Cisco TelePresence IP VCR 3.0

Online help (printable format)

D14832.01

March 2011

Contents

Logging into the web interface

The IP VCR web interface is used for administering the IP VCR device, managing recordings, users, and pre-defined endpoints. You can also perform many recording-related tasks using the web interface that you cannot otherwise do.

When connecting to the IP VCR web interface, you must log in so that the IP VCR can associate the session with your configured user and a set of access privileges. The IP VCR has a set of configured users, and each user has a username and password that are used for logging in.

1. Using a web browser, enter the host name or IP address of the IP VCR.
2. To log in, click **Log in** and enter your assigned **Username** and **Password**.
3. Click **OK**.

The main menu appears, restricting the available options based on your access privileges. Administrators have full access; standard users can upload new recordings and manage their profiles; guest users typically can access publicly available recordings.

The **Login** page of the IP VCR displays a welcome banner which administrators can configure to display text relevant to your organization. For more information, refer to Customizing the user interface.

If you have problems logging in, see Failing to log into the web interface.

Failing to log into the web interface

When connecting to the IP VCR web interface, you must log in so that the IP VCR can associate the session with your configured user and a set of access privileges. The IP VCR has a set of configured users, and each user has an ID and password that are used for logging in.

If you see the **Access denied** page, you have not been able to log in for one of the following reasons:

- Invalid username/password: you have typed the incorrect username and/or password.

  If Advanced account security mode is enabled (see Configuring security settings) and you incorrectly type the username and/or password three times and if this is an admin account, it is disabled for 30 minutes; for any other account, it is disabled indefinitely (or until you, the administrator, re-enable the account from the **User** page)
- No free sessions: the maximum number of sessions allowed simultaneously on the IP VCR has been exceeded
- Your IP address does not match that of the browser cookie you supplied: try deleting your cookies and log in again
- You do not have access rights to view this page: you do not have the access rights necessary to view the page that you attempted to see
- Page expired: the **Change password** page can expire if the IP VCR is not entirely happy that the user who requested to change password, is actually the user submitting the change password request. (This may happen if you use a new browser tab to submit the request.)

Watching a recording from the IP VCR

The IP VCR offers a variety of ways to watch stored recordings. These include watching recordings using an H.323 endpoint and watching recordings by web streaming. Watching recordings can be an interactive experience. The following pages provide detailed explanations of the options available. Refer to these for more information.

- Using a video endpoint to watch recordings
- Using an auto attendant
- Using streaming to view recordings

Using a video endpoint to watch recordings

You can watch recordings stored on the IP VCR using an H.323 or SIP video endpoint. (Also see Using streaming to view recordings.) There are a number of ways to connect to the IP VCR; refer to the sections below for details of the options available to you:

- Connecting directly using a phone number
- Connecting via the auto attendant
- Being called by the IP VCR

Note that in the current release, HD recordings cannot be played back by an endpoint.

Watching recordings is an interactive experience. Playback can be paused, rewound and so on. Refer to the section below for an explanation of the playback controls available:

- Using playback controls from a video endpoint

Connecting directly using a phone number

Your system administrator may have configured the IP VCR to allow you to use your video endpoint to watch a recording by dialing a particular phone number. Each recording will have a different number to call. Consult your system administrator for details.

If the recording is protected, you must enter a PIN before you can start playback (see Entering a PIN).

Connecting via the auto attendant

The IP VCR features a sophisticated auto attendant menu system that allows you to see a list of which recordings are available, and select the one you want to watch with the aid of video previews for unprotected recordings. Refer to Using an auto attendant for full details on how to navigate the menu.

If you choose to watch a protected recording, you are prompted to enter a PIN before you can start playback (see Entering a PIN).

Depending on how your system administrator has configured the IP VCR, you may be able to connect to the auto attendant by dialing a phone number, or by dialing the IP address of the IP VCR. Consult your system administrator for which options are available to you.

Being called by the IP VCR

As an alternative to calling the IP VCR from your video endpoint, you can instead use the web interface to initiate a call from the IP VCR to your endpoint. Refer to the section Calling out from the IP VCR for details.

Once connected, the playback experience is identical to if you had called the IP VCR using one of the methods described above. Similarly, you may be asked to enter a PIN before playback of protected recordings will start.

Entering a PIN

If you connect to a protected recording, you see the PIN entry screen, and will hear audio prompts playing.

Use your endpoint's numeric keypad to enter the PIN, followed by #. (Note that some endpoints require you to activate the keypad before dialing, for example by pressing the # key.)

Using playback controls from a video endpoint

It is possible to control the playback directly from your video endpoint while watching a stored recording using the Far-End Camera Controls (FECC). Refer to the sections below for details of the controls available, and for the meanings of on-screen status icons that can be displayed.

Basic control

To play and pause recordings:

1. Change the camera control to “far”.
2. Use the **down** control to pause playback.
3. Use the **up** control to resume playback.
4. When playback reaches the end of the recording, it will stop or automatically return to the start of the recording and continue playing, depending on how the IP VCR is configured.
5. When you have finished watching the recording, simply hang up the call

Refer to the following table for assistance interpreting the icons that appear on-screen.

Icon	Icon description
▶	Playback is in progress. The icon will disappear after a few seconds.
⏸	Playback is paused. The icon will remain on screen (blinking) while playback is paused.
■	Playback finished. The icon will remain on screen.

Further control

To advance quickly though a recording (fast-forward):

1. Change the camera control to “far”.
2. Use the **right** control to engage fast forward mode. The video will rapidly advance, and the playback time will be shown in the corner of the screen.
3. When you reach the point from which you want to resume playback, press either **up** to resume or **down** to pause playback as required.
4. If the end of the recording is reached, fast forward will stop.
5. Continue to watch the recording as normal, using playback controls as required.

To skip quickly backwards though a recording (fast rewind):

1. Change the camera control to “far”.
2. Use the **left** control to engage rewind mode. The video will rapidly rewind, skipping several seconds backwards at a time, and the playback time will be shown in the corner of the screen.
3. When you reach the point from which you want to resume playback, press either **up** to resume or **down** to pause playback as required.
4. If the start of the recording is reached, rewind will stop and playback will pause.
5. Continue to watch the recording as normal, using playback controls as required.

Refer to the following table for assistance interpreting the icons that appear on-screen.

Icon	Icon description

Icon	Icon description
⏩	Playback is in fast forward mode. The icon will blink while the recording is being fast forwarded.
⏪	Playback is in fast rewind mode. The icon blinks while the recording is rewound.

Using an auto attendant

Your system administrator may have set up an auto attendant for you to use to view stored recordings. An auto attendant presents you with a menu from which you can choose a recording to watch.

For further information about watching and creating recordings, refer to the document "Watching Recordings", available in the Documentation area of the web site and see the following topics: Using the IP VCR to make a recording, Understanding the recording list and Using streaming to view recordings.

Calling an auto attendant

There are typically two ways to call an auto attendant using your video endpoint. Depending on how the IP VCR is configured, neither, one or both of these will be available to you. Your system administrator should provide you with information about which method you should use:

- Enter the IP address or host name of the IP VCR device
- Dial using a standard E.164 phone number

Accessing the main menu

When you successfully connect to the IP VCR, the main menu displays on your video screen, and you should also hear the audio instructions.

Navigate the auto attendant using the Far-End Camera Controls (FECC) on your video endpoint. Use the up and down controls to highlight the option or item you require; use right to make your selection. To return to a parent folder from a sub-folder, use left.

You can jump to the end of the menu when at the start by using the up control; similarly, you will loop back to the start if you are at the end and use the down control. Note that there is a scroll bar in the bottom right of the video display to indicate where you are in the auto attendant menu. From anywhere in the menu, you can jump to the first entry with #2 and to the last entry with #8.

By default, the number keys on your endpoint are used to play back a recording by entering its configured numeric ID, followed by a '#'. If the recording has a configured security PIN, you are prompted to enter that PIN before the play back will start. As you start to enter a numeric ID, the sequence you have typed is shown at the base of the auto attendant screen. You can cancel the numeric ID entry (for instance to correct an error) by pressing '*'.

If you have connected to the auto attendant using an endpoint that has no FECC capability (for example many SIP endpoints), you can use the number keys on your endpoint to navigate the menus; this is called "DTMF navigation mode". DTMF navigation mode enables you to use the number keys: 2, 4, 6, and 8 in the place of up, left, right, and down respectively.

To enter DTMF navigation mode:

- on connecting to the auto attendant, press the pound (hash) key twice as follows:
  ##
  The message "DTMF menu navigation enabled" appears briefly at the bottom of the auto attendant display.

To exit DTMF navigation mode:

- press the pound (hash) key twice as follows:
  ##
  The message "DTMF menu navigation disabled" appears briefly at the bottom of the auto attendant display.

When in DTMF navigation mode, you will not be able to use the number keys to enter the numeric ID of a recording.

Typically, you will have these options:

Record this session

This option enables you to record the video that your endpoint is sending to the IP VCR. You are presented with the recording console (see Using the recording console). From here you are able to monitor your video before and during recording.

Replay a recording

All recordings stored on the IP VCR in the current folder display here, listed in the order of most recently made first. The default auto attendant corresponds to the top-level (root) folder.

Unless a recording is PIN-protected, highlighting a recording will show a small preview.

If you select a protected recording, you are presented with the PIN entry screen, and will hear audio prompts playing. Use your endpoint's numeric keypad to enter the PIN, followed by #. (Note that some endpoints require you to activate the keypad before dialing, for example by pressing the # key.)

Access other folders

If the IP VCR has been configured with a hierarchy of folders, you can access child folders of the current location, giving you access to the recordings in those folders.

When you have finished watching a recording or making a new recording, simply hang up. If you need to make or watch another recording, you will need to make a new call to the auto attendant.

Using the streaming interface

The streaming interface enables you to enter the ID of a recording and view it in a web browser on your PC . You do not have to have a user account on the IP VCR to be able to do this.

By default, the streaming interface is accessible by all users (even those who have not logged into the IP VCR). However, administrators can disable public access to the streaming interface. To do so, go to **Settings > User interface**.

If you do need to log in to the IP VCR, use the **Log in** link on the top right of the screen.

Stream a recording

Refer to this table for assistance streaming a recording. After you have completed the fields, click **Stream this recording**.

Field	Field description	More information
Recording ID	The numeric ID that uniquely identifies the recording that you want to stream.	
PIN	If the recording that you want to stream is protected by a PIN, enter it here.	
Media	Select the media player and rate that you prefer to use.	

Advanced streaming options

You can enter advanced streaming options by clicking the **show advanced streaming options** link.

Field	Field description	More information
Prefer multicast	When selected, multicast will be used when streaming this recording.	When enabled, the IP VCR's streaming page will attempt to access the multicast media stream for the chosen recording. Note that if the streaming page fails to stream the recording, you can return to this page and clear this option; doing so will cause the IP VCR to attempt to stream the recording using unicast streaming.
Play audio and main video	Select this option to stream the audio and video.	If you clear this option, then neither the audio nor video will play.
Video size	Select a size (resolution) for the video.	This option affects the size of the media player when it opens.
View content channel	Select this option to stream the content channel.	If you clear this option, the content channel will not play.
Content size	Select a size for the content channel.	

Using streaming to view recordings

The IP VCR supports streaming, which involves sending recorded media (audio and video) to a remote computer, allowing the user to watch and listen to the recording.

To view a recording using streaming:

1. Go to **Recordings**.
2. Click **Watch** next to a stored or in-progress recording. (Note that HD recordings cannot be streamed until the recording has completed and the video has been transcoded into streaming media.)
3. If you want to display and choose advanced streaming settings, click the link. Choose the settings you require referring to the following table for tips.
4. Click **Start streaming** to view the recording.

Field	Field description	More information
Media	The preferred bandwidth to use for streaming. The exact options available depend on how the IP VCR was configured when the recording was made; typically you can choose to stream the audio portion only, or audio and video at one of two bandwidths.	Consider your network speed when choosing a bandwidth. For example, you might use a lower bandwidth if you are connecting over ISDN or a higher bandwidth over a T1. Use *Audio only* if you are not interested in the video or are connecting over a very low bandwidth link.
Prefer multicast	For live 'in progress' recordings, where more than one user is viewing the recording, select *Prefer multicast*.	Multicast streaming allows an unlimited number of people to view a recording while it is being made on an IP VCR. It cannot be used for streaming completed IP VCR recordings: more than one person can view the same completed recording at the same time, but each does so on their own unicast connection. Note that you cannot use Windows Media Player to view a live recording on the IP VCR in multicast mode.
Play audio and main video	Select this option to stream the audio and video.	If you clear this option, then neither the audio nor video will play.
Video size	Choose a size (resolution) for the video.	This option affects the size of the media player when it opens.
View content channel	Select this option to stream the content channel.	If you clear this option, the content channel will not play.
Content size	Choose a size (resolution) for the content channel.	This option affects the size of the media player when it opens.

Playback controls when web streaming

If you watch a recording using web streaming, control of playback is performed using the streaming application you are using. To play, pause, fast-forward and so on, refer to the documentation that accompanies your streaming viewer. The player size can be chosen from the drop-down list on the 'View Stream' page.

Using the IP VCR to make a recording

The IP VCR allows you to create recordings in a number of different ways. These include recording conferences on the MCU, recording single video endpoints non-interactively and via the recording console, and transparent recording of point-to-point calls with another endpoint. The following pages provide detailed explanations of the options available. Refer to these for more information.

- Automatically recording a conference on an MCU
- Non-interactive recording of an endpoint
- Using the recording console
- Recording point-to-point calls

In addition to creating recordings using the IP VCR, it is possible to upload existing recordings. Refer to Transferring recordings for more information.

Automatically recording a conference on an MCU

There are a number of ways in which you can configure your IP VCR and MCU to record conferences that take place on the MCU. The following are described here:

- Configuring the MCU to call the IP address of the IP VCR
- Using gatekeeper IDs to record conferences directly into folders on the IP VCR
- Configuring the IP VCR as a gateway on the MCU to record conferences directly into folders on the IP VCR

Configuring the MCU to call the IP address of the IP VCR

When you add a new conference, you can add the IP address of the IP VCR as one of the participants. If you have set the default incoming call action of the IP VCR to be *Record session*, then when the conference begins, the IP VCR will record the conference. Recordings made using this method will always be made into the root folder of the IP VCR.

1. On the IP VCR, go to **Settings > Connections** and for **Default incoming call action** select *Record session* (see Configuring global connection settings).
2. On the MCU, go to **Conferences** and click **Add new conference**. For information about conference configuration, refer to the MCU's online help.
3. From the **Conference list**, select the conference you have created and click **Add participant**. In the **Address** field, type the IP address of the IP VCR and complete the page using the MCU's online help for more information. Note that Cisco recommends that you configure the call to the IP VCR to use the H.323 protocol and not SIP (because SIP calls do not support the content channel or encryption).

When the conference starts, the IP VCR starts recording into its root folder. Note that the name of the conference will be the name of the MCU and will also include the date and time if the **Use date and time in new recording names** field is selected on the **Settings > Recordings** page.

Using gatekeeper IDs to record conferences directly into folders on the IP VCR

By using a gatekeeper and gatekeeper IDs, you can automatically record conferences directly into the folders of your choice on the IP VCR.

1. Set up a gatekeeper: go to **Settings > Gatekeeper**. For more information about using a gatekeeper, refer to Configuring gatekeeper settings. To use the method described in this procedure, ensure that you select **Register folder IDs**.
2. For each folder into which you want to record directly, ensure that you have set a **Recording ID** (see Adding and updating folders). The IP VCR registers these IDs with the gatekeeper.
3. On the MCU, go to **Conferences** and click **Add new conference**. For information about conference configuration, refer to the MCU's online help.
4. From the **Conference list**, select the conference you have created and click **Add participant**. In the **Address** field, type the recording ID of the folder into which you want to record the conference and complete the page using the MCU's online help for more information. Note that you might want to set **Initial video status** and **Initial video status** to Muted. Enable **Automatic disconnection**; this ensures that the IP VCR stops recording when the conference ends.

When the conference starts, the IP VCR will start recording the session into the folder with the recording ID that you used in step 4.

Note that if you are intending to use this method frequently with the same folder, it will be quicker to configure the recording ID as an endpoint on the MCU. The procedure is the same as when you configure an H.323 endpoint on the MCU. For more information, on the MCU, go to **Endpoints > Add H.323 endpoint** and view the online help.

Configuring the IP VCR as a gateway on the MCU

By configuring the IP VCR as a gateway on the MCU in conjunction with using recording IDs on the IP VCR, you can automatically record conferences directly into the folders of your choice on the IP VCR without the need for a gatekeeper.

1. Configure the IP VCR as a gateway on the MCU: on the MCU, go to **Gateways** and click **Add new H.323 gateway**. Enter the name and IP address of the IP VCR and complete the page using the MCU's online help for more information.
2. On the MCU, go to **Conferences** and click **Add new conference**. For information about conference configuration, refer to the MCU's online help.
3. From the **Conference list**, select the conference you have created and click **Add participant**.
4. In the **Address** field, type the recording ID for the IP VCR folder into which you want to record.
5. Select the gateway you configured in step 1 and complete the page using the MCU online help for more information. Note that you might want to set **Initial video status** and **Initial video status** to Muted. Enable **Automatic disconnection**; this ensures that the IP VCR stops recording when the conference ends.

When the conference starts, the IP VCR will start recording the session into the folder with the recording ID that you used in step 4.

Note that if you are intending to use this method frequently with the same folder, it will be quicker to configure the recording ID as an endpoint on the MCU. The procedure is the same as when you configure an H.323 endpoint on the MCU. For more information, on the MCU, go to **Endpoints > Add H.323 endpoint** and view the online help.

Non-interactive recording of an endpoint

Depending on the configuration of the IP VCR, you may be able to make recordings non-interactively. That is, after connecting to the IP VCR, recording takes place automatically, and with no feedback to the user. If you would prefer to have more feedback when making recordings, consider using the recording console (see Using the recording console). Otherwise, refer to the sections below for further information on making non-interactive recordings:

- Understanding non-interactive recordings
- Connecting in order to make a recording
- Controlling the recording

Understanding non-interactive recordings

Non-interactive recording gives no feedback as to the status of recording. The IP VCR will not send video to your endpoint, typically causing your endpoint to display a blank screen. You will not be able to monitor how the recording will look.

When the call to or from the IP VCR is connected, recording will typically start immediately. However, the IP VCR may have been configured to delay recording until coherent video is seen. Your system administrator may have configured the IP VCR in this way to ensure the best quality of recordings.

If you are unsure of whether the IP VCR will start recording immediately or not, wait a few seconds before starting to speak; this will ensure the best quality recording in all circumstances.

Connecting in order to make a recording

Calling the IP VCR from a video endpoint

To make a non-interactive recording by calling the IP VCR using your video endpoint, follow these steps:

Confirm with your system administrator that the **Default incoming call action** of the IP VCR is to answer incoming calls by recording them immediately (non-interactively) (see Configuring global connection settings).

Alternatively, determine whether the IP VCR has any **Recording IDs** configured and registered with a gatekeeper, allowing you to make a recording by dialing a phone number (see Configuring gatekeeper settings).

1. Connect to the IP VCR using the method chosen in the previous step.
2. Recording will start when the call is answered.

You can also call into the IP VCR from an MCU. See Automatically recording a conference on an MCU

Being called by the IP VCR

You can use the IP VCR web interface to call out to your video endpoint and record the session non-interactively. To make a recording in this way, follow these steps:

1. Log in to the IP VCR web interface as an administrator or user (see Logging in to the web interface).
2. Go to **Recordings**.
3. Click **Call out and record**. The Recording parameters page is displayed (see Calling out from the IP VCR).
4. Name your recording, and identify the endpoint you want to call out to.

5. Ensure **Use recording console display** is not selected.
6. Click **Call endpoint** or **Call selected endpoint**.
7. Answer the call on the video endpoint. Recording will start.

Controlling the recording

The nature of non-interactive recording is that the user has little or no control over recording. When you have finished recording, simply hang up the call to end and store the recording.

Using the recording console

The recording console allows you to make recordings interactively. That is, it allows you to monitor the recording while it is in progress, to check that the view is as you require.

Refer to the sections below for further information on using the recording console:

- Connecting to the recording console
- Understanding the recording console display
- Controlling the recording console

Connecting to the recording console

Calling in via the auto attendant

To access the recording console by calling the IP VCR via the auto attendant, follow these steps:

1. Confirm with your system administrator that you can call the auto attendant of the IP VCR, either by using the IP address of the IP VCR or by dialing a phone number.
2. Connect to the auto attendant using the method chosen in the previous step.
3. Navigate the auto attendant menus (see Using an auto attendant) to select **Record this session**.
4. The recording console is displayed.

Being called by the IP VCR

You can use the IP VCR web interface to call out to your video endpoint and display the recording console. To connect to the recording console in this way, follow these steps:

1. Log into the IP VCR web interface as an administrator or user (see Logging in to the web interface).
2. Use your browser to navigate to **Recordings**.
3. Click **Call out and record**. The recording parameters page is displayed (see Calling out from the IP VCR).
4. Name your recording, and identify the endpoint you want to call out to.
5. Select **Use recording console display**.
6. Click **Call endpoint** or **Call selected endpoint**.
7. Answer the call on the video endpoint. The recording console is displayed.

Understanding the recording console display

The recording console display is intentionally simple. Refer to the following table for a description of the different parts of the display:

Control	Control Description
Preview window	In the center of the screen, a window shows a live preview of the video being sent by the endpoint to the IP VCR. Use this preview to ensure the recorded view is composed as you require before starting to record. You can also monitor this view whilst recording. Note that although the audio portion of the call will also be recorded, this is not sent back to the endpoint like the video preview, as this would cause undesirable feedback effects.
Status	A status indication is displayed in the bottom left-hand corner of the recording console. It shows the current state of recording. When you first enter the recording console, the

Control	Control Description
	status indication will show *paused*.
Recording length	The length of the recording is shown in the bottom right-hand corner of the screen, as minutes and seconds. When you first enter the recording console, this will show a zero-length recording. The recording length will update in real-time as recording progresses. Use this as a guide to how long your recording will be.
Recording indicator ● REC	The recording indicator is shown only whilst recording is in progress, and hence will not be visible when you first enter the recording console. When you start recording, this indicator will blink near the top right-hand corner of the screen.

Controlling the recording console

When you first enter the recording console, you will hear audio instructions on which controls you can use. Recording will not start until you are ready. Refer to the following table for details:

Control	Control description	Usage tips
Up	Starts recording. The status line will change from *paused* to *resuming...* then to *recording*.	When you start recording, the IP VCR waits for a suitable moment before actually starting to record. This is to ensure the best possible quality video is recorded. During this time the status line shows *resuming...*. Be sure to wait until the status line says *recording* before starting to speak.
Down	Stops recording. The status line will change from *recording* to *finished*.	When you have finished recording, you will not be disconnected from the IP VCR unless you hang up the call. Note that even when you have finished recording, IP VCR resources are still in use until the call is ended, possibly preventing other users from making recordings in the meantime.

You do not have to explicitly stop recording. If you want, you can simply hang up the call when you have finished. Whether you click stop or simply hang up, the recording is stored automatically by the IP VCR.

Recording point-to-point calls

The IP VCR is able to transparently record point-to-point calls. A point-to-point call is one where just two endpoints are involved - the traditional type of call. If you want to record point-to-point calls, the gatekeeper settings of the IP VCR must be configured correctly (see Configuring gatekeeper settings).

Instead of simply calling the other endpoint by dialing its E.164 number from your video endpoint, you must add a prefix that tells the H.323 gatekeeper to pass the call to the IP VCR rather than directly to the other endpoint. Your system administrator can advise you which prefix to use. The IP VCR will then attempt to call the other endpoint on your behalf, transparently passing media as normal when the call is connected. With the exception of needing to dial a slightly different number, the experience of calling the other endpoint should be identical to as if you had called it directly.

While the point-to-point call is in progress, the IP VCR records both sides of the call using one of the configured layouts (see Configuring recording settings). The options include showing both endpoint views side-by-side, and showing the loudest speaker in a full-screen view with the other shown picture-in-picture.

To make a point-to-point recording, follow these steps:

1. Call the remote endpoint using its E.164 number, including the prefix to pass the call through the IP VCR.
2. Recording will start immediately or shortly after the call is connected, depending on how the IP VCR is configured.
3. After you have completed your call, simply hang up. The IP VCR disconnects the other endpoint for you, and the recording is stored automatically and displayed in the Recordings list.

Recording of point-to-point calls is transparent. The calling or called endpoint cannot start or stop recording other than by hanging up the call.

Calling out from the IP VCR

As well as using your video endpoint to call into the IP VCR in order to make and watch recordings, you can also perform both of these functions using the IP VCR to call out to your endpoint. The sections below explain how to call out from the IP VCR to make and watch recordings:

- Calling out to watch a recording
- Calling out to make a recording
- Understanding the playback and recording parameters pages

Calling out to watch a recording

To call a video endpoint from the IP VCR in order to play a stored recording:

1. Go to **Recordings**.
2. Use the **Recording list** to select the recording that you want to watch.
3. Click the recording name. The **Recording information** page is displayed (see Viewing and updating recording details).
4. Click **Call out and play session**. The **Playback parameters** page is displayed.
5. Refer to the following table for details of the fields displayed.
6. Click **Call endpoint** or **Call selected endpoint**. The IP VCR will attempt to call the specified endpoint.
7. Answer the call on your video endpoint to commence playback.
8. Watch the recording as if you had called into the IP VCR. Similarly, you can control progress using the Far-End Camera Controls of your video endpoint (see Using a video endpoint to watch recording).

Calling out to make a recording

To call a video endpoint from the IP VCR in order to make a new recording, follow these steps:

1. Go to **Recordings**.
2. Browse to the folder in which you want to place the new recording.
3. Click **Call out and record**. The **Recording parameters** page is displayed.
4. Refer to the following table for details of the fields displayed.
5. Click **Call endpoint** or **Call selected endpoint**. The IP VCR will attempt to call the specified endpoint.
6. Answer the call on your video endpoint. Recording will either start immediately (see Non-interactive recording) or the recording console is displayed (see Using the recording console).
7. Continue to make your recording as if you had called into the IP VCR.

Understanding the playback and recording parameters pages

Whether calling out to play back or to record, you must specify which endpoint you want to call. The **Playback parameters** and **Recording parameters** pages are very similar. Refer to the following table for details:

Field	Field description	Usage tips
Playback parameters		

Field	Field description	Usage tips
	There are no playback-specific parameters.	
Recording parameters		
Name of recording to create	Specify a name for the new recording.	The name you choose will be displayed in the **Recordings list** (see Understanding the recordings list), and in the auto attendant menu. You cannot choose a name that is already used by another recording.
Use recording console display	Select to call the endpoint using the Recording console to make the recording. Leave it clear to make a non-interactive recording.	See Using the recording console and Non-interactive recording for more information on the implications of this option
New endpoint		
Host name or IP address	Specify the host name or IP address of the endpoint you want to call out to.	Alternatively you can specify an E.164 number if you also select an **H.323 gateway**. To make a call out via a H.323 gateway that has not been specifically configured on the IP VCR, you can enter an address here of the form <gateway address>!<E.164>.
Call protocol	If the endpoint is an H.323 endpoint, select H.323. If it is a SIP endpoint, select SIP.	
H.323 gateway	If you want to call the endpoint using an E.164 number via a previously-configured H.323 gateway, you can select an H.323 gateway from the list of configured gateways.	If you are calling by host name or IP address, you need not specify a gateway.
Use SIP registrar	If the endpoint is a SIP endpoint, and you want it to use a SIP registrar, select this option.	
Motion / sharpness trade off	Choose whether to use the box-wide setting for motion/sharpness trade off, or configure an individual setting for use with this endpoint. Choose from: ▸ *Use box-wide setting*: this is the default value. In this case, the connection to this endpoint will use the motion / sharpness tradeoff setting from the **Settings > Connections** page. ▸ *Favor motion*: the IP VCR will try and use a high frame rate. That is, the IP VCR will strongly favor a resolution of at least 25 frames per second. ▸ *Favor sharpness*: the IP VCR will use	The settings for motion (frames per second) and sharpness (frame size or resolution) are negotiated between the endpoint and the IP VCR. This setting controls how the IP VCR will negotiate the settings to be used with this endpoint.

Field	Field description	Usage tips
	the highest resolution that is appropriate for what is being viewed. - *Balanced*: the IP VCR will select settings that balance resolution and frame rate (where the frame rate will not be less than 12 frames per second).	
Transmitted video resolutions	Choose the setting for transmitted video resolutions from the IP VCR to this endpoint. This setting overrides the unit-wide/blade-wide setting on the **Settings > Connections** page.	Retain the default setting (*use box-wide setting*) unless you are experiencing problems with the display of certain resolutions by this endpoint. Endpoints advertise the resolutions that they are able to display. The IP VCR then chooses from those advertised resolutions, the resolution that it will use to transmit video. However, some endpoints do not display widescreen resolutions optimally. Therefore, you might want to use this setting to restrict the resolutions available to the IP VCR for transmissions to this endpoint.
Preferred bandwidth from IP VCR	Use these fields to specify the preferred call bandwidth from the IP VCR to the endpoint and from the endpoint to the IP VCR, respectively.	If you choose *use default value*, the preferred bandwidth is chosen to be the same as that set in the global connection settings.
Preferred bandwidth to IP VCR		
Custom codec selection	Can be used to ensure only specific codecs are permitted on calls to (and received from) this endpoint.	If *Enabled*, you can choose which codecs are allowed to be used when communicating with this endpoint.
Configured endpoints		
<Pre-configured endpoints>	Select one of the endpoints that has been configured on the IP VCR to call by selecting it in the list and clicking **Call selected endpoint**.	

Content channel video support

The IP VCR supports an additional video stream known as the content channel to or from each connected endpoint if the **Content status** field on the **Settings > Content** page is *Enabled* (see Configuring content settings). Therefore, there are potentially three media streams between each endpoint and the IP VCR: audio, main video and content channel video. In general, the main video channel is used for motion video (i.e. high frame rate streams) and the content channel for less dynamic video such as an accompanying presentation - this is typically a high resolution, low frame rate video stream.

Support for content channel video on the IP VCR encompasses:

- Sourcing the content channel from an H.323 endpoint's H.239 video stream, or a SIP endpoint supporting content using BFCP, in either single-endpoint recordings, point-to-point recordings or MCU conferences. (Also see Configuring H.323 endpoints and Configuring SIP endpoints.)
- Playing back recorded content channel data to H.323 endpoints via H.239 or to SIP endpoints using BFCP (Binary Floor Control Protocol)
- Streaming the content channel to users' desktop machines

Recording content

When an endpoint is being recorded, that endpoint may open a content channel video stream, in addition to its main video channel. The IP VCR records both video channels, and both are available when that recording is played back.

When using the Recording console, the presence of content channel video is indicated by a "Content" icon on the right of the screen.

In a point-to-point recording, only one of the recorded endpoints is able to supply the content channel at any one time. Specifically, this means that if one endpoint is supplying the content channel stream then it must stop transmitting video before the other endpoint can start. (However, see the **Automatic content handover** field on the **Settings > Content** page.) This is in contrast to the main video channel, which both endpoints are able to transmit and receive simultaneously without restriction.

Playing back content channel video

If a recording includes a content channel video stream, that content channel stream can be played back to either other endpoints or to users viewing a recording via streaming.

Playing back to H.323/SIP endpoints

Stored content channel video can only be played back to an endpoint if that endpoint is capable of receiving a H.239 video stream (H.323 endpoints) or a BFCP stream (SIP endpoints) in addition to its main video channel. When playing back a recording which includes content channel video, an endpoint without this capability will see just the main video channel unless **Playback content in main video channel** is *Enabled* on the **Settings > Content** page.

Streaming content channel video

Recorded content channel streams can be played back to users' desktops via web browser-based streaming in addition to the recorded main video and audio streams. When streaming, users have the choice of playing back just the audio and main video streams, just the recorded content channel, or both together.

The play back of content channel video is accomplished through use of a Java applet, and therefore Java must be installed on any machine wanting to view the recorded content channel.

Creating customized MPEG and Windows Media Video format files

The MPEG and WM Converter Tool is a tool that converts recorded files to MPEG-1 or Windows Media Video (.wmv) format. It is available from the Support area of the web site. The MPEG and WM Converter Tool enables you to create MPEG videos or Windows Media videos that include up to two video streams and/or the content channel. The resulting encoded MPEG/'.wmv' files can be stored on PCs or servers and can be viewed via streaming applications on users' desktops.

Understanding the recordings list

The Recordings list displays information about stored recordings. To view the recordings list, go to **Recordings > Recording list**. See the tables below for an explanation of the fields that display.

Stored recordings are one of:

- recordings that have been made using the IP VCR
- recordings that have been uploaded to the IP VCR (see Transferring recordings)
- recordings that are stored externally in a Network Files System (NFS) (see Storing recordings externally)

Stored recordings are presented in a hierarchical view of folders in which recordings can be stored. Each folder can contain multiple recordings and sub folders.

The folder structure is browsable in the Recordings list, and also by going to **Recordings > Folders**, or by an endpoint user calling the IP VCR using an auto attendant.

- Folders
- Stored recordings
- Recording controls
- Name and numeric ID clashes

Folders

Field	Field description	Usage tips
Folder	The name of the folder that you are viewing.	
Recording ID	The recording ID for this folder.	Setting a Recording ID enables a new recording to be placed directly into this folder, by using a gatekeeper. For more information, refer to Understanding the folders list.
Recording console ID	The recording console ID for this folder.	Setting a recording console ID enables a recording made through a recording console to be placed directly into this folder. For more information, refer to Understanding the folders list.
Auto attendant ID	The auto attendant ID for this folder.	Setting an auto attendant ID enables someone to call in to an auto attendant that displays only the recordings in this folder. For more information, refer to Understanding the folders list.
Point-to-point prefix	The point-to-point prefix for this folder.	Setting a point-to-point prefix enables someone to make a call using that prefix and start recording a call between two endpoints into this folder. For more information, refer to Understanding the folders list.
External location	If the folder is linked to an external location, it is specified here.	For more information, refer to Storing recordings externally.
Sub folders	A list of sub folders of the folder that you are currently viewing.	If you are not in the top-level folder, use the **Move up** option to go up one level in the folder hierarchy. To view a list of stored recordings in a folder, click the name of the folder.

Stored recordings

The Stored Recordings table displays a list of all recordings stored in the folder that you are currently viewing.

The following information is displayed for each stored recording.

Field	Field description	Usage tips
Watch	Displays the recording streaming page. Some recordings may require a PIN to access this feature.	See Using streaming to view recordings for more information.
Name	The name of the recording. Depending on how the recording was made, this is a name entered by the user, or a name chosen automatically by the IP VCR.	You can rename a recording by clicking its entry in the list and editing the name field (see Viewing and updating recording details).
Location	Whether the recording is internally or externally stored.	See Storing recordings externally for more information.
Status	A brief indication of whether this recording is in use (recording or playback in progress), or not. If this recording is currently being transcoded to streaming format, this is also indicated.	If you have sufficient access rights, a **stop** link is displayed next to the status for active recordings. To stop the recording, click the link. A confirmation message is displayed. A recording that is not being made or played back is referred to as *Idle*. *Invalid media* indicates that the recording is partially invalid. For example, the recording might be valid but the streaming media could be invalid caused by power loss to the IP VCR during the transcode. *Truncated streaming media* indicates that the IP VCR was shut down during the transcoding of the recording to streaming format. If there is a problem with the streaming media, you can start the transcode again by clicking **Transcode to streaming format** on the recording's details page.
Numeric ID	The Numeric ID of the recording, if it has one.	You can edit a recording's details to allocate it with a Numeric ID (see Viewing and updating recording details).
Registration	If a recording has a **Numeric ID** set and that ID is configured to register with an H.323 gatekeeper and/or a SIP registrar, this field shows the state of the registration, or *n/a* if no identifier is set.	To register a recording with an H.323 gatekeeper, the IP VCR must be configured with a gatekeeper (see Configuring gatekeeper settings). To register a recording with a SIP registrar, the IP VCR must be configured with a SIP registrar (see Configuring SIP settings).
Length	The length of the recording.	
Recorded at	The time at which a recording was started or uploaded.	

Recording controls

Removing recordings

To remove recordings from the IP VCR, select the recordings to remove and click **Delete selected**. Recordings are permanently removed.

Calling out to make a recording

You can initiate a recording session from the IP VCR. To do this, click **Call out and record** to display the Recording parameters page. Then specify an endpoint to call, either directly by entering an IP address, or by selecting a configured endpoint. The recording will be placed in the folder that you are currently viewing. For more details see Calling out from the IP VCR.

Uploading recordings

You can upload recordings directly to the IP VCR: click **Upload recording** to display the Recording upload page. Then specify the file you want to upload, as well as a name for the recording. The uploaded recording will be placed in the folder that you are currently viewing. For more details see Transferring recordings.

Name and numeric ID clashes

Because recordings can be stored both internally on the IP VCR and externally on an NFS server, it is possible that the Name and/or the Numeric ID of a recording could clash with that of another recording. Where this is the case, it is indicated on the web interface of the IP VCR and it is not possible to call out and play, or to delete the recording. However, you can rename and/or reallocate a Numeric ID to the recording to resolve the clash.

Viewing and updating recording details

To view recording information for a particular recording, on the IP VCR web interface, go to **Recordings**. Click on the name of the recording that you are interested in using the **Stored recordings** list.

The Recording information page allows you to change a number of properties including the displayed name of a stored recording and whether the recording is to be registered to an H.323 gatekeeper and/or SIP registrar. In addition, you can review extended details, and download files in a number of formats for subsequent playback or transfer to another IP VCR.

Refer to the following sections for further details:

- Recording configuration
- Recording status
- Recording controls
- Summary information

Recording configuration

You can review and edit a number of details pertaining to a recording. Make changes as required, and then click **Update configuration**. Refer to the following table for more information on the fields displayed:

Field	Field description	Usage tips
Name	Displays the current name of the recording. You can specify a new name if required.	The recording name is shown in the recordings list and in auto attendant menus. You cannot rename a recording with the same name as an existing recording.
Numeric ID	You can specify a numeric ID that can be used in conjunction with a gateway to allow users to dial the recording directly from their endpoint.	The Numeric ID can be registered with the H.323 gatekeeper or with a SIP registrar to enable users to dial the recording directly and have it displayed on their endpoint. Select the appropriate check box(es) in **Numeric ID registration** below. When dialing, H.323 users might need to prefix this gatekeeper ID if a prefix is set in the IP VCR gatekeeper registration.
PIN	You can specify a security PIN to restrict access to a recording.	If a PIN is set, users wanting to watch the recording using a video endpoint or using streaming will be asked for the PIN before they can proceed.
Numeric ID registration	If you want to register the recording with the H.323 gatekeeper and/or the SIP registrar, select the relevant check box(es).	Note that, in addition: H.323 gatekeeper and/or SIP registrar usage must be enabled, as appropriate, in the **Settings > H.323** and/or **Settings > SIP** page. **ID registration for recordings** must be selected in the **Settings > SIP** page for recordings to be registered with a SIP registrar
Allow play back and streaming	Enables the storing of private recordings by determining which users can stream or download this recording.	When selected, this recording can be streamed or downloaded by any user. When clear, this recording can only be streamed or downloaded by admin users.

Recording status

Full details of a recording are shown here. Refer to the following table for more information on the fields displayed:

Field	Field description	Usage tips
Time of recording	Displays the time and date when this recording was started or uploaded.	
Duration	Displays the length of the recording.	
Recorded media	Displays full details about the recording and displays information about the streaming format media if that has been created.	This information can be useful if you are going to use the MPEG and WM Converter tools. For more information see the web site.
Complete recording file size (bytes)	Shows the complete size of the recorded media (including streaming media if present).	Click **download recording** to transfer the *.codian* file to your PC (see Transferring recordings).
Projected MPEG file size (bytes)	Shows the projected size of the exported MPEG should you choose to download it.	Click **download MPEG file** to transfer the file to your PC (see Transferring recordings). This is an estimated value based on the MPEG1 video bit rate. This value is not displayed if MPEG1 export is disabled; this is configured on the **Settings > Recordings** page.
Gatekeeper state	Shows the registration status of this recording with the gatekeeper.	
SIP registrar state	Shows the registration status of this recording with the SIP registrar.	
Active streaming playbacks	Displays the number of playbacks of this recording currently in progress via streaming.	This figure includes streaming playbacks.
Active H.323/SIP playbacks	Displays the number of playbacks of this recording currently in progress on H.323 or SIP endpoints.	
Active downloads	Displays the number of downloads of this recording currently in progress.	
Completed playbacks	Displays the number of playbacks of this recording that were once in progress but are no longer.	
Completed downloads	Displays the number of downloads of this recording that have completed.	

Recording controls

You can call into the IP VCR from a video endpoint to watch this recording. Alternatively, the IP VCR can call out to the endpoint and begin playback when the call is answered. To do this, click **Call out and play recording**. For more details, see Calling out from the IP VCR. Note that for HD recordings, this option will not be available; in the current release, HD recordings cannot be played back on a video endpoint.

To transcode this recording for streaming, click **Transcode to streaming format**. Note that you can configure the IP VCR to automatically transcode and store all new recordings to streaming format; to do this go to **Settings > Recordings**. You can transcode a recording for streaming more than once if you want to change the bit rate for example; to change the bit rate of streaming media, go to **Settings > Recordings**. Note that if the unit reboots during the transcoding to streaming media, the streaming media file will either be invalid or truncated; in this case, delete the streaming media and perform the transcoding again. The option to transcode to streaming format is only available for recordings stored on the IP VCR and not available for recordings stored on an external NFS system.

To delete the transcoded streaming media, click **Delete streaming media**. This can be useful when space is short on the IP VCR's internal disk.

Summary information

You may want to give users instructions on how to view this recording using streaming, information on when it was made and so on.

Click the **Summary information** icon to display further details about this recording. The information can be copied to the clipboard for convenience.

Transferring recordings

Although you can make and view recordings with the IP VCR you are not restricted to watching only recordings made with the IP VCR. Neither must you use the IP VCR to watch recordings you have made. Refer to the sections below for how to transfer recordings to and from the IP VCR.

- Uploading recordings onto the IP VCR
- Downloading recordings from the IP VCR

Uploading recordings onto the IP VCR

As well as using the IP VCR to make recordings directly by using automatic and interactive recording of sessions or point-to-point calls, it is also possible to upload video clips via the web interface.

To upload a video clip to the IP VCR, follow these steps:

1. On the IP VCR web interface, go to **Recordings**.
2. Browse to the folder in which you want to place the uploaded recording.
3. Click **Upload recording**. The **Recording upload** page is displayed.
4. Click **Browse** to locate the file that you want to upload. Consult your system administrator if you are unsure of the format of a particular file.
5. Choose a name for the uploaded recording. This name will be displayed in the recordings list and in the auto attendant menus.
6. Click **Commence upload** to begin the transfer of the file to the IP VCR.

Note that the upload can take several minutes for long recordings. Do not navigate away from the upload page until the upload has completed or it may be aborted.

.codian and MPEG 1 format files can be uploaded via the IP VCR web interface in this way.

When the upload is complete, the video clip will display in the **Recordings List** (see Understanding the recordings lists), and can be played back via H.323 or streaming like any other recording.

Downloading recordings from the IP VCR

You can download recordings from the IP VCR which can then be:

- transferred to another IP VCR
- played on your PC using any application that supports MPEG video clips, such as QuickTime Viewer
- converted into a MPEG (.mpg file) using the MPEG Converter tool, that is available from the web site
- converted into a Windows Media Video (.wmv file) using the WM Converter tool, that is available from the web site

Clips can be downloaded from the IP VCR in one of two formats: MPEG and .codian. Clips downloaded in MPEG format can be played on a PC as discussed above; either format can be transferred to another IP VCR, though the (bigger) .codian files will transfer much more quickly.

Note that if you want to create an MPEG file that includes the content channel (or control the size and positioning of streams within the MPEG), you will need to use the MPEG Converter tool. MPEGs downloaded directly from the IP VCR will not include the content channel.

To download a recording from the IP VCR follow these steps:

1. On the IP VCR web interface, go to **Recordings**.

2. Browse the folder hierarchy to locate the recording you want to download and click on its name.
3. The **Recording details** page is displayed (see Viewing and updating recording details).
4. Click **download MPEG file** to download the recording in MPEG format, or **download recording** to download in .codian format.
5. Save the file.

Understanding the folder list

The Folder list displays the hierarchy of folders on the IP VCR. Folders are used to group stored recordings together in a convenient manner. Stored recordings are one of:

- recordings that have been made using the IP VCR
- recordings that have been uploaded to the IP VCR (see Transferring recordings)
- recordings that are stored externally in an Network Files System (NFS) (see Storing recordings externally)

To view the Folder list, go to **Recordings > Folders**.

The **Expand all** button displays the entire folder tree. This also displays recordings stored physically on the IP VCR inside the folders. Externally stored recordings are not displayed in the Folder list; they are displayed in the Recording list.

The **Collapse all** button causes the display to show the folder hierarchy without recordings listed. Click the 'plus' sign (+) on individual folders, to show the recordings stored in that folder.

Each folder can contain multiple recordings and sub folders. Next to each folder name in the Folder list, the number of recordings in that folder is displayed. For folders that are linked to external storage locations, the number of externally stored recordings is also listed and in this case the number of recordings in the folder includes the number of externally stored recordings (that is, the number of recordings in the folder is the *total* number of recordings in the folder).

The folder structure is browsable in the Recordings list (go to **Recordings > Recording list**), and by an H.323 endpoint user calling the IP VCR using an auto attendant. Each folder will appear as a separate auto attendant. If you assign auto attendant IDs to folders, H.323 users will be able to connect directly to that folder.

If you assign Numeric IDs to recordings, the recordings can then be registered with an H.323 gatekeeper and/or a SIP registrar enabling users to directly dial a recording. Note that externally stored recordings cannot currently be accessed via a SIP registrar.

You can create up to 50 folders on the IP VCR.

You can create recordings directly into a particular folder, by assigning a folder with a Recording ID and using a gatekeeper. For more information about recording IDs, refer to Adding and updating folders.

Moving recordings and folders

To move a recording stored on the IP VCR or a folder:

1. Go to **Recordings > Folders**.
2. Drag the recording or folder to the destination folder.

Note that only internally stored recordings can be moved in this way.

Deleting folders

To delete a folder:

1. Go to **Recordings > Folders**.
2. Click the **delete folder** link next to the name of the folder that you want to delete.

Note that when you delete a folder, any recordings stored on the IP VCR inside the folder are moved to the top level folder and are not themselves deleted. (Note that any externally stored recordings inside a folder that you delete will not be deleted; they will not become associated with any other folder, but will remain in the NFS location.)

Note that when you delete a folder, any sub folders of that folder are moved to the top-level folder and are not themselves deleted.

Adding and updating folders

To add or update a folder:

1. Go to **Recordings > Folders** to display the Folder list:
   - To create a new folder, click the **create subfolder** link next the folder hierarchy in which you want to create a new folder
   - To update an existing folder, click the **configuration** link next to the folder that you want to update
2. Complete the **Add new folder** page. Refer to the following table for more information:

Field	Field description	Usage tips
Folder parameters		
Name	The name of the folder that you are creating or updating.	
PIN	The PIN for the folder you are creating or updating. Users wanting to see the contents of a PIN protected folder via the Streaming-only interface or the auto-attendant must enter the PIN. You do not have to set a PIN for a folder.	If you have enabled the **New recordings inherit folder's PIN** option on the **Settings > Recordings** page, new recordings created in this folder will inherit this PIN. You can change the PIN for a recording (see Viewing and updating recording details). Any sub folders that you create inside this folder will not automatically inherit this PIN.
Recording ID	The recording ID for the folder that you are creating or updating.	Setting a recording ID enables a new recording to be placed directly into this folder. For more information, refer to Configuring gatekeeper settings. This ID must be unique across all numeric IDs on the IP VCR.
Recording console ID	The recording console ID for this folder.	Setting a recording console ID enables a recording made through a recording console to be placed directly into this folder by using a gatekeeper. For more information, refer to Configuring Gatekeeper Settings. This ID must be unique across all numeric IDs on the IP VCR.
Auto attendant ID	The auto attendant ID for this folder.	Setting an auto attendant ID enables someone to connect directly to this folder and select from only the recordings in this folder and access recordings in subfolders of this folder, by using a gatekeeper. For more information, refer to Configuring gatekeeper settings. This ID must be unique across all numeric IDs on the IP VCR.
Point-to-point call incoming prefix	Specifies a sequence of digits that the H.323 gatekeeper can use to identify which calls to route through the IP VCR to make recordings in this folder of point-to-point calls.	If specified, this value will be registered as a prefix with the gatekeeper. This field is required if you want users to be able to make recordings of point-to-point calls in this folder.
Point-to-point call outgoing prefix	Specifies an optional sequence of digits to add when the IP VCR tries to make the outgoing part of a point-to-point call that has been routed through it.	This value has a local effect only – it will not be registered as a prefix with the gatekeeper. When making point-to-point calls through the IP VCR, the *Point-to-point call incoming prefix* is stripped from the dialed number and the

Field	Field description	Usage tips
		outgoing prefix added before the outgoing part of the call is attempted. Your dial plan may not require you to specify an outgoing prefix.
Able to make new recordings via the auto attendant	Select this setting to allow new recordings to be created in this folder from the auto attendant (that is, by using the **Record this session** option from the auto attendant).	If you clear this setting, users will not be able to create new recordings in this folder from the auto attendant. Regardless of how this setting is configured, you will be able to call out and record from the web interface, and/or dial directly to this folder's **Recording ID** or **Recording console ID** (if those are configured).
Able to stream and play back new recordings	Select this setting to allow all new recordings in this folder to be viewed via the streaming-only interface, or to be played back from the Recording list.	New recordings in the folder automatically inherit this setting. This setting provides the initial value for each new recording's "Allow play back and streaming" setting (on the recording's details page). If this setting is selected, any new recording in this folder can be streamed from the streaming-only interface or played back from the Recording list. If this setting is not selected, any new recordings inside this folder cannot be streamed from the streaming-only interface or played back from the Recording list. Each recording can be individually configured to allow it to be streamed from the streaming-only interface or played back from the Recording list (or you can configure it such that it cannot be streamed from the streaming-only interface or played back from the Recording list). This is controlled by the "Allow play back and streaming" setting on each recording's details page (see Viewing and updating recording details).
Publically accessible	Select this setting to allow users to access this folder from the Streaming-only web interface. This will not affect folders above or below this folder in the folder hierarchy.	When a folder is publically accessible, the folder name appears as a link on the Streaming-only web interface. Users can stream the recordings inside the folder without logging in. A publically accessible folder can be PIN protected or not. The list of publically accessible folders on the Streaming-only interface provides no indication of folder hierarchy. Therefore, any folders with the same name are indistinguishable on the Streaming-only interface.
External storage		
NFS path	The path to the external storage location is expressed in the following format: <IP address>:<path> For example: treasure-island:/storage/vcr31 Note that it is not necessary to prefix the server name with a double-backslash (\\).	Using a Network Files System (NFS) is useful where you have a lot of recordings stored on the IP VCR and space has become short. This is also a useful solution where multiple IP VCRs need access to the same recordings. For more information, refer to Storing recordings externally.
Export internal recordings	Whether to export recordings stored in this folder to the specified external location.	When **Export internal recordings** is selected for an NFS link for a folder: newly-created recordings in that folder will be exported to the NFS location when they are complete newly-uploaded recordings in that folder will be exported to the NFS location when the upload

Field	Field description	Usage tips
		is complete existing recordings in that folder on the internal disk of the IP VCR will be exported to the NFS location recordings physically stored in the NFS location are visible, and can be played, streamed, and recording details can be edited (renamed, given new PIN etc) When **Export internal recordings** is not selected for an NFS link for a folder: recordings physically stored in the NFS location are visible, and can be played, streamed, and recording details can be edited (renamed, given new PIN etc)
Register external recordings with gatekeeper	Select this option to enable recordings stored externally to be registered with an H.323 gatekeeper.	Note that registration of recordings can only take place if the recording has been allocated a Numeric ID and H.323 registration has been enabled for that recording (refer to Viewing and updating recording details).
Current status		
Recording ID gatekeeper state **Recording console ID gatekeeper state** **Auto attendant ID gatekeeper state**	The status of a folder's IDs with respect to its H.323 gatekeeper registration. The possible states for each folder ID are: *n/a* This ID is not configured to be registered with a gatekeeper; because of this, there is no applicable registration status to show. *Registering* This ID is in the process of registering with the gatekeeper. *Deregistering* The ID is in the process of unregistering with the gatekeeper. This might occur if: Gatekeeper registration has been turned off for the entire IP VCR Registration of folder IDs has been turned off for the entire IP VCR via the **Settings > Gatekeeper** page The configured gatekeeper has just been changed and the IP VCR is in the process of unregistering from the previous gatekeeper before registering with the new one. *Re-registration pending* / *Retry timeout* If the IP VCR fails to register an ID with the gatekeeper, it enters these states temporarily before re-attempting the registration. *<number> registered* The ID has been registered successfully with the gatekeeper using the number indicated. *<no ID set>* The ID is configured to register with a gatekeeper, but has not had a numeric identifier set.	
Point-to-point call incoming prefix	Displays the prefix that the H.323 gatekeeper uses to identify which calls to route though the IP VCR for the purposes of making point-to-point recordings.	For more information about this prefix, refer to the table above.
External storage	Indicates whether the server is responding or not and, if it is responding, the amount of free	

Field	Field description	Usage tips
state	space is displayed.	

Storing recordings externally

In this section:

About external storage

Any IP VCR folder (including the root) can be configured to link to an external Network File System (NFS) location.

Recordings in a folder configured to link to an NFS location can either physically be stored on the IP VCR or in the NFS location. The set of recordings associated with that folder is the combined set of those physically stored on the IP VCR (and configured to be in that folder), and those in the external location (which is linked to that folder). Recordings in the specified NFS location are visible to the IP VCR and can be played and streamed.

For each folder that you link to an NFS location (see Understanding the folders list), you can choose to **Export internal recordings** or not (refer to Adding and updating folders). When **Export internal recordings** is selected for an NFS link for a folder:

- newly-created recordings in that folder will be exported to the NFS location when they are complete
- newly-uploaded recordings in that folder will be exported to the NFS location when the upload is complete
- existing recordings in that folder on the internal disk of the IP VCR will be exported to the NFS location
- recordings physically stored in the NFS location are visible, and can be played, streamed, and recording details can be edited (renamed, given new PIN etc)
- HD recordings that are transcoded for streaming are transcoded before being exported to the NFS location

Note that there must be sufficient space for new recordings on the IP VCR, because the recording is made onto the IP VCR in the first instance, and then exported to the NFS when complete. The **Status > Recording** page displays the free disk space of the IP VCR.

When **Export internal recordings** is *not* selected for an NFS link for a folder:

- recordings physically stored in the NFS location are visible, and can be played, streamed, and recording details can be edited (renamed, given new PIN etc)

Recordings stored externally (and/or automatically exported) are in the *.codian* file format only. You can copy *.codian* files into the external location and they are "seen" by any IP VCR folder linked to that external location. Multiple IP VCRs can have access to the same external location (or set of external locations). The recordings stored in the external location can be played back via the IP VCR in the usual ways, or downloaded to a PC and converted into MPEG or Windows Media Video formats using the converters (available from the web site).

Consistency of file information across multiple IP VCRs

To ensure that multiple IP VCRs listing a single recording show consistent information, that is PIN, Numeric ID, and Name, each exported recording consists of two parts:

- a *.codian* file

- an associated (by filename stem) XML "sidecar" file. This "sidecar" file is not required in order to play back the recording (whether that play back is an H.323 viewing, web-based streaming, or processing by an application such as the Converters) but is required so that if the information relating to that recording (that is the PIN, Numeric ID, or Name) has been changed by one IP VCR then the new information is seen by any other IP VCR

H.323 gatekeeper registration of externally stored recordings

Each IP VCR folder that links to an external location has a separate "Register external recordings with gatekeeper" setting. When this is selected, each external recording retains its own H.323 gatekeeper and SIP registration option. If "Register external recordings with gatekeeper" is not selected then the recordings in this folder that are stored in the external location will not be accessible via the gatekeeper (unless this has been configured via another IP VCR). Note that unless an individual recording is configured to be registered with an H.323 gatekeeper, then no registration of that recording's Numeric ID will take place (refer to Viewing and updating recording details).

This enables your configuration of the IP VCR to navigate the issues that will arise if multiple IP VCRs are able to see the same set of recordings at an external location and if these recordings are registered with a gatekeeper. For example:

- if you have multiple IP VCRs registered with the same gatekeeper, in which case no more than one would be able to register a recording's configured Numeric ID
- if you have IP VCRs registered with different gatekeepers, in which case it would be valid for them to register the same set of IDs
- multiple IP VCRs might be registered with the same gatekeeper but using different prefixes; again, the same set of recordings could be registered by multiple IP VCRs

Note that currently there is no corresponding SIP registrar option for externally stored recordings.

NFS server information

NFS version 3 is supported by the IP VCR . This does not support client-based user / password authentication, instead requiring server-side access control (typically based on remote address).

The NFS server can be configured as "read-write" or "read-only". If the server is "read-only", the IP VCR will not be able to modify the XML "sidecar" file of an external recording or export recordings. If the server is "read-write", the IP VCR can modify the XML "sidecar" file of external recordings and export recordings (if the folder is in "export" mode).

Understanding the Connections list

The Connections list displays information about all recordings and playbacks currently in progress, as well as calls to the auto attendant (see Understanding the recordings list and Using an auto attendant). To view the Connections list, go to **Connections**. See the following table for an explanation of the fields that display:

- Active connections
- Connection controls

Active connections

An active connection refers to any call into or out of the IP VCR (whether to watch or make a recording), or a web streaming session. The following information is displayed for each connection:

Field	Field description	Usage tips
Name	The name of the recording being made or played back. Click on the name to display the **connection status** page, which shows more detailed connection information (see Viewing connection status).	Alternatively this field may display a special purpose name, for example *Auto attendant* if the auto attendant is in use and a recording has not yet been selected for playback.
Description	A brief description of the type of connection, for example *Streaming playback*, *Recording* or *Auto attendant*.	Sort the list by this field to group all active recordings for easy reference.
Status	A more detailed indication of the connection progress.	A recording session may indicate that recording has yet to start, while a playback session may show how far through the recording playback has reached, as well as the total recording length. If relevant the number of streaming viewers is shown.
Start time	The time when the connection was created.	A connection is created for each call into or out of the IP VCR.
Preview	Displays a sample still video capture of either the playback or recording, if available.	For recording sessions, the video media being recorded is previewed; for H.323 playback, the video media being played back is previewed. A preview may not be available for all connections, for example when web streaming or if **HD video capture mode** (see Configuring recording settings) is on.

Connection controls

Ending connections

To end a connection, either recording or playback, select which connection you want to disconnect by selecting its associated check box in the Active connections list, and clicking **Disconnect selected**. You can end several connections at once.

Viewing connection status

Extended details about active connections can be viewed on the **Connection status** page. To view these:

1. Go to **Connections**.
2. Click a connection name to display the **Connection status** page.

An overview of the connection status is shown on this page. Basic connection details are shown, as well as per-endpoint details. For playback and direct recording connections, information for just one endpoint is shown; for point-to-point recordings, information for both endpoints is shown. Refer to the sections below for more details:

- Connection status
- Endpoint status
- Extended endpoint information

Connection status

For each connection, basic information is displayed, such as when playback or recording started.

Endpoint status

Endpoint specific information is displayed for each endpoint associated with a connection. For playback and direct recording connections, information for just one endpoint is shown; for point-to-point recordings, information for both endpoints is shown. The same information is shown whether one or two endpoints are displayed.

Endpoint information is not available for streaming playback connections.

Extended endpoint information

Further endpoint information and control can be accessed via the page tabs. Refer to the following sections for more details:

- Viewing a connected endpoint's display
- Viewing a connected endpoint's camera
- Viewing a connected endpoint's audio signals
- Viewing a connected endpoint's media statistics
- Viewing a connected endpoint's diagnostics

Viewing a connected endpoint's display

When watching a recording, you can monitor the playback shown on a user's video endpoint. You can also monitor the display when making point-to-point recordings. The monitor display is not available for streaming playback connections. To monitor the display:

1. Go to **Connections**.
2. Click a connection name to display the Connection status page.
3. Click the **Display** tab.
4. Select which endpoint's display you want to view (point-to-point recordings only).

Display monitoring is not available for non-interactive recordings.

Viewing a connected endpoint's camera

When making a recording, you can control the viewing angle, zoom and focus of the camera on your video endpoint. These settings are not available for streaming playback connections. To customize the view:

1. Go to **Connections**.
2. Click a connection name to display the connection status page.
3. Click the **Camera** tab.
4. Select which endpoint's camera you want to control (point-to-point recordings only).

Camera preview and control is not available for any kind of playback connection.

Field	Field description	Usage tips
Movement	Click on one of the directional arrows to change the view direction of the camera.	Not all endpoints will respond to these controls. In particular, endpoints with fixed cameras such as most webcams will not respond to these controls.
Zoom	Click on one of the magnifying options to zoom the view in or out.	Not all endpoints will respond to the zoom controls, possibly including those that do respond to the **Movement** controls
Focus	Click on one of the adjustment options to improve the clarity of the image.	Not all endpoints will respond to the focus controls, possibly including those that do respond to the **Movement** controls .

Viewing a connected endpoint's audio signals

In general, the audio settings are for advanced troubleshooting. Audio settings are not available for streaming playbacks. You can view these settings by selecting this option:

1. Go to **Connections**.
2. Click a connection name to display the **Connection status** page.
3. Click the **Audio** tab.
4. Select which endpoint's audio signals you want to view (point-to-point recordings only).

The information and controls displayed are mainly for troubleshooting audio problems with recordings.

Audio information is not available for streaming playback connections.

Viewing a connected endpoint's media statistics

You can view statistics about the video and audio streams to and from the IP VCR while making and watching recordings. The statistics are not available for streaming playback connections. To view the connection statistics:

1. Go to **Connections**.
2. Click a connection name to display the **Connection status** page.
3. Click the **Statistics** tab.
4. Select which endpoint's display you want to view (point-to-point recordings only).

Media statistics

Media statistics provide detailed information about the actual voice and video streams (Realtime Transport Protocol (RTP) packets).

Refer to the following table for additional information.

Field	Field description	Usage tips
Audio		
Receive stream	The audio codec in use, along with the current packet size (in milliseconds) if known.	If the IP VCR has received information that an endpoint has been muted at the far end, this is indicated here.
Receive address	The IP address and port from which the media is originating.	
Encryption	Whether or not encryption is being used on the audio receive stream by this endpoint.	This field will only appear if the encryption feature key is present on the IP VCR.
Received jitter	The apparent variation in arrival time from that expected for the media packets (in milliseconds). The current jitter buffer also displays in parentheses.	You should expect to see small values for this setting. Consistently large numbers typically imply potential network problems. The jitter buffer shows the current playout delay added to the media to accommodate the packet arrival jitter. Large jitter values indicate a longer buffer.
Received energy	Represents the audio volume originating from the endpoint.	
Packets received	The number of audio packets destined for the IP VCR from this endpoint.	
Packet errors	The number of packet errors, including sequence errors, and packets of the wrong type.	You should expect to see small values for this setting. Consistently large numbers typically imply potential network problems.
Frame errors	Frame errors, as *A/B* where *A* is the number of frame errors, and *B* is the total number of frames received.	A frame is a unit of audio, the size of which is dependent on codec. You should expect to see small values for this setting. Consistently large numbers typically imply potential network problems.
Media information	If the time stamps or marker bits (or both) are detected to be unreliable in the incoming video stream, information is displayed here.	This field is not displayed when there is no problem with the time stamps and marker bits. Where there is a problem the following text is displayed: "Media timestamps unreliable", "Media marker bits unreliable", or both if both conditions detected.

Field	Field description	Usage tips
Transmit stream	The audio codec being sent from the IP VCR to the endpoint, along with the chosen packet size in milliseconds.	
Transmit address	The IP address and port to which the media is being sent.	
Encryption	Whether or not encryption is being used on the audio transmit stream by this endpoint.	This field will only appear if the encryption key is present on the IP VCR.
Packets sent	A count of the number of packets that have been sent from the IP VCR to the endpoint.	
Video (primary channel and content shown separately)		
Receive stream	The codec in use and the size of the picture that the IP VCR is receiving from the specific participant. If the picture is a standard size (for example, CIF, QCIF, 4CIF, SIF) then this name is shown in parentheses afterwards.	
Receive address	The IP address and port (<IP address>:<port>) of the device from which video is being sent	
Encryption	Whether or not encryption is being used on the video receive stream from this endpoint.	This field will only appear if the encryption key is present on the IP VCR.
Channel bit rate	The negotiated bit rate available for the endpoint to send video in.	This value represents the maximum amount of video traffic that the remote endpoint will send to the IP VCR. It may send less data than this (if it does not need to use the full channel bit rate or the IP VCR has requested a lower rate), but it should not send more.
Receive bit rate	The bit rate (in bits per second) that the IP VCR has requested that the remote endpoint sends. The most-recently measured actual bit rate displays in parentheses.	This value might be less than the **Channel bit rate** if: the IP VCR detects that the network path to the remote endpoint has insufficient capacity to maintain a higher traffic rate that endpoint's video stream's position in the active conference compositions does not require it it has been necessary to reduce the video bit rate because of the overall call bit rate; the audio bit rate plus the video bit rate should not exceed the call bit rate For example, if all participants in the conference were watching a single participant at full screen, no other participants' video streams would be needed at all. So the IP VCR would request that those streams were sent at a low bit rate in order to avoid needless use of network bandwidth. If the receive bit rate has been limited to below the maximum channel bit rate, the reason for this limitation can be seen by moving over the icon.
Received jitter	Represents the variation in video packet at arrival time at the IP VCR.	
Packets received	The number of video packets destined for the IP VCR from this endpoint	

Field	Field description	Usage tips
Packet errors	Video packet-level errors such as sequence discontinuities, incorrect RTP details, and so on. This is not the same as packets where the content (the actual video data) is somehow in error.	This value does not represent packets in which the actual video data in the packets is in error.
Frame rate	The frame rate of the video stream currently being received from the endpoint.	
Frame errors	The number of frames with errors versus the total number of video frames received.	
Transmit stream	The codec, size and type of video being sent from the IP VCR to the endpoint.	
Transmit address	The IP address and port of the device to which the IP VCR is sending video.	
Encryption	Whether or not encryption is being used on the video transmit stream to this endpoint.	This field will only appear if the encryption key is present on the IP VCR.
Channel bit rate	The negotiated available bandwidth for the IP VCR to send video to the endpoint in.	
Transmit bit rate	The bit rate the IP VCR is attempting to send at this moment, which may be less than the channel bit rate which is an effective maximum. The actual bit rate, which is simply the measured rate of video data leaving the IP VCR, displays in parentheses.	The **Transmit bit rate** value might be less than the **Channel bit rate** if : the remote endpoint receiving the video stream from the IP VCR has sent flow control commands to reduce the bit rate it has been necessary to reduce the primary video bit rate to allow sufficient bandwidth for a content video stream If the transmit bit rate has been limited to below the maximum channel bit rate, the reason for this limitation can be seen by moving over the ? icon.
Packets sent	The number of video packets sent from the IP VCR to this endpoint.	
Frame rate	The frame rate of the video stream currently being sent to the endpoint.	
Temporal/spatial	A number that represents the tradeoff between video quality and frame rate.	A smaller number implies that the IP VCR prioritizes sending quality video at the expense of a lower frame rate. A larger number implies that the IP VCR is prepared to send lower quality video at a higher frame rate.

Control statistics

Control statistics provide information about the control channels that are established in order that the endpoints can exchange information about the voice and video streams (Real Time Control Protocol (RTCP) packets). Refer to the following table for additional information.

Field	Field description	Usage tips
Audio		
RTCP receive address	The IP address and port to which RTCP (Real Time Control Protocol) packets are being received for the audio and video streams	
Receiver reports	A count of the number of "receiver report" type RTCP packets seen by the IP VCR.	A single RTCP packet may contain more than one report of more than one type. These are

Field	Field description	Usage tips
		generally sent by any device receiving RTP (Real Time Protocol) media from the network and are used for auditing bandwidth, errors, and so on by the IP VCR.
Packet loss reported	Media packet loss reported by receiver reports sent to the IP VCR by the far end.	
Sender reports	A count of the number of "sender report" type RTCP packets received by the IP VCR.	These are typically sent by any device that is sending RTP media.
Other	A count of the number of reports seen by the IP VCR that are neither sender nor receiver reports.	
RTCP transmit address	The IP address and port to which the IP VCR is sending RTCP packets about this stream.	
Packets sent	The number of packets sent.	
Video (primary channel and content shown separately)		
RTCP receive address	The IP address and port to which RTCP (Real Time Control Protocol) packets are being sent for the audio and video streams.	
Receiver reports	A count of the number of "receiver report" type RTCP packets seen by the IP VCR.	A single RTCP packet can contain more than one report of more than one type. These are generally sent by any device receiving RTP (Real Time Protocol) media from the network and are used for auditing bandwidth, errors, and so on by the IP VCR.
Packet loss reported	A count of the reported packet loss on the control channel.	
Sender reports	A count of the number of "sender report" type RTCP packets sent by the IP VCR.	These are typically sent by any device that is sending RTP media.
Other	A count of the number of reports seen by the IP VCR that are neither sender nor receiver reports.	
RTCP transmit address	The IP address and port to which the IP VCR is sending RTCP packets about this stream.	
Packets sent	The number of packets sent.	
Fast update requests	The number of fast update requests sent and received.	
Flow control messages	The number of flow control messages sent and received.	

Viewing a connected endpoint's diagnostics

You can view diagnostics for an endpoint's connection to the IP VCR while making and watching recordings. The diagnostics are not available for streaming playback connections. To view the diagnostics:

1. Go to **Connections**.
2. Click a connection name to display the Connection status page.
3. Click the **Diagnostics** tab.
4. Select which endpoint's diagnostics you want to view (point-to-point recordings only).

Participant diagnostics

This page shows various low-level details pertaining to the endpoint's communication with the IP VCR. You are not likely to need to use any of the information on this page except when troubleshooting specific issues under the guidance of Customer support.

Displaying the Endpoint list

To display the Endpoint List, go to **Endpoints**.

The Endpoint list displays all endpoints that have been configured on the IP VCR.

- To add a new H.323 endpoint, select **Add H.323**.
- To add a new SIP endpoint, select **Add SIP**.
- To delete configured endpoints, select the one(s) that you want to delete and click **Delete selected**.

Field	Field description
Name	The name of the endpoint.
Address	The IP address, host name, or SIP URI of the endpoint.
Type	Whether it is an H.323 or a SIP endpoint.

Configuring H.323 endpoints

You can configure H.323 endpoints to work with the IP VCR by choosing **Endpoints > Add H.323**. This makes it easier to call out to endpoints because you can select names from a list rather than adding network addresses. (For information about SIP endpoints, see Configuring SIP endpoints.)

Refer to the following table for tips on adding an H.323 endpoint to the IP VCR. After entering the settings, click **Add endpoint**. The endpoint appears in the Endpoint list.

Field	Field description	Usage tips
Name	The name of the endpoint.	
Address	The IP address, host name, or an E.164 address (phone number).	You can configure this endpoint as needing to be reached via an H.323 gateway without that gateway being already configured on the IP VCR. To do this, set this field to be *<gateway address>!<E.164>*.
H.323 gateway	The gateway through which the endpoint connects.	To configure a gateway on the IP VCR, go to **Gateways**. For more information, refer to Adding and updating gateways.
DTMF sequence	The DTMF sequence to be sent to an audio conferencing bridge.	Allows the MCU to send DTMF tones to an audio bridge after the audio bridge has answered the call. In this way, the MCU can navigate audio menus. This is useful where a conference on the MCU dials out to an audio-only conference on an audio bridge. You can configure an audio bridge with a DTMF sequence as a pre-configured endpoint (either H.323 or SIP) which can then be added to any conference. Alternatively, you can add the audio bridge to an individual conference as a participant. You must specify the DTMF sequence in the Call-out parameters for that endpoint. The DTMF sequence can include digits 0-9 and * and #. There is a two second pause after the call connects after which the MCU will send the DTMF tones which are sent one every half second. You can insert as many additional two second pauses as you want by inserting commas into the DTMF sequence. Each comma represents a two second pause. For example, you want the MCU to dial out to a PIN-protected audio conference on an audio bridge. The conference ID is 555 and the PIN is 888. The audio bridge requires that you press # after entering the ID and after entering the PIN. In this example the DTMF sequence is: 555#,,888#. The two commas represent a four second pause which allows the audio bridge's automated menu system time to process the ID and request the PIN.
Call-in match parameters	These fields are used to identify incoming calls as being from the endpoint: **Name**: This must be the name that the endpoint sends to the IP VCR **IP address**: The IP address of the endpoint **E.164**: The E.164 number with which the endpoint is registered with the gatekeeper	The endpoint is recognized if all filled-in fields in this section are matched. Fields left blank are not considered in the match. When you configure **Call-in match parameters**, an endpoint is recognized as *this* pre-configured endpoint and the **Connection parameters** are applied to a call from this endpoint.
Motion / sharpness	Select whether to use the unit-wide/blade-wide setting for motion/sharpness trade off, or	The settings for motion (frames per second) and sharpness (frame size or resolution) are

Field	Field description	Usage tips
trade off	configure an individual setting for use with this endpoint. Select from: *<use box-wide setting>*: this is the default value. In this case, the connection to the endpoint will use the motion / sharpness tradeoff setting from the **Settings > Connections** page. *Favor motion*: the IP VCR will try and use a high frame rate. That is, the IP VCR will strongly favor a resolution of at least 25 frames per second *Favor sharpness*: the IP VCR will use the highest resolution that is appropriate for what is being viewed *Balanced*: the IP VCR will select settings that balance resolution and frame rate (where the frame rate will not be less than 12 frames per second)	negotiated between the endpoint and the IP VCR. This setting controls how the IP VCR will negotiate the settings to be used with this endpoint.
Transmitted video resolutions	Select the setting for transmitted video resolutions from the IP VCR to this endpoint. This setting overrides the unit-wide/blade-wide setting on the **Settings > Connections** page.	Retain the default setting (*use box-wide setting*) unless you are experiencing problems with the display of certain resolutions by this endpoint. Endpoints advertise the resolutions that they are able to display. The IP VCR then chooses from those advertised resolutions, the resolution that it will use to transmit video. However, some endpoints do not display widescreen resolutions optimally. Therefore, you might want to use this setting to restrict the resolutions available to the IP VCR for transmissions to this endpoint.
Content contribution	Whether this endpoint is permitted to contribute a content channel when making a new recording.	
Content receive	Whether this endpoint is allowed to receive a separate content stream when playing back a stored recording.	
Preferred bandwidth from IP VCR	The network capacity (measured in bits per second) used by the media channels established by the IP VCR to a single participant.	These settings take priority over the **Default bandwidth from IP VCR** setting configured in the global Connection settings (see Connection settings).
Preferred bandwidth to IP VCR	The maximum combined media bandwidth advertised by the IP VCR to endpoints.	These settings take priority over the **Default bandwidth to IP VCR** setting configured in the global Connection settings (see Connection settings).
Custom codec selection	Used to ensure only specific codecs are permitted on calls to (and received from) this endpoint.	Select *Enabled* to display fields in which you can select the codecs to use when communicating with this endpoint. When *Enabled*, these selections override the unit-wide/blade-wide codec selection on the **Settings > Connections** page for this endpoint.

Configuring SIP endpoints

To configure the SIP endpoints to work with the IP VCR, go to **Endpoints > Add SIP**. This makes it easier to call out to endpoints because you can select names from a list rather than adding network addresses. (For information about SIP endpoints, see Configuring H.323 endpoints.)

Refer to the following table for tips on adding a SIP endpoint to the IP VCR. After entering the settings, click **Add endpoint.** The endpoint appears in the Endpoint list.

Field	Field description	Usage tips
Name	The name of the endpoint.	
Address	The IP address, host name, or SIP URI (in the format 1234@cisco.com).	The address of the SIP endpoint can be a directory number if you are using a SIP registrar.
Use SIP registrar	Allows calls to this endpoint to use a directory number (in the *Address* field) and the SIP registrar.	If you have this enabled, you must configure the SIP registrar on the **Settings > SIP** page.
Call-in match parameters	These fields are used to identify incoming calls as being from the endpoint.	The endpoint is recognized if all filled-in fields in this section are matched. Fields left blank are not considered in the match. Note that in some cases a SIP registrar can cause a call to appear to come from the IP address of the registrar rather than the IP address of the endpoint. In this case, to use call-in match parameters, leave the IP address field blank and enter the correct username. The call will be matched by username. When using LCS, the username that will be matched is the user's display name (e.g. Peter Rabbit) rather than the sign-in name (bluecoat@cisco.com).
Motion / sharpness trade off	Choose whether to use the box-wide setting for motion/sharpness trade off, or configure an individual setting for this endpoint. Choose from: *Use box-wide setting*: this is the default value. In this case, the endpoint will use the motion/sharpness tradeoff setting from the **Settings > Connections** page *Favor motion*: the IP VCR will try and use a high frame rate. That is, the IP VCR will strongly favor a resolution of at least 25 frames per second *Favor sharpness*: the IP VCR will use the highest resolution that is appropriate for what is being viewed *Balanced*: the IP VCR will select settings that balance resolution and frame rate (where the frame rate will not be less than 12 frames per second)	The settings for motion (frames per second) and sharpness (frame size or resolution) are negotiated between the endpoint and the IP VCR. This setting controls how the IP VCR will negotiate the settings to be used with this endpoint.
Transmitted video resolutions	Choose the setting for transmitted video resolutions from the IP VCR to this endpoint. This setting overrides the unit-wide/blade-wide setting on the **Settings > Connections** page.	Retain the default setting (*use box-wide setting*) unless you are experiencing problems with the display of certain resolutions by this endpoint. Endpoints advertise the resolutions that they are able to display. The IP VCR then chooses from those advertised resolutions, the resolution that it will use to transmit video. However, some endpoints do not display

Field	Field description	Usage tips
		widescreen resolutions optimally. Therefore, you might want to use this setting to restrict the resolutions available to the IP VCR for transmissions to this endpoint.
Content receive	Whether this endpoint is allowed to receive a separate content stream when playing back a stored recording.	
Preferred bandwidth from IP VCR	The network capacity (measured in bits per second) used by the media channels established by the IP VCR to a single participant.	These settings take priority over the **Default bandwidth from IP VCR** setting configured in the global Connection settings (see Connection settings).
Preferred bandwidth to IP VCR	The maximum combined media bandwidth advertised by the IP VCR to endpoints.	These settings take priority over the **Default bandwidth to IP VCR** setting configured in the global Connection settings (see Connection settings).
Custom codec selection	Can be used to ensure only specific codecs are permitted on calls to (and received from) this endpoint.	Select *Enabled*, to display fields in which you can choose which codecs are used when communicating with this endpoint. When *Enabled*, this setting overrides the unit-wide/blade-wide codec selection on the **Settings > Connections** page.

Displaying the gateway list

You can configure the IP VCR to work with one or more H.323 gateways. The IP VCR can then effectively call through these configured gateways to one or more endpoints which are registered with the gateway but would not be reachable directly from the IP VCR.

For example, an IP PBX could be configured as a gateway, and the IP VCR could then call its registered E.164 numbers. An ISDN gateway can be configured as a gateway on the IP VCR allowing calls to ISDN endpoints and telephones.

The gateway list shows all of the currently configured H.323 gateways. To access this list, go to **Gateways**.

To add a gateway, click **Add H.323 gateway** and see Adding and updating gateways .

To delete configured gateways, select the ones that you want to delete and select **Delete selected**.

Field	Field description
Name	The descriptive name of the gateway.
Address	The IP address or host name of the gateway.
Receive bandwidth	The configured preferred bandwidth to the IP VCR from the gateway, or <*default value*> if no preference has been specified.
Transmit bandwidth	The configured preferred bandwidth from the IP VCR to the gateway, or <*default value*> if no preference has been specified.

Adding and updating gateways

You can configure the IP VCR with one or more H.323 gateways:

- To add an H.323 gateway, go to **Gateways > Add new H.323 gateway**. After entering the settings described below, click **Add H.323 gateway**.
- To update an existing H.323 gateway, go to **Gateways** to display the Gateway list and click on a gateway name. After updating the settings described below, click **Update H.323 gateway**.

Field	Field description	More information
Name	The descriptive name of the gateway.	All gateways must have a unique name.
Address	The IP address or host name of the gateway.	
Motion / sharpness trade off	Choose whether to use the unit-wide/blade-wide setting for motion/sharpness trade off, or configure an individual setting for this gateway. Choose from: *Use box-wide setting*: this is the default value. In this case, connections to the gateway will use the motion/sharpness tradeoff setting from the **Settings > Connections** page *Favor motion*: the IP VCR will try and use a high frame rate. That is, the IP VCR will strongly favor a resolution of at least 25 frames per second *Favor sharpness*: the IP VCR will use the highest resolution that is appropriate for what is being viewed *Balanced*: the IP VCR will select settings that balance resolution and frame rate (where the frame rate will not be less than 12 frames per second)	The settings for motion (frames per second) and sharpness (frame size or resolution) are negotiated between the endpoint and the IP VCR. This setting controls how the IP VCR will negotiate the settings to be used with this endpoint.
Preferred bandwidth from IP VCR	The network capacity (measured in bits per second) used by the media channels established by the IP VCR to a single participant.	
Preferred bandwidth to IP VCR	Sets the bandwidth that the endpoint will advertise to the IP VCR when it calls it.	

Displaying the built-in gatekeeper registration list

The IP VCR contains a built-in gatekeeper with which devices can register multiple IDs. IDs can be numbers, H.323 IDs (e.g. Fredsendpoint) or prefixes.

Up to 25 devices can be registered without a feature key. Feature keys can be purchased to increase this number.

Note: The IP VCR can register with its own built-in gatekeeper. The IP VCR then counts as one registered device. See Configuring gatekeeper settings.

Configuring the built-in gatekeeper

To start the gatekeeper, go to **Network > Services** and select **H.323 gatekeeper** to open a port for the gatekeeper (see Configuring IP services). (On the IP VCR, ports are not open by default for security reasons.) Then go to **Gatekeeper**, select *Enabled* in the Status field and click **Apply changes**. If you attempt to enable the built-in gatekeeper without opening the port, an error message is displayed.

Configuring neighboring gatekeepers

You can optionally configure the built-in gatekeeper with up to two neighboring gatekeepers. This means that if the built-in gatekeeper receives a request (known as an Admission Request or ARQ) to resolve an ID to an IP address and that ID is not currently registered with it then it will forward that request to its neighbor gatekeeper(s), as a Location Request (LRQ). The built-in gatekeeper will then use the information received from the neighbor(s) to reply to the original request.

You can also configure the behavior of the built-in gatekeeper on receipt of LRQs from another gatekeeper. It can:

- send LRQs regarding unknown IDs to its neighbor(s)
- reply to LRQs from other gatekeepers
- accept LCFs (Locations Confirms) from non-neighboring gatekeepers

Refer to this table for assistance when configuring the built-in gatekeeper:

Field	Field description	Usage tips
Status	Enables or disables the built-in gatekeeper.	To use the built-in gatekeeper, you must enable it here.
Neighbor gatekeeper 1 and 2	Enter the IP address(es), or hostname(s) (or <host>:<port number> to specify a port number on the neighboring gatekeeper), of the neighboring gatekeeper(s).	These are the gatekeepers to which the built-in gatekeeper will send an LRQ if it has received an ARQ to resolve an ID which it does not currently have registered. The built-in gatekeeper will then use the information received from the neighbor(s) to reply to the original request.
Accept LRQs	Configures the built-in gatekeeper to reply to LRQs from other gatekeepers.	These requests can come from any gatekeeper which has the IP VCR's built-in gatekeeper configured as one of its neighbors.
Forward LRQs for unknown IDs	Configures the built-in gatekeeper to send (or not to send) LRQs regarding unknown IDs to its neighbor(s). Choose from the options: *Disabled*: The IP VCR will only respond to LRQs about IDs	Unless you have selected to **Accept LRQs**, you cannot configure the IP VCR to forward any LRQs. Enabling *using received return address* can be a significant security risk. Only use this setting with proper cause.

Field	Field description	Usage tips
	registered with itself. It will not forward LRQs about IDs that are not registered with itself to neighboring gatekeepers. *Enabled, using local return address*: The IP VCR will put, in the LRQ, its own address as the return address for the LCF. *Enabled, using received return address*: The IP VCR will put, in the LRQ, the address of the gatekeeper that originated the request as the return address for the LCF. Use this option only if you are configuring the IP VCR to operate in an environment with a multiple-level gatekeeper hierarchy. For example, the 'received address' is required by the national gatekeepers connected to the Global Dialing Scheme (GDS).	
Accept LCFs from non-neighbors	This setting enables the built-in gatekeeper to accept LCF message responses from any IP address.	This setting is for use in environments with a multiple-level gatekeeper hierarchy. For example, this feature is required by the national gatekeepers connected to the Global Dialing Scheme (GDS). Enabling this setting can be a significant security risk. Only use this setting with proper cause.

Gatekeeper status

The number of registered devices is shown in the format X / Y where Y is the number of registered devices that your built-in gatekeeper is licensed for. Equally, the total number of registered IDs is shown as Z / 1000, where 1000 is the maximum number of registrations allowed over all registered devices.

Below these summary figures is a table showing individual registrations. Registrations can be viewed by registered ID (the "ID view") or by device (the "Registration view"), giving complete and easily searchable lists. Switch between the views by clicking on the appropriate button.

The Registration view shows the summary per device (also known as the registrant), while the ID view shows individual registrations. This means that registrations from the same device are not necessarily listed together in the ID view but the view can be sorted by Registrant or Index to help you identify IDs belonging to the same registrant.

ID view

Field	Field description	Usage tips
ID	The ID which the registrant has registered with the gatekeeper.	IDs can be numbers, H.323 IDs or prefixes.
Type	The type of registration.	One of: E.164 (digits), H.323 ID or Prefix.
Index	This registrations index within the total number of registrations that this registrant has made with the gatekeeper.	In the format X / Y where Y is the number of registrations that this registrant has made with the built-in gatekeeper, and X is this particular registration's position within the total. Therefore, if a device registered 3 IDs with the gatekeeper and this was the second registration to be made, the Index would be 2 /

Field	Field description	Usage tips
		3.
Registrant	The IP address of the device that this registration was made from.	If the remote device has indicated via the RAI (Resource Availability Indication) mechanism that it is close to its resource limit, the Registrant label is "almost out of resources".

Registration view

This view shows a one-line summary for each device registered with the built-in gatekeeper.

To deregister one or more devices (and all registrations for these devices), select the appropriate entries and then click **Deregister selected**.

Field	Field description	Usage tips
Registrant	The IP address of the device.	If the remote device has indicated via the RAI (Resource Availability Indication) mechanism that it is close to its resource limit, the Registrant label is "almost out of resources".
H.323 ID	The registered H.323 ID of the device.	To help identify registering devices, if the registrant has registered a H.323 ID (which will typically be its device name) that H.323 ID is shown here. If the device has registered multiple H.323 IDs, only the first is displayed.
Registered IDs	The number of registrations that this device has made with the built-in gatekeeper.	Click **(view)** to display individual registrations for the selected device. (The format is the same as the ID view, but the table only includes entries for one device.)
Registration time	The time today or date and time of the last registration.	

System defined users

The IP VCR is pre-configured with two user accounts ("admin" and "guest"), but you can also add other users (see Adding and updating users). Refer to the following table for descriptions of the pre-configured users.

User ID	Description	Usage tips
admin	The IP VCR must have at least one configured user with administrator privileges. By default, the User ID is "admin" and no password is required. If you configure the IP VCR with advanced account security mode, a password is required. For more information about advanced account security mode, refer to Configuring security settings.	After logging into the IP VCR for the first time (see Logging into the web interface), you can change the User ID and password for this account. The privilege level is fixed at *administrator* for the admin user - who can see all the pages and change settings.
guest	The IP VCR must have at least one configured user with access privileges below *administrator*. The fixed User ID for this user is "guest" and by default no password is required. If you configure the IP VCR with advanced account security mode, the guest account requires a password that adheres to secure password criteria. For more information about advanced account security mode, refer to Configuring security settings.	You cannot change the name of the "guest" User ID. You can add a password.

You can modify the system defined user accounts if you need to. For example, for security, you should add a password to the admin account.

Note that you can also create new accounts with administrator or lower access privileges in addition to these pre-defined users (see Adding and updating users).

User privilege levels

Every configured user in the IP VCR has an associated privilege level. Privilege levels determine the amount of control the user has over the IP VCR and its settings. Refer to the following table for details.

Privilege level	Access
administrator	The main difference between an administrator and users with lower privilege levels is that administrators can change settings that affect all recordings and the configuration of the IP VCR itself, whereas other users only have access to individual recordings and to their own profiles. Users with administrator access can: • View IP VCR-wide status (**Status**) • Perform software upgrades (**Settings > Upgrade**) • Change system-wide connection settings (**Settings > Connections**) • Change recording settings (**Settings > Recording**) • View the Event log (**Events**) • Configure H.323 gateways (**Gateways**) • Manage users (**Users**) • Manage endpoints (**Endpoints**) • Fully control recordings (**Recordings**)
full recording access	Users with this privilege level can: • Change their own profile (**Profile**) • View the list of stored recordings (**Recordings**) • View recordings via streaming (**Recordings**) • Upload new recordings (**Recordings**) • Fully control recordings (**Recordings**) • View and modify active connections (**Connections**) • Configure H.323 gateways (**Gateways**) • Manage endpoints (**Endpoints**)
recording detail	Users with this privilege level can: • Change their own profile (**Profile**) • View the list of stored recordings (**Recordings**) • View recordings via streaming (**Recordings**) • Download recordings in MPEG format (**Recordings**)
recording list plus streaming	Users with this privilege level can: • Change their own profile (**Profile**) • View the list of stored recordings (**Recordings**) • View recordings via streaming (**Recordings**)
recording list only	Users with this privilege level can: • Change their own profile (**Profile**) • View the list of stored recordings (**Recordings**) The recordings list shows any configured E.164 numbers, and so is useful for finding out what number to dial to play back a stored recording to a H.323 video conferencing endpoint. See Connecting directly using a phone number for additional information.

Displaying the User list

Go to **Users** to see an overview of configured users on the IP VCR and a summary of some of their settings. Refer to the following table for assistance.

Field	Field description
User ID	The user name that the user needs to access the web interface of the IP VCR. Although you can enter text in whichever character set you require, some browsers and FTP clients do not support Unicode characters.
Name	The full name of the user.
Privilege	Access privileges associated with this user.

Deleting users

To delete a user, select the user you want to delete and click **Delete selected users**. You cannot delete the admin and guest users.

Adding and updating users

You can add users to and update users on the IP VCR. Although most information is identical for both tasks, some fields differ.
The IP VCR supports up to 200 users.

Adding a user

To add a user:

1. Go to **Users**.
2. Click **Add user**.
3. Complete the fields referring to the following table to determine the most appropriate settings for the user.
4. Click **Add user**.

Updating a user

To update an existing user:

1. Go to **Users**.
2. Click the name of the user that you want to update.
3. Change the fields as appropriate referring to the following table.
4. Click **Update user settings**.
5. To change the user's password, type in the current password once and the new password twice.
6. Click **Update password**.

Field	Field description	More information
User ID	Identifies the log-in name that the user will use to access the IP VCR web interface.	Although you can enter text in whichever character set you require, some browsers and FTP clients do not support Unicode characters.
Name	The full name of the user.	
Password	The required password, if any.	Although you can enter text in whichever character set you require, some browsers and FTP clients do not support Unicode characters. Note that passwords are stored in the configuration.xml file as plain text unless the IP VCR is configured (or has ever been configured) to use advanced account security mode. For more information, refer to Configuring security settings. Note that this field is only active when adding a new user. If you are updating an existing user and want to change that user's password, click **Change password** instead.
Re-enter password	Verifies the required password.	
Disable user account	Select to disable this account.	This can be useful if you want to keep an account's details, but do not want anyone to be able to use it at the moment. You cannot disable the system-created admin

Field	Field description	More information
		account. The system-created guest account is disabled by default. If you enable it, the IP VCR will create a security warning. In advanced account security mode, a non-admin account will expire after 30 days of inactivity; that is, the IP VCR will disable it. To re-enable a disabled account, clear this option. For more information about advanced account security mode, refer to Configuring security settings.
Lock password	Prevents user from changing password.	This is useful where you want multiple users to be able to use the same user ID. The system-created guest account has *Lock password* enabled by default.
Force user to change password on next login	Select this option to force a user to change their password. Next time this user attempts to log in to the IP VCR, a change password prompt will appear.	This option is enabled by default for a newly created account. It is a good idea for new users to set their own secure passwords. This option is not available for accounts where *Lock password* is selected. When the user changes his password, the IP VCR clears this check box automatically.
Privilege level	The access privileges to be granted to this user.	See User privileges for detailed explanations.

Updating your user profile

You can make some changes to your user profile. To do this, go to **Update user profile**. Refer to the following table for tips.

Field	Field description	More information
Name	Your name, which identifies you to other users.	Changing this field does not change your log-in User ID.
Password	You can enter a new password.	
Re-enter password	Verify the new password.	

Changing your password

Go to **Profiles** to change your password. (Users with administrator privileges can also change the password of other users.)

In advanced account security mode (set in **Settings > Security)**, passwords must have:

- at least fifteen characters
- at least two uppercase alphabetic characters
- at least two lowercase alphabetic characters
- at least two numeric characters
- at least two non-alphanumeric (special) characters
- not more than two consecutive repeating characters. That is, two repeating characters are allowed, three are not

In advanced account security mode:

- A new password must be different to the previous 10 passwords that have been used with an account.
- If a user logs in with a correct but expired password the IP VCR asks that user to change the password. If the user chooses not to change it, that user is allowed two more login attempts to change the password before the account gets disabled.
- Users other than administrator users are not allowed to change their password more than once in a 24 hour period.

If the IP VCR is in advanced account security mode, the above criteria for passwords are displayed on the **Change password** page.

If the IP VCR is not in advanced account security mode, there are no criteria for password selection.

(For more information see, Configuring security settings, Understanding security warnings, User privilege levels and Adding and updating users.)

Configuring global connection settings

You can modify the global connection settings for the IP VCR by going to **Settings > Connections**. However, many of these values can be overwritten by other IP VCR or endpoint settings.

- Connection settings
- Advanced settings

Connection settings

Refer to this table for assistance configuring the connection settings. After making any configuration changes, click **Apply changes**.

Field	Field description	Usage tips
Maximum video size	Identifies the greatest video size that the IP VCR will send and receive when connected to a video endpoint.	This option is only available if the MCU 4CIF (HRO) feature key is present.
Motion / sharpness trade off	Choose the unit-wide/blade-wide setting for motion/sharpness trade off. The options are: *Favor motion*: the IP VCR will try and use a high frame rate. That is, the IP VCR will strongly favor a resolution of at least 25 frames per second *Favor sharpness*: the IP VCR will use the highest resolution that is appropriate for what is being viewed *Balanced*: the IP VCR will select settings that balance resolution and frame rate (where the frame rate will not be less than 12 frames per second)	The settings for motion (frames per second) and sharpness (frame size or resolution) are negotiated between the endpoint and the IP VCR. This setting controls how the IP VCR will negotiate the settings to be used with an endpoint.
Transmitted video resolutions	Choose the unit-wide/blade-wide setting for transmitted video resolutions. This setting can be overridden by individual configured endpoint settings.	Retain the default setting (*Allow all resolutions*) unless you are experiencing problems with the display of certain resolutions by endpoints. Endpoints advertise the resolutions that they are able to display. The IP VCR then chooses from those advertised resolutions, the resolution that it will use to transmit video. However, some endpoints do not display widescreen resolutions optimally. In these cases, you might want to use this setting to restrict the resolutions available to the IP VCR. Note that you can configure this setting for individual configured endpoints if you do not need to restrict transmitted video resolutions for all endpoints.
Default bandwidth from IP VCR	Identifies the network capacity (measured in bits per second) used by the media channels established by the IP VCR to a single participant.	When the IP VCR makes a call to an endpoint, the IP VCR chooses the maximum bandwidth that is allowed to be used for the media channels which comprise that call. This field sets that maximum bandwidth, and is the total bandwidth of the audio channel and video channel combined. (for more information, see Creating video recordings.) This setting can be overridden by individual endpoints' **Preferred bandwidth from IP VCR** values.
Default bandwidth	Sets the bandwidth that the IP VCR will advertise to the endpoint when it calls it.	This setting can be overridden by individual endpoints' **Preferred bandwidth to IP VCR**

Field	Field description	Usage tips
to IP VCR		values.
Default incoming call action	Determines what the user experience will be when they call the IP VCR. • *Connect to auto attendant* The user will be presented with the default auto attendant from which they can view stored recordings or potentially make a recording of the session (see Using an auto attendant). • *Record session* The user will be presented with the video recording screen (see Using the recording console), allowing them to record the video from their endpoint. • *Disconnect caller* Users cannot call the IP VCR in this way; the call will be terminated.	The default call action is applied to calls to: • the IP address of the IP VCR • to E.164 numbers that do not match a specific recording or folder ID (using the service prefix). In this case, if the default action is *Record session*, the recording will be made into the root folder of the IP VCR and the recording will be given the numbers that follow the dialed service prefix as the recording ID. For example, if the registered service prefix is 33 and the dialed number is 331234 (and 1234 does not already match a recording or folder ID) a recording will be made in the root folder with the recording ID: 1234 For more information refer to Configuring gatekeeper settings. Recording a session uses one recording port.
Show recording participant names	Controls whether participant names will be overlaid onto the recorded video when making a point-to-point recording.	You may want to disable the overlaying of names by the IP VCR if the devices in the call add their own text to their video streams.

Advanced settings

You typically only need to modify these advanced settings if you are working with a support engineer or setting up more complicated configurations.

Field	Field description	Usage tips
Audio codecs from IP VCR	Restricts the IP VCR's choice of audio codecs to be used for receiving audio from the endpoints.	When communicating with an endpoint, the IP VCR receives a list of supported audio codecs from the endpoint. The IP VCR chooses an audio codec from those available, and sends audio data to the endpoint in that format.
Audio codecs to IP VCR	Which audio codecs the IP VCR advertises to remote endpoints, restricting the endpoints' choice of channels available for sending audio data to the IP VCR.	
Video codecs from IP VCR	Restricts the IP VCR's choice of video codecs to be used for receiving video from the endpoints.	When communicating with an endpoint, the IP VCR receives a list of supported video codecs from the endpoint. The IP VCR chooses a video codec from those available, and sends video data to the endpoint in that format.
Video codecs to IP VCR	Which video codecs the IP VCR advertises to remote endpoints, restricting the endpoints' choice of channels available for sending video data to the IP VCR.	
Video transmit size optimization	Allows the IP VCR to vary the resolution and codec of the video being sent to a remote endpoint within the video channel established to that endpoint. The options are: • *None*: Do not allow video size to be changed during transmission • *Dynamic resolution only*: Allow video size to be optimized during	With this option enabled, the IP VCR can, for instance, decide to send CIF video within a 4CIF channel if this will increase the viewed video quality. The circumstances under which decreasing the video resolution can improve the video quality include: if the original size of the viewed video is

Field	Field description	Usage tips
	transmission - *Dynamic codec and resolution*: Allow video size to be optimized during transmission and/or dynamic codec selection	smaller than the outgoing channel if the remote endpoint has used flow control commands to reduce the bandwidth of the IP VCR video transmission Typically, lowering the resolution means that the IP VCR can transmit video at a higher frame-rate.
Video resolution selection mode	This setting can be used to influence the choice of outgoing video resolution made by the IP VCR in certain circumstances. - *Default* The IP VCR will use its normal internal algorithms to dynamically decide which resolution to send in order to maximize the received video quality. - *Favor 448p* The IP VCR will heavily favor sending 448p or w448p video (resolutions of 576 x 448 and 768 x 448 pixels respectively) to those endpoints that are known to work best with these resolutions.	You should leave this at *Default* unless your environment dictates 448p or w448p resolutions only.
Video format	The video format used and transmitted by the IP VCR. - *NTSC - 30fps* The IP VCR will favor transmitting video at 30 frames per second, at SIF-like resolutions. - *PAL - 25fps* The IP VCR will favor transmitting video at 25 frames per second, at CIF-like resolutions.	NTSC is typically used in North America, while PAL is typically used in the UK and Europe. Setting this field to match the most common type of endpoint used with the IP VCR will improve the smoothness of the video sent by the IP VCR to the endpoints. Regardless of how this setting is configured, the IP VCR will accept video from endpoints at either frame-rate.
Maximum transmitted video packet size	The maximum payload size (in bytes) of the packets sent by the IP VCR for outgoing video streams (from the IP VCR to connected video endpoints).	Typically, you only need to set this value to lower than the default (1400 bytes) if there was a known packet size restriction in the path between the IP VCR and potential connected endpoints. Video streams generally contain packets of different lengths. This parameter only sets the *maximum* size of a transmitted network datagram. The IP VCR optimally splits the video stream into packets of this size or smaller. Thus, most transmitted packets will not reach this maximum size.
Interlaced video optimization	Whether the IP VCR restricts video resolutions in order to reduce the effect of interlacing artifacts.	You should only enable this option if you are seeing video interlacing artifacts or on the advice of Customer support. Note that all resolution restrictions imposed by this setting apply only to video being sent from endpoints to the IP VCR.
Video receive bit rate optimization	Enables the IP VCR to send bandwidth control messages to optimize the video bandwidth being used.	The IP VCR can send these messages to endpoints requesting that the bandwidth of the video that they are sending be decreased or increased, up to the maximum bandwidth of the channel.
Flow control on video errors	Enables the IP VCR to request that the endpoint send lower speed video if it fails to receive all the packets which comprise the far	The IP VCR can send these messages to endpoints requesting that the bandwidth of the video that they are sending be decreased

Field	Field description	Usage tips
	end's video stream.	based on the quality of video received by the IP VCR. If there is a bandwidth limitation in the path between the endpoint and the IP VCR, it is better for the IP VCR to receive every packet of a lower rate stream than to miss some packets of a higher rate stream.
Use recording or folder name as caller / called ID	When selected, the recording or folder name is used for the ID instead of the default device name.	When selected, the called ID for calls in to the IP VCR will be: the recording's name for calls directly to a recording for play back the default device name for calls to the (unnamed) root folder's auto attendant, recording ID or recording console ID the folder's configured name for calls to a (named) non-root folder's auto attendant, recording ID or recording console ID **Note:** When an endpoint calls the IP VCR to start a point-to-point recording, it will see the called ID as the remote device name rather than the IP VCR. When selected, the caller ID for calls from the IP VCR will be: • the recording's name when calling out to play back a recording • the specified recording name when calling out to make a new recording • the default device name when calling out to make a new recording in the root folder with no recording name specified • the folder's configured name when calling out to make a new recording in a non-root folder with no recording name specified With this setting is not selected, the caller/called ID is the name of the IP VCR.
Advertise out of band DTMF	If this option is selected, the IP VCR advertises the ability to receive out of band DTMF. If this option is selected, endpoints are allowed to send out of band DTMF. If this option is not selected, the IP VCR will not advertise the ability to accept out of band DTMF and endpoints will instead be forced to use in band DTMF.	Prior to release 3.0, the IP VCR always advertised to endpoints the ability to receive out of band DTMF tones. Now you can disable this functionality if required. If you clear this option, endpoints are forced to send DTMF in band (in the audio channel). This means that the IP VCR can pass DTMF tones on to an audio conferencing bridge.

Configuring gatekeeper settings

To configure gatekeeper settings, go to **Settings > H.323**.

You can configure the IP VCR to use a gatekeeper, which can make it easier for end-users to watch and make recordings using directory numbers rather than requiring them to know the IP address or host name of the IP VCR.

Note that recording IDs, recording console IDs, and auto attendant IDs are properties of folders (refer to Understanding the folders list) and can all be registered with the gatekeeper. To register these IDs with the gatekeeper, select **Register folder IDs**. For more information, refer to the following table.

In this section:

- Gatekeeper settings
- Gatekeeper status

Gatekeeper settings

Refer to this table for assistance configuring the gatekeeper settings. After making any configuration changes, click **Apply changes**.

Field	Field description	Usage tips
H.323 gatekeeper usage	Enables the IP VCR to use an H.323 gatekeeper for registration of numeric IDs of recordings, and for recording IDs, recording console IDs, and auto attendant IDs of folders.	When set to *Disabled* then no gatekeeper registrations are attempted (and existing registrations are torn down), regardless of other gatekeeper or per-recording settings. When set to *Enabled* registrations with the gatekeeper are attempted, and the gatekeeper is contacted for incoming and outgoing calls. If the gatekeeper does not respond, calls are still connected if possible. When set to *Required* registrations with the gatekeeper are attempted but calls are not connected if the gatekeeper cannot be contacted.
H.323 gatekeeper address	Identifies the network address of the gatekeeper to which IP VCR registrations should be made.	This can be specified either as a host name or as an IP address. This field will have no effect if **H.323 Gatekeeper usage** (see above) is set to *Disabled*. The gatekeeper can be either the built-in gatekeeper enabled on the **Gatekeeper** page (see Displaying the built-in gatekeeper registration list) or an external gatekeeper. To use the built-in gatekeeper enter "127.0.0.1". For an external gatekeeper, enter its host name or IP address.
Gatekeeper registration type	Controls how the IP VCR identifies itself when registering with its configured gatekeeper.	Cisco recommends that you use the *Terminal / gateway* option unless you are using a service prefix or point-to-point prefix (in this case, use *Gateway*). Only use a different option if you are: • having specific problems • using the Cisco Gatekeeper (with or without a service prefix), in which case use *Gateway (Cisco GK compatible)* • using the VCON MXM Gatekeeper (with or without a service prefix), in which case use *Gateway*

Field	Field description	Usage tips
		- In particular, if you are using the **Deregister recording prefixes when all recording ports are in use** setting (below), set the **Gatekeeper registration type** to *Gateway* (and on your gatekeeper, set gatekeeper call routing to "direct call" mode). Refer to the list of knoweldgebase articles in the Support section of the web site for more details about interoperability with gatekeepers.
Ethernet port association	Whether a call involves consultation with the configured gatekeeper also depends on the *Port A* and *Port B* settings. For all incoming calls, and outgoing calls dialed by address rather than by E.164 phone number, the gatekeeper is used to validate the connection only if the network port over which the connection is made is selected here.	
(Mandatory) H.323 ID to register	Specifies an identifier that the IP VCR can use to register itself with the H.323 gatekeeper.	Before the IP VCR can register any recordings with the H.323 gatekeeper, it must make a unit-wide/blade-wide registration. This field is required for gatekeeper registration. It will have no effect if **H.323 gatekeeper usage** is disabled.
Use password	If the configured gatekeeper required password authentication from registrants, select **Use password** and type in the password.	Note that where password authentication is used, the **(Mandatory) H.323 ID to register** will be used as the username.
Prefix for IP VCR registrations	Specifies an optional group of digits that can be used as a prefix in either (or both) of the following ways: - **use as prefix for registrations**: the numbers are added to the beginning of each recording's **Numeric ID** (or any of a folder's IDs) before registering it with the H.323 gatekeeper (you must have selected **register with H.323 gatekeeper** in the recording's settings). For example, if a recording has a numeric ID of "2222" and the registration prefix is "99", then the recording will be registered with the gatekeeper with a **gatekeeper ID** of "992222" - **register as a service prefix**: the numbers are used as a service prefix for the IP VCR on the gatekeeper. That means that any number beginning with the prefix will be directed to the IP VCR. Any numbers following the prefix will be identified by the IP VCR as a recording number (or folder ID). For example, if a recording has Numeric ID "3333" and the IP VCR has a service prefix of "99" registered with the gatekeeper, then a user dialing "993333" will be directed to that recording This setting does not affect point-to-point calls for which prefixes can be set on a per-folder basis (see Adding and updating folders).	Recordings registered with a gatekeeper have a unique number that can be entered from a video conferencing endpoint to connect directly to the recording. This eliminates the need for users to navigate the auto attendant or to know the IP address of the IP VCR. Folders registered with a gatekeeper have: - an auto attendant ID that can be entered from an endpoint to connect directly with the auto attendant of that folder - a recording console ID, that will start up the recording console - a recording ID that will cause the IP VCR to start a recording and place it in the folder associated with that recording ID **Using registration prefixes:** To usefully partition the dialing space, you might need to ensure that all recordings registered with a gatekeeper from a single IP VCR start with the same sequence of digits Using registration prefixes also can benefit large-scale dial plan changes. For example, you can change all IP VCR registrations to begin with "121" instead of "11" by changing a single IP VCR configuration field rather than individually amending every recording's associated gatekeeper ID If you want to use folder IDs in conjunction with a registration prefix, select **Register folder IDs** further down the page

Field	Field description	Usage tips
		Using service prefixes: By using a service prefix, the gatekeeper will automatically forward calls starting with the service prefix to the IP VCR. The IP VCR will determine whether the call matches a valid recording (in which case the recording will be played back), folder ID (in which case the call will be recorded into that folder) or an auto attendant ID (in which case the auto attendant is displayed). If no match is found, the default incoming call action will be applied (see Configuring global connection settings). You do not have to individually register recordings or folder IDs with the gatekeeper These settings will have no effect if **H.323 gatekeeper usage** is disabled.
Play back prefix	Specifies an optional extra prefix that the IP VCR should register with the H.323 gatekeeper specifically for play back.	See **Deregister play back prefix when all play back ports are in use** below.
Deregister recording prefixes when all recording ports are in use	When selected, configured recording prefixes (both the **Prefix for IP VCR registrations** if used as a service prefix and the **Point-to-point call incoming prefix** set for any folders) will be deregistered when all recording ports are in use on the IP VCR.	This setting is for use in load-balanced environments. By deregistering the recording prefixes of one IP VCR, the gatekeeper will contact another IP VCR that is registered with the same prefix(es), if necessary, when users call the prefix to make new recordings.
Deregister play back prefix when all play back ports are in use	When selected, the IP VCR will deregister the configured **Play back prefix** from the H.323 gatekeeper when all play back ports are in use.	This setting is for use in load-balanced environments. By deregistering the play back prefix of one IP VCR, the gatekeeper will contact another IP VCR that is registered with the same prefix, if necessary, when users call the prefix to play back a recording.
Register folder IDs	When selected IDs associated with all folders will be registered with the H.323 gatekeeper.	Folder IDs are configurable when you create or update a folder. For more information, refer to Understanding the folders list and Adding and updating folders. This setting does not apply to folders' configured **Point-to-point call incoming prefix** registrations.

Gatekeeper status

The IP VCR also displays brief status information about its registrations with the configured gatekeeper.

Field	Field description	Usage tips
H.323 gatekeeper status	Displays the IP address of the gatekeeper currently being used by the IP VCR.	This information might be useful if the gatekeeper has been specified with a host name rather than with an IP address. If the IP VCR has been unable to reach the configured gatekeeper and has instead registered with an alternate gatekeeper, the status displayed here is "registered with alternate gatekeeper <IP address>".
Registered address	Displays the local IP address and port number that the IP VCR has registered with the gatekeeper.	This information might be useful if the IP VCR has more than one IP address, for instance if both Ethernet interfaces are in use.
Alternate	Displays the number of 'alternate' gatekeepers	Where the configured gatekeeper has told the

Field	Field description	Usage tips
gatekeepers available	configured on the H.323 gatekeeper. This figure comes from the gatekeeper itself; if there are any 'alternate' gatekeepers configured, the gatekeeper tells the IP VCR their IP addresses.	IP VCR about any configured 'alternate' gatekeepers and if the IP VCR loses contact with the configured gatekeeper, the IP VCR will attempt to register with each of the 'alternates' in turn. If none of the 'alternate' gatekeepers responds, the IP VCR will report that the registration has failed. If the IP VCR successfully registers with an 'alternate' gatekeeper: • the **H.323 gatekeeper status** will indicate that registration is with an 'alternate' • the list of 'alternates' received from the new gatekeeper will replace the previous list • the IP VCR will only revert back to the original gatekeeper if the 'alternate' fails and only if the original gatekeeper is configured as an 'alternate' on the current gatekeeper's list of 'alternates' **Note:** If the IP VCR registers with an 'alternate' that does not itself supply a list of 'alternates', the IP VCR will retain the original list and if it loses contact with the current gatekeeper, each one will be attempted from the top again as before.
Number of active registrations	Displays the number of E.164 numbers plus H.323 IDs plus prefixes that the IP VCR has registered with the gatekeeper.	It also shows how many registrations are in progress but are not fully registered yet. Full information on the gatekeeper registrations being made by the IP VCR can be seen by clicking **details**; this takes you to the Active registrations page.
H.323 ID registration	Displays the identifier that the IP VCR has used to register itself with the H.323 gatekeeper.	For more information about the H.323 ID, refer to the table above.
Prefix for IP VCR registrations	Displays the prefix registered with the gatekeeper for all registrations from the IP VCR.	For more information about this prefix, refer to the table above.
Play back prefix	Displays the prefix registered with the gatekeeper for playing back stored recordings.	For more information about this prefix, refer to the table above.

Active registrations page

Click **details** (next to the **Number of active registrations** status field) to go to the **Active registrations** page. This page shows the complete set of IDs that the IP VCR is attempting to register with the configured H.323 gatekeeper, and includes the H.323 ID, prefixes, and specific E.164 number registrations for recordings and folders.

Filters

You can configure filters so that only specific registrations are shown in the list. This may help you to find a registration whose number or name you know if the list is very long. The filtered registration list is automatically updated when you change the ID and name filters; to stop filtering the list either delete the filters or click **Clear filters**. If both the ID filter and the name filter are defined, the registration list will show only those entries which match both filters.

Registration list

The registration list shows, for each registered ID, the type of that ID (H.323 ID, prefix or E.164 number), the object it relates to, and the status of that registration. If you want to modify or remove a specific registered ID, click on the link in its **Details** column to be taken to the relevant configuration page.

Displaying active gatekeeper registrations

To display a complete list of all IDs that the IP VCR is attempting to register with the configured H.323 gatekeeper, go to **Settings > H.323** and click **details**, shown next to the **Number of active registrations** status entry. You are taken to the **Active registrations** page. This page shows the complete set of IDs that the IP VCR is attempting to register with the configured H.323 gatekeeper, and includes the H.323 ID, prefixes, and specific E.164 number registrations.

Filters

You can configure filters so that only specific registrations are shown in the list. This may help you to find a registration whose number or name you know if the list is very long.

The filtered registration list is automatically updated when you change the ID and name filters; to stop filtering the list either delete the filters or click **Clear filters**. If both the ID filter and the name filter are defined, the registration list will show only those entries which match both filters.

Field	Field description	Usage tips
ID filter	Type the ID, or a part of the ID for which you want to see details.	The filtered registration list is automatically updated when you change the ID and name filters. Applying a filter will filter all registrations and display any that match, even if those registrations are not on the page currently displayed.
Details filter	Type the text, or a part of the text that will appear in the "Details" column of the Registrations table.	

Registration list

The registration list shows, for each registered ID, the type of that ID (H.323 ID, prefix or E.164 number), the object it relates to, and the status of that registration. If you want to modify or remove a specific registered ID, click on the link in its **Details** column to be taken to the relevant configuration page.

IP VCR gatekeeper registration behavior

This is a summary of the gatekeeper registration behavior on the IP VCR. It also explains how you can use a gatekeeper for load balancing.

Choice of registered IDs

With the exception of point-to-point prefixes (which are explained below), gatekeeper usage starts with configuring unique **Numeric ID**s for individual stored recordings and for folders. For each folder you can configure an **Auto attendant ID**, **Recording ID** and **Recording console ID** (together called folders IDs in this topic).

After configuring these IDs you can then:

- choose on a per-recording basis whether to register that recording's numeric ID individually with the gatekeeper using the **Numeric ID registration** field
- choose on a per-device basis whether to register folders' auto attendant, recording and recording console IDs individually with the gatekeeper using the **Register folder IDs** field
- for all recording and folder IDs, choose whether to add a specified prefix to those IDs when registering them individually with the gatekeeper using the **Prefix for IP VCR registrations** field with **use as prefix for registrations** selected.
- choose not to register recording or folder IDs individually with the gatekeeper but instead make them all available through one or more registered prefixes using the **Prefix for IP VCR registrations** field with **register as a service prefix** selected and the **Play back prefix** field. (With a prefix registered, then typically a gatekeeper will send all calls which start with the prefix to the device which registered the prefix)

You may need to use a prefix if:

- you want more than 100 IDs (recording or folder IDs) to be available through the gatekeeper. (The IP VCR has a limit of 100 individual dial strings that it is able to register with its configured gatekeeper)
- the number of IDs that you want to be available via the gatekeeper is less than 100 but more than the gatekeeper that you are using can support
- you want to load balance recording or play back functionality across multiple IP VCRs which register the same prefix(es). In this case you should configure these IP VCRs so that they deregister those prefixes when all recording ports are in use. See Load balancing below.

You may not be able to use a prefix if: your gatekeeper does not support prefixes - not all gatekeepers offer this functionality.

Matching incoming called numbers

A call can reach the IP VCR with a called ID number when:

- a user dials a number that the IP VCR has specifically registered with the gatekeeper
- a user dials a number that starts with a prefix that the IP VCR has registered with the gatekeeper
- a H.323 call is made directly to the IP VCR as a gateway and a subsidiary number is supplied.

When the IP VCR receives an incoming call involving a called ID, it decides what to do with the incoming call by following a number of rules in a specific order. If any of these rules provides a decision on what to do with the call, the process stops at that point and no further rules are tested. The rules in order are:

1. If the **Prefix for IP VCR registrations** has been configured and the called number starts with that prefix, then the IP VCR tries to match the rest of the called ID number (i.e. the part after the prefix) to a recording's **Numeric ID** or to one of the folder IDs.

2. If a **Play back prefix** has been configured and it matches the called number, then the IP VCR tries to match the rest of the called number (i.e. the part after the prefix) to a recording's **Numeric ID**.
3. The IP VCR tries to match the whole of the called number to a recording's **Numeric ID** or to one of the folder IDs.
4. The IP VCR tries to match the called number against a folder's configured **Point-to-point call incoming prefix**. In the event that more than one folder's **Point-to-point call incoming prefix** matches the called number, the IP VCR chooses the folder which gives the longest prefix match
5. The call is treated as a call to just the IP VCR's IP address and the configured **Default incoming call action** is followed.

Resulting action

If the above sequence results in a match against a recording's **Numeric ID**, then the recording is played back. If a folder's **Auto attendant ID** is matched, then the endpoint is connected to the auto attendant menu for that folder. If the call matches a folder's **Recording ID** or **Recording console ID**, the IP VCR starts a new recording in that folder (and starts up a recording console, if appropriate).

Which IDs are registered with the gatekeeper

Registering a recording's numeric ID

No individual registration will be made for a recording unless **H.323 gatekeeper** in the **Numeric ID registration** field is selected. In addition, if the recording is external (i.e. not stored on the IP VCR's own disk but accessed through a link to an external NFS server) the folder's **Register external recordings with gatekeeper** setting must be selected as well as the recording's own **H.323 gatekeeper** setting.

If the unit-wide/blade-wide **Prefix for IP VCR registrations** has not been configured, the IP VCR will register just the recording's **Numeric ID**. However, if the **Prefix for IP VCR registrations** has been configured and **Use as prefix for registrations** is selected, the IP VCR will prepend that prefix to the recording's **Numeric ID** before registering it with the gatekeeper.

Registering a folder's auto attendant ID, recording ID, and recording console ID

No folder IDs will be registered with the gatekeeper unless the unit-wide/blade-wide **Register folder IDs** setting is selected. If it is selected, then all configured **Auto attendant IDs**, **Recording IDs** and **Recording console IDs** for all folders will be registered with the gatekeeper.

If the **Prefix for IP VCR registrations** has been configured and **Use as prefix for registrations** selected for this field, then the IP VCR will prepend that prefix to all folders IDs before registering them with the gatekeeper.

Registering a folder's point-to-point prefixes

In normal operation, whenever a folder has a configured **Point-to-point call incoming prefix**, that prefix will be registered with the gatekeeper: there is no other unit-wide/blade-wide setting to enable or disable registration unlike the other folder IDs. However, see Load balancing below.

Load balancing

You can use prefixes to balance the load between a number of IP VCRs by registering them with the same prefixes and selecting the "deregister" options:

- the **Play back prefix** will be deregistered if the **Deregister play back prefix when all play back ports are in use** setting is selected and all play back ports are in use
- the **Point-to-point call incoming prefix** for all folders will be deregistered as will the **Prefix for IP VCR registrations** (if **register as a service prefix** is selected) if **Deregister recording prefixes when all recording ports are in use** is selected and all recording ports are in use.

When deregistration occurs, the gatekeeper will chose another IP VCR which is registered with the same prefix when a call comes in rather than rejecting it.

Configuration rules

One folder's **Point-to-point incoming prefix** can be the same as another folder's followed by some more digits; in this case the IP VCR will use the longest match to determine which folder to create a new point-to-point recording in. For example, if one folder uses the prefix "123" and another uses "1234", then calls to "12345" and "12346" will use the folder that registered "1234" and calls to "1235" and "1236" will use the folder associated with the prefix "123".

One folder's **Point-to-point incoming prefix** can be the same as a non-prefix ID; for example a recording can be registered as "1234" in addition to this being a folder's **Point-to-point incoming prefix**. In this case a call to "1234" will play back the recording, and a call to a number that starts with "1234" but has more than 4 digits will trigger a new point-to-point recording that will be stored in that folder.

A non-prefix ID can be the same as a folder's recording prefix plus some other digits. For example, you can have a recording registered as "1234" as well as a point-to-point incoming prefix "123" for a folder - the IP VCR always matches non-prefix IDs first; therefore a call to "1234" would go to the recording that had specifically registered this ID, whereas a call to "1235" or "1236" would start a point-to-point recording.

The following are not allowed:

- 2 identical non-prefix numeric IDs: all recordings' numeric IDs, folders' auto attendant, recording IDs and recording console IDs must be unique, and all must be different to the unit-wide/blade-wide H.323 ID
- 2 identical prefixes: all folders' **Point-to-point incoming prefix** must be unique and must all be different to the unit-wide/blade-wide **Play back prefix** and **Prefix for IP VCR registrations** (if **register as a service prefix** is selected)

Configuring SIP settings

A SIP call will select the audio and video codecs to use from the set of those both those allowed on the **Settings > Connections** page and supported by SIP (go to **Settings > SIP**), unless the call is with an endpoint configured with a *Custom codec* (refer to Configuring SIP endpoints for more information).

Refer to this table for assistance configuring the SIP settings. After making any configuration changes, click **Apply changes**.

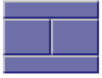
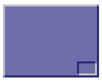
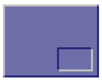
Field	Field description	Usage tips
SIP registrar settings		
SIP registrar usage	Enables the IP VCR to use a SIP registrar for registrations of numeric identifiers for its recordings.	When set to *Disabled,* then no SIP registrar registrations are attempted (and existing registrations are torn down), regardless of other settings. When set to *Enabled,* registrations with the registrar are attempted, and calls can be made through the registrar.
SIP registrar domain	Identifies the network address of the SIP registrar to which IP VCR registrations should be made.	This can be specified either as a host name or as an IP address. This field will have no effect if **SIP registration settings** is set to *No registration*.
SIP registrar type	Choose between: *Standard SIP*: for non-Microsoft SIP registrars *Microsoft OCS/LCS*: for Microsoft SIP registrars	Your choice is dependent on the type of SIP registrar you are using. This field will have no effect if **SIP registration settings** is set to *No registration*.
Username	The login name for the IP VCR on the SIP registrar.	You need to configure the SIP registrar with details of the devices that will register with it and create a login for each device. If you are using Microsoft OCS or LCS, you need to enter the full URI (for example, MCU@example.com).
Password	The password for the IP VCR on the SIP registrar.	You need to configure the SIP registrar with details of the devices that will register with it and create a login for each device. The password configured on this page needs to match the password in the SIP registrar. Note that this username will be used anywhere where one is required in a SIP call; for example, it will be used where authentication is required with a SIP server where no registrar is used.
ID registration for recordings	Allows recordings to be registered to the SIP registrar.	If selected, you can choose whether to register a particular recording by opening its recording information page and selecting *SIP registrar* in the **Numeric ID registration** field.
SIP call settings		
SIP proxy address	Identifies the network address of the SIP proxy.	If set, the proxy is used for all SIP calls, whether through a registrar or not.
Maximum bit rate from Microsoft OCS/LCS clients	Select a maximum bit rate to use from Microsoft OCS/LCS clients.	Microsoft OCS/LCS clients will try to use the maximum bit rate that the IP VCR advertises during the initial call setup. In most scenarios, you will not want OCS/LCS clients to use the **Default bandwidth from IP VCR** that is configured on the **Settings > Conferences** page (Configuring global conference settings).

Field	Field description	Usage tips
		Use this setting to select an appropriate bit rate for Microsoft OCS/LCS clients. *<limit disabled>* will cause the IP VCR to advertise the *Default bandwidth from IP VCR*.
Outgoing transport	Identifies the protocol to be used for call control messages for outgoing call connections.	If your SIP devices use TCP, select TCP as the outgoing transport. If your SIP devices use UDP, select UDP as the outgoing transport. The IP VCR can accept connections on TCP, UDP, and TLS providing those services are enabled on the **Network > Services** page (Configuring network services).
Use local certificate for outgoing connections and registrations	Select this option to force the IP VCR to present its local certificate when registering with the SIP registrar and when making outgoing TLS calls.	Often, the SIP registrar will not require the local certificate from the IP VCR. Only select this option if your environment dictates that the SIP registrar must receive the local certificate.

Configuring recording settings

You can customize a variety of the recording settings for the IP VCR to most closely fit your needs. To view and change the recording settings, choose **Settings > Recording**. When you have finished editing any of the fields, click **Apply changes** to make them take effect. Refer to the following table for a description of the different fields:

Recording settings

Field	Field description	Usage tips
Loop when playing back recordings via H.323/SIP	Select this option if you want recordings to automatically return to the start and continue playing when the end is reached during playback.	Even if this field is set, recordings will not loop while fast-forwarding. This setting applies only to playback by H.323 or SIP and not to streaming
Always send video to participants being recorded	If this option is selected, the IP VCR will always send video to any participants being recorded. If the recording console is not in use, the video sent to the remote system is blank.	When recording a conference on a remote MCU, if the IP VCR sends video to the far end as well as recording the video it receives, it may be the case that the video sent by the IP VCR ends up as part of the recorded conference in addition to the "real" participants in that conference. In theory, the IP VCR should not need to send video to an endpoint or MCU device that it is recording. However, some devices are programmed not to transmit video unless video is sent to them, and so this option allows the IP VCR to work with such systems.
Use date and time in new recording names	Select this option to have the date and time included in the names of new recordings.	Recording names are either entered by a user or automatically generated by the IP VCR. This option applies to names that the IP VCR has generated. Note that the IP VCR generates recording names from the name supplied by the recorded endpoint.
New recordings inherit folder's PIN	Select this option to have new recordings' PINs set to the same value as the PIN of the folder in which they are initially stored.	With this option clear, even if a folder has a PIN, any new recordings made into that folder will not automatically be assigned a PIN. With this option selected, users navigating to this folder via the Streaming-only interface or the auto-attendant will have to enter the PIN once to view the contents of the folder and again to watch a recording. However, with this option selected, users directly accessing recordings in this folder will only have to remember one PIN.
Point-to-point layout	Choose one of these layouts for making point-to-point recordings: Side-by-side  Loudest speaker with small picture-in-picture  Loudest speaker with large picture-in-picture 	Picture-in-picture views display the currently loudest speaker in a full-screen view, with the other displayed reduced in size in one corner. The speakers will exchange places depending on who is speaking.

Field	Field description	Usage tips
Multicast transmit IP address range	Use these fields to specify the range of multicast addresses to which the IP VCR can send multicast media for streaming.	If these values are not configured, the IP VCR is unable to stream recordings using multicast media. Multicast addresses are in the range 224.0.0.0 to 239.255.255.255 inclusive.
Multicast transmit port number range	Sets the range of port numbers to which multicast media will be sent.	This UDP port number range is used in conjunction with the **Multicast transmit IP address range**. You must set both the start and end port numbers to transmit recordings by multicast streaming.
Players allowed	Sets the media players that can be used for watching recordings.	This is a unit-wide/blade-wide setting that affects the options available to a user selecting to watch a recording.
Streaming protocol for Windows Media Player	Sets the protocol that Windows Media Player will use.	The default protocol for Windows Media Player is *HTTP*. Note that from v11 Windows Media Player no longer supports *MMS over UDP* or *MMS over TCP*.

Media settings

Field	Field description	Usage tips
Native media		
HD video capture mode	Enables the IP VCR to record video at up to HD quality. If you leave this option not selected, the IP VCR will record the video at up to SD quality only. Only enable this mode if you want to make HD recordings.	When **HD video capture mode** is selected, live streaming is automatically disabled. This is because HD video recordings cannot be live streamed on the IP VCR; HD recordings must be transcoded before they can be streamed. Note that this setting takes effect when a recording is started. If you change this setting, recordings in progress will use the setting with which they started. You can temporarily enable this mode for individual recordings if required. HD recordings cannot be played back on a video endpoint. You can, however, choose either to have all recordings transcoded to streaming media by selecting **Store streaming media** (below) or to transcode individual recordings to streaming media (refer to Viewing and updating recording details). Any SD recordings made while **HD video capture mode** is selected, can be played back on a video endpoint.
Streaming media		
Allow live streaming	Enables live streaming on the IP VCR. Live streaming is the streaming of video that is currently being recorded.	Note that live streaming is disabled if you have allowed the recording of HD video (see above). When live streaming is enabled, the IP VCR simultaneously records and transcodes to streaming media. However, the IP VCR will not store the transcoded media for streaming after the recording is complete; select **Store streaming media** if you require the streaming media to be stored.
Store streaming	This option controls the transcoding of new recordings to streaming media. It configures the IP VCR to transcode and store *every* new	With this option selected, new recordings are transcoded to streaming format.

Field	Field description	Usage tips
media	recording for streaming.	Recordings that start when **HD video capture mode** is selected are transcoded when the recording is complete. Streaming can take place when the transcoding is complete. Live streaming cannot be used with these recordings. Recordings made when **HD video capture mode** is not selected are simultaneously transcoded. Streaming can take place as soon as the recording is complete. Live streaming can be used with these recordings if you select **Allow live streaming**. Streaming media takes up extra space on the IP VCR. You might disable the creation of streaming formatted recordings if space has become short on the IP VCR. Note that where space has become short you might want to consider Storing recordings externally. Note that for every recording, on the recording's details page, there is a button that allows you to transcode the recording for streaming. There is also a button that deletes the streaming media for that recording.
Streaming recording video bit rate 1 **Streaming recording video bit rate 2**	When making recordings, as well as storing the incoming media packets as they are received, the IP VCR also re-encodes the media (using two different video bit rates) in a form suitable for *streaming* to users' desktop machines (see Using streaming to view recordings). These settings control which bit rates are used for the streaming video – typical usage would be to configure one low value suitable for users connecting over a low bandwidth link, and a higher value to give better quality to users with a faster network connection to the IP VCR.	Select the **Multicast** option next to one or both of the streaming recording settings to enable multicast streaming of "live" recordings (i.e. those in the process of being made). Note that you cannot use Windows Media Player to stream a conference in multicast mode. In addition to the video bit rates specified, streaming media includes an additional 64kbit/s audio stream; the total media rate, in bits per second, when streaming will thus be one of the specified video bit rates plus 64000.
Content channel recording bit rate	When recording content channel video, the IP VCR re-encodes the content stream to a form that can be served to users' desktop machines. This setting determines the bit rate of the recorded content channel streaming video.	This bit rate controls the rate at which content channel streaming video is *recorded*. Once a recording has been made, all later streaming of the content channel video will use the bit rate set at record time, so this value should not be so high as to exceed the available bandwidth between the IP VCR and potential streaming viewers.
Media export		
Allow MPEG1 export	Enables the downloading of recordings in MPEG1 format.	This option controls whether or not the "download MPEG file" link appears on a recording's details page.
MPEG1 export video bit rate	The IP VCR records raw media packets from H.323 video conferencing endpoints. It also provides the facility to export recordings in MPEG format (typically for download and playback on a PC), and this setting controls the video bit rate of such exported files. MPEG1 system stream files generated by the IP VCR comprise video plus 64kbit/s audio, and so the total media bit rate will be the specified video bit rate plus 64000.	A higher bit rate will give better quality, at the expense of generating larger download files; higher bit rate files will also take longer to be produced.

Configuring content settings

The content settings affect the behavior of the IP VCR with regard to H.239 and BFCP (Binary Floor Control Protocol).

H.239 is the protocol that allows for an additional video channel (known as the content channel) alongside the main video channel in a video-conferencing call that uses H.323; BFCP is a protocol that allows for an additional video channel (known as the content channel) alongside the main video channel in a video-conferencing call that uses SIP. For example, a conference participant may want to contribute a slide presentation from a laptop within a video conference.

For more information about content support in conferences, refer to Content channel video support.)

To access these settings, go to **Settings > Content**.

Refer to this table for assistance configuring the content settings. After making any changes, click **Apply changes**.

Field	Field description	Usage tips
Content status	Controls whether the IP VCR as a whole is permitted to use content.	If this setting is *Disabled*, no new recordings can use content, and it will not be possible to view existing recorded content during playing back. If this setting is *H.239 only*, no conference will be able to use BFCP content. Certain video conferencing endpoints and infrastructure such as gatekeepers may not operate correctly when communicating with equipment (such as the IP VCR) which declares content capability. Therefore it may be necessary to set this to *Disabled* in order to work with legacy devices (this will, of course, also prevent content video streams being used with H.239- or BFCP-aware equipment).
Playback content in main video channel	Whether the IP VCR will render recorded content channel video data in endpoints' main video channels when playing back recordings.	The IP VCR may not be able to open a separate content channel to an endpoint when playing back a recording that includes content channel video. For instance, the endpoint may have no H.239 capability, or the BFCP service is not enabled. In these cases, if this option is set to *Enabled*, the IP VCR will play back the recorded content video in the main video channel.

Adding a custom auto attendant banner

You can add a custom banner image to the auto attendant configured on the IP VCR as follows:

1. Go to **Settings > Banner**.
2. Set the banner up using the following table to determine the most appropriate settings.
3. Click **Update**.

Field	Field description	Usage tips
Auto attendant banner		
Default	Chooses the default IP VCR graphic to use for your banner.	
Specific to this auto attendant	The custom banner identified for this auto attendant. Click **Remove banner** to remove this graphic as the banner. Click **Update** after uploading a new graphic.	Nothing displays here until you upload the custom graphic as described below.
Banner upload		
Banner for this auto attendant	The custom graphic to be used for a banner. Click **Browse** to locate the file on your hard drive.	The image file can be a JPEG, GIF or Windows BMP format with a maximum size of 352 x 64 pixels.
Background color	Sets a custom background color. Enter the color values in each field. Click **Upload new file** to display.	

Configuring encryption settings

You can configure the IP VCR to record encrypted conferences on an MCU and encrypted calls from H.323 endpoints, and to encrypt the connection when playing back a recording to an H.323 endpoint.

Note: An encrypted recording can be later played back to an endpoint that is not capable of AES encryption, and conversely a non-encrypted recording can be played back on an encrypted connection at a later date.

The encryption technology that the IP VCR uses for encryption to and from H.323 endpoints is Advanced Encryption Standard (AES).

The encryption technology that the IP VCR uses for encryption to and from SIP endpoints is Secure Real-time Transport Protocol (SRTP).

To use encryption, you must have the Encryption feature key present on the IP VCR. For information about installing feature keys, refer to Upgrading the firmware. To access encryption settings, go to **Settings > Encryption**.

Refer to this table for assistance configuring the encryption settings. After making any configuration changes, click **Apply changes**.

Field	Field description	Usage tips
Encryption status	Whether the IP VCR is able to use encryption or not.	If you enable encryption, any connection to the IP VCR can either be encrypted or unencrypted. That is, the IP VCR advertises itself as being able to use encryption and will use encryption if required to do so by an endpoint. If you disable encryption, the IP VCR will not allow encryption for any connection.

Configuring security settings

To configure security settings, go to **Settings > Security**.

Field	Field description
Security settings	
Advanced account security mode	Advanced account security mode causes the IP VCR to hash passwords before storing them in the configuration.xml file (see below). Note that hashing user passwords is an irreversible process. Before you enable advanced account security mode, we recommend that you back up your configuration. The IP VCR gives you the option to do that after you have enabled advanced account security mode. If you enable advanced account security mode, all current passwords (created when the IP VCR was not in advanced account security mode) will expire and users must change them. Advanced account security mode is described in greater detail below.
Redirect HTTP requests to HTTPS	Enable this option to have HTTP requests to the IP VCR automatically redirected to HTTPS. This option is unavailable if either HTTP (**Web**) or HTTPS (**Secure web**) access is disabled on the **Network > Services** page.
Idle web session timeout	The timeout setting for idle web sessions. The user must log in again if the web session expires. The timeout value must be between 1 and 60 minutes. Note that status web pages that auto-refresh will keep a web session active indefinitely. You can configure the IP VCR not to auto-refresh those pages; to do so, go to **Settings > User interface** .
Serial console settings	
Hide log messages on console	The serial console interface displays log messages. If that is considered to be a security weakness in your environment, select this option to hide those messages.
Disable serial input during startup	Select this option for enhanced serial port security.
Require administrator login	Select this option to require an administrator login by anyone attempting to connect to the IP VCR via the console port. If this is not enabled, anyone with physical access to the MCU (or with access to your terminal server) can potentially enter commands on the serial console.
Idle console session timeout	If you have enabled **Require administrator login** , you can configure a session timeout period. The timeout setting for idle console sessions. The admin must log in again if the console session expires. The timeout value must be between 1 and 60 minutes.

Advanced account security mode

You can configure the IP VCR to use advanced account security mode. Advanced account security mode has the following features:

- The IP VCR will hash passwords before storing them in the configuration.xml file (see below)
- The IP VCR will demand that passwords fulfill certain criteria, using a mixture of alphanumeric and non-alphanumeric (special) characters (see below)
- Passwords will expire after 60 days
- A new password for an account must be different from the last ten passwords used with that account
- The IP VCR will disable a user's account if that user incorrectly enters a password three times consecutively. If this is an admin account, it is disabled for 30 minutes; for any other account, it is disabled indefinitely (or until you, the administrator, re-enable the account from the **Users** page)

- Non-administrator account holders are not allowed to change their password more than once in any 24 hour period
- Administrators can change any user account’s password and force any account to change its password by selecting **Force user to change password on next login** on the **Users** page. Administrators can prevent any non-administrator account from changing its password by selecting **Lock password** on the **Users** page.
- The IP VCR will disable any non-administrator account after a 30 day period of account inactivity. To re-enable the account, you must edit that account's settings on the **User** page

If you enable advanced security, all current passwords (created when the IP VCR was not in advanced account security mode) will expire and users must change them.

When using Advanced account security mode, we recommend that you rename the default administrator account. This is especially true where the IP VCR is connected to the public internet because security attacks will often use “admin” when attempting to access a device with a public IP address. Even on a secure network, if the default administrator account is “admin”, it is not inconceivable that innocent attempts to log into the IP VCR will cause you to be locked out for 30 minutes.

We recommend that you create several accounts with administrator privileges. This will mean that you will have an account through which you can access the IP VCR even if one administrator account has been locked out.

If there are API applications accessing the IP VCR, we recommend that you create dedicated administrator accounts for each application.

In advanced account security mode, if a user logs in with a correct but expired password the IP VCR asks that user to change the password. If the user chooses not to change it, that user is allowed two more login attempts to change the password before the account gets disabled.

Hashing passwords

In advanced account security mode, the IP VCR will hash passwords before storing them in the configuration.xml file. The configuration.xml file is used for backing up and restoring the configuration of the IP VCR (see Upgrading and backing up the IP VCR). If you do not select to use advanced password security, all user passwords are stored in plain text in the configuration.xml; this might be a security issue. If you select to use advanced password security, they will not be stored anywhere on the IP VCR in plain text; instead the passwords will be stored as hash sums. Note that hashing user passwords is an irreversible process.

Password format

In advanced account security mode, passwords must have:

- at least fifteen characters
- at least two uppercase alphabetic characters
- at least two lowercase alphabetic characters
- at least two numeric characters
- at least two non-alphanumeric (special) characters
- not more than two consecutive repeating characters. That is, two repeating characters are allowed, three are not

In advanced account security mode, a new password must be different to the previous 10 passwords that have been used with an account.

Expiring passwords

In advanced account security mode, if a user logs in with a correct but expired password the IP VCR asks that user to change the password. If the user chooses not to change it, that user is allowed two more login attempts to change the password before the account gets disabled.

Configuring network settings

To configure the network settings on the IP VCR and check the network status, go to **Network > Port A** or **Network > Port B**.

The IP VCR has two Ethernet interfaces, Port A and Port B. The configuration pages for the two interfaces look and behave similarly, and therefore are described together. Differences are noted as appropriate.

Port A can be configured to be allocated its IP address by DHCP. Port B cannot use DHCP. Connect Port A to your local network and connect Port B to a second subnet or the internet depending on your application of the IP VCR.

In this section:

- IP configuration settings
- IP status
- Ethernet configuration
- Ethernet status

IP configuration settings

These settings determine the IP configuration for the appropriate Ethernet port of the IP VCR. When you have finished, click **Update IP configuration** and then reboot the IP VCR.

Field	Field description	Usage tips
IPv4 configuration		
IP configuration	Specifies whether the port should be configured manually or automatically. If set to *Automatic via DHCP* the IP VCR obtains its own IP address for this port automatically via DHCP (Dynamic Host Configuration Protocol). If set to *Manual* the IP VCR will use the values that you specify in the Manual configuration fields below.	Click **Renew DHCP** to request a new IP address if you have selected automatic configuration. Port A should never be disabled because it is the primary interface of the IP VCR.
Manual configuration		
IP address	The dot-separated IPv4 address for this port, for example 192.168.4.45.	You only need to specify this option if you have chosen *Manual* IP configuration, as described above. For Port A, if the IP configuration setting is set to *Automatic by DHCP* this setting is ignored.
Subnet mask	The subnet mask required for the IP address you want to use, for example 255.255.255.0	
Default gateway	The IP address of the default gateway on this subnet, for example 192.168.4.1	
DNS configuration		
Host name	Specifies a name for the IP VCR.	Depending on your network configuration, you may be able to use this host name to communicate with the IP VCR, without needing to know its IP address.
DNS configuration	Specifies whether DNS should be configured manually or automatically. If set to *Manual* the IP VCR will use the values that you specify in the three configuration fields below.	
Name server	The IP address of the name server.	

Field	Field description	Usage tips
Secondary name server	Identifies an optional second name server.	The secondary DNS server is only used if the first is unavailable. If the first returns that it does not know an address, the secondary DNS server will not be queried.
Domain name (DNS suffix)	Specifies an optional suffix to add when performing DNS lookups.	This can allow you to use non-fully qualified host names when referring to a device by host name instead of IP address. For example, if the domain name is set to *cisco.com*, then a request to the name server to look up the IP address of host *endpoint* will actually lookup *endpoint.cisco.com*.

IP status

Use the IP status fields to verify the current IP settings for the appropriate Ethernet port of the IP VCR, which were obtained using DHCP or configured manually (see IP configuration settings) including:

- Host name
- DHCP
- IP address
- Subnet mask
- Default gateway
- Name server
- Secondary name server
- Domain name (DNS suffix)

Ethernet configuration

These settings determine the Ethernet settings for the appropriate port of the IP VCR. Refer to the table for assistance with these settings. When you have finished, click **Update Ethernet configuration**.

Field	Field description	Usage tips
Ethernet settings	Specify whether you want this Ethernet port to automatically negotiate its Ethernet settings with the device it is connected to, or if it should use the values that you specify in the Manual configuration fields below.	It is important that your Ethernet settings match those of the device to which this port is connected. For example, both devices must be configured to use automatic negotiation, or both configured with fixed and matching speed and duplex settings (see below).
Manual configuration		
Speed	Identifies the connection speed: *10 Mbit/s* or *100 Mbit/s*. Use automatic negotiation if a connection speed of *1000 Mbit/s* is required.	The connection speed must match that of the device to which this port is connected. You only need to select this option if you have chosen *Manual* Ethernet settings, as described above.
Duplex	Identifies the connection duplex mode: *Full duplex* Both devices can send data to each other at the same time *Half duplex* Only one device can send to the other at a time	The duplex setting must match that of the device to which this port is connected. You only need to select this option if you have chosen *Manual* Ethernet settings, as described above.

Ethernet status

Field	Field description	Usage tips
Link status	Indicates whether this Ethernet port is connected to or disconnected from the network.	
Speed	The speed (*10*/*100*/*1000 Mbit/s*) of the network connection to the IP VCR on this port.	This value is negotiated with the device to which this port is connected or based on your Manual configuration selected above.
Duplex	The duplex mode (*Full duplex* or *Half duplex*) of the network connection to this port.	This value is negotiated with the device to which this port is connected or based on your Manual configuration selected above.
MAC address	The fixed hardware MAC (Media Access Control) address of this port.	This value cannot be changed and is for information only.
Packets sent	Displays a count of the total number of packets sent from this port by the IP VCR. This includes all TCP and UDP traffic.	When troubleshooting connectivity issues, this information can help you confirm that the IP VCR is transmitting packets into the network.
Packets received	Displays a count of the total number of packets received by this port of the IP VCR. This includes all TCP and UDP traffic.	When troubleshooting connectivity issues, this information can help you confirm that the IP VCR is receiving packets from the network.
Statistics:	These fields display further statistics for this port. • Multicast packets sent • Multicast packets received • Total bytes sent • Total bytes received • Receive queue drops • Collisions • Transmit errors • Receive errors	Use these fields for advanced network diagnostics, such as resolution of problems with Ethernet link speed and duplex negotiation.

Configuring IP routes settings

You need to set up one or more routing settings to control how IP traffic flows in and out of the IP VCR.

It is important that these settings are configured correctly, or you may be unable to make calls or access the web interface.

To configure the route settings, go to **Network > Routes**.

In this section:

- Port preferences
- IP routes configuration
- Current IP status

Port preferences

If both Ethernet ports are enabled, it is necessary to specify which port is used in certain special circumstances. Make the appropriate selections described below. Click **Apply changes**.

Field	Field description	Usage tips
IPv4 gateway preference	The IP address to which the IP VCR will send packets in the absence of more specific routing (see IP routes configuration). Therefore, it only makes sense to have precisely one default gateway, even though *different* default gateways may have been configured for Ports A and B. Use this option to decide which port's default gateway configuration to use as the IP VCR's default gateway.	If Ethernet Port B is disabled, you cannot specify that port as the default gateway preference. Selecting Port B as default gateway preference then disabling Port B will cause the preference to revert to Port A.
Name server (DNS) preference	The IP address to which the IP VCR will send requests to look up unrecognized host names in order to determine their corresponding IP addresses. Only one name server (and associated secondary name server) can be used, even though *different* name servers can have been configured for Ports A and B. Use this option to decide which port's name server configuration to use as the IP VCR's name server.	If Ethernet Port B is disabled, you cannot specify that port as the name server preference. Selecting Port B as name server preference then disabling Port B will cause the preference to revert to Port A.

IP routes configuration

In this section you can control how IP packets should be directed out of the IP VCR. You should only change this configuration if you have a good understanding of the topology of the network(s) to which the IP VCR is connected.

Configuration of routes is divided into two sections: addition of new routes, and the display and removal of existing routes.

Adding a new IP route

To add a new route, enter the details using the following table for reference. Click **Add IP route** to make the addition. If the route already exists, or aliases (overlaps) an existing route, you are prompted to correct the problem and try again.

Field	Field description	Usage tips

Field	Field description	Usage tips
IP address / mask length	Use these fields to define the type of IP addresses to which this route applies. The IP address pattern must be in the dot-separated IPv4 format, while the mask length is chosen in the **IP address / mask length** field. The mask field specifies how many bits of the address are fixed; unfixed bits must be set to zero in the address specified.	To route all IP addresses in the range 192.168.4.128 to 192.168.4.255 for example, specify the IP address as 192.168.4.128 and the mask length as 25, to indicate that all but the last seven bits address are fixed.
Route	Use this field to control how packets destined for addresses matching the specified pattern are routed.	You can select *Port A*, *Port B* or *Gateway*. If *Gateway* is selected, specify the IP address of the gateway to which you want packets to be directed. Selecting *Port A* results in matching packets being routed to Port A's default gateway (see Configuring network settings). Selecting *Port B* will cause matching packets to be routed to Port B's default gateway. If Ethernet Port B is disabled, the option to route packets to Port B is disabled.

Viewing and deleting existing IP routes

Configured routes are listed below the **Add IP route** section. For each route, the following details are shown:

- The IP address pattern and mask
- Where matching packets will be routed, with the possibilities being:
  - *Port A* - meaning the default gateway configured for Port A
  - *Port B* - meaning the default gateway configured for Port B
  - *<IP address>* - a specific address has been chosen
- Whether the route has been configured automatically as a consequence of other settings, or added by the user as described above.

The *default* route is configured automatically in correspondence with the **Default gateway preference** field (see Port preferences) and cannot be deleted. Any packets not covered by manually configured routes will be routed according to this route.

Manually configured routes can be deleted by selecting the appropriate check box(es) and clicking **Delete selected**.

Routes behavior with disabled ports

If the default gateway preference is set to Port B and that port is disabled, the default route is updated automatically to route packets not covered by any manually configured route via Port A.

If a manually configured route specifies Port B and that port is disabled, packets matching that route **will not** be automatically routed via Port A, but discarded. You should take care to avoid this situation.

Current IP status

This table shows the current default gateway and name server(s) for Ethernet Ports A and B. No fields can be changed, and are provided for reference when configuring the other parameters described in the sections above.

Configuring IP services

To configure IP services, go to **Network > Services**.

Use this page to control the type of services that can be accessed via Ethernet Ports A and B. For example, if one Ethernet port is connected to a network outside your organization's firewall, and you want to restrict the level of access that external users are entitled to, for example, by disabling FTP access via Port B.

Refer to the following table for more details.

In addition to controlling the Ethernet interfaces over which a service operates, this page also allows an administrator to specify the port number on which that service is provided. If the port number for a service is changed, it is necessary to ensure that the new value chosen does not clash with the port number used by any of the other services; it is not, however, normally necessary to use anything other than the pre-configured default values.

Note that by default SNMP Traps are sent to port UDP port 162 (on the destination network management station); this is configurable. For more information, refer to Configuring SNMP settings.

To reset all values back to their factory default settings, click **Reset to default** and then click **Apply changes**.

Field	Field description	Usage tips
TCP service		
Web	Enable/disable web access on the specified interface or change the port that is used for this service.	Web access is required to view and change the IP VCR web pages and read online help files. If you disable web access on both Ports A and B you will need to use the serial console interface to re-enable it. Note that QuickTime uses RTSP by default which is listed as **Streaming (other)** on the **Network > Services** page. However, the QuickTime player can be configured to use HTTP (that is it will come from the web service port) instead. If a port is disabled, this option is unavailable.
Secure web	Enable/disable secure (HTTPS) web access on the specified interface or change the port that is used for this service.	This field is only visible if the IP VCR has the *Secure management (HTTPS)* feature key or an *Encryption* feature key installed. For more information about installing feature keys, refer to Upgrading and backing up the IP VCR. By default, the IP VCR has its own SSL certificate and private key. However, you can upload a new private key and certificates if required. For more information about SSL certificates, refer to Configuring SSL certificates. If a port is disabled, this option is unavailable.
Incoming H.323	Enable/disable the ability to receive incoming calls to the IP VCR using H.323 or change the port that is used for this service.	Disabling this option will not prevent outgoing calls to H.323 devices being made by the IP VCR. That is, the IP VCR will need to dial out to conference participants who are using H.323. If a port is disabled, this option is unavailable.
SIP (TCP)	Allow/reject calls to the IP VCR using SIP over TCP or change the port that is used for this service.	Disabling this option will not prevent outgoing calls to SIP devices being made by the IP VCR. That is, the IP VCR will need to dial out to conference participants who are using SIP over TCP.

Field	Field description	Usage tips
		If a port is disabled, this option is unavailable.
Encrypted SIP (TLS)	Allow/reject encrypted SIP calls to the IP VCR using SIP over TLS or change the port that is used for this service.	Disabling this option will not prevent outgoing calls to SIP devices being made by the IP VCR. If a port is disabled, this option is unavailable.
Streaming (Windows Media Player)	Allow/disable streaming from the IP VCR to Windows Media Player or change the port that is used for this service.	If a port is disabled, this option is unavailable.
Streaming (other)	Allow/disable RTSP (Real Time Streaming Protocol) streaming from the IP VCR to QuickTime or RealPlayer or change the port that is used for this service.	If a port is disabled, this option is unavailable.
FTP	Enable/disable FTP access on the specified interface or change the port that is used for this service.	FTP can be used to upload and download recordings, and IP VCR configuration. You should consider disabling FTP access on any port that is outside your organization's firewall. If you require advanced security for the IP VCR, disable FTP access. If a port is disabled, this option is unavailable.
UDP service		
SNMP	Enable/disable the receiving of the SNMP protocol on this port or change the port that is used for this service.	If a port is disabled, this option is unavailable. You must use the same port number for both Port A and Port B. The number is automatically refreshed for Port B. You cannot change the Port B UDP port numbers and they are always grayed-out; if you want to enable the receiving of the SNMP protocol on Port B, ensure that you have the video firewall as an activated feature (refer to Upgrading and backing up the IP VCR) and that you have selected the check box for SNMP on Port B. Note that by default SNMP Traps are sent to port UDP port 162 (on the destination network management station); this is configurable. For more information, refer to Configuring SNMP settings. If you require advanced security for the IP VCR, disable the SNMP service.
SIP (UDP)	Allow/reject incoming and outgoing calls to the IP VCR using SIP over UDP or change the port that is used for this service.	Disabling this option will prevent calls using SIP over UDP. If a port is disabled, this option is unavailable. You must use the same port number for both Port A and Port B. The number is automatically refreshed for Port B. You cannot change the Port B UDP port numbers and they are always grayed-out; if you want to allow incoming and outgoing SIP (UDP) calls on Port B, ensure that you have the video firewall as an activated feature (refer to Upgrading and backing up the IP VCR) and you have selected the check box for SIP (UDP) on Port B.
H.323 gatekeeper	Enable/disable access to the built-in H.323 gatekeeper or change the port that is used for the built-in H.323 gatekeeper.	If a port is disabled, this option is unavailable. You must use the same port number for both Port A and Port B. The number is automatically refreshed for Port B. You cannot change the

Field	Field description	Usage tips
		Port B UDP port numbers and they are always grayed-out; if you want to open Port B for the H.323 gatekeeper, ensure that you have the video firewall as an activated feature (refer to Upgrading and backing up the IP VCR) and you have selected the check box for H.323 gatekeeper on Port B.

Configuring SNMP settings

To configure monitoring using SNMP, go to **Network > SNMP**.

The IP VCR sends out an SNMP trap when the device is shut down or started up. The SMNP page allows you to set various parameters; when you are satisfied with the settings, click **Update SNMP settings**.

Note:

- The 'system up time' that appears in the trap is the time since SNMP was initialized on the IP VCR (and therefore will differ from the **Up time** reported by the IP VCR on the **Status > General** page).
- The SNMP MIBs are read-only.

System information

Field	Field description	Usage tips
Name	Identifies the IP VCR in the SNMP system MIB.	Usually you would give every device a unique name. The default setting is *IP VCR*.
Location	The location that appears in the system MIB.	An optional field. It is useful where you have more than one IP VCR to identify where the IP VCR is located. The default setting is *Unknown*
Contact	The contact details that appear in the system MIB.	An optional field. The default setting is *Unknown* Add the administrator's email address or name to identify who to contact when there is a problem with the device. If SNMP is enabled for a port on the public network, take care with the details you provide here.
Description	A description that appears in the system MIB.	An optional field, by default this will indicate the model number of the IP VCR. Can be used to provide more information on the IP VCR.

Configured trap receivers

Field	Field description	Usage tips
Enable traps	Select to enable the IP VCR to send traps.	If you do not select this check box, no traps will be sent.
Enable authentication failure trap	Select to enable authentication failure traps.	You cannot select this check box unless you have selected to **Enable traps** above. Authentication failure traps are generated and sent to the trap receivers when someone tries to read or write a MIB value with an incorrect community string.
Trap receiver addresses 1 to 4	Enter the IP address or hostname for up to four devices that will receive both the general and the authentication failure traps.	The traps that are sent by the IP VCR are all SNMP v1 traps. You can configure trap receivers or you can view the MIB using a MIB browser. You can set the UDP port number for the trap in the format <IP address>: <port number>. By default the UDP port number is 162.

Access control

Field	Field description	Usage tips
RO community	Community string/password that gives read-only access to all trap information.	Note that SNMP community strings are not secure. They are sent in plain text across the network. It is advisable to change the community strings before enabling SNMP as the defaults are well known.
RW community	Community string/password that gives read/write access to all trap information.	
Trap community	Community string/password that is sent with all traps.	Some trap receivers can filter on trap community.

Configuring QoS settings

To configure Quality of Service (QoS) on the IP VCR for audio and video, go to **Network > QoS**.

QoS is a term that refers to a network's ability to customize the treatment of specific classes of data. For example, QoS can be used to prioritize audio transmissions and video transmissions over HTTP traffic. These settings affect all audio and video packets to H.323 and SIP endpoints, and to streaming viewers. All other packets are sent with a QoS of 0.

The IP VCR allows you to set six bits that can be interpreted by networks as either Type of Service (ToS) or Differentiated Services (DiffServ).

Note: Do not alter the QoS settings unless you need to do so.

To configure the QoS settings you need to enter a six bit binary value.

Further information about QoS, including values for ToS and DiffServ, can be found in the following RFCs, available on the Internet Engineering Task Force web site www.ietf.org:

- RFC 791
- RFC 2474
- RFC 2597
- RFC 3246

In this section:

- About QoS configuration settings
- ToS configuration
- DiffServ configuration
- Default settings

About QoS configuration settings

The following table describes the settings on the **Network > QoS** page.

Click **Update QoS settings** after making any changes.

Field	Field description	Usage tips
Audio	Six bit binary field for prioritizing audio data packets on the network.	Do not alter this setting unless you need to.
Video	Six bit binary field for prioritizing video data packets on the network.	Do not alter this setting unless you need to.

ToS configuration

ToS configuration represents a tradeoff between the abstract parameters of precedence, delay, throughput, and reliability.

ToS uses six out of a possible eight bits. The IP VCR allows you to set bits 0 to 5, and will place zeros for bits 6 and 7.

- Bits 0-2 set IP precedence (the priority of the packet).
- Bit 3 sets delay: 0 = normal delay, 1 = low delay.
- Bit 4 sets throughput: 0 = normal throughput, 1 = high throughput.
- Bit 5 sets reliability: 0 = normal reliability, 1 = high reliability.
- Bits 6-7 are reserved for future use and cannot be set using the IP VCR interface.

You need to create a balance by assigning priority to audio and video packets whilst not causing undue delay to other packets on the network. For example, do not set every value to 1.

DiffServ configuration

DiffServ uses six out of a possible eight bits to set a codepoint. (There are 64 possible codepoints.) The IP VCR allows you to set bits 0 to 5, and will place zeros for bits 6 and 7. The codepoint is interpreted by DiffServ nodes to determine how the packet is treated.

Default settings

The default settings for QoS are:

- *Audio 101110*:
  - For ToS, this means IP precedence is set to 5 giving relatively high priority. Delay is set to low, throughput is set to high, and reliability is set to normal.
  - For Diff Serv, this means expedited forwarding.
- *Video 100010*:
  - For ToS, this means IP precedence is set to 4 giving quite high priority (but not quite as high as the audio precedence). Delay is set to normal, throughput is set to high, and reliability is set to normal.
  - For DiffServ, this means assured forwarding (codepoint 41).

To return the settings to the default settings, click **Reset to default**.

Displaying and resetting system time

The system date and time for the IP VCR can be set manually or using the Network Time Protocol (NTP).

To configure Time settings, go to **Settings > Time**.

System time

The current system date and time is displayed.

If you do not have NTP enabled and need to update the system date and/or time manually, type the new values and click **Change system time**.

NTP

The IP VCR supports the NTP protocol. If you are using it, configure the settings as required, and then click **Update NTP settings**.

The IP VCR re-synchronizes with the NTP server via NTP every hour.

If there is a firewall between the IP VCR and the NTP server, configure the firewall to allow NTP traffic to UDP port 123.

If the NTP server is local to Port A or Port B then the IP VCR will automatically use the appropriate port to communicate with the NTP server. If the NTP server is not local, the IP VCR will use the port that is configured as the default gateway to communicate with the NTP server, unless a specific IP route to the NTP server's network/IP address is specified. To configure the default gateway or an IP route, go to **Network > Routes**.

Port A and B must be configured on different subnets

Field	Field description	Usage tips
Enable NTP	If selected, the IP VCR uses the NTP protocol.	
UTC offset	The offset of the time zone that you are in from Greenwich Mean Time.	You must update the offset manually when the clocks go backwards or forwards: the IP VCR does not adjust for daylight saving automatically.
NTP host	The IP address of the server that is acting as the time keeper for the network.	

Using NTP over NAT (Network Address Translation)

If NAT is used between the IP VCR and the NTP server, with the IP VCR on the NAT's local network (and not the NTP server), no extra configuration is required.

If NAT is used between the IP VCR and the NTP server, with the NTP server on the NAT's local network, then configure the NAT forwarding table to forward all data to UDP port 123 to the NTP server.

Upgrading and backing up the IP VCR

In this section:

Upgrading the main IP VCR software image

The main IP VCR software image is the only firmware component that you will need to upgrade.

To upgrade the main IP VCR software image:

1. Go to **Settings > Upgrade**.
2. Note the **Current version** of the main software image to verify the currently installed version.
3. Log onto the support pages to identify whether a more recent image is available.
4. Download the latest available image and save it to a local hard drive.
5. Unzip the image file.
6. Log on to the IP VCR web browser interface.
7. Go to **Settings > Upgrade**.
8. Click **Browse** to locate the unzipped file on your hard drive.
9. Click **Upload software image**. The browser begins uploading the file to the IP VCR, and a new browser window opens to indicate the progress of the upload. When finished, the browser window refreshes and indicates that the "Main image upgrade completed".
10. The upgrade status displays in the **IP VCR software upgrade status** field.
11. Shutting down and restarting the IP VCR.

Upgrading the loader software image

Upgrades for the loader software image are not typically available as often as upgrades to the main software image.

To upgrade the loader software image:

1. Go to **Settings > Upgrade**.
2. Select the **Current version** of the loader software to verify the currently installed version.
3. Go to the software download pages of the web site to identify whether a more recent image is available.
4. Download the latest available image and save it to a local hard drive.
5. Unzip the image file.
6. Click **Browse** to locate the unzipped file on your hard drive.
7. Click **Upload software image**. The browser begins uploading the file to the IP VCR, and a new browser window opens to indicate the progress of the upload. When finished, the browser window refreshes and indicates that the "Loader image upgrade completed."
8. The upgrade status displays in the **Loader upgrade status** field.
9. Shutting down and restarting the IP VCR.

Backing up and restoring the configuration

The Backup and restore section of the **Upgrade** (**Settings > Upgrade**) page allows you to back up and restore the configuration of the IP VCR using the web interface. This enables you to either go back to a previous configuration after making changes or to effectively "clone" one unit as another by copying its configuration.

To back up the configuration, click **Save backup file** and save the resulting "configuration.xml" file to a secure location.

To restore configuration at a later date, locate a previously-saved "configuration.xml" file and click **Restore backup file**. When restoring a new configuration file to an IP VCR you can control which parts of the configuration are overwritten:

- If you select **Network settings**, the network configuration is overwritten with the network settings in the supplied file. Typically, you would only select this check box if you were restoring from a file backed up from the same IP VCR or if you were intending to replace an out of service IP VCR. If you copy the network settings from a different, active, IP VCR and there is a clash (for instance, both are now configured to use the same fixed IP address) one or both IP VCRs may become unreachable via IP. If you do not select **Network settings**, the restore operation will not overwrite the existing network settings, with the one exception of the QoS settings. QoS settings are overwritten regardless of the **Network settings**.
- If you select **User settings**, the current user accounts and passwords are overwritten with those in the supplied file. If you overwrite the user settings and there is no user account in the restored file corresponding to your current login, you need to log in again after the file has been uploaded.

By default, the overwrite controls are not selected, and therefore the existing network settings and user accounts are preserved.

Note that you can also backup and restore the configuration of the IP VCR using FTP. For more information, refer to Backing up and restoring the configuration using FTP.

Enabling IP VCR features

The IP VCR requires activation before most of its features can be used. (If the IP VCR has not been activated, the banner at the top of the web interface will show a prominent warning; in every other respect the web interface will look and behave normally.)

Advanced IP VCR features (such as *Video Firewall*) are not enabled as standard, and require additional activation. For information about configuring the video firewall, refer to the Knowledge Base section in the support pages of the web site.

If this is a new IP VCR you should receive the IP VCR already activated; if it is not, and you have upgraded to a newer firmware version, or you are enabling a new feature, you contact your supplier to obtain an appropriate activation code. Activation codes are unique to a particular IP VCR so ensure that you know the unit's/blade's serial number such that you receive a code appropriate to your IP VCR.

Regardless of whether you are activating the IP VCR or enabling an advanced feature, the process is the same.

To activate the IP VCR or enable an advanced feature:

1. Select the **Activated features** (IP VCR activation is shown in this same list) to confirm that the feature you require is not already activated.
2. Enter the new feature code into the **Activation code** field exactly as you received it, including any dashes.
3. Click **Update features**. The browser window should refresh and list the newly activated feature, showing the activation code beside it. Activation codes may be time-limited. If this is the case, an expiry date is displayed, or a warning that the feature has already expired. Expired activation codes remain listed, but the corresponding feature will not be activated. If the activation code is not valid, you are prompted to re-enter it.

4. Cisco recommends that you record the activation code in case you need to re-enter it in the future.

Successful IP VCR or feature activation has immediate effect and will persist even if the IP VCR is restarted.

Note that you can remove some IP VCR feature keys by clicking the **Remove** link next to the feature key in this page.

Shutting down and restarting the IP VCR

It is sometimes necessary to shut down the IP VCR, generally to restart as part of an upgrade (see Upgrading and backing up the IP VCR). You should also shut down the IP VCR before intentionally removing power from it.

Shutting down the IP VCR will cause all playbacks to finish, allows the IP VCR to ensure that all recordings are cleanly ended and stored, and disconnects all recording and playback H.323 connections. In addition, the hard disk in the IP VCR is shut down safely - this is important to ensure the integrity of stored recordings. You lose network connectivity with the IP VCR for a few minutes while you restart the unit.

To shut down the IP VCR:

1. Go to **Settings > Shutdown**.
2. Click **Shut down VCR**.
3. Confirmation of shutdown is required; the button changes to **Confirm VCR shutdown**.
4. Click again to confirm.

   The IP VCR begins to shut down. The banner at the top of the page changes to indicate this.

   When the shutdown is complete, the button changes to **Restart VCR**.
5. Click this button a final time to restart the VCR.

Displaying general status

The **General status** page displays an overview of the IP VCR status. To access this information, go to **Status > General.**

Refer to the following table for details of the information displayed

Field	Field Description
System status	
Model	The specific IP VCR model.
Serial number	The unique serial number of the IP VCR.
Software version	The installed software version. You will need to provide this information when speaking to Customer support.
Build	The build version of installed software. You will need to provide this information when speaking to Customer support.
Uptime	The time since the last restart of the IP VCR.
Host name	The host name assigned to the IP VCR.
IP address	The IP address assigned to the IP VCR.
CPU load	The current processor utilization of the IP VCR.
Media processing load	An overview of the current media loading of the IP VCR.
System time	
Current time	The system time on the IP VCR. Click **New time** to modify this value. The **Time Settings** page opens in which you can update the system date and time manually or refresh the time from an NTP server. For more information about the **Time Settings** page, refer to Displaying and resetting system time.
System log	
User requested shutdown User requested upgrade Unknown	The system log displays the last eight shutdown and upgrade events in date order with the most recent system log event at the top of the list. The log will also display *unknown* if there has been an unexpected reboot or power failure, which you should report to Customer support if it happens repeatedly.
Diagnostic information	
Download diagnostic information	If required to do so by Customer support, click **Download diagnostic information** to save a set of diagnostic files.

Displaying recording status

The Recording status displays the status of stored recordings and recordings being played back. To access this information, go to **Status > Recording.**

Many of the fields show the current value, the highest value attained (in parentheses), and the maximum value . To reset to the maximum values, click **Reset maximum values**.

Refer to the following table for assistance in interpreting the information displayed.

Field	Field Description
Number of folders	The number of folders currently on the IP VCR.
Number of recordings	The total number of recordings accessible by the IP VCR. This includes recordings made using the IP VCR, those uploaded to it and those stored externally on an NFS server.
Number of internal recordings	The number of recordings currently stored internally on the IP VCR. This includes recordings made using the IP VCR as well as those uploaded to it.(The figure excludes recordings stored externally.)
Number of recordings in progress	The number of recordings that are currently being made.
Number of H.323 /SIP playbacks in progress	The number of people currently watching stored recordings using an H.323 endpoint. This includes auto attendant connections which are showing a preview of a recording.
Number of UDP and TCP streaming sessions in progress	The number of people currently watching stored or live recordings using conventional streaming via a streaming application such as Apple QuickTime or RealPlayer. The maximum number of streaming sessions can only be reached for the streaming of live recordings. For the streaming of stored recordings, the maximum number might be less.
Number of TCP streaming sessions in progress	The number of people currently watching stored or live recordings using streaming over TCP. The maximum number of streaming sessions can only be reached for the streaming of live recordings. For the streaming of stored recordings, the maximum number might be less.
Number of recording uploads in progress	The number of recordings currently being uploaded to the IP VCR for later playback.
Number of downloads in progress	The number of recordings that are currently being downloaded from the IP VCR.
Number of completed playbacks	The number of people who were once watching stored recordings but are now not. Includes all types of playback, including streaming and playback using an H.323 endpoint
Number of completed downloads	The number of recordings that have been downloaded from the IP VCR.
Number of completed recordings	The number of recordings that have been made since the IP VCR was last restarted.
Total length of recordings	The combined duration of all recordings accessible by the IP VCR. This includes recordings made using the IP VCR, those uploaded to it and those stored externally on an NFS server.
Total length of internal recordings	The combined duration of all recordings stored internally on the IP VCR. This includes recordings made using the IP VCR and those uploaded to it.
Total size of internal recordings	The combined storage capacity used by all recordings stored internally on the IP VCR.
Free disk space	The remaining storage capacity of the IP VCR.

Displaying hardware health status

The Health Status displays information about the hardware components of the IP VCR. To access this information, go to **Status > Health.**

To reset these values, click **Clear**. Refer to the following table for assistance in interpreting the information displayed.

Field	Field description	Usage tips
Fans (2200 series only) **Voltages** **RTC battery**	Displays two possible states: *OK* *Out of spec* States indicate both **Current status** and **Worst status seen** conditions.	*OK* – component is functioning properly *Out of spec* – Check with your support provider; component might require service If the **Worst status seen** column displays *Out of spec*, but **Current status** is *OK*, monitor the status regularly to verify that it was only a temporary condition.
Temperature	Displays three possible states: *OK* *Out of spec* *Critical* States indicate both **Current status** and **Worst status seen** conditions.	*OK* – temperature of the IP VCR is within the appropriate range *Out of spec* – Check the ambient temperature (should be less than 34 degrees Celsius) and verify that the air vents are not blocked *Critical* – temperature of IP VCR is too high. An error also appears in the event log indicating that the system will shutdown in 60 seconds if the condition persists If the **Worst status seen** column displays *Out of spec*, but **Current status** is *OK*, monitor the status regularly to verify that it was only a temporary condition.

Displaying security status

The Security status page displays a list of active security warnings for the IP VCR. To access this information, go to **Status > Security.**

Security warnings identify potential weaknesses in the security of the IP VCR's configuration. Note that some security warnings might not be relevant for your organization. For example, if the IP VCR is inside a secure network, enabling HTTP may not be a security issue. For information about all possible security warnings, refer to Understanding security warnings.

To acknowledge a security warning, select that warning and click **Acknowledge selected**. Acknowledged warnings will not appear on the IP VCR's Home page. If the IP VCR reboots, the warnings are reset and previously acknowledged warnings will need re-acknowledging.

To fix a security issue, click on the **Action** link for the warning message relating to the issue. When you fix a security issue, the security warning disappears from this list (on the **Status > Security** page).

Refer to the following table for details of the information displayed.

Field	Field Description
Warning	The text of the security warning.
State	For every security warning, the state will one of: *New*: A new security warning is one that has been raised by the IP VCR, but you have not acknowledged it. New warnings also appear on the IP VCR Home page. *Acknowledged*: An acknowledged security warning is one that you have acknowledged, but have not fixed. When you fix a security issue, the security warning disappears from this list..
Action	For every security warning, there is a corresponding action that explains how to fix the security issue. Usually this is a link that takes you to the page where you can make the configuration change that will fix the security issue.

Working with the event logs

If you are experiencing complex issues that require advanced troubleshooting, you may need to collect information from the IP VCR logs. Typically, you will be working with Customer support who can help you obtain these logs.

Event log

The last 2000 status messages generated by the IP VCR are displayed in the **Event log** page (**Logs > Event log)**. In general these messages are provided for information, and occasionally *Warnings* or *Errors* may be shown in the Event log. The presence of such messages is not cause for concern necessarily; if you are experiencing a specific problem with the operation or performance of the IP VCR, Customer support can interpret logged messages and their significance for you.

You can:

- Change the level of detail collected in the traces by editing the **Event capture filter** page. You should not modify these settings unless instructed to do so by Customer support.
- Display the log as text: go to **Logs > Event log** and click **Download as text**.
- Change which of the stored Event log entries are displayed by editing the **Event display filter** page.
- Send the event log to one or more syslog servers on the network for storage or analysis. The servers are defined in the **Syslog** page.

  For more information, refer to Logging using syslog
- Empty the log by clicking **Clear log**.

Event capture filter

The Event capture filter allows you to change the level of detail to collect in the Event log traces.

Note: You should not modify these settings unless instructed to do so by Customer support. Modifying these settings can impair the performance of your IP VCR.

Normally, the capture filter should be set to the default of *Errors, warnings and information* for all logging sources. There is no advantage in changing the setting of any source without advice from Customer support. There is a limited amount of space available to store logged messages and enabling anything other than *Errors, warnings and information* could cause the log to become full quickly.

Event display filter

The Event display filter allows you to view or highlight stored Event log entries. Normally, you should not need to view or modify any of the settings on this page.

Syslog

You can configure the IP VCR to send event messages to up to four syslog servers. To add or remove a syslog server, go to **Logs > Syslog** and make the changes you require. See Logging using syslog.

H.323/SIP log

The **H.323/SIP log** page records every H.323 and SIP message received or transmitted from the IP VCR. The log can be exported in an .xml file by clicking **Download as XML**.

By default the H.323/SIP log is disabled because it affects performance, but Customer support may ask you to enable it if there is a problem with an IP VCR in your network. To do this, click **Enable H323/SIP logging**

Management event receivers

If the IP VCR is being managed by a remote management system, for instance TMS, information on that remote system may be shown on this page. In certain circumstances you may need to remove the link between the external system and the IP VCR. To do so, click **Clear**.

Understanding security warnings

The **Security status** page displays a list of active security warnings for the IP VCR. To access this information, go to **Status > Security**. Security warnings identify potential weaknesses in the security of the IP VCR's configuration. For more information on configuring security settings, refer to Configuring security settings. For more detailed information on the security status, refer to Displaying security status.

The following table details the warnings that appear, and the relevant actions needed to rectify them.

Warning	Action	Explanation
Advanced password security is disabled	Enable **advanced account security mode** in security settings	If advanced account security mode is not enabled, passwords will be stored in plain text in the configuration file, and therefore be unsecure. To enable advanced account security mode, go to **Settings > Security** and enable *Advanced account security mode*.
Hide log messages on console is disabled	Enable hide log messages on console in serial console settings	To hide log messages on the console, go to **Settings > Security** and select **Hide log messages on console**. This will stop event messages appearing on the console.
Require administrator login to console is disabled	Enable require administrator login in serial console settings	You must log in using an admin account to access serial console commands, in this way the serial console will be more secure. To do this, go to **Settings > Security** and select **Require administrator login**.
Guest account is enabled	Disable the guest account.	By default the guest user account is assigned the privilege of 'conference list only', meaning that users who log in as guest can view the list of active conferences and change their own profile. Disabling the guest account makes the IP VCR more secure. To disable the guest account, go to **Users > User list** and select **Guest**. Select **Disable user account**.
Admin account has default username	Change the admin account username	The IP VCR must have at least one configured user with administrator privileges. By default, the User ID is "admin" and no password is required. To change the admin account username, go to **Users > User list** and select **admin**. Enter a new username in the **User ID** field and click **Update user settings**.
Unsecured FTP service is enabled	Disable FTP in network TCP services	Information sent using FTP is unencrypted and sent in plain text; therefore, it is possible for people to discover usernames and passwords easily. To disable FTP, go to **Network > Services** and ensure **FTP** is not selected.
Unsecured HTTP service is enabled	Disable HTTP in network TCP services	Information sent using HTTP (Web) is unsecured and not encrypted. To disable HTTP, go to **Network > Services** and ensure **Web** is not selected. We recommend that you select **Secure web**.
Unsecured SNMP service is enabled	Disable SNMP in network UDP services	Information sent using SNMP is unencrypted and sent in plain text; therefore, it is possible for people to discover usernames and

Warning	Action	Explanation
		passwords easily. To disable SNMP, go to **Network > Services** and ensure **SNMP** is not selected.
Auto-refresh of web pages is enabled	Change auto-refresh interval to "No auto-refresh"	If your IP VCR is set to auto-refresh it could mean that on an idle IP VCR a session will never time out. To turn off auto-refresh, go to **Settings > User interface** and change **Status page auto-refresh interval** to *No auto-refresh*.
Audit logging of configuration changes is disabled	Enable the audit log	If the audit log is disabled, the IP VCR will not create an audit log. To enable audit logs, go to **Logs > Audit log** and select **Enable auditing**. (See Working with the audit log.) For more information on the audit log, refer to Configuring security settings.
Audit logs hash check failed, audit system integrity compromised	Check system configuration for possible security changes	If audit logs checks fail, it is possible that your IP VCR has been compromised. For example, someone may have taken the compact flash card out and deleted some audit logs. For more information on the audit log, refer to Configuring security settings
Call encryption is disabled	Enable call encryption	When encryption status is *Disabled*, no calls on the IP VCR can use encryption. To enable encryption, go to **Settings > Encryption**. For **Encryption status**, select *Enabled*.
Audit log above 75% capacity	Download and delete audit logs	The audit log has a maximum capacity of 100,000 audit events, or the size limit of the compact flash card. When you are nearing either of these limits, the IP VCR will give you this warning. If you reach full capacity of the compact flash card, the IP VCR will 'wrap' meaning that older logs are deleted. To rectify this problem download and clear the audit log. To do this, go to **Logs > Audit log** and select **Download as XML**. Once this has completed, click **Delete all records**.
Audit log above 90% capacity	Download and delete audit logs.	The audit log has a maximum capacity of 100,000 audit events, or the size limit of the compact flash card. When you are nearing either of these limits, the IP VCR will give you this warning. If you reach full capacity of the compact flash card, the IP VCR will 'wrap' meaning that older logs are deleted. To rectify this problem download and clear the audit log. To do this, go to **Logs > Audit log** and select **Download as XML**. Once this has completed, click **Delete all records**.
Shell not secured for startup	Disable the serial input during startup.	If **Disable serial input during startup** isn't selected, the serial console is not protected during application startup. This means users will have access to debug services in the operating system. To disable this, go to **Settings > Security**, and select **Disable serial input during startup**.

Logging using syslog

You can send the Event log to one or more syslog servers on the network for storage or analysis.

To configure the syslog facility, go to **Logs > Syslog**.

In this section:

- Syslog settings
- Using syslog

Syslog settings

Refer to this table for assistance when configuring Syslog settings:

Field	Field description	Usage tips
Host address 1 to 4	Enter the IP addresses of up to four Syslog receiver hosts.	The number of packets sent to each configured host is displayed next to its IP address.
Facility value	A configurable value for the purposes of identifying events from the IP VCR on the Syslog host. Choose from the following options: *0 - kernel messages* *1 - user-level messages* *2 - mail system* *3 - system daemons* *4 - security/authorization messages (see Note 1)* *5 - messages generated internally by syslogd* *6 - line printer subsystem* *7 - network news subsystem* *8 - UUCP subsystem* *9 - clock daemon (see Note 2)* *10 - security/authorization messages (see Note 1)* *11 - FTP daemon* *12 - NTP subsystem* *13 - log audit (see Note 1)* *14 - log alert (see Note 1)* *15 - clock daemon (see Note 2)* *16 - local use 0 (local0)* *17 - local use 1 (local1)* *18 - local use 2 (local2)* *19 - local use 3 (local3)* *20 - local use 4 (local4)* *21 - local use 5 (local5)* *22 - local use 6 (local6)* *23 - local use 7 (local7)*	Choose a value that you will remember as being the IP VCR. **Note 1:** Various operating system daemons and processes have been found to utilize Facilities 4, 10, 13 and 14 for security/authorization, audit, and alert messages which seem to be similar. **Note 2:** Various operating systems have been found to utilize both Facilities 9 and 15 for clock (cron/at) messages. Processes and daemons that have not been explicitly assigned a Facility value may use any of the "local use" facilities (16 to 21) or they may use the "user-level" facility (1) - and these are the values that we recommend you select.

Using syslog

The events that are forwarded to the syslog receiver hosts are controlled by the event log capture filter.

To define a syslog server, simply enter its IP address and then click **Update syslog settings**. The number of packets sent to each configured host is displayed next to its IP address.

Note: Each event will have a severity indicator as follows:

- 0 - Emergency: system is unusable (unused by the IP VCR)
- 1 - Alert: action must be taken immediately (unused by the IP VCR)
- 2 - Critical: critical conditions (unused by the IP VCR)
- 3 - Error: error conditions (used by IP VCR *error* events)
- 4 - Warning: warning conditions (used by IP VCR *warning* events)
- 5 - Notice: normal but significant condition (used by IP VCR *info* events)
- 6 - Informational: informational messages (used by IP VCR *trace* events)
- 7 - Debug: debug-level messages (used by IP VCR *detailed trace* events)

Feedback receivers

If the IP VCR is being managed by a remote management system, for instance TMS, information on that remote system may be shown on this page. In certain circumstances, you may need to remove the link between the external system and the IP VCR: to do so, click **Clear**.

SIP: Advanced

SIP implementation

The IP VCR implements SIP as defined in RFC 3261. Any product wanting to establish SIP calls with the IP VCR must implement INVITE, ACK, BYE, and CANCEL messages along with responses from 1xx to 6xx. The IP VCR acts as a client and does not return 5xx and 6xx responses; however, proxies and other intermediaries may do so.

To use a SIP registrar in conjunction with the IP VCR, you must register an ID for the IP VCR with the SIP registrar.

The IP VCR can register itself and individual folders with a SIP registrar. To make calls via a registrar, the product should implement the REGISTER request, along with a facility for HTTP digest authentication.

For video Fast Update Requests, the IP VCR uses a type that involves sending an INFO message with an XML body. This only applies to video endpoints, but these endpoints should be able to correctly reply to INFO requests whether or not they understand them as Fast Update Requests.

Authentication details

The username and password that you provide on the **Settings > SIP** page are the authentication details for all SIP authentication from the IP VCR. That is, for the SIP registrar and any SIP proxy.

Customizing the user interface

In this section:

- Configuring user interface settings:
  - Controlling the auto-refreshing of status pages on the IP VCR
  - Controlling the display of thumbnail preview images
- Configuring welcome messages on the Login and Home pages
- Customizing voice prompts on the IP VCR

The IP VCR provides you with options for customizing the voice prompts, the viewing of thumbnail previews, the text of the welcome messages and for controlling the auto-refreshing of user interface pages.

Note: the user interface (that is the text you see on the web interface of the IP VCR) can be localized by Cisco or by your reseller. This type of customization is the localization of the text on the web interface and these online help pages. That is, the text has been translated into your local language. In the case where you have a localized unit or blade, **Use localization package** is selected. For more information refer to Customization: more information.

Some localization packages are available on the FTP site.

The IP VCR allows you to type using any character set when entering text into the web interface. For example, when naming endpoints or users, you can use any character set you require.

Configuring user interface settings

Controlling the auto-refreshing of status pages on the IP VCR

Some pages on the IP VCR auto-refresh to ensure that the information displayed is current. Auto-refreshing pages keep web sessions alive indefinitely meaning that an administrator login will never timeout. This may be considered to be a security weakness, and if necessary you can disable all auto-refreshing.

To control the auto-refreshing of status pages on the IP VCR:

1. Go to **Settings > User interface**.
2. Choose the time interval for page auto-refreshes or, to stop pages from auto-refreshing, choose *No auto-refresh*.
3. Click **Apply changes**.

The status pages affected by this control are as follows:

- **Status > General**
- **Status > Health**

Controlling the display of thumbnail preview images

To control the display of thumbnail preview images on the IP VCR:

1. Go to **Settings > User interface**.
2. Choose whether you want to **Show video thumbnail images** or not. This controls whether or not you will see a preview of the recording on the **Connections** page.
3. Click **Apply changes**.

Controlling the availability of public pages

You can allow users access to the Streaming and Recording list pages without having to authenticate with the IP VCR. By default, these pages are accessible to users who have not logged in. However, you can disable access as follows:

1. Go to **Settings > User interface**.
2. In the **Public pages** section, ensure that **Streaming** and/or **Recording list** are not selected.
3. Click **Apply changes**.

Configuring welcome messages for the Login and Home pages

You can configure a message banner to appear on the Login page of the IP VCR. For example, some organizations might require some legal text on the login page of the IP VCR. You can also configure a message banner to appear on the Home page. You can configure a separate title (maximum: 100 characters) and text (maximum: 1500 characters) for each banner. To configure the message banners:

1. Go to **Settings > User interface**.
2. In the **Welcome messages** section, enter the text you require for the titles and the text of the messages.
3. Click **Apply changes**.

Customizing voice prompts on the IP VCR

By default the IP VCR includes English voice prompts spoken by an American woman.

These prompts are used by the IP VCR to provide callers with information, for example: "Connecting you to your destination".

You may want to replace these prompts with your own in order to change the wording, language or accent used. Alternative prompts can be uploaded individually using the web interface. Alternatively, a collection of voice prompts can be uploaded in one go by means of a *resource package* (see Uploading a customization package).

Some customization packages are available on the FTP site.

The customization of voice prompts is controlled via the web interface. Go to **Settings > User interface**. Refer to the sections below for details of the options available and for a description of the information displayed:

- Using default US English voice prompts
- Uploading a customization package
- Viewing the available voice prompts
- Uploading and downloading customized voice prompts
- Voice prompt specification
- Making the best possible recordings

Using default US English voice prompts

The default set of voice prompts is provided in US English and is the standard set of voice prompts supplied with the IP VCR. These are spoken by a female voice in Americanized English.

If your unit or blade is using customized voice prompts and you want to return to using the default set of voice prompts:

1. Go to **Settings > User interface**.
2. In the **Select customization** section, clear **Use customized voice prompts**.

3. If your unit or blade was provided to you as a localized unit/blade, clear **Use localization package**.
4. Click **Apply changes**.

The default voice prompts will be applied immediately, although it may take a few seconds before everyone connected to the IP VCR is able to hear the new prompts.

Uploading a customization package

It is possible to upload a collection of alternative voice prompts to the IP VCR with a single upload operation, using a *customization package*. Such a package may have been supplied to you by Cisco or one of its representatives, or you may have created the package yourself (see Downloading a customization package).

To upload a package:

Go to **Settings > User interface**.

In the **Upload customization package** section, click **Browse** and locate the *.package* file on your computer.

Click **Upload package**.

The upload can take several seconds, depending on the size of the package file and the speed of your network connection. When the upload is complete, a status screen will be shown, displaying some or all of the individual voice prompt customizations included in the package if the upload was a success, or an error message if the upload failed for some reason.

To apply the uploaded customization package:

- In the **Select customization** section, select **Use customized voice prompts**.

Note: If you were already using uploaded alternative voice prompts on the IP VCR, then these will be immediately replaced by those in the customization package. If a particular customized file is not included in the package, then any existing customization is unchanged. This allows customization sets to be built up using several different packages if required.

Viewing the available voice prompts

You can review the voice prompt customizations available in the table headed **Voice prompts**. The **Voice prompts** list displays all voice prompt customizations, providing details for those which have alternatives uploaded. Because these lists can be quite long, by default they are hidden. Instead, the number of customizations (files) available is shown. If any have been modified (meaning an alternative customization has been uploaded, either individually, or as part of a package), then this is indicated by an asterisk after the table name.

To expand any list to show all customizations, click **show file details**; you can subsequently hide it again by clicking **hide file details**.

In the expanded state, the table shows, for each customization, a description of the file, the standard IP VCR filename for the customization, and the length and date modified (uploaded) of alternative customizations present. Extra information is provided by the following symbols:

- Customizations where an alternative is available that can be individually uploaded or downloaded are indicated by two asterisks (**) after their name
- Customizations where an alternative is available that cannot be uploaded or downloaded individually are indicated by one asterisk (*) (these are files that have been provided by Customer support)
- Customizations that are part of a localization package from Cisco or your reseller are indicated by a plus sign (+)

Uploading and downloading customized voice prompts

Refer to the sections below for details of further functionality provided by the **Installed voice prompts** list:

- Uploading individual voice prompts
- Downloading individual voice prompts
- Downloading a customization package
- Deleting customized voice prompts

Uploading individual voice prompts

You can upload individual voice prompts. To do this:

1. Go to **Settings > User interface**.
2. In the **Installed voice prompts** section, click **show files details** and locate the voice prompt file you require.
3. For that voice prompt, click **upload**. You can do this regardless of whether an alternative customization has already been uploaded.
4. You see a new screen, allowing you to locate and upload the customization of your choice. Click **Browse** to locate the voice prompt file on your computer. Voice prompt files must be in the following format:
   - Microsoft WAVE (.WAV) format
   - 16kHz (16000Hz) sample rate
   - Mono
   - Uncompressed
   - Maximum 10 seconds long

   If you upload a file that is not in this format, the upload may fail or the voice prompt may sound distorted when heard by users. Use an audio editing package of your choice to make any conversions required. See Making the best possible recordings for how to obtain the best possible voice prompts for your IP VCR customization.

   Note that in addition to the 10 second length limit per prompt, there is a total length limit of four minutes for the full set of prompts. That is, if all samples were played back-to-back, it should take no more than 240 seconds.
5. When you have located the file you want to upload, click **Upload customization**. If the upload is successful, you see the size of the uploaded file; otherwise an error is shown. If the upload fails, check that your audio file matches the specification above before contacting your support representative.

Downloading individual voice prompts

You may want to review a customization that has been previously uploaded to the IP VCR. To do this:

1. Go to **Settings > User interface**.
2. In the **Installed voice prompts** section, locate the voice prompt file you require.
3. For that voice prompt, right-click **download** and choose **Save Target As** (or your web browser's equivalent operation). The file is downloaded to your computer for reference.

Only alternative customizations can be downloaded in this way; the default voice prompts cannot be downloaded. In addition, only customizations uploaded as individual files can be downloaded; those uploaded as part of a package cannot be downloaded.

Downloading a customization package

Once you are satisfied with your customizations, you may want to apply the entire set to another IP VCR. Rather than individually uploading the alternative voice prompts to each one, you can create a *customization package*.

To create a customization package containing all of the alternative voice prompts previously uploaded:

1. Go to **Settings > User interface**.
2. Click **Download package** at the bottom of the **Installed voice prompts** list. The customization package is downloaded to your computer.

A package can only contain resources uploaded as separate files; those uploaded as part of another package cannot be included. The package download option may be unavailable if no voice prompts qualify for inclusion.

Deleting customized voice prompts

If you are dissatisfied with a voice prompt that you have uploaded to the IP VCR, you can delete it in the following manner:

1. Locate the voice prompt of interest in the list.
2. Select it.
3. Click **Delete selected** to remove the voice prompt.

Only alternative voice prompts can be deleted in this way; the default voice prompts cannot be deleted. If you delete an alternative customization, it will immediately revert to the default prompt, even if you have selected **Use customized voice prompts** at the top of the page.

You may want to delete all customizations. To do this, click **Delete all**. Remember that you can revert to the default set of voice prompts without needing to delete any alternative customizations (see Using default voice prompts).

Voice prompt specification

Below is a complete list of the voice prompts that can be customized. The default wording is shown for each prompt. You do not have to use exactly the same wordings if they are not appropriate for your needs, and are provided only as a guide.

Filename	Default wording
voice_prompt_control_use_fecc	Please use the far end camera control on your remote to make your selection
voice_prompt_enter_pin	Please enter the security PIN
voice_prompt_pin_incorrect	Sorry, I did not recognize that security PIN, please try again
voice_prompt_playback_start	Playback is starting now
voice_prompt_recording_paused	Recording is paused
voice_prompt_welcome_vcr	Hello. Welcome to the video call recording system
voice_prompt_recording_control_start	Use up to start recording
voice_prompt_recording_control_stop	Use down to stop recording
voice_prompt_recording_home	This is the main recording screen

Making the best possible recordings

There are many factors to consider when recording alternative voice prompts in order to get the best results. Below is a summary of the points to bear in mind.

Recording format

It is best to make each recording with the ideal settings and hence avoid any sample-rate or resolution changes. As discussed, the ideal format is Microsoft Wave (.WAV) format, uncompressed, mono, at 16 kHz and 16-bit resolution.

If you are unable to make mono recordings, the IP VCR can convert stereo recordings.

Background noise

It is important to minimize background noise (hiss) as much as possible. This includes ambient noises such as road noise and slamming doors etc. but also try to keep fan noise and similar to a minimum.

When played back by the IP VCR, samples with background noise are very apparent.

Consistency

If possible, record all voice prompts in one session. This will ensure that all voice and background conditions remain constant and the recorded voice will sound similar from prompt to prompt.

Volume

Record prompts using a relatively constant loudness of voice. Although it can take some trial and error, the best recordings will result from speaking loud enough that the voice is recorded loudly compared to any residual background noise, but not so loudly that it sounds distorted when played back.

Customization: More information

There are three customization levels on the unit or blade (for voice-prompts, web interface, help pages, and text messages):

- the factory default files that are provided in US English
- localization files that are sometimes installed by a reseller
- customized voice prompts files that can be uploaded and downloaded by you

Precedence

For every customizable file:

1. If there is a customization file present and **Use customized voice prompts** is selected, that file is used.
2. Otherwise, if **Use localization package** is selected, the unit or blade will use the localized file.
3. If 1 and 2 are not true, then the unit or blade will use the default US English file.

The factory default file set

The files that compose the default file set for the web interface, the voice prompts, the help pages, and text messages cannot be deleted. If you are using your own customization files or a localized unit or blade you can return it to using the default file set:

To return to the defaults:

1. Go to **Settings > User interface**.
2. Ensure **Use localization package** and **Use customized voice prompts** are not selected.

Note that the default voice prompts are used where there is no alternative voice prompt available, even if **Use customized voice prompts** is selected.

Localization files

In some parts of the world, units and blades are available where the help pages, the voice prompts, the text messages, and some of the web interface are in the local language. In this case, Cisco or the reseller has uploaded a package that provides localized files to replace files in the default file set. This localization process can only be performed by Cisco or by a reseller. If you have a localized unit or blade, you are able to select to return to the default US English file set (see above). Localization is a global change and affects all customizable files. If you have a localized unit or blade, you cannot upload and download localized files on a file by file basis.

Customization files

Customization files for voice prompts can be recorded and uploaded by any admin user of the IP VCR. These files can be uploaded one by one of as a package. You can create your own package by uploading all the files you require to an IP VCR and then downloading them as a package. For more information, refer to Customizing the user interface. A customization package does not have to include a complete set of files. Where a file name duplicates an existing uploaded voice prompt file, that file will be overwritten.

Backing up and restoring the configuration using FTP

You can back up and restore the configuration of the IP VCR through its web interface. To do so, go to **Settings > Upgrade**. For more information, refer to Upgrading and backing up the IP VCR.

You can also save the configuration of the IP VCR using FTP.

To back up the configuration via FTP:

1. On the **Network > Services** page ensure that **FTP** is enabled.
2. Connect to the IP VCR using an FTP client. When asked for a user name and password, enter the same ones that you use to log in to the IP VCR's web interface as an administrator.
   You will see a file called configuration.xml. This contains the complete configuration of your IP VCR.
3. Copy this file and store it somewhere safe.

The backup process is now complete.

To restore the configuration using FTP:

1. Locate the copy of the configuration.xml file that you want to restore.
2. On the **Network > Services** page ensure that **FTP** is enabled.
3. Connect to the IP VCR using an FTP client. When asked for a user name and password, use the same ones that use to log in to the IP VCR's web interface as an administrator.
4. Upload your configuration.xml file to the IP VCR, overwriting the existing file on the IP VCR.

The restore process is now complete.

Note: The same process can be used to transfer a configuration from one IP VCR to another of the same model number. However, before doing this, be sure to keep a copy of the original feature keys from the IP VCR whose configuration is being replaced.

If you are using the configuration file to configure a duplicate IP VCR, for example in a network where you have more than one, be aware that if the original IP VCR was configured with a static address, you will need to reconfigure the IP address on any others on which you have used the configuration file.

Network connectivity testing

The Network connectivity page can be used for troubleshooting issues that arise because of problems in the network between the IP VCR and a remote video conferencing device being called (or a device from which a user is attempting to call the IP VCR).

The page enables you to attempt to 'ping' another device from the IP VCR's web interface and perform a 'traceroute' of the network path to that device. The results show whether or not you have network connectivity between the IP VCR and another device. You can see from which port the IP VCR will route to that address. For a hostname, the IP address to which it has been resolved is displayed.

To test connectivity with a remote device, go to **Network > Connectivity**. In the text box, enter the IP address or hostname of the device to which you want to test connectivity and click **Test connectivity**.

For each successful 'ping', the time taken for the ICMP echo packet to reach the host and for the reply packet to return to the IP VCR is displayed in milliseconds (the round trip time). The TTL (Time To Live) value on the echo reply is also displayed.

For each intermediate host (typically routers) on the route between the IP VCR and the remote device, the host's IP address and the time taken to receive a response from that host is shown. Not all devices will respond to the messages sent by the IP VCR to analyze the route; routing entries for non-responding devices is shown as <unknown>. Some devices are known to send invalid ICMP response packets (e.g. with invalid ICMP checksums); these responses are not recognized by the IP VCR and therefore these hosts' entries are also shown as <unknown>.

Note: The ping message is sent from the IP VCR to the IP address of the endpoint that you enter. Therefore, if the IP VCR has an IP route to the given IP address, regardless of whether that route lies out of port A or port B, the ping will be successful. This feature allows the IP VCR’s IP routing configuration to be tested, and it has no security implications.

If you are unable to ping the device then check your network configuration especially any firewalls using NAT.

Configuring SSL certificates

If the IP VCR has the Secure management (HTTPS) or Encryption feature key installed, and you enable *Secure web* on the **Network > Services** page (Configuring IP services) , you are able to access the web interface of the IP VCR using HTTPS. The IP VCR has a local certificate and private key pre-installed and this is used by default when you access the unit using HTTPS. However, we recommend that you upload your own certificate and private key to ensure security because all IP VCRs have identical default certificates and keys.

To upload your own certificate and key, go to **Network > SSL certificates**. Complete the fields using the following table for help and click **Upload certificate and key**. Note that you must upload a certificate and key simultaneously. After uploading a new certificate and key, you must restart the IP VCR.

If you have uploaded your own certificate and key, you can remove it later if necessary; to do this, click **Delete custom certificate and key**.

The following table details the fields you see on the **Network > SSL certificates** page.

Field	Field description	Usage tips
Local certificate		
Subject	The details of the business to which the certificate has been issued: • **C**: the country where the business is registered • **ST**: the state or province where the business is located • **L**: the locality or city where the business is located • **O**: the legal name of the business • **OU**: the organizational unit or department • **CN**: the common name for the certificate, or the domain name	
Issuer	The details of the issuer of the certificate.	Where the certificate has been self-issued, these details are the same as for the **Subject**.
Issued	The date on which the certificate was issued.	
Expires	The date on which the certificate will expire.	
Private key	Whether the private key matches the certificate.	Your web browser uses the SSL certificate's public key to encrypt the data that it sends back to the IP VCR. The private key is used by the IP VCR to decrypt that data. If the **Private key** field shows 'Key matches certificate' then the data is securely encrypted in both directions.
Local certificate configuration		
Certificate	If your organization has bought a certificate, or you have your own way of generating certificates, you can upload it. Browse to find the certificate file.	
Private key	Browse to find the private key file that accompanies your	

Field	Field description	Usage tips
	certificate.	
Private key encryption password	If your private key is stored in an encrypted format, you must enter the password here so that you can upload the key to the IP VCR.	
Trust store		
Subject	The details of the business to which the trust store certificate has been issued: • **C**: the country where the business is registered • **ST**: the state or province where the business is located • **L**: the locality or city where the business is located • **O**: the legal name of the business • **OU**: the organizational unit or department • **CN**: the common name for the certificate, or the domain name	
Issuer	The details of the issuer of the trust store certificate.	Where the certificate has been self-issued, these details are the same as for the **Subject**.
Issued	The date on which the trust store certificate was issued.	
Expires	The date on which the trust store certificate will expire.	
Certificate verification settings	Choose to what extent the IP VCR will verify the identity of the far end for a connection: • *No verification*: all outgoing connections are permitted to proceed, even if the far end does not present a valid and trusted certificate. • *Outgoing connections only*: outgoing connections are only permitted if the far end has a certificate which is trusted. • *Outgoing connections and incoming calls*: outgoing connections and incoming connections for SIP calls using TLS must have a certificate which is trusted otherwise the IP VCR will not allow the connection to proceed.	Outgoing connections are connections such as SIP calls which use TLS.

Contact details and license information

Please refer to the following sections for details of where to get further help and for additional software license information:

- TANDBERG
- Software licenses

TANDBERG

TANDBERG is now part of Cisco. TANDBERG Products UK Ltd is a wholly owned subsidiary of Cisco Systems, Inc.

The IP VCR firmware is Copyright © TANDBERG Products UK Ltd 2003-2010 except where specifically mentioned below. All rights reserved.

For further assistance and updates visit the web site.

This product contains an authentication function which uses an encrypted digital signature and a public key infrastructure. It is your responsibility to ensure that any import into or export from your territory and any use of the product in your territory is in compliance with your local laws. This product may not be exported to any country embargoed by the US or any member of the European Union without the prior written consent.

Software licenses

The IP VCR includes software developed by the NetBSD Foundation, Inc. and its contributors (specifically the NetBSD operating system), software developed by Spirit Corporation (specifically G.728 and MPEG audio layer 2 codec implementations) , software developed by Tecgraf, PUC-Rio (specifically Lua), software developed by the Internet Systems Consortium, Inc (specifically DHCP), and software developed by Polycom, Inc. (specifically Polycom® Siren14™ audio codec).

This product can use HMAC-SHA1 to authenticate packets and AES to encrypt them.

The following copyright notices are reproduced here in order to comply with the terms of the respective licenses.

- NetBSD
- Info-ZIP
- Independent JPEG Group
- The OpenSSL Project
- Spirit Corporation
- AES
- HMAC
- SHA1
- Lua
- DHCP
- Polycom Inc
- Fraunhofer IIS

NetBSD

The IP VCR includes software developed by the authors listed below. These notices are required to satisfy the license terms of the software mentioned in this document. All product names mentioned herein are trademarks of their respective owners.

- The University of California, Berkeley and its contributors.
- The University of California, Lawrence Berkeley Laboratory and its contributors.
- The NetBSD Foundation, Inc. and its contributors.
- Jonathan R. Stone, Manuel Bouyer, Charles M. Hannum, Christopher G. Demetriou, TooLs GmbH, Terrence R. Lambert, Theo de Raadt, Christos Zoulas, Paul Kranenburg, Adam Glass, Winning Strategies, Inc, Frank van der Linden, Jason R. Thorpe, Chris Provenzano.

Info-ZIP

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.
4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

Independent JPEG Group's JPEG software

This software is based in part on the work of the Independent JPEG Group

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright © 1991-1998, Thomas G. Lane. All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

1. If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.
2. If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".
3. Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

The OpenSSL Project

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
==

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Spirit Corporation

Copyright © 1995-2003, SPIRIT

The IP VCR includes a G.728 audio codec used under license from Spirit Corporation.

The IP VCR includes a MPEG layer 2 audio codec used under license from Spirit Corporation.

AES License

Copyright (c) 2001, Dr Brian Gladman, Worcester, UK.

All rights reserved.

LICENSE TERMS

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;
2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;
3. the copyright holder's name is not used to endorse products built using this software without specific written permission.

DISCLAIMER

This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and fitness for purpose.

Issue Date: 29/07/2002

HMAC License

Copyright (c) 2002, Dr Brian Gladman, Worcester, UK. All rights reserved.

LICENSE TERMS

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;
2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;

3. the copyright holder's name is not used to endorse products built using this software without specific written permission.

ALTERNATIVELY, provided that this notice is retained in full, this product may be distributed under the terms of the GNU General Public License (GPL), in which case the provisions of the GPL apply INSTEAD OF those given above.

DISCLAIMER

This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and/or fitness for purpose.

Issue Date: 26/08/2003

SHA1 License

Copyright (c) 2002, Dr Brian Gladman, Worcester, UK. All rights reserved.

LICENSE TERMS

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;
2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;
3. the copyright holder's name is not used to endorse products built using this software without specific written permission.

ALTERNATIVELY, provided that this notice is retained in full, this product may be distributed under the terms of the GNU General Public License (GPL), in which case the provisions of the GPL apply INSTEAD OF those given above.

DISCLAIMER

This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and/or fitness for purpose.

Issue Date: 01/08/2005

Lua

Lua 5.0 license

Copyright © 2003-2004 Tecgraf, PUC-Rio.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

1. The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

DHCP

Copyright © 2004 Internet Systems Consortium, Inc. ("ISC")

Copyright © 1995-2003 Internet Software Consortium.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of ISC, ISC DHCP, nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY INTERNET SYSTEMS CONSORTIUM AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL ISC OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Polycom, Inc.

The Polycom® Siren14™ audio coding technology, including patents relating to that technology, is licensed from Polycom, Inc.

Fraunhofer IIS

IIS
Fraunhofer Institut
Integrierte Schaltungen

MPEG-4 AAC audio coding technology licensed by Fraunhofer IIS
http://www.iis.fraunhofer.de/amm/

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.