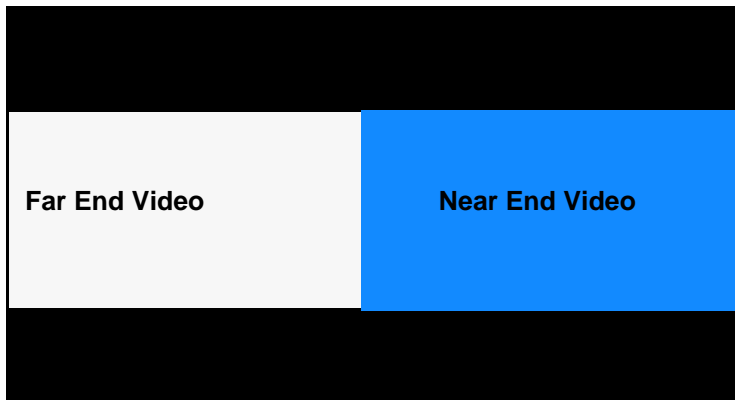
Layout 3/6



Layouts 4/6 and 5/6





Layout 6/6






Controlling a Far End Camera

You can control a far end PTZ camera during a video conference in the same way you control a near end PTZ camera if the far end camera is enabled properly. Avaya Video Camera 100 does not support camera control.

During a video call, a camera icon appears in the video image of the participant whose camera you are controlling when the user interface is visible. An orange camera icon  indicates control of the primary (near) input. A blue camera icon  in a far end video image indicates control of the far end camera. By default, the near camera is selected.


To select a far end camera to control, do the following from any call screen:

Press the **near/far**  camera button on the remote control. The blue camera icon  appears in the far end video image in the call. You can choose the far end input device to control by pressing the **input**  button on the remote control. A menu of the input devices that are available for selection appears. Use the arrow keys on the remote control to select a device and then press **OK**.

Using Avaya Video Camera 150 Presets During a Call

You can configure an Avaya Video Camera 150 preset before placing a call or during a call. To configure a camera preset on the near camera before placing a call, refer to “Configuring Avaya Video Camera 150 Presets” on page 11. To configure a camera preset during a call, ensure that the numeric keys are functioning as presets as indicated in the following steps, select the camera you wish to control, and then configure the preset.

To use a camera preset during a call, follow these steps:

1. In the navigation bar from any call screen, **Presets** must appear to the right of the numeric keys icons in the navigation bar to indicate that the numeric keys on the remote control are functioning as presets. If **Touch Tones** appears instead, change the function of the keys to **Presets** by pressing the .

Access the **Call Manager** by pressing **OK**. Use the arrow keys to select **Presets** and then press the  button to close the **Call Manager**.

The **Presets** label appears next to the numeric key icons in the navigation bar of the user interface.

Note: To use presets during a call, you must use the remote control.


2. To use a preset, press the numeric key on the remote control that represents the preset you wish to use. **Preset x**, where x is the numeric key associated with the preset, appears on the screen.

If you configured a preset for a far end camera of a participant in the call, you must select the far end camera to use the preset. Refer to “Controlling a Far End Camera” on page 23.

Note: The numeric keys work as presets during a call only when you are in a call screen.

Viewing Call Statistics

To view statistical information about a call, follow these steps:

1. During a call, press the  button.
2. Audio and video statistics for the current call appear on the screen.

Two columns of statistics, **Receive** and **Transmit** appear. The total bandwidth used for audio and video appear beside each column heading. Each column has a video and audio block.

Video statistics include the following:

- **resolution** shows the resolution, in pixels, of the video image transmitted or received.
- **codec** shows the video codec used to compress and decompress the video.
- **bandwidth** shows the amount of video data transferred per second in kilobits.
- **frame rate** shows the video frame rate in frames per second.

Audio statistics include the following:


- **codec** shows the audio codec used to compress and decompress the audio.
- **bandwidth** shows the amount of audio data transferred per second in kilobits.
- **packet rate** shows the amount of audio data packets transferred or received per second in kilobytes.

Both the Audio and Video block include the following:

- **jitter** shows the variation, in milliseconds, in the time between packets arriving, caused by network congestion, timing drift, or route changes.
- **packet loss** shows the number of packets of data that fail to reach their destination. Packet loss can be caused by a number of factors, including signal degradation over the network medium, oversaturated network links, corrupted packets rejected in-transit, faulty networking hardware, misaligned system drivers or network applications, or normal routing routines.
- **cumulative** shows the up to date count of packets lost in the call.
- **percentage** shows packet loss as a percentage of the total packets sent.


The following additional information appears below the Audio statistics block:

- the call duration
- the make and model of the far end video communication device and the software version it is using

-
3. To hide the statistics, press the  button again. Statistics automatically refresh every 5 seconds and hide after 5 minutes.

Ending a Call

You can end a call using any of the following options:

- **hang up**  button on the remote control
- **Call Manager** dialog
- **REDIAL** list


Ending a Call from the Call Manager

To hang up a call from the **Call Manager** dialog, follow these steps:

1. From any call screen, press **OK**.
The **Call Manager** dialog appears.
2. To hang up a call, press **OK** again to end the call.

Ending a Call from the REDIAL List

To hang up a call from the **REDIAL** list, follow these steps:


1. Press the  button to return to the main screen.
2. On the **REDIAL** list, an orange LED indicator appears to the left of the voice or video number currently in the call. Use the arrow keys to select the entry.
3. Press **OK**.

Managing the REDIAL List

You can perform the following tasks to manage the **REDIAL** list:


- Lock an entry to prevent it from being removed automatically from the list.
- Unlock a locked entry.
- Remove an entry.
- Add an entry to the local directory (if available).
- Adjust the maximum number of entries that can appear.

Locking and Unlocking Entries in the REDIAL List

You can lock and unlock entries in the **REDIAL** list. Locking an entry prevents it from being removed after the maximum number of entries in the list has been reached. The lock symbol  appears next to the name in the entry when the entry is selected.


Note: Locking an entry does not prevent it from being removed from the list manually. Refer to “Removing an Entry from the REDIAL List” on page 27.

To lock or unlock an entry in the **REDIAL** list, follow these steps:

1. Using the arrow keys on the remote control, select the entry you wish to lock or unlock.
2. Press the  button.
3. Select **Lock** (or **Unlock** if the entry is locked) from the menu, and press **OK**.

Removing an Entry from the REDIAL List


To remove an entry from the **REDIAL** list, follow these steps:

1. Using the arrow keys on the remote control, select the entry you wish to remove.
2. Press the  button.
3. Select **Remove** from the menu, and press **OK**.

Adding a REDIAL List Entry to the Directory

You can add an entry from the **REDIAL** list to the local directory.

Note: An administrator can choose to hide the local directory from users, in which case, a user cannot perform this task.




1. Using the arrow keys on the remote control, select the entry you wish to add to the directory.
2. Press the  button.
3. Select **Save** on the menu and press **OK**.
4. Press **OK** again to close the confirmation dialog.

Managing the Directory

If you have access to the local directory, you can add, remove, or edit entries.

Adding an Entry to the Local Directory

You can create up to 1000 entries in the local directory. To add an entry to the local directory, follow these steps:



1. Access the directory by pressing the  button from the main screen.
2. Using the arrow keys, select the **Local** directory.
3. Select the **Add New Entry** button and press **OK**.
4. Use the arrow keys to select fields in the **New Directory Entry** screen. Press **OK** to enter a value in a selected field. Enter a system name, video and voice numbers, and IP address or ISDN numbers. If necessary, press the  button to change the method of text entry for text fields or press  to access the keyboard. After entering a value, hide the keyboard (if you used it to enter the value) and press **OK** to exit the field.
5. If a hierarchy has been predefined for the local directory, in the **Hierarchy** field, enter the path to the location in the hierarchy in which to place the entry. Hierarchies can be defined, for example, by location or department. You must identify the full path (separated by commas) of a predefined hierarchy in which to add an entry prior to completing the new entry screen. If you leave the **Hierarchy** field empty, the new entry is inserted at the top of the hierarchy (if defined) or is grouped alphabetically.

For example, suppose your administrator defined a hierarchy by location where Home Office is the top of the hierarchy, and Sales Office 1 and Sales Office 2 are at the next level below the Home Office. To place an entry in Sales Office 2, the value for **Hierarchy** is *Home Office, Sales Office 2*.

6. When you have completed the fields, select **Add Entry** and press **OK**.



Copying an Entry from the Corporate to Local Directory

You can copy an entry from the corporate directory to the local directory.

1. Access the directory by pressing the  button from the main screen.
2. Select the **Corporate** directory.
3. Select the entry you wish to copy to the local directory.
4. Press the  button.
5. Select **Copy to local** and press **OK**.
6. Press **OK** to save the entry.


Removing an Entry from the Local Directory

You can remove an entry from the local directory.


1. Access the directory by pressing the  button from the main screen.
2. Select the **Local** directory.
3. Select the entry you wish to remove.
4. Press the  button.
5. Select **Remove** and press **OK**.
6. Select **Yes** and press **OK**.

Editing an Entry in the Local or Directory

You can edit an entry in the local directory.

1. Select the entry you wish to edit.
2. Press the  button.
3. Select **Edit** from the menu, and press **OK**.

-
4. Modify values in the **Edit Directory Entry** dialog.
 - a. Press **OK** to select a field you wish to modify.

Note: If necessary, press the  button to change the method of text entry for text fields.
 - b. After completing your changes, press **OK** to exit the field.
 5. Using the arrow keys, select **Save Changes** and press **OK**.

Troubleshooting

The following sections describe symptoms, possible causes, and potential solutions for common problems you may encounter with your Avaya system.

When experiencing a problem, visually inspect the unit. Ensure the system has not been exposed to water or heat sources or appears physically damaged.

Improperly connected or loose cables are common causes of problems with hardware units. When investigating a system problem, first inspect all the external controls and cable connections. Ensure that connections are correct and secure, and that nothing is obstructing the cables. Contact your administrator for information about proper cabling.

Adjusting Room Lighting

You can assist the system to maintain the best possible image quality by altering the environmental lighting and background colors of your environment. If light levels are too low you may consider adding artificial lighting. Indirect light from shaded sources or reflected light from pale walls often produces excellent results.

Avoid the following:

- direct sunlight on the subject matter, the background, or the camera lens which creates harsh contrasts
- direct illumination of the subject matter and camera lens
- colored lighting
- harsh side lighting or strong light from above

You can also improve dim scenes by adjusting the camera brightness. Refer to “Adjusting Camera Brightness” on page 31.

Camera Issues

If you are unable to pan, tilt, or zoom a camera that has these capabilities, ensure the remote control contains three AAA batteries that are in good working condition. Also verify that no objects are obstructing the sensor on the front of the camera and that the LED on front of the camera flashes bright blue when you use the remote control to perform a task.

If no video displays from the camera, ensure the camera is connected to the Avaya system with a camera cable to the appropriate camera input or contact your administrator.

Verify that the blue LED on the front of the camera is lit, indicating that power is active, and reboot the system if necessary to verify that the camera turns on. To reboot the system, refer to “Power and Connectivity Issues” on page 33.

Using Camera Diagnostic Preferences

You can use the camera diagnostic preferences in **User Preferences : Diagnostics** to adjust camera brightness and white balance and correct for some types of flicker that may appear in the video. Diagnostic camera preferences for camera brightness and white balance are available only if the selected camera is connected to the codec and **Ready** appears as the status for the camera on the **System Information** page.

Adjusting Camera Brightness

Camera brightness refers to the amount of light received through the lens of the camera. You can improve dim scenes by adjusting room lighting and manually adjusting the camera brightness. To adjust camera brightness, set the **HD Camera Brightness** preference in **User Preferences : Diagnostics : High Definition Camera**.

Adjusting Camera White Balance

Camera white balance refers to how a camera references the color white, which is a mixture of all colors. Adjust the white balance when video color appears to be unbalanced. White balance is affected by the type of light source. To adjust the camera white balance adjust the **HD Camera White Balance** preference in **User Preferences : Diagnostics : High Definition Camera**.

Adjusting the Camera Anti-Flicker Preference

Lights powered by a 50 Hz power source can produce a flicker that the camera captures and transmits to the system. If you are using lights powered by a 50 Hz power source and observe a flicker in the video displayed in your system, select the *50 Hz* option in **User Preferences : Diagnostics : High Definition Camera : Camera Anti-Flicker**. The default option is *Auto*.

Some camera exposure settings designed to be used in rooms lit by sunlight may result in a flicker. To remove the flicker, increase the **HD Camera Brightness** setting in **User Preferences : Diagnostics : High Definition Camera**.

Display Issues

The following issues are related to the user interface or the display.

Display Failures

If data does not appear on the display, ensure cables are properly connected on the display and that the display cable is connected to the HD Display 1 output on the codec.

If the video image and user interface appear washed out or too bright, examine the input settings of your HDTV to make sure the HDTV is displaying the appropriate resolution. Some HDTVs (particularly plasma displays) allow you to configure the native resolution of the input device from the HDTV administration interface.

Poor Quality Display

If the colors on the display appear incorrect, verify that the display cable is properly connected to the display.

Poor Quality Far End Video

During a call, the Avaya system automatically selects the best video algorithm based on the video source and capabilities of the remote system. If you experience poor motion handling or visible tiling in the far end picture during a video call, contact your administrator.

Audio Issues

An Avaya system automatically selects the best audio algorithm based on the call rate and the capabilities of the remote system. The following issues are related to the audio quality.

Problematic Sound Quality

If you are unable to hear the ringer when an incoming call arrives, adjust the **Ring Tone Volume** preference in **User Preferences : Audio**.

Muffled audio reception from the far side may be caused by highly reverberant rooms. If you are experiencing poor audio reception, add more sound absorbency to the room and speak in close proximity to the microphone.

Degradation in the audio quality can also be caused by faulty microphones or dust and debris on the microphones. Do not use any kind of liquid or aerosol cleaner on Avaya devices that include microphones. A soft, slightly damp cloth is sufficient to clean the top surface of the units if necessary.

Distorted Audio

Ensure that speakers are not obscured or damaged at either end of the call. Ensure both ends are not muted. Verify that the audio out cables are properly connected to the display and that any external speaker systems are powered and configured correctly.

Power and Connectivity Issues

If a call does not successfully connect, verify that you have dialed a working number and that the far end destination is powered on and available. Verify that the network is ready and available. Network status is indicated at all times in the status bar. If the Avaya system is connected to the local network, a green network status icon appears. A yellow or red network status icon indicates a problem with the network connection. Refer to “The Main Screen” on page 8 for a visual depiction and description of the network status icons.


You may need to reboot a system that is not responding to commands from the remote control. To reboot the system, access **User Preferences : Diagnostics : System Reboot**.


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 35. 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. Refer to the Avaya 1010/1020 Release Notes for the supported Flash Player version. Release Notes are available from support.avaya.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 manage the administrator and user passwords and control remote access to the system through the web, telnet, SNMP and ssh.

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**.

Controlling Remote Administration

By default, remote access to an Avaya 1010/1020 system through the web (http), SNMP, and ssh is enabled; remote access through a telnet session is disabled. To enable or disable remote access through any of these mechanisms, configure preferences in **Administrator Preferences : Security : General**.

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.

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 one or more URLs separated by semicolons that specifies the location of 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; passport.
#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 an Avaya 1010/1020 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/passport.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 : General : 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 that appear in the user interface 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 42.

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	6 UDP ports
Voice	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.

Configuring Communications Preferences

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

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 *Avaya 1010/1020 Installation Guide* for more information about these preferences.

Receiving Presentations



Avaya 1010/1020 can receive but not initiate presentations during a call through a secondary H.239 media channel. By default, the presentation function is enabled. 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.

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  appears when your Avaya system is trying to register with the SIP server. If the registration fails, the red SIP icon  appears.

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

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 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 “Placing a Call” on page 12 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.

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 “Placing a Call” on page 12 for more information.

Enabling Telepresence

You can set Avaya 1010/1020 to telepresence mode 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).

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 1010/1020 can connect to more than one microphone device for audio input during calls (for example, Avaya Video Camera 100, and 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** are Auto (default), Microphone In, and Camera 1.


Camera 1 specifies 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 Microphone In, and then Camera 1, in that order.

Adjusting the Active Microphone Volume

To control the volume of the active microphone, adjust the **Active Microphone Volume** preference in **User Preferences** or **Administrator Preferences : Audio**. For information about using audio meters to set the volume, refer to “Managing Audio” on page 18.

Checking Microphone Status

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 indicating that no active microphone is available.

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*).

Testing Primary Audio Output

You can send audio test tones 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.

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)—Boost the higher frequencies in the sound range for audio output.
- **Line Out Bass** (dB)—Boost the lower frequencies in the sound range for audio 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.
- **System Ringer Volume**—Select the volume level of the system ringer.
- **System Ringer Tone**—Select one of five preset system ringer tones.

Configuring Video Behaviors

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

Controlling Avaya Video Camera 150 Use by Far End Users

To prevent far end users from controlling your PTZ 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 Avaya Video Camera 150 Presets

By default, all users can configure PTZ 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 Avaya Video Camera 150 Pan Direction

You can define the pan direction of the PTZ 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.

Customizing Input Device Names

You can define a custom input name by changing the default value for **HD Camera 1 Name** in **Administrator Preferences : Video : Video Control**. Customized names are limited to 16 characters. The default name is *HD Camera 1*.

Selecting Priority of Quality Metrics for Source Video

You can favor sharpness or motion as a priority for the quality of primary video that Avaya 1010/1020 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.

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, refer to “Placing a Call from the Directory” on page 14.

Administrators 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

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 54.

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 directory. 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**. 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. 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. By default, when an Avaya system joins a network, it sends a broadcast packet to the local subnet to announce its presence. Any Avaya system on the local subnet that receives the packet and has **Auto Discovery** set to *Enabled* replies by sending address information about itself and a list of IP addresses of other Avaya systems that it has discovered.

The Avaya system creates an entry in its corporate directory for every system on the local subnet from which it received a response. It then queries the list of other IP addresses that it received and the IP addresses that are stored in its own Redial list, but only if those addresses are allowed by the filters that you specify in the **Auto Discovery Subnets** and **Auto Discovery Ignored Subnets** preferences. By default, the system replies and sends queries to other Avaya systems in the local subnet only.

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
- the language in which the user interface appears
- 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 53.

Video Layout Preferences

All users can configure the **Picture In Picture** video layout preference in **User Preferences : Appearance**. Refer to “Managing PIP” on page 20 for more information about setting this preference.

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 resolutions when you install your system or change a display and to troubleshoot display issues. Refer to the *Avaya 1010/1020 Installation Guide* for more information.

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 display 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 and a system reboot option. For information about using these preferences and tools, refer to “Using Camera Diagnostic Preferences” on page 31. 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**).
 - 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 42.

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 42. 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 not available from the user interface.

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. Images must be 1280 x 720, .jpg file type, and have unique display names.

Note: Adding a new background image is not supported with the FireFox browser or other browsers based on Mozilla code.

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.

Using Advanced Directory Features

Advanced usage of the directory is available only from the web administration interface. On the **Directory** tab, the **List All** button retrieves the current directory data. You can import and export entries to and from the local directory using the **Import** and **Export** buttons; you can export entries from the corporate directory. **Clear All** deletes all entries in the local directory. **Search** enables you to locate a specific entry in the directory.

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.

Note: System restore is not supported with the FireFox browser or other browsers based on Mozilla code.

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 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. When you move the pointer over an interface element, a tool tip appears to assist you with 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:

- The camera you intend to use with the system is connected to the codec properly.

Note: A camera 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 34.
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** check box.
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 appears 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** check box in step 9, you must first reconfigure your system. Refer to the *Avaya 1010/1020 Installation Guide* for information about initial configuration.

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 Technical Services or your Avaya Partner.

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.

Code	Problem	Description
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.
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.