Cisco TelePresence Video Communication Server X6.1

Software release notes

D14787.05

April 2011

Contents

Document revision history

Revision	Date	Description
D14787.01	December 2010	Initial release.
D14787.02	January 2011	Included upgrade guidance for device authentication configuration.
D14787.03	January 2011	Included upgrade guidance for Cisco VCS and Cisco TMS connectivity issues (applied to X6.0 only).
D14787.04	January 2011	Included upgrade guidance for traversal links between Cisco VCSs (applied to X6.0 only).
D14787.05	April 2011	Revisions for X6.1 release.

Introduction

These release notes describe the features and capabilities included in the Cisco TelePresence Video Communication Server (Cisco VCS) software version X6.1.

Upgrading to VCS X6.1

WARNING: If you are upgrading a cluster, you must follow the directions in the “VCS Cluster Creation and Maintenance” deployment guide (document D14367), otherwise the cluster will not synchronize.

There is a **software dependency** between **VCS X6.n** and **TMS 12.6 or later**. If you are running Cisco TelePresence Management Suite (Cisco TMS) with Provisioning or FindMe, or your Cisco VCSs are clustered and you want to upgrade your Cisco VCS to X6.0 or later, you must also upgrade Cisco TMS to TMS 12.6 or later, see the table below.

Deployment using Provisioning, Clustering or FindMe				
Software version	**TMS 12.1**	**TMS 12.2**	**TMS 12.5**	**TMS 12.6 or later**
X4.n	√	√	X	X
X5.0, X5.1.1	X	X	√	X
X5.2	X	X	X	√
X6.n	X	X	X	√

Note: If you are running TMS 12.5 you must upgrade it to 12.6 or later before upgrading to VCS X6.n.

Note: You should backup your system before upgrading. If you later need to downgrade to an earlier release you will have to restore a backup made against that previous release.

It is **vital** that you upgrade the **Cisco VCS** and **Cisco TMS** correctly – instructions for the upgrade are documented in the ”Updating to X6” section of this document.

Upgrading to X6.1 from X5.0 or earlier

If you are currently running VCS X5.0 or earlier you must first upgrade to X5.2 and then upgrade from X5.2 to X6.1.

You can only upgrade directly to X6.1 if you have version X5.1 or later.

Device authentication: provisioning of Movi and other devices

Upgrades from release X5.2 or earlier to X6.1

If device authentication is not enabled when the Cisco VCS is upgraded to X6.1, the upgrade process will configure all zones and subzones (except the default zone) on the Cisco VCS with authentication set to ‘Treat as authenticated’. This ensures that:

- CPL continues to work as expected
- Caller ID can be set to the FindMe ID for calls originating from endpoints specified in a FindMe
- The provisioning request is challenged by the provisioning server

If you are upgrading from X6.0 to X6.1 your existing authentication configuration will not be changed.

Note that if TMS Agent (rather than the Cisco VCS) challenges for authentication of provisioning data, the initial presence publication by Movi (if running Movi version 4.1 or earlier) will fail; to publish Movi presence, users must manually set their presence status after logging in.

Cisco VCS Starter Pack Express

If you have a Cisco VCS Starter Pack Express and you want to authenticate Movi devices then you must set the Default Zone to check credentials. This is because the starter pack provisioning server that runs on the Cisco VCS does not check credentials.

Cisco VCS upgrades where authentication is already enabled

If device authentication is enabled when the Cisco VCS is upgraded to X6.1, the upgrade process will configure the Cisco VCS with authentication set to ‘Check credentials’. This means that:

- CPL continues to work as expected
- Caller ID can be set to the FindMe ID for calls originating from endpoints specified in a FindMe
- The provisioning request is challenged by the Cisco VCS

If the Cisco VCS is set to ‘Check credentials’ on subzones, and the TMS Agent provisioning server is authenticating provisioning – the usernames and passwords on VCS must be configured to be the same as the provisioning usernames and passwords.

Recommendations

Device authentication

You should review your whole network and consider whether authentication should be enabled for all endpoints and enable authentication where possible.

CPL modifications

In CPL, the ‘origin’ field is a short-hand for ‘authenticated-origin’. You are recommended to update your CPL to make it explicit whether the CPL is looking at the authenticated or unauthenticated origin. If CPL is required to look at the unauthenticated origin (e.g. when checking non-authenticated callers) the CPL must use “unauthenticated-origin”. To check the authenticated origin (only available for authenticated or “treat as authenticated” devices) the CPL should use “authenticated-origin”. Note that:

- authenticated-origin is available for endpoints where ‘Check credentials’ succeeded, and for endpoints where they are registered to a ‘Treat as authenticated’ subzone
- unauthenticated-origin is available for all endpoints, whether authenticated or unauthenticated

New features in X6.1

New feature descriptions

Session management

Administrator and user session management features have been introduced. You can:

- specify the maximum number of concurrent administrator sessions (on a total and per-account basis) allowed on each VCS
- display status details of all active administrator and user sessions

Client certificate-based authentication

Support for certificate-based authentication is provided. This can be combined with a smart card (also referred to as a Common Access Card or CAC) device to provide two-factor authentication for access to VCS administration tasks.

Automatic updating of CRLs (certificate revocation lists)

You can now configure CRL distribution points and schedule the VCS to perform automatic CRL updates. This ensures the latest CRLs are available for certificate validation. Previously CRL updates had to be uploaded manually.

Cisco AM GW available on VCS Expressway

Cisco AM GW features are now available on both VCS Control and VCS Expressway platforms.

Movi ClearPath provisioning

The Cisco VCS Starter Pack now supports the provisioning of ClearPath to Movi.

Improved cluster set-up process

The process for setting-up a cluster has been simplified such that the replication of configuration and FindMe information is set up automatically when a new peer is added into a cluster via the web interface.

Presence configuration

The Subscription expiration time and Publication expiration time settings can no longer be configured on the Presence page. They can still be modified via the CLI.

Device authentication using Active Directory Service and NTLM for Movi endpoints

Device authentication can be performed using a direct connection between the VCS and an Active Directory Service (ADS). This allows Movi 4.2 (or later) endpoint users to use their Windows Active Directory (AD) credentials to authenticate via the NTLM protocol with the VCS. Note that this feature can only be configured via the CLI.

For guidance on deploying NTLM with Movi and Cisco VCS, refer to the *Cisco TMS Provisioning* deployment guide and the *Authenticating Devices* deployment guide.

Microsoft Lync 2010 support

This release supports Microsoft Lync 2010.

New features in X6.0

New feature descriptions

Enhanced authentication policy

Authentication policy can now be applied at the zone and subzone levels. It controls how the Cisco VCS authenticates incoming messages from that zone or subzone and whether those messages are rejected or are subsequently treated as authenticated or unauthenticated within the Cisco VCS. This provides increased flexibility and allows system administrators to:

- control registrations via subzones; this allows, if required, a combination of authenticated and unauthenticated endpoints to register to the same Cisco VCS
- limit the services available to unregistered or unauthenticated endpoints and devices
- cater for endpoints from third-party suppliers that do not support authentication within their registration mechanism through a “treat as authenticated” setting

External policy services

The Cisco VCS can use external policy services to manage its registration and call policies.

This is particularly suitable for large-scale deployments where policy decisions can be managed through an external, centralized service rather than by configuring policy rules on the Cisco VCS itself.

Secure communication between cluster peers

The Cisco VCS uses IPsec (Internet Protocol Security) to enable secure communication between each cluster peer.

Authentication is carried out via a pre-shared access key (configured on the Clustering page).

View registrations and calls across a cluster

You can now view all of the registrations and calls across a cluster from any one of the peers in the cluster. A Peer column on the registrations and calls status pages identifies the relevant peer.

Client-initiated connection management

Support has been implemented for RFC 5626 (known as “SIP Outbound”). This allows a UA to route calls when a peer in a cluster has failed, and also allows a UA to close all listening ports ensuring all calls can only be routed via their existing (authenticated, authorized) connection to the Cisco VCS.

Starter Pack enhancements

- The Cisco VCS Starter Pack Express supports device provisioning for E20 and Ex series endpoints. Multiway and TURN settings are provisioned to endpoints where supported.
- Additional call license option keys can be added to extend the default limit of 5 concurrent calls.
- You can restrict users from adding, deleting or modifying their own devices.

User interface language packs

Multiple language support has been enabled on the Cisco VCS's web interface. Language packs will be made available for download in the future. Contact your Cisco support representative for more information on supported languages.

Enhanced online help

The context-sensitive help available through the Help link at the top of every page on the web interface now contains additional conceptual and reference information. The help is fully searchable and also includes a table of contents to aid navigation between topics. Consequently, the link from the web interface to the PDF of the Administrator Guide has been removed (however, the PDF is still available on the support area of the website).

Cisco VCS unit LCD panel

The LCD panel on the front of the Cisco VCS hardware unit can be configured to show additional status information. It can display the system name, all IP addresses, warnings, and the number of current traversal calls, non-traversal calls and registrations.

Multiple external syslog servers

The Cisco VCS can be configured with the IP address or FQDN of up to 4 remote RFC 5424 compliant syslog servers.

SNMPv3 support

The Cisco VCS now supports secure SNMPv3 authentication and encryption.

Cisco Unity integration

The Cisco VCS now supports the use of Cisco Unity voicemail as an onbusy or noanswer target voicemail device in a FindMe.

Factory reset command

You can reset the Cisco VCS unit to a factory state by using the **`factory-reset`** command while logged in as the root user.

Note:

- this command should only be performed on the advice of Cisco customer support
- you are recommended to only perform this command over a serial connection to the Cisco VCS unit
- it reinitializes the hard disk

Changes and improvements

Web interface

- The **VCS configuration > Search rules** menu has been renamed as **VCS configuration > Dial plan**. It contains the following submenu items:
  - **Configuration**: used to configure how the Cisco VCS routes calls in specific call scenarios.
  - **Transforms**: the pre-search transforms configuration option previously found directly under the VCS configuration main menu.

  - **Search rules**: used to configure search rules.
  - **Policy services**: defines the policy services that can be used as a target of a search rule.
- The **Overview** top-level menu option has been removed and the Overview page is now accessed by going to **Status > Overview**.
- The **System configuration** top-level menu option is now just called the **System** menu.
- The **HTTPS client certificate validation** setting has been moved to the **System administration page** (**System > System**).

Setting the Caller ID to the FindMe ID for authenticated aliases only

Setting of the Caller ID to the FindMe ID for calls originating from endpoints specified in a FindMe has been changed so that only authenticated aliases are presented as the FindMe ID. Previously the Cisco VCS would present all source aliases as the FindMe ID if this feature was enabled.

CPL

The **origin** attribute of the **field** parameter of the **address-switch** and **rule** nodes in CPL has been changed to now mean **authenticated-origin**. This means the **origin** attribute now means the same as the **authenticated-origin** attribute.

Resolved caveats

The following issues were found in previous releases and were resolved in X6.n.

Resolved in X6.1

Reference ID	Summary
85612, 85615	**External policy**: a problem where modifying the **Registration restriction policy** or **Call Policy mode** resulted in an incorrect policy service password being stored has been fixed.
75287	**Encrypted Duo Video calls**: stability issues when encrypted Duo Video calls are started and stopped repeatedly have been fixed.
86688	**Cisco TMS and Cisco VCS connectivity issues**: the problem where the Cisco VCS would not accept TLS connection requests from Cisco TMS has been fixed.
86881	**Traversal links between Cisco VCSs (Controls and Expressways)**: the problem where a traversal link between an X6.0 and an X5.n or earlier system may result in calls failing mid-call and Movi not being able to publish presence has been fixed.
87871	**CVE-2011-0947: packets are only ESP encoded in one direction**: this security vulnerability found within X6.0 has been fixed as of X6.1. **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/3.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&amp;version=2&amp;vector=AV:N/AC:M/Au:N/C:P/I:N/A:N/E:F/RL:OF/RC:C CVE ID CVE-2011-0947 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
various	**OCS Relay performance improvements**: a number of issues regarding stalled OCS Relay communications have been fixed. This will improve OCS Relay's handling of registrations and presence reporting.

Resolved in X6.0

CUCM interoperability

Reference ID	Summary
84065	Fixed instability issue in the Cisco VCS caused by an unlikely scenario where media lines get reordered during SIP signaling. This scenario could have happened during an interworked call over a SIP trunk to CUCM 8.5.
78476	Fixed issue with scenarios where the Cisco VCS received a SIP message with an FQDN present in the top Via line from a neighbor zone that caused the call to fail to be established due to the Cisco VCS being unable to allocate media resources.
83565	Cisco VCS fixed to never use an authentication tag length of less than 80 bits for SRTCP streams.
82159	In scenarios where the Cisco VCS is interworking a SIP call to H.323 and it receives a mid call empty offer it would incorrectly send an empty TCS to the H.323 side. This would then cause the call to drop. This has been fixed so that the Cisco VCS now sends capabilities instead. This scenario would happen when the Cisco VCS interworks calls to the CUCM over a SIP trunk.

Reference ID	Summary
78410, 81372	If an H.323 call is put on hold between the Cisco VCS & CUCM and a change in time capabilities of an audio codec in a TCS happens while the call is on hold then the Cisco VCS was not updating the time setting when reopening the H.323 OLC towards the CUCM. This issue has now been fixed.
82778	A workaround has been put into the Cisco VCS to strip UPDATE from Allowed: header in all requests and responses destined to CUCM SIP zones. This means early dialog is not supported by the Cisco VCS and the call will now continue using other supported methods.

Other

Reference ID	Summary
62432	Bandwidth limits can now be applied to a group of endpoints specified via URI regex in a subzone.
71238	When IPv4 is selected, Ethernet ports no longer send out or respond to any IPv6 messages.
75813	Sorting by priority on search rules page (and other pages) has been fixed.
77556	In scenarios where large (>2MB) CPL files are uploaded to a Cisco VCS, registrations can fail due to the Cisco VCS becoming unresponsive during the upload of the file. This issue has now been fixed so that the Cisco VCS still functions normally during large CPL file uploads.
79972	Fixed an edge condition where the Cisco VCS became unstable if a SIP NAPTR record was not specified in the correct case due to the Cisco VCS being case sensitive in its matching.
80390	Fixed an issue where in certain situations if a Cisco VCS received an H.323 LCF off the wire that it failed to decode it would not free up the search resource being used. This would eventually result in the Cisco VCS being unable to accept any calls until it was restarted.
80413	An issue existed where a Cisco VCS would incorrectly match MCU prefixes against IP address aliases for SIP calls thus stopping IP address dialing working for SIP initiated calls. This has now been fixed so that the Cisco VCS will only match MCU prefixes against non IP Address aliases.
80983	Fixed an edge condition where the Cisco VCS would become unstable if it received an H.460 or ASSENT traversal call from a non-traversal zone.
82626	Fixed an issue where under very rare timing conditions the Cisco VCS could become unstable and restart.
83314	Cisco VCS has now been made case insensitive when looking up ENUM records in NAPTR.
83773	For presence, Cisco VCS favors a 407 response over a 412 and so when presence times out its tag, it will never be able to publish presence again. This has now been fixed so that Cisco VCS favors 412.

Known limitations

Polycom

Reference ID	Equipment	Summary
	Polycom PVX ver. 8.0.2	During the registration of the SIP client, the PVX does not re-register within the configured expire time of the Cisco VCS. The result of this action is the PVX does not stay registered to the Cisco VCS. This issue has been presented to Polycom.
	Polycom MGC	If a conference is configured on the Polycom MGC and is set to validate endpoints via IP address, calls will not successfully connect as the Cisco VCS provides its own IP address as the call signaling IP address in an H.225 setup message.

Linksys

Reference ID	Equipment	Summary
	Linksys WRT54G hardware ver. 5.0	Linksys Router WRT54G version hardware 5.0 appears to change the source ports of outbound connections opened for a prolonged period of time. As such, H.323 and SIP calls that are made from or to systems registered to a Cisco VCS behind this router will disconnect at random times.

Sony

Reference ID	Equipment	Summary
	Sony PCS-1 ver 3.4.1	During the registration as a SIP client, the Sony does not re-register within the configured expire time of the Cisco VCS. The result of this action is the PCS-1 does not stay registered to the Cisco VCS.

Firefox

Reference ID	Equipment	Summary
633001	Mozilla Firefox Version 4.0	It is not possible to access the Cisco VCS HTTPS web interface in Mozilla Firefox Version 4.0 using a raw IPv6 address. It is possible with IPv4 addresses and in earlier versions of Firefox, or if a hostname is used instead of the raw IPv6 address. This is being tracked by Mozilla as bug 633001.

Open caveats

The following issues currently apply to this version of the Cisco VCS.

Reference ID	Summary
85593	**External policy**: when editing a policy service under the **VCS configuration > Dial plan > Policy services** web page it is not possible to change the password used for remote authentication. The password can however be changed via the CLI interface or by deleting and then recreating the whole policy service with the new password.
N/A	**Hardware shutdown procedure**: the Cisco VCS is shipped with a 250 GB Hard Drive, which is utilized for saving logs and the TMS Device Provisioning Agent. You are recommended to shut down the Cisco VCS prior to it being unplugged to ensure a clean shutdown process. This can be done from the web interface.
N/A	**TANDBERG Gatekeeper interoperability**: if a TANDBERG Gatekeeper is configured as a client in a traversal relationship with a Cisco VCS running X3.0 or newer, then it is recommended that the Gatekeeper be upgraded to N6.1. If the Gatekeeper is not upgraded, it may occasionally restart when a call is attempted.
N/A	**TANDBERG Border Controller interoperability**: if a TANDBERG Border Controller is configured as a server in a traversal relationship with a Cisco VCS running X3.0 or newer, then it is recommended that the Border Controller be upgraded to Q6.1. If the Border Controller is not upgraded, it may occasionally restart when a call is attempted.
69881	**TURN server port configuration**: if the port of the TURN server is changed while the TURN server is running, then the TURN server must be restarted before the port change takes effect. This can be achieved by turning TURN services Off and then On again from the TURN configuration page.
79180	**Out of date call and registration status:** call and registration status displays can be out of date if the status changes mid-call or mid-registration. The call/registration status display is only updated when it ends. This means that the registration out-of-resources status will not be reflected in until an MCU unregisters.
85692	**Truncated SNMP object value**: the SNMP sysObjectID scalar MIB object value is being returned truncated by the Cisco VCS. Instead of returning 1.3.6.1.4.1.5596.130.6.4.1 it actually returns 1. This means that if Cisco TMS is configured to find devices using SNMP (the default configuration) it will not discover the Cisco VCS. The workaround for this when adding a system to Cisco TMS (via **Systems > Navigator**) is to expand the **Advanced Settings** section and select the **Discover Non-SNMP Systems** check box.
88084	**Incorrect responses to attempts to communicate with the Cisco VCS on ports in range 4369–4380**: the Cisco VCS incorrectly responds with an ISAKMP message if a device attempts to connect to a VCS port in the range 4369–4380.
88239	**Viewing web pages with IE8 in compatibility mode:** there are display problems with the Cisco VCS web interface when viewing web pages with IE8 in compatibility mode. The workaround is to switch off IE8 compatibility mode.
88493	**Internal server error when unregistering and blocking an alias**: if the VCS Registration Policy is set to Deny List, use of the **Unregister and block** button on the **Registration details** page will generate an internal server error message. The workaround is to manually add the alias to the Deny List and then use the **Unregister** button on the **Registration details** page.

Interoperability

The systems below have been tested and verified with this software release.

Gatekeepers / traversal servers

Equipment	Software revision	H.460.18/.19	Comments
Cisco VCS	X4.1, X4.2.1, X4.3, X5.1, X5.1.1, X5.2 X6.0	Yes	Please review the 'Open Caveats' section for more information
TANDBERG Gatekeeper	N4.1, N3.2	No	
	N6.3, N6.1, N5.2	Yes	
TANDBERG Border Controller	Q2.2	No	
	Q6.3, Q6.1, Q5.2, Q3.1	Yes	Q3.n does not support multiplexed media
Cisco MCM/IOS Gatekeeper	12.3(10)	No	
Polycom PathNavigator	7.00.03	No	
Polycom ReadiManager SE200	3.00.02.ER019	No	
RADVISION ECS	4.0.0.25	No	

Gateway interoperability

Equipment	Software revision	H.460.18/.19	Comments
Cisco TelePresence MPS	J3.3	No	The MPS supports Assent traversal natively
	J4.3, J4.0	Yes	
TANDBERG Gateway	G3.2	No	
TANDBERG 3G Gateway	R1.0, R2.0	No	
TANDBERG Video Portal	V2.0	No	
TANDBERG Entrypoint	EP1.2	No	
Cisco TelePresence ISDN Gateway Series	1.4(1.9)	No	
Cisco TelePresence IP Gateway 3500 Series	2.0(1.2)	No	
Cisco 3545 GW	5.6.1.0.2	No	
Polycom MGC50	9.0.3.1	No	
Polycom MGC25	9.0.3.1	No	
Polycom RMX2000	6.0.0.105	No	
RADVISION P20 Gateway	5.1.0.0.15	No	

MCU interoperability

Equipment	Software revision	H.460.18/.19	Comments
Cisco TelePresence MPS	J3.3, J2.4	No	The MPS supports Assent traversal natively. Both SIP and H.323 support were tested.
	J4.3, J4.0	Yes	Both SIP and H.323 support were tested.
Cisco TelePresence MCU Series	D3.10	No	
Cisco TelePresence MCU 4210	2.4(1.18)	No	Only H.323 support was tested.
Cisco TelePresence MCU 4505	2.4(1.18)	No	Only H.323 support was tested.
Cisco IPVC 3540	4.4.0.0.23	No	
Cisco IPVC 3545 MCU	5.7.0.0.21	No	
Polycom MG C25, C50	9.0.1.8	No	Tested IP, SIP and ISDN
Polycom RMX2000	6.0.0.105	No	Tested IP, SIP and ISDN
RADVISION viaIP 400 MCU	4.2.10	No	

Streaming servers

Equipment	Software revision	H.460.18/.19	Comments
Cisco TelePresence Recording Server	S3.2, S2.3	Yes	
	S1.1	No	

PC video interoperability

Equipment	Software revision	H.460.18/.19	Comments
Cisco TelePresence Movi	3.1, 4, 4.1, 4.2	n/a	
Microsoft Office Communicator	2007 R2, Lync 2010	n/a	

Endpoint interoperability

Equipment	Software revision	H.460.18/.19	Comments
Cisco IP Video Phone E20	TE4.0	No	
Cisco TelePresence System EX90	TC3.1.0	Yes	
Cisco TelePresence System	TC3.1.0	Yes	

Integrator C Series			
Cisco TelePresence System Profile MXP	F8.2	Yes	F4.n does not support multiplexed media. Both SIP and H.323 support were tested.
TANDBERG FieldView	4.0.6.4	No	
Aethra Vega Star Sliver	6.0.49	No	Tested IP, SIP, & ISDN
LifeSize Room, Express	4.2.7 (8), 4.6.0 (48)	No	
Polycom FX	6.0.5	No	Tested IP, ISDN
Polycom PVX	8.0.2.0235	No	Tested IP, SIP
Polycom v500	9.0.6	Yes	Tested IP, SIP
Polycom Viewstation MP512	7.5.4	No	Tested IP, ISDN
Polycom HDX 4000, 8006, 9004	2.5.0.8-4035,	Yes	Tested IP, SIP, & ISDN Do not use code versions 2.6 and 3.0 (it fails to respond to an Invite for H.323 to SIP calls)
Polycom VSX 3000, 7000, 8000	9.0.5.2, 9.0.6	Yes	Tested IP, SIP, & ISDN Polycom8000 calls to Movi at call rates below 1152 have distorted video on Movi and no video on Polycom (ref 79071)
Sony PCS-1	3.42	Yes	Tested IP, SIP, & ISDN
Sony PCS-TL50	2.42	No	Tested IP, SIP, & ISDN

Firewall interoperability

Equipment	Software revision	Comments
Cisco PIX 501, 505	6.3(5)	
Cisco PIX 506e, 515e	6.3(3), 7.0(4)	
Cisco Linksys WTR54GS	v2081	
PfSense	2.0	
Checkpoint CPXP-SC1-50-NG	R60, R70, R71	
Juniper SSG5, SSG550	5.4.0r7.0	
Yamaha RTX1100	8.02.43	
PCI MZK-MF150	1.00.16	

Updating to X6.1

WARNING: If you are upgrading a cluster, you must follow the directions in the "VCS Cluster Creation and Maintenance" deployment guide (document D14367), otherwise the cluster will not synchronize.

Prerequisites and software dependencies

Cisco VCS and Cisco TMS software dependency

There is a software dependency between VCS X6.n and TMS 12.6 or later. If you are running Cisco TMS with Provisioning or FindMe, or your Cisco VCSs are clustered and you want to upgrade your Cisco VCS to X6.n or later, you must also upgrade Cisco TMS to TMS 12.6 or later.

The "Cluster creation and maintenance" deployment guide (document D14367) contains full instructions on how to upgrade to VCS X6.1 and TMS 12.6 or later. Please use these instructions accompanied by the TMS upgrade procedures found in the relevant Cisco TMS Installation and Getting Started Guide.

If you are running TMS 12.5 you must upgrade it to 12.6 or later before upgrading to VCS X6.n.

You must use the procedures in the preceding documents if you use any of the following features:

- Clustering, or
- Device provisioning, or
- FindMe (with Cisco TMS managing Cisco VCS)

For other Cisco VCS deployments you may follow the Basic Cisco VCS X6.n upgrade procedure below.

Note that if you are running a single Cisco VCS with FindMe (without clustering or Cisco TMS) you can follow the Basic Cisco VCS X6.1 upgrade procedure below. Note, if you configure FindMe on a single VCS with no replication to TMS and at a later date you include this Cisco VCS in a cluster you will have to re-enter your FindMe accounts as they will be overwritten by Cisco TMS. To avoid this problem you are recommended to use Cisco TMS 12.6 or later and Cisco VCS X6.n and replicate your Cisco VCS FindMe accounts with Cisco TMS.

Basic VCS X6.1 upgrade procedure

Follow this procedure for upgrading Cisco VCS to X6.1, only if *all* of the following apply:

- The Cisco VCS is not part of a cluster, and
- Provisioning is not in use, and
- Cisco TMS is not managing the Cisco VCS
- Cisco VCS is currently X5.1.1 or later

Note: It is recommended that if FindMe™ is used that it is replicated with Cisco TMS. This allows a standalone Cisco VCS to be clustered in the future and the FindMe™ data kept. (If the FindMe™ data is not replicated with Cisco TMS, if the Cisco VCS is ever clustered the FindMe™ data from the Cisco VCS will be lost).

This procedure upgrades the Cisco VCS:

1. Backup the Cisco VCS.

   Note: You should backup your system before upgrading. If you later need to downgrade to an earlier release you will have to restore a backup made against that previous release.

2. Enable maintenance mode.
   Log in to the Cisco VCS as admin (SSH, telnet or serial), and at a command prompt, type:
   ```
   xConfiguration SystemUnit Maintenance Mode: On
   ```
3. Wait for all calls to clear and registrations to timeout.
   - If necessary, manually remove any calls that do not clear automatically (**Status > Calls**, click **Select all** and then click **Disconnect**).
   - If necessary, manually remove any registrations that do not clear automatically (**Status > Registrations > By device**, click **Select all** and then click **Unregister**).
4. Upgrade and restart the Cisco VCS (**Maintenance > Upgrade**).

   Note: The web browser interface may timeout during the restart process, after the progress bar has reached the end. (This may happen if the Cisco VCS initiates a disk file system check – which it does approximately once every 30 restarts.)

The upgrade is now complete and all Cisco VCS configuration should be as expected.

Upgrading from older releases

- It is not possible to upgrade from releases prior to X5.1 to X6.n. You must first upgrade to X5.2 and then to X6.n. See the X5.2 release note, document reference D50582, for details.

Checking for updates and getting help

Cisco recommends registering your product at http://www.tandberg.com/services/video-conferencing-product-registration.jsp in order to receive notifications about the latest software and security updates. New feature and maintenance releases are published regularly, and we recommend that your Cisco VCS software is always kept up to date.

If you experience any problems when configuring or using your Cisco VCS, consult the online help (available within the UI of your Cisco VCS) for an explanation of how its individual features and settings work. If you cannot find the answer you need, check on the web site at http://www.tandberg.com/support to make sure that your Cisco VCS is running the most up-to-date software and for further relevant documentation.

You or your reseller can get help from our support team by raising a case at http://www.tandberg.com/support/video-conferencing-online-support.jsp. Make sure you have the following information ready:

- The serial number and product model number of the unit
- The software build number which can be found on the product user interface
- Your contact email address or telephone number
- Details of the problem, including a description of what you observed and what you had expected to happen

References and related documents

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

Name	Document reference
Cisco VCS Administrator Guide	D14049
Cisco VCS Command Reference	D14754
Cisco VCS Getting Started Guide	D14350
Cisco VCS Deployment Guide – Cluster creation and maintenance	D14367
Cisco VCS Deployment Guide – Basic Configuration – Single Cisco VCS Control	D14524
Cisco VCS Deployment Guide – Basic Configuration – Cisco VCS Expressway with Cisco VCS Control	D14651
Cisco VCS Deployment Guide – Cisco VCS Starter Pack Express	D14618
Cisco VCS Deployment Guide – FindMe	D14525
Cisco VCS Multiway Deployment Guide	D14366
Cisco TMS Provisioning Deployment Guide 13.0	D14368
Cisco VCS Deployment Guide – Cisco Unified Communications Manager with Cisco VCS using a SIP trunk	D14602
Cisco VCS Deployment Guide – Microsoft OCS 2007 (R1 and R2) and Cisco VCS Control	D14269
Cisco VCS Deployment Guide – Microsoft OCS 2007, Cisco VCS Control and Cisco AM GW	D14652
Cisco VCS Deployment Guide – Authenticating Cisco VCS accounts using LDAP	D14526
Cisco VCS Deployment Guide – Certificate Creation and use with Cisco VCS	D14548
Cisco VCS Deployment Guide – ENUM dialing on Cisco VCS	D14465
Cisco VCS Deployment Guide – VCS and Cisco Unity Connection Voicemail Integration	D14809
Cisco VCS Deployment Guide – Authenticating Devices	D14819
Cisco TMS Release Note 13.0	D14741
Cisco TMS Installation Guide 13.0	D14389
Cisco TMS Administration Guide 13.0	D13741
Cisco TMS Provisioning Troubleshooting Guide	D14427

Appendix A — Supplemental notes

AES encryption support

The Cisco VCS uses one of the following software files for X4.0 or later software, where x<y_y_y> represents the software version (for example x610 represents X6__1).

Software	Software file properties
s42700x<y_y_y>	Supports AES
s42701x<y_y_y>	Does not support AES

Network support

The Cisco VCS is an H.323 and SIP compliant device and is designed to be connected to an 802.3 IP network.

The first (or with dual network interface option, the first two) 802.3 Ethernet ports are used which are labeled LAN 1 (and LAN 2); the remaining two are currently unused. The Ethernet interfaces on the Cisco VCS support both manual configuration and auto speed and duplex detection for 1000Mbit Full Duplex, 100Mbit Full or Half Duplex or 10Mbit Full or Half Duplex.

It is recommended that speed and duplex setting should be set to auto unless the Ethernet switch that the Cisco VCS is connected to doesn't support auto-negotiation, if manually configured, ensure that full duplex is configured.

SIP RFCs

The following RFCs are supported within the VCS X6.1 release:

RFC	Description
1889	RTP / RTCP
2327	SDP
2976	SIP INFO method
3261	Session Initiation Protocol
3263	Locating SIP Servers
3264	An Offer/Answer Model with the Session Description Protocol (SDP)
3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
3326	The Reason Header Field for the Session initiation Protocol (SIP)
3265	Session Initiation Protocol (SIP) – Specific Event Notification
3327	Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts
3515	Refer method
3581	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
3856	A Presence Event Package for the Session Initiation Protocol (SIP)
3863	Presence Information Data Format (PIDF)
3880	Call Processing Language (CPL): A Language for User Control of Internet Telephony Services

RFC	Description
3891	Replaces header
3892	Referred-by header
3903	Session Initiation Protocol (SIP) Extension for Event State Publication
3944	H.350 Directory Services
4028	Session Timers in the Session Initiation Protocol
4479	A Data Model for Presence
4480	RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)
5245	Interactive Connectivity Establishment (ICE)
5626	Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)

Getting the software

Customers should contact their Cisco maintenance provider for support and assistance with their Cisco products, including release keys and software files.

Web site	www.cisco.com

Initial installation

Initial configuration of the Cisco VCS IP address, subnet and gateway can be accomplished through the installation wizard via the serial port or through the front LCD panel.

Layer 4 ports used

The following IP Layer 4 ports are used by the Cisco VCS:

Function	Type	Direction
SSH (Includes SCP)	22 TCP	Host → Cisco VCS
Telnet	23 TCP	Host → Cisco VCS
HTTP / XML	80 TCP	Host → Cisco VCS
HTTPS / XML	443 TCP	Host → Cisco VCS
SNMP (queries)	161 UDP	Host → Cisco VCS
NTP	123 UDP	↔
Syslog	514 UDP	Cisco VCS → Host
LDAP communication	389 TCP	↔
LDAPS communication	636 TCP	↔
TMS cluster replication	443 TCP	Cisco TMS ↔ Cisco VCS
SSH cluster replication	22 TCP	Cisco VCS ↔ Cisco VCS
IPSEC cluster communication	500 UDP	Cisco VCS ↔ Cisco VCS
Intra-cluster communication	4369:4380 TCP	Cisco VCS ↔ Cisco VCS
Device provisioning	389 TCP	Cisco TMS → Cisco VCS
Device provisioning replication	8989 TCP	Cisco TMS → Cisco VCS

VCS database and TMS Agent	4444 TCP	Host → Cisco VCS
Gatekeeper discovery*	1718 UDP	Host → Cisco VCS
Gatekeeper RAS*	1719 UDP	↔
Incoming H.323 setup*	1720 TCP	Host → Cisco VCS
H.225/Q.931 call setup (non-traversal)*	15000:19999 TCP	↔
H.323 call signaling for Assent/H.460 traversal**	6001 UDP	Host → Cisco VCS
SIP call signaling for Assent traversal**	7001 TCP	Host → Cisco VCS
H.225/Q.931 call setup (Assent)*	2776 TCP	Host → Cisco VCS
H.225.Q931 call setup (H.460.18)*	1720 TCP	Host → Cisco VCS
H.245 call control (non-traversal)*	15000:19999 TCP	↔
H.245 call control (Assent)*	2776 TCP	Host → Cisco VCS
H.245 call control (H.460.18)*	2777 TCP	Host → Cisco VCS
H.323 / SIP media (RTP, RTCP) (non-traversal)*	50000:52399 UDP	↔
Media (Assent, H.460.19 multiplexed media)*	2776:2777 UDP	Host → Cisco VCS
Media (H.460.19 non-multiplexed media)*	50000:52399 UDP	Host → Cisco VCS
SIP call signaling*	5060 UDP	Host → Cisco VCS
SIP call signaling*	5060 TCP	Host → Cisco VCS
SIP call signaling*	5061 TLS	Host → Cisco VCS
SIP media (Assent)	2776:2777 UDP	Host → Cisco VCS
TURN services*	3478 UDP	Host → Cisco VCS
TURN media*	60000:61200 UDP	Host → Cisco VCS
Ephemeral port range	40000:49999 TCP	Cisco VCS → Host
Outbound SIP connections*	25000:29999 TCP	Cisco VCS → Host

* All of these ports are default settings. Any ports denoted with * may be manually reconfigured, if desired. However, you are recommended not to adjust these ports unless specifically needed.

** These ports are the default settings for the first configured traversal zone. Each additional traversal zone increments the port values by 1. Any ports denoted with ** may be manually reconfigured, if desired. However, you are recommended not to adjust these ports unless specifically needed.

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.