Microsoft OCS 2007 and Cisco VCS

Cisco TelePresence Deployment Guide

Cisco VCS X5.2
Microsoft OCS 2007 (R1 & R2)

D14269.04

November 2010

Contents

Introduction

Objectives and intended audience

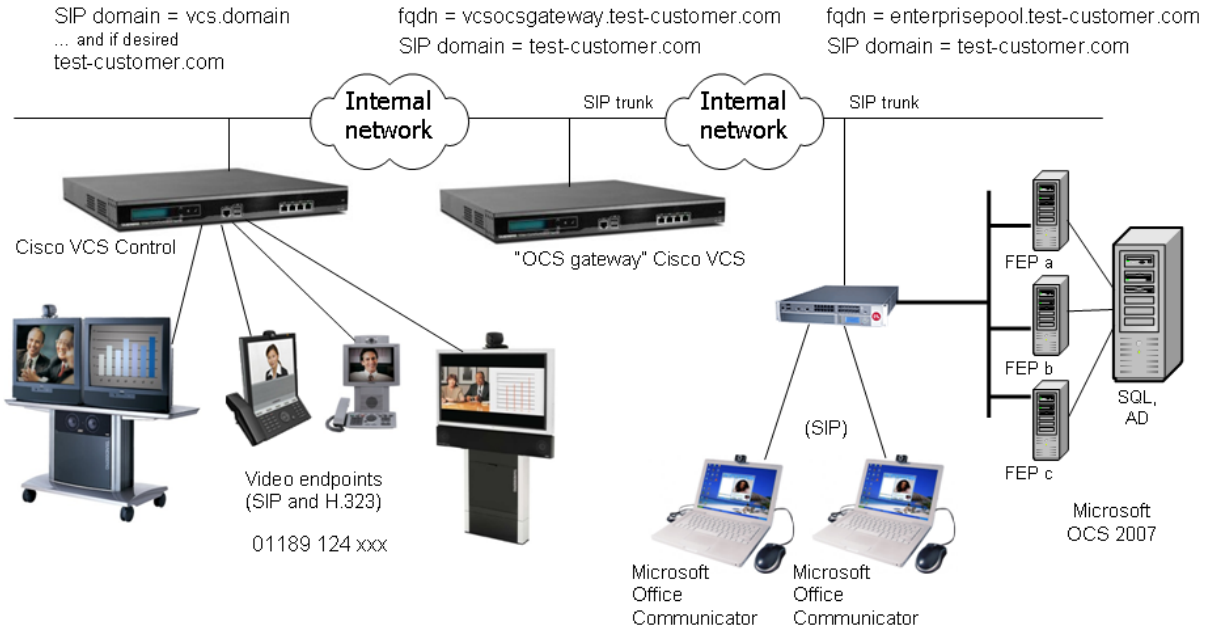
This deployment guide provides instructions on how to configure a Cisco TelePresence Video Communication Server (Cisco VCS) Control version X5.2 and OCS (Microsoft OCS 2007 R1 or R2) to interwork.

This guide also highlights the capabilities and limitations of interoperation of Cisco VCS Control and OCS.

Note: For information about connecting Cisco VCS X3 or X4 to Microsoft OCS, see 'Cisco VCS deployment guide - Microsoft OCS 2007 (R1 and R2) and Cisco VCS Control (X3 and X4) - D14269.01'.

Deployment scenario

A company is introducing an OCS system into their network to provide Microsoft Office Communicator (MOC) clients on everyone's desk to supply messaging and presence capabilities for all staff. Integrating this with their existing Video Network, which handles their video conferencing, provides the ability for video endpoints to make calls to and receive calls from MOC clients, and for MOC clients to see the presence of the video endpoints.



In this scenario, dialing will typically be carried out by users clicking on one of their buddies in MOC, or selecting a destination from an electronic address book on the video endpoint.

This deployment guide describes how to connect OCS and a Cisco VCS Control using a SIP trunk across an IP network. The example presented uses the following setup:

- A new Cisco VCS Control (or cluster of Cisco VCS control peers) – the "OCS gateway" – to act as the link between the existing Video Network and OCS.
- The OCS's SIP domain is **test-customer.com**.

Note: the SIP domain for OCS need not be the same as the AD domain of MOC users (the MOC user's login domain – used in the login user name - may be different from the SIP domain – used in the sign-in address.)

- The existing Video Network's domain is **vcs.domain**, and can, if desired, also include devices registering with the domain **test-customer.com**.
- Endpoints registered to the Video Network may be SIP or H.323 endpoints; they must register with an ID in the format name@domain, where domain is a domain hosted on the Video Network (for example **vcs.domain**, or if desired **test-customer.com**).
- MOC clients registered to OCS are identified by URIs, for example:
  - Steve with a URI steve.hight@test-customer.com
  - Mary with a URI mary.jones@test-customer.com
- Endpoints registered to the Video Network are identified by URIs, frequently including the location of the endpoint, for example:
  - Mary with an h.323 ID mary.jones.office@vcs.domain
  - Mary with a SIP URI mary.jones.external@vcs.domain
  - Steve with an H.323 ID steve.hight.office@vcs.domain
  - Steve with a SIP URI steve.hight.external@vcs.domain
- When using OCS Relay functionality on Cisco VCS, together with OCS R2 or later:
  - The "OCS gateway" Cisco VCS Control supports the **test-customer.com** domain for OCS Relay FindMe™ users.
  - OCS Relay FindMe™ user names are constructed in exactly the same way as OCS URIs, for example:
    - Steve with a URI steve.hight@test-customer.com
    - Mary with a URI mary.jones@test-customer.com
  - These OCS Relay FindMe™ users (with the same domain as OCS) register to OCS as though they are MOC clients. If a corresponding MOC client also exists on a PC, the MOC endpoint on the PC and the Video endpoints specified in the FindMe™ will ring simultaneously when called, whether called from an endpoint communicating with Cisco VCS, or whether called from an endpoint communicating with OCS.
  - These OCS Relay FindMe™ users can specify single or multiple endpoints as primary devices to call; the primary devices can be located anywhere in the Video network or be accessible via the Video Network.
- "Available", "off-line" and "in-call" presence may be observed by MOC clients for OCS Relay FindMe™ users registered by the "OCS gateway" Cisco VCS (when OCS Relay is enabled). "Available" and "off-line" presence may be observed by MOC clients for other devices or FindMe™ users which provide presence information in the Video Network.
- It is assumed that the "OCS gateway" Cisco VCS Control is running X5 code (or later) and has at least the following option keys applied:
  - H323-SIP interworking
  - Registrations
  - Traversal calls
  - Non-traversal calls
  - User Policy (FindMe™) - optional but recommended; necessary to take advantage of the OCS Relay functionality.
- Traversal call and non-traversal call option keys are both needed on the "OCS gateway" Cisco VCS Control
  - OCS to SIP calls that do not use encryption are non-traversal calls
  - OCS to H.323 calls are traversal calls as they need to be interworked from SIP RTP to H.323 RTP
- The version of OCS must be Microsoft OCS 2007 version 3.0.6362.0 (OCS R1) or OCS R2.
- The version of operating system That OCS runs on must be Microsoft Server 2003, 2003 R2 or 2008. It must not be Microsoft Server 2008 R2.
- The version of MOC client must be the version distributed with OCS R1 or OCS R2.

Why add an "OCS Gateway" Cisco VCS Control?

The "OCS gateway" Cisco VCS is an interface between an existing working video network and the Microsoft OCS system. There are a number of settings that need to be configured on the "OCS gateway" that are different from the recommended configurations for standard video routing Cisco VCSs. For instance the "OCS gateway" Cisco VCS requires that Call routed mode be set to "Always", as the Cisco VCS has to modify the OCS SIP signaling to make it suitable for standard video endpoints, MCUs etc. The knock-on effect of this is that call licenses are always used on this "OCS gateway" Cisco VCS. It also requires interworking to be "On" rather than "RegisteredOnly" which can cause calls to be interworked when they need not.

Having the separate "OCS gateway" Cisco VCS and making it the video network presence server also allows this Cisco VCS or cluster of Cisco VCS peers to handle the subscriptions and presence requests from OCS for video network users. Handling them in the "OCS gateway" prevents the OCS presence requests being "spammed" into the existing video network and adversely affecting the run time operation of the previously working system.

OCS Relay requires dedicated CPL. If CPL is required anywhere else in the network (for example, to limit which calls are allowed to be routed to ISDN gateways or other resources) it is hard to merge different CPL scripts.

For FindMe™ to re-write the caller ID, calls must be routed through the Cisco VCS holding the relevant FindMe™; having an "OCS gateway" helps funnel all calls through the correct place.

OCS can only send calls to

- Cisco VCSs that have "same domain" OCS Relay FindMe™ users registered to the OCS, and
- a single FQDN (though this may have a round robin DNS address to support a cluster of Cisco VCSs for resilience) for calls to endpoints accessible via a static domain route defined in OCS

If OCS supports multiple domains, all domains can be handled by a single "OCS gateway" Cisco VCS / cluster, or one "OCS gateway" Cisco VCS / cluster can be used for each domain.

- If different OCS domains are handled by different "OCS gateway" Cisco VCSs or Cisco VCS clusters, take care to ensure that each "OCS gateway" Cisco VCS or Cisco VCS cluster is authoritative for the presence information that is required for the OCS Relay FindMe™ users and all endpoints that are referenced by those FindMe™ entries.
- If one "OCS gateway" Cisco VCS or Cisco VCS cluster is used, note that only one domain can be handled by OCS Relay.

Having a dedicated "OCS gateway" Cisco VCS or Cisco VCS cluster also limits the number of trusted devices that need to be configured in OCS.

Although in the example, nothing is shown registered to the "OCS gateway" Cisco VCS, it is often a good place to register an MCU if significant numbers of MOC callers are going to be sharing conferences with standard video endpoint users.

Small test and demo networks?

For small test and demo networks, video endpoints may be registered to the "OCS gateway" Cisco VCS Control, the small Video Network being controlled by the same Cisco VCS that is the interface to OCS.

Scaling up from a small test and demo network

As extra capacity, regional management and reduced license usage is required it is possible to scale away from the 'small test and demo network' system to the "OCS gateway" Cisco VCS connected to video network approach. This is achieved by adding video network Cisco VCSs and neighboring them (directly, or indirectly through other Cisco VCSs) to the "OCS gateway" Cisco VCS. Endpoints can be added to the video network Cisco VCSs and endpoints and other devices then gradually migrated off the "OCS gateway" Cisco VCS onto the video network Cisco VCSs.

Features and capabilities with different versions of software

The versions of software (Cisco VCS X3 or X4, and OCS R1 or R2 / standard, enterprise) affect the capabilities of the deployed system.

Cisco VCS works equally well with OCS Standard edition and OCS Enterprise edition.

Cisco VCS X4.2 or X4.3 and OCS R1

- Cisco VCS can be in:
  - the same domain as OCS
  - a separate domain from OCS
  - the same and separate domains from OCS
- Same domain is used by FindMe™ entries on Cisco VCS, which register as MOC devices on OCS (using OCS Relay)
  - domain static route(s) are set up on OCS to route calls to Cisco VCS's separate domain(s)
- Presence is only supported Cisco VCS to OCS
  - "Off-line" and "Available" and "In-call" are supported for "same domain" OCS Relay FindMe™ users
  - "Off-line" and "Available" (not "In-call") are reported for "separate domain" users
- Passing MOC presence to devices registered to Cisco VCS is not supported.
- Same domain calls OCS to Cisco VCS can only be made to "same domain" OCS Relay FindMe™ users.
- OCS does not accept call hold request - this means that MOC devices cannot be joined into a Multiway conference.
- MOC devices registering through a Microsoft Edge Server and then calling Cisco VCS registered endpoints is not supported:
  - Cisco VCS registered devices calling OCS registered devices will work, but MOC devices registering through an Edge server get no video if they call a Cisco VCS registered endpoint
- Calls to Microsoft Mediation Servers from endpoints in the Cisco VCS Video Network are not supported.
- In H.323 / SIP interworking, Cisco VCS X4.2 and later code requests full picture updates to work around a "lack of video on MOC" problem.

Cisco VCS X4.2 or X4.3 and OCS R2

- Cisco VCS can be in:
  - the same domain as OCS
  - a separate domain from OCS
  - the same and separate domains from OCS
- Same domain is used by FindMe™ entries on Cisco VCS, which register as MOC devices on OCS (using OCS Relay):
  - domain static route(s) are set up on OCS to route calls to Cisco VCS's separate domain(s)
  - a domain static route is set up on OCS to route calls to Cisco VCS's same domain devices (that are not OCS Relay FindMe™ entries)
- Presence is only supported Cisco VCS to OCS:
  - "Off-line" and "Available" are "In-call" are supported for "same domain" OCS Relay FindMe™ users
  - "Off-line" and "Available" (not "In-call") are reported for "separate domain" users
  - "Off-line" and "Available" (not "In-call") are reported for "same domain" users which are not OCS Relay FindMe™ users
- Passing MOC presence to devices registered to Cisco VCS is not supported.
- Same domain calls OCS to Cisco VCS can be made to "same domain" OCS Relay FindMe™ users and also to other devices with that domain which are routable from the "OCS gateway" Cisco VCS.
- OCS accepts and handles call hold (and resume) requests.
- OCS MOC clients can be joined into a Multiway™ conference.
- OCS connecting to a cluster of Cisco VCSs is not supported when using OCS Relay; without OCS Relay use of Cisco VCS clusters with OCS is only for resilience, not for capacity, as OCS does not support the load balancing of calls to an attached cluster of devices.
- MOC devices registering through a Microsoft Edge Server and then calling Cisco VCS registered endpoints is not supported:
  - Cisco VCS registered devices calling OCS registered devices will work, but MOC devices registering through an Edge server get no video if they call a Cisco VCS registered endpoint
- Calls to Microsoft Mediation Servers work from endpoints in the Cisco VCS Video Network for SIP initiated calls, but do not work for interworked H.323 initiated calls.
- A single Cisco VCS can communicate to a pool of OCS FEPs via a hardware load balancer. OCS systems may use hardware load balancers for resilience and capacity.
- A "lack of video on MOC" problem occurs due to MOC R2 clients not displaying video until a full video frame has been received. A full frame is sent either when requested by a fast picture update request, or when the video stream is paused and then re-started. MOC R2 does not request fast picture updates.
  - latest versions of endpoints recognize when they are connected in a SIP call to an OCS and will send appropriate full frames to allow MOC to display video
  - with Cisco VCS X4.2 and later, H.323 to OCS SIP interworked calls will also have periodic full frames sent to ensure MOC gets video
  - MCU code 3.1 and later recognizes when it is connected in a SIP call to an OCS and will send appropriate full frames to allow MOC to display video
  - third party SIP endpoints are unlikely to allow video to be displayed on MOC

Note: Although the Cisco TelePresence MCU can register directly to OCS R1, due to changes made by Microsoft, the MCU cannot register directly to OCS R2.

To use an MCU with OCS R2, register the MCU to Cisco VCS; Cisco VCS handles the protocol differences on behalf of the MCU.

Cisco VCS X5 or later and OCS R1

As in X4:

- Cisco VCS can be in:
  - the same domain as OCS
  - a separate domain from OCS
  - the same and separate domains from OCS
- Same domain is used by FindMe™ entries on Cisco VCS, which register as MOC devices on OCS (using OCS Relay):
  - domain static route(s) are set up on OCS to route calls to Cisco VCS's separate domain(s)
- Presence is only supported Cisco VCS to OCS:
  - "Off-line" and "Available" and "In-call" are supported for "same domain" OCS Relay FindMe™ users
  - "Off-line" and "Available" (not "In-call") are reported for "separate domain" users
- Passing MOC presence to devices registered to Cisco VCS is not supported.
- OCS does not accept call hold request - this means that MOC devices cannot be joined into a Multiway conference.
- MOC devices registering through a Microsoft Edge Server and then calling Cisco VCS registered endpoints is not supported:
  - Cisco VCS registered devices calling OCS registered devices will work, but MOC devices registering through an Edge server get no video if they call a Cisco VCS registered endpoint
- Calls to Microsoft Mediation Servers from endpoints in the Cisco VCS video network is not supported.
- In H.323 / SIP interworking, Cisco VCS X4.2 and later code requests full picture updates to work around a "lack of video on MOC" problem.

Plus:

- OCS can be connected to a cluster of Cisco VCS peers.
- Cisco VCS forces SIP encryption off on the OCS zone so that video endpoints do not need to have encryption turned off.
- Subzones are no longer needed on the Cisco VCS control for locally registered endpoints.

Cisco VCS X5 or later and OCS R2

As in X4:

- Cisco VCS can be in:
  - the same domain as OCS
  - a separate domain from OCS
  - the same and separate domains from OCS
- Same domain is used by FindMe™ entries on Cisco VCS, which register as MOC devices on OCS (using OCS Relay):
  - domain static route(s) are set up on OCS to route calls to Cisco VCS's separate domain(s)
  - a domain static route is set up on OCS to route calls to Cisco VCS's same domain devices (that are not OCS Relay FindMe™ entries)
- Presence is only supported Cisco VCS to OCS:
  - "Off-line" and "Available" are "In-call" are supported for "same domain" OCS Relay FindMe™ users
  - "Off-line" and "Available" (not "In-call") are reported for "separate domain" users
  - "Off-line" and "Available" (not "In-call") are reported for "same domain" users which are not OCS Relay FindMe™ users
- Passing MOC presence to devices registered to Cisco VCS is not supported.

- Same domain calls OCS to Cisco VCS can be made to “same domain” OCS Relay FindMe™ users and also to other devices with that domain which are routable from the “OCS gateway” Cisco VCS.
- OCS accepts and handles call hold (and resume) requests.
- OCS MOC clients can be joined into a Multiway™ conference.
- MOC devices registering through a Microsoft Edge Server and then calling Cisco VCS registered endpoints is not supported:
  - Cisco VCS registered devices calling OCS registered devices will work, but MOC devices registering through an Edge server get no video if they call a Cisco VCS registered endpoint
- Calls to Microsoft Mediation Servers work from endpoints in the Cisco VCS Video Network for SIP initiated calls, but do not work for interworked H.323 initiated calls.
- A single Cisco VCS can communicate to a pool of OCS FEPs via a hardware load balancer. OCS systems may use hardware load balancers for resilience and capacity.
- A “lack of video on MOC” problem occurs due to MOC R2 clients not displaying video until a full video frame has been received. A full frame is sent either when requested by a fast picture update request, or when the video stream is paused and then re-started. MOC R2 does not request fast picture updates.
  - latest versions of endpoints recognize when they are connected in a SIP call to an OCS and will send appropriate full frames to allow MOC to display video
  - with Cisco VCS X4.2 and later, H.323 to OCS SIP interworked calls will also have periodic full frames sent to ensure MOC gets video
  - MCU code 3.1 and later recognizes when it is connected in a SIP call to an OCS and will send appropriate full frames to allow MOC to display video
  - third party SIP endpoints are unlikely to allow video to be displayed on MOC

Plus:

- OCS can be connected to a cluster of Cisco VCS peers.
- Cisco VCS forces SIP encryption off on the OCS zone so that video endpoints do not need to have encryption turned off. (This functionality is removed in version X5.2 where encryption is available between Cisco VCS and OCS.)
- OCS Director is supported.
- Subzones are no longer needed on the Cisco VCS Control for locally registered endpoints.

Plus with X5.2:

- Media encryption (SRTP) is supported when TLS is used between Cisco VCS and OCS and the **Enhanced OCS collaboration** option key is added to the Cisco VCS.

Note: Although the Cisco TelePresence MCU can register directly to OCS R1, due to changes made by Microsoft, the MCU cannot register directly to OCS R2.

To use an MCU with OCS R2, register the MCU to Cisco VCS; Cisco VCS handles the protocol differences on behalf of the MCU.

Use of Cisco VCS X5 or later software is recommended in order to get the cleanest interface with OCS R1 and OCS R2.

Summary of configuration process

This document describes how to configure both the OCS (version R1 and R2) and the Cisco VCS Control (version X5.x) so that calls can be made from:

- SIP and H.323 video endpoints registered in the video network to other SIP and H.323 video endpoints registered in that same video network.
- Microsoft Office Communicator (MOC) clients registered on OCS to other MOC clients registered on that OCS.

- SIP and H.323 video endpoints registered in the Video Network to MOC clients registered on OCS.
- MOC clients registered on OCS to SIP and H.323 video endpoints registered in the Video Network.

It also describes how to enable presence so that MOC clients can see the presence status of endpoints registered in the video network.

The configuration process describes each of these stages separately, so that individual stages can be implemented and tested before moving on to the next.

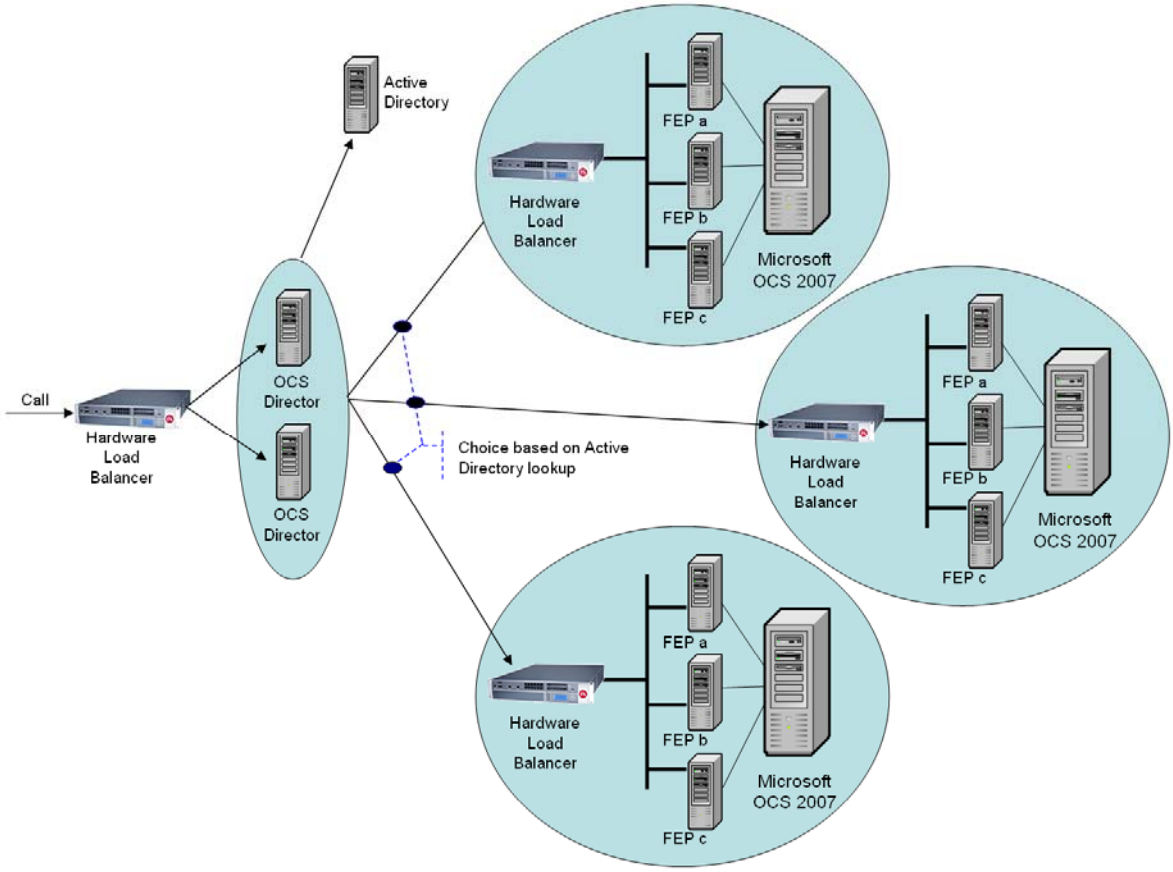
An advanced configuration stage (OCS Relay configuration of “OCS gateway” Cisco VCS) is also documented for systems running Cisco VCS X5 or later and OCS R2 or later, which enables Cisco VCS to register FindMe™ users as though they are MOC clients, so that:

- “In-call” as well as “Available” and “Off-line” can be seen for these FindMe™ users.
- OCS will fork calls to FindMe™ users at the same time as MOC users with the same name, so that calls can be taken on MOC or a video endpoint, as desired.

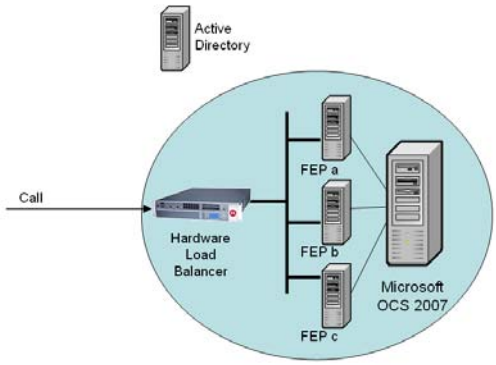
Different structures for OCS

OCS systems have a number of building blocks, and so OCS systems may be constructed in many ways.

A full scale OCS deployment is likely to use OCS Director, Hardware Load Balancers (HLBs), Front End Processors (FEPs) in enterprise pools, and a redundant AD server. For example:



A smaller deployment may not use OCS Director servers, but may just use a Hardware Load Balancer in front of a set of Front End Processors.



The simplest deployment will have AD and FEP on a single server, with no Hardware Load Balancer needed as OCS is a single server.

OCS deployments may also contain Edge servers to allow MOC clients to register from outside the local network through the Edge server to OCS. This is not shown in the diagrams above, because currently the Cisco VCS implementation only supports interoperation with MOC devices directly registered to OCS.

OCS should be configured so that:

1. If the OCS system is fronted by a Hardware Load Balancer in front of OCS Directors then calls to and from the video network will go via the Directors; they will not be routed directly to or from the FEPs:
   - OCS Directors should trust the "OCS gateway" Cisco VCS(s)
   - OCS Directors should route Video network SIP domain(s) (and the OCS SIP domain) to the "OCS gateway" Cisco VCS cluster FQDN (or if only a single Cisco VCS, the FQDN of that Cisco VCS)
   - FEPs will route traffic that they don't know how to route to Director, and Director will route the calls to the Cisco VCS.
2. If the OCS system is fronted by a single OCS Director then calls to and from the video network will go via that Director; they will not be routed directly to or from the FEPs:
   - OCS Director should trust the "OCS gateway" Cisco VCS(s)
   - OCS Director should route Video network SIP domain(s) (and the OCS SIP domain) to the "OCS gateway" Cisco VCS cluster FQDN (or if only a single Cisco VCS, the FQDN of that Cisco VCS)
   - FEPs will route traffic that they don't know how to route to Director, and Director will route the calls to the Cisco VCS.
3. If the OCS system has no OCS Director but a Hardware Load Balancer in front of Front End Processor pool(s) then configure the pool(s) (not each FEP) to route calls for the video network directly to The "OCS gateway" Cisco VCS(s) – configuring the pool ensures that the same configuration is applied to every FEP in the pool:
   - The FEP pools should trust the "OCS gateway" Cisco VCS(s)
   - All FEP pools should route calls to the "OCS gateway" Cisco VCS cluster FQDN (or if only a single Cisco VCS, the FQDN of that Cisco VCS)

4. If OCS is a single FEP then that FEP should be configured to route calls for the Video Network directly to the "OCS gateway" Cisco VCS(s):
   - the single FEP should trust the "OCS gateway" Cisco VCS(s)
   - the single FEP should route calls to the "OCS gateway" Cisco VCS cluster FQDN (or if only a single Cisco VCS, the FQDN of that Cisco VCS)

Cisco VCS should be configured such that:

1. If the OCS system is fronted by a Hardware Load Balancer in front of OCS Directors then the "OCS gateway" Cisco VCS(s) should be configured to route calls for OCS through the Hardware Load Balancer in front of the OCS Directors, and receive calls from either of the OCS Directors:
   - the "OCS gateway" Cisco VCS(s) need to neighbor to the Hardware Load Balancer.
   - the "OCS gateway" Cisco VCS(s) also need to have another neighbor zones that contain the Peer addresses of both OCS Directors.
   - the Hardware Load Balancer neighbor zone is pointed to by the Search rule(s) that route calls to OCS.
   - the neighbor zones to the other FEPs must also have their Zone profile set to Microsoft Office Communications Server 2007 but must not be referenced by any Search rules.

2. If the OCS system is fronted by an OCS Director then the "OCS gateway" Cisco VCS(s) should be configured to route calls for OCS through the OCS Director, and receive calls from the OCS Director:
   - configure the OCS Director as the Peer address in the neighbor zone

3. If the OCS system has no OCS Director but a Hardware Load Balancer in front of Front End Processors then the "OCS gateway" Cisco VCS(s) should be configured to route calls for the Video Network directly to the Hardware Load Balancer, and receive calls from any of the FEPs:
   - the "OCS gateway" Cisco VCS(s) need to neighbor to the Hardware Load Balancer.

- the “OCS gateway” Cisco VCS(s) also need to have 1 or more neighbor zones that contain the Peer addresses of all the OCS FEPs.
- the Hardware Load Balancer neighbor zone is pointed to by the Search rule(s) that route calls to OCS.
- the neighbor zones to the other FEPs must also have their Zone profile set to Microsoft Office Communications Server 2007 but must not be referenced by any Search rules.

4. If OCS is a single FEP then the “OCS gateway” Cisco VCS(s) should be configured to route calls for OCS to the single FEP directly, and receive calls from the FEP:
   - configure the single FEP as the Peer address in the neighbor zone

For more details about OCS Director, see “Appendix 14 – Cisco VCS and Microsoft OCS Director’.

Prerequisites prior to configuring Cisco VCS and OCS to interoperate

Before configuring the Video Network and the OCS system to interwork, make sure that the following is operational:

- OCS is configured and operational and access is available to Active Directory for managing users.
- The FQDN of OCS (enterprisepool.test-customer.com in this example) is resolvable via the DNS server that Cisco VCS Control is configured to use (often the DNS server on OCS).
- The FQDNs of each of the “OCS gateway” Cisco VCSs and the FQDN of the “OCS gateway” cluster must be resolvable via the DNS server.
- The video endpoints registered to the Video Network must support the H.263 video codec – this is the only video codec which is common to MOC clients and standard video endpoints.
- Validation of the Front End Servers on all OCS Directors and OCS FEPs must show no errors. (Log into each OCS Director and each OCS FEP, select the Director or FEP, then select Validation, select Front End Server and follow the wizard instructions.)
- If TLS is to be used (recommended) ensure that the DNS server supports reverse DNS lookup (often supported using PTR records).

Enabling calls between endpoints registered on Cisco VCS Controls in the video network

Video network Cisco VCS Control configuration summary

The configuration of the Cisco VCS Control(s) in the video network to allow calls to be made between endpoints that register to them should already have been carried out.

Ensure that the following 2 items are configured:

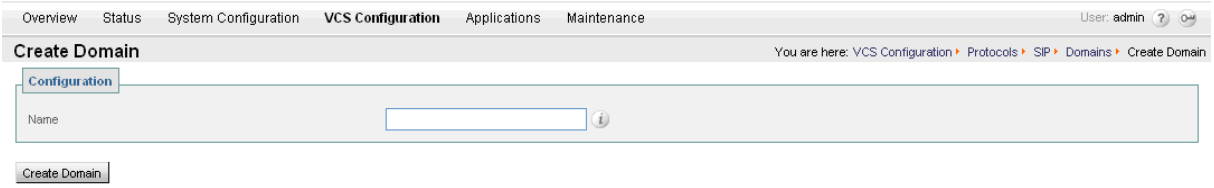
1. SIP domain of the video network - needed for SIP registration and presence handling.
2. Default links between the Cisco VCS Control's zones.

Note: In small test and demo networks this configuration is carried out on the same Cisco VCS that is the "OCS Gateway" Cisco VCS

Ensure that the SIP domain of Cisco VCS Control(s) in the video network are configured

SIP endpoints register with the Cisco VCS Control with a URI in the format **user-id@sip-domain**. The Cisco VCS Controls accepting these registrations must be configured with the SIP domain information so that it will accept these registrations.

1. Go to the **Domains** page (**VCS configuration > Protocols > SIP > Domains**).
2. Select **New**.
3. Set **Name** to, for example, *vcs.domain*.
4. Select **Create Domain**.



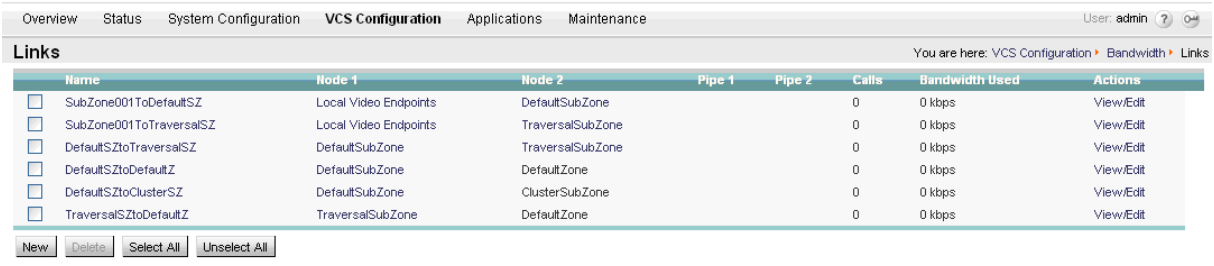
Ensure that default links between the Cisco VCS Control's zones are set up

For a call to succeed there must be appropriate links between Zones.

Links must exist from:

- Default Subzone to Traversal Subzone
- Default Subzone to Default Zone
- Default Subzone to Cluster Subzone (*this is required even if Cisco VCS is not part of a cluster)*
- Traversal Subzone to Default Zone

Check these on the Links page (**VCS configuration > Bandwidth > Links**).



If any links are missing, log onto the command line interface and execute the command:
`xcommand DefaultLinksAdd`

OCS configuration

No configuration is required on OCS to allow endpoints registered on the Cisco VCS Control to call other endpoints registered on the Cisco VCS Control.

Registering endpoints to the Video Network

Endpoint configuration.

For H.323, configure the endpoints as follows:

- H.323 ID (for example, mary@VCS.domain)
- H.323 Call Setup = Gatekeeper
- Gatekeeper IP address = IP address of Cisco VCS Control

For SIP, configure the endpoints as follows:

- SIP Address (URI) (for example, john@VCS.domain)
- Server Address (Proxy address) = IP address of Cisco VCS Control

Confirming registrations

Registration status can be confirmed on the **Registrations** page (**Status > Registrations**).

By default the Cisco VCS Control accepts all registrations to SIP domains configured in the Cisco VCS Control. It is possible to limit registrations by explicitly allowing or denying individual registrations (see the Cisco VCS Configuration section of the Cisco VCS Administrator Guide for further details).

Calls can now be made between endpoints registered on Cisco VCS Control.

Testing the configuration

To test the configuration:

1. Make some test calls between the endpoints.
2. Clear the calls.
3. Check the **Call history** page on the Cisco VCS Control (**Status > Call History**).

Enabling calls between MOC clients registered on OCS

Cisco VCS Control configuration

No configuration is required on Cisco VCS Control for endpoints registered on OCS to call other endpoints registered on OCS.

OCS configuration summary

To configure OCS to enable calls to be made between MOC clients that register to it:

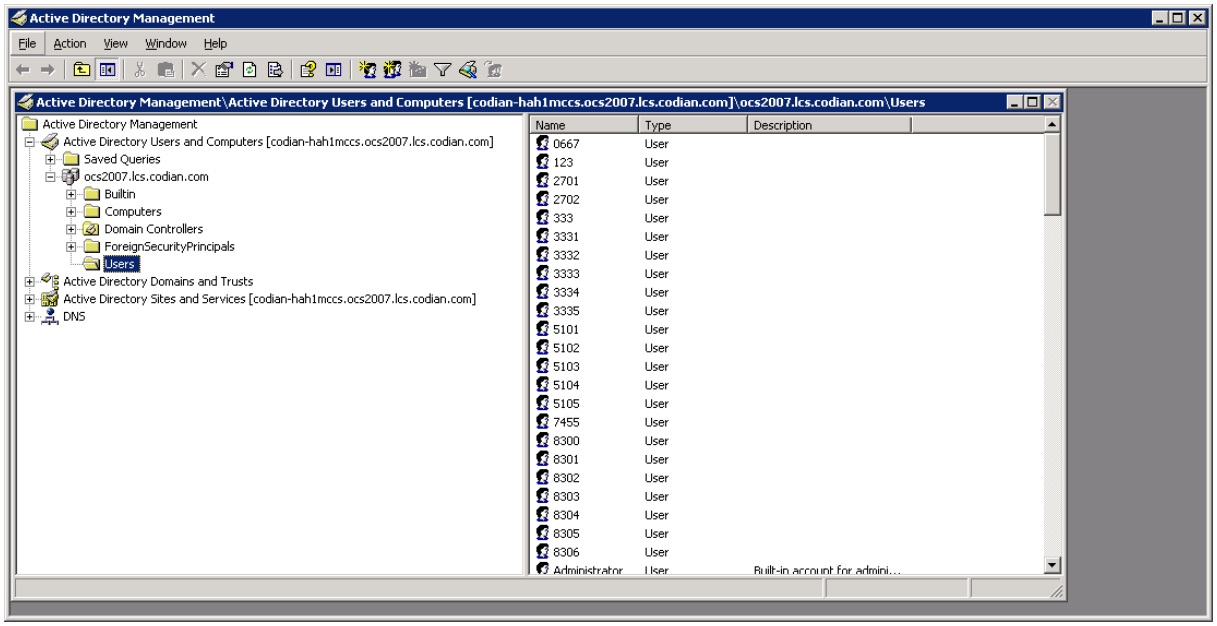
1. Create new users (if required) using active directory
2. Edit user properties to allow MOC usage
3. Register MOC clients to OCS

Diagrams are taken for an OCS R2 installation – OCS R1 screenshots may be different.

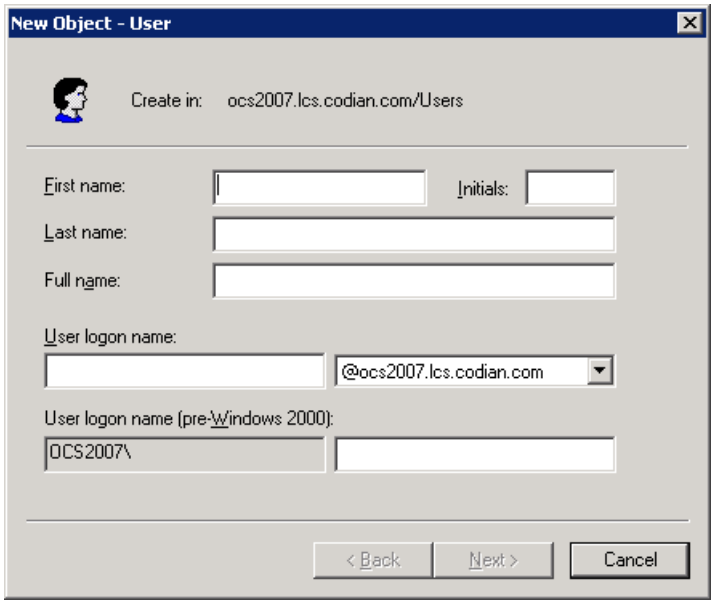
Create new users in Active Directory

On the OCS server:

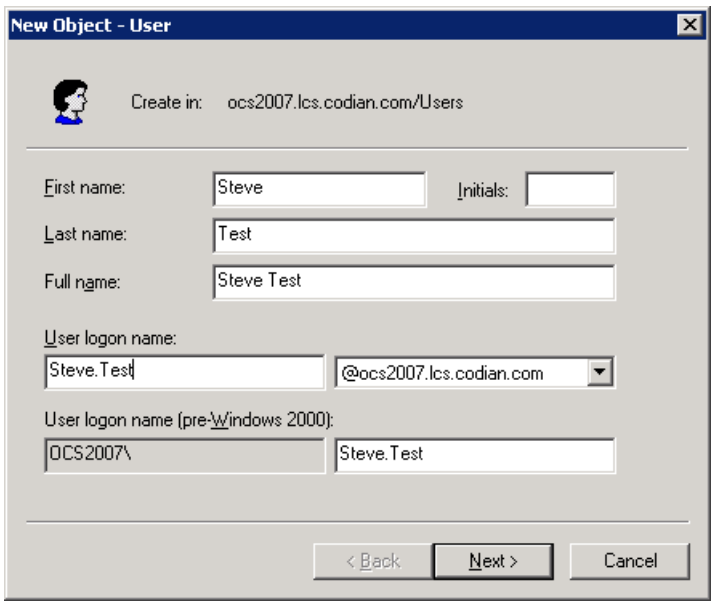
1. Select **Active Directory Management**.
2. Expand **Active Directory Users and Computers**.
3. Expand the relevant domain.



4. Right-click on Users and choose **New > User**.

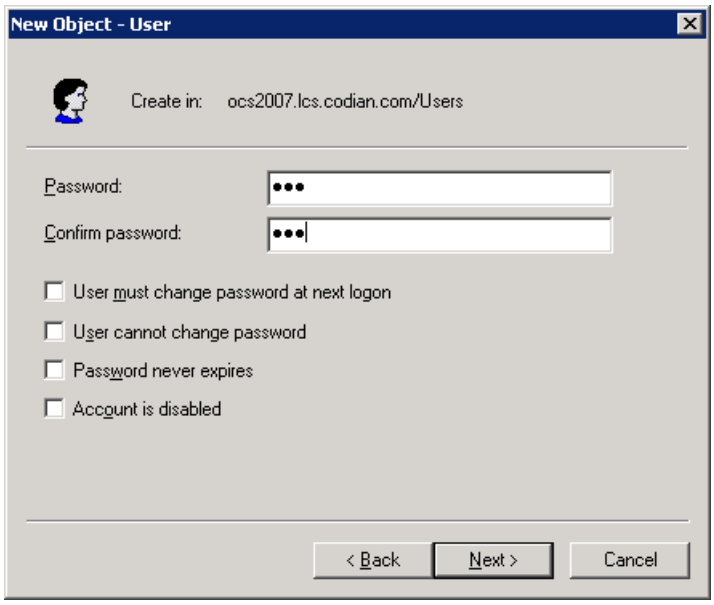


5. Enter details of the new user: **First name**, **Last name** and **User logon name** (Steve.Test and Steve.Test for example).

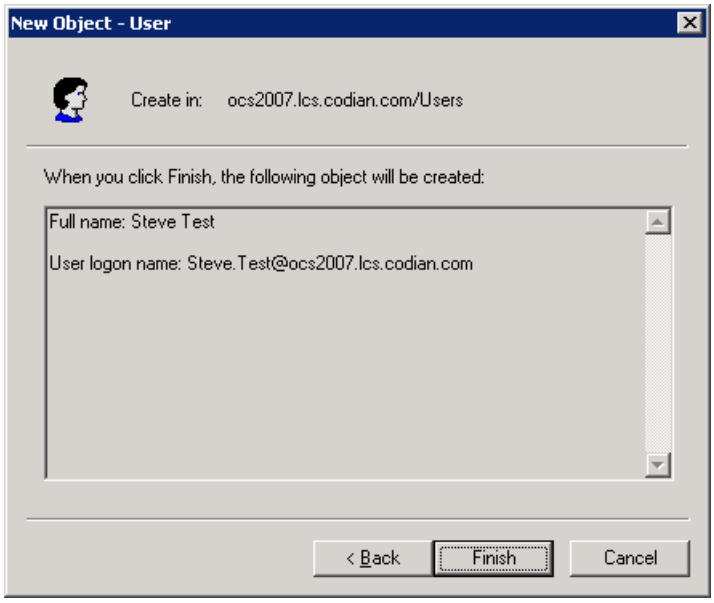


6. Click **Next**.

7. Enter and confirm a password for the user and select the required password handling options:



8. Click **Next**.

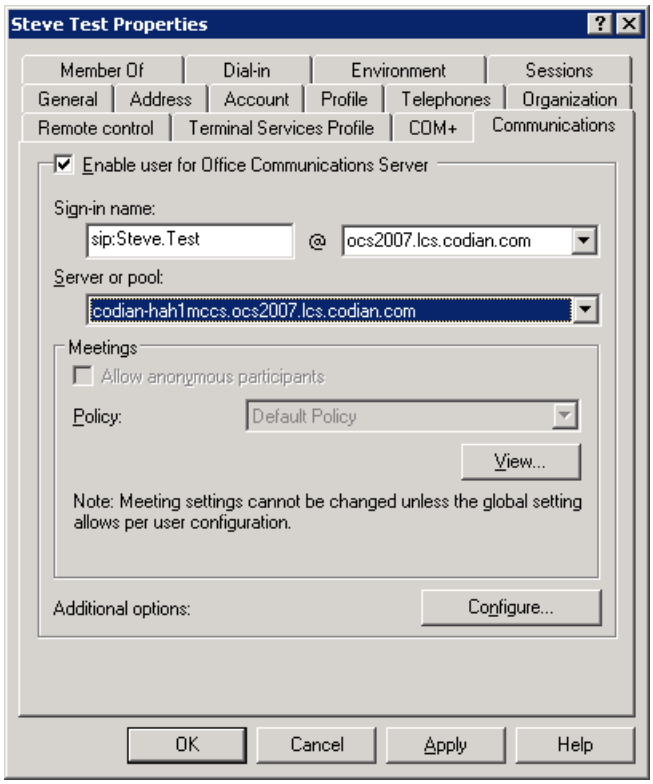


9. Click **Finish**.

Edit user properties to allow MOC usage

In Active Directory now set up the properties of the user:

1. From this **Users** directory, right-click on this newly created user (Steve Test, for example) and choose **Properties**.
2. Select the **Communications** tab.
3. Select **Enable user for Office Communications Server**.
4. Set up the **Sign in name** to match the **User logon name** prefixed with *sip:* (for example sip:Steve.Test) and select the relevant OCS domain from the drop-down.
5. Select the relevant FQDN of the OCS server from the **Server or pool** drop-down. (Note: Microsoft recommend that you do not select OCS Director, but choose an FEP pool – or FEP).

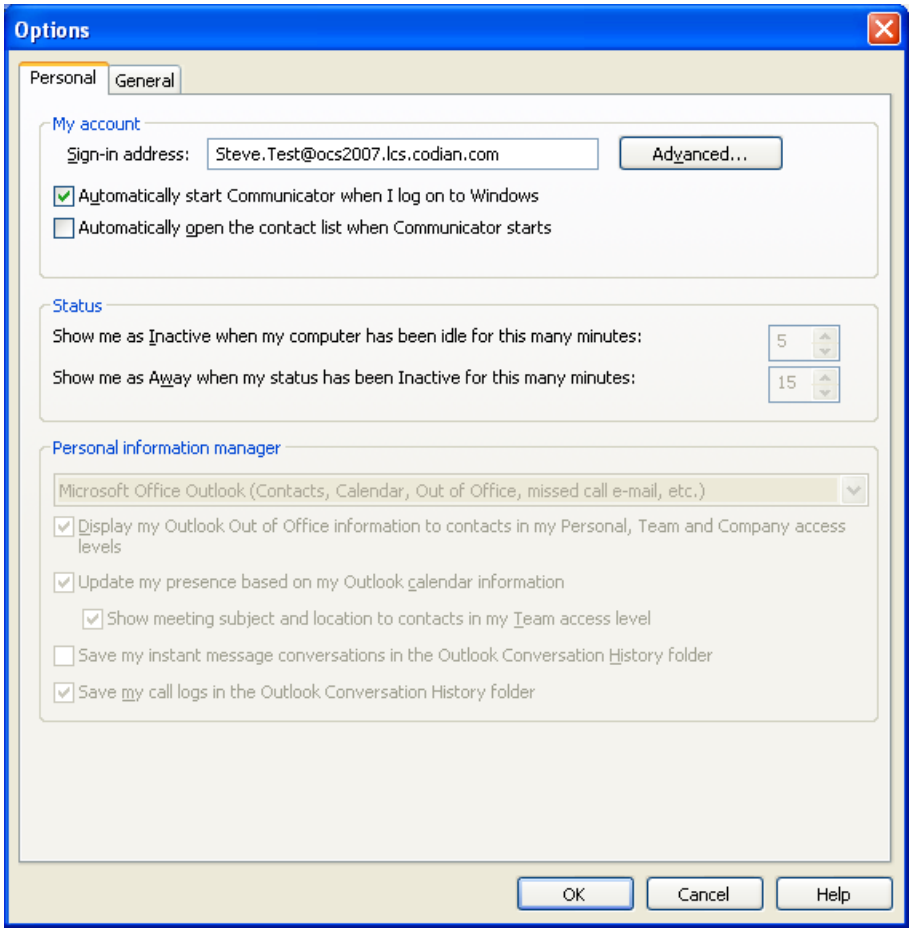

Steve Test Properties
Member Of
Dial-in
Environment
Sessions
General
Address
Account
Profile
Telephones
Organization
Remote control
Terminal Services Profile
COM+
Communications
Enable user for Office Communications Server
Sign-in name:
sip:Steve.Test
@
ocs2007.lcs.codian.com
Server or pool:
codian-hah1mccs.ocs2007.lcs.codian.com
Meetings
Allow anonymous participants
Policy:
Default Policy
View...
Note: Meeting settings cannot be changed unless the global setting allows per user configuration.
Additional options:
Configure...
OK
Cancel
Apply
Help

6. Click **OK**.

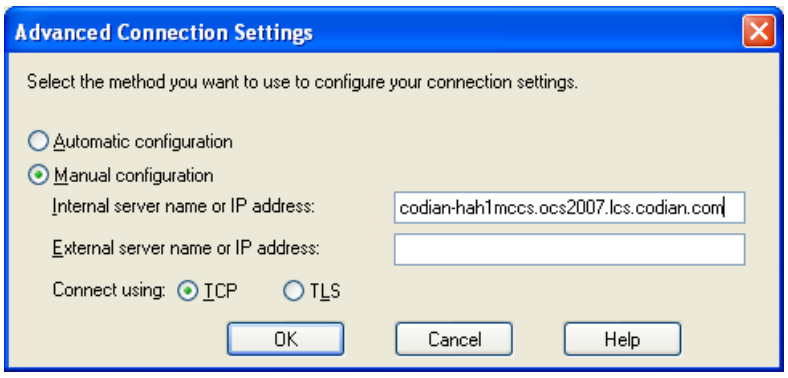
Registering MOC clients to the OCS

MOC client configuration

1. Install MOC (Microsoft Office Communicator 2007).
2. From the menu, go to **Connect > Change Sign-In address…**

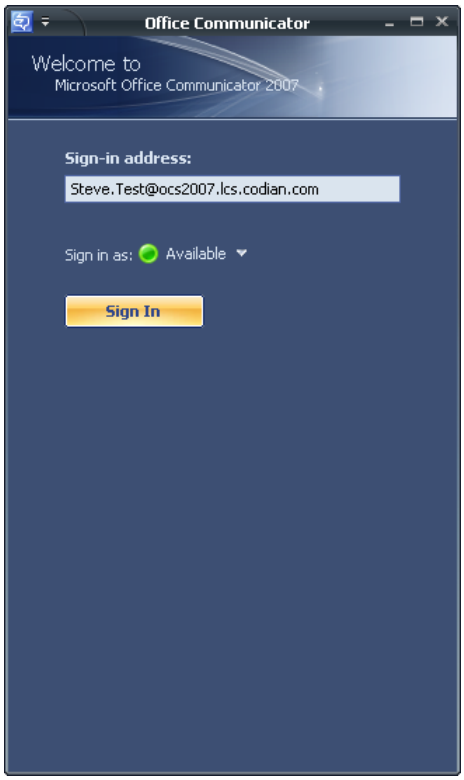


3. Set up **Sign-in address** as required. This is the SIP URI of the MOC; if this user also has Video endpoints on the Video network, this URI will be the same URI as that configured as the OCS Relay FindMe™ user ID (set up later), for example steve.hight@test-customer.com.
4. Click **Advanced**.



5. In a production environment ensure **Automatic configuration** is selected.
   If this proves not to work select **Manual configuration** and set **Internal server name or IP address** to the FQDN of the OCS server.
6. Click **OK** to return to the **Options** dialog.

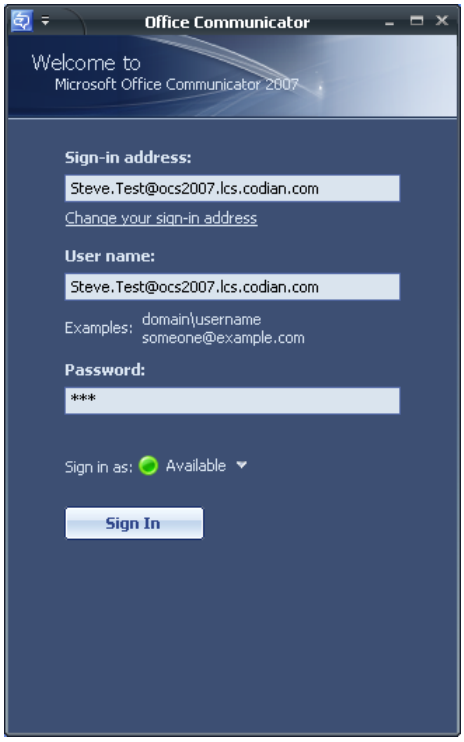
7. Click **OK** to return to the **Office Communicator** panel.



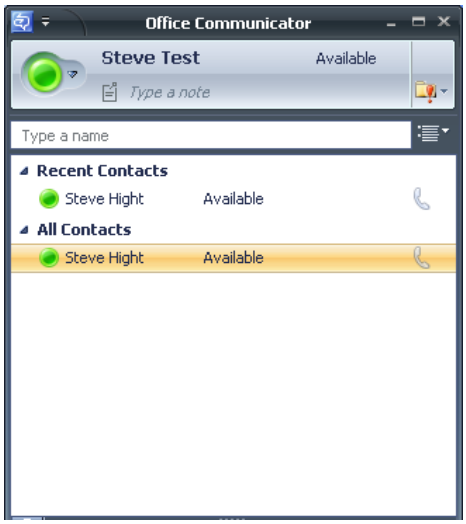
8. Click **Sign In**.
9. Username is the Active Directory name of the user. This may or may not be the same as the sign in address.

Note: Depending on how the network is configured, the **User name** may need to be in the form <domain>\<user> rather than <user>@<domain> for example ocs2007.lcs.codian.com\Steve.Test instead of Steve.Test@ocs2007.lcs.codian.com

10. Enter the **Password** – this is the AD password for this user.



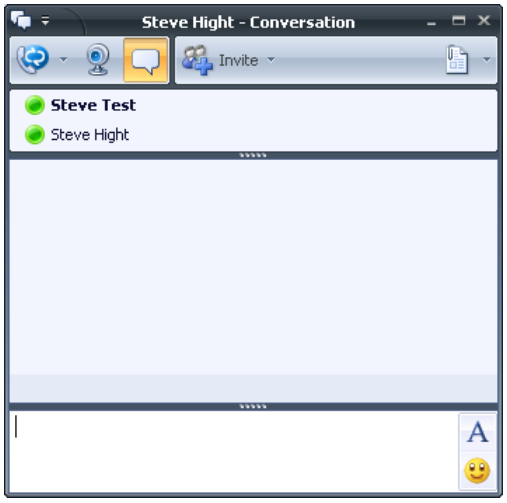
11. Click **Sign In**.



Testing the configuration

To make a video call between MOC endpoints:

1. Double-click on the buddy you want to call.



2. Click  (the web-cam).
3. Answer the call on the receiving MOC Client.

Enabling endpoints registered on the video network to call MOC clients registered on OCS

This is configured in 4 stages:

1. Video Network Cisco VCS Control Configuration
2. “OCS gateway” Cisco VCS Control configuration (1)
3. OCS Configuration
4. “OCS gateway” Cisco VCS Control configuration (2)

Video network Cisco VCS Control configuration

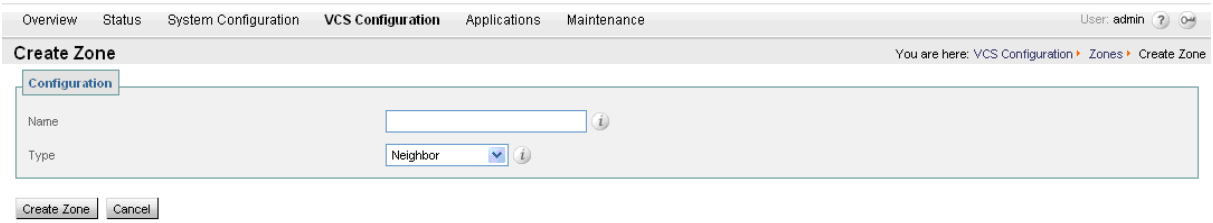
The video network must have a link to the “OCS gateway”; to configure this:

1. Set up a neighbor zone to the “OCS gateway” Cisco VCS (cluster).
2. Set up a Search rule to route calls with the OCS domain to the “OCS gateway” Cisco VCS (cluster).

Note: In small test and demo networks this configuration is not necessary - the video network Cisco VCS is the “OCS Gateway” Cisco VCS. Go to ‘“OCS gateway” Cisco VCS Control configuration (1)’ on page 28.

Set up a neighbor zone to the “OCS gateway” Cisco VCS (cluster)

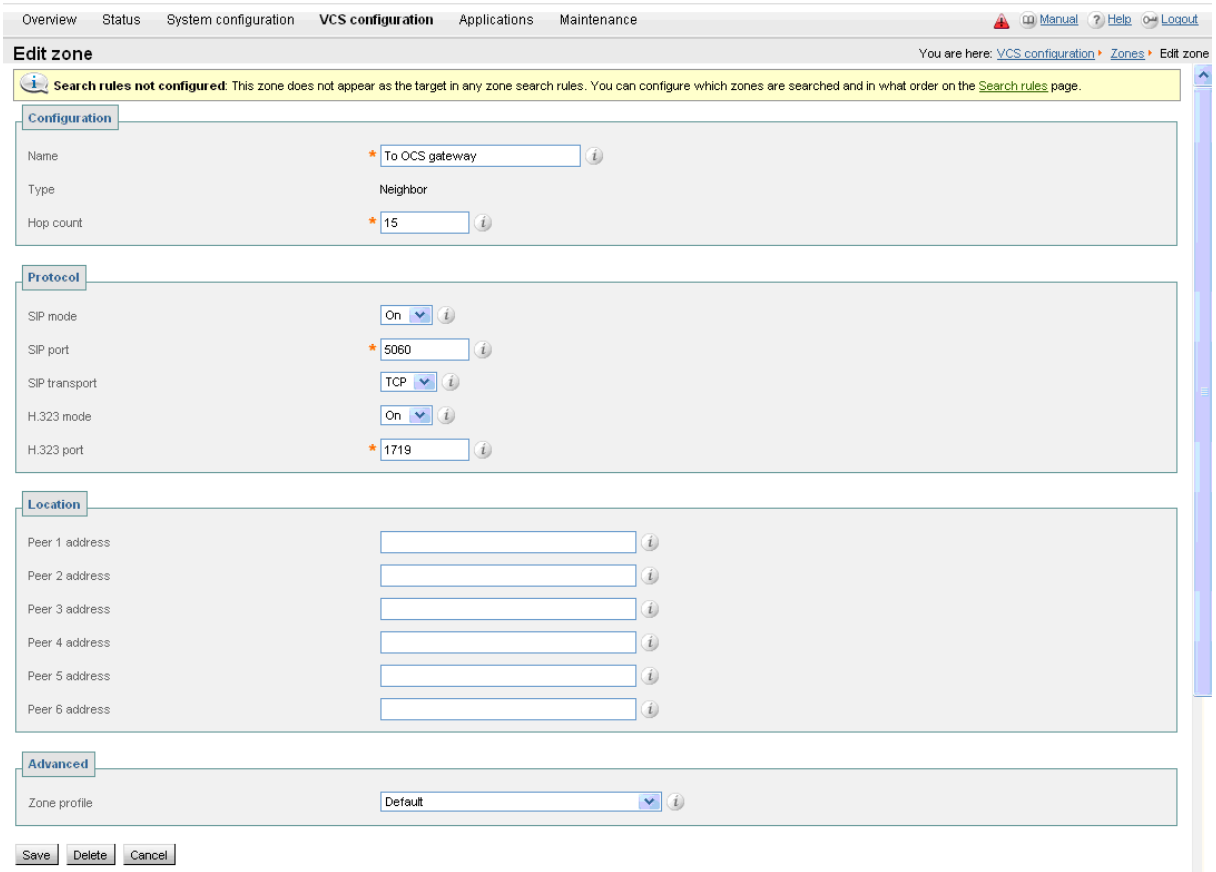
1. Go to the **Zones** page (**VCS Configuration > Zones).**
2. Click **New**.



3. Configure the following fields:

Name	An appropriate name, for example “To OCS gateway”
Type	Neighbor

4. Click **Create Zone**.



It is recommended that the connection to the "OCS gateway" Cisco VCS uses SIP over TLS to communicate so that encrypted calls can be handled. H.323 mode should also be enabled, so that any interworking that has to be done for calls with OCS is carried out on the "OCS gateway" Cisco VCS.

5. Configure the following fields:

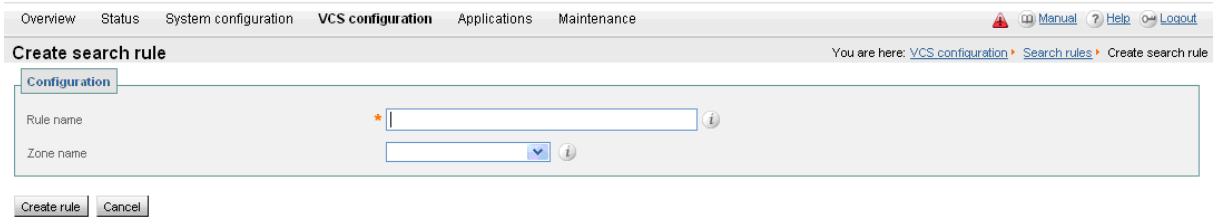
SIP mode	**On**
SIP port	**5061** (or the value that is the same as that configured on the "OCS gateway" Cisco VCS for TLS mode SIP)
SIP transport	**TLS**
H.323 mode	**On**
In the **Location** section: **Peer 1 address**	IP address or FQDN of the "OCS gateway" Cisco VCS (or the 1st Cisco VCS in the "OCS gateway" Cisco VCS cluster)
In the **Location** section: **Peer 2 address** to **Peer 6 address**	IP address or FQDN of the 2nd to 6th "OCS gateway" cluster peers (if any)
In the **Advanced** section: **Zone profile**	**Default**

6. Click **Save**.

Note: Do not worry about the status section indicating Failed. This will change to Active after the zone's IP address / FQDN has been saved.

Set up a search rule to route calls with the OCS domain to the "OCS gateway" Cisco VCS (cluster).

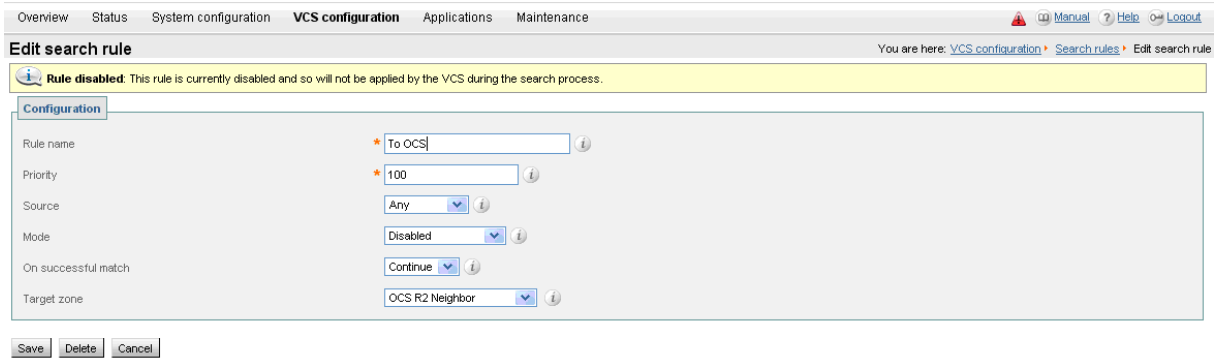
1. Go to the **Rules** page (**VCS Configuration > Search rules > Rules**).
2. Click **New**.



3. Configure the following fields:

Rule name	An appropriate name, for example "Route to OCS gateway"
Zone name	Select the OCS gateway zone, for example **"To OCS gateway"**

4. Click **Create rule**.



5. Configure the following fields:

Rule name	Leave as set above
Priority	Leave as default, for example 100
Source	**Any**
Mode	**AliasPatterMatch**
Pattern type	**Regex**
Pattern string	.*@test-customer.com.*
Pattern behavior	**Leave**
On successful match	**Continue**
Target zone	Leave as set above

6. Click **Save**.

"OCS gateway" Cisco VCS Control configuration (1)

- If "OCS gateway" is a cluster, unless this guide states that configuration is required on each peer, configure the Master Cisco VCS in the cluster and allow the configuration to be replicated to the other peers automatically.
- If the "OCS gateway" is just a single Cisco VCS then set up the configuration on that Cisco VCS.

It is recommended to use TLS connectivity between Cisco VCS and OCS, but TCP connection is also explained. (TCP may not work for OCS configurations that include HLBs and / or OCS Director).

To configure an “OCS gateway” Cisco VCS Control:

1. Generate and load private key, root certificate and server certificate onto Cisco VCS.
2. Set up the SIP domain of the “OCS gateway” Cisco VCS.
3. Ensure that the default links between the “OCS gateway” Cisco VCS Control’s zones are set up.
4. Configure DNS.
5. Ensure that cluster name is configured.
6. Configure an NTP server.
7. Switch on TLS in SIP configuration.
8. Set H.323 <--> SIP interworking to On.
9. Set Call routed mode to Always.

Generate and load private key, root certificate, and server certificate onto “OCS gateway” Cisco VCS Control (Not needed if TCP connection is to be used)

Obtain and load Root CA certificate, server certificate and private key into the Cisco VCS.

Note: For mutual TLS authentication the Server certificate must be capable of being used as a Client certificate as well.

Either a single server certificate can be created to cover the “OCS gateway” cluster, or a server certificate can be created for each Cisco VCS. If the “OCS gateway” is a non-clustered Cisco VCS then use the section “Server certificate for each Cisco VCS”

Details on how to create certificates for Cisco VCS are documented in “Cisco VCS Deployment Guide – Certificate creation and use with Cisco VCS”.

Single server certificate that can be loaded into each cluster peer:

The Certificate must specify:

- **Subject name**: the Cisco VCS cluster’s routable domain, e.g.vcsocsgateway.test-customer.com
- **Subject Alternate Name**: a comma separated list of the Cisco VCS peers’ routable domains (DNS Local hostname concatenated with DNS Domain)
  e.g. vcsocspeer1.test-customer.com,vcsocspeer2.test-customer.com

Server certificate for each Cisco VCS:

A certificate must be created for each “OCS gateway” Cisco VCS; the Certificate must specify:

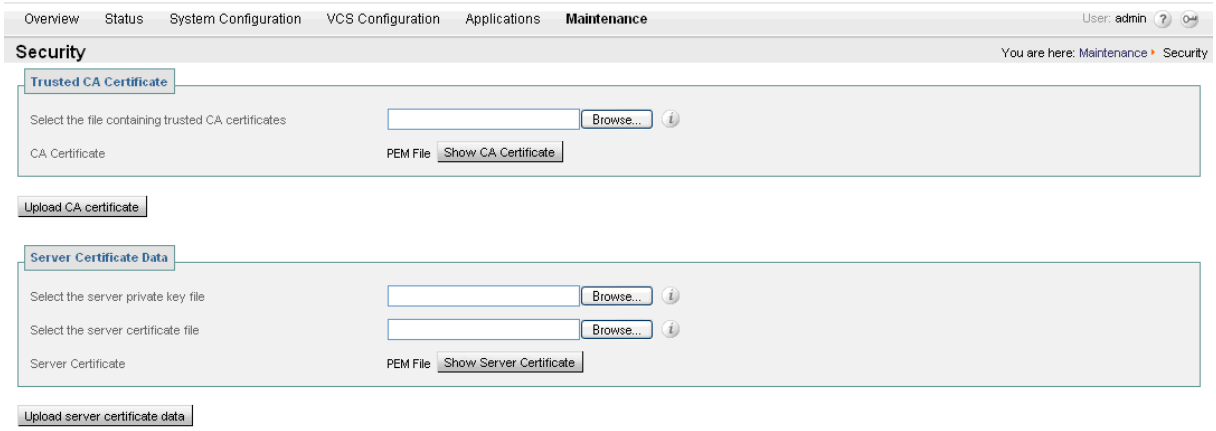
- **Subject name**: the Cisco VCS peer’s routable domain (DNS Local hostname concatenated with DNS Domain) e.g. vcsocspeer1.test-customer.com

and if it is part of a cluster:

- **Subject Alternate Name**: the Cisco VCS cluster’s routable domain, e.g. vcsocsgateway.test-customer.com

Load the certificates:

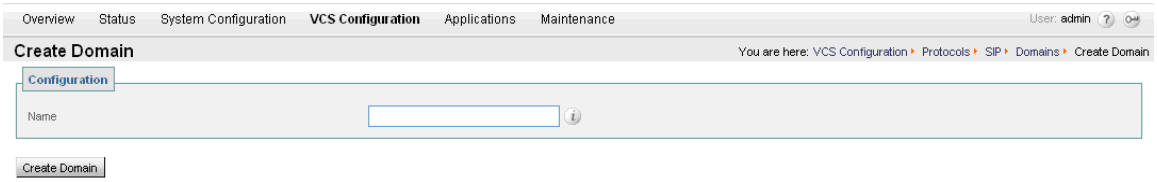
Load the certificates on the **Security** page (**Maintenance > Security**):



Set up the SIP domain of the "OCS gateway" Cisco VCS

OCS Relay FindMe™ users need to have the "OCS gateway" Cisco VCS handle the OCS's domain.

1. Go to the **Domains** page (**VCS Configuration > Protocols > SIP > Domains**).
2. Click **New**.



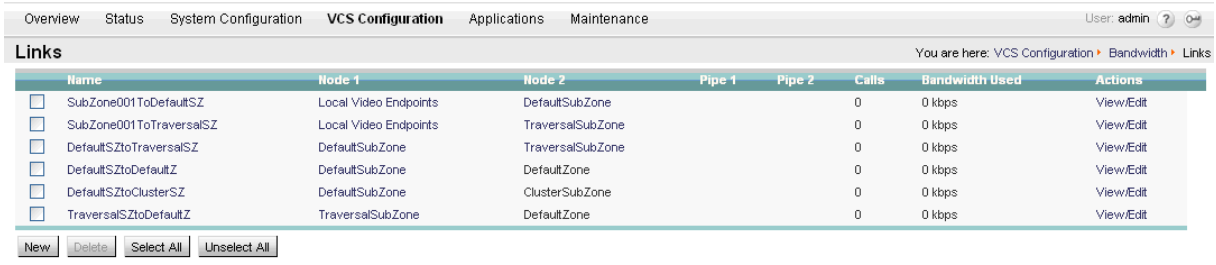
3. Set **Name** to *test-customer.com*.
4. Click **Create Domain**.

Ensure that default links between the "OCS gateway" Cisco VCS Control's zones are set up

For a call to succeed there must be appropriate links between Zones, links must exist from:

- Default Subzone to Traversal Subzone
- Default Subzone to Default Zone
- Default Subzone to Cluster Subzone (*this is required even if Cisco VCS is not part of a cluster)*
- Traversal Subzone to Default Zone

Check these on the **Links** page (**VCS Configuration > Bandwidth > Links**):



If any links are missing, log onto the command line interface and run the command:

```
xcommand DefaultLinksAdd
```

Configure DNS details

Configure the DNS Server details

The “OCS gateway” Cisco VCS(s) should be configured to use the same DNS servers as OCS.

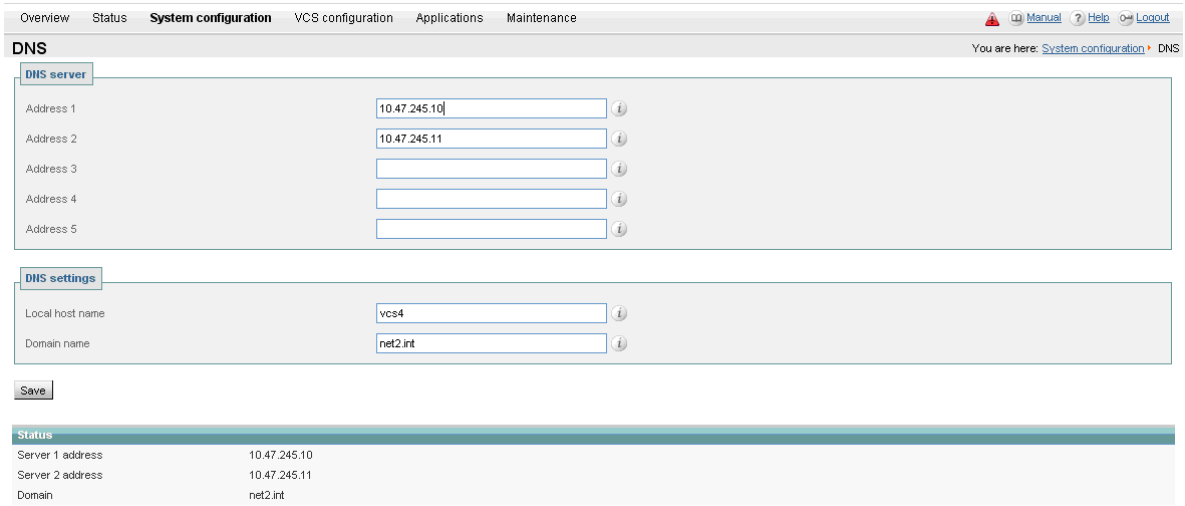
On the machine running OCS:

1. From the Windows **Start** menu choose **Run**.
2. Type `cmd` into the **Open** field and click **OK**. A command window opens.
3. In the cmd.exe window type:
   `ipconfig /all`
4. Note down the DNS servers.

Note: If the DNS server IP address is 127.0.0.1 that means that OCS is using a DNS server on its own hardware. Instead of entering 127.0.0.1 on the Cisco VCS, use the IP address of the OCS platform instead.

On each “OCS gateway” Cisco VCS Control peer:

1. Go to the **DNS** page (**System Configuration > DNS**).



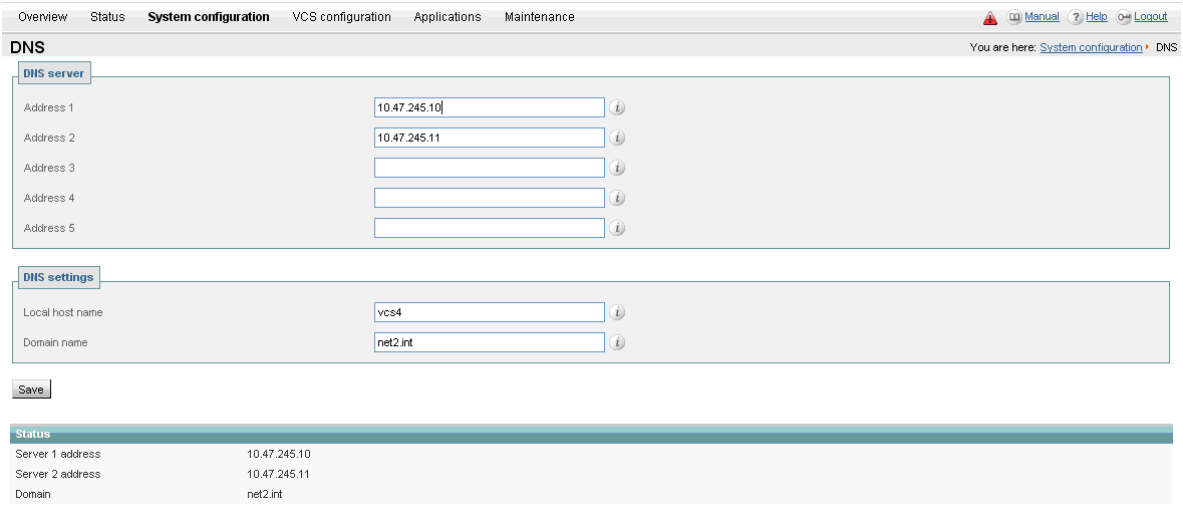
2. Set **DNS Server Address 1** to the IP address of DNS server noted earlier.
3. If OCS has more than one DNS server defined, configure the remaining fields as follows:

DNS Server Address 2	IP address of DNS server 2 (if there is a second DNS server)
DNS Server Address 3	IP address of DNS server 3 (if there is a third DNS server)
DNS Server Address 4	IP address of DNS server 4 (if there is a fourth DNS server)
DNS Server Address 5	IP address of DNS server 5 (if there is a fifth DNS server)

4. Click **Save**.

Ensure that Local hostname and DNS domain are configured

For each “OCS gateway” Cisco VCS peer, ensure that a unique **Local host name** is set up and that the DNS **Domain name** is set up:



1. On the DNS page (**System configuration > DNS**) set:
   - **Local host name** to a unique hostname for this Cisco VCS
   - **Domain name** to the domain name for this Cisco VCS
2. Click **Save**.

Note that the **Local host name** concatenated with **DNS Domain** name is the routable FQDN of this Cisco VCS.

Note: If these are not configured and the connection between OCS and Cisco VCS is TLS, then although the neighbor zone goes active and Cisco VCS can send messaging to OCS, OCS will never open a TLS connection back to Cisco VCS, resulting in no calls OCS to Cisco VCS and other strange behavior.

Ensure that cluster name is configured

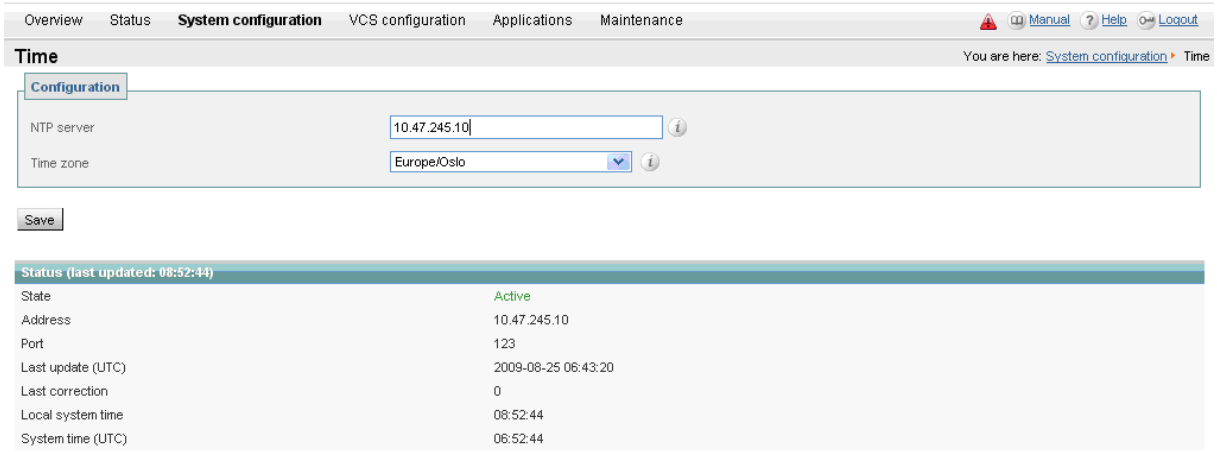
This should be configured whether the Cisco VCS is part of a cluster or not; this value is used with FindMe™ as well as clustering.

For each “OCS gateway” Cisco VCS peer, ensure that **Cluster name** is the same, and is set up to be the FQDN of the cluster. Note that this should have been set up when the cluster was created – see “Cisco VCS Deployment Guide - Creating a Cluster of Cisco VCS peers (Cisco VCS X5) - D1436702”. If the cluster name needs changing follow the procedure in that document.

Configure an NTP server

On each "OCS gateway" Cisco VCS Control peer:

1. Go to the **Time** page (**System Configuration > Time**).

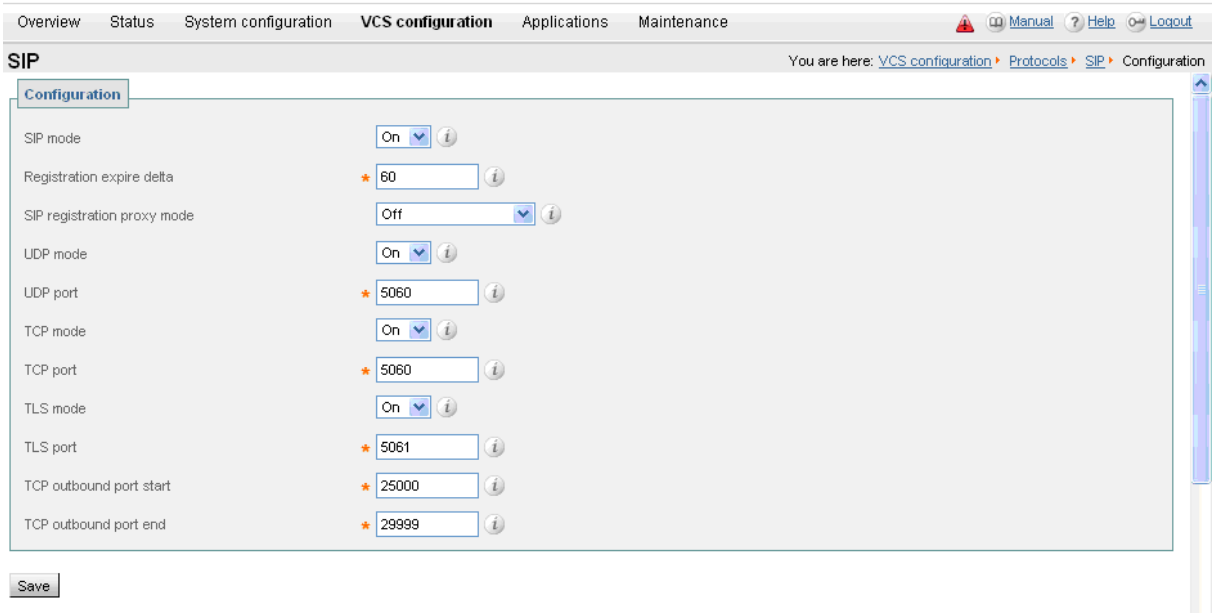


2. Set **NTP server** to the IP address of an NTP server
3. Set **Time zone** as appropriate to the location of the Cisco VCS.

Note: You can find out which time server that windows server is using by typing 'net time /querysntp' from a windows command line

Switch on TLS in SIP configuration (not needed if TCP connection is to be used)

1. Go to the SIP page (**VCS Configuration > Protocols > SIP > Configuration**).



2. Ensure that **TLS mode** is **On**.

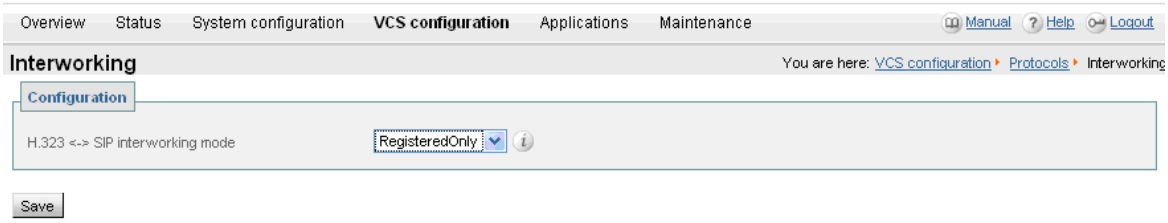
Set up H.323 ←→ SIP interworking

For H.323 endpoints to be able to communicate with OCS, Cisco VCS must interwork the SIP signaling and H.323 signaling.

When H.323 endpoints are interworked to OCS SIP, the Cisco VCS carrying out the interworking needs to know that it is interworking to OCS (as the interworking functionality needs to specifically handle the requirements of OCS), therefore the interworking must be carried out on the "OCS gateway" Cisco VCS.

To ensure interworking is carried out on this "OCS gateway" Cisco VCS, set **H.323 ←→ SIP interworking mode** to **On** (rather than **RegisteredOnly**, as usually recommended).

1. Go to the **Interworking** page (**VCS Configuration > Protocols > Interworking**).

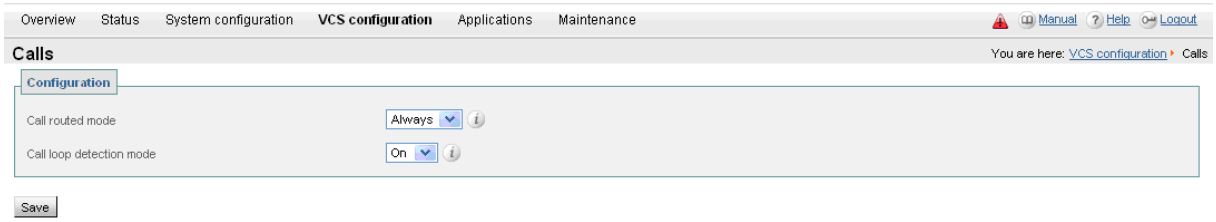


2. Set **H.323 ←→ SIP interworking mode** to **On**.
3. Click **Save**.

Set Call routed mode to Always

Even if the "OCS gateway" Cisco VCS is part of a cluster, and the cluster deployment guide says that Call routed mode should be set to Optimal, when connecting to OCS, Call routed mode must be set to Always, so that the signaling from OCS is always processed by the "OCS gateway" Cisco VCS.

Go to the **Calls** page (**VCS configuration > Calls**)



1. Set **Call routed mode** to **Always**.
2. Click **Save**.

OCS configuration

The configuration will vary depending upon the architecture of the OCS installation.

- If an OCS Director is in use then configure the OCS Director (pool) to trust the "OCS Gateway" Cisco VCS and to route traffic to Cisco VCS. (Other FEPs receiving calls for the Video domain will not know how to route them, so will pass the calls to the Director for routing.)
  - If there is just a hardware load balancer in front of a set of FEP pools, configure each FEP pool.
    - If there is just a single FEP, configure it.

To allow the "OCS gateway" Cisco VCS to communicate with OCS:

1. For a TLS (encrypted signaling) connection between the "OCS gateway" Cisco VCS and OCS (recommended):
   - TLS must be allowed on OCS

   For a TCP connection (not recommended):
   - TCP must be allowed on OCS
2. Configure OCS to trust the "OCS gateway" Cisco VCS(s).
3. Configure Static Route(s) to route calls to the "OCS gateway" Cisco VCS(s).
4. Configure OCS to make media encryption optional.

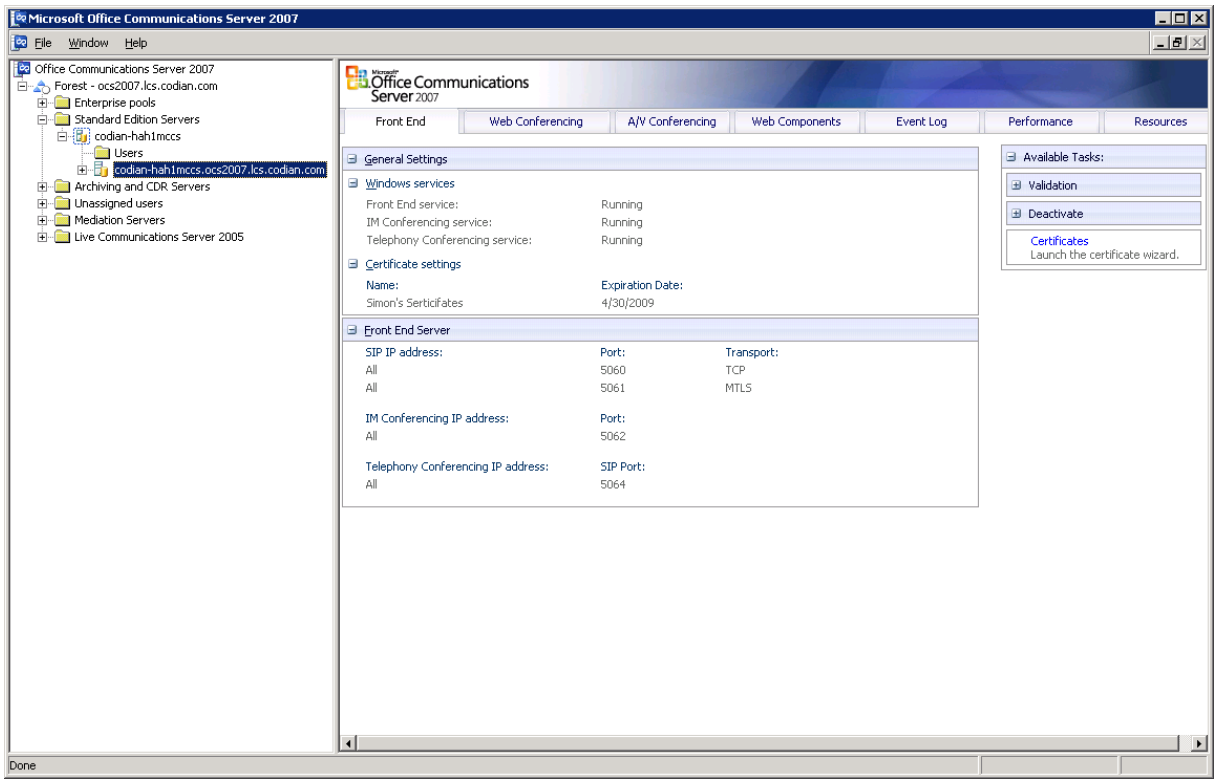
Allow (M)TLS or TCP connection to OCS

MTLS or TCP is configured on each OCS Director, or Each FEP – whichever the Cisco VCS communicates directly with.

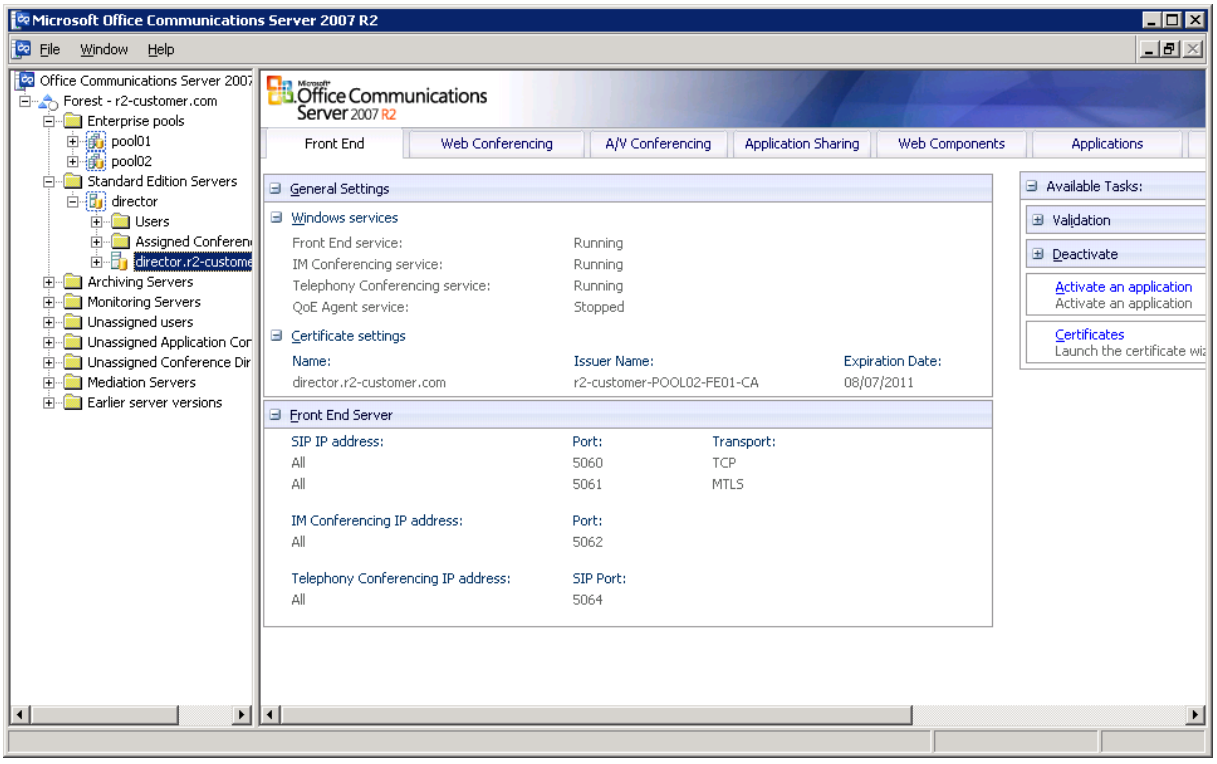
On OCS, for all OCS Directors, or FEPs:

1. Select **Start > Administrative Tools > Office Communications Server 2007**.
2. Select the specific OCS.
   - If an OCS Director is available, then select the OCS Director (pool)
   - otherwise, if a Hardware Load Balancer front ends multiple FEPs select and configure each FEP in turn
   - otherwise, if there is just one FEP, right-click on that one

   For example if using Standard Edition Servers:
   a. Expand **Standard Edition Servers**.
   b. Expand OCS Pool for example, **codian-hah1mccs** or **director**.
   c. If FEPs are being configured, right click on the FEP, e.g. **codian-hah1mccs.ocs2007.lcs.codian.com** and choose **Properties > Front End Properties.**



or if OCS Directors are being configured, right click on the OCS Director and choose **Properties > Front End Properties.**

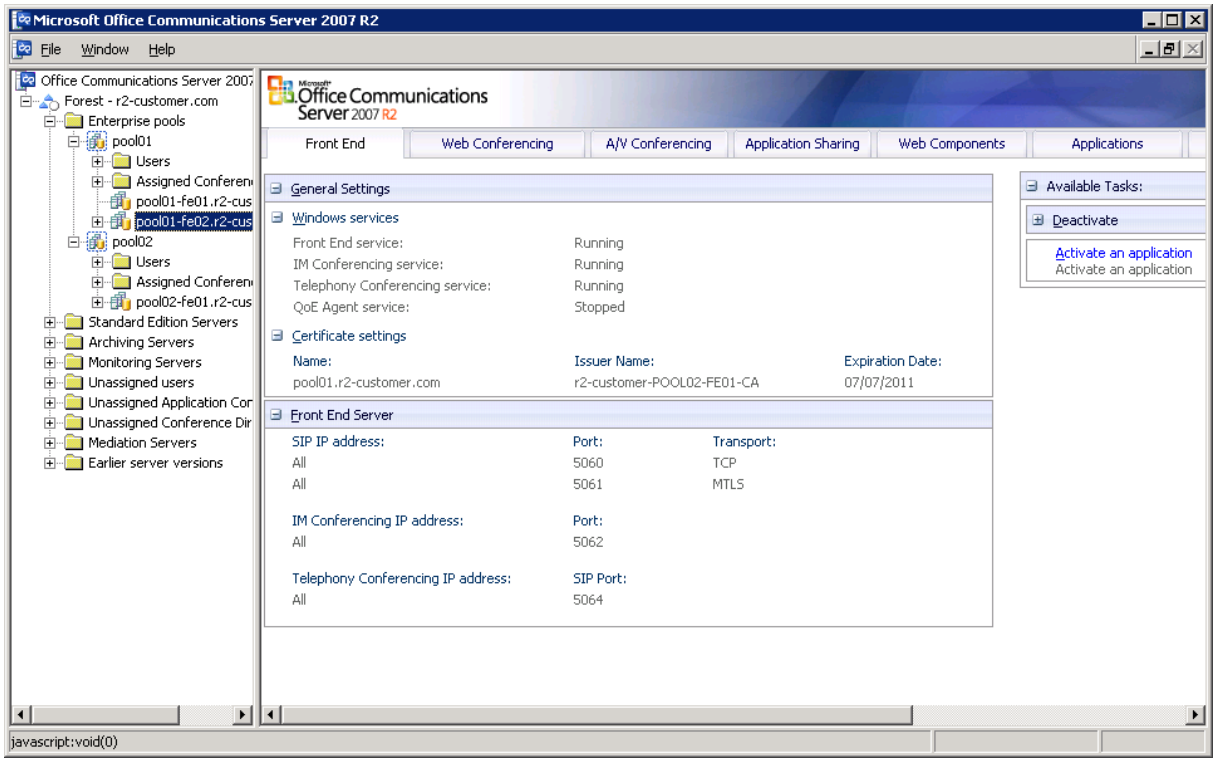


If using Enterprise Edition Servers:

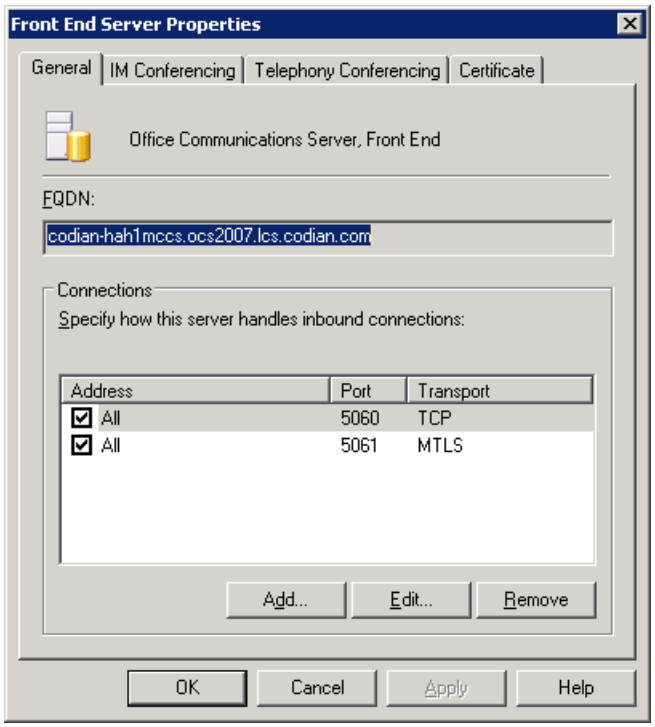
a. Expand **Enterprise Pools**.

b. Expand the required **Pool**.

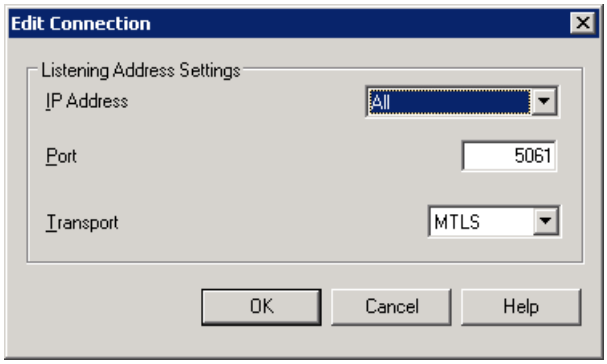
c. Right click on the relevant FEP and choose **Properties > Front End Properties.**



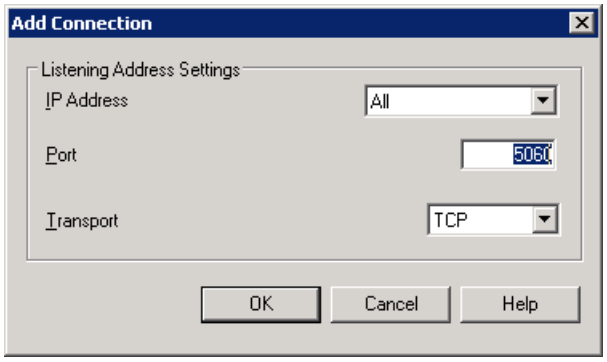
3. Select the **General** tab



4. For TLS (recommended):
   Ensure that there is an entry that allows MTLS (Mutual Transport Layer Security) connectivity on port 5061. Typically this will be allowed from any IP address but could be limited to the "OCS gateway" Cisco VCS(s)' IP address(es). If required, to create a new entry, click **Add**.



   For TCP (not recommended):
   Ensure that there is an entry that allows TCP connectivity on port 5060. Typically this will be allowed from any IP address but could be limited to the "OCS gateway" Cisco VCS(s)' IP address(es). If required, to create a new entry, click **Add**.



5. Repeat steps 2 to 4 for each OCS Director, or if there is no OCS Director, repeat steps 2 to 4 until all FEPs are configured.

Configure OCS to trust the "OCS gateway" Cisco VCS(s)

OCS must be told which devices to trust for the receipt and sending of signaling messages. IF OCS Director is used, configure the OCS Director pool, otherwise configure all FEP pools.
For TLS (recommended):

- Configure the FQDN of all "OCS gateway" Cisco VCSs and the FQDN of the "OCS gateway" cluster as trusted hosts on the OCS.

For TCP (not recommended):

- Configure the IP of all "OCS gateway" Cisco VCSs as trusted hosts on the OCS.

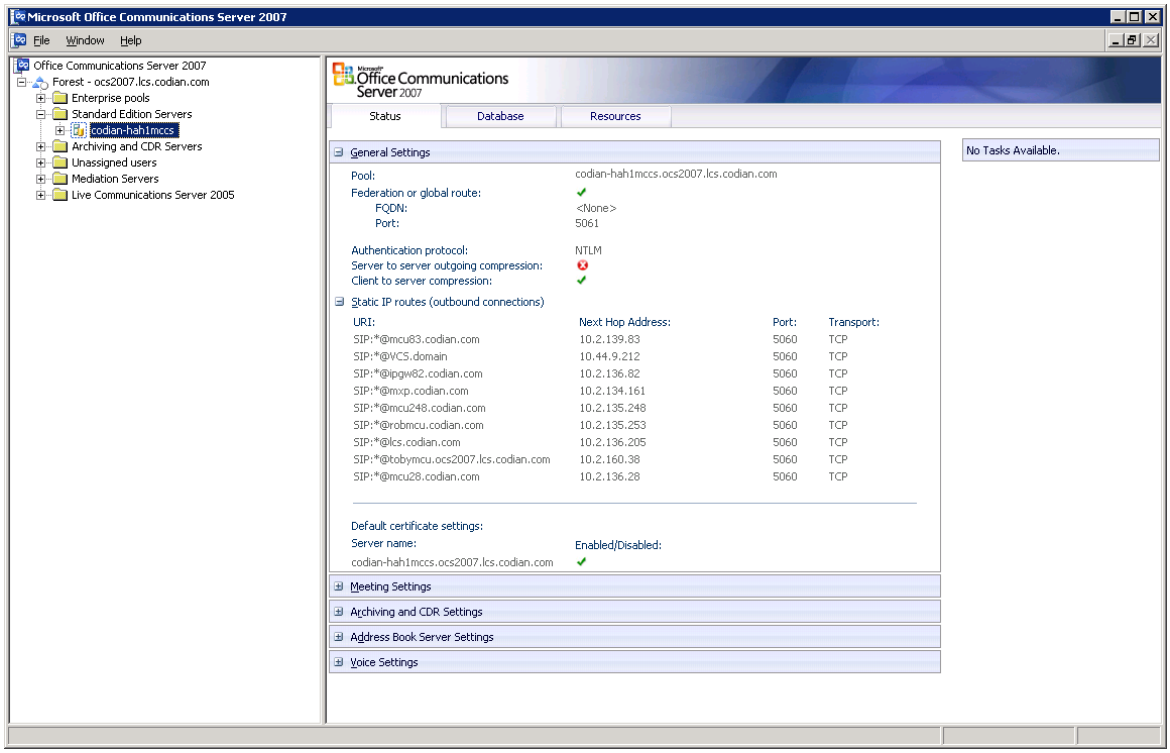
On OCS:

1. Choose **Start > Administrative Tools > Office Communications Server 2007**.
2. Select the specific OCS pool.
   - If an OCS Director is available, then select the OCS Director pool
   - otherwise, if a Hardware Load Balancer front ends multiple FEP pools select and configure each FEP pool in turn
   - otherwise, if there is just one FEP pool, right-click on that one

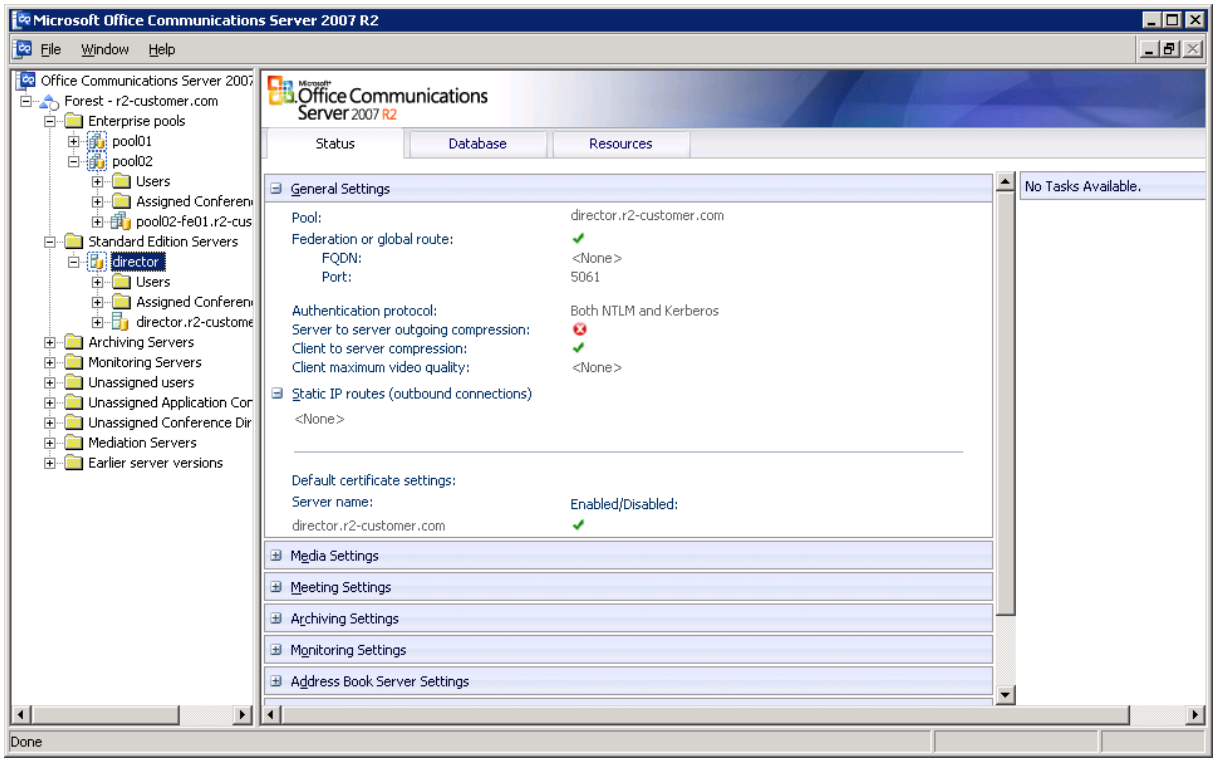
   For example if using Standard Edition Servers:

a. expand **Standard Edition Servers**.

b. right-click on the specific OCS FEP pool and choose **Properties > Front End Properties.**



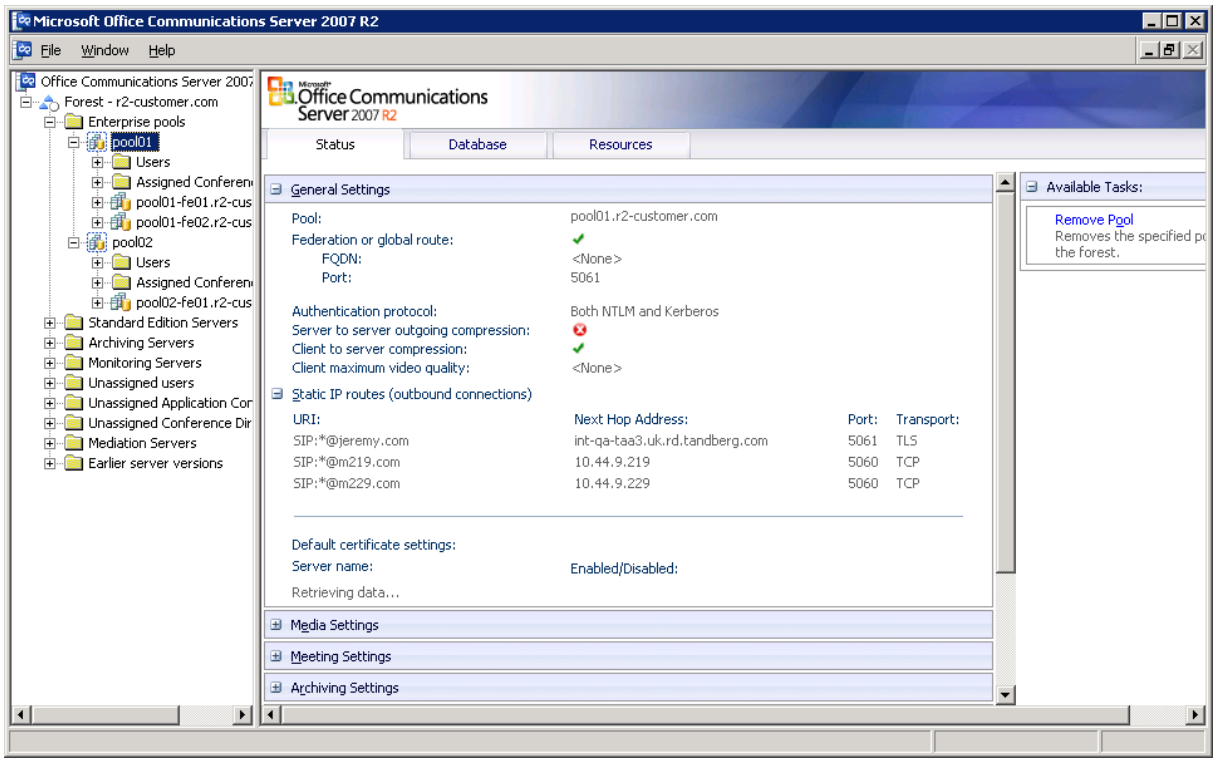
or right click on the OCS Director pool and choose **Properties > Front End Properties.**



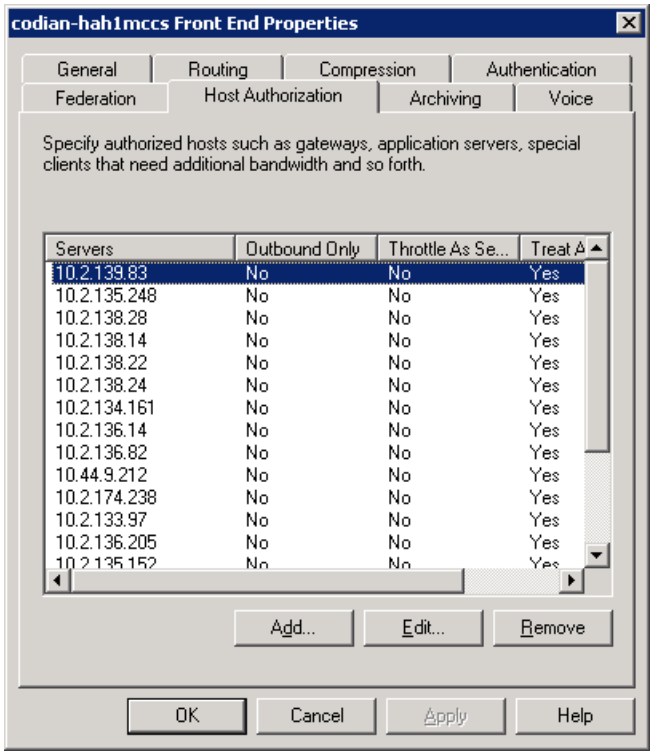
If using an Enterprise Edition Server:

a. expand **Enterprise Pools**.

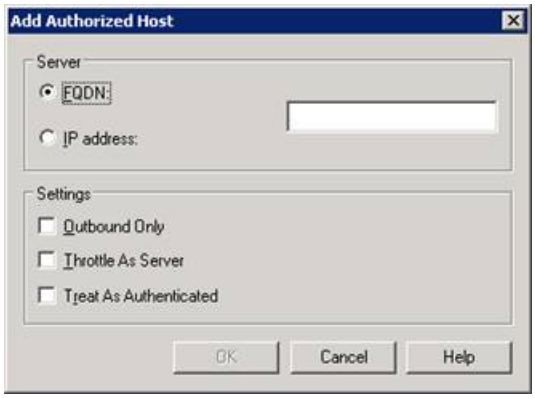
b. right-click on the FEP pool and choose **Properties > Front End Properties.**



3. On the Front End Properties dialog select the **Host Authorization** tab.



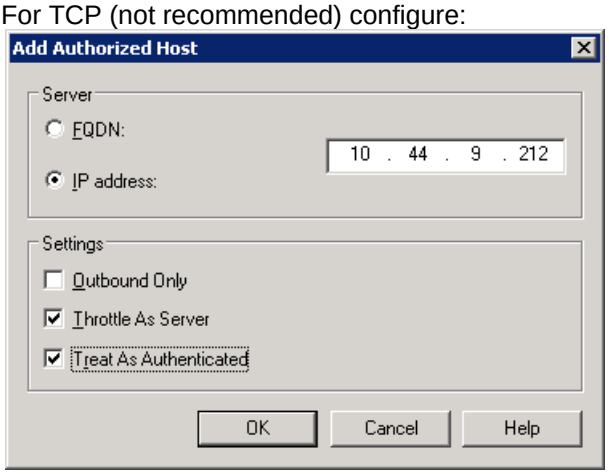
4. Click **Add** or **Edit** (depending on whether a new entry is to be added, or a previous one modified).
5. For TLS (recommended) configure:



FQDN	FQDN of the "OCS gateway" cluster or FQDN of an "OCS gateway" Cisco VCS, for example vcsocsgateway.test-customer.com, or vcsocspeerX.test-customer.com
Outbound Only	Leave unselected
Throttle As Server	Select this check box It reduces the message throttling as it knows the trusted device is a server not a client
Treat As Authenticated	Select this check box

and click **OK**.

For TCP (not recommended) configure:



IP address	IP address of the "OCS gateway" Cisco VCS (or one peer of the "OCS gateway" Cisco VCS cluster)
Outbound only	Leave unselected
Throttle as server	Select this check box It reduces the message throttling as it knows the trusted device is a server not a client
Treat As Authenticated	Select this check box

and click **OK**.

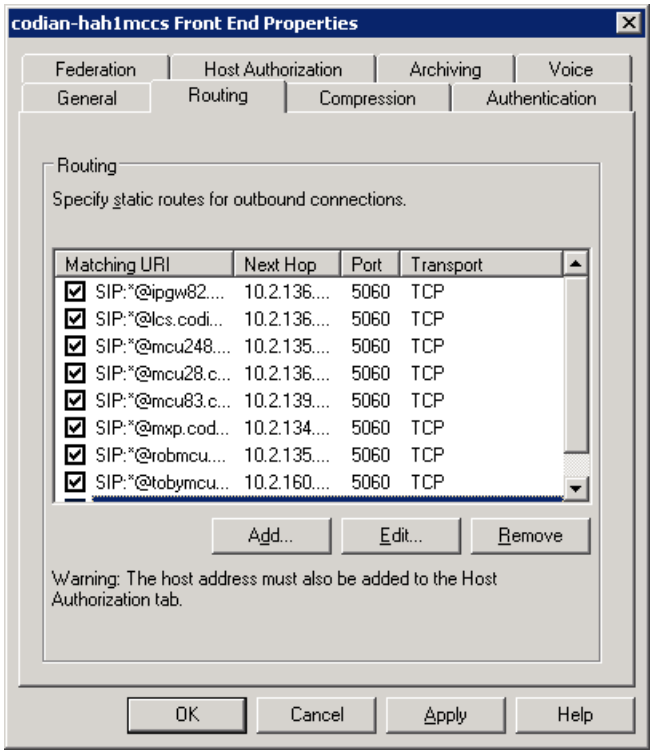
6. Repeat steps 4 and 5 for each "OCS gateway" Cisco VCS peer and, if configuring TLS, the FQDN of the "OCS gateway" cluster.
7. Repeat steps 2 to 6 for all pools that can directly communicate to Cisco VCS.

Configure static route(s) to route calls to the "OCS gateway" Cisco VCS(s)

If a call is to be routed to a Video Network device that is not registered to OCS (i.e. that is not an OCS Relay FindMe™ user), OCS needs to have static domain routes set up to identify which domains are video network domains accessible via the "OCS gateway" Cisco VCS(s).

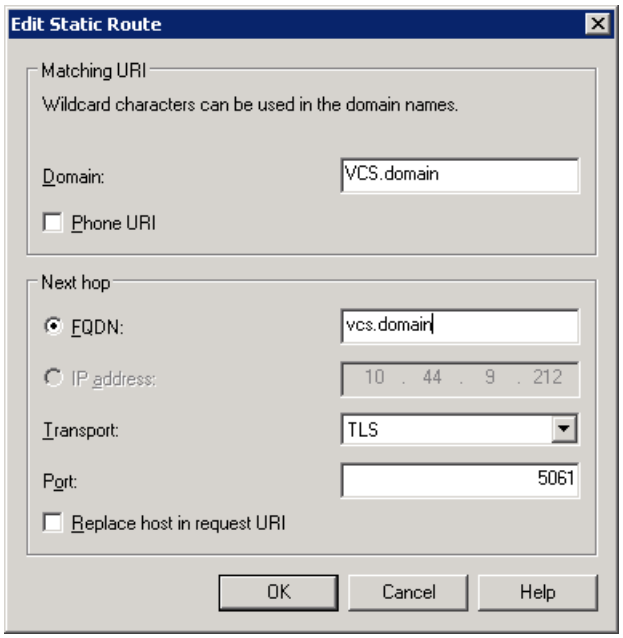
Set up a static route(s) identifying the "OCS gateway" Cisco VCS (cluster) as the recipient of calls to the video network domain(s) (for example .*@vcs.domain).

1. Select the OCS device that will route calls to the "OCS gateway" Cisco VCS:
   - If an OCS Director is available, then select the OCS Director (pool)
   - otherwise, if a Hardware Load Balancer front ends multiple FEP pools select and configure each FEP pool in turn
   - otherwise, if there is just one FEP pool, configure that one
2. Right click on the relevant pool.
3. Select the **Routing** tab.



4. If the video network static route has not been set up, click **Add**, otherwise select the video network static route and click **Edit**.
5. For TLS (recommended) configure:

Domain	Video network domain, for example vcs.domain
Next hop FQDN	FQDN of the "OCS gateway" cluster, or if not clustered the FQDN of the "OCS gateway" Cisco VCS
Next hop Transport	**TLS**
Next hop Port	**5061**

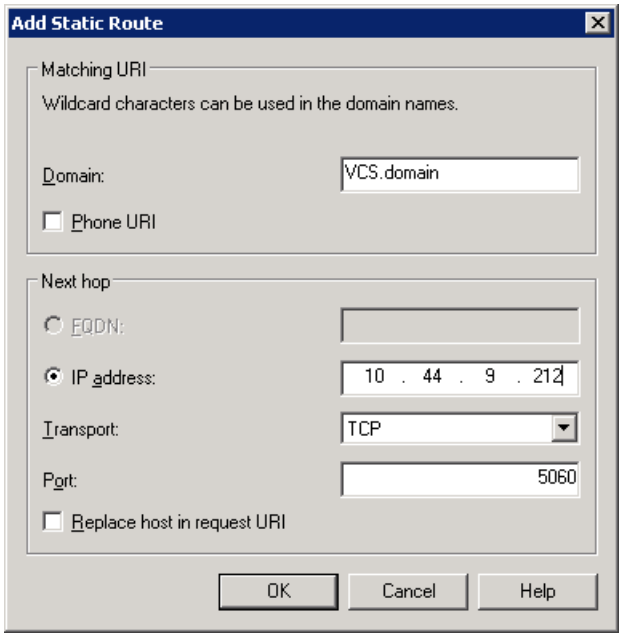


Note: The **FQDN** and the **Domain** do not have to be identical:

- The **FQDN** must be a routable domain name for the "OCS gateway" Cisco VCS / cluster of Cisco VCS peers; a DNS lookup must correctly resolve the FQDN to the IP address of the Cisco VCS / Cisco VCS peers e.g. vcsocsgateway.test-customer.com.
- The **Domain** is the domain to be routed from OCS to Cisco VCS e.g. vcs.domain

For TCP (not recommended) configure:

Domain	Video network domain, for example vcs.domain
Next hop IP address	IP address of the "OCS gateway" Cisco VCS
Next hop Transport	**TCP**
Next hop Port	**5060**



6. Repeat steps 3 to 5 for all domains routable to or through the “OCS gateway” Cisco VCS(s), including the domain shared between OCS and Cisco VCS (If there is a shared domain).

Note: Static routes should be set up for all domains handled by the Cisco VCS, including the domain shared by Cisco VCS and OCS if Cisco VCS and OCS share the same domain.

- If OCS tries to route a call to the domain shared between OCS and Cisco VCS:
  - OCS will first check all its registrations, both OCS MOC registrations and OCS Relay FindMe™ registrations registered to OCS. If any registration is found that matches the called URI the call will be sent to that device, or if multiple registrations exist, the call will be forked to all registered devices that match the URI.
  - If there is no registration and OCS is OCS R2, OCS will then check the static domain routes and if there is one for this domain OCS will route the call to the destination specified.

- If OCS tries to route a call to a domain that is not shared between OCS and Cisco VCS:
  - OCS (both R1 and R2) will check the static domain routes and if there is one for this domain OCS will route the call to the destination specified.

Note: Although the primary access to end users registered on Cisco VCS may be via a specific domain, providing static routes for other domains handled by Cisco VCS means that:

- Endpoints in different domains that may call OCS can be called back using their ‘caller ID’ which may have a domain other than the primary domain.

- When using OCS Relay and OCS and Cisco VCS have the same domain for registered devices, devices like MCUs and ISDN gateways which may register IDs in the same domain as OCS, but not have FindMe™ IDs associated with them (e.g. because they are ad hoc conferences) will be able to be called by OCS (if OCS is OCS R2).

7. Repeat steps 2 to 6 for all pools that can directly communicate to Cisco VCS.

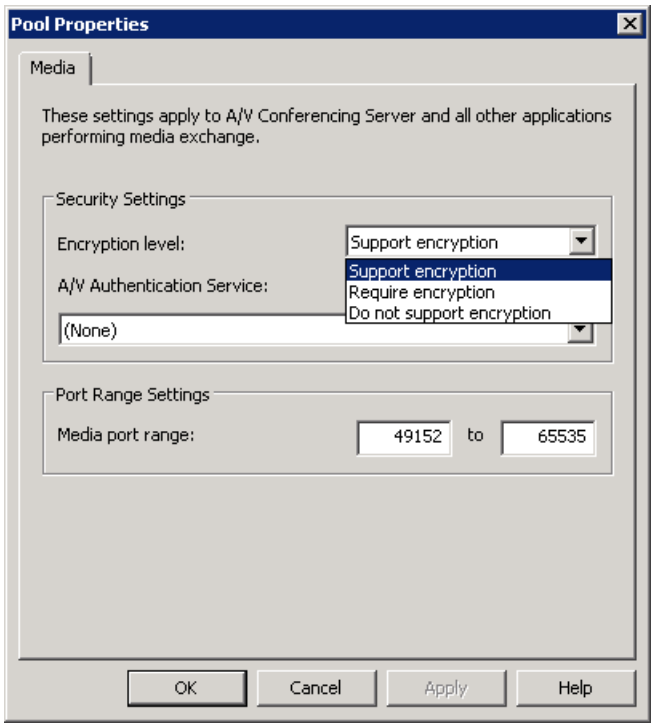
Configure OCS to make media encryption optional

By default OCS mandates the use of encrypted media. The headers used in OCS SRTP, however, are different from those used by video network devices. Calls between the video network and OCS must therefore use unencrypted media, unless you are using Cisco VCS version X5.2 or later with the **Enhanced OCS Collaboration** option key and the connection between the Cisco VCS and OCS is TLS.

If the Cisco VCS is not using the **Enhanced OCS Collaboration** option key or is not connected to OCS via TLS, then the Microsoft Office Communications Server 2007 zone configuration in the “OCS gateway” Cisco VCS(s) handles the signaling to ensure that media encryption is not negotiated. OCS needs to be configured to accept calls where media is not encrypted.

For the OCS Director pool and every OCS FEP pool:

1. Select the Pool.
2. Select **Properties > Pool Properties**.
3. Change **Encryption level** from Require Encryption to **Supports Encryption**
4. Click **Apply.**



Note: This parameter is a value communicated to MOC to affect its operation. To activate this change on a MOC client, the MOC client must be logged off and logged back in again.
It may take a while for the parameter to be shared throughout the pool (up to an hour) so you may have to wait a while before restarting the MOC clients for them take on the new value.

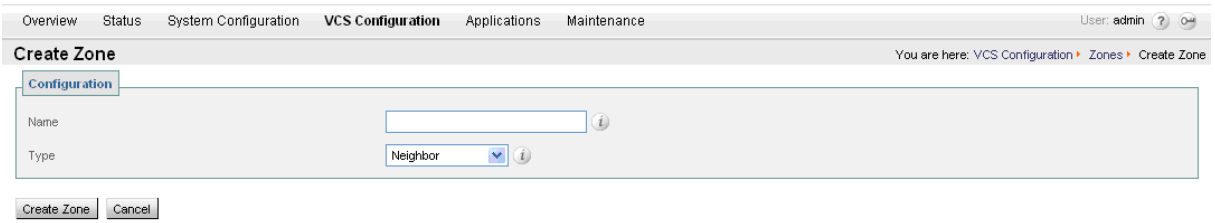
Note: If the **Enhanced OCS Collaboration** option key is installed and the connection between the Cisco VCS and OCS is TLS, then the default setting of **Require encryption** may be left selected. However, be aware that if **Require encryption** is selected, any calls with video endpoints that do not support encryption will fail – in this case **Support encryption** should be selected instead.

"OCS gateway" Cisco VCS Control configuration (2)

1. Configure the "OCS gateway" Cisco VCS with a neighbor zone that contains OCS.
2. Set up a Search rule to select what gets routed to the OCS zone.
3. If Hardware Load Balancers are used, set up neighbor zones to receive calls from OCS

Configure the "OCS gateway" Cisco VCS with a neighbor zone that contains OCS

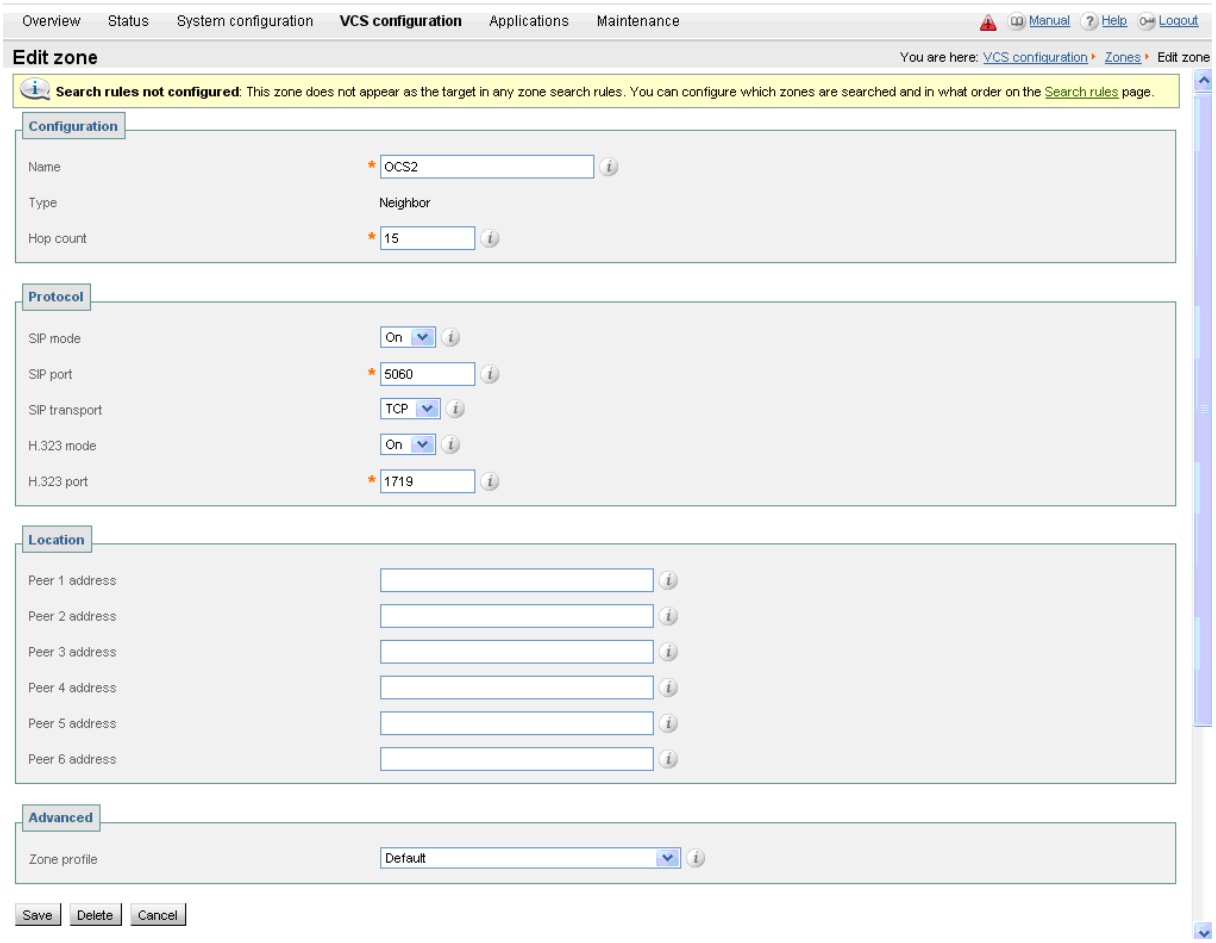
1. Go to the **Zones** page (**VCS configuration > Zones).**
2. Select **New**.



3. Configure the fields as follows:

Name	"OCS"
Type	Neighbor

4. Click **Create Zone**.



It is recommended that the "OCS gateway" Cisco VCS uses SIP over TLS to communicate with OCS.

5. For SIP over TLS configure the following fields:

SIP mode	**On**
SIP port	**5061** (or the value that is the same as that configured on OCS for Cisco VCS access over TLS)
SIP transport	**TLS**

Not recommended, but if SIP over TCP is required, configure the following fields:

SIP mode	**On**
SIP port	**5060** (or the value that is the same as that configured on OCS for Cisco VCS access over TCP)
SIP transport	**TCP**

6. For TLS and TCP configure the following fields:

H.323 mode	**Off** (H.323 access is not required for communication with OCS)
In the **Location** section: **Peer 1 address**	FQDN of OCS (OCS Director, Hardware Load Balancer or FEP as appropriate), for example: enterprisepool.test-customer.com
In the **Advanced** section: **Zone profile**	**Microsoft Office Communications Server 2007**

Note: 'Appendix 5 – Advanced parameters set by selecting zone profile 'Microsoft Office Communications Server 2007' identifies the advanced configuration values that selecting Microsoft Office Communications Server 2007 selects.

7. Click **Save**.

Note: Do not worry about the status section indicating Failed. This will change to Active once the zone's IP address / FQDN has been saved.

Note: OCS does not accept INVITEs with no SDP; it requires the calling party to choose the audio and video codecs. When interworking an H.323 call to Microsoft OCS 2007, Cisco VCS offers a default set of codecs. By default Cisco VCS chooses a sensible audio and video codec for OCS, but see *Appendix 6 – Setting default codecs for H.323 to SIP calls* if it is desired to modify the codecs offered in the initial INVITE of an interworked call.

Set up a Search rule to select what gets routed to the OCS zone

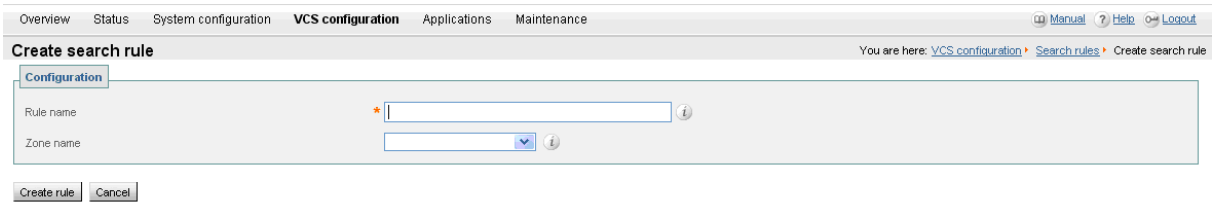
Search rules are used to specify the URIs to be forwarded to this neighbor OCS (for example, by matching the domain of the destination or by matching some element in the URI).

Search rules can also be used to transform URIs before they are sent to a neighbor, for example to add or modify the domain or add, remove or translate user-id prefixes and even to add extra tags to SIP URIs, such as user=phone (see "*Appendix 8 – TEL URI handling for Cisco VCS to OCS calls*" for further information about user=phone).

For this scenario, anything with a domain test-customer.com will be matched (and passed to OCS); no transformation is required.

("*Appendix 7 – Presence with and without transforms*" provides additional details about using transforms and what needs to be done if presence is to be used when transforms are applied in the Search rule.)

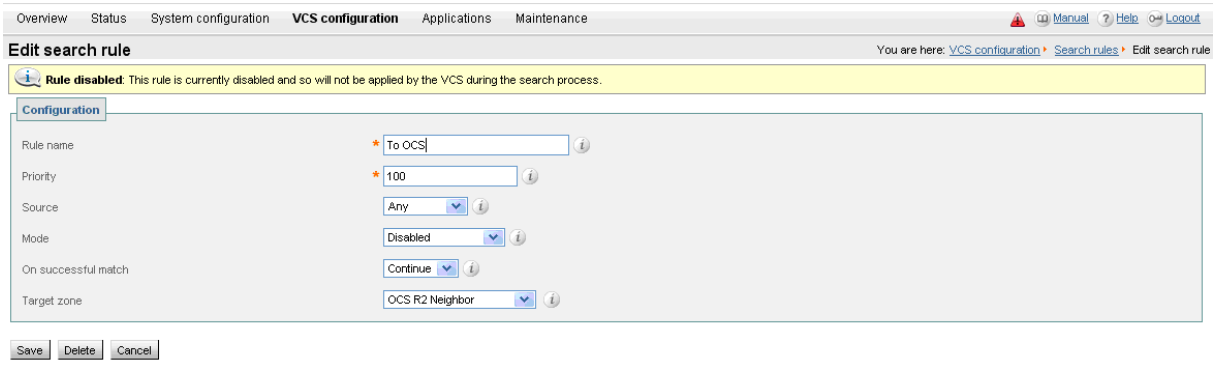
1. Go to the **Search rule** page (**VCS configuration > Search rules > Rules**).
2. Click **New**.



3. Configure the following fields:

Rule name	**To OCS**
Zone name	**OCS**

4. Click **Create rule**.



5. Configure the Search Rule so that all calls to URIs in the format **.*@test-customer.com** are forwarded to OCS. (To handle presence messaging a **.*** is included at the end of the domain to allow any parameters following the domain to be retained in the SIP messaging.)

Priority	**100**
Source	**Any**
Mode	**AliasPatternMatch**
Pattern type	**Regex**
Pattern string	.*@test-customer\.com.*
Pattern behavior	**Leave**
On successful match	**Stop**
Target zone	**OCS**

6. Click **Save**.

See the Zones and Neighbors section of the Cisco VCS Administrator Guide for further details.

Note: Never use a **Mode** of **AnyAlias** - always use a pattern string which matches the OCS registrations as closely as possible so that only calls, notifies and other messages that are handled by this zone get routed to this neighbor.

If **AnyAlias** were to be selected, then all calls and other messages would be routed to the OCS zone — subject to no higher priority Search rules matching — whether or not OCS supports that call or message.

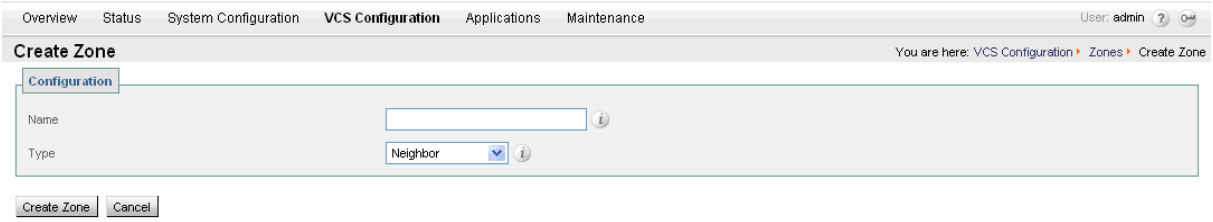
If Hardware Load Balancers are used, set up neighbor zones on the "OCS gateway" Cisco VCS(s) to receive calls from OCS

If Hardware Load Balancers are used then OCS will still send messages to Cisco VCS from the devices directly behind the main Hardware Load Balancer.

If the main Hardware Load Balancer is in front of OCS Directors, then neighbor zones need to be configured that reference the OCS Directors, so that Cisco VCS will treat calls received from these devices as OCS calls.

If the main Hardware Load Balancer is in front of FEPs, then neighbor zones need to be configured that reference all the FEPs, so that calls received from these devices are treated as OCS calls.

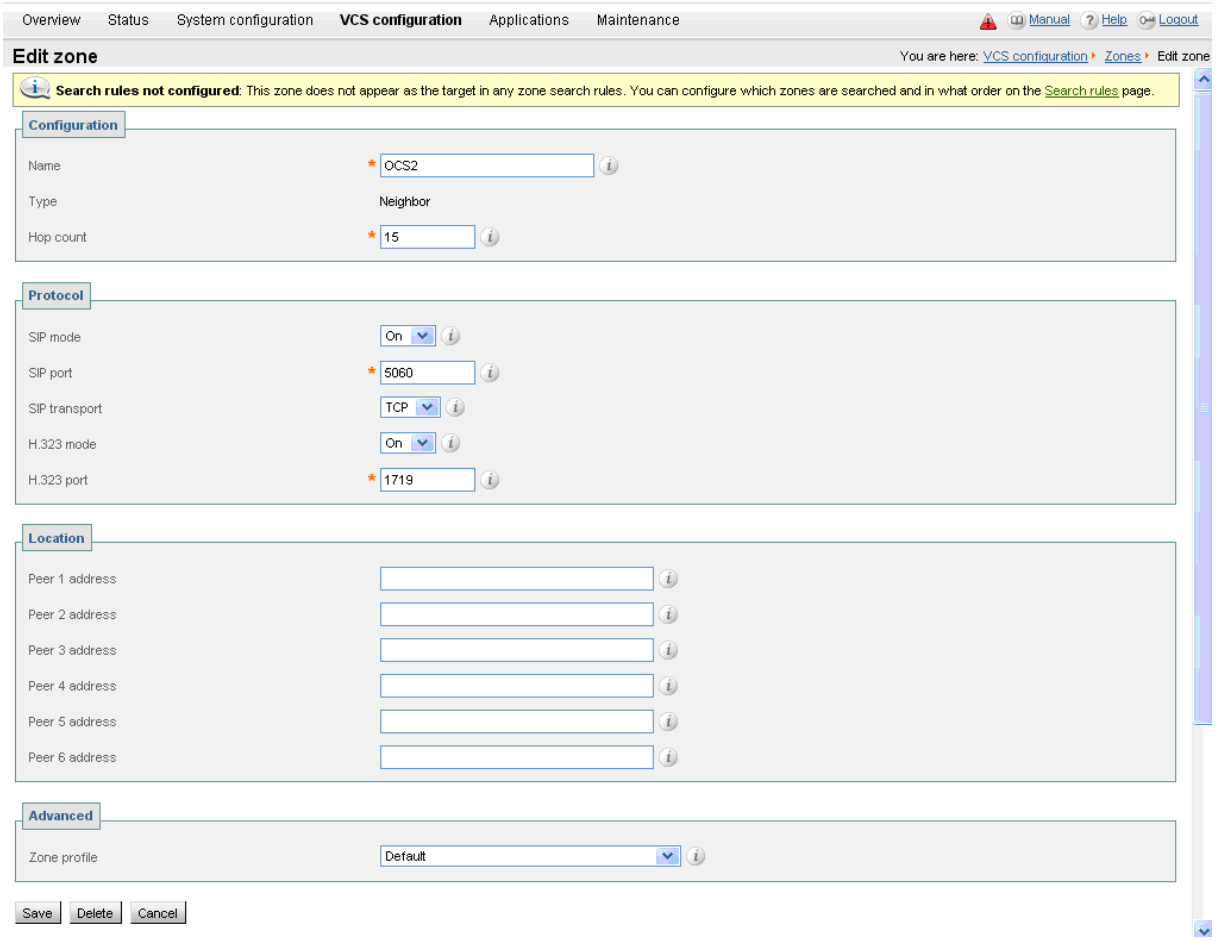
1. Go to the **Zones** page (**VCS configuration > Zones).**
2. Select **New**.



3. Configure the fields as follows:

Name	"OCS receive only 1"
Type	Neighbor

4. Click **Create Zone**.



5. For SIP over TLS configure the following fields:

SIP mode	**On**
SIP port	**5061** (or the value that is the same as that configured on OCS for Cisco VCS access over TLS)
SIP transport	**TLS**

Not recommended, but if SIP over TCP is used, configure the following fields:

SIP mode	**On**
SIP port	**5060** (or the value that is the same as that configured on OCS for Cisco VCS access over TCP)
SIP transport	**TCP**

6. For TLS and TCP configure the following fields:

H.323 mode	**Off** (H.323 access is not required for communication with OCS)
In the **Location** section: **Peer 1 address**	FQDN of an OCS Director or an FEP as appropriate
In the **Location** section: **Peer 2 address**	FQDN of an OCS Director or an FEP as appropriate
In the **Location** section: **Peer 3 address**	FQDN of an OCS Director or an FEP as appropriate – if any more than 2
In the **Location** section: **Peer 4 address**	FQDN of an OCS Director or an FEP as appropriate – if any more than 3
In the **Location** section: **Peer 5 address**	FQDN of an OCS Director or an FEP as appropriate – if any more than 4
In the **Location** section: **Peer 6 address**	FQDN of an OCS Director or an FEP as appropriate – if any more than 5
In the **Advanced** section: **Zone profile**	**Microsoft Office Communications Server 2007**

7. Click **Save**.

Note: Do not worry about the status section indicating Failed. This will change to Active once the zone's IP address / FQDN has been saved.

If there are more than 6 FEPs behind the main Hardware load balancer, add further neighbor zones (each with unique names) until all FEPs are referenced as a Peer x Address.

Note: Do not configure any Search rules to point to these zones. These zones are receive only.

Calls can now be made between SIP and H.323 endpoints registered on the Video Network to MOC clients registered on OCS.

Testing the configuration

Test calls from endpoints registered on the video network to MOC clients registered on OCS.

For example, call steve.hight@test-customer.com or mary.jones@test-customer.com from both SIP and H.323 endpoints registered on Cisco VCS Control.

Enabling MOC clients registered on OCS to call endpoints registered on the video network

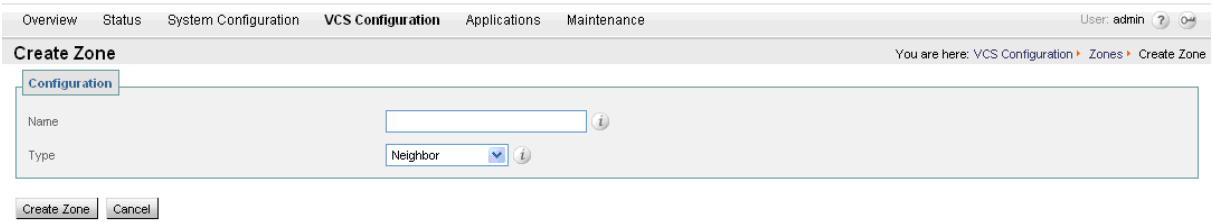
”OCS gateway” Cisco VCS Control configuration

1. Configure the “OCS gateway” Cisco VCS with a neighbor zone that contains the video network.
2. Set up one or more Search rules to route calls with video network domains to the video network.

Note: In small test and demo networks this configuration is not necessary as the video network Cisco VCS is the “OCS Gateway” Cisco VCS. You can skip this section and go to “OCS configuration” on page 53.

Configure the “OCS gateway” Cisco VCS with a neighbor zone that contains the video network

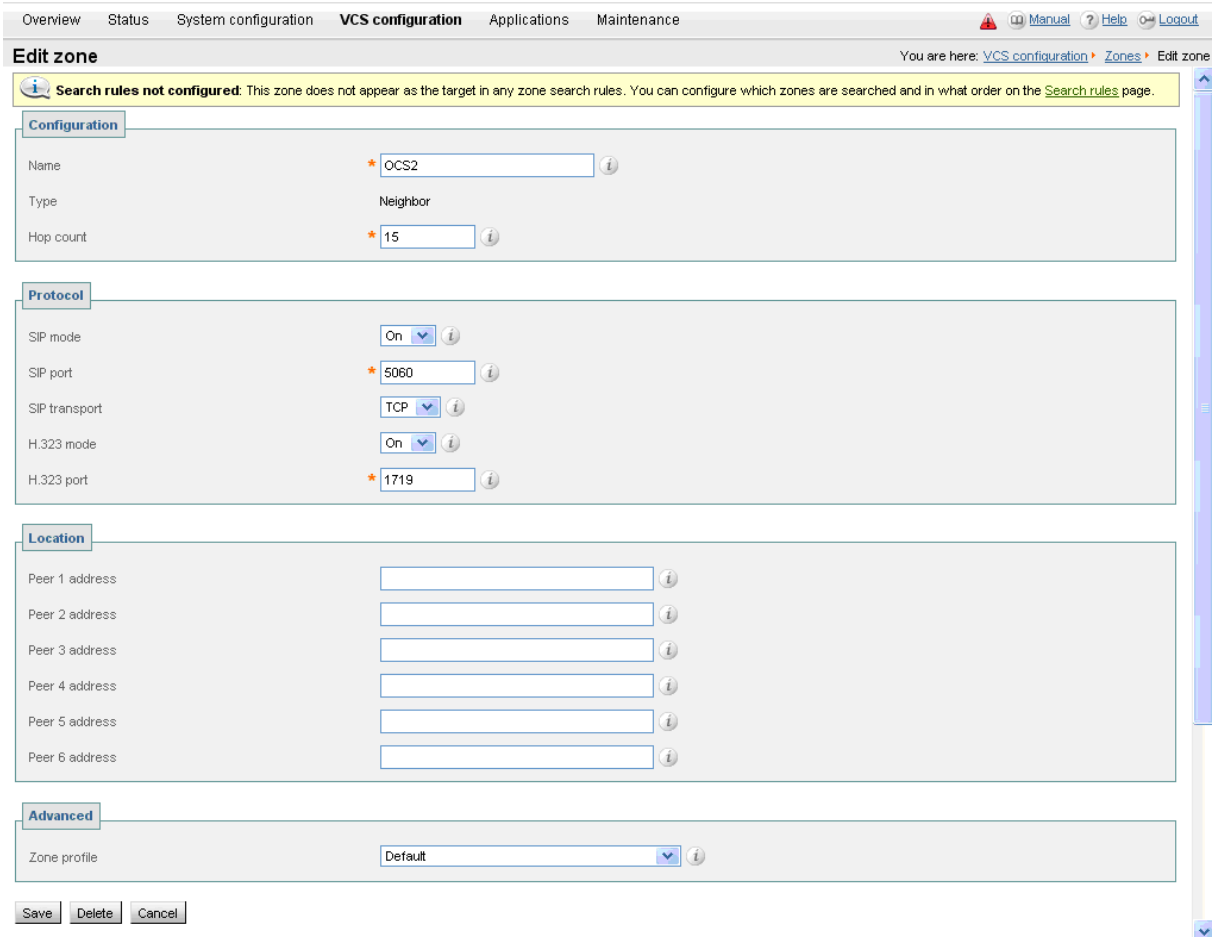
1. Go to the **Zones** page (**VCS configuration > Zones).**
2. Click **New**.



3. Configure the fields as follows:

Name	“To Video network”
Type	Neighbor

4. Click **Create Zone**.



It is recommended that the connection to the "OCS gateway" Cisco VCS uses SIP over TLS to communicate so that encrypted calls can be handled. H.323 mode should also be enabled, so that any interworking that has to be done for calls with OCS is carried out on the "OCS gateway" Cisco VCS.

5. Configure the following fields:

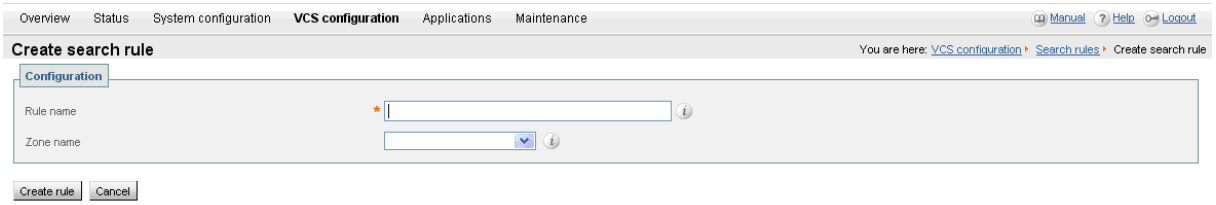
SIP mode	**On**
SIP port	**5061** (or the value that is the same as that configured on the "OCS gateway" Cisco VCS for TLS mode SIP)
SIP transport	**TLS**
H.323 mode	**On**
In the **Location** section: **Peer 1 address**	IP address or FQDN of the video network Cisco VCS (or the 1st Cisco VCS in the Video network cluster)
In the **Location** section: **Peer 2 address** to **Peer 6 address**	IP address or FQDN of the 2nd to 6th video network cluster peers (if any)
In the **Advanced** section: **Zone profile**	**Default**

6. Click **Save**.

Note: Do not worry about the status section indicating Failed. This will change to Active once the zone's IP address / FQDN has been saved.

Set up one or more search rules to route calls with video network domains to the video network

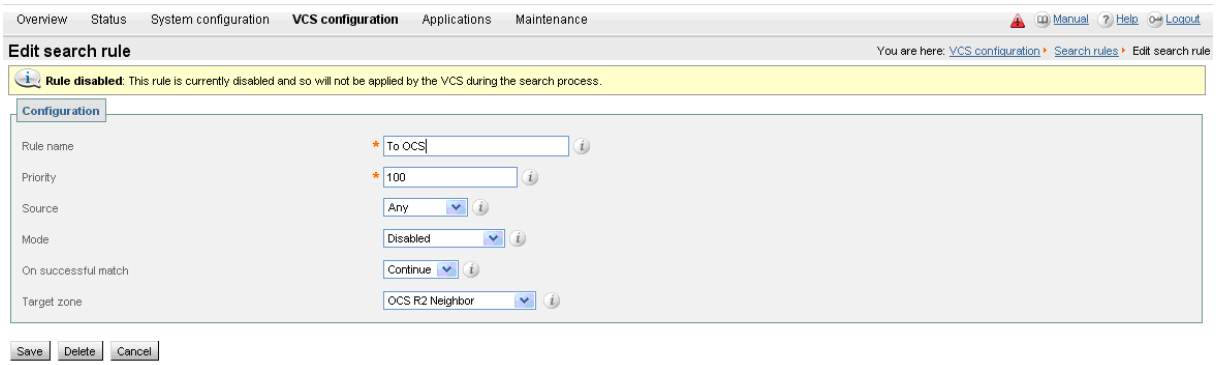
1. Go to the **Rules** page (**VCS Configuration > Search rules > Rules)**
2. Click **New**.



3. Configure the following fields:

Rule name	An appropriate name, for example “Route to Video network”
Zone name	Select the Video network zone, for example **“To Video network”**

4. Click **Create rule**.



5. Configure the Search Rule to match the domain supported in the video network:

Rule name	Leave as set above
Priority	Leave as default, for example 100
Source	**Any**
Mode	**AliasPatternMatch**
Pattern type	**Regex**
Pattern string	Anything in the Video network domain, for example .*@vcs.domain.*
Pattern behavior	**Leave**
On successful match	**Continue**
Target zone	Leave as set above

6. Click **Save**.
7. Repeat until there is a rule for each video network domain.

OCS configuration

No further configuration (beyond that carried out above) is required on OCS to allow calls from MOC clients to endpoints registered on Cisco VCS Control.

Testing the configuration

Test calls from MOC Clients registered on OCS to endpoints registered on Cisco VCS Control.

For example, call mary@vcs.domain or john@vcs.domain from a MOC client registered on OCS.

(Double click on the buddy then click  to make a video call.)

Enabling MOC clients to see the presence status of endpoints registered on Cisco VCS Control

- Using SIP-SIMPLE, OCS only supports the reception of the "available" status, so presence is limited to buddies indicating "gray" (not available), or "green" (available). "In-call" and other rich presence states are not handled by OCS.
- OCS does not supply presence status information about its registered endpoints using SIP-SIMPLE and so no presence information can be supplied to endpoints registered on Cisco VCS about endpoints registered on OCS.
- MOC clients registered to OCS can see the presence status of other MOC clients registered to OCS.
- Endpoints registered to Cisco VCS Control can see the presence status of other endpoints registered to Cisco VCS Control.

In summary:

	… to Cisco VCS	***… to OCS***
Cisco VCS to … *(no OCS Relay)*	*Full presence available*	*Presence = Available only*
Cisco VCS to … *(with OCS Relay)*	*Full presence available*	*Presence = Available and In-Call*
OCS to …	*No presence information available*	*Full presence available*

Cisco VCS configuration

If endpoints registered to the Cisco VCS Control supply their own presence information the Cisco VCS Control can be configured to be a Presence Server, aggregating presence information and providing presence status to users who subscribe for the information.

If endpoints registered to the Cisco VCS Control do not support the generation of presence information, the Cisco VCS Control can be asked to generate it by enabling the PUA (Presence User Agent):

- Cisco VCS PUA generates Presence = available if endpoint is registered
- Cisco VCS PUA generates Presence = In-call if the endpoint is in a call

If an endpoint generates presence and the PUA is enabled, the Cisco VCS Presence Server will aggregate both results – if there are results from the PUA plus just one other Presence Publisher, the Presence Server deems the PUA to be monitoring the other publisher, so the other publisher's status always wins – otherwise the Presence Server will supply the "highest interest" presence information available, for example "in-call" will be reported in preference to "on-line". The Presence Server also supports richer presence information – such as "Busy, in a meeting" – which may be supplied by the endpoint.

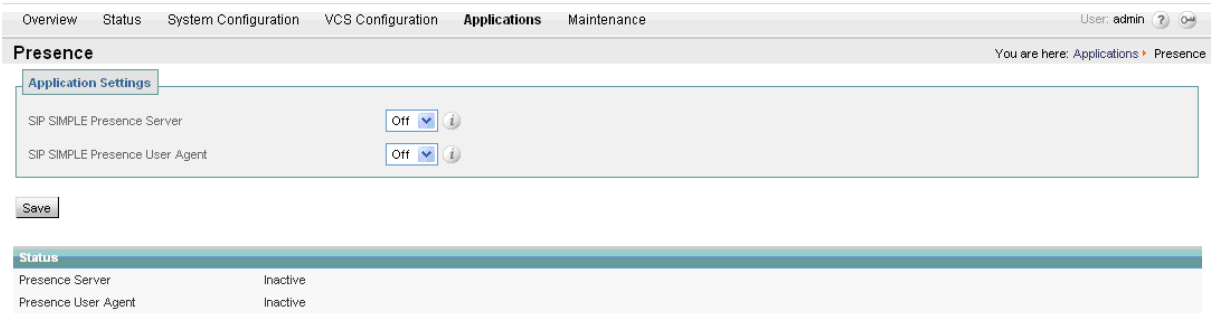
Note: For H.323 devices to supply presence (via the PUA) the registered H323 ID of that endpoint must resemble a SIP URI. The presence will be published for that URI.

To configure presence on the Cisco VCS Control:

1. Go to the **Presence** page **Applications > Presence**.
2. Configure the following fields:

SIP SIMPLE Presence Server	**On**

SIP SIMPLE Presence User Agent	**On** (if Cisco VCS Control is to generate presence information for registered endpoints)



Note: The Cisco VCS that connects to OCS should be the presence server for ALL sip domains that OCS might want to look at for presence; this limits the number of Cisco VCSs that OCS's presence requests will travel through.

Presence requests use up SIP resources and with OCS typically having thousands of MOC clients connected that may be requesting presence, it is best to limit the range of where the presence requests can go, especially not letting them reach Cisco VCSs that already heavily used for taking calls.

For more details on presence see "Presence" in the Applications section of the Cisco VCS Administrator Guide.

OCS configuration

No further configuration (beyond that carried out above) is required on OCS to support presence.

Testing the configuration

Test calls from endpoints registered on Cisco VCS Control to MOC clients registered on OCS.

For example, call steve.hight@test-customer.com or mary.jones@test-customer.com from both SIP and H.323 endpoints registered on Cisco VCS Control.

Set up the endpoints registered on Cisco VCS Control as buddies in MOC.

- See the icon change from gray to green when an endpoint is registered on Cisco VCS Control.
- See the icon change from green to gray if the endpoint becomes de-registered from Cisco VCS Control.

OCS Relay configuration of “OCS gateway” Cisco VCS(s)

The OCS Relay function allows personal video endpoints to appear in a similar manner to an MXP endpoint registered directly to OCS with the same credentials as an existing OC user, but still maintain the benefits of having the endpoint register to the Cisco VCS which is designed to support video calling.

The OCS Relay function also means that the user credentials are no longer needed on each individual video endpoint. This is possible because the Cisco VCS is configured as a trusted host to OCS. This simplifies the long term endpoint management since passwords do not need to be updated on the endpoints.

In which versions can I use OCS Relay?

OCS Relay functionality was introduced into Cisco VCS in version X4.1.

It needs OCS R2 or later to operate properly.

What does OCS Relay do?

When enabled, OCS Relay registers FindMe™ users that are in the same domain as OCS to OCS so that they appear like MOC users to other MOC devices.

This means that if a MOC user registers to OCS, and FindMe™ registers that same ID to OCS, when the ID is called by another MOC device, the call will be forked to both the registered MOC client and also to Cisco VCS’s FindMe™. This means that MOC and all video endpoints configured as primary devices in the FindMe™ will ring when called at the MOC address.

Without OCS Relay and FindMe™, OCS will not fork the call to Cisco VCS, but:

- if a MOC is registered with the called address then just that MOC will ring.
- if there is no MOC registered but there is a static domain route to the Cisco VCS for OCS’s domain and OCS is R2 or later the call will be routed to Cisco VCS to handle.
- if there is no MOC registered and there is no static domain route for this call (or OCS is R1) then the call will just fail.

Note: OCS only allows FindMe™ users to register if the FindMe™ ID being registered is a valid user in the OCS Active Directory (in the same way that MOC users can only register if they have a valid account enabled in the OCS AD).

- OCS Relay also allows the presence of FindMe™ users registered to OCS to provide ‘in-call’ as well as ‘available’ and ‘off-line’ status to MOC users.
  - Endpoint devices and FindMe™ entries that are not registered to OCS can only communicate ‘available’ and ‘off-line’ status to OCS, even if OCS Relay is enabled.
  - Without OCS Relay and FindMe™, Cisco VCS can only communicate ‘available’ and ‘off-line’ status to OCS.

Note: The “OCS gateway” Cisco VCS(s) must host the presence server for the domain of the OCS network (test-customer.com) in order for presence to be provided to OCS.
Presence of a FindMe™ entry can only be provided if the presence status of the device(s) in the active location of the FindMe™ entry are hosted on the “OCS gateway” Cisco VCS(s). The “OCS gateway” Cisco VCS(s) must therefore also host the presence server for the domain of the video network (vcs.domain).
If FindMe™ entries contain multiple devices in the active location, Cisco VCS will aggregate the

presence of those devices whose presence is hosted on the “OCS gateway” Cisco VCS(s) and present the appropriate overall presence status.

Use of FindMe™ also allows any endpoint that is referred to in the FindMe™ to take on the caller ID of that FindMe™ entry. This means that which ever video endpoint makes the call, the receiving MOC and video endpoints will see the call as having come from the FindMe™ ID. This is especially useful when the called party wishes to return the call; the return call calls the FindMe™ ID resulting in all endpoints relating to this FindMe™ and any MOC users registered with this ID all ringing simultaneously – rather than the return call being addressed directly back to the single endpoint that made the call.

OCS Relay and a cluster of Cisco VCSs

From Cisco VCS X5.0 OCS Relay can be enabled in a cluster of Cisco VCSs. When used in a cluster of Cisco VCSs, the OCS Relay FindMe™ users will be shared across cluster peers (using an algorithmic distribution scheme). Each cluster peer will register its own OCS Relay FindMe™ users to OCS. When calls are made from OCS to OCS Relay FindMe™ users OCS will send the call to the Cisco VCS peer that registered that user – hence the calls are statically load-shared across the Cisco VCS peers.

Note: calls to Video endpoint IDs that are not OCS Relay FindMe™ user IDs will not match a registered user, and so will be routed by the static domain route configured in OCS. These calls to non-OCS Relay FindMe™ endpoints will therefore be delivered to a single Cisco VCS peer or a range of Cisco VCS peers (slowly rotating) if a round-robin DNS address is configured in OCS. (When using round-robin, OCS rotates peers approximately once per 5 seconds - this helps with resilience, but is not fast enough to provide effective load sharing.

Configure OCS Relay and FindMe™

It is best practice to keep the video endpoints in their own domain, and just have the FindMe™ users on the “OCS gateway” Cisco VCS with the same domain as OCS. This avoids any confusion as to what functionality will be received for each entity. When a call arrives for the FindMe™ user, FindMe™ will forward calls appropriately to the defined endpoints, whichever domain they are in.

For example, when mary.jones@test-customer.com is called, the call will fork to the MOC client with the same name, and also to mary.jones.office@vcs.domain and mary.jones.external@vcs.domain (assuming that these two vcs.domain devices are listed as primary devices in Mary Jones’ FindMe™.

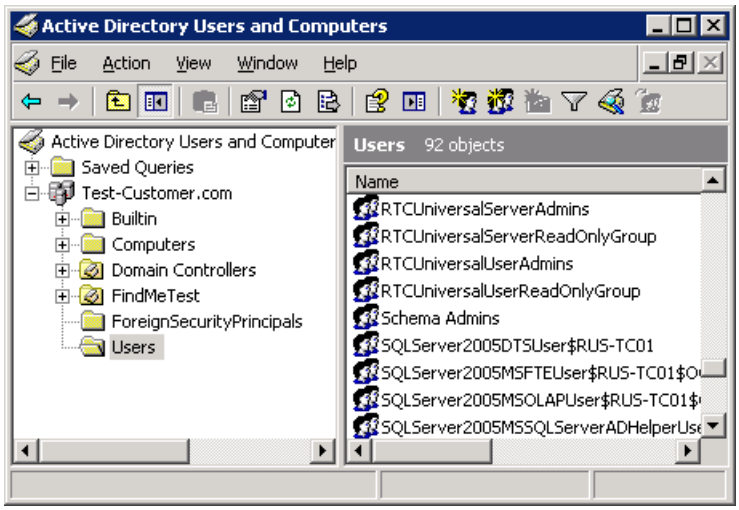
It is strongly recommended that the user is created on OCS first and then FindMe™ accounts created on Cisco VCS 5 to 10 minutes later, when the user is fully available on OCS.

Active Directory configuration

Ensure that Active Directory user accounts exist for all FindMe™ accounts on the “OCS gateway” Cisco VCS(s) that will register to OCS (FindMe™ accounts that have the same domain as OCS).

On the PC running the Active Directory for OCS users:

1. Select **Start > Control Panel > Administrative Tools > Active Directory Users and Computers**.
2. Select the ‘Users’ folder under the required domain:



For each new user that needs to be created:

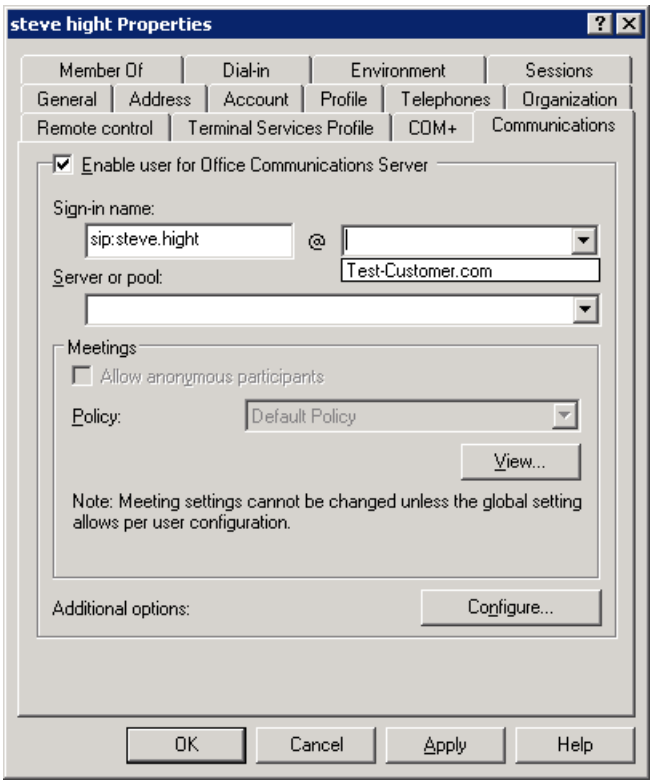
3. Click **Create new user in the current container**.
4. Configure the following fields:

First name	The user’s first name
Last name	The user’s last name
User logon name	The user’s logon name

5. Click **Next**.
6. Configure the following fields:

Password	The user’s password
Confirm password	Retype the password
Password never expires	Select this check box.

7. Click **Next**.
8. Click **Finish**.
9. In the **Active Directory Users and Computers > domain > Users**, right-click on the newly created user and choose **Properties**.
10. Select the **Communications** tab and configure the following fields:
    a. Select **Enable user for Office Communications Server**.
    b. After **sip:** enter the login name.
    c. After @ select the domain name of the server.
    d. Select the **Server or pool**.



11. Click **OK**.
12. Repeat steps 3 to 11 for each new user account that needs to be set up.
13. Wait approximately 10 minutes for Active Directory / OCS to replicate the relevant data.

To verify that OCS now recognizes this new user, log in to MOC as this new user.

“OCS gateway” Cisco VCS Configuration

The shared Cisco VCS / OCS domain **test-customer.com** is highlighted below so that it is easy to see which entries need to be changed to the shared domain used in your installation.

1. Go to the **Option keys** page (**Maintenance > Option keys**).
   In the **Software option** section, in **Add option key**, enter the “User Policy” key (116341U00-1-xxxxxxxx).
2. Click **Add option**.
3. Go to the **FindMe Configuration** page (**Applications > FindMe > Configuration**).
   a. Ensure **Mode** is set to **Local**.
   b. Set **Caller ID** to **FindMeID**.
4. Click **Save**.
5. Configure Cisco VCS to be authoritative for the OCS domain so that FindMe™ users with that domain can be handled by this Cisco VCS and registered as MOC devices to OCS.
   Go to the **Domains** page (**VCS Configuration > Protocols > SIP > Domains**).
6. Click **New**.
7. In **Name** enter the domain shared with OCS (for example, **test-customer.com**).
8. Click **Create domain**.
9. Go to the **SIP** page (**VCS Configuration > Protocols > SIP > Configuration**).
10. Set **SIP registration proxy mode** to **ProxyToKnownOnly**.
11. Click **Save**.

Note: If **SIP registration proxy mode** is already configured as **ProxyToAny** this is also suitable.

12. Ensure that presence is enabled (as described in *Enabling MOC clients to see the presence status of endpoints registered on Cisco VCS Control*).
13. Ensure that the OCS Neighbor zone is set up as described in”“OCS gateway” Cisco VCS Control configuration (2)”.
    (If the OCS Neighbor zone is named anything other than “**OCS**”, then the CPL below must be updated to match the OCS Neighbor zone **Name**.)
14. Modify the “To OCS” Search rule set up in “Set up a Search rule to select what gets routed to the OCS zone”, replace the rule with:

Priority	40
Source	**Any**
Mode	**AliasPatternMatch**
Pattern type	**Regex**
Pattern string	(.*)ocs\.(**test-customer\.com**.*)
Pattern behavior	**Replace**
Replace string	\1\2
On successful match	**Stop**
Target Zone	**OCS**

Note: If multiple domains are supported on OCS, only a single domain can be used with OCS Relay functionality (Cisco VCS registering as a MOC) – other domains should be handled using the Search rules configured previously.

15. Click **Save**.

Note: The CPL below converts calls to test-customer.com destined for OCS to calls to ocs.test-customer.com.
A second Search rule, as defined in ‘OCS receiving Presence from non-OCS Relay FindMe™ entries, where there is a transform for Cisco VCS devices accessing OCS’ (in *Appendix 7 – Presence with and without transforms*) is not necessary for OCS to see the presence of OCS Relay FindMe™ users. The OCS Relay communicates presence to OCS using Microsoft signaling.

16. Create a text file containing the following call policy (CPL), but replacing **test-customer.com** with the name of the sip domain shared between the Cisco VCS and OCS (and also the zone name if not “**OCS**”). Save it as a “.txt” file.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
   xmlns:taa="http://www.tandberg.net/cpl-extensions"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
      <taa:routed>
     <!-- VCS / OCS CPL version 1.3 -->
         <taa:rule-switch>
            <!-- Don't fork calls from OCS back to OCS -->
            <taa:rule originating-zone="(OCS|AMGW)" destination="(.+)@test-customer\.com">
               <proxy />
            </taa:rule>
            <!-- Only send to OCS things sent to OCS's contact details (e.g. presence Notify)-->
            <taa:rule origin="(.*)" destination="(.+)@test-customer\.com;opaque=user:epid.*">
               <taa:location clear="yes" regex="(.+)@(.+);.*" replace="\1@ocs.\2">
                  <proxy />
               </taa:location>
            </taa:rule>
            <!-- Fork other calls to OCS -->
            <taa:rule origin="(.*)" destination="(.+)@test-customer\.com">
               <taa:location clear="no" regex="(.+)@(.+)" replace="\1@ocs.\2">
                  <proxy />
               </taa:location>
            </taa:rule>
         </taa:rule-switch>
      </taa:routed>
</cpl>
```

Note: Take care when copying CPL – non printing characters may cause CPL not to load, giving an error message such as:

17. Go to the **Call Policy configuration** page (**VCS Configuration > Call Policy > Configuration**).
18. Set **Call Policy mode** to **On**.
19. Click **Save**.
20. Upload the new policy file:
    a. Click **Browse**.
    b. Select the text file (“.txt” created above) containing the CPL and Select **Open**.
    c. Click **Upload file**.
21. Set FindMe™ to present the FindMe™ ID (rather than the endpoint ID) when any device in the primary list of FindMe™ devices makes a call – so that when a called party rings the caller ID back all FindMe™ endpoints ring, not just the endpoint that made the initial call will ring.
    a. Go to **Application > FindMe > Configuration**.
    b. Set **Caller ID** to **FindMeId**.
22. For each OCS user that is to share MOC and Cisco VCS endpoints, create a FindMe™ user account on the Cisco VCS with the same URI as the OCS user.
    a. Go to the **FindMe™ accounts** page (**Maintenance > Login accounts > FindMe accounts**).
    b. Click **New**.
    c. Configure the following fields:

Username	Username used by the FindMe™ user to log in to Cisco VCS to administer this account

Display name	Full name of this user
Phone number	E164 number to use when outdialing to a gateway
FindMe ID	URI with OCS’s domain that will register to OCS as though it were a MOC
Principal device address	Routable endpoint URI / E164 or H.323 ID to call when this FindMe™ is called.
Initial password	Password needed by the FindMe™ user to log in to Cisco VCS to administer this account
Confirm password	As Initial password

23. Make sure the domain shared with the OCS is DNS resolvable, usually by adding the OCS server as a DNS server address on the Cisco VCS. See “Configure the DNS” above.
24. Configure the OCS Relay App on the Cisco VCS:
    a. Go to the OCS Relay page (**Applications->OCS Relay**).
    b. Configure the following fields:

OCS Relay mode	**On**
OCS Relay domain	**test-customer.com**
OCS Relay routing prefix	**ocs** (the default value)

Note: OCS Relay can take up to 3 minutes to pick up a new OCS Relay FindMe™ entry and register it. If a number of entries get deleted and the same number get added, it can take OCS Relay up to 60 minutes to observe the change in identities and update the registrations.

Verify FindMe™ accounts are registered

After the FindMe™ accounts have been configured for at least 60 seconds:
1. Go to the **OCS Relay** status page (**Status > Applications > OCS Relay**).
2. Verify the following for each FindMe™:
   - Registrations state is Registered
   - Subscription state is Active
   - Presence state is Online

If the states are not as expected, verify that the FindMe™ and OCS (Active Directory) registered names are identical.

Testing the Configuration

- Test that calls to OCS registered FindMe™ users from Cisco VCS registered endpoints fork to Cisco VCS registered endpoints listed in the FindMe™ entry and also to the MOC client for this user.
- Test that calls to OCS registered FindMe™ users from MOC clients fork to the MOC client and also to Cisco VCS registered endpoints listed in the FindMe™ entry for this user.
- Test that the presence of Cisco VCS endpoints is reflected in MOC presence – log out of the MOC client for a user and check that the Off-Line, Available and In-Call status of the Cisco VCS endpoint listed in the relevant FindMe™ is presented as the presence state in a MOC client watching presence for that user.

Appendix 1 - Troubleshooting

Problems connecting Cisco VCS Control local calls

Look at Search History to check the applied transforms.

1. Go to the **Search history** page (**Status > Search history**).

   Search history entries report on any searches initiated from a SETUP/ARQ /LRQ in H323 and from an INVITE/OPTIONS in SIP. The summary shows the source and destination call aliases, and whether the destination alias was found.
2. Select the relevant search attempt. The Search History for that search attempt shows:
   - the incoming call's details
   - any transforms applied by admin or user policy or cpl
   - in priority order, zones which matched the required (transformed) destination, reporting on:
     - any transforms the zone may apply
     - found or not found status
     - if not found, the error code as seen in the zone's search response
     - repeated until a zone is found that can accept the call, or all prioritized zone matches have been attempted.

   (the search may be 'not found' due to lack of bandwidth or because the search from the zone resulted in an H.323 rejection reason or a non 2xx response to a SIP request)

   If the Search indicates:
   - **Found**: False
   - **Reason**: 480 Temporarily Not Available

   it is likely that the Cisco VCS's zone links are not correctly set up. From the command line execute:

   ```
   xcommand DefaultLinksAdd
   ```

   to set up the required links for Cisco VCS default zones. Also check the links for other zones that have been created.

Note: Each H.323 call will have 2 entries in the Search History:

- An ARQ to see if the endpoint can be found.
- The Setup to actually route the call.

The ARQ search does not worry about links or link bandwidth, and so if links do not exist or link bandwidth is insufficient it may still pass, even though the Setup search will subsequently fail.

Each SIP call will usually only have a single Search History entry for the SIP INVITE.

Look at 'Call History' to check how the call progressed

1. Go to the **Call history** page (**Status > Call History).**

   The summary shows the source and destination call aliases, the call duration and whether the call is a SIP, H.323 or SIP< -- >H.323 interworking call.
2. Select the relevant call attempt.

   The entry shows the incoming and outgoing call leg details, the call's status and the zones that the Cisco VCS Control used to route the call.

Check for errors

Event log

Check the **Event log** (**Status > Logs > Event log**).

Real time detailed event log

To obtain a more detailed log of key events and errors, start up netlog level 1 logging and then try the call or initiate a presence action.

1. Log in to Cisco VCS Control as **admin** using an SSH or Telnet connection.
2. At the prompt type:
   ```
   netlog 1
   ```
3. To turn off tracing, at the prompt type:
   ```
   netlog off
   ```

Information displayed between typing netlog 1 and netlog off contains the key events and error messages that occurred between those two times.

Tracing calls

Tracing calls at SIP / H.323 level

1. Log in to Cisco VCS Control as **admin** using an SSH or Telnet connection.
2. At the prompt type:
   ```
   netlog 2
   ```
3. To turn off tracing, at the prompt type:
   ```
   netlog off
   ```

Information displayed between typing netlog 2 and netlog off contains the SIP and H.323 messaging received and sent out by the Cisco VCS.

Information displayed by netlog 2 includes the key event and error message information reported by netlog 1. Viewing netlog 1 and netlog 2 information separately can be useful so that netlog 1 messages are not lost within the detailed SIP / H.323 messaging.

Presence not observed as expected

Presence Server status

- To check who is providing presence information to the Cisco VCS Presence Server:
  - Go to **Status > Presence > Publishers**

- To check whose presence is being watched for (on domains handled by Cisco VCS Presence Server):
  - Go to **Status > Presence > Presentities**

- To check who is watching for presence (of one or more entities in domains handled by Cisco VCS Presence Server):
  - Go to **Status > Presence > Subscribers**

No presence being observed

Check that there is no transform that may be inadvertently corrupting the presence Publication, Subscription or Notify – e.g. that there is no transform modifying the presence URI. (Notifies are sent to the subscription contact ID, typically <name>@<IP address>:<IP port>;transport=xxx. Any transforms that modify this are likely to stop the presence Notify being routed appropriately)

MOC client fails to update status information

If a MOC client is started before the presence server is enabled, the MOC client may need to be logged out and logged back in again before it will display the correct presence information.

Check for errors

Checking for presence problems should be carried out in the same way as checking for errors with calls: check the event log (available from the web browser) and the syslog 1 log. If there are still problems, trace the SIP messaging using syslog 2.

TLS Neighbor zone to OCS is active, and messaging gets sent from Cisco VCS to OCS, but OCS debug says OCS fails to open a connection to Cisco VCS.

The Local host name and Domain name fields must be configured in the Cisco VCS System configuration > DNS page so that Cisco VCS can use the Cisco VCS hostname (rather than IP address) in communications. OCS requires use of Cisco VCS hostname in order to open a TLS connection to the Cisco VCS.

OCS initiated call fails to connect

If a call fails to connect, check that the endpoint, IP Gateway, MCU or ISDN Gateway is NOT in Microsoft mode; ensure that it is in Standard or Auto mode. (From a netlog 2 trace, an indication that the device is in Microsoft mode is the presence of a “proxy=replace” field in the contact header of the OK from the device.)

Call connects but clears after about 25 seconds

If a call connects but almost immediately clears, this is likely to be because the ACK to the OK is not getting through.

Cisco VCS to OCS calls fail – DNS Server

Cisco VCS needs to have details about DNS names of OCS pools etc, and so needs to have one of its DNS entries set to point to the OCS’s DNS server. (On Cisco VCS go to **System configuration > DNS**, and check the **DNS server address**).

Cisco VCS to OCS calls fail - HLB

If the OCS has FEPs with an HLB in front, ensure that the Cisco VCS is neighbored with the HLB. If it is neighbored with an FEP directly, trust for Cisco VCS will be with the FEP. Cisco VCS will send call requests to the FEP, but the FEP will record-route the message such that the ACK response should be sent to the HLB. The ACK sent to the HLB gets rejected by OCS, so OCS clears the call after the SIP timeout due to the FEP not seeing the ACK.

(Calls MOC – registered to the FEP – to Cisco VCS may still work.)

Calls between MOC and an endpoint that is not registered to the OCS gateway Cisco VCS clear shortly after connecting

Check that **Call routed mode** is set to **Always** on the **VCS configuration > Calls** page.

One way media: MOC → endpoint registered to Cisco VCS

When using Microsoft Edge Server

When MOC registers to OCS through a Microsoft Edge Server, the local IP address and port that the MOC declares are usually private and un-routable (assuming that MOC is behind a firewall and not registered on a public IP address). In order to identify alternate addresses to route media to, the MOC uses ICE candidates.

Handling MOC ICE candidates is not supported in Cisco VCS up to and including Cisco VCS X5.

Calls should connect OK, and media should flow from MOC to the video endpoint. Audio and video from the endpoint are unlikely to be received by MOC, because the destination information is encoded in the MOC ICE candidate lines.

When using a Hardware Load Balancer in front of OCS

Cisco VCS modifies the application part of INVITEs / OKs received from MOC to make them compatible with traditional SIP SDP messaging. Cisco VCS only does this when it knows that the call is with OCS. If there are problems with one-way media (media only going from MOC to the Cisco VCS registered endpoint), check the Search history and ensure that the call is seen coming from an OCS neighbor zone.

If it is not, then the call may be coming from a FEP rather than the load balancer. See the section on configuring Cisco VCS and Hardware Load Balancers, and set up the relevant neighbor zones without any associated search rules, but with Peer addresses containing the FEP IPs.

OCS rejects Cisco VCS zone alive OPTIONS checks with '401 Unauthorized' and INFO messages with '400 Missing Correct Via Header'

- A response '400 Missing Correct Via Header' is an indication that OCS doesn't trust the sender of the message.
- A response '401 Unauthorized' response to OPTIONS is another indication that OCS doesn't trust the sender of the OPTIONS message.

Ensure that the Cisco VCS sending these message is included in the OCS's Front End Processors > Host Authorization list.

Note, this can be seen if a load balancer is used in front of the OCS, and OCS is configured with the Host Authorization authorizing the Cisco VCS – OCS sees calls coming from the hardware load balancer rather than from the Cisco VCS. See *Appendix 13 – Cisco VCS and hardware load* balancers.

MOC stays in 'Connecting …' state

MOC does not change into the connected state until it receives RTP (media) from the device it is connecting to.

No audio on audio call through an ISDN gateway

- Upgrade Cisco TelePresence ISDN GW to version 1.5.

Prior to version 1.5 the ISDN GW sent RTP traffic from SSRC = 0; MOC would not accept RTP traffic with SSRC = 0.

From version 1.5 the ISDN GW sends RTP traffic from a random, non zero, SSRC and MOC receives this correctly.

No video through an ISDN gateway

Some ISDN endpoints initiate a call using one set of codecs, then before media is sent, change the codecs to better codecs (for example an initial offering of H.261 is updated to H.263). Neither MOC R1, nor MOC R2 accepts a change in codec before media is sent.

To work around this, “Meet me” on a conference, so that the ISDN endpoint sets up a call and connects to the MCU and MOC sets up a call and connects to the MCU independently.

Call to PSTN or other device requiring caller to be authorized fails with 404 not found.

In Some OCS configurations, especially where OCS PSTN gateways are used, calls are only allowed to be made if the calling party is authorized. This actually means that the calling party’s domain must be the OCS’s domain.

For calls from endpoints that are not part of a FindMe™ this means that the endpoints must register to the video network with a domain that is the same as the OCS domain.

For calls from endpoints that are part of a FindMe™ the endpoints can register with any domain so long as the FindMe™ ID has the same domain as OCS and in the FindMe™ configuration Caller ID is set to FindMeID (instead of IncomingID).

MOC endpoints try to register with Cisco VCS Expressway.

SIP video endpoints usually use DNS SRV records:

- _sips._tcp.<domain>
- _sip._tcp.<domain> and
- _sip._udp.<domain>

in that order to route calls to Cisco VCS.

MOC uses:

- _sipinternaltls._tcp.<domain> - for internal TLS connections
- _sipinternal._tcp. <domain> - for internal TCP connections (only if TCP is allowed)
- _sip._tls. <domain> - for external TLS connections
- _sip._tcp.<domain> - for external TCP connections (R1 only)

_sip._tcp.<domain> is common to both when MOC R1 is used on an external network. From R2 MOC only supports TLS connection to the Edge Server. The _sip._tcp.<domain> DNS SRV record should be used for the Cisco VCS Expressway. Configure MOC to use encryption (set OCS to ‘Supports encryption’ – as specified in the configuration process) and ensure that TCP is not forced in the Advanced section of the sign in address configuration on MOC.

OCS Relay problems

OCS Relay FindMe™ users take a long time to register.

OCS Relay can take up to 3 minutes to pick up a new OCS Relay FindMe™ entry and register it. If a number of entries get deleted and the same number get added, it can take OCS Relay up to 60 minutes to observe the change in identities and update the registrations.

OCS Relay FindMe™ users fail to register.

If OCS Relay fails to register FindMe™ users (Registration status = failed), check:

1. The FindMe™ name is correctly entered into Active Directory.
2. A MOC client can register as the FindMe™ name.
3. The Cisco VCS **SIP registration proxy mode** is set to **ProxyToKnownOnly** (or **ProxyToAny**).
4. That there is no transform that may be inadvertently corrupting the registration – e.g. appending an **@domain** to a name which contains no @ (as registrations proxied to OCS have a URI which is the **domain** only - no @).
5. Check cpl is as defined in the 'OCS Relay configuration of "OCS gateway" Cisco VCS(s)' section.
6. Check that the zone details have been updated as defined in 'OCS Relay configuration of "OCS gateway" Cisco VCS(s)'.

Troubleshooting OCS Relay

OCS Relay produces an event log file that contains useful information about its operation.

This is only available through root login to Cisco VCS. It is a big file and so it is usually best to 'tail' the file to look at the last few entries.

To view the last 300 entries of the OCS Relay log file:

1. Login as root on Cisco VCS
2. Type:
   ```
   tail -300 /mnt/harddisk/log/elbe.log
   ```

OCS problems

As a starting point, running the OCS 'Best Practices Analyzer' will help identify configurations that may be incorrect on OCS. Details and the download may be found at: http://www.microsoft.com/downloads/details.aspx?FamilyID=62f9fb8e-1f08-4a94-b21b-9cc7fe4550de&displaylang=en

OCS running on Microsoft Server 2008 R2

Operation of TLS has been changed in this version of Server software – this version is not recommended for use.

OCS stops running after an upgrade

Ensure that Automatic upgrades are turned off. There are occasions when an upgrade comes through which will affect operation of OCS. Check the validity of the upgrade before installing.

Do not install upgrade KB974571.

Problems with certificates

If a non-OCS application is used to create certificates to load onto Cisco VCS for use with OCS (e.g. purchased from a certificate authority) it is vital that the Subject name and Subject Alternate Name contain the same details as they would if the certificates were created by OCS.

Specifically, if both Subject name and Subject Alternate Name are used, then the name entered in the Subject name must also appear in the Subject Alternative Name list.

Appendix 2 – Known interoperating capabilities

SIP and H.323 endpoints making basic calls

- SIP and H.323 endpoints can make calls via Cisco VCS Control to MOC clients registered to OCS.
- MOC clients registered to OCS can make calls to SIP and H.323 endpoints on Cisco VCS Control.

Upspeeding from a voice call to a video call

If a voice call is made from a MOC client to a video endpoint registered to Cisco VCS Control and then the video button is selected to enhance the call to a video call, the video endpoint will correctly up-speed to video.

Note that:

- Endpoints must connect to the Cisco VCS using TCP not TLS, and must be in SIP mode.
- Interworking a MOC client to an H.323 endpoint, the call will only up-speed from voice to video if the up-speed request occurs before the endpoint sends a BRQ lowering the connection bandwidth.

Multiway™ generation of ad hoc conferences

Endpoints can join OCS R2 MOC clients into an ad hoc conference using the Multiway™ feature. See the “Cisco VCS Multiway™ deployment guide”.

Cisco VCS Cluster and OCS Relay

The OCS Relay feature is able to run in a cluster of Cisco VCS peers from version X5.

Appendix 3 – Benefits of using Cisco VCS with OCS

Separate management of video systems and PC based systems

Video managers can manage the video endpoints in the Cisco VCS environment that they know, and IT managers can focus on managing the PCs without needing to learn about video.

Cisco VCS brings H.323 integration to OCS

OCS works with SIP. Cisco VCS Control works with SIP and H.323 and can interwork H.323 calls to SIP calls allowing H.323 endpoints to be used in the OCS environment.

Duo Video

Sharing presentations in a conference is not supported in OCS, but it is supported by Cisco VCS.

Bandwidth management

The Cisco VCS uses the concept of pipes which allow you to apply bandwidth restrictions to a link. This ensures that calls are not attempted if they would overload a link's bandwidth. If a link's bandwidth would be exceeded, the call may be diverted to a different zone (link), down-sped to a lower bandwidth or rejected – depending on configuration.

The Cisco VCS bandwidth management operates on calls where:

- media traverses the Cisco VCS (traversal subzone)
- the source or destination device is in the Cisco VCS's local zone (default subzone, and IP addresses specified by explicit subzones)

For other calls, e.g. neighbor zone to neighbor zone non-traversal calls, where Cisco VCS has no idea of where or how the media is routed, it cannot perform bandwidth management.

FindMe™

FindMe™ allows users to set up groups of video endpoints / phones to ring when a call arrives. So, for example, the video phone can ring at the office, in the home office and on the laptop soft video phone at the same time – giving the highest likelihood of the person being able to answer their video call.

FindMe™ also allows devices to be called if the primary set are not answered or are busy, for example, to route them through to a mobile phone or video mail so that the call can always be handled.

FindMe™ can be configured such that calls from any device in the FindMe™ active location will present the FindMe™ ID as the caller ID

Appendix 4 – Known interoperating limitations

Video codecs

If MOC (Microsoft Office Communicator) is used, then the video endpoints registered to the Cisco VCS Control must support H.263; this is the common video codec supported by endpoints and the MOC client. (The MOC client does not support H.264.)

Video codec selection

When the Cisco VCS Control receives an H.323 call destined for OCS, the Cisco VCS must interwork the call to SIP and generate a SIP INVITE to send to the OCS. OCS does not support INVITES with no SDP – in other words, without a list of codecs that can be used for the call, so the Cisco VCS Control must populate the SDP with a "pre-chosen" list of codecs from which the OCS can select.

The codecs offered and selected, therefore, may not reflect the best codecs that could have been selected by the endpoints.

Joining a MOC conference (AV MCU)

Using a MOC client to invite a third party to join the call does not work whether the third endpoint is the endpoint registered to the Cisco VCS Control or whether the endpoint registered to the Cisco VCS Control is already in the call and another MOC client is introduced into the call.

This is because when the MOC client invites a third party to join a call, the MOC client tries to create a conference using Microsoft proprietary messaging (xml in SIP messages), and this is not supported by standards-based video endpoints.

Neither Cisco VCS Control nor standards-based video endpoints support the Microsoft proprietary signaling.
Note, however use of Multiway™ on endpoints can join MOC clients into an ad hoc conference. See the Cisco VCS Multiway™ deployment guide.

Up-speeding from a voice call to a video call

Interworking a MOC client to an H.323 endpoint, the call will only up-speed from voice to video if the up-speed request occurs before the endpoint sends a BRQ lowering the connection bandwidth.

MOC accessing OCS through Microsoft Edge Server

When MOC registers to OCS through a Microsoft Edge Server, the sdp from MOC contains Microsoft ICE candidates, and the non local candidate needs to be used.

This functionality is not supported in Cisco VCS X5. Calls made from an endpoint registered to Cisco VCS to MOC should work, but calls made from MOC to an endpoint registered to Cisco VCS are likely to result in audio and video on the endpoint registered to Cisco VCS, but no video or audio on MOC.

Microsoft Mediation Server

Using OCS R1

Calls to Microsoft Mediation Servers are not supported by Cisco VCS.

Using OCS R2

Calls to Microsoft Mediation Servers work from endpoints in the Cisco VCS Video Network for SIP initiated calls, but do not work for interworked H.323 initiated calls (the mediation server does not respond to the Cisco VCS INFO message, sent to check availability of the destination number).

A workaround is possible if the format of the numbers that will be routed to the mediation server can be configured into Cisco VCS: make a second zone to OCS, select the **Custom** Zone profile, select the same options as would be selected if the **Microsoft Office Communications Server 2007** Zone profile had been selected and in addition select 'Searches are automatically responded to'=On. Then configure one or more Search rules so that calls destined for the mediation server are routed to this zone rather than to the standard Microsoft Office Communications Server 2007 zone.

Cisco VCS Cluster without OCS Relay

OCS does not have a way of load balancing calls to a cluster of Cisco VCSs. There is no way to tell OCS that there are multiple peers to receive calls for the Cisco VCS domain, and OCS will not load balance on a DNS SRV record, and there is a limit in OCS (and Windows) that the min TTL on Round Robin DNS is 5 minutes.

Use of Cisco VCS clusters with OCS and without OCS Relay therefore provides resilience, not extra capacity.

No audio on audio call through an ISDN gateway

Prior to version 1.5 the Cisco TelePresence ISDN GW sent RTP traffic from SSRC = 0; MOC would not accept RTP traffic with SSRC = 0. From version 1.5 the ISDN GW sends RTP traffic from a random, non zero, SSRC and MOC receives this correctly.

No video through an ISDN gateway

Prior to X5 there was an issue with ISDN endpoints that initiated a call using one set of codecs, then before sending media, changed the codecs to "better" codecs (for example, an initial offering of H.261 updated to H.263). Neither MOC R1, nor MOC R2 accepts a change in codec before media is sent.

In X5 Cisco VCS delays sending the original capabilities for 7 seconds to wait and see if they will get updated.

MOC receives no video if it holds and then resumes a call

MOC does not request fast picture updates and so unless full frames are automatically sent from time to time by endpoints this results in no video on the MOC.

Video will be seen by MOC when using:

- MXP F8.0 or later SIP - as this supports the auto-generation of full video frames
- Cisco VCS X4.2 or later for calls interworked with H.323 endpoints – as Cisco VCS interworking supports the auto-generation of full frame update requests.

Even with these fixes, sometimes MOC complains that it has no audio device configured when selecting resume … follow MOC's instructions to update the audio device and resume will then work.

DTMF

MOC R1 generates in-band DTMF only – this is good as it will work with any recipient requiring DTMF, whether the call is delivered to the endpoint as a SIP call or whether the call is delivered interworked to H.323.

MOC R2 generates RFC2833 DTMF only – this causes problems if the OCS call is interworked by Cisco VCS to H.323. Although Cisco VCS interworks the signaling, it does not interwork out-of-band DTMF, instead the Cisco VCS interworking function does not accept the request from OCS to use RFC 2833 telephone events. With MOC R2, if a recipient H.323 device needs DTMF key entry (e.g. for PIN entry) rather than supplying DTMF as in-band tones when the DTMF selection is made, it just reports to the user that it cannot send the RFC 2833 tones.

Microsoft Server

In Microsoft Server 2008 R2 the TLS configuration has changed. This has been seen to cause problems with Cisco VCS connecting to OCS over TLS, and also cause problems for OCS components to talk to one another if connecting over TLS.

At this stage it is recommended that Microsoft Server 2008 R2 is not used as the server to install OCS components on.

Further details on changes and limitations imposed when using Microsoft Server 2008 R2 may be found on the Microsoft support site: http://support.microsoft.com/kb/982021/.

Microsoft Servers recommended are:

- Microsoft Server 2003
- Microsoft Server 2003 R2
- Microsoft Server 2008

Call forward from MOC to a Cisco VCS FindMe™ or endpoint results in a 'loop detected' call.

If a call from Cisco VCS is made to a MOC Client which has a forward to another Cisco VCS registered endpoint or a FindMe™ then Cisco VCS sees this as a looped call.

FindMe™ Caller ID set to FindMeID causes calls from MOC to fail

If:

- FindMe™ Caller ID is set to FindMeID and
- a MOC client's URI is in the active location of a FindMe™ and
- a call is made from that MOC to a SIP destination

the call will fail because OCS does not like the caller ID (From: header) being modified.

If the call is interworked on the "OCS gateway" Cisco VCS, the call will work as required.

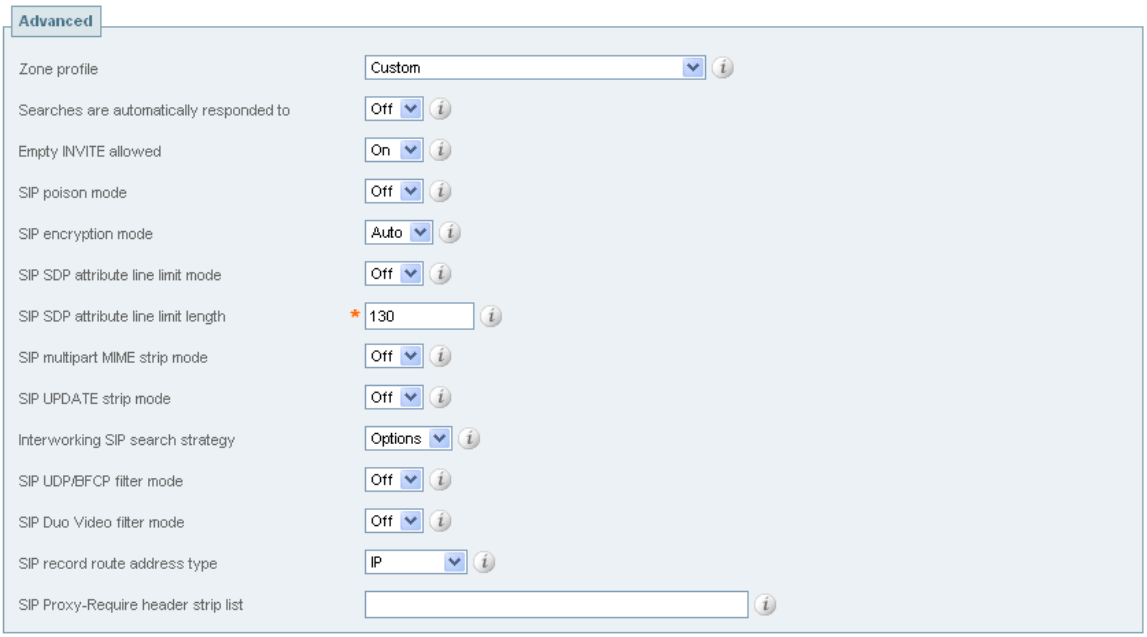
Best practice is that a MOC endpoint should never be included as a FindMe™ device. If MOC devices and video endpoints are to be related, OCS Relay should be used and a FindMe™ ID which is the same as the MOC URI should be created.

Appendix 5 – Advanced parameters set by selecting zone profile 'Microsoft Office Communications Server 2007'

By setting the **Zone profile** to **Microsoft OCS 2007**, the following Advanced zone parameters are set:

Searches are automatically responded to	**Off**
Empty INVITE allowed	**Off** See "*Appendix 6 – Setting default codecs for H.323 to SIP calls*" to modify codecs offered in the initial INVITE.
SIP poison mode	**On**
SIP encryption mode	**Off**
SIP SDP attribute line limit mode	**On**
SIP SDP attribute line limit length	**130**
SIP multipart MIME strip mode	**On**
SIP UPDATE strip mode	**On**
Interworking SIP Search Strategy	**Info**
SIP UDP/BFCP filter mode	**Off**
SIP Duo Video filter mode	**On**
SIP record route address type	**Hostname**
SIP Proxy-Require header strip list	**<Blank>**

If these need to be modified, select custom zone and configure as required:



Appendix 6 – Setting default codecs for H.323 to SIP calls

Codecs to be offered

H.323 video calls typically do not provide codec information until after the call has connected. By contrast, in SIP, the codec information exchange is typically started in the original INVITE. By default, when interworking an H.323 call to a SIP call, Cisco VCS Control will start the SIP interworked call with an INVITE which has no SDP, requesting that the called party initiates the codec offering.

Microsoft OCS does not accept a SIP INVITE without an SDP.

Setting **Empty INVITE allowed** to **Off** in the Cisco VCS Control's **Edit Zone** page (**VCS Configuration > Zones > OCS Neighbor**) instructs Cisco VCS Control to put an SDP into the INVITE, and therefore to propose a set of codecs to use.

The default set of codecs to use are codecs supported by OCS; if, however, a change is required the set of codecs proposed can be configured from the Command Line Interface.

The default audio codec to offer is configured using:

```
xConfiguration Zones Zone [1..200] Neighbor Interworking SIP Audio
   DefaultCodec:
   <G711u/G711a/G722_48/G722_56/G722_64/G722_1_16/G722_1_24/G722_1_32/G722_1_48
   /G723_1/G728/G729/AALCD_48/AALCD_56/AALCD_64/AMR>
```

… note only a single codec may be selected.

The default video codec to offer is configured using:

```
xConfiguration Zones Zone [1..200] Neighbor Interworking SIP Video
   DefaultCodec: <None/H261/H263/H263p/H263pp/H264>
```

… note only a single codec may be selected.

The default bit rate to offer is configured using:

```
xConfiguration Zones Zone [1..200] Neighbor Interworking SIP Video
   DefaultBitrate: <64..2048>
```

… note only a single bit rate may be selected.

The default resolution to offer is configured using:

```
xConfiguration Zones Zone [1..200] Neighbor Interworking SIP Video
   DefaultResolution: <None/QCIF/CIF/4CIF/SIF/4SIF/VGA/SVGA/XGA>
```

… note only a single resolution may be selected.

Appendix 7 – Presence with and without transforms

Presence SIP messages often have extra parameters in the URI header after the user-id@domain. In order to ensure that these extra parameters do not cause the search rules to fail to match, a '**.***' is appended to pattern strings.

OCS receiving Presence from non-OCS Relay FindMe™ entries, where there is no transform for Cisco VCS devices accessing OCS

For example, where to reach a MOC steve.hight@test-customer.com the video endpoint calls steve.hight@test-customer.com

The documentation above specifies the required configuration to allow calls and presence to be routed when the video network device calls the MOC endpoint's registered name to call it.

OCS receiving Presence from non-OCS Relay FindMe™ entries, where there is a transform for Cisco VCS devices accessing OCS

For example, where to reach a MOC steve.hight@test-customer.com the video endpoint calls steve.hight@ocs.domain

If a search rule has been created with a domain name transform, for example to allow callers to dial steve.hight@ocs.domain as well / instead of steve.hight@test-customer.com, an additional search rule with a pattern string for the raw domain (in this example .*@test-customer.com.*) must be added to allow presence messages through (OCS requests that the presence Notifies are sent to the OCS's raw domain).

Allowing calls to the raw domain as well as the pre-transform domain is also useful for endpoints supporting dial back to caller. The calling party's caller identity will contain the raw domain information.

For example, if non OCS Relay set Search Rule 1 as follows:

Priority	**100**
Source	**Any**
Mode	**AliasPatternMatch**
Pattern type	**Regex**
Pattern string	(.*)@ocs.domain
Pattern behavior	**Replace**
Replace string	\1@test-customer.com
On successful match	**Stop**
Target zone	**OCS**

Add a second search rule:

Priority	**100**
Source	**Any**
Mode	**AliasPatternMatch**

Pattern type	**Regex**
Pattern string	.*@test-customer.com.*
Pattern behavior	**Leave**
On successful match	**Stop**
Target zone	**OCS**

Appendix 8 – TEL URI handling for Cisco VCS to OCS calls

If an endpoint wants to dial a telephone number rather than selecting a user from a directory, the Cisco VCS Control must format the telephone number appropriately for OCS to be able to look it up.

OCS expects to see telephone numbers (known as TEL: URIs) in the form:

```
+<country code><full dialed number>
```

Cisco VCS Control can use transforms to appropriately format the telephone numbers. These transforms can either be implemented globally using **VCS Configuration > Transforms** or just for the OCS Neighbor zone by configuring the transform in the appropriate Search rules.

For example, for 4 digit extension number dialing to be expanded to a full telephone number for a company in Bracknell UK whose telephone number is 781xxx, an extension number 1008 would need to be expanded to +441344781008.

For a non OCS Relay system this can be implemented as follows:

Priority	80 (match in preference to the no transform needed rule - 80 is higher priority than 100)
Source	**Any**
Mode	**AliasPatternMatch**
Pattern type	**Regex**
Pattern string	(1…)(@vcs.domain)?(.*) (@vcs.domain will exist in SIP originated calls but not in H.323 originated calls)
Patter behavior	**Replace**
Replace string	+44134478\1;@test-customer.com;user=phone\3
On successful match	**Continue**
Target Zone	**OCS**

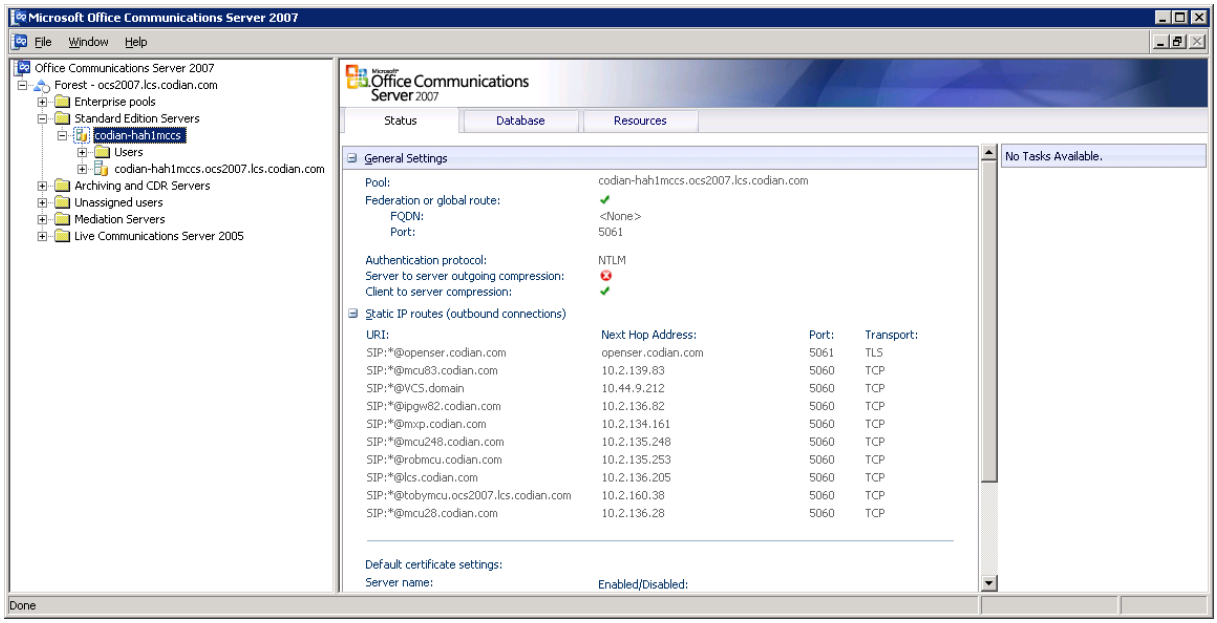
Appendix 9 – Debugging on OCS

Use of OCS Logging tool

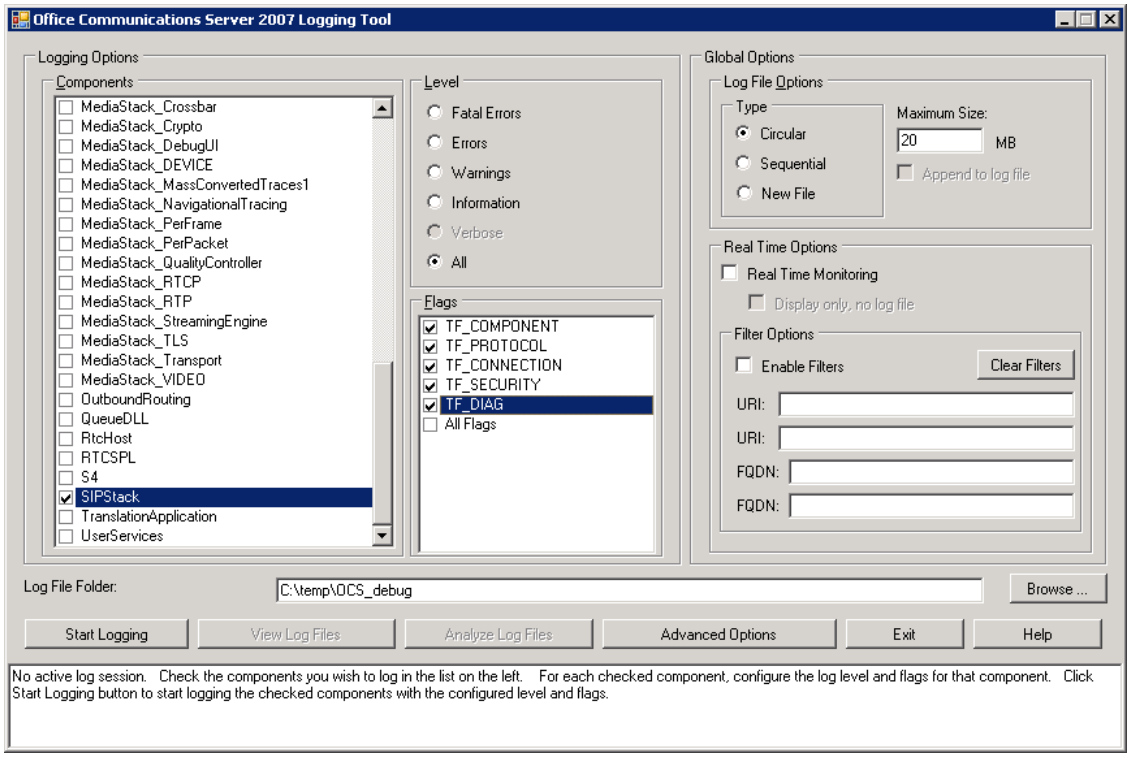
For debugging it is important to enable the logging on the appropriate OCS pool. If an OCS Director is in use, tracing here is a good starting point.

Looking at the record-route headers from OCS will identify the FEP and Director involved in the call.

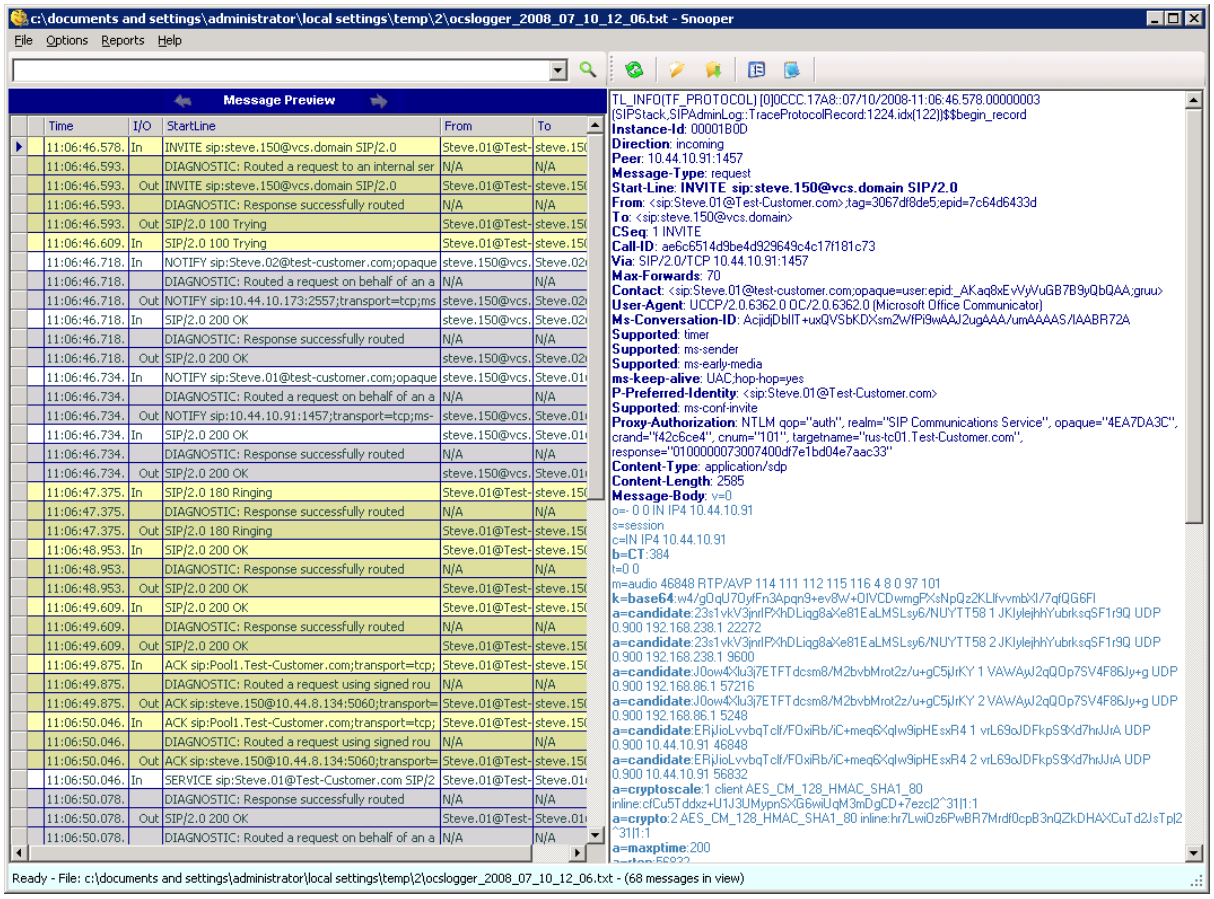
1. On OCS select **Start > Administrative Tools > Office Communications Server 2007**.
2. Expand **Enterprise pools** or **Standard Edition Servers** as required.



3. Right-click on the OCS Director pool, or FEP Pool, for example codian-hah1mccs ,and choose **Logging Tool > New Debug Session**.



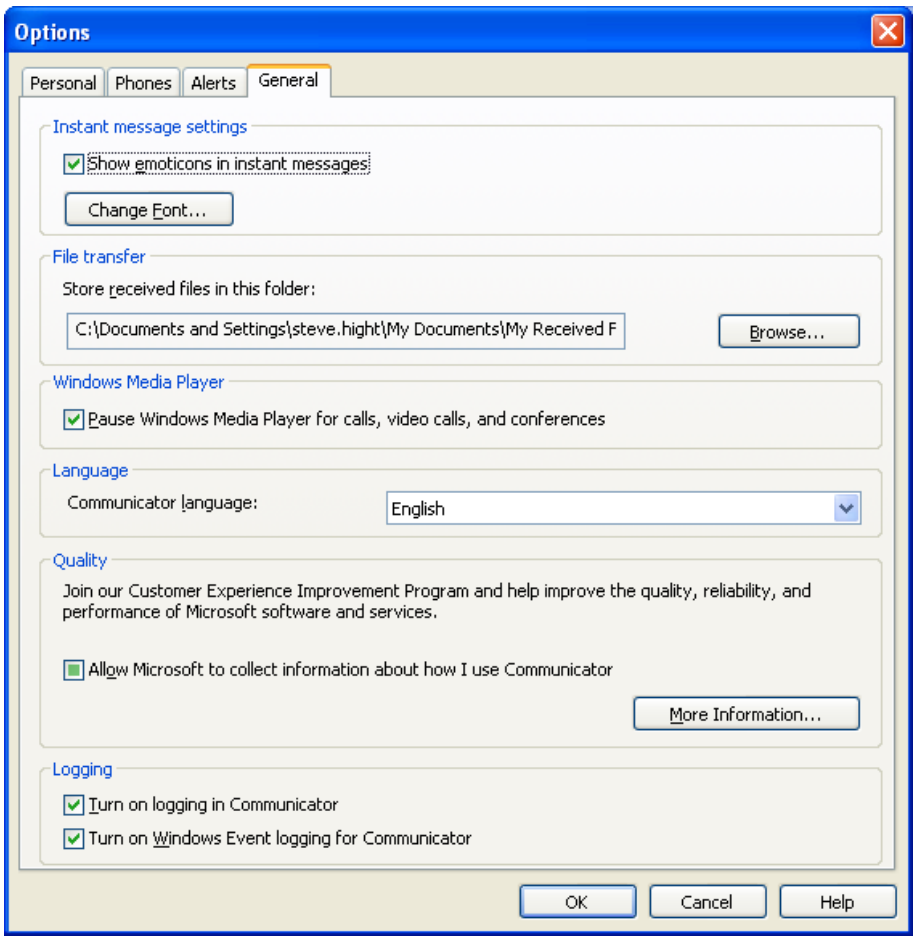
4. Select the logging option, for example SIPStack to look at SIP logs. (Details about all the logging options may be found at: http://technet.microsoft.com/en-us/library/bb936621.aspx)
5. Click **Start Logging**.
6. Make the call, or perform the function that needs to be debugged.
7. Click **Stop Logging**.
8. Click **Analyze Log Files** (install the OCS Resource Kit Tools if prompted to do so).
9. Review the trace:



Appendix 10 – Enable Debug on MOC

If MOC is not behaving as it should, then logging can be enabled and SIP messaging and other logging can be checked.

1. Select **Tools > Options**.
2. Select the **General** tab.
3. In the Logging section:
   - Select **Turn on logging in Communicator**
   - Select **Turn on Windows Event logging for Communicator**



Communicator log files may be found in: `c:\Documents and Settings\<user>\Tracing` where `<user>` is the login name of the windows login.

The `.uccplog` file can be viewed with a text editor, or (more clearly) with the application provided in the OCS resource kit 'snooper.exe'.

Windows event logging can be observed using the Windows Event Viewer.

Appendix 11 – Endpoint specific configuration

T150

- Use code version L5.1 or greater.
- Set **Network > SIP Settings > Server Type** to **Auto** (not Microsoft).
- For versions prior to L6.0 set **Security > Encryption** to **Off**

MXP 1000, MXP 1700 and MXP 6000

- Use code version F7.0 or greater.
- Set **Network > LAN Settings > SIP Settings > SIP Server Settings > Server Type** to **Auto** (not Microsoft).

C20, C60 and C90 (including T1 and T3 systems)

- Use code version TC2.0.0 or greater .
- Set **Advanced configuration > SIP > Profile 1 > Type** to **Standard** (not Microsoft).
- For versions up to and including 2.1.0 set Encryption = Off (not Best effort).

E20

- Use code version TE2.0.0 or greater.
- Set **Advanced configuration > SIP > Profile 1 > Type** to **Standard** (not Microsoft).

Cisco TelePresence Movi

Movi 2

Movi 2 only supports H.264 video – MOC Clients do not support H.264; Movi can only make a video call to a MOC client if an IP gateway or an MCU is used to transcode between H.263 and H.264 media.

Movi 3

Movi 3 supports H.263 – as supporthed by OCS. No special configuration is required.

Cisco TelePresence IP GW

- Use code version greater than 2.0(1.2).
- Set **SIP Registrar type** to **Standard SIP** (not Microsoft OCS/LCS).

Cisco TelePresence ISDN gateway

- Use code version 1.5 or greater.
- ISDN gateway is H.323 only and so calls between the gateway and OCS will be interworked by Cisco VCS.

Other endpoints

Other endpoints need to be tested for compatibility and required configuration. Although Cisco VCS does some manipulation of signaling data to make Microsoft SIP work with standard SIP and H.323 endpoints, Cisco VCS is not designed to fully insulated the Cisco VCS registered devices from OCS signaling nor OCS from the signaling of devices registered to the Cisco VCS.

The Polycom FX endpoint running version 6.0.5 code is known to generate H.263 video which is not compatible with Microsoft's MOC client. The Polycom FX v6.0.5 can only make a video call to a MOC client if an IP gateway (in transcoding mode) or an MCU is used to transcode the H.263 media.

Appendix 12 – Cisco TelePresence MCU configuration

MCU connectivity with OCS R1, OCS R2 and Cisco VCS

When using OCS R1, MCUs can be configured to register to Cisco VCS or can be configured to register directly with OCS R1.

With the changes Microsoft introduced in OCS R2, which include the use of multi-part mime, MCUs can not accept OCS R2 calls directly. Cisco VCS however contains the smarts to convert OCS R2 messaging into a format that the MCUs can handle.

Therefore for OCS R2 and beyond, MCUs must be registered to Cisco VCS in order for MOC callers to be able to join conferences.

When using Cisco VCS to route MOC calls to an MCU, the MCU should be configured to support SIP access to conferences. Cisco VCS should also be configured to keep MOC calls in native SIP where possible. Although Cisco VCS will handle media and signaling conversion for SIP to H.323 calls, Cisco VCS does not convert RFC 2833 DTMF to H.323 DTMF signaling.

OCS Relay

When OCS Relay is used, FindMe™ accounts can be set up for static conferences (for example if the In-Call presence status of the conference is wanted). For Ad hoc conferences (for example those created and used by Multiway™), a static route to the MCU's domain must be set up in order that calls can be routed to non FindMe™ destinations.

Configuration of Cisco VCS and MCUs registered to Cisco VCS

The configuration of both the Cisco VCS and the MCU documented in the 'Cisco VCS Multiway™ deployment guide' is the correct configuration for Cisco VCS and MCU when working with OCS. Please see that document for further details.

Configuration of OCS to support MOC clients creating / joining ad hoc conferences

Ensure that OCS has a static domain route to the MCU's domain.

Appendix 13 – Cisco VCS and hardware load balancers in front of a bank of FEPS

Background

For OCS to scale to support large numbers of users, a pool of Front End Processors (FEPs) can be created for the OCS system. Each FEP is then run on a separate piece of physical hardware so that the hardware resources of a single platform are no longer the limitation on call and IM processing.

So that endpoints (MOC clients, peer proxies etc) do not have to be individually configured to route their traffic to specific Front End Processors, a Hardware Load Balancer (HLB) is used to share out the traffic amongst the FEPs. The HLB provides a single virtual IP address for all of the FEPs.

When a HLB is sent data (like a SIP message), it uses an algorithm to decide where to route that message.

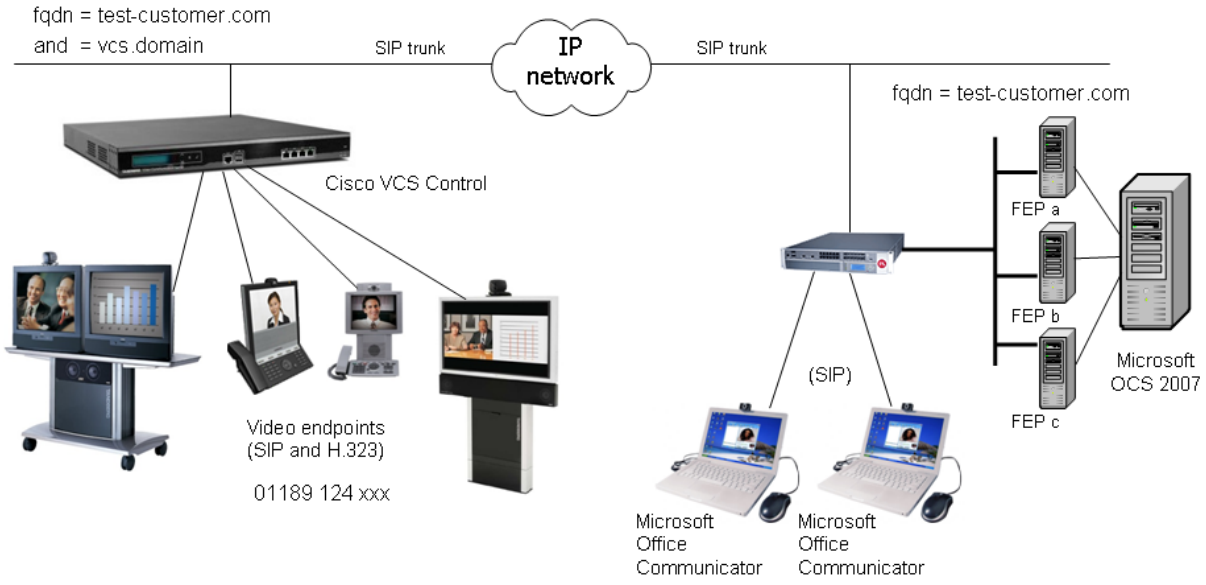
- Frequently source address routing is initially used, so that if a device has already communicated with an FEP (within the recent past) any further traffic from that device will also be routed to that same FEP.
- If source address routing does not define which FEP to send the message to, then either round-robin, or another more sophisticated algorithm that can tell the loading of the FEP will be used to find an appropriate FEP to route this new communication to.
- Some hardware load balancers have the ability to receive SIP traffic, and rather than routing it based on source address can route it based on the SIP device it relates to (allowing load balancing of SIP traffic from a proxy, like Cisco VCS).

The HLB will perform destination address NATing, meaning that messages addressed to the hardware load balancer's (Virtual) IP address will be re-addressed to the required FEP.

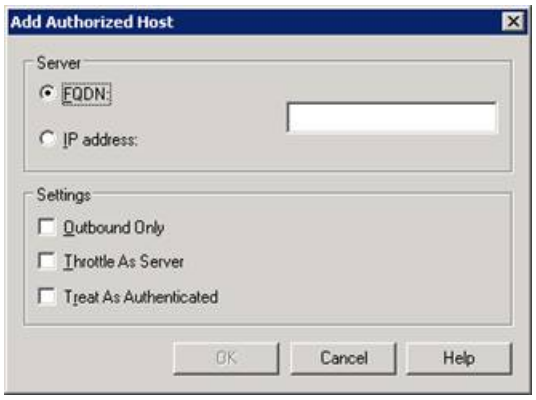
Many load balancers also perform source address NATing by default in order to get replies for outside devices routed back via the load balancer, so that the outside device (Cisco VCS, for example) sees responses coming from the single IP address that it knows to be "OCS".

The content of any messaging is left unchanged.

Example infrastructure is shown below:



When connecting a Cisco VCS to an OCS system, OCS requires that a host peer proxy (like the Cisco VCS) is authorized to communicate with the OCS FEP. This Host Authorization can be set up to be FQDN authorization, or IP Address authorization.

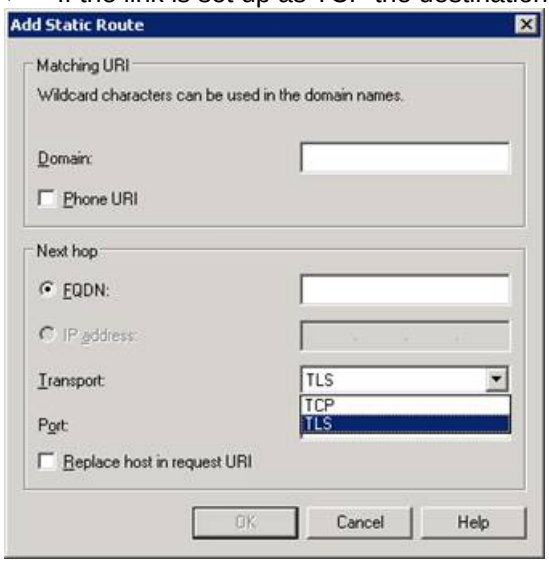


If Host Authorization is set to IP, the FEP checks that the source IP address of any incoming messages match an authorized IP address, if not they are rejected.

If Host Authorization is set to FQDN, then the connection to OCS must be TLS, and that link must have certificates that authenticates that the connection comes from the stated FQDN. (A certificate can be generated on the OCS system, or can be created externally. It must then be processed and loaded onto Cisco VCS – see "Cisco VCS deployment guide - Certificate creation and use with Cisco VCS").

For outbound messaging from OCS (to non registered devices) a static route needs to be set up.

- If TLS is chosen the destination must be specified as an FQDN.
- If the link is set up as TCP the destination must be specified as an IP address.



In SIP signaling, the messaging from endpoints registered to Cisco VCS communicating with OCS contains route headers that direct responses to the Cisco VCS – bypassing the HLB. If the Cisco VCS is in the same subnet as the FEPs and the HLB, the FEPs route the SIP messages directly back to the Cisco VCS rather than through the HLB.

TLS connection

When a TLS connection is made through the load balancer, the load balancer routes the whole TLS stream through to the same destination device (FEP). If the FEP were to fail then the load balancer would route the TLS traffic to an alternative FEP. Having all traffic routed to the same FEP is not a disadvantage in that the majority of traffic into OCS is from MOC clients, and it is these that need to be balanced across FEPs. The HLB provides the resilience required for the Cisco VCS such that if an FEP fails, Cisco VCS will be routed to another FEP, and in fact all traffic going through a single FEP makes following the signaling path easier in case debugging is required.

Responses directly from devices behind a Hardware Load Balancer

If Source Address NATing is enabled on the HLB, responses to messages (like TRYING to an INVITE) will be routed back to the Cisco VCS via the HLB because the new transaction will be sent to the 'From' address, however, mid dialogue requests (like Re-INVITE and BYE) will be sent to the Cisco VCS directly because they will be sent to the device identified in the Record-route header.

Authentication with TCP

Authorizing an IP address (the alternative to communicating over TLS) is a security risk if the HLB is performing Source Address NATing, because in this case the FEPs will have to Authorize the IP address of the HLB, and so any message sent via the HLB would be treated as authorized.

If Source Address NATing is not enabled on the HLB then the IP address of the Cisco VCS can be authorized.

Appendix 14 – Cisco VCS and Microsoft OCS Director

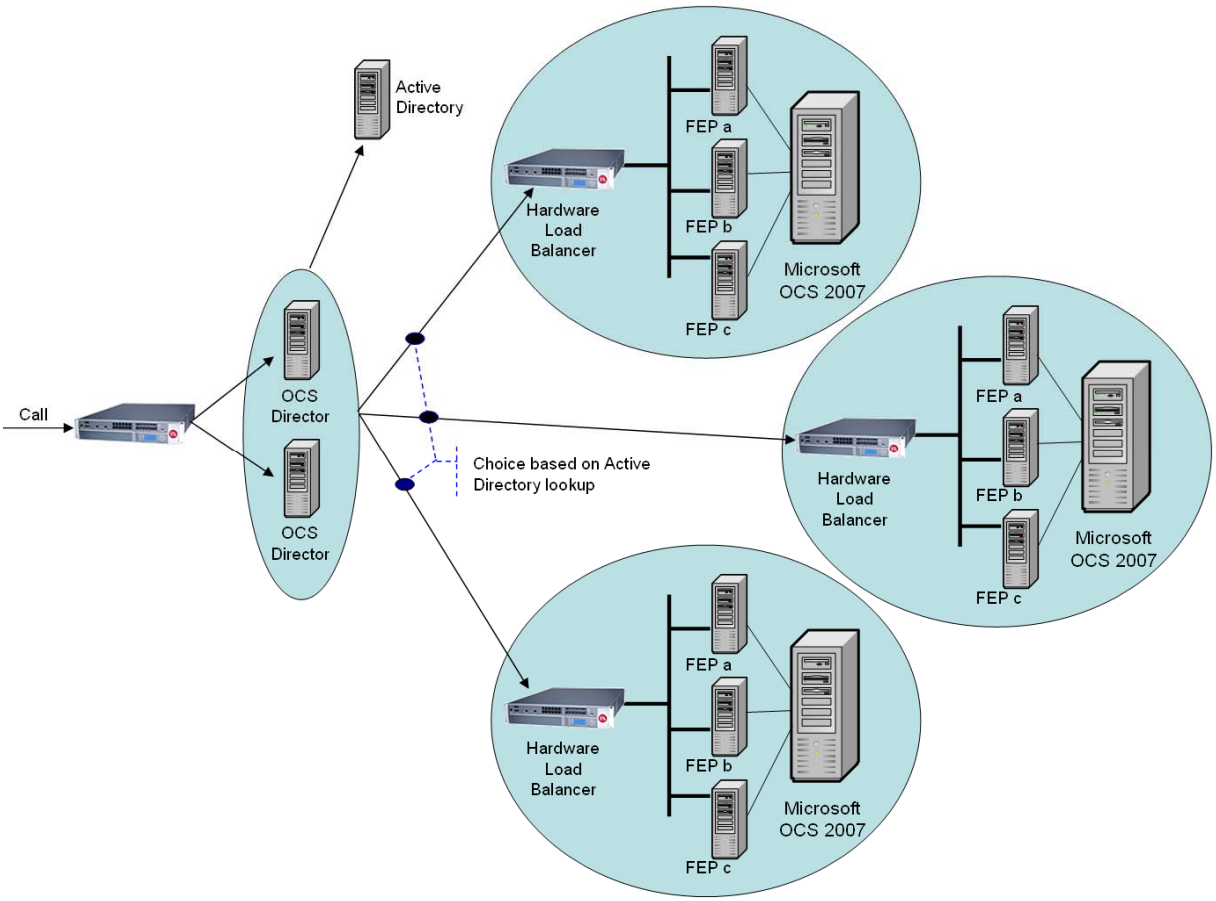
Background

Microsoft recommends that OCS Director is deployed when an organization hosts multiple Standard Edition Servers or Enterprise pools.

Microsoft OCS Director accesses the AD domain controllers for the whole network and can therefore both authenticate incoming requests, and also directs them to the appropriate enterprise pool or Standard edition server.

If a Director is not used, calls will use up resources on the Enterprise pool or Standard Edition Server that the call is initially received on, as that device will proxy the call to the correct home pool / server (remaining in-line). Not using Director thus uses resources on two devices rather than just the one and so affects the maximum capacity that the deployment can support.

Enterprise pools use Hardware Load Balancers (HLBs) to balance traffic across Front End Processors within that Enterprise Pool.



When handling a Register request, Director matches the source caller to their home Pool / standard edition server and uses a 301 response (permanently moved) to the initiator of the message to make them route this and future messages for this caller to the correct Pool / standard edition server.

When used with Cisco VCS the OCS Director should be configured to be the receiver of calls from the "OCS gateway" Cisco VCS and the source of calls from OCS to the "OCS gateway" Cisco VCS (see configuration sections in the main part of this document).

When used with a Microsoft Edge Server, OCS Director proxies messaging (not requesting a redirect) as endpoints outside the home network cannot be re-directed to communicate with another internal IP address which is not exposed to the public internet.

Configuration

Configure the "OCS gateway" Cisco VCS(s)

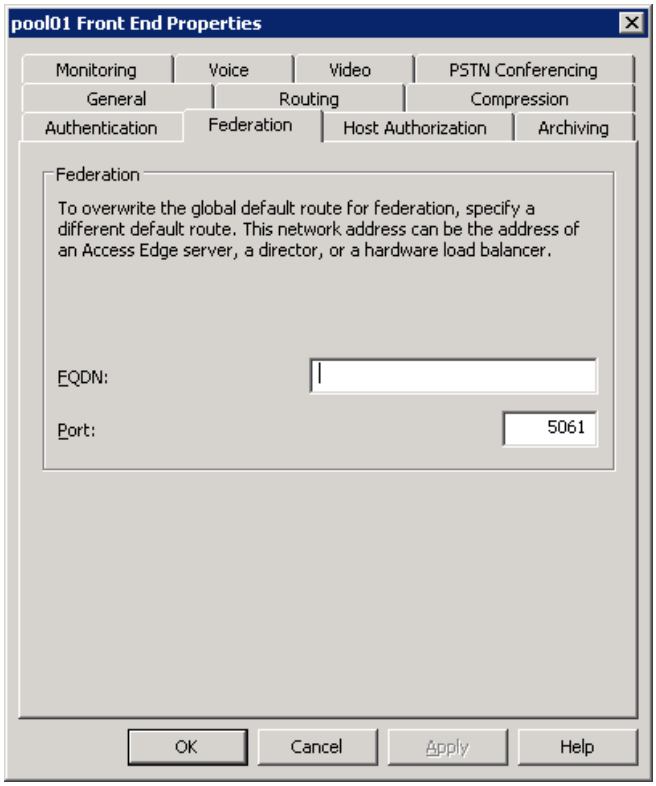
Configuration of the "OCS gateway" Cisco VCSs is described in the main body of this document.

Configure OCS Director

Configuration of the "OCS Director" is described in the main body of this document.

Configure OCS with an Edge Server

1. Right click on the relevant Front End Pool.
2. Select **Properties** > **Front End Properties**.
3. Select the **Federation** tab.



4. Enter the FQDN and port number of the Edge Server.

Appendix 15 – Cisco VCS and OCS voicemail

Video endpoints picking up voicemail from OCS

If you want to pick up voicemail from OCS using a SIP video network endpoint rather than using MOC, this can be achieved by calling the MOC URI with "`;opaque=app:voicemail`" appended, e.g. `steve.hight@test-customer.com;opaque=app:voicemail`

If the user is a FindMe™ ID (e.g. an OCSRela FindMe™) then this call request will be forked back to all FindMe™ devices for that ID as well as OCS. OCS voicemail will answer the call and other devices will display a missed call.

To avoid Cisco VCS forking calls that are aimed for the voicemail system to the FindMe™ ID devices, a transform should be added to the Cisco VCS: pre-pend the domain portion of the URI with "ocs." if the call is for voicemail. This forces the Cisco VCS to route the calls to OCS only.
e.g. `(.+)@(test-customer.com;opaque=app:voicemail.*) --> \1@ocs.\2`

The SIP calling device must support RFC2833 telephone events for presenting DTMF in order to communicate with the OCS voicemail server.

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.

© 2010 Cisco Systems, Inc. All rights reserved.