Contents

Introduction ......................................................................................................................... 4
Prerequisites ......................................................................................................................... 5
  Required configuration information ................................................................................. 5
Configuring the Cisco VCS ................................................................................................. 6
  Configure the neighbor zone to the Cisco AM GW ......................................................... 6
  Configure Cisco VCS's Advanced Media Gateway settings ........................................... 8
    Identify the Cisco AM GW zone and configure the Cisco AM GW policy .................... 8
    Cisco AM GW routing policy ....................................................................................... 9
Configuring the Cisco AM GW .......................................................................................... 11
  Network port A settings ................................................................................................. 11
  Network services .......................................................................................................... 12
  System settings ............................................................................................................ 12
  Resource settings ......................................................................................................... 13
  Time .............................................................................................................................. 13
  Proxies ......................................................................................................................... 14
  Shut down and restart the Cisco AM GW ...................................................................... 14
Requirements and usage of MOC ..................................................................................... 15
  PC requirements .......................................................................................................... 15
  Increasing the resolution of a MOC call ....................................................................... 15
Appendix 1 – Troubleshooting ......................................................................................... 17
  Cisco VCS / OCS ........................................................................................................... 17
    Cisco VCS search history and Status > Calls ............................................................... 17
    MOC debug ............................................................................................................... 17
    OCS debug ................................................................................................................. 17
  Cisco VCS / Cisco AM GW .......................................................................................... 17
    Cisco VCS search history and Status > Calls ............................................................... 17
    Cisco AM GW Event log ............................................................................................ 17
    Cisco AM GW SIP log ............................................................................................... 18
    Cisco AM GW CDRs ................................................................................................. 18
Appendix 2 – Known limitations ....................................................................................... 19
  Call transfer .................................................................................................................. 19
  Multiway ....................................................................................................................... 19
  Duo Video ..................................................................................................................... 19
  Simultaneous answer ................................................................................................. 19
  OCS Edge Server ........................................................................................................ 19
  Encrypted calls .......................................................................................................... 19
  AVMCU / livemeeting calls ....................................................................................... 19
Appendix 3 – Reaching Cisco AM GW capacity ............................................................... 20
Appendix 4 – Bandwidth control ..................................................................................... 21
Appendix 5 – Call license usage ....................................................................................... 22
Appendix 6 – Endpoint specific configuration
Introduction

The Unified Communications (UC) gateway for OCS is the combination of the “OCS 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 gateway” Cisco VCS allows traditional video codecs such as H.261, H.263 and H.264 to be converted into the Microsoft RT Video codec. Use of the RT Video codec allows MOC to scale its displayed image from CIF resolution, through VGA to 720p.

The deployment of the UC gateway should be as shown:

This builds upon the deployment described in “Cisco VCS Deployment Guide - Microsoft OCS 2007 (R1 and R2) and Cisco VCS Control (X6)” which created the architecture as shown:

For small test and demo systems the “OCS gateway” Cisco 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 gateway” Cisco VCS Control?’ in “Cisco VCS Deployment Guide - Microsoft OCS 2007 (R1 and R2) and Cisco VCS Control (X6)”.

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

For additional information on the Cisco AM GW see the “Cisco AM GW Getting Started Guide”.

---

Introduction

The Unified Communications (UC) gateway for OCS is the combination of the “OCS 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 gateway” Cisco VCS allows traditional video codecs such as H.261, H.263 and H.264 to be converted into the Microsoft RT Video codec. Use of the RT Video codec allows MOC to scale its displayed image from CIF resolution, through VGA to 720p.

The deployment of the UC gateway should be as shown:

This builds upon the deployment described in “Cisco VCS Deployment Guide - Microsoft OCS 2007 (R1 and R2) and Cisco VCS Control (X6)” which created the architecture as shown:

For small test and demo systems the “OCS gateway” Cisco 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 gateway” Cisco VCS Control?’ in “Cisco VCS Deployment Guide - Microsoft OCS 2007 (R1 and R2) and Cisco VCS Control (X6)”.

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

For additional information on the Cisco AM GW see the “Cisco AM GW Getting Started Guide”.

---
Prerequisites

- Microsoft OCS must be Microsoft OCS 2007 R2.
- The “OCS gateway” Cisco VCS must be running version X5.1.1 or later.
- The Cisco AM GW must be running version 1.0 or later.
- The “OCS gateway” Cisco VCS can be a Cisco VCS Control or a Cisco VCS Expressway.
- Cisco VCS architecture configured with an “OCS gateway” Cisco VCS as described in “Cisco VCS Deployment Guide - Microsoft OCS 2007 (R1 and R2) and Cisco VCS Control (X5)”.

Required configuration information

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

Configure the neighbor zone to the Cisco AM GW

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>For example “To AM Gateway”</td>
</tr>
<tr>
<td>H.323 Mode</td>
<td>Off</td>
</tr>
<tr>
<td>H.323 Port</td>
<td>1719</td>
</tr>
<tr>
<td>SIP Mode</td>
<td>On</td>
</tr>
<tr>
<td>SIP Port</td>
<td>5061</td>
</tr>
<tr>
<td>SIP Transport</td>
<td>TLS</td>
</tr>
<tr>
<td>TLS verify mode</td>
<td>Off</td>
</tr>
<tr>
<td>Accept proxied registrations</td>
<td>Deny</td>
</tr>
<tr>
<td>Authentication policy</td>
<td>Configure this setting according to your authentication policy</td>
</tr>
<tr>
<td>SIP authentication trust mode</td>
<td>Off</td>
</tr>
<tr>
<td>Peer 1 address</td>
<td>Address of first Cisco AM GW</td>
</tr>
<tr>
<td>Peer 2 .. 6 addresses</td>
<td>Addresses of any additional Cisco AM GWs</td>
</tr>
<tr>
<td>Zone profile</td>
<td>Cisco Advanced Media Gateway</td>
</tr>
</tbody>
</table>
4. Click **Create Zone**.
Configure Cisco VCS’s Advanced Media Gateway settings

Identify the Cisco AM GW zone and configure the Cisco AM GW policy

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 Off) all calls to or from OCS 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 On and then set up policy rules to deny specific calls based on alias pattern matches as described in the next section.
   Off: all OCS calls go via the Cisco AM GW
   On: allows control over which OCS calls go via the Cisco AM GW

3. Click Save.

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.
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:

<table>
<thead>
<tr>
<th>Rule name</th>
<th>To configure an Allow rule e.g. allow <a href="mailto:John@company.com">John@company.com</a> to use the Cisco AM GW</th>
<th>To configure a Deny rule e.g. deny all</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>As required, e.g. “Allow John”</td>
<td>As required, e.g. “Deny All”</td>
</tr>
<tr>
<td>Priority</td>
<td>e.g. 100</td>
<td>e.g. 500</td>
</tr>
<tr>
<td>Pattern type</td>
<td>Exact</td>
<td>Regex</td>
</tr>
<tr>
<td>Pattern string</td>
<td>e.g. <a href="mailto:John@company.com">John@company.com</a></td>
<td>e.g. .*</td>
</tr>
<tr>
<td>Action</td>
<td>Allow</td>
<td>Deny</td>
</tr>
<tr>
<td>State</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Note: Even when Advanced Media Gateway policy mode is On, all calls to and from OCS 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.

**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 and Video endpoints dial FindMe IDs then the FindMe IDs must be included in the “allowed” policy rules.
- If MOC and video endpoints are dialed directly then the MOC and video endpoint IDs must be included in the “allowed” policy rules.
- If MOC clients are included as devices in FindMe profiles then the MOC 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 not recommended that MOC clients are included as devices in FindMe profiles – use OCS Relay to allow MOC 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP configuration</td>
<td>Manual</td>
</tr>
<tr>
<td>IP address</td>
<td>Required IP address for this Cisco AM GW</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Subnet mask for the subnet</td>
</tr>
<tr>
<td>Default gateway</td>
<td>Default gateway for the subnet</td>
</tr>
<tr>
<td>Host name</td>
<td>Hostname of the Cisco AM GW (optional)</td>
</tr>
<tr>
<td>Name server</td>
<td>IP address of DNS server</td>
</tr>
<tr>
<td>Secondary name server</td>
<td>Optional secondary DNS server IP address</td>
</tr>
</tbody>
</table>
Domain name (DNS Suffix) | DNS suffix to add to a hostname to make it an FQDN (optional)
---|---
3. Click Update IP configuration.

**Network services**

1. Go to the Services page (Network > Services).

2. Ensure that:

   - **Incoming Encrypted SIP (TLS)** Ticked and Port A = 5061

3. If any modification was required, select **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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motion / sharpness tradeoff</td>
<td>As required, e.g. Balanced</td>
</tr>
<tr>
<td>Default bandwidth from AM GW</td>
<td>As required, e.g. 2.00 Mbit/s</td>
</tr>
<tr>
<td>Default bandwidth to AM GW</td>
<td>&lt;same as transmit&gt;</td>
</tr>
<tr>
<td>&lt;other parameters&gt;</td>
<td>As required</td>
</tr>
</tbody>
</table>

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

Click **Apply changes**.

**Resource settings**

1. Go to the **Resource settings** page (Settings > Resource settings).

2. Configure the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
</table>
   | Call capability | Allow HD – supports high definition video calls at up to 720p at 30fps  
                   | SD only – supports calls at up to w448p at 30fps  |

   **Note:** The number of calls supported in the selected mode is shown. This depends on the model of AM gateway you are using.

3. Click **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 Cisco AM GW’ on page 14).

**Time**

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

<table>
<thead>
<tr>
<th>Enable NTP</th>
<th>Select this option</th>
</tr>
</thead>
<tbody>
<tr>
<td>UTC offset</td>
<td>Configure as required for local timezone</td>
</tr>
<tr>
<td>NTP host</td>
<td>IP address or DNS name of NTP (time) server</td>
</tr>
</tbody>
</table>

3. Click **Update NTP settings**.

### Proxies

1. Go to the Proxies page (Proxies > Proxies)
2. Select **Add new proxy**.

<table>
<thead>
<tr>
<th>Name</th>
<th>Descriptive name (for display purposes only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>IP address of Cisco VCS</td>
</tr>
<tr>
<td>Outgoing transport</td>
<td>TLS</td>
</tr>
</tbody>
</table>

4. Click **Add proxy**.

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.

**Note**: If the 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).

### 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:

1. Go to the Shutdown page (Maintenance > Shutdown)
2. 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.

3. Click **Restart AM GW**.

   “AM GW RESTART IN PROGRESS” will confirm that a restart is occurring.
Requirements and usage of MOC

PC requirements

To support 720p RT Video operation, the MOC 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 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 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

Calls between endpoints and OCS 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

Cisco VCS / OCS

Troubleshooting calls between Cisco VCS and OCS is very much the same as troubleshooting any Cisco VCS / OCS call scenario. See the Troubleshooting section in “Cisco VCS Deployment Guide - Microsoft OCS 2007 (R1 and R2) and Cisco VCS Control (X5)”. 

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 debug

This will give the MOC client’s view of the call.

OCS debug

This will provide OCS’s view of communications between OCS and Cisco VCS and OCS and MOC.

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 “Cisco VCS Deployment Guide - Microsoft OCS 2007 (R1 and R2) and Cisco VCS Control (X5)".

Call transfer
Although call hold and resume work as expected, call transfer is not supported.

Multiway
Calls using the Cisco AM GW may not be added into a Multiway call.

Duo Video
Duo Video is not supported into the Microsoft OCS 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 Relay FindMe account location.

OCS Edge Server
Calls to / from MOC clients registered to OCS through an Edge Server are not supported.

Encrypted calls
Encrypted calls between OCS and the Cisco AM GW are not supported – see the configuration required in “Cisco VCS Deployment Guide - Microsoft OCS 2007 (R1 and R2) and Cisco VCS Control (X5)".

AVMCU / livemeeting calls
Calls to / from AVMCU and livemeeting are not supported.
Appendix 3 – Reaching Cisco AM GW capacity

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

The calls will succeed, but the image resolution will be limited to CIF in both directions, from MOC to video endpoint and from video endpoint to MOC, whatever the image size selected on MOC.
Appendix 4 – Bandwidth control

For calls direct to OCS, bandwidth can be controlled using pipes over links to the OCS 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 are not included in the bandwidth figures in the link to the OCS neighbor zone.
## Appendix 5 – Call license usage

<table>
<thead>
<tr>
<th>Call type</th>
<th>Traversal call licenses</th>
<th>Non-traversal call licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP to OCS call via Cisco AM GW</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>H.323 to OCS call via Cisco AM GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>SIP to OCS direct from Cisco VCS</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>H.323 to OCS direct from Cisco VCS</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
Appendix 6 – Endpoint specific configuration

See the endpoint specific configuration appendix in document “Cisco VCS Deployment Guide - Microsoft OCS 2007 (R1 and R2) and Cisco VCS Control (X5)” for general settings for use of video endpoints with Cisco VCS and OCS.

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