



Microsoft OCS 2007, Lync 2010, Cisco VCS and Cisco AM GW Deployment Guide

**Cisco VCS X7.0
Microsoft OCS 2007 R2, Lync 2010
Cisco AM GW 1.0, 1.1**

D14652.04

October 2011

Contents

Document revision history	4
Introduction	5
New features in AM GW 1.1	6
Prerequisites to setting up a Cisco AM GW	7
Required configuration information	7
Configuring the Cisco VCS	8
Cisco VCS in B2BUA mode.....	8
Specify the Cisco AM GWs: B2BUA mode	8
Configure the Cisco AM GWs as trusted hosts: B2BUA mode.....	8
Cisco VCS in non-B2BUA mode	9
Configure the neighbor zone to the Cisco AM GW: non-B2BUA mode.....	9
Specify the Cisco AM GW zone: Non-B2BUA mode	10
Specify the Cisco AM GW routing policy.....	12
What should I allow?	12
Configuring the Cisco AM GW	14
Network port A settings	14
DNS settings.....	14
Network services	15
System settings	15
Resource settings.....	16
Time.....	17
Proxies.....	17
Shut down and restart the Cisco AM GW.....	18
Requirements and usage of MOC/Lync client	19
PC requirements.....	19
Increasing the resolution of a MOC/Lync client call	19
Appendix 1 – Troubleshooting.....	21
Cisco VCS and OCS/Lync.....	21
Cisco VCS search history and Status > Calls	21
MOC/Lync client debug	21
OCS/Lync debug	21
Cisco VCS / Cisco AM GW.....	21
Cisco VCS search history and Status > Calls	21
Cisco AM GW Event log.....	21
Cisco AM GW SIP log	22
Cisco AM GW CDRs	22
Appendix 2 – Known limitations	23
Restrictions	23
Duo Video.....	23

Simultaneous answer	23
AVMCU / livemeeting calls	23
Removed restrictions	23
Call transfer	23
Multiway	23
OCS/Lync Edge Server	23
Encrypted calls	23
Calls from OCS clear after 22 minutes.....	24
Appendix 3 – Reaching Cisco AM GW capacity	25
Appendix 4 – Bandwidth control	26
Non-B2BUA mode	26
B2BUA mode	26
Appendix 5 – Call license usage.....	27
Non-B2BUA mode	27
B2BUA mode	27
Appendix 6 – Endpoint specific configuration	28
AMGW 1.0	28
AMGW 1.1	28
Appendix 7 – Communicator for MAC.....	29

Document revision history

The following table summarizes the changes that have been applied to this document.

Revision	Date	Description
1	April 2010	Initial release.
2	November 2010	New document styles applied.
3	February 2011	Updated for VCS X6.1.
4	October 2011	Major revision to cover Cisco VCS X7.0 (including B2BUA), Microsoft Lync 2010 and Cisco AM GW 1.1.

Introduction

The Unified Communications (UC) gateway for OCS/Lync is the combination of the "OCS/Lync gateway" Cisco TelePresence Video Communication Server (Cisco VCS) and the Cisco TelePresence Advanced Media Gateway (Cisco AM GW).

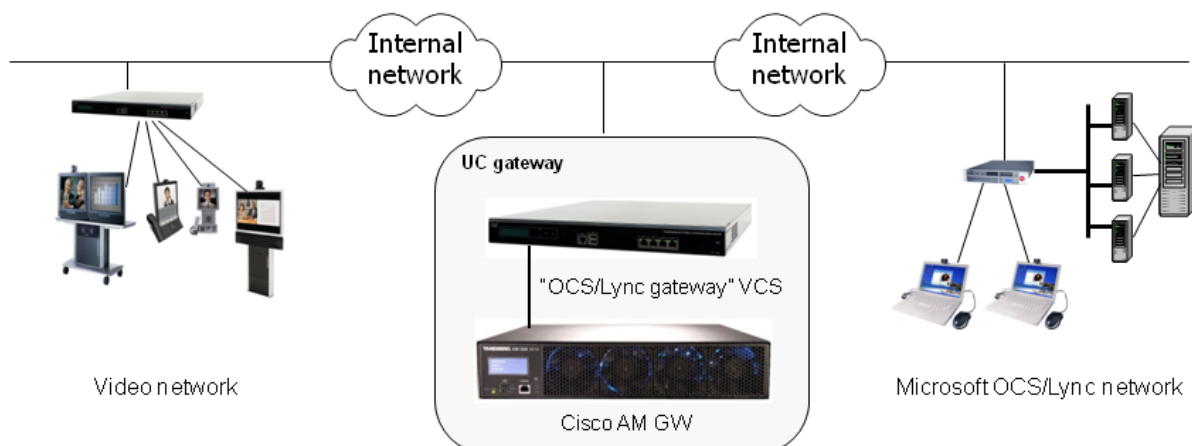
The addition of the Cisco AM GW to the "OCS/Lync gateway" VCS allows traditional video codecs such as H.261, H.263 and H.264 to be converted to and from the Microsoft RT Video codec. Use of the RT Video codec allows a MOC/Lync client to scale its displayed image from CIF resolution, through VGA to 720p.

The Cisco AM GW enhances the video experience by upscaling the video format sent from OCS/Lync clients. Upscaling only occurs if ClearVision is enabled on the AM GW (it is disabled by default).

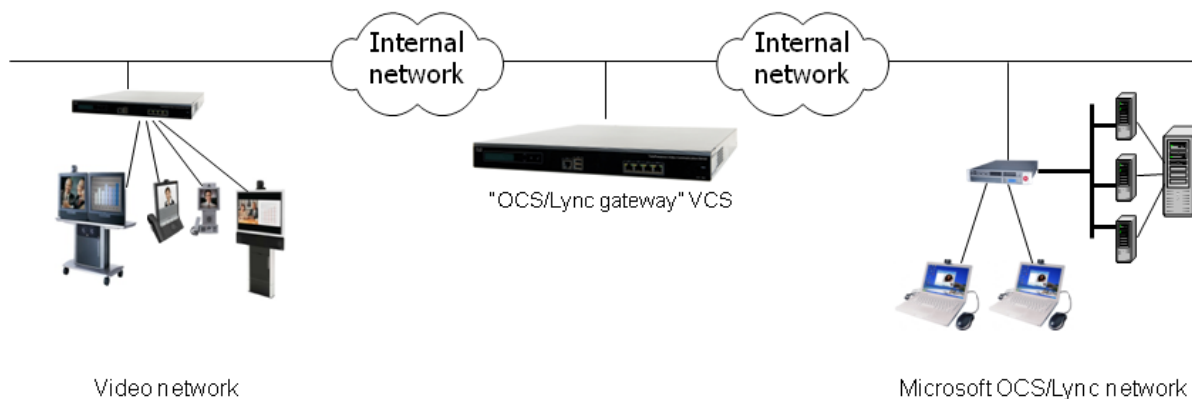
Resolution sent from Microsoft client	Upscaled resolution
CIF (352x288)	4CIF (704x576)
VGA (640x480)	XGA (1024x768)
HD (1280x720)	not applicable (remains 1280x720)

Use of the Unified Communications gateway is essential if Communicator for MAC clients is used – MAC clients do not support any traditional video codecs; they only support RT Video, hence to have video communications the Cisco AM GW is needed to transcode the video.

The deployment of the UC gateway should be as shown:



This builds upon the deployment described in [Microsoft OCS 2007, Lync 2010 and Cisco VCS X7.0 deployment guide](#) which created the architecture as shown:



For small test and demo systems the “OCS/Lync gateway” VCS can be used as the main routing Cisco VCS in the video network, though use of a standalone UC gateway is recommended – see the section ‘Why add an “OCS/Lync gateway” VCS Control?’ in [Microsoft OCS 2007, Lync 2010 and Cisco VCS X7.0 deployment guide](#).

This deployment guide describes how to add the Cisco AM GW to an existing “OCS/Lync gateway” VCS deployment.

For additional information about the Cisco AM GW see the [Cisco AM GW Getting Started Guide](#).

New features in AM GW 1.1

AM gateway 1.1 introduces the following new features:

- With OCS 2007 R2, MOC Client and Communicator for MAC 2011 are supported
- Lync Server is supported
- With Lync Server 2010, Lync Client 2010 and Communicator for MAC 2011 are supported
- Encryption is supported (to use encryption with OCS/Lync the Cisco VCS must have the Enhanced OCS Collaboration option key installed)

Prerequisites to setting up a Cisco AM GW

The prerequisites for setting up a Cisco AM GW are:

- Microsoft OCS must be Microsoft OCS 2007 R2.
- Microsoft Lync must be Microsoft Lync 2010.
- The “OCS/Lync gateway” VCS must be running version X5.1.1 or later. Use of VCS X6.1 or later is required for operation with Microsoft Lync 2010. Use of VCS X7.0 or later and the B2BUA is required for operation with Microsoft Edge Server.
- The Cisco AM GW must be running version 1.0 or later if used with OCS; the Cisco AM GW must be running version 1.1 or later if used with Lync.
- The Cisco AM GW must be running version 1.1 or later if used with the VCS B2BUA.
- The “OCS/Lync gateway” VCS can be a Cisco VCS Control or a Cisco VCS Expressway.
- Cisco VCS architecture configured with an “OCS/Lync gateway” VCS as described in [Microsoft OCS 2007, Lync 2010 and Cisco VCS X7.0 deployment guide](#).

Required configuration information

Item	Notes for your reference
Address of one or more Cisco AM GWs – IP address or DNS name	
List of URIs allowed to use the Cisco AM GW to get enhanced video (if there is to be a limit on personnel using this resource)	
IP address of Cisco AM GW	
Subnet mask for Cisco AM GW	
Default gateway address for Cisco AM GW	
IP address of DNS server for Cisco AM GW	
NTP (time) server address – IP address or DNS name	
IP address or DNS name of “OCS/Lync gateway” VCS - standalone Cisco VCS or cluster peer 1	
IP address or DNS name of “OCS/Lync gateway” VCS - cluster peer 2 (if it exists)	
IP address or DNS name of “OCS/Lync gateway” VCS - cluster peer 3 (if it exists)	
IP address or DNS name of “OCS/Lync gateway” VCS - cluster peer 4 (if it exists)	
IP address or DNS name of “OCS/Lync gateway” VCS - cluster peer 5 (if it exists)	
IP address or DNS name of “OCS/Lync gateway” VCS - cluster peer 6 (if it exists)	

Configuring the Cisco VCS

Cisco VCS in B2BUA mode

Specify the Cisco AM GWs: B2BUA mode

1. Go to the **Transcoders** page (**Applications > B2BUA > Transcoders**) and click **New**.

2. Configure the fields as follows:

Address	IP address or FQDN of the AM gateway
Port	IP port on the Cisco AM GW – typically 5061 (for TLS)

3. Click **Create transcoder**.
4. Repeat for all transcoders that the VCS will use (up to a total of 6 transcoders).

Note: if the Cisco AM GWs (transcoders) reach their capacity, any calls that would normally route via the Cisco AM GW will not fail but will be routed directly. Any calls that are routed directly will not be able to support the higher resolutions in MOC/Lync client.

Configure the Cisco AM GWs as trusted hosts: B2BUA mode

1. Go to the **Microsoft OCS/Lync B2BUA trusted hosts** page (**Applications > B2BUA > Microsoft OCS/Lync > B2BUA trusted hosts**) and click **New**.
2. Configure the fields as follows:

IP Address	IP address of the Cisco AM GW (must not be an FQDN).
Type	<i>Transcoder</i>

3. Click **Create trusted host**.
4. Repeat for all transcoders that the VCS will use (up to a total of 6 transcoders).

Note: If the Cisco AM gateways (transcoders) reach their capacity, any calls that would normally route via the Cisco AM GW will not fail but will be routed directly. Any calls that are routed directly will not be able to support the higher resolutions in MOC/Lync client.

Cisco VCS in non-B2BUA mode

Configure the neighbor zone to the Cisco AM GW: non-B2BUA mode

Create a neighbor zone called, for example, "To AM Gateway".

1. Go to the [Zones](#) page ([VCS configuration > Zones](#)).
2. Click **New**. You are taken to the **Create zone** page.
3. Configure the fields as follows:

Name	For example "To AM Gateway"
H.323 Mode	<i>Off</i>
H.323 Port	1719
SIP Mode	<i>On</i>
SIP Port	5061
SIP Transport	<i>TLS</i>
TLS verify mode	<i>Off</i>
Accept proxied registrations	<i>Deny</i>
Authentication policy	Configure this setting according to your authentication policy
SIP authentication trust mode	<i>Off</i>
Peer 1 address	Address of first Cisco AM GW
Peer 2 .. 6 addresses	Addresses of any additional Cisco AM GWs
Zone profile	Cisco Advanced Media Gateway

4. Click **Create Zone**.

Status System **VCS configuration** Applications Maintenance ? 0m

Create zone You are here: [VCS configuration](#) > [Zones](#) > Create zone

Configuration

Name * i

Type * i

Hop count * i

H.323

Mode i

Port * i

SIP

Mode i

Port * i

Transport i

TLS verify mode i

Accept proxied registrations i

Authentication

Authentication policy i

SIP authentication trust mode i

Location

Peer 1 address i

Peer 2 address i

Peer 3 address i

Peer 4 address i

Peer 5 address i

Peer 6 address i

Advanced

Zone profile i

Specify the Cisco AM GW zone: Non-B2BUA mode

This is where you select the Cisco AM GW zone to use, and decide whether to set up policy rules to control which calls can use the Cisco AM GW.

1. Go to the **Advanced Media Gateway configuration** page (**VCS configuration > Advanced Media Gateway > Configuration**).
2. Configure the fields as follows:

Advanced Media Gateway zone	Select the zone that you configured for the Cisco AM GWs e.g. "To AM Gateway"
Policy mode	By default (where Policy mode is <i>Off</i>) all calls to or from OCS/Lync are sent via the selected Cisco AM GW zone. If you want to limit which calls go via the Cisco AM GW, set the Policy mode to <i>On</i> and then set up policy rules to deny

specific calls based on alias pattern matches as described in the next section.
Off: all OCS/Lync calls go via the Cisco AM GW.
On: allows control over which OCS/Lync calls go via the Cisco AM GW.

3. Click **Save**.

The screenshot shows the Cisco TelePresence Video Communication Server Control interface. The top navigation bar includes 'Status', 'System', 'VCS configuration', 'Applications', and 'Maintenance'. The 'VCS configuration' tab is active. Below the navigation bar, the page title is 'Advanced Media Gateway configuration'. The main configuration area is titled 'Configuration' and contains two settings: 'Advanced Media Gateway zone' set to 'To AM Gateway' and 'Policy mode' set to 'Off'. Both settings have a dropdown arrow and an information icon. A 'Save' button is located at the bottom left of the configuration area.

Note: if the Cisco AM GW reaches its capacity, any calls that would normally route via the Cisco AM GW will not fail but will be routed directly. Any calls that are routed directly will not be able to support the higher resolutions in MOC/Lync client.

Specify the Cisco AM GW routing policy

This is where you can set up policy rules to control which calls can use the Cisco AM GW.

1. Go to the **Advanced Media Gateway policy rules** page (**VCS configuration > Advanced Media Gateway > Policy rules**).
2. Click **New**. You are taken to the **Create Advanced Media Gateway policy rule** page.
3. Configure the fields as follows:

	To configure an Allow rule e.g. allow John@company.com to use the Cisco AM GW	To configure a Deny rule e.g. deny all
Rule name	As required, e.g. "Allow John"	As required, e.g. "Deny All"
Description	Descriptive text as required	Descriptive text as required
Priority	e.g. 100	e.g. 500
Pattern type	<i>Exact</i>	<i>Regex</i>
Pattern string	e.g. John@company.com	e.g. .*
Action	<i>Allow</i>	<i>Deny</i>
State	<i>Enabled</i>	<i>Enabled</i>

Note: even when **Advanced Media Gateway policy mode** is *On*, all calls to and from OCS/Lync will still use the Cisco AM GW unless specific policy rules deny its use. When using policy, it is usual to set up a set of allow rules for allowed personnel, then at the lowest priority set up a "Deny all" rule (**Pattern type** = *Regex*, **Pattern string** = *.**)

4. Click **Create Advanced Media Gateway rule**.

The screenshot shows the Cisco TelePresence Video Communication Server Control interface. The main heading is "Create Advanced Media Gateway policy rule". Below this, there is a "Configuration" section with the following fields:

- Rule name: Text input field
- Description: Text input field
- Priority: Text input field with value "100"
- Pattern type: Dropdown menu set to "Exact"
- Pattern string: Text input field
- Action: Dropdown menu set to "Allow"
- State: Dropdown menu set to "Enabled"

At the bottom of the configuration section, there are two buttons: "Create Advanced Media Gateway rule" and "Cancel".

What should I allow?

The Advanced Media Gateway policy rules match against dialed URIs and caller IDs, i.e. both the called and calling parties.

- If MOC/Lync client and Video endpoints dial FindMe IDs then the FindMe IDs must be included in the "allowed" policy rules.
- If MOC/Lync client and video endpoints are dialed directly then the MOC/Lync client and video endpoint IDs must be included in the "allowed" policy rules.

- If MOC/Lync clients are included as devices in FindMe profiles then the MOC/Lync client URI must be included in the “allowed” policy rules (as FindMe will fork the call before the Cisco AM GW policy checks the dialed URI).

Note: if the Cisco VCS's FindMe configuration has **Caller ID** set to *FindMe ID*, it is recommended that MOC/Lync clients are not included as devices in FindMe profiles – the “OCS/Lync gateway” VCS registering FindMe users to OCS/Lync allows MOC/Lync client and video endpoints to be called simultaneously by calling a single URI.

- If the Cisco VCS's FindMe configuration has **Caller ID** set to *FindMe ID* then the FindMe IDs must be included in the “allowed” policy rules. If **Caller ID** is set to *Incoming ID* then the video endpoint IDs must be included in the “allowed” policy rules.

Configuring the Cisco AM GW

Network port A settings

1. Go to the **Port A settings** page (**Network > Port A settings**).
2. Configure the fields as follows:

IP configuration	<i>Manual</i>
IP address	Required IP address for this Cisco AM GW
Subnet mask	Subnet mask for the subnet
Default gateway	Default gateway for the subnet

3. Click **Update IP configuration**.

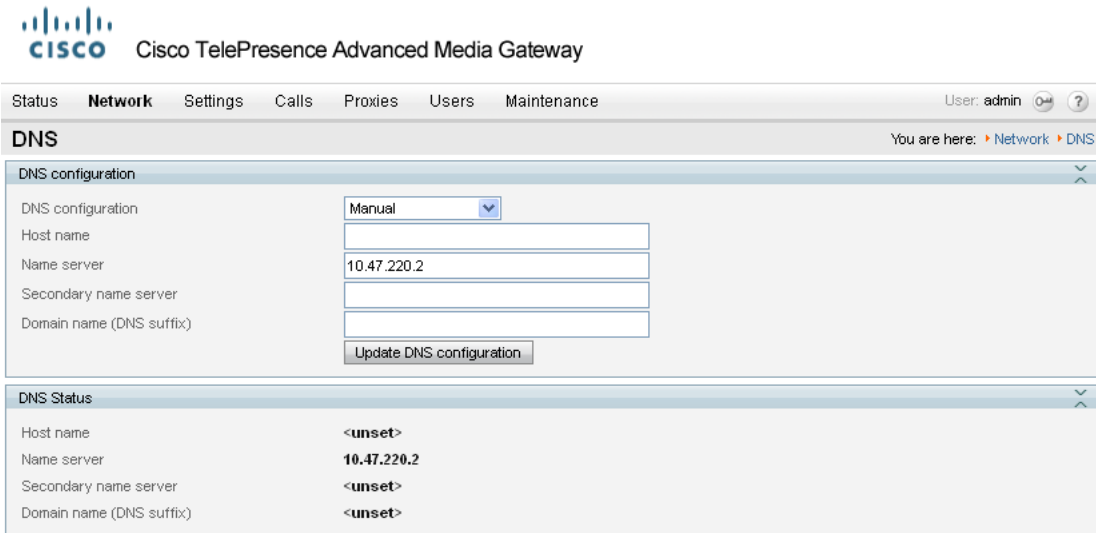
The screenshot shows the Cisco TelePresence Advanced Media Gateway web interface. The top navigation bar includes Status, Network, Settings, Calls, Proxies, Users, and Maintenance. The user is logged in as 'admin'. The main content area is titled 'Port A settings' and shows the 'Port A IP configuration' section. The 'IP configuration' dropdown is set to 'Manual'. The 'Manual configuration' section has three input fields: 'IP address' (10.47.221.101), 'Subnet mask' (255.255.252.0), and 'Default gateway' (10.47.220.1). Below these fields is a 'Update IP configuration' button. The 'Port A IP status' section below shows the current configuration: DHCP is '<not in use>', IP address is '10.47.221.101', Subnet mask is '255.255.252.0', and Default gateway is '10.47.220.1'.

DNS settings

1. Go to the **DNS** page (**Network > DNS**).
2. Configure the fields as follows:

Host name	Hostname of the Cisco AM GW (optional)
Name server	IP address of DNS server
Secondary name server	Secondary DNS server IP address (optional)
Domain name (DNS Suffix)	DNS suffix to add to a hostname to make it an FQDN (optional)

3. Click **Update DNS configuration**.

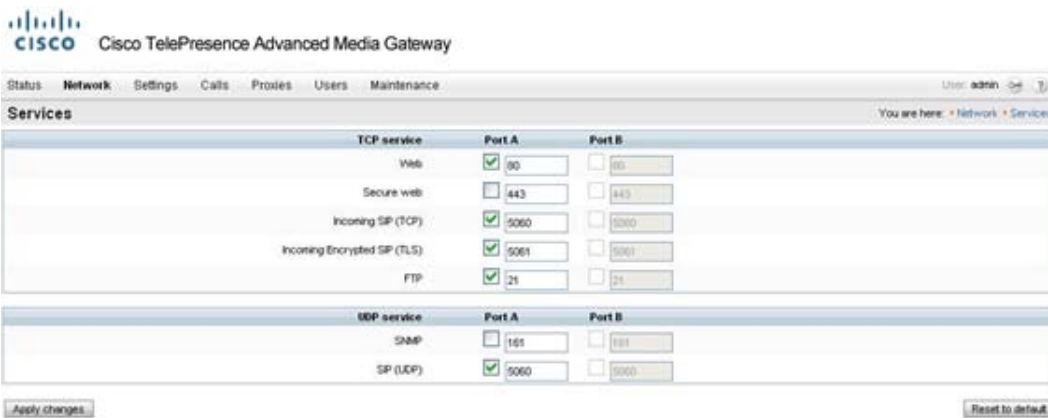


Network services

1. Go to the **Services** page (**Network > Services**).
2. Ensure that:

Incoming Encrypted SIP (TLS)	Selected ✓ and Port A = 5061
-------------------------------------	------------------------------

3. If any modification was required, click **Apply changes**.



Note: if the Incoming Encrypted SIP (TLS) option is not displayed, obtain the “Encryption” option for the Cisco AM GW and update the features in the **Feature management** section of the **Upgrade** page (**Maintenance > Upgrade**).

System settings

1. Go to the **System settings** page (**Settings > System settings**).
2. Configure the fields as follows:

Motion / sharpness tradeoff	As required, e.g. <i>Balanced</i>
Default bandwidth from AM GW	As required, e.g. 2.00 Mbit/s
Default bandwidth to AM GW	<same as transmit>

<other parameters>	As required
--------------------	-------------

3. Click **Apply changes**.

The screenshot shows the Cisco TelePresence Advanced Media Gateway web interface. The 'Settings' tab is active, and the 'System settings' page is displayed. The 'Call settings' section is expanded, showing the following configurations:

- Motion / sharpness tradeoff: Balanced
- Default bandwidth from AM GW: 2.00 Mbit/s
- Default bandwidth to AM GW: <same as transmit>
- Convert out-of-band to in-band DTMF:
- Overlay participant name:
- Welcome message: (empty text box)
- Welcome message duration: <never shows> no message set
- Allow widescreen video cropping:
- Flow control on video errors:
- Conceal video errors:
- Limit transmitted video from Communicator for Mac clients to VGA:
- Video transmit size optimization: Dynamic codec and resolution
- Video resolution selection mode: Default
- Maximum transmitted video packet size: 1400 bytes
- Audio codecs from AM GW:
 - G.711 G.722 G.722.1 G.723.1 G.728 G.729 Polycom(R) Siren7(TM)
 - Polycom(R) Siren14(TM) G.722.1 Annex C AAC-LC AAC-LD
- Audio codecs to AM GW:
 - G.711 G.722 G.722.1 G.723.1 G.728 G.729 Polycom(R) Siren7(TM)
 - Polycom(R) Siren14(TM) G.722.1 Annex C AAC-LC AAC-LD
- Video codecs from AM GW:
 - H.261 H.263 H.263+ H.264 Microsoft RTVideo
- Video codecs to AM GW:
 - H.261 H.263 H.263+ H.264 Microsoft RTVideo

The 'User interface settings' section shows 'Show video thumbnail images' checked. An 'Apply changes' button is located at the bottom of the settings area.

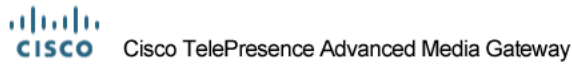
Note: some endpoints and network equipment do not support as many codecs as the Cisco AM GW can offer. For best interoperability it is recommended that at least one audio codec is left unselected in the **Audio codecs from AM GW** and **Audio codecs to AM GW** sections.

Resource settings

- Go to the **Resource settings** page (**Settings > Resource settings**).
- Configure the fields as follows:

Call capability	<p><i>Allow HD</i> – supports high definition video calls at up to 720p at 30fps</p> <p><i>SD only</i> – supports calls at up to w448p at 30fps</p> <p>The number of calls supported in the selected mode is shown. This depends on the model of AM gateway you are using.</p>
------------------------	--

3. Click **Apply changes**.



Status Network **Settings** Calls Proxies Users Maintenance User: admin

Resource settings You are here: Settings > Resource settings

Resource allocation

Call capability Allow HD

Call capacity 10 calls

Apply changes

Note: if this setting is changed the Cisco AM GW will need to be shut down and restarted (see ‘Shut down and restart the Cisco AM GW’ on page 18).

Time

1. Go to the **Time** page (**Settings > Time**).
2. Configure the fields as follows:

Enable NTP	Select this option
UTC offset	Configure as required for local time zone
NTP host	IP address or DNS name of NTP (time) server

3. Click **Update NTP settings**.

Cisco logo and Cisco TelePresence Advanced Media Gateway text

Status Network **Settings** Calls Proxies Users Maintenance Debug User: admin

Time You are here: Settings > Time

System time

Current time 15:37, October 11 2011

New time 15 : 37 New date 11 October 2011

Change system time

NTP

Enable NTP

UTC offset 0

NTP host ntp01.ciscotp.com

Update NTP settings

Proxies

1. Go to the **Proxies** page (**Proxies > Proxies**)
2. Click **Add new proxy**.
3. Configure the fields as follows:

Name	Descriptive name (for display purposes only)
Address	VCS in B2BUA mode: IP address of Cisco VCS:65080 (65080 is the default “Port on B2BUA for transcoder communications” as configured on VCS.)

	VCS in non-B2BUA mode: IP address of Cisco VCS
Outgoing transport Note: this is AM GW 1.0 only	<p><i>TLS</i></p> <ul style="list-style-type: none"> If the <i>TLS</i> option is not displayed, obtain the "Encryption" option for the Cisco AM GW and update the features in the Feature management section of the Upgrade page (Maintenance > Upgrade). AM GW 1.1 uses the same transport for outgoing messages as the transport used in the received messages.

- Click **Add proxy**.

The screenshot shows the Cisco TelePresence Advanced Media Gateway web interface. The top navigation bar includes 'Status', 'Network', 'Settings', 'Calls', 'Proxies', 'Users', and 'Maintenance'. The user is logged in as 'admin'. The main heading is 'Add new proxy'. Below this, there is a 'Proxy information' section with two input fields: 'Name' and 'Address'. An 'Add proxy' button is located at the bottom of the form.

If the Cisco AM GW is connected to a cluster of Cisco VCSs then set up proxy entries for each Cisco VCS peer in the cluster.

Shut down and restart the Cisco AM GW

The Cisco AM GW only needs to be shut down and restarted if the HD / SD setting on the **Resource settings** page has been changed. If it has been changed:

- Go to the **Shutdown** page (**Maintenance > Shutdown**)
- Click **Shutdown AM GW** and then click **Confirm AM GW shutdown**.

A red banner will appear confirming "AM GW SHUT DOWN. Restart required".

Note: if the confirm is not carried out immediately the system may timeout and the procedure above will have to be repeated.

- Click **Restart AM GW**.

"AM GW RESTART IN PROGRESS" will confirm that a restart is occurring.

Requirements and usage of MOC/Lync client

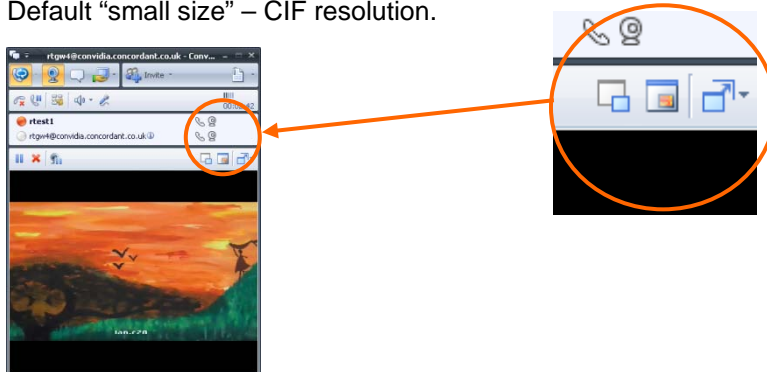
PC requirements


To support 720p RT Video operation, the MOC/Lync client needs to be running on a quad core processor PC. A dual core processor will support up to VGA resolution. Single core supports only CIF resolution.

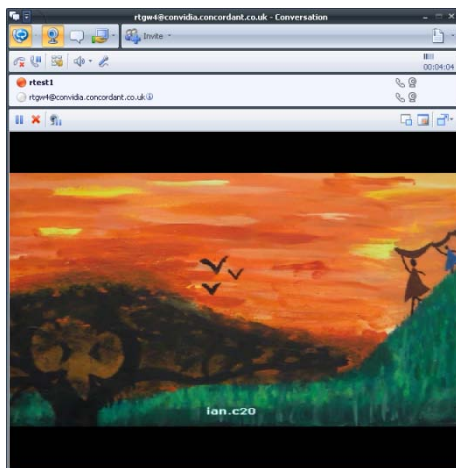
Increasing the resolution of a MOC/Lync client call


When in a call the resolution of the image (size of the picture seen on the screen) can be altered.

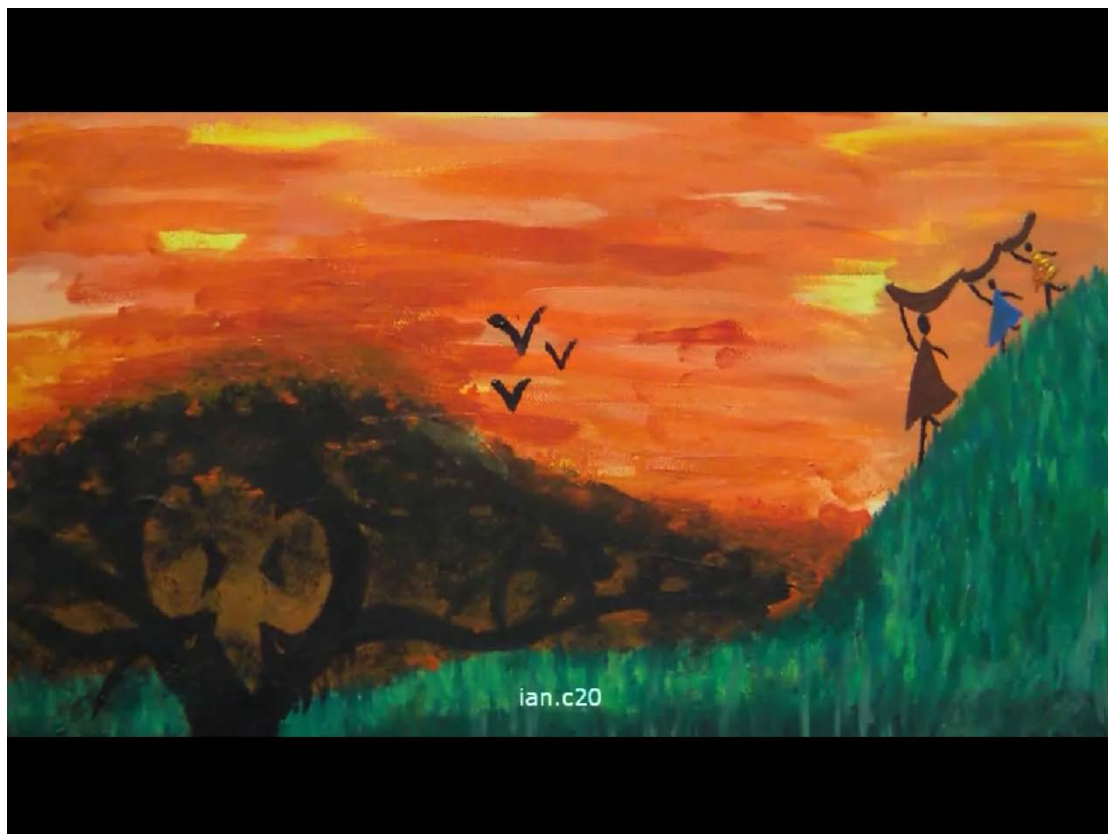
- Default “small size” – CIF resolution.



- Click the  icon and choose “large size” – this uses VGA resolution if the PC supports it.



- Click the  icon and choose “full screen” – this uses 720p resolution if the PC supports it.



From “full screen” mode, press the escape key to return to the previous “small size” or “large size” resolution – whichever was selected before “full screen” was selected.

Appendix 1 – Troubleshooting

Calls between endpoints and OCS/Lync via the UC gateway where the Cisco AM GW is not involved consist of a single call with two call legs.

- Leg a) between the endpoint and Cisco VCS
- Leg b) between Cisco VCS and OCS/Lync

Calls between endpoints and OCS/Lync via the UC gateway where the Cisco AM GW is involved consist of two calls and four call legs.

- Leg a) between the endpoint and Cisco VCS
- Leg b) between Cisco VCS and the Cisco AM GW
- Leg c) between the Cisco AM GW and Cisco VCS
- Leg d) between Cisco VCS and OCS/Lync

Cisco VCS and OCS/Lync

Troubleshooting calls between Cisco VCS and OCS/Lync is very much the same as troubleshooting any Cisco VCS / OCS/Lync call scenario. See the Troubleshooting section in [Microsoft OCS 2007, Lync 2010 and Cisco VCS X7.0 deployment guide](#).

Cisco VCS search history and Status > Calls

As a starting point, consider **Search history** and **Status > Calls** on the Cisco VCS.

Check that the calls are being made as expected.

MOC/Lync client debug

This will give the MOC/Lync client client's view of the call.

OCS/Lync debug

This will provide OCS/Lync's view of communications between OCS/Lync and Cisco VCS and OCS/Lync and MOC/Lync Client.

Cisco VCS / Cisco AM GW

Cisco VCS search history and Status > Calls

As a starting point, consider **Search history** and **Status > Calls** on the Cisco VCS.

Check that the calls are being made as expected.

Cisco AM GW Event log

The **Event log (Maintenance > Logs > Event log)** shows key events including incoming calls, connecting calls and disconnecting calls and error events.

Note: the oldest event information is shown on page 1 – the opposite order to the event information on Cisco VCS where page 1 is the most recent information.

The level of tracing (to save more or less information in the Event log) can be configured in the **Event capture filter** page (**Maintenance > Logs > Event capture filter**).

When displaying the Event log, this information or a subset of it can be displayed. In the **Event display filter** page (**Maintenance > Logs > Event capture filter**) filters can be set to remove information from the displayed log, to enable the reader to focus in on the most relevant information.

Cisco AM GW SIP log

The Cisco AM GW can perform SIP level logging. On the **SIP log** page (**Maintenance > Logs > SIP log**) select **Enable SIP logging**. Refresh the page to see the log.

Cisco AM GW CDRs

The Cisco AM GW can perform CDR logging. On the **CDR log** page (**Maintenance > Logs > CDR log**) select **Enable CDR logging**. Refresh the page or click **Update display** to see the log.

The main view shows four messages per call:

- Participant “<caller id 1>” initiated a call >>
 - clicking >> provides details of the destination of that call
- Participant “<caller id 1>” (<IP>) disconnected >>
 - clicking >> provides details of the media codecs, bandwidth and resolution used
- Participant “<caller id 2>” (<IP>) disconnected >>
 - clicking >> provides details of the media codecs, bandwidth and resolution used
- Call terminated after <time> >>
 - clicking >> provides the disconnect reason

Appendix 2 – Known limitations

See also the “Known limitations” section in document [Microsoft OCS 2007, Lync 2010 and Cisco VCS X7.0 deployment guide](#).

Restrictions

Duo Video

- Duo Video is not supported into the Microsoft OCS/Lync environment (with or without the Cisco AM GW).

Simultaneous answer

- Multiple answer is not supported – it is not recommended to have auto-answer with the same timeout enabled on multiple endpoints in any Cisco VCS OCS/Lync Relay FindMe account location.

AVMCU / livemeeting calls

- Calls to / from AVMCU and livemeeting are not supported.

Removed restrictions

Some restrictions have been removed with the upgrade of AM GW from version 1.0 to 1.1, others are removed with the use of the VCS B2BUA mode.

Call transfer

- When VCS is in B2BUA mode call transfer works as expected.
- When VCS is not in B2BUA mode, although call hold and resume work as expected, call transfer is not supported.

Multiway

- When VCS is in B2BUA mode video endpoints can add OCS/Lync clients into Multiway calls as expected.
- When VCS is not in B2BUA mode, calls using the Cisco AM GW may not be added into a Multiway call.

OCS/Lync Edge Server

- Calls to / from MOC/Lync client clients registered to OCS/Lync through an Edge Server are supported from VCS X7.0 when the B2BUA is enabled – the Enhanced OCS Collaboration option key is also needed to allow this functionality.

Encrypted calls

- Encrypted calls between OCS/Lync and the Cisco AM GW are supported from AMGW 1.1 – use with VCS X7.0 and the B2BUA – see the configuration required in [Microsoft OCS 2007, Lync 2010 and Cisco VCS X7.0 deployment guide](#).
(Using encryption with OCS/Lync also requires that the VCS has the Enhanced OCS Collaboration option key installed).

Calls from OCS clear after 22 minutes

- When VCS is in B2BUA mode, there is no 22 minute call limitation.
- When VCS is not in B2BUA mode and OCS or Lync is used, calls from MOC clients and MAC communicator to video endpoints will clear after 22 minutes due to MOC clients and MAC communicator not issuing the session refresh keepalives. (Note that this issue does not affect Lync clients; but it does affect both OCS and Lync server.)

Appendix 3 – Reaching Cisco AM GW capacity

If the call capacity of the Cisco AM GWs is reached, new calls to and from OCS/Lync will be routed directly between Cisco VCS and OCS/Lync.

The calls will succeed, but the image resolution will be limited to CIF in both directions, from MOC/Lync client to video endpoint and from video endpoint to MOC/Lync client, whatever the image size selected on MOC/Lync client.

Appendix 4 – Bandwidth control

Non-B2BUA mode

- For calls direct to OCS/Lync, bandwidth can be controlled using pipes over links to the OCS/Lync neighbor zone.
- For calls via the Cisco AM GW, bandwidth is controlled using pipes over the link to the Cisco AM GW zone.

Note: calls from the Cisco AM GW to OCS/Lync are not included in the bandwidth figures in the link to the OCS/Lync neighbor zone.

B2BUA mode

If the B2BUA is in use, bandwidth can be controlled using pipes over links to the “To Microsoft OCS/Lync Server via B2BUA” neighbor zone.

Appendix 5 – Call license usage

Non-B2BUA mode

Call type	Traversal call licenses	Non-traversal call licenses
SIP to OCS/Lync call via Cisco AM GW	1	1
H.323 to OCS/Lync call via Cisco AM GW	2	0
SIP to OCS/Lync direct from Cisco VCS	1	0
H.323 to OCS/Lync direct from Cisco VCS	1	0

B2BUA mode

Call type	Traversal call licenses	Non-traversal call licenses
SIP to OCS/Lync call via Cisco AM GW	0	1
H.323 to OCS/Lync call via Cisco AM GW	1	0
SIP to OCS/Lync direct from Cisco VCS	0	1
H.323 to OCS/Lync direct from Cisco VCS	1	0

Appendix 6 – Endpoint specific configuration

See the endpoint specific configuration appendix in document [Microsoft OCS 2007, Lync 2010 and Cisco VCS X7.0 deployment guide](#) for general settings for use of video endpoints with Cisco VCS and OCS.

AMGW 1.0

With Cisco AM GW deployments, ensure that all video endpoints are configured with:

- **Encryption** = *Off* or
- **Encryption** = *Auto* or
- **Encryption** = *Best effort*

Ensure that the endpoint is NOT configured as

Encryption = *On*

AMGW 1.1

There is no restriction on **Encryption** settings so long as the VCS and OCS/Lync have been set to operate with encryption.

Appendix 7 – Communicator for MAC

Low power MAC machines may experience high resource consumption when handling calls with video endpoints. AMGW has a configuration to limit video communications from Communicator for MAC to VGA to avoid this excessive resource usage.

To limit Communicator for MAC calls to only use VGA:

1. Go to the **Systems Settings** page (**Settings > System Settings**).
2. Configure the field as follows:

Limit transmitted video from Communicator for MAC clients to VGA	Select the tick box
---	---------------------

3. Click **Apply changes**.

Note: this will affect the video quality of calls with all Communicators for MAC.

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.