



Cisco TelePresence Movi

Administrator Guide

D14410.09

April 2011

Software version 4.2.0.10318

Contents

Introduction	5
Prerequisites	6
Infrastructure requirements	6
NTLM authentication client requirements	6
PC requirements	7
Mac requirements	7
Multimedia device requirements	7
Microphone	7
Camera	7
Obtaining the setup files	8
Configuring the client	9
Pre-configuration	9
Advanced settings	9
Using DNS	9
Windows client pre-configuration	10
Registry settings	10
Using the Windows installer	10
Mac OS X client pre-configuration	11
Installer tools	11
Provisioning the client	12
Uploading provisioning templates to Cisco TMS	12
Provisioning options	12
Distributing and installing the setup file	17
New deployment	17
Upgrading	17
Upgrading to Cisco TelePresence Movi 4.2 from versions older than 4.1	17
Default file locations	18
Launching Movi calls from other applications	19
Testing the protocol handler	19

Use cases.....	19
How communication works.....	20
SIP communication.....	20
Media communication.....	20
Port ranges.....	20
Duo video–Binary Floor Control Protocol (BFCP).....	21
Traversal calls.....	21
Media routing.....	21
Media routing without ICE.....	21
Media routing with ICE.....	21
Enabling ICE.....	21
Configuring Movi's TURN port.....	22
Running the client.....	23
Signing in.....	23
Subscribing to the Cisco VCS.....	23
Registering to the Cisco VCS.....	23
Movi is registered to the Cisco VCS.....	23
Presence.....	23
SIP keep alive.....	24
Losing connection.....	24
Searching for a contact.....	24
Call setup.....	24
Encryption.....	25
Sent and received bandwidth.....	25
Resolution.....	25
Video and audio standards.....	26
Far-end camera control and ICE negotiation.....	27
During a call.....	27
Multiway initiation.....	27
Muting media streams.....	27

Automatic bandwidth adaptation.....	27
Automatic CPU adaptation.....	28
Conference information.....	28
Checking for updates and getting help.....	30
Related documents.....	31

Introduction

This guide provides comprehensive information on Cisco TelePresence Movi, its capabilities and functions.

Movi works in conjunction with other Cisco videoconferencing infrastructure products, primarily the Cisco TelePresence Video Communication Server (Cisco VCS), the Cisco TelePresence Management Suite (Cisco TMS) and provisioning. Some knowledge of these products is assumed in this document.

The [References and related documents](#) section contains a list of documents referred to in this guide.

Cisco TelePresence Movi for Windows is a certified Windows 7 application.

Prerequisites

Infrastructure requirements

Movi requires the Provisioning option on the Cisco VCS and in Cisco TMS to be enabled.

Product	Version required
Cisco TelePresence Management Suite (Cisco TMS)	12.6 or later
Cisco Video Communication Server (Cisco VCS)	X5.2 or later X6.0 or later for ICE support X6.1 or later for NTLM support

NTLM authentication client requirements

Movi now supports authentication with Active Directory and NTLM. For instructions on deploying NTLM authentication with Movi and Cisco VCS, refer to the *Authenticating Devices Cisco TelePresence Deployment Guide*.

Note that to use Movi for NTLM authentication with Cisco VCS, NTLMv2 must be supported by the client computer.

This requirement is especially important to be aware of if there are older computers and/or Windows XP users in your network.

On the client computer:

1. Go to **My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa**
2. If the **LmCompatibilityLevel** setting (REG_DWORD) is **1**, set to 2 or higher.
3. Save your changes.

WARNING: With a setting of **1**, authentication will fail for the client, and no warnings or error messages will be received from Cisco VCS, which passes the request on to the Active Directory server.

PC requirements

Processor	A processor supporting SSE3 (such as Pentium 4 Prescott) or better. For business-quality HD video, we recommend using the Cisco PrecisionHD™ USB camera and a 2 GHz Core 2 Duo processor or better.
Memory	512MB RAM or more.
Operating system	<ul style="list-style-type: none">■ Windows XP SP2 or later■ Windows Vista SP1 or later■ Windows 7
Connection	IP network connection (broadband, LAN, wireless). At least 24 kbps is required for an audio connection. For a video connection, the recommended minimum is 128 kbps.
Graphics card	OpenGL version 1.2 or higher. Hardware support for DirectX 8 or higher.
Sound card	Any standard sound card (full-duplex, 16-bit or better) should work with Movi.

Note: On computers with limited processing power and/or memory, Movi will use a lot of system resources, and reduced performance can be expected.

Mac requirements

Processor	Any Intel processor. For business-quality HD video, Cisco recommends using the Cisco PrecisionHD™ USB camera and a 2 GHz Core 2 Duo processor or better.
Operating system	Mac OS X 10.6 or later is recommended. Ensure that the latest security updates are installed.
Connection	IP network connection (broadband, LAN, wireless). At least 24 kbps is required for an audio connection. For a video connection, the recommended minimum is 128 kbps.

Multimedia device requirements

Microphone

All microphones work well with Movi. Note that some cameras have built-in microphones.

Camera

Movi works with most common web cameras. See the Cisco Knowledge Base for [updated information on Movi and cameras](#).

Obtaining the setup files

When a new version of Movi is available, you will get a Cisco TMS ticket if:

1. Automatic update checking is enabled. To do this:
 - a. In Cisco TMS, go to **Administrative Tools > Configuration > Network Settings**.
 - b. Under **Automatic Software Update**, set **Automatically Check for Updates** to Yes.
2. Cisco TMS Agents are enabled. To do this:
 - a. In Cisco TMS, go to **Administrative Tools > Configuration > General Settings**.
 - b. Set **Enable TMS Agents** to Yes.

The description field of the Cisco TMS ticket includes a link to a .zip archive containing the files described below.

File name	Description
Movi<version>.msi	For organizations creating their own Movi installer for Windows
MoviSetup<version>.exe	Ready-made installer for Windows containing the .msi file
MoviSetup<version>.dmg	Application bundle for Mac OS X
MoviProvisioningConfigTemplate<version>.xml	Adds Movi provisioning configurations to Cisco TMS. See the Provisioning the client section for more information.
Movi_Release_Notes_<version>.pdf	Software release notes describing the changes from the last to the current version of Cisco TelePresence Movi.

Configuring the client

This section describes the configuration settings that Movi requires to operate, and makes recommendations on how to configure these settings.

Pre-configuration

We recommend that administrators create an installation file with pre-configured Advanced settings, as described in the sections [Windows client pre-configuration](#) and [Mac OS X pre-configuration](#) below.

With a pre-configured Movi installer, **Advanced** settings will be populated automatically. The client will know how to locate and authenticate with the provisioning server on first startup, without users having to worry about servers and domains.

Settings can be defined per individual computer user or per host computer. Movi will look for user-specific configurations first.

Advanced settings

Network communication settings are available by clicking **Advanced** in Movi's sign-in window.

Setting	Description
SIP Domain	Identical to the SIP domain configured on the Cisco VCS, in VCS configuration > Protocols > SIP > Domains .
Internal VCS	The DNS address of the Cisco VCS Control cluster you want to connect to. Movi will always look for this address first when connecting. It is possible to specify which port on the Cisco VCS Movi should connect to. For example InternalVCS.example.com:5063.
External VCS	The DNS address of the Cisco VCS Expressway cluster you want Movi to connect to. If Movi fails to connect to the Internal VCS, it will try this address. It is possible to specify which port on the Cisco VCS Movi should connect to. For example ExternalVCS.example.com:5063.

Using DNS

Movi can use IP or DNS addresses to locate the Cisco VCSs.

Using DNS addresses offers advantages such as:

- Redundancy: if you have more than one Cisco VCS, using a DNS that translates to the IP address of all Cisco VCSs will enable Movi to "fail over" to other Cisco VCSs in case of a fault in one Cisco VCS.
- Location awareness: for global companies, it is possible to configure the DNS servers so that Movi will be directed to the "local" Cisco VCS wherever it may be.
- Flexibility: using DNS makes it possible to change the IP address of your Cisco VCS later on.

Movi also supports DNS SRV records, which allow for even greater redundancy and flexibility because they contain information such as "Priority" and "Weight".

Windows client pre-configuration

Registry settings

Movi registry keys can be used to preconfigure the Windows client. They are located at:

- **HKEY_LOCAL_MACHINE\Software\Cisco\Movi\2.0**: default settings for all users on the computer
- **HKEY_CURRENT_USER\Software\Cisco\Movi\2.0**: settings for a specific user on the computer

Note: The "2.0" registry keys are valid for all versions of Movi (starting with version 2.0).

Value name	Type	Example value data
InternalVcs	REG_SZ	internal.example.com
ExternalVcs	REG_SZ	external.example.com
Domain	REG_SZ	example.com

Using the Windows installer

In addition to the standard **MsiExec.exe** public properties, the Movi installer supports the following public properties for pre-configuration of the client. Note that the configurations will be written to the registry for the host computer (see above).

Public property	Description
DOMAIN	Corresponds to SIP Domain in the Advanced settings.
EXTERNALVCS	Corresponds to External VCS in the Advanced settings.
INTERNALVCS	Corresponds to Internal VCS in the Advanced settings.
HIDEADVANCEDLOGIN	A value of 1 hides the Advanced settings link in the Movi client sign-in screen. Cisco recommends using this setting so that end users will not be able to make changes to the Advanced settings.
USEWINDOWSUSERNAME	<p>A value of 1 has the following effects:</p> <ul style="list-style-type: none"> ■ Movi uses the current Windows user's logon name as username ■ The Username and Password fields are disabled. ■ The Remember my Username/Password check boxes in the login window are selected and disabled. ■ The Clear sign-in link is disabled. <p>For information on how to disable authentication on the Cisco VCS and Cisco TMS Agent, contact your support representative.</p>

MoviSetup.exe

The **MoviSetup.exe** file supplied by Cisco is a basic InstallShield-generated installer.

MoviSetup.exe can be run with standard InstallShield switches. In addition, by using the format `/v"<properties>"`, **MoviSetup.exe** will be made to run **MsiExec.exe** to set these properties.

For example, from the command line or script, run:

```
MoviSetup.exe /s /v"/qn DOMAIN=example.com  
HIDEADVANCEDLOGIN=1 "
```

Explanation:

- **/s** is a basic InstallShield switch that hides the initialization dialog.
- **/v"<properties>"** passes the properties to the **MsiExec.exe** that is actually performing the installation, see above.
- **/qn** is a basic **MsiExec.exe** switch, an instruction to install silently.
- **DOMAIN=example.com** sets the **SIP Domain** field in the Advanced settings of the Movi client to example.com.
- **HIDEADVANCEDLOGIN=1** hides the Advanced settings link in the Movi client sign-in screen.

Mac OS X client pre-configuration

The Movi client for Mac OS X can be preset by installing Movi and setting the **Preferences** files, which are located at:

- **Library/Preferences/Cisco.Movi.plist**—default settings for the computer (corresponding to LOCAL_MACHINE on Windows)
- **~/Library/Preferences/Cisco.Movi.plist**—defines the default settings per user on the computer

Preferences may be configured by using the **defaults** tool. For example, set the SIP domain by starting Terminal and typing:

```
defaults write Cisco.Movi Domain example.com
```

Explanation:

- **write** sets a new value (to erase an existing value, use **delete**)
- **Cisco.Movi** specifies the file to write to
- **Domain** is the name of the preference you want to modify, in this case corresponding to the **SIP Domain** in Movi's Advanced settings
- **example.com** is the value you want to set for the preference specified

Installer tools

To prepare a pre-configured installer for Mac OS X, we recommend using a tool such as PackageMaker, which is part of the Mac OS X Developer tools. For more information, refer to the [PackageMaker User Guide](#).

Provisioning the client

Note: Before provisioning, Cisco TMS and Cisco VCS must be configured appropriately. See the *Cisco TelePresence Provisioning Deployment Guide* for detailed information.

Provisioning is a powerful tool for the administrator to control the Movi clients. Upon subscribing to the Cisco VCS, the Movi client will receive provisioning information from the Cisco TMS Agent and act on it.

To access the Cisco TMS provisioning configurations, go to **Systems > Provisioning > Directory** and the **Configurations** pane.

Uploading provisioning templates to Cisco TMS

Each version of Cisco TelePresence Movi comes with a provisioning template that must be uploaded to Cisco TMS.

1. Go to **Systems > Provisioning > Directory**.
2. Click the link **Manage Configuration Templates**.
3. In the dialog box that opens, click the button **Upload New**.
4. Locate the **MoviProvisioningConfigTemplate<version>.xml** file on your computer (see [Obtaining the setup files](#)).
5. Click **Open**, and the template will be uploaded to Cisco TMS.

For more on managing provisioning templates, see the *Provisioning deployment guide*.

Provisioning options

The following table details the provisioning options available, including tips on how they can be used and in which situations.

The "Default" column in the table describes how Movi behaves if no specific provisioning information is configured by the administrator.

Note: "Public" provisioning options apply to Movicients connecting from outside of the organization's network. Unless values for the "public" settings are explicitly configured, they will be inherited from their "non-public" counterparts.

Field	Default	Description
ClearPath	<i>On</i>	ClearPath is a Cisco TelePresence solution that minimizes the negative effects of packet loss in a non-optimal network. Among the mechanisms used are H.264-specific error recovery techniques, feedback from decoders and forward error correction (FEC). Both call participants must support ClearPath for it to take effect.

Field	Default	Description
Default Mediatype Candidate	<i>Host</i>	<p>The address to use before ICE negotiation has completed, if ICE fails, or if the remote side does not understand ICE. The available options are:</p> <ul style="list-style-type: none"> ■ <i>Host</i> - the local network address ■ <i>Rflx</i> - the corporate public IP address seen from the outside of the organization's network (public IP) ■ <i>Relay</i> - the address of the TURN relay server <p><i>Relay</i> is typically needed when Movi is deployed in environments where most other endpoints do not understand ICE. See Enabling ICE for more information.</p>
Encryption Policy	<i>Auto</i>	<p>Determines the encryption policy for the account. This configuration affects both the SIP communication (Transport TLS or TCP) and the media communication (SRTP or no SRTP).</p> <p>See Encryption for more information.</p>
Far End Camera Control	<i>On</i>	<p>This setting lets Movi control far end cameras, when allowed by the far end.</p>
ICE	<i>Off</i>	<p>Interactive Connectivity Establishment (ICE) dynamically discovers the best possible path for media to travel between call participants.</p> <p>See Media routing for more information on what is required to enable this setting.</p>
IP version	<i>4</i>	<p>Available options:</p> <ul style="list-style-type: none"> ■ <i>Auto</i> ■ <i>4</i> ■ <i>6</i> <hr/> <p>WARNING: Do not force Movi to use IPv6 unless all users are permanently on an IPv6 network. Users who sign in over IPv4, for example from a home network, will otherwise be rejected.</p> <hr/> <p>Also note that ICE is not supported with IPv6 for Movi. When Movi signs in over an IPv6 connection, ICE will be disabled.</p>
Maximum In Bandwidth	512 kbps (adjustable to up to 2014 kbps from within the client)	<p>Determines the maximum bandwidth that can be received/sent by the account. The Movi client will be set to send the provisioned value. With no provisioning, the default starting level is lower than the maximum that can be set by the user.</p> <p>High bandwidth is directly related to good video quality, but bandwidth control can be useful to prevent a client from trying to receive/send beyond its capacity, as this may result in packet loss, jitter and general low video quality.</p>
Maximum Out Bandwidth	384 (adjustable to up to 2014 kbps from within the client)	

Field	Default	Description
Media Port Range End	21900	The upper/lower bound of the port numbers that are used in the video and audio communication.
Media Port Range Start	21000	These can be configured to control security/firewall issues. A range of minimum 10 ports must be provisioned, or Movi will revert to default.
MNS Mode	<i>Off</i>	Enabling this option forces relayed media to be relayed via private HD links with guaranteed capacity to ensure quality of video. This setting relies on ICE being enabled. Private dedicated links are provided by companies such as Media Network Services.
Multiple Server Connections	<i>Off</i>	Enable this option to allow Movi to keep open connections with several servers in a cluster, and failover by transferring automatically to the next server in the cluster should one server go down. Should one connection be lost, Movi will also be reachable from multiple servers. Note that the feature can only be enabled if SIP Outbound (RFC 5626) is supported by the backend. For Cisco VCS, this requires version X6.0 or later.
Multiway Participant URI		When Multiway is initiated, participants are directed to this Uniform Resource Identifier (URI). See Multiway initiation for more information.
OS X Software URL		URL linking to the setup file for the new version of the Movi client for Mac OS X. Note: Current versions of Cisco TMS do not support uploading files with the .dmg extension. The Movi installer must therefore either be added using the file system or hosted on a different server. The combination of this and the OSX Software Version setting allows the administrator to inform Movi users that a new version is available, and provide a clickable link from within the client to the setup file.
OS X Software Version		Indicates the version number of the new Movi client for Mac OS X. The setting should indicate the version that the users will have once they have upgraded, including software build number. The complete version number is included on the front page of the release notes for each version.
Phone Book Server URI	If no value is set, the Movi client will not be able to search for contacts.	Enables the account to search for other accounts in the Cisco TMS Agent database. This configuration should be a URI on the form: phonebook@<sip_domain>.com
Presence Server URI	If no value is set, the Movi client will not be able to publish presence and will appear offline.	Enables the account to send presence status. This configuration should be a URI on the form: presence@<sip_domain>.com

Field	Default	Description
Public Default Mediatype Candidate	Uses the value set for Default Mediatype Candidate (changes dynamically).	<p>The address to use before ICE has completed, if ICE fails or if the remote side does not understand ICE. The available options are:</p> <ul style="list-style-type: none"> ■ <i>Host</i> - the local network address ■ <i>Rflx</i> - the corporate public IP address seen from the outside of the organization's network (public IP) ■ <i>Relay</i> - the address of the TURN relay server <p><i>Relay</i> is recommended for Movi clients connecting from outside of the organization's network. ICE negotiation can take a few seconds to complete, and using the TURN relay will help media flow through the firewalls from the beginning of the call. Once ICE negotiation has completed, media will be redirected if a superior media path has been located. See Enabling ICE for more information.</p>
Public IP version	Uses the value set for IP Version (changes dynamically).	<p>Available options:</p> <ul style="list-style-type: none"> ■ <i>Auto</i> ■ 4 ■ 6 <hr/> <p>WARNING: Do not force Movi to use IPv6 unless all users are permanently on an IPv6 network. Users who sign in over IPv4, for example from a home network, will otherwise be rejected.</p> <hr/> <p>Also note that ICE is not supported with IPv6 for Movi. When Movi signs in over an IPv6 connection, ICE will be disabled.</p>
Public Maximum In Bandwidth	Uses Maximum In Bandwidth (changes dynamically).	<p>Determines the maximum bandwidth that can be received/sent by the account after connecting to the external Cisco VCS configured in Movi's Advanced settings.</p> <p>The settings may be useful for controlling the bandwidth of users that connect from outside of the company's network. These users may have slow network connections, or the company may want to limit their bandwidth usage.</p>
Public Maximum Out Bandwidth	Uses value set for Maximum Out Bandwidth (changes dynamically).	
Public Multiple Server Connections	Uses the value set for Multiple Server Connections (changes dynamically).	<p>Enable this option to allow Movi to keep open connections with several servers in a cluster, and failover by transferring automatically to the next server in the cluster should one server go down. Should one connection be lost, Movi will also be reachable from multiple servers. Note that the feature can only be enabled if SIP Outbound (RFC 5626) is supported by the backend. For Cisco VCS, this requires version X6.0 or later.</p>
Public Phone Book Server URI	Uses value set for Phone Book Server URI (changes dynamically).	<p>Enable the account to search for other accounts in the Cisco TMS Agent database after connecting to the external Cisco VCS configured in Movi's Advanced settings.</p> <p>It is sufficient to set the Phone Book Uri configuration.</p>

Field	Default	Description
Public Presence Server URI	Uses value set for Presence Server URI (changes dynamically).	Enables the account to send presence status after connecting to the external Cisco VCS configured in Movi's Advanced settings. It is sufficient to set the Presence Book Uri configuration.
Public SIP Server Address	Uses value set for SIP Server Address (changes dynamically).	Address of the server to which the user should send a register request after connecting to the external Cisco VCS configured in Movi's Advanced settings. Generally, this configuration should be the same as External VCS in the Movi Advanced settings.
Resolution Preferences	<i>High</i>	Restricts incoming and outgoing video resolution. Windows users may modify Movi's video resolution with the provisioned value as the maximum. The Mac OS X client will always use the provisioned value. The restrictions depend on many factors, but as a general rule: <ul style="list-style-type: none"> ■ <i>High</i> will allow the highest resolution possible up to widescreen HD (1280x720). ■ <i>Medium</i> will restrict resolutions to wide CIF (512x288) or lower. ■ <i>Low</i> will restrict resolutions to wide QCIF (256x144) or lower. See Resolution for more on how video resolution is determined by Movi.
SIP Keep Alive Interval	24 seconds	The interval at which SIP Keep Alive messages are sent. For more information, see Movi is registered to the Cisco VCS .
SIP Listening Port		
SIP Server Address	The SIP server (Cisco VCS) that the client subscribed to.	Address of the server the user should send a register request to. Should be the same as the Internal VCS configuration in the Movi Advanced settings.
TurnAuthPassword		TURN server settings that are required for enabling ICE. See Enabling ICE for more information.
TurnAuthUsername		
TurnServer		
Windows Software URL		URL linking to the setup file for the new version of the Movi client for Windows. The combination of this and the Software Version setting allows the administrator to inform Movi users that a new version is available, and provide a clickable link from within the client to the setup file.
Windows Software Version		Indicates the version number of the new Movi client for Windows. The setting should indicate the version that the users will have once they have upgraded, including software build number. The complete version number is included on the front page of the release notes for each version.

Distributing and installing the setup file

This section describes the process of distributing and installing the Movi client, whether this is the first installation of Cisco TelePresence Movi or an upgrade from a previous version.

Note: Installing Movi requires administrative rights on the computer.

New deployment

For new deployments, Cisco recommends that you use your own deployment tools.

To distribute to end users, you can send a customized email message from TMS:

1. Go to **Systems > Provisioning > Directory**.
2. In the **Workspace** pane, click **Send Account Info**.
3. In the dialog that opens, click **Configure email settings**.
4. Verify that SMTP host, username, and password have been added correctly, or add them yourself.
5. Choose a suitable subject for the email notification.
6. By default, this email message will contain login credentials for Movi and Cisco TelePresence System E20. If you want users to download and install Movi themselves, you can add the download link to the same message.

Upgrading

The process of upgrading Movi is controlled by the IT administrator through four provisioning options in Cisco TelePresence Management Suite:

- **Windows Software URL** and **OS X Software URL**
- **Windows Software Version** and **OS X Software Version**

When these two options are correctly configured, users can upgrade their own Movi client by clicking a link in the application, which downloads the setup file for the new version.

This method presents users with a choice to upgrade their Movi client. If you want to make absolutely sure that all clients are upgraded, you can instead opt to use your deployment tool(s) to force the upgrade.

Upgrading to Cisco TelePresence Movi 4.2 from versions older than 4.1

Due to the changes in product name and brand, the Movi 4.2 installer will make some changes to previous installations. The installer will uninstall whichever previous version of Movi is present on the system, and the program file and icons are completely removed. However, all profile folders and files are kept intact on uninstall.

Movi will then install itself to the program file paths described under [File locations](#).

When Movi is launched:

- Windows: Existing profile folders and registry settings are renamed from `~\TANDBERG\~` to `~\Cisco\~`.
- Mac OS X: The `com.tandberg.Movi.plist` file is renamed to `com.cisco.Movi.plist`

Note: Movi 4.2 will also install itself as the operating system's default SIP protocol handler, see the section [Launching Movi from other applications](#).

Default file locations

Files	Windows location	Mac OS X location
Program file	<ul style="list-style-type: none"> Windows Vista and 7 (64 bit): %Program Files (x86)%\Cisco\ Windows Vista and 7 (32 bit) : %Program Files%\Cisco\ Windows XP: ~\Program Files\Cisco\ 	/Applications/Cisco TelePresence Movi
Favorites and History	%APPDATA%\Cisco\Movi\2.0	~/Library/Application Support/Movi
Log files for debugging purposes	<p><CSIDL_LOCAL_APPDATA>\Cisco\Movi\2.0\Logs\.</p> <p>The <CSIDL_LOCAL_APPDATA> directory is hidden by default and can be found at</p> <ul style="list-style-type: none"> Windows XP: %USERPROFILE%\Local Settings\Application Data\ Windows Vista and Windows 7: %LOCALAPPDATA% (typically %USERPROFILE%\AppData) 	~/Library/Logs/Movi

On a Windows computer, the Favorites and History are individual to each user logging on to Movi.

On Mac OS X, the Favorites and History are specific to the Mac user account, regardless of which Movi user is logged in.

Launching Movi calls from other applications

Movi will install itself as the default SIP protocol handler on the operating system. As long as Movi remains the default SIP client, activating any SIP URI link will launch a call from Movi.

It is also possible to use "movi:" as the protocol rather than "sip:". This will ensure that Movi is always used even if another SIP client is the system default.

Testing the protocol handler

1. Have the latest version of Cisco TelePresence Movi installed
2. Open a web browser (or a keyboard launch application such as Quicksilver or Launchy).
3. In the input (URL) field, type a SIP URI, then hit **Enter**.

Movi will now open and launch a call to the URI provided.

Note: Adding "/" after the "movi:" and "sip:" protocols is not supported by the Movi protocol handler.

Use cases

- Add SIP URIs to default employee email signatures and vcards.
- Embed SIP URI links in intranet employee profiles, helpdesk contact pages, and similar.
- Integrate with any application that can send a protocol request to the operating system.

How communication works

This section includes general information on Movi's main types of communication and is essential for the subsequent section, which describes specific messages.

SIP communication

Movi communicates with the Cisco VCS using the Session Initiation Protocol (SIP). Subscribing, registering, presence querying, call invites—all communication except video and audio, is done in SIP. SIP messages are sent using TCP, with or without TLS encryption depending on the provisioned settings.

The default SIP listening ports used on the Cisco VCS are

- 5060 (unencrypted)
- 5061 (encrypted)

These are both configurable. Go to **VCS Configurations > Protocols > SIP > Configuration** to change the listening ports.

Note: If you change the SIP listening port number on the Cisco VCS, you must also configure the Movi clients to contact the Cisco VCS on this port. See Advanced settings for more information.

Movi itself will use ephemeral TCP ports for this communication. These ports are handed over to the Movi client by the TCP stack and are not configurable.

To enable communication with endpoints and other devices that rely on H.323 and do not support SIP, interworking on the Cisco VCS can be used.

Media communication

Media data is transferred through up to nine UDP links (ports). There are at most five media streams:

- Audio
- Primary video
- Secondary video (presentation sharing)
- BFCP (management of presentation sharing/duo video, see below)
- Far end camera control (FECC)

With the exception of BFCP, each of these streams requires two links: one link for RTP packets and one link for RTCP packets. The SRTP protocol is used if encryption is enabled.

Port ranges

The default port range for Movi to receive media is 21,000-21,900. This range is configurable in Cisco TMS:

1. Go to **Systems > Provisioning > Directory**.
2. Add (or select) the configuration's Media Port Range Start and Media Port Range End.

Note: A minimum range of 10 ports must be configured, or Movi will revert to default.

The default port range used on the Cisco VCS is 50,000-52,399. To configure:

1. Go to **VCS Configuration > Local zone > Traversal subzone**.
2. Set the Traversal media port start and Traversal media port end.

Note that in both cases, the port numbers used will be consecutive, but chosen randomly within the specified range.

Duo video—Binary Floor Control Protocol (BFCP)

Movi supports BFCP for handling the control of duo video. BFCP communication can be sent over a UDP or a TCP link. Movi uses the same ports as for audio and video for this communication.

On the Cisco VCS, a port will be chosen at random from the same range that has been assigned to the media links.

Traversal calls

Media links can be established directly between the two endpoints in non-traversal calls, or between Movi and the Cisco VCS in traversal calls. As a general rule, non-traversal calls are defined as calls between two participants that are on the same network and do not require interworking.

Note that SIP to H.323 calls require interworking and are therefore traversal calls irrespective of whether the endpoints are on the same network. For detailed information, see the latest Cisco VCS Administrator guide.

Media routing

Cisco TelePresence Movi supports Interactive Connectivity Establishment (ICE) for better media routing. ICE will be used if enabled both in Movi and the far end.

Media routing without ICE

When the ICE protocol is used in a call, media links are established directly between the two endpoints in non-traversal calls, or between Movi and the VCS in traversal calls. As a general rule, non-traversal calls are defined as calls between two participants that are on the same network and that don't require interworking.

Note that SIP to H.323 calls require interworking and are therefore traversal calls irrespective of whether the endpoints are on the same network. For detailed information, see the latest VCS Administrator Guide.

Media routing with ICE

ICE dynamically discovers the best possible path for media to travel between call participants.

It is possible to further improve the routing of media and force it through dedicated links by using the **Enable MNS Mode** Provisioning configuration.

Enabling ICE

Media routing using ICE requires a TURN server. VCS Expressway running version X5.2 or later can function as a TURN server if it has TURN Relay licenses. Having the TURN server option key is required.

To start setting up the Cisco VCS Expressway, go to **VCS configuration > Expressway > TURN** and configure the fields as described below.

Setting	Change to
TURN services	<i>On</i>
Port	<i>3478</i>
Media port range start	<i>60000</i>
Media port range end	<i>61399</i>

To finish setup on the Cisco VCS Expressway:

1. Go to **VCS configuration > Authentication > Devices > Configuration** and set the **Database type** to *LocalDatabase*.
2. Go to **VCS configuration > Authentication > Devices > Local database** and create a username and password. The username and password are necessary to allow for use of TURN Relay licenses. The Movi client is provisioned with the username and password as described below.

To enable ICE on the Movi client, go to **Systems > Provisioning > Directory** and the **Configurations** pane for Movi, then update the fields as described below.

Setting	Change to
Enable ICE	<i>On</i>
TurnAuthPassword	Password created when setting up the Cisco VCS Expressway
TurnAuthUsername	Username created when setting up the Cisco VCS Expressway
TurnServer	The address of the server media is relayed through in an "ICE call", typically the address of the Cisco VCS Expressway

Note: The ICE Provisioning configurations are not available by default. See the [Provisioning](#) section for more information.

Configuring Movi's TURN port

TURN port configuration should be controlled through DNS. Movi will do an SRV lookup for the TURN ip, pri, weight, and port. As TURN runs over UDP, the lookup will be for `_turn._udp.<domain>`. If no SRV record for TURN is found, Movi will perform an A record lookup (IPv4) or an AAAA lookup (IPv6), but will default to port 3478.

If the port needs to be provisioned, you can append it to the IP address in the **TurnServer** field, for example `192.0.2.0:3478`.

Running the client

Movi is designed to be straight forward and easy to use, but as a highly versatile tool it also has many hidden configurations and features of use to the administrator. This section details these options so that you as an administrator will know how to make the most of these features. It also provides an overview of Movi's communication with the servers, which should help you identify which part of the process to troubleshoot if you are having problems with your setup.

Signing in

Movi will attempt to sign in to a Cisco VCS according to its **Advanced** settings, whether pre-configured or provided manually. The sign-in stages are described below.

Subscribing to the Cisco VCS

Movi first attempts to subscribe to the internal Cisco VCS configured in its Advanced settings. If this fails, for example because the user's computer is connected to the public internet, Movi will try to subscribe to the external Cisco VCS.

However, if the internal Cisco VCS is a DNS address that translates to more than one IP address, Movi will attempt to connect to all these IP numbers before trying the external Cisco VCS. If the DNS server contains SRV records, Movi will adhere to the priority and weight of the IP addresses, otherwise they will be tried in random order.

Typically, the Cisco VCS or the Cisco TMS Agent will challenge the first subscription message. Movi will answer this challenge by sending another SUBSCRIBE message with the authentication information.

After the subscription has been authenticated, the Cisco TMS Agent will send provisioning information to the Movi client.

Registering to the Cisco VCS

Movi will register to the Cisco VCS according to the provisioning configuration in Cisco TMS; SIP Server URI or Public SIP Server URI. If this provisioning configuration is identical to the Advanced setting in the Movi client (recommended), Movi will register to the same Cisco VCS it subscribed to. As long as the client is registered, the Cisco VCS will know to forward messages to the client.

After initial registration, Movi will continue to send registration messages to the Cisco VCS according to the Registration expire delta setting under **VCS configuration > Protocols > SIP > Configuration**. Movi will send the message after 75% of the specified time interval has elapsed.

Movi is registered to the Cisco VCS

After Movi has signed in, a number of tasks are performed continuously.

Presence

The presence status service is provided by the Cisco VCS. Movi publishes its own presence to the Cisco VCS and subscribes to presence statuses for any SIP URIs the user has stored as favorites.

Subscribing to the presence status of a contact informs the Cisco VCS that the client should be notified when the contact's presence status changes.

In **Applications > Presence** there are two settings that determine timeouts for the Presence server:

- **Subscription expiration time**
- **Publication expiration time**

Movi will subscribe and publish when 75% of the specified time intervals have elapsed. The client will be automatically subscribed to the presence status of any contact that is added.

In addition to these periodic messages, Movi will also publish presence information when the user's status has been changed, either manually or because the user is in a call.

See the "Presence" section of the [Cisco VCS Administrators Guide](#) for more information about the presence server.

SIP keep alive

To make sure that the connection between the Movi client and the Cisco VCS remains open and does not get closed by a firewall as an idle connection, Movi sends SIP Keep Alive messages.

By default the interval for these messages is 24 seconds. To configure the SIP Keep Alive Interval:

1. In Cisco TMS, go to **Systems > Provisioning > Directory**.
2. Click on the group or user you want to provision and find the **Configurations** pane.
3. Change the **SIP Keep Alive Interval** configuration if it exists, or add one

Losing connection

If Movi gets an indication that the connection has been lost or is unable to continue registering to the Cisco VCS, Movi will sign out and display the sign-in screen.

If the **Sign in automatically** box is checked, Movi will attempt to sign in again. The first attempt will be one second after connection got lost, the second attempt after two, the third after four, then eight and next sixteen. From the ninth attempt onwards, Movi will try to sign in only once every 5 minutes, to prevent putting too much strain on system resources.

Searching for a contact

Every time a user types a character in the search field of the Movi client, Movi queries the TMS Agent on the Cisco VCS, and the TMS Agent answers with matching results.

Note: Phone book search results are determined by the Cisco VCS/TMS Agent and dependent on Cisco VCS version.

When a search result is selected, Movi will also query the Cisco VCS for the presence status of that contact.

Call setup



Call setup is communicated using SIP messages passed through the Cisco VCS. The following describes how the call's attributes are determined during call setup.

Encryption

For a call to be encrypted, both the SIP and the media communication must be encrypted, and all parties must support encryption. Encrypted media communication is sent using the Secure Real-time Transport Protocol (SRTP) with a 128-bit Advanced Encryption Standard (AES).

The Encryption policy setting is provisioned to the client as configured in **Systems > Provisioning > Directory** in Cisco TMS.

- *Force TLS/TCP* determines whether the SIP communication is encrypted (TLS) or not (TCP). The TLS version used by Movi is currently 1.0.
- *Force/No Srtp* determines whether the media communication is encrypted or not.
- *Auto* means the Movi client will try to have an encrypted call, but if not possible, it will allow the call to be unencrypted.

Note: Users can tell whether their current call is encrypted by the icon in the information bar at the top of the video window.  means the call is encrypted,  means it is unencrypted.

Sent and received bandwidth

During call setup Movi signals the maximum bandwidth it would like to receive according to the settings in the client. It is up to the system on the other end of the call to respect this signaling.

Both the maximum bandwidth to be sent during call and the bandwidth sent at the start of the call are determined at call setup.

During the call, Movi can change and send more or less bandwidth, but never more than the maximum bandwidth decided during call setup.

Maximum bandwidth sent

To determine the maximum bandwidth to be sent, Movi chooses the lowest of these two values:

- Max outgoing bandwidth, configured in the Movi client's settings
- Max incoming bandwidth restriction from the far end

Bandwidth sent at the start of the call

To determine the initial bandwidth for a new call, Movi uses its traffic data history, pulled from a database of your last 250 calls. The calls are indexed by the network locations from which the calls were made. Based on what Movi knows about the network and the far end SIP URI, a "safe" initial bandwidth is chosen.

The database resides in the Windows user profile:

- Windows XP: %userprofile%\Local Settings\Application Data\Cisco\Movi\2.0
- Windows Vista and Windows 7: %userprofile%\AppData\Local\Cisco\Movi\2.0

Resolution

Note: High image resolution is not the only factor linked to high video quality. Frame rate, scene lighting and optical quality of the cameras used in the conference are also important.

Resolution preferences

The **Resolution Preferences** provisioning setting limits the resolution for both incoming and outgoing video. See [Provisioning the client](#).

Movi for Windows treats the provisioned value as the maximum, with end-user configuration available through the client's settings. Users with older Windows computers with limited system resources may need to lower the resolution setting for their Movicient to ensure that it runs smoothly.

Note: It is up to the far end to obey restrictions on incoming video.

Outgoing video resolution

Movi determines which resolution to send according to the following criteria:

- Movi must be able to get the resolution in native format from the camera.
- Priority is given to resolutions that can be received from the camera at 30 frames per second.
- The resolution must be permitted by Movi's own settings, as described above.
- The resolution must be permitted by the receiving end.
- Sending high resolution at low bandwidth will result in poor quality. The bandwidth sent must be sufficient for the resolution:
 - HD (1280x720) requires a minimum of 1200 kbps.
 - VGA (640x480) requires a minimum of 442 kbps.Increasing the bandwidth further will improve image quality. Bandwidth permissions are controlled by the **Maximum Out Bandwidth** settings, see [Provisioning the client](#).

If HD resolution is not achieved despite sufficient bandwidth as described above, this can usually be attributed to one or both of the following:

- Issues with network connection, including packet loss
- Adaptation due to high CPU usage by Movi. See [Automatic CPU adaptation](#).

Incoming video resolution

Bandwidth permissions for incoming video are controlled by the **Maximum In Bandwidth** settings, see [Provisioning the client](#). The bandwidth required for incoming HD video will vary with the capabilities and limitations of each far-end endpoint.

Note that even with an HD-capable endpoint at the far end and no restrictions on bandwidth, network connection issues, such as packet loss, may still cause incoming video not to achieve HD resolution.

Presentation resolution

The maximum resolution for a shared presentation is dependent on the video codec used (H.263/H.263+/H.264), the available bandwidth and the capabilities of the far end.

For a Movi-to-Movi call on unlimited bandwidth, the presentation resolution would be 1280x800.

The resolution for presentations is not configurable.

Video and audio standards

Movi supports both sending and receiving the standards described below. Movi will always use the best standard that is supported by the far end.

Audio

- MPEG4/AAC-LD
- G.722.1
- G.711

Note: If the bandwidth available is less than 192kbps and the far end supports G.722.1 at 24kbps, Movi will send that protocol in order to free up bandwidth for better video quality.

Video

- H.264
- H.263+
- H.263

Far-end camera control and ICE negotiation

Once the call has been established, far-end camera control (FECC) and ICE are negotiated if enabled and supported by both call participants.

Please note that:

- FECC negotiations may take several seconds. The **FECC** button in the Movi client is enabled once negotiations are complete.
- ICE negotiations take a couple of seconds and require nine TURN server licenses; one license for each media link.

During a call

Once a call has been set up, there are a number of actions that can be prompted in Movi, either as a result of a user action or as an automated response to changing conditions.

Multiway initiation

Multiway is the ability for a user to join calls and seamlessly create a multi-participant conference. If multiway is initiated by the user, the current call is put on hold (there has to be at least one other call already on hold) and all the endpoints are redirected to a multi-conference system according to the **Multiway Participant URI** provisioning option.

Muting media streams

If the camera or microphone is muted, Movi allocates the bandwidth for the other media links to use. This means that if the user does not have enough bandwidth for two video streams, it is possible to mute one video stream and improve the quality of the other stream.

To prevent the unused link from being closed (for example by a firewall), Movi sends STUN keep alive messages every 7 seconds.

Automatic bandwidth adaptation

In case of a Movi client sending or receiving bandwidth which exceeds the network capabilities, high packet loss may occur and the user may experience poor call quality. Movi uses automatic bandwidth

adaptation mechanisms to tackle bandwidth issues.

Note: Automatic adaptations take time. Configuring the client to fit the network and system capabilities is always recommended.

Automatic CPU adaptation

Running Movi with the highest video quality on a less powerful computer might result in 100% CPU usage and a poor call quality. Movi monitors the CPU usage of the computer.

If CPU usage exceeds 95% for 10 seconds or more:

- if Movi is responsible for less than 90% of the CPU usage, it will display a warning asking the user to close other applications.
- if Movi is responsible for 90% or more of the CPU usage, it will lower the resolution for the video picture sent.

Note: Automatic adaptations take time. Configuring the client to fit the network and system capabilities is always recommended.

Conference information

When moving the cursor over the video window, an information bar appears at the top. Clicking the **i** button opens **Conference information**, an overview of outgoing (transmit) and incoming (receive) traffic data.

Field name	Description
Max allowed bitrate	Restrictions taken from Movi's settings.
Signaled bitrate	The signaled bitrate combines Movi's restrictions with those from the far end.
Configured bitrate	The configured bitrate varies based on automatic bandwidth adaptation. This value is not transmitted to the far end.
Encryption	This field is blank if no encryption is used.
Protocol	The video and audio standards currently in use.
Resolution	The current outgoing and incoming resolution. This value changes based on automatic adaptation.
Bitrate	The actual bandwidth sent and received, which will always be equal to or lower than the configured bitrate.
Total packet loss	Number of packets lost during the call so far.
Current packet loss	Percentage of packets lost in the last five seconds (transmit) or three seconds (receive).

Field name	Description
Post FEC total	Number of packets recovered (FEC = forward error correction) by ClearPath.
Post FEC current	Percentage of packets recovered by ClearPath in the last three seconds.
Jitter	Jitter is a continuously calculated estimate of the mean deviation of the difference in transit time of adjacent packets. The transmit jitter information is based on RTCP reports from the far end. High jitter affects the call quality and is usually indicative of poor network conditions.

Checking for updates and getting help

We recommend 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 software is always kept up to date.

If you experience any problems when configuring or using the product, consult the documentation at <http://www.tandberg.com/support/video-conferencing-documentation.jsp> for an explanation of how its individual features and settings work. You can also check the support site at <http://www.tandberg.com/support/> to make sure you are running the latest software version.

You or your reseller can also get help from our support team by raising a case at <http://www.tandberg.com/support/>. Make sure you have the following information ready:

- The software build number which can be found in the product user interface (if applicable).
- Your contact email address or telephone number.
- The serial number of the hardware unit (if applicable).

Related documents

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

Document title	Document reference
<i>Cisco TelePresence Movi Release Notes 4.2</i>	D14835
<i>Cisco TelePresence Movi for Windows User Guide</i>	D14409
<i>Cisco TelePresence Movi for Mac User Guide</i>	D14733
<i>Authenticating Devices Cisco TelePresence Deployment Guide</i>	D14819
<i>Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)</i> http://tools.ietf.org/html/rfc5626	RFC 5626
<i>PackageMaker User Guide</i> http://developer.apple.com/library/mac/#documentation/DeveloperTools/Conceptual/PackageMakerUserGuide/	N/A

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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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.

© 2011 Cisco Systems, Inc. All rights reserved.