AVAYA

Avaya 1010 and1020
User and Administrator Guide

Welcome to Avaya Video Conferencing Systems

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 User and 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 | Note: Avaya 1010 and 1020 video conferencing systems are not administrable on H.323 video gatekeepers. |

This guide is divided into four sections. Use the following table to navigate the content.

Using	Describes how to place and manage calls; start a presentation; and create a recording. Read more at Using Avaya 1010 and 1020.
Configuring	Describes how to administer the system. Administrator functionality is password protected. Read more at Configuring Avaya 1010 and 1020.
Preferences	Lists configuration preferences and their default values. Read more at Preferences.
Troubleshooting	Describes symptoms, possible causes, and potential solutions to issues you may encounter with your system. Read more at Troubleshooting.

Section 1: Using Avaya 1010 and 1020

Getting Started

When your Avaya system is idle, a screen saver appears or the screen is black. An incoming call or pressing any button on the remote control automatically activates the system. Point the remote control at the IR receiver (typically located on the camera or the codec), not the screen, to activate the system.

The navigation bar at the bottom of your Avaya system's main screen contains icons that correspond to buttons on the remote control. As you use the arrow keys on the remote control to navigate to different parts of the screen, the icons change depending on available actions. Use the remote control to perform the following tasks:

Placing, answering, and ending a call	From the main screen, select **Video Call** (or **Voice Call**) and press **OK**. Enter the number and press [icon] to place a call. Press **OK** to answer a call and [icon] to end a call. Read more at Placing a Call, Automatically Answering Calls, and Managing a Call.
Controlling a near or far end camera	To adjust a near end PTZ camera when the system is idle, press the **near/far** [icon] camera button. During a call, press [icon] to switch between the near and far end cameras. Read more at Controlling a Far End Camera.
Selecting a screen layout	Press [icon] to change the screen layout during a call. Read more at Managing Video Layouts.
Initiating a presentation through AvayaVirtualLink	With AvayaVirtualLink installed on your laptop, Avaya 1010 and 1020 can share IP-based presentation data during a call. When AvayaVirtualLink initiates the presentation, click **OK** from the Avaya 1010 and 1020 prompt. Read more in the *AvayaVirtualLink Installation Guide*. Download AvayaVirtualLink from support.avaya.com.
Creating a recording	With LifeSize Video Center configured, you may create an out-of-call recording. Read more at Creating a Recording.

Placing a Call

Place a video or voice call with your Avaya system as follows:

- Placing a Call from the REDIAL List on the main screen or Placing a Call from the Directory.

A video icon [icon] represents a video call in progress. A voice icon [icon] represents a voice call.

By default, the system information, status bar, and navigation bar are hidden after a call has been connected for 10 seconds. These items reappear after interaction with the system. Adjust the fade out interval in **User Preferences : Appearance : Fade Out Timeout**. To hide or show user interface elements during a call, press [icon].

Dialing a Number from the Main Screen

1. Use the arrow keys on the remote control to select **Video Call** (or **Voice Call**) and press **OK**.

2. Enter the number you wish to call. The last number entered appears by default. Press 🟢 to delete the number.

3. Press **call** 🔲 .

Additional options:

Edit options	Before placing the call, you may edit the number as follows:
	• Press 🟢 to delete a character.
	• Press 🔺 to change the text entry method. By default, text entry is numeric and **123** appears at the bottom of the screen. To enter a hostname, such as *meetingroom.company.com*, select the **abc** option.
	• Press 🔵 to display 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**.
	Video Calls Only: Press **OK** to exit the field.
Maximum video bandwidth	Set the maximum bandwidth for video calls by navigating to the list next to the entry box for numbers and pressing **OK**. Use the arrow keys to select a maximum bandwidth for the call and then press **OK**.

Placing a Call from the REDIAL List

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

The **REDIAL** list stores up to 15 recently dialed numbers. The last call placed always appears at the top of the list. Unless it is locked, the oldest entry in the list is automatically removed when the system receives a call after the maximum number of entries has been reached.

Each entry includes the name of the system called and an icon that indicates whether the call was a voice 📞 or video 🎦 call. 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.

Adjust the maximum number of entries in the **REDIAL** list in **User Preferences : Calls : Maximum Redial Entries**. You can also remove or lock entries; and add entries from the **REDIAL** list to the local directory. For more information, refer to Managing the REDIAL List.

Automatically Answering Calls

Configure your system to automatically answer incoming calls in **User Preferences : Calls**.

Call Preference	Description	Default Value
Auto Answer	If set to *Disabled*, you must manually answer or ignore incoming calls.	Disabled
Auto Answer Mute	If set to *Enabled* and **Auto Answer** is set to *Enabled*, the system is muted when a call connects.	Enabled
Auto Answer Multiway Call	If set to *Enabled*, the system automatically answers an incoming audio call after the first call has connected. The system beeps to indicate when a new call connects. The **New Call Automatically Answered** dialog box displays the name and number of the added voice caller. Select **Hang Up** and press **OK** to hang up the call. If you ignore the dialog box, the system accepts the call.	Enabled

Enabling Do Not Disturb During Calls

Enable the do not disturb feature from any call screen during a call as follows:

1. Press **OK** on the remote control to display the **Call Manager**.

2. Use the arrow keys to navigate to **Do Not Disturb**.

3. Press **OK**.

If you receive an incoming call during a call and **Auto Answer Multiway Call** is set to *Disabled*, you can choose **Do Not Disturb**, which ignores the incoming call and prevents other calls from interrupting for the duration of the call. The caller hears a busy signal. Calls missed while the do not disturb feature is enabled appear in the **REDIAL** list on the main screen.

Using System Do Not Disturb

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. 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 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, press ⊙ to access the system menu.

2. Use the down arrow key to select **Do Not Disturb**.

3. Click **OK**.

   A dialog box indicates that the system do not disturb feature is enabled.

4. Press **OK** to return the system to normal operation.

Managing a Call

During a call, you can view call status, manage audio output and video images, and control the PTZ camera.

To view call statistics during a call, press ⬤. Statistics include audio and video transmit and receive data such as bandwidth and packet loss, and commonly indicate the cause of problems you may experience during a call. Statistics automatically refresh every 5 seconds and disappear from view after 5 minutes.

Call Encryption

If a video or voice call is encrypted, one of the following icons appears next to the caller ID:

	Denotes a voice call that is encrypted. In the Call Status, Call Manager list, and Call Statistics list, the following icon appears: 📞ₜ

Video Calls Only: If your Avaya system is participating in a multiway call that another Avaya system is hosting and your connection to the host is encrypted, your display shows the encryption status of the participant's connection to the host. If your connection to the host is not encrypted, all connections appear as unencrypted.

Adjusting Audio Preferences

Adjust volume preferences for audio inputs at **User Preferences : Audio**. Preferences appear with an 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.

Use the audio meter to determine the best volume setting. If you adjust the volume of the active microphone, position yourself the same distance from the microphone as participants would be in the room during a video conference. Speak and observe the color of the bars that appear in the audio meter. 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.

For **Active Microphone Volume**, Avaya recommends a volume setting of 5 to 8 for most Avaya Video MicPod 1000 configurations and 5 to 10 for most Avaya Video Camera 100 configurations.

Managing Video Layouts

To change the screen layout of near and far end video images, press [icon] at any time during a call.

The number of the selected screen layout (*x*) and the total number of available screen layouts (*y*) appear in the center of the screen above the status bar as *x/y*.

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.

Two-way Call

Layouts 1/2 and 2/3

Far video

Layout 2/3: Far and near video swap positions

Near video (disappears)

Layout 3/3

Far video	Near video
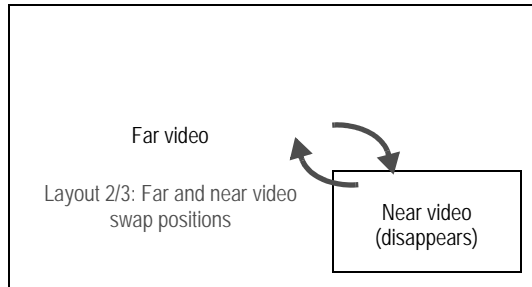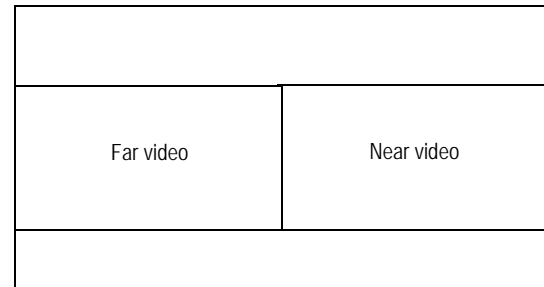
Two-way Call with Presentation

Layouts 1/6 and 2/6

Presentation

Layout 2/6: Presentation and near video swap positions

Near video (disappears)

Layout 3/6

Presentation	Near video

Layouts 4/6 and 5/6

Far video

Layout 5/6: Far and near video swap positions

Near video (disappears)

Layout 6/6

Far video	Near video
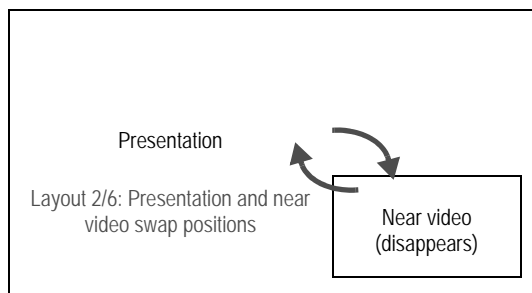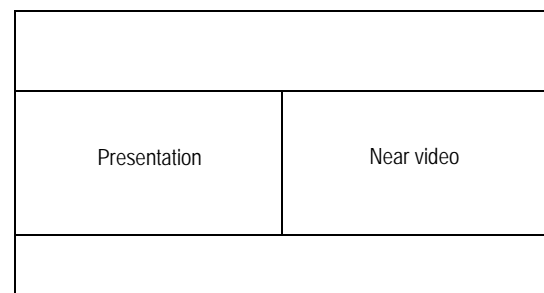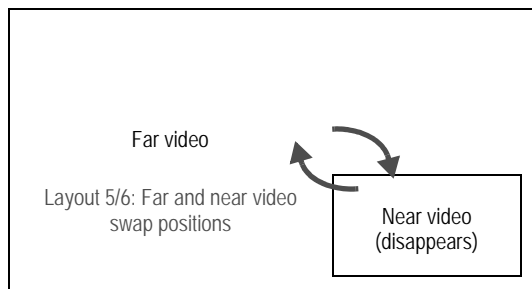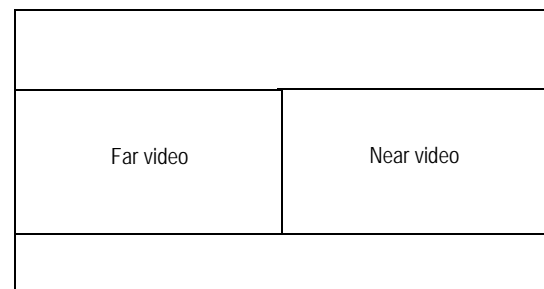
Controlling a Far End Camera

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. 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.

Selecting a Far End Camera

Do the following from any call screen:

1. Press the **near/far** [icon] camera button.

    The blue camera icon [icon] appears in the far end video image in the call.

2. If more than one video participant is connected, continue to press [icon] until [icon] appears in the far end video image of the participant whose camera you wish to control.

3. Use the arrow and zoom keys on the remote control to adjust the PTZ camera.

Selecting the Far End Primary Input

1. Select the far end participant whose input device you wish to control by following the steps in Selecting a Far End Camera.

2. Press **input** [icon] to choose the far end input device.

    A menu of available input devices appears.

3. Use the arrow keys on the remote control to select a device and press **OK**.

Ending a Call

Remote control	Press **hang up** [icon]. Pressing [icon] in a two-way call, ends the call. When you press [icon] in a multiway call, the Call Manager appears.
Call Manager	Press **OK** to show the Call Manager and select **Hang Up**.
REDIAL list	Press [icon] to show the main screen and REDIAL list. Select the call you wish to end and press **OK**.

NOTE   If your Avaya system is participating in a multiway video call hosted by another Avaya system, all visible callers appear in the Call Manager rather than only the system hosting the call. You can hang up only your connection to the system hosting the call.

Managing the REDIAL List

Manage an entry in the REDIAL list by selecting the entry and pressing ⌘ on the remote control. The following options are available:

Save	Adds the entry to the local directory.
Remove	Removes the entry from the REDIAL list.
Lock	Prevents the entry 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. Locking an entry does not prevent it from being removed from the list manually.

Adjust the maximum number of entries in the **REDIAL** list by setting **User Preferences : Calls : Maximum Redial Entries**. Choosing *None* removes entries from the **REDIAL** list and prevents new entries from appearing on the list.

Creating a Recording

With LifeSize Video Center configured in your environment, you may initiate an out-of-call recording. Read more in the *LifeSize Video Center Administrator Guide.*

1. From the main screen, press ⬛.
2. Press ⚫.
3. If prompted, enter a valid recording key. If successful, the recording begins and the recording icon appears.
4. To end the recording, press ⚫.

Advanced Camera Functions

Avaya Video Camera 100 does not support advanced camera functions.

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

Configure and use presets in the **Primary Input** screen before placing a call as follows:

1. Press **near/far** 🔘 to select the near end camera and then adjust its position.

2. Press and hold a numeric key (1 through 9) on the remote control until **Preset *x* saved** appears above the status bar. The current position of the camera is associated with the numeric key.

    If you choose a numeric key that already has a preset configured, it is overwritten. If an existing preset associated with the key is locked, **Preset *x* locked** appears. 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*** appears above the status bar.

Using Camera Presets During a Call

1. If not already selected, press **near/far** 🔘 to select the near end camera.

2. Ensure that **Presets** appears to the right of the numeric keys icons in the navigation bar from any call screen. If **Touch Tones** appears instead, change the function of the keys to **Presets** by pressing 🔘.

3. Press the numeric key on the remote control that represents the preset you wish to use. **Preset *x*** appears on the screen.

    If you configured a preset for a far end camera in the call, you must select the far end camera to use the preset. Refer to Controlling a Far End Camera.

    NOTE   During a call, the numeric keys work as presets only from a call screen.

Locking Camera Presets

By default, all users can configure camera presets. To prevent all users (near and far end) from configuring camera presets, administrators can set **Administrator Preferences : Video : Video Control : Camera Presets Lock** to *Locked*. To prevent only far end users from configuring camera presets, set **Far Control of Near Camera** or **Far Set of Camera Presets** to *Disabled*.

Working with Directories

The directory includes three subdirectories:

Local	Each entry contains dialing information for a single device.
Corporate	Each read-only entry contains dialing information for a single device.
Meetings	Each entry contains dialing information for one or multiple devices. When you place a call, the system dials all the devices in the entry.

Placing a Call from the Directory

1. From the main screen, press ⬆ to access the directory.

2. Use the arrow keys to select the **Local**, **Corporate**, or **Meetings** directory and press **OK**.

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.

---

3. Use the arrow keys to select the entry that you wish to dial.

4. Press **OK** to place the call.

Browsing the Directory

Browse the directory using 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. Place an entry into a hierarchy when you create the entry or at any time by editing the **Hierarchy** field. Using the hierarchical method, 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 ⬆. Use the ⊕ and ⊖ buttons to move up or down a page of entries when an entry is selected.

Adding an Entry to the Local or Meetings Directory

Create up to 1000 entries in the local directory and 100 entries in the meetings directory.

1. From the main screen, press ⬆ to access the directory.

2. Using the arrow keys, select the **Local** or **Meetings** directory.

3. Select **Add New Entry** and press **OK**.

4. Do one of the following:

    -   *Local directory*: 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.

NOTE   If necessary, press ⬆ 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.

- *Meetings directory*: Select **Meeting Name** and press **OK**. Enter a name for the meeting.

  Select the directory (**Local**, **Corporate**, or **Both**) from which you wish to choose entries to add.

  In the **Available Entries** column, select an entry to add to the **Participants** column and press **OK**.

  If the entry has more than one number, a submenu that contains each number appears. Select the number on the submenu that you wish to dial for the meeting and press **OK**. Select an entry from the **Available Entries** column for each participant that you wish to add to the meeting entry.

5. *Predefined hierarchy*: In the **Hierarchy** field, enter the path for the entry's location in the hierarchy. Hierarchies can be defined by location or department. You must identify the full path (separated by commas) of a predefined hierarchy in which to add an entry before you leave 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 grouped alphabetically.

   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. Select **Add Entry** (or **Add Meeting**) and press **OK.**

Copying, Removing, and Editing Entries

Copy, remove, or edit an entry by accessing the directory ⏶; selecting the entry; and pressing ⌘ . Depending on the entry, the following options may be available:

Copy to local	When you access the corporate directory, you can copy an entry to the local directory.
Remove	Selecting this option removes the entry from the local or meetings directory.
Edit	Modify values in the **Edit Directory Entry** or **Edit Meeting Entry** dialog box. If necessary, press ⏶ to change the method of text entry for text fields.

Section 2: Configuring Avaya 1010 and 1020

This section describes how to administer your Avaya video communications system.

Initial configuration	At installation, your Avaya system prompts you to configure basic required settings. Initial configuration screens also appear after you restore the system to default settings. Read more at Initial Configuration.
Passwords	Manage user and administrator passwords. Read more at Administrator and User Passwords.
System management	Manage your system with the remote control; through a browser or with Avaya Video Conferencing Manager. Learn more at Managing Your System.
Network	Configure network preferences. Read more at Configuring Network Usage.
Appearance	Configure video layout and display preferences. Read more at Configuring Appearance.
Calls	Manage call bandwidth and set a maximum call time. Read more at Configuring Call Preferences.
Communications	Control the protocols the system uses during calls. Read more at Configuring Communications Preferences.
Audio	Select the active microphone and adjust audio levels. Read more at Configuring Audio Behaviors.
Video	Control cameras and video quality. Read more at Configuring Video Behaviors.
Directories	Manage the local, corporate, and meetings directories. Read more at Directories.
Interface lock	Lock the interface and cameras. Read more at Locking the Interface.
Maintenance and upgrade	Learn how to upgrade system software; update license keys; and restore a system to its default settings at Maintaining Your System.

NOTE   Administrator functionality is password protected.

Initial Configuration

At the end of the installation process, your Avaya system prompts you to configure preferences required for the system to start. The initial configuration screens also appear when you perform a system reset.

Language	Select the language to display in the user interface. The default is English.
Passwords	Manage the administrator and user passwords. Read more at Administrator and User Passwords.
System identification	Set the location, time zone, system name, video number, and voice number.
Communications	Select the video and voice protocols.
Network	By default, DHCP is enabled on Avaya systems. If you disable DHCP, you must specify the system's IP address, subnet mask, and default gateway. Read more at Specifying a Locally Configured IP Address. Enter the hostname of the system and the IP addresses to configure DNS servers if you do not have a DHCP server that automatically sets a DNS server. Read more at Specifying the Hostname and DNS Servers. If you set the network speed, ensure that the option matches the speed and duplex configured on your network switch. Read more at Specifying Network Speed. The system shows the date and time automatically with DHCP enabled or when you specify the hostname or IP address of an NTP server. Read more at Specifying an NTP Server.
Audio	By default, the system detects attached audio input devices and selects the active microphone. To adjust audio preferences, refer to the following: • Selecting the Active Microphone • Adjusting the Active Microphone Volume • Testing primary audio output

NOTE After initial configuration, manage these preferences from the main interface or through the web administration interface. Read more at Managing Your System.

Administrator and User Passwords

Change the user and administrator passwords during initial configuration or in **Administrator Preferences : Security : Passwords**. Passwords can be up to 16 characters in length and contain any combination of the numbers 0-9 and the symbols * (star) and # (pound).

The default administrator password is 1 2 3 4. Avaya recommends that you protect the administrator preferences with a secure password.

Set a user password to control access to **User Preferences** screens. By default, the user password is not set. If you set a user password, you can also access the **User Preferences** screens with the administrator password.

Managing Your System

Remote control	To configure your Avaya system with the remote control, follow these steps:
	1. From the main screen, press ⊙ to access the **System Menu**.
	2. Select **Administrator Preferences** and press **OK**.
	3. Enter the administrator password (by default, 1 2 3 4) and press **OK**.
	If you enter an incorrect password, press ↩ to clear the error message.
Browser	To configure your Avaya system from a web browser, you must have Adobe Flash Player installed and configured on your web browser.
	1. Open a web browser and enter the IP address of the Avaya system. The IP address of the system appears at the top of the main screen.
	2. Enter the administrator password and click **Submit**. This is a secure Internet connection and you may receive an unknown certificate warning.
	By default, remote access to an Avaya system through a web browser is enabled. To disable remote access through a web browser, set **Administrator Preferences : Security : General : HTTP** to *Disabled*.
Avaya Video Conferencing Manager	With Avaya Video Conferencing Manager, administrators can manage video systems across the enterprise. Avaya Video Conferencing Manager features include resource scheduling, monitoring, reporting, and remote upgrading.

Viewing Recent Configuration Changes

To quickly access a preference that has been recently changed, navigate to **Administrator Preferences : Recent**. Preferences that have dependencies on other preference settings, such as SIP server preferences, may not appear in **Recent**.

NOTE   Upgrading the system software removes all preferences from **Recent**.

Configuring Network Usage

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 the following:

IP address	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
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, 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 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.

- A configuration file that contains Avaya command line interface commands must exist at the location specified by the DHCP option. Read more at Saving and Restoring a System Configuration.

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.

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

        "Avaya: server=<*path*>"

where <*path*> is a URL that specifies the configuration file location. Separate multiple URLs with a semicolon. 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.

If the server requires a username and password to access the file (for example, to log into an FTP server), you can include the username and password in the URL. 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. Use the underscore character to replace the colon between bytes. The MAC address resolves to a hexadecimal number with lowercase letters.
#S	Replaced by the system model: 1010/1020
#I	Replaced by the assigned IP address.

If a machine name or IP address is used alone as a path element, 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.

The first file found is used. If the checksum of the file is different from the last configuration file loaded into the system, 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 when 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 DNS Servers

Enter the hostname of the system and the IP addresses to configure Domain Name Service (DNS) servers in **Administrator Preferences : Network : General : Hostname** and **DNS Servers**. DNS translates names of network nodes into addresses. Specify this preference to use DNS to resolve the hostnames of devices to IP addresses. You can also enter the domain names to search when resolving hostnames in **Name Search Domains**.

Specifying Network Speed

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

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, configure your Avaya system to apply a VLAN tag to outgoing packets and accept only incoming tagged packets that have the same VLAN identifier. Specify the VLAN identifier of the VLAN to which the system is assigned in **Administrator Preferences : Network : General : VLAN Tag**. The value is a number in the range 1 through 4094.

If you set or modify **VLAN Tag**, 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:

- **Administrator Preferences : Network : General : DHCP** is enabled and the DHCP server can pass an NTP server address to your system.

  - or -

- **Administrator Preferences : Network : General : NTP Server Hostname** specifies the hostname or IP address of an NTP server.

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

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

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. Specify the time zone in **Administrator Preferences : System : Date and Time**.

Configuring Appearance

Configure how to display information on your system in **Administrator Preferences : Appearance**.

Picture in Picture

With Picture In Picture (PIP) enabled, the primary input always appears. Change the default setting so that PIP never or always appears in **Administrator Preferences : Appearance : Layout**.

Display Preferences

Specify display types, resolutions, and energy management options in **Administrator Preferences : Appearance : Displays**. Typically, you configure display resolutions when you install your system or change a display and when you troubleshoot display issues. Refer to the *Avaya 1010 and 1020 Installation Guide* for more information.

Set **Display Energy Saver** 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.

Hiding User Interface Elements

Hide the following user interface elements in **Administrator Preferences : Appearance : General**.

Preference	Description	Default Value
Company Logo	Choose *None* to hide the Avaya logo in the user interface and screen saver. The *Default* option shows the logo.	Default
Clear Last Number Dialed	When enabled, clears the last number manually dialed from the main screen.	Disabled

To hide all IP addresses in the user interface, enable **Hide IP Addresses** and **Clear Last Number Dialed**.

Custom Backgrounds

Manage the system's background from the user interface and the web administration interface.

Specifying a Background Color

1. Navigate to **Administrator Preferences : Appearance : Backgrounds**.

2. Set **Background Image** to *None*.

3. Set **Display Background Color** to the desired color.

Adding a Custom Background Image

You can add or remove custom background images only from the web administration interface.

1. Open a browser and enter the system's IP address to log into the web administration interface.

2. Access **Preferences : Appearance : Backgrounds**.

3. Click **Add** and browse to the image file. Images must be 1280 x 720 JPGs with unique display names.

4. To apply the new image, select it and click the desired display.

Choosing a Background Color from the Interface

You can choose a custom background color only from the web administration interface.

1. Open a browser and enter the system's IP address to log into the web administration interface.

2. Access **Preferences : Appearance : Backgrounds**.

3. Click the color swatch next to the current background for the display.

4. Use the eye dropper 🖊 to choose a color from the web administration interface.

5. Click the display to apply the color.

Defining a Custom Color

You can define a custom color only from the web administration interface.

1. Open a browser and enter the system's IP address to log into the web administration interface.

2. Access **Preferences : Appearance : Backgrounds**.

3. Click the color wheel 🔵 to access the color editor.

4. Specify a custom color by supplying RGB values or a hexadecimal value; or choose a predefined color by clicking a color swatch from the color editor.

5. Click **Save Changes**.

6. Click the display to apply the color.

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. Read more at Automatically Answering Calls and Managing the REDIAL List.

Administrators configure additional call preferences in **Administrator Preferences : Calls**.

Managing Bandwidth

Specify the maximum bandwidth that an outgoing or incoming call uses by setting **Outgoing Call Bandwidth** or **Incoming Call Bandwidth** in **Administrator Preferences : Calls**. The value for **Outgoing Call Bandwidth** becomes the maximum value that users can choose from the dropdown menu when manually placing a call from the main page or when specifying a bandwidth in a directory entry.

If a user specifies *Auto* for the bandwidth when placing a call, the outgoing bandwidth becomes the starting point for negotiating bandwidth when the call connects. In addition, the system uses the appropriate bandwidth based on the following:

*   display resolution and frame rate of the device: 1080p30 or 720p60

*   capability of the input device

Outgoing Total Bandwidth and **Incoming Total Bandwidth** set the maximum amount of network bandwidth to use for all outgoing and incoming calls.

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

Selecting a Maximum Call Time

Control the amount of time that a call stays connected at **Administrator Preferences : Calls : Maximum Call Time**. When this preference is set and the time expires, the call stops without an option to extend.

Admission Control

Admission control rejects calls to multiway capable systems under a heavy call load. Enable or disable this preference in **Administrator Preferences : Calls : Admission Control**.

Hiding the Dominant Speaker Icon

The dominant speaker icon indicates which participant is speaking. Hide the icon by disabling **Administrator Preferences : Calls : Dominant Speaker Icon**.

Configuring Communications Preferences

Specify protocols the system uses during calls in **Administrator Preferences : Communications**.

Disabling Multiway Calling

Disable multiway calling by setting **Administrator Preferences : Communications : General : Multiway Calls** to *Disabled*. You can configure this preference only when the system is not in a call. Choosing *Disabled* allows only one call, voice or video, to connect to the system.

Enabling Presentations

Avaya 1010 and 1020 can share data during a call with the following preferences enabled in **Administrator Preferences : Communications : General**:

Presentations	By default, Avaya 1010 and 1020 can receive presentations. Consider disabling the presentation function if your system experiences interoperability issues with third party systems that do not support presentations.
Network Presentations	With AvayaVirtualLink installed on the presenter's laptop, Avaya 1010 and 1020 can initiate presentations by sharing data over IP during a call. By default, support for network presentations is enabled. Read more in the *AvayaVirtualLink Installation Guide*.

Configuring SIP Settings

By default, Avaya systems support Session Initiation Protocol (SIP). Disable support for SIP calls in **Administrator Preferences : Communications : SIP** when the system is not in a call.

NOTE   If **SIP** is disabled, a warning message indicates that video calls cannot be placed or received with this configuration.

Preference	Description	Default Value
SIP	When enabled, allows you to specify a SIP name to use when placing a call.	Enabled
SIP Username	SIP username for the device.	Avaya
Authorization Name	SIP server authorization username. Set a value only if required by the registrar or proxy.	No default
Authorization Password	SIP server authorization password. Set a value only if required by the registrar or proxy.	No default
SIP Server Type	Type of SIP registrar and proxy servers.	Auto
SIP Registration	Communication path to use when registering with a SIP registrar. SIP devices use register settings to dynamically register their current location.	Through Proxy
SIP Proxy	When enabled, uses a SIP proxy server.	Disabled
Proxy Hostname	Hostname or IP address of the SIP proxy server.	No default
SIP Registrar	When enabled, uses a SIP registrar server.	Disabled
Registrar Hostname	Hostname or IP address of the SIP registrar server.	No default
SIP Signaling	Preferred SIP signaling protocol. To specify the signaling protocol, a SIP registrar must be enabled. Signaling protocols are mutually exclusive; that is, enabling one disables the others. Disabling the SIP registrar automatically sets the signaling protocol to *Auto*.	Auto
UDP Signaling Port	UDP port number of the SIP configuration.	5060
TCP Signaling Port	TCP port number of the SIP configuration.	5060

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

NOTE   The system reboots if you change the signaling port; or enable or disable signaling.

Configuring Audio Behaviors

Adjust audio behaviors in **Administrator Preferences : Audio** by Selecting the Active Microphone and Adjusting Audio Volume.

Additional audio settings include:

Microphone status	The **Active Microphone** field on the **System Information** page shows which device is functioning as the active microphone. When the value is *None*, ⬤ appears in the status bar of the user interface.
	The **Microphone In** field appears on 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	Test audio output to speakers connected to the codec as the primary audio output device during initial configuration or in **Administrator Preferences : Audio : Primary Audio Output Test**. Select a channel to test, or select *Auto*. The *Auto* option cycles through available channels and plays 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.
Configuring audio codec order	Change the order of audio codecs the system uses when placing calls in **Administrator Preferences : Audio : Audio Codec Order**.

Selecting the Active Microphone

Avaya 1010 and 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.

Select a device to serve as the active microphone during initial configuration or in **Administrator Preferences : Audio : Active Microphone**. The options that are available for the **Active Microphone** are *Auto* (default), *Microphone In*, and *Camera 1* (specifies Avaya Video Camera 100 as the active microphone).

When **Active Microphone** is set to *Auto* (the default), or if the option selected is not connected to the codec, the system automatically attempts to select Microphone In, and then Camera 1, in that order.

Adjusting Audio Volume

Adjusting the Active Microphone Volume

Adjust **Active Microphone Volume** in **User Preferences** or **Administrator 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**.

The audio meter displays the level of the transmitted voice in decibels (dB) root mean square (RMS) below digital full scale (DFS). The meter is accurate to ± 1 dB. The maximum level is 0 dB. Levels below –50 dB are not displayed, and indicate a very quiet or inactive input. Typical levels during a call peak around –28 to –22 dB DFS.

To set the level for your audio input, position someone approximately one meter from the microphone, facing it, speaking 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 **Active Microphone Volume** for most Avaya Video MicPod 1000 applications and a volume setting of 5 to 10 for most Avaya Video Camera 100 applications. Use the audio meter to visually verify that the transmit level peaks in the desired -28 to -22 dB range.

Adjusting Audio Levels

Line Out Treble (dB)	Adjust the higher frequencies in the sound range for the audio output.
Line Out Bass (dB)	Adjust the lower frequencies in the sound range for the 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 control cameras and video quality in **Administrator Preferences : Video**.

Controlling Camera Use by Far End Users

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

Controlling Camera Pan Direction

Define the camera's pan direction 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.

Adaptive Motion Control

Adaptive motion control minimizes video problems caused by minor packet loss and improves video reproduction. For packet loss of 5% or less, this feature eliminates or greatly reduces video artifacts. This feature is enabled by default in **Administrator Preferences : Video : Video Quality : Adaptive Motion Control**.

Customizing Input Device Names

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 for the quality of primary video that Avaya 1010 and 1020 sends to the far end during a call. If you favor sharpness by selecting a smaller number in **Administrator Preferences : Video : Video Quality : Primary Video Motion**, in lower bandwidth calls the system sends the primary video at a lower frame rate and a higher resolution. The default value (10) favors motion. Consider adjusting this preference if bandwidth is limited.

Adjusting Video Encoder Quality

Adjust the quality of the video image sent to the far end during a call by specifying a relative lower or higher resolution in **Administrator Preferences : Video : Video Quality : Video Encoder Quality**. Moving the slider to the right improves the quality of the video image.

Adjusting the MTU of Video Packets

Video packets that exceed the maximum transmission unit (MTU) size for any router or segment along the network path may be fragmented or dropped. This results in poor quality video at the receiving device. Set the MTU of video packets that your Avaya system sends in **Administrator Preferences : Video : Video Quality : Video MTU**. The default value is 1440 bytes. The allowed range is 900 -1500 bytes.

Configuring Avaya Video Communications Systems to Record

With LifeSize Video Center in your environment, Avaya video systems can initiate an out-of-call recording to LifeSize Video Center. By default, the recording capability is disabled. To enable recording, complete these steps:

1. On the Avaya video communications system, navigate to **Administrator Preferences : Video : Record and Stream**.

2. Set **Recorder** to *Enabled*.

3. In **Recorder Hostname**, enter the IP or DNS address of the recording and streaming server. In most cases, you can accept the default of **Recorder Port** set to 443.

    NOTE   If your network uses NAT with port forwarding rules that remap port 443 between the video communications system and the server, **Recorder Port** must reflect the remapped port number.

4. To provide a default key to use for server authorization for all recordings from this system, enter it in **Recording Key**. If you leave this setting blank, the system prompts users to enter a key for each recording.

Directories

Your Avaya system includes three directories: local, corporate, and meetings. Users can place calls from all directories; and add entries to the local and meetings directories. Read more at Working with Directories.

Disabling Access to the Local Directory

By default, users can add, remove, or modify entries; and place calls from the local directory. Disable user access to the local directory by setting **Local Directory** to *Disabled* in **Administrator Preferences : Directory : General**. Disabling access to the local directory also disables the following:

• Saving entries from the **REDIAL** list to the local directory.

• Copying corporate directory entries to the local directory.

• Selecting entries from the local directory when creating an entry in the meetings directory.

Even if access is disabled from the user interface, you can access the local directory on the **Directory** page in the web administration interface. Read more at Managing Directories from the Web Administration Interface.

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 alphabetical and hierarchical format. All users can manage entries in the local and meetings directories. Only administrators can manage entries in the corporate directory.

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

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.

LDAP Connection Status	Description
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. When an Avaya system joins a network, by default 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 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 **Auto Discovery Subnets** and **Auto Discovery Ignored Subnets**. By default, the system replies and sends queries to other Avaya systems in the local subnet only.

Configure **Auto Discovery Subnets** and **Auto Discovery Ignored Subnets** 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 **Auto Discovery Subnets** to identify the subnets where the Avaya system can send queries and replies. By default, the preference is empty and 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 **Auto Discovery Ignored Subnets**. If a destination address does not match one of the filters in **Auto Discovery Subnets**, or if it matches one of the filters in **Auto Discovery Ignored Subnets**, the Avaya system does not query or reply to the Avaya system at that address.

For example, configure **Auto Discovery Subnets** to include a large subnet and **Auto Discovery Ignored Subnets** 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 **Auto Discovery Subnets** and 10.85.* in **Auto Discovery Ignored Subnets**, 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.

Managing Directories from the Web Administration Interface

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

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

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

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

Locking the Interface

To lock the interface and cameras, set **Administrator Preferences : Telepresence : Telepresence** to *Enabled*.

During a call, the user interface behaves as follows:

•   Video from the call and the mute indicators appear.

•   The navigation bar, PIP windows, caller ID information, and call status messages do not appear.

Users interact with the system using an attached phone. Additionally, during a call, users can do the following:

•   Press **OK** on the remote control to show the **Call Manager**.

•   Press to show call statistics.

•   Press to change the layout.

•   Use the numeric keys on the remote control play touch tones. Change this behavior from the **Call Manager**.

NOTE   To hide all user interface items while in a call, enable **Hide User Interface**.

When the system is idle, only the background image appears in the display.

To access the locked interface, press **OK** and enter the administrator password.

Maintaining Your System

Upgrading System Software

This section describes how to apply software updates to your system. Use the same process to downgrade your system to a previous version. Before performing an upgrade or downgrade, consider saving your configuration. Read more at Saving and Restoring a System Configuration.

NOTE	After performing a downgrade, you must reset the system to factory defaults.

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

* The camera you intend to use with the system is properly connected to the codec. 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. Download the upgrade to a local directory on your system.

2. Access the web administration interface by entering the IP address of your system in a supported web browser and logging in.

3. Click the **Maintenance** tab.

4. Click **System Upgrade**.

5. If your upgrade requires you to reset the system to the original default settings, select **Reset to Default State**.

6. Browse for the upgrade file you downloaded in step 1.

7. Click **Upgrade**.

NOTE	If calls are connected to the system, a dialog box prompts 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; users cannot cancel the screen; and the system rejects incoming calls.

8. A system upgrade status message appears when the upgrade is complete. Close the status and the administrator configuration windows.

9. If you selected **Reset to Default State** in step 5, you must reconfigure your system. Read more at Initial Configuration.

10. To access all web administration options after an upgrade (or downgrade), close your web browser, clear the browser cache, and reopen your web browser.

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.

Upgrade Error Codes

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 while copying the image to the upgrade partition. This typically occurs when you use an upgrade image for another Avaya product.
4	Read failed	Reading incoming data failed during the image upload. This typically occurs if the connection is broken during the upload.
5	Upgrade script failed	After the image successfully uploads, the system runs an upgrade script for final processing. This error indicates a failure in the script. This typically occurs when you use 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 you use an upgrade image for another Avaya product.
7	Unable to mount upgrade partition	After the image was copied to the system, the system failed to mount the image. This typically occurs if the upgrade image is corrupt or when you use 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 because of 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 you use 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 supports only one upgrade at a time.

Default Settings

Administrator preferences contain the system configuration settings. You may need to reset the system to its default state to correct problems or to return to a known configuration. 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

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. Users can then access **User Preferences** without a password. The system prompts you to complete the Initial Configuration.

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

Resetting a System Using the Reset Button

Manually reset the system using the **Reset** button on the back of the codec.

NOTE   You can use the reset button without removing power to the system.

Press and hold the reset button. The blue LED on the front of the codec changes color or behavior approximately every five seconds until the LED turns solid blue. The following table indicates the sequence of color and behavior changes of the LED and the corresponding system behavior 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 default settings.
flashing blue (shorter duration on than off)	The system reboots using the alternate software image installed on the system and resets preferences to default settings.
solid blue	The system reboots without changes to the configuration.

Rebooting the System

The system reboots when you do any of the following:

Reboot the system.	**Administrator Preferences : Diagnostics : System Reboot** **User Preferences : Diagnostics : System Reboot**
Reset the system to its default state.	**Administrator Preferences : System : System Reset**
Restore a system configuration.	*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 system software.	*Web administration interface*: **Maintenance : System Upgrade**
Initiate changes that result in fragmented memory and prevent the user interface from being successfully reloaded.	Repeatedly change the language that appears in the user interface or the display connected to an Avaya system to a resolution that requires the user interface to be reloaded into memory; for example, from 720 to 1080.

If the user interface is not responding and you are unable to reboot the system, you can reboot the system by pressing the reset button on the back of the codec. Avaya recommends that you do not unplug power from the codec to reboot it.

Saving and Restoring a System Configuration

System Save in the web administration interface creates a text file that contains command line interface commands to restore a saved configuration. The saved configuration includes preferences that can be set through the command line interface except the command line interface password and the password for the default SNMP user. Consider using **System Save** as part of regular system maintenance.

System Restore restores a system configuration using the saved configuration file. To customize a configuration, edit the file manually before restoring it. If you use a system configuration file for multiple systems, ensure that you edit unique settings, such as the system name or other credentials.

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

Saving a System Configuration

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**.

Restoring a System Configuration

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

---

1. 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.

2. Hang up all calls connected to the system. If calls are connected when you perform a restore, a dialog box prompts you to continue or cancel the restore. If you continue, the system restore process terminates the calls.

3. In the web administration interface, navigate to **Preferences : System : System Reset**.

4. Click **System Restore**.

5. Click **Continue**. The Avaya system reboots and a dialog appears indicating that the restore succeeded.

Identifying the System

Change the system name, dialing numbers, and geographic location specified for the system in **Administrator Preferences : System : Identification**.

Setting System Date and Time

Set the system time zone; or manually set the date and time in **Administrator Preferences : System : Date and Time**.

Section 3: Preferences

This section lists configuration preferences as they are grouped in the interface. As you work with preferences, consider the following:

- Administrators have access to all of the preferences; users have access to a subset.

- Defaults for both users are the same.

- Changing a value in **Administrator Preferences** also changes the value in **User Preferences**. Likewise, changing a value in **User Preferences** changes the value in **Administrator Preferences**.

Access preferences as follows:

1. From the main screen, press ⦿ to access the **System Menu**.

2. Select one of the following:

    - **User Preferences**

    - **Administrator Preferences**

3. Press **OK**.

4. If prompted, enter the password and press **OK**.

    By default, the administrator password is 1 2 3 4, and the user password is not set.

Calls

Administrator Preferences : Calls User Preferences : Calls	Default Value	Available in User Preferences
Outgoing Call Bandwidth	Auto	
Incoming Call Bandwidth	Auto	
Outgoing Total Bandwidth	Auto	
Incoming Total Bandwidth	Auto	
Auto Bandwidth	Enabled	
Maximum Call Time	8 hours	
Maximum Redial Entries	10	X
Dominant Speaker Icon	Enabled	
Auto Answer	Disabled	X
Auto Answer Mute	Enabled	X
Auto Answer Multiway Call	Enabled	X
Admission Control	Enabled	

Audio

Administrator Preferences : Audio User Preferences : Audio	Default Value	Available in User Preferences
Audio Codec Order: 1. AAC-LC 2. G.722.1C, licensed from Polycom® (48 kb/s) 3. G.722.1C, licensed from Polycom® (32 kb/s) 4. G.722.1C, licensed from Polycom® (24 kb/s) 5. G722.1, licensed from Polycom® (24 kb/s) 6. G.722 7. G.729 8. G.728 9. G.711 (μ-Law) 10. G.711 (A-Law)	N/A	
Active Microphone	Auto	
Active Microphone Volume	5	X
Primary Audio Output Test	Off	
Video Call Audio Output	HD Out	
Voice Call Audio Output	HD Out	
Line Out Treble	0 dB	X
Line Out Bass	0 dB	X
Ring Tone Volume	5	X

Administrator Preferences : Audio User Preferences : Audio	Default Value	Available in User Preferences
DTMF Tone Volume	5	X
Status Tone Volume	5	X
System Ringer	Enabled	
System Ringer Volume	5	X
System Ringer Tone	Tone 1	

Telepresence

Administrator Preferences : Telepresence	Default Value	Available in User Preferences
Telepresence	Disabled	
Hide User Interface	Disabled	
HD Camera 1 Movement	Unlocked	

Video

Administrator Preferences : Video : Video Control	Default Value	Available in User Preferences
Far Control of Near Camera	Enabled	
Far Set of Camera Presets	Disabled	
Far Move to Camera Presets	Enabled	
Camera Presets Lock	Unlocked	
Camera Pan Direction	Perceived	
HD Camera 1 Name	HD Camera 1	

Administrator Preferences : Video : Video Quality	Default Value	Available in User Preferences
Video Bandwidth Balance	90%/10%	
Primary Video Motion	10	
Video Encoder Quality	-2	
Adaptive Motion Control	Enabled	

Administrator Preferences : Video : Record and Stream	Default Value	Available in User Preferences
Recorder	Disabled	
Recorder Hostname	No default	
Recorder Port	443	
Recording Key	No default	

Security

Administrator Preferences : Security : General	Default Value	Available in User Preferences
FIPS 140-2	Disabled	
HTTP	Enabled	
SNMP	Enabled	

Administrator Preferences : Security : Passwords	Default Value	Available in User Preferences
Administrator Password	1234	
User Password	not set	

Network

Administrator Preferences : Network : General	Default Value	Available in User Preferences
DHCP	Enabled	
IP Address	No default	
Subnet Mask	255.255.255.0	
Default Gateway	No default	
Hostname	Avaya	
DNS Servers	No default	
Name Search Domains	No default	
Network Speed	Auto	
VLAN Tag	No default	
NTP Server Hostname	No default	
802.1x Authentication	Disabled	

Administrator Preferences : Network : NAT	Default Value	Available in User Preferences
NAT	Disabled	
NAT Public IP Address	No default	

Administrator Preferences : Network : Reserved Ports	Default Value	Available in User Preferences
UDP Lowest Value	60000	
UDP Highest Value	64999	
TCP Lowest Value	60000	
TCP Highest Value	64999	

Administrator Preferences : Network : Network QoS	Default Value	Available in User Preferences
Network QoS	None	
DiffServ Audio Priority	46	
DiffServ Video Priority	34	
DiffServ Data Priority	46	
IntServ Audio Priority	5	
IntServ Video Priority	4	
IntServ Data Priority	5	
IntServ ToS	None	

Administrator Preferences : Network : LifeSize Transit	Default Value	Available in User Preferences
Not Available		

Communications

Administrator Preferences : Communications : General	Default Value	Available in User Preferences
Multiway Calls	Enabled	
Presentations	Enabled	
Network Presentations	Enabled	

Administrator Preferences : Communications : SIP	Default Value	Available in User Preferences
SIP	Enabled	
SIP Username	Avaya	
Authorization Name	No default	
Authorization Password	No default	
SIP Registration	Through Proxy	
SIP Proxy	Disabled	
Proxy Hostname	No default	
SIP Registrar	Disabled	
Registrar Hostname	No default	
SIP Signaling	Auto	
UDP Signaling Port	5060	
TCP Signaling Port	5060	

Administrator Preferences : Communications : H.323	Default Value	Available in User Preferences
Not Available		

System

Administrator Preferences : System : General	Default Value	Available in User Preferences
Auto Reboot	No	

Administrator Preferences : System : Identification	Default Value	Available in User Preferences
System Name	Conference Room	
Video Number	No default	
Voice Number	No default	
Location	United States	

Administrator Preferences : System : Date and Time	Default Value	Available in User Preferences
Time Zone	GMT (Greenwich Mean Time)	
Day, Month, Year, Hour, Minutes, Seconds	GMT values	

Administrator Preferences : System : Serial Ports	Default Value	Available in User Preferences
USB Serial Shell	None	
USB Serial VISCA Input	None	
USB Serial Baud Rate	115200	
USB Serial Erase Character	Backspace (Ctrl-H, ASCII 10)	
USB Serial Flow Control	None	

Administrator Preferences : System : License Keys	Default Value	Available in User Preferences
Not Available		

Administrator Preferences : System : System Reset	Default Value	Available in User Preferences
System Reset	prompt for administrator password	

Recent

Administrator Preferences : Recent	Default Value	Available in User Preferences
Fields reflect recent changes	No default	

Directory

Administrator Preferences : Directory : General	Default Value	Available in User Preferences
Local Directory	Enabled	
Corporate Directory	Enabled	
Meetings Directory	Enabled	

Administrator Preferences : Directory : Auto Discovery	Default Value	Available in User Preferences
Auto Discovery	Enabled	
Auto Discovery Subnets	No default; discovers local subnet only if left blank	
Auto Discovery Ignored Subnets	No default	

Administrator Preferences : Directory : LDAP	Default Value	Available in User Preferences
LDAP	Disabled	
LDAP Hostname	No default	
LDAP Username	No default	
LDAP Password	No default	
LDAP Base	No default	
LDAP Filter	No default	
LDAP Refresh	Never	

Appearance

Administrator Preferences : Appearance : General User Preferences : Appearance	Default Value	Available in User Preferences
Language	English (US)	X
Fade Out Timeout	10 seconds	X
Caller ID Timeout	1 minute	X
Company Logo	Default	
Screen Saver	Logo	X
Screen Saver Timeout	10 minutes	X
Sleep Timeout	10 minutes	X
Hide IP Addresses	Disabled	
Clear Last Number Dialed	Disabled	

Administrator Preferences : Appearance : Backgrounds User Preferences : Backgrounds	Default Value	Available in User Preferences
Display 1 Background Image	Default	X
Display 1 Background Color	Sky Blue	X

Administrator Preferences : Appearance : Layout User Preferences : Appearance	Default Value	Available in User Preferences
Picture In Picture	Auto	X

Administrator Preferences : Appearance : Displays	Default Value	Available in User Preferences
Display 1	No default; information field	
Display 1 Resolution	Auto	
Display 1 Energy Saver	Disabled	

Diagnostics

Administrator Preferences : Diagnostics : High Definition Camera 1 User Preferences : Diagnostics : High Definition Camera 1	Default Value	Available in User Preferences
HD Camera 1 Auto Exposure	Full Frame	X
HD Camera 1 Brightness	0	X
HD Camera 1 White Balance	Auto	X
Camera Anti-Flicker	Auto	X
HD Camera 1 Color Temperature	0	X

Administrator Preferences : Diagnostics : Color Bars	Default Value	Available in User Preferences
Color Bars	Not configurable; used to calibrate display	

Administrator Preferences : Diagnostics : Call Counters	Value	Available in User Preferences
Since System Reset: Total Calls Connected Video Calls Connected Voice Calls Connected Last Call Time Total Call Time Longest Call Time	No default; information fields	
Since System Reboot: Total Calls Connected Video Calls Connected Voice Calls Connected Total Call Time Longest Call Time	No default; information fields	

Administrator Preferences : Diagnostics : Network Utilities	Default Value	Available in User Preferences
Command	Ping	

Administrator Preferences : Diagnostics : Network Utilities	Default Value	Available in User Preferences
IP Address	No default	
Start/Stop	Start	

Administrator Preferences : Diagnostics : System Reboot	Default Value	Available in User Preferences
Dialog Prompt	Yes/(No)	X

Section 4: 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 that the system has not been exposed to water or heat sources or was physically damaged.

Improperly connected or loose cables are common problems with hardware units. When investigating a system problem, first inspect 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.

Initialization

As your system initializes, one or more of the following icons may appear in the user interface:

Icon	Condition
	Indicates that the communication subsystem is initializing. If this icon reappears after the system has booted, a problem has occurred. Reboot the system.
	Indicates that 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 this icon persists, a problem has occurred and rebooting the system is necessary.
	Indicates that the system is enabling FIPS security.

Adjusting Room Lighting

Ensure that the system maintains the best possible image quality by altering the 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

Improve dim scenes by Adjusting Camera Brightness.

Camera Issues

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

If the camera does not display video, ensure that 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, which indicates that power is active, and reboot the system if necessary to verify that the camera turns on. To reboot the system, access **User Preferences : Diagnostics : System Reboot**.

Read more at Using Camera Diagnostic Preferences.

Packet Loss

Packet loss can result in noticeable video or audio performance issues and can be caused by signal degradation over the network medium, oversaturated network links, corrupted packets rejected in-transit, faulty networking hardware, and misconfigured system drivers or network applications.

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 output on the codec.

If the video image and user interface appear washed out or too bright, examine your HDTV input settings to make sure the HDTV has 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 for 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 for the call rate and the remote system's capabilities. 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 **Ring Tone Volume** 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 should be sufficient to clean the top surface of the units.

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 external speaker systems are powered and configured correctly.

Power and Connectivity Issues

If a call does not successfully connect, verify that you dialed a working number and that the far end 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.

You may need to reboot a system that is not responding to commands from the remote control.

Using the Remote Control in the Web Administration Interface

From the web administration interface, press **Remote Control** to display an image that allows you to control your system in the same way as the physical remote control. As you use the web remote control, consider the following:

- Clicking the Avaya logo on the image switches the image and functionality from a black to a silver remote control (or from silver to black). Click the logo again to switch back.

- The web administration interface synchronizes with the physical remote control used. If a control system uses a command that emulates the silver remote control, the web administration interface shows the silver remote.

Using Diagnostic Preferences and Tools

Diagnostic preferences and tools that are available to all users include high-definition camera preferences and a system reboot option. Administrators can access these preferences and tools through **User Preferences** or **Administrator Preferences : Diagnostics**. Read more at Preferences.

NOTE   *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

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.

Using Camera Diagnostic Preferences

Use the camera diagnostic preferences in **Administrator Preferences** or **User Preferences : Diagnostics** to adjust camera brightness and white balance and correct 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. Improve dim scenes by adjusting room lighting and manually adjusting the camera brightness. To adjust camera brightness, set **HD Camera Brightness** 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, set **HD Camera White Balance** in **User Preferences : Diagnostics : High Definition Camera**.

By default, your Avaya system determines the proper value for the camera's white balance by testing the initial lighting mix in the room. The video system does not continuously or periodically retest the room lighting to adjust the white balance. If you change the lighting during a call, allow the video system to adjust to the new lighting as follows:

1. Navigate to **Administrator Preferences : Diagnostics : High Definition Camera 1 : HD Camera 1 White Balance** and select a value other than *Auto*.

2. Return the setting to *Auto*.

Adjusting Camera Anti-Flicker

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, 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 for use 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**.

Adjusting Camera Color Temperature

With **Camera White Balance** set to a value other than *Auto*, adjust **Color Temperature** to favor red or blue. Adjust the slider to the left to favor red and to the right to favor blue.

NOTE   You cannot set **Color Temperature** for Avaya Video Camera 100.

Downloading Call History

Download call history as a comma separated value (CSV) file 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. Downloading call history from the web administration interface retrieves a maximum of 26 records.

Copying Screen Text to the Clipboard

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

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 registered 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.