# Cisco TelePresence IP VCR Version 3.0(1.22)

Software release notes

D14241.07

March 2011

# Contents

# Document revision history

| Revision | Date | Description |
|---|---|---|
| D14241.07 | 03/2011 | Version 3.0 (1.22) Software release notes |
| D14241.06 | 12/2010 | Version 3.0 (1.11) Release Candidate release notes |
| D14241.05 | 12/2010 | Version 3.0 (1.8) Beta release notes |
| D14241.04 | 04/2010 | Version 2.4(1.2) release notes |
| D14241.03 | 10/2009 | Version 2.3(1.2) release notes |

# Introduction

This document accompanies version 3.0(1.22) of the Cisco TelePresence IP VCR software (referred to as IP VCR), which may be installed on the following Cisco TelePresence hardware products:

- Cisco TelePresence IP VCR series (includes IP VCR 2210, IP VCR 2220 and IP VCR 2240 models)
- Cisco TelePresence VCR MSE 8220 (referred to as VCR MSE 8220)

The most recent prior version of IP VCR is version 2.4. This release (version 3.0) includes the following new features and updates:

- Changes to log in screen
- SIP encryption (SRTP + TLS support)
- SIP content (BFCP) – IP VCR can record and playback content to SIP endpoints
- Alternate gatekeepers
- Advanced account security mode
- Web sessions
- Redirect HTTP requests
- Welcome messages
- Secure serial console
- Security status
- Back up and restore of configuration files
- API enhancements. The Cisco TelePresence IP VCR API version 2.7 (referred to as ‘API’) applies to version 3.0 of the Cisco TelePresence IP VCR software.

# New features and functionality in IP VCR 3.0

## Changes to log in screen

In this release we have changed the initial log in screen so that the 'log in' link is now in the top right of the screen, rather than appearing as a button. This will enable the IP VCR to display more options on this page in the future if required.

## SIP encryption

**Note:** If you record an encrypted call or conference with IP VCR version 3.0, and then downgrade to an earlier release (2.4 and earlier), the unit will not be able to play back the encrypted recording.

Similarly, the VCR Converter 1.0 (1.8) or later is required to convert encrypted files recorded by IP VCR 3.0. This applies to encrypted H.323 and SIP recordings.

### SRTP support

This release introduces support for Secure Real-time Transport Protocol (SRTP). SRTP is an encryption format widely used in SIP. When SRTP is in use, the audio and video media are encrypted. When using SRTP, the default mechanism for exchanging keys is Session Description Protocol Security Description (SDES). SDES exchanges keys in clear text, so it is a good idea to use SRTP in conjunction with a secure transport for call control messages. You can configure the IP VCR to also use Transport Layer Security (TLS) which is a secure transport mechanism that can be used for SIP call control messages.

You can configure the IP VCR to use SRTP only for calls that use TLS, or SRTP can be used for all transports. To configure which calls will use SRTP, use the SRTP encryption option on the **Settings > Encryption** page. For more information about using TLS, see below. (The other available transports are UDP and TCP).

To use SRTP encryption, you must have the *Encryption* feature key present on the IP VCR. To enable SRTP, go to the **Settings > Encryption** page in the web interface.

Note that SRTP will not be used for calls with Microsoft Office Communications Server (OCS).

### TLS support

This release introduces support for Transport Layer Security (TLS). TLS enables the signaling portion of a SIP call to be encrypted. This is important because without this, if the call uses SRTP (see above), the key exchange will be in clear text in this part of the call, meaning that although the media is encrypted, someone who read the key exchange could decrypt the call.

To use TLS, you must have the *Encryption* feature key present on the IP VCR. You can configure to use TLS for all SIP calls on the **Settings > SIP** page. However, you can also configure the TLS setting for individual endpoints that will override the unit-wide setting (using the **Endpoints > Add SIP endpoint** page).

## TLS certificate verification

This release introduces the ability to import a certificate trust store. This enables you to configure the IP VCR to verify the identity of the far end of a connection when using TLS (Transport Layer Security). For example, the trust store can be used by the IP VCR to verify the identity of a SIP endpoint.

To upload a trust store (in *.pem* format), go to **Network > SSL certificates**. Refer to the online help for more information.

When you have uploaded a trust store, you can choose to what extent the IP VCR will verify the connection. Note that in the following descriptions, outgoing connections are connections such as SIP calls which use TLS:

- **No verification**: all outgoing connections are permitted to proceed, even if the far end does not present a valid and trusted certificate. This is the default setting
- **Outgoing connections only**: outgoing connections are only permitted if the far end has a certificate which is in the trusted store
- **Outgoing connections and incoming calls**: for all outgoing connections and for incoming SIP calls that use TLS, there must be a certificate which is listed in the trusted store otherwise the IP VCR will not allow the connection to proceed:

Regardless of whether or not you choose to use TLS for outgoing connections, the IP VCR will accept incoming calls using TCP, UDP, and TLS providing those services are enabled on the **Network > Services** page.

## IP VCR can receive and send content channel from SIP endpoints

Support for Binary Floor Control Protocol (BFCP) is introduced in this release.

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. The content channel is often used by endpoints to show a presentation.

If a SIP endpoint supports the use of BFCP, it can open a BFCP channel to the IP VCR and contribute a content video stream, such as that supplied by a second camera or an attached PC.

When the IP VCR plays back a recording that includes a recorded content channel, the IP VCR can open a channel to the endpoint to send the recorded content, provided that the endpoint supports BFCP.

## ‘Alternate’ gatekeepers

This release introduces support for the use of alternate gatekeepers. That is, where the configured gatekeeper has told the 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 either the original gatekeeper is configured as an ‘alternate’ on the current gatekeeper’s list of alternates or there is no response from any of the alternates

Note that if the IP VCR registers with an alternate that does not 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.

## Advanced account security mode

**Note:** Advanced account security mode causes passwords to be hashed in an enhanced way. This hashing of passwords is an irreversible process that is not compatible with previous releases.

The IP VCR will prompt you to save the configuration when you enable Advanced account security mode. If you do not keep an appropriate configuration file and you attempt to downgrade to a previous software version without using this configuration file, you will no longer be able to log in to your IP VCR.

This release introduces the option for Advanced account security mode enabling the following features:

- The IP VCR will demand that passwords fulfill certain criteria, using a mixture of alphanumeric and non-alphanumeric (special) characters explained in 'Password format' below.
- The IP VCR will hash passwords before storing them in the configuration.xml file. This is an irreversible process.
- 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 until the administrator re-enables the account from the **Users** page.
- Non-administrator account holders are not allowed to change their password more than once during 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 **Users** page.

To enable Advanced account security mode, go to **Settings > Security**.

## Administrator accounts in Advanced account security mode

When using Advanced account security mode, it is a good idea to 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.

It is recommended 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 applications accessing the IP VCR via the API, you should create dedicated administrator accounts for each application.

## 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 that account.

### Enhanced encryption and hashing algorithms

This release has enhanced encryption ciphers for HTTPS and for SIP calls using Transport Layer Security (TLS). This may restrict the use of HTTPS with early versions of web browsers.

The password hashing algorithm has also been enhanced. This new method of hashing passwords is an irreversible process that is not compatible with previous releases. To use the new password hashing algorithm, you must enable Advanced account security mode.

### 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 logins. If a user without admin privileges attempts to login a fourth time the IP VCR will disable that user's account indefinitely. A user with admin privileges will have their account disabled for 30 minutes on their fourth attempt, after which they may log in and change their password.

## Web sessions

This release introduces the use of sessions to the IP VCR for user verification. The IP VCR no longer uses digest authentication and therefore is less secure if you are using HTTP. This may cause some third-party tools to stop working. It is recommended that you use HTTPS to protect user names and passwords.

**Note:** You must have the 'Encryption' feature key to use HTTPS.

## Redirect HTTP requests

This release introduces the option to have HTTP web 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.

This feature is enabled by default. To disable this feature, go to **Settings > Security** and select *Redirect HTTP requests to HTTPS*.

**Note:** You must have the 'Encryption' feature key to use HTTPS.

## Welcome messages

This release introduces welcome messages. This means you can configure a login message to appear on the Login page of the IP VCR. You can also configure a home page message to appear on the Home page. You can configure a separate title (maximum: 100 characters) and text (maximum: 1500 characters) for each message.

To configure the welcome messages, go to **Settings > User interface**. In the **Welcome messages** section, under **Login message** enter the text you require for the messages in the *Title* and *Text* fields. Under the **Home page message** section, enter the text you require for the messages in the *Title* and *Text* fields.

## Secure serial console

This release introduces additional security settings for the serial console. The serial console now has the following features:

- Require administrator login – If this is not enabled, anyone with physical access to the IP VCR (or with access to your terminal server) can potentially enter commands on the serial console. If enabled, a user must login with administrator privileges to access the serial console.

Enabling this feature also allows you to configure a timeout for a session on the serial console. To enable this feature, go to **Settings > Security** and select *Require administrator login.*

- Advanced account security mode – When running in Advanced account security mode and with *Require administrator login* enabled, all the features of Advanced account security mode will apply, including the disabling of accounts – see 'Advanced account security mode' for more information.
- Hiding log messages on the serial console – Log messages on the serial console can be hidden by enabling *Hide log messages on console* on the **Settings > Security** page.
- Reset password – Passwords can no longer be reset through the serial console.
- Welcome messages on the serial console – The Login Welcome messages (discussed above) also appear when logging in to the serial console. Note that *Require administrator login* must be enabled. See above for details.
- Disable the serial input during startup – The features above do not protect the serial console during system startup, therefore an option has been added to disable the serial input during startup. To disable access, go to **Settings > Security** and select *Disable serial input during startup.*

## Security status

This release introduces the Security status page. 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. 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).

## Backup and restore of configuration files

This release introduces the ability to back up and restore the configuration files via the web interface.

The **Backup and restore** section of the **Settings > Upgrade** page allows you to back up and restore the configuration of the IP VCR. 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 a "configuration.xml" file, type in, or browse to the backup file to be restored 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 check the *Network settings* box, the network configuration will be overwritten with the network settings in the supplied file. Typically you would only check this 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 boxes may become unreachable via IP.
- If you check the *User settings* box, the current user accounts and passwords will be 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 will need to log in again after the file has been uploaded.

By default, the overwrite controls are unchecked, and so the existing network settings and user accounts will be preserved.

**Note:** You can also back up and restore the configuration of the IP VCR using FTP. For more information, see the Online Help.

## API updates

The IP VCR API has a few new methods and publishes feedback events to improve remote monitoring. The commonly used enumerate methods have been updated to accept and return some new parameters.

You can find more details on the API changes in the IP VCR API guide.

# Known limitations

## Maximum port count with complex audio

In order to support playbacks at the maximum port count and at the very best quality, we recommend that you select the ‘Favor Motion’ option and to use the G.722 audio codec.

## Windows Media Player and RealPlayer

MPEGs downloaded from the IP VCR can be reported to have incorrect lengths when played back in RealPlayer and Windows Media Player.

## Distortion or discoloration of part of the image when streaming live

Sometimes when streaming live; that is while a recording is being made, part of the image is distorted or discolored. There is a work around for this in release 2.1 onwards. Go to Recordings, click on the recording file. Then click to Transcode to streaming media. This re-transcodes the recording and deletes the current file.

## Content Applet will always appear when live streaming even if content is disabled

The way that we do live streaming means that we have to bring up the content applet when we open the page or not at all. Since content can start at any time, the page has to be ready even though there is no content when the page is opened initially.

## Polycom 512 doesn't receive video on a point to point call to a VSX using H263

Legacy Polycom endpoints do not receive video from the IP VCR in a point to point call via the IP VCR to Polycom VSX endpoints. Point to point calls using H.261 work fine to VSX endpoints.

## Different behavior between disabling Windows Media Player and QuickTime ports

Windows Media Player is still able to stream when "Streaming (Windows Media Player)" is disabled. Quick Time, however, cannot stream when "Streaming (other)" is disabled.

This is because in "Network > Services" disabling "Streaming (Windows Media Player)" doesn't block Windows Media Player streaming through HTTP, whereas disabling “Streaming (other)" does block QuickTime through both port 554 and HTTP.

## Playback quality issue in Firefox for Mac OS

Poor playback quality was observed when viewing a recording in Firefox for MacOS. This has not been reliably reproduced and is suspected of being an issue of the browser’s compatibility with the QuickTime player.

Use the Safari browser to view IP VCR recordings on this platform if you encounter playback issues while using Firefox.

# Resolved caveats

The following issues were found in previous releases and were resolved in Version 3.0(1.22):

| Reference ID | Summary |
|---|---|
| 5816 | Audio prompts from signed localization packages did not load correctly on earlier versions (since Version 2.3). |
| 7130 | Streaming using the Safari web browser was not supported in previous releases. Streaming using the native Safari browser on Macs is now supported. |
| 12672 | DTMF tones sent from the Polycom ViewStation were not reliably detected by earlier versions. |
| 13369 | Custom welcome messages (user supplied text on login page and home page) with more than one line are now being displayed correctly. |

# Upgrade to version 3.0

CAUTION: You **must** back up your configuration **before** upgrading to version 3.0.

You must also remember the administrator user name and password for the backup configuration. You will need these if you ever need to make use of this backup file.

## Prerequisites and software dependencies

To upgrade the software you need to restart the hardware. Notify users who may be affected by this loss of service.

You should have the new software image file for the upgrade and the current software image file in case you need to reverse the upgrade.

Back up your configuration before you start the upgrade.

## Upgrade via the web interface

1. Unzip the image file to a local folder.
2. Navigate to the web interface of the IP VCR using your web browser.
3. Log in to the web interface (the username of the default administrative user, on a new unit, is **admin** with no password).
4. Go to **Home > Settings > Upgrade**.
5. In **Main software image** browse to the extracted image file (or type in the file path).
6. Click **Upgrade software image.**

   The Web browser uploads the file to the IP VCR. This takes some time; do not navigate away from or refresh the web page.

   The Web browser refreshes automatically after the upload completes and displays an upload completed message.
7. Close the success message.
8. Click **Shutdown** on the main upgrade page.
9. Click **Confirm IP VCR shutdown**.
10. Click **Restart IP VCR and Upgrade**.

    The unit reboots and upgrades itself. This takes some time.

    If the system logs you out due to inactivity, log in again and click **Restart IP VCR and upgrade**.

## Upgrade via FTP

1. Connect to the IP VCR via ftp.

   For example, type **ftp *IP Address*** at the command prompt, or use an FTP client with a graphical user interface.
2. Supply the administrator username and password.

   Username is **admin** without a password (on a new unit).
3. Upload the upgrade file.

   For example, enter **put *ImageFilename*** at the ftp prompt.
4. Reboot the hardware after the upload. You can reboot via the upgrade page on the web interface.

   The unit upgrades itself when it restarts.

### Notes

- FTP is generally more reliable for upgrades than the web interface.
- You can monitor the upgrade progress via the serial port.
- The upgrade time depends on the speed of your network connection. With a fast connection, the total time to download, upgrade and restart the IP VCR is in the order of several minutes.

## Downgrade instructions

If you need to reverse your upgrade, you can re-install the former version of the software.

The downgrade procedure is the same as the upgrade procedure except you will use the earlier software image.

You need the correct version of the software and your saved configuration before you proceed.

1. Follow the upgrade procedure using the earlier software image.
2. Restart the hardware and check the status via the web interface.

   The status report indicates the software version.
3. Restore your configuration from the saved XML file.

# Get updates or support

We recommend that you register your product to receive notifications about the latest software and security updates.

We regularly publish feature and maintenance releases and we recommend that you keep your IP VCR software up to date.

If you experience any problems when configuring or using your hardware, consult the online help in its web interface. If you cannot resolve your query, check our website for software updates and additional documentation.

If you need to raise a support case, collect the following information before you raise the case:

- The serial number and product model number of the unit (displayed on the hardware)
- The software build number (displayed in the unit's web interface)
- Your contact details.

# References and related documents

The following table lists documents and web sites referenced in this document. All product documentation can be found on our web site.

| Name | Document reference |
|---|---|
| Cisco TelePresence IP VCR Remote Management API 2.7 | D14661.04 |