



# **Cisco TelePresence Video Communication Server Basic Configuration (Single VCS Control)**

## **Deployment Guide**

---

Cisco VCS X8.5.2

April 2015

---

# Contents

<b>Introduction</b> .....	<b>3</b>
Example network deployment .....	3
Network elements .....	4
Internal network elements .....	4
SIP and H.323 domain .....	4
<b>Prerequisites and process summary</b> .....	<b>5</b>
Prerequisites .....	5
Summary of process .....	5
<b>VCS system configuration</b> .....	<b>6</b>
Task 1: Performing initial configuration .....	6
Task 2: Setting the system name .....	6
Task 3: Configuring DNS .....	7
System host name .....	7
Domain name .....	7
DNS servers .....	7
Task 4: Replacing the default server certificate .....	8
Task 5: Configuring NTP servers .....	9
Task 6: Configuring SIP domains .....	10
<b>Routing configuration</b> .....	<b>11</b>
Pre-search transforms .....	11
Search rules .....	11
Task 7: Configuring transforms .....	11
Task 8: Configuring Local Zone search rules .....	12
<b>Endpoint registration</b> .....	<b>15</b>
<b>System checks</b> .....	<b>16</b>
Registration status .....	16
Call signaling .....	16
<b>Maintenance routine</b> .....	<b>17</b>
Creating a system backup .....	17
<b>Optional configuration tasks</b> .....	<b>18</b>
Task 9: Configuring Cisco TMS (optional) .....	18
Task 10: Configuring logging (optional) .....	20
Task 11: Configuring registration restriction policy (optional) .....	20
Task 12: Configuring device authentication policy (optional) .....	21
Task 13: Restricting access to ISDN gateways (optional) .....	22
<b>Appendix 1: Configuration details</b> .....	<b>25</b>
<b>Appendix 2: DNS records</b> .....	<b>27</b>
Local DNS A record .....	27
Local DNS SRV records .....	27
<b>Technical support</b> .....	<b>28</b>
<b>Document revision history</b> .....	<b>29</b>

# Introduction

The Cisco TelePresence Video Communication Server (VCS) software simplifies session management and control of telepresence conferences. It provides flexible and extensible conferencing applications, enabling organizations to benefit from increased employee productivity and enhanced communication with partners and customers.



The VCS delivers exceptional scalability and resiliency, secure communications, and simplified large-scale provisioning and network administration in conjunction with Cisco TelePresence Management Suite (Cisco TMS).

The VCS interworks transparently with Cisco Unified Communications Manager (Unified CM), bringing rich telepresence services to organizations with Unified CM. It also offers interoperability with third-party unified communications, IP telephony networks, and voice-over-IP (VoIP) systems.

This document describes how to configure a single VCS Control platform for use in a basic video infrastructure deployment. If your deployment includes a VCS Expressway, use *VCS Basic Configuration (Control with Expressway) Deployment Guide* instead.

Detailed reference information is contained in this document's appendices:

- [Appendix 1: Configuration details \[p.25\]](#) lists the VCS configuration details used in this document.
- [Appendix 2: DNS records \[p.27\]](#) describes the DNS records required for this example deployment.

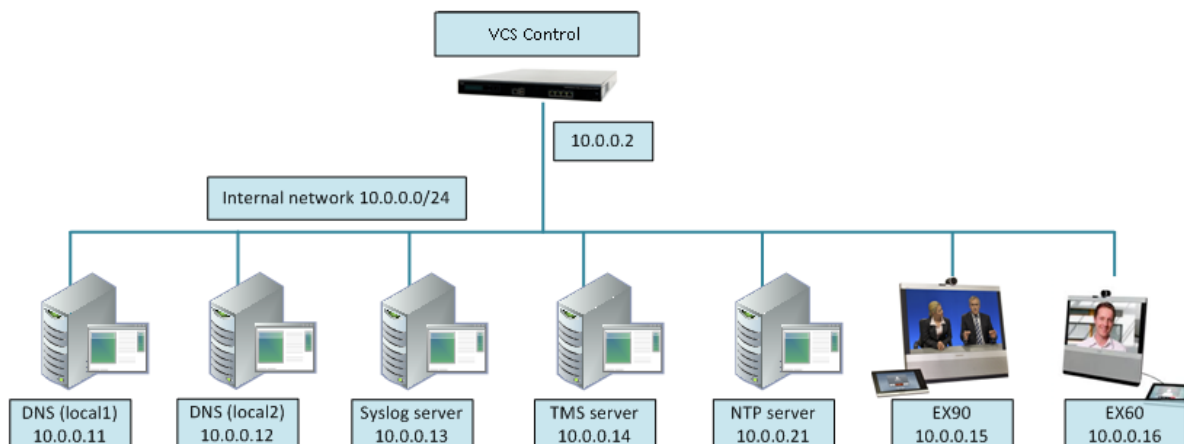
Descriptions of system configuration parameters can be found in [VCS Administrator Guide](#) and the VCS web application's online field help  and page help .

This document does not describe details of how to deploy a cluster of VCSs, or systems running device provisioning, device authentication or FindMe applications. For more details on these features, see the following documents:

- [VCS Cluster Creation and Maintenance Deployment Guide](#)
- [Cisco TMS Provisioning Extension Deployment Guide](#)
- [FindMe Express Deployment Guide](#)
- [Device Authentication on VCS Deployment Guide](#)

## Example network deployment

The example network shown below is used as the basis for the deployment described in this document.



## Network elements

### Internal network elements

The internal network elements are devices which are hosted on the organization's local area network.

Elements on the internal network have an internal network domain name. This internal network domain name is not resolvable by a public DNS. For example, the VCS Control is configured with an internally resolvable name of `vcsc.internal-domain.net` (which resolves to an IP address of 10.0.0.2 by the internal DNS servers).

#### VCS Control

The VCS Control is a SIP Registrar & Proxy and H.323 Gatekeeper for devices which are located on the internal network.

#### EX90 and EX60

These are example endpoints hosted on the internal network which register to the VCS Control.

#### DNS (local 1 & local 2)

DNS servers used by the VCS Control, to perform DNS lookups (resolve network names on the internal network).

#### DHCP server

The DHCP server provides host, IP gateway, DNS server, and NTP server addresses to endpoints located on the internal network.

#### Cisco TMS server

A management and scheduling server (see [Task 9: Configuring Cisco TMS \(optional\) \[p. 18\]](#)).

#### Syslog server

A logging server for Syslog messages (see [Task 10: Configuring logging \(optional\) \[p.20\]](#)).

#### NTP server

An NTP server which provides the clock source used to synchronize devices.

### SIP and H.323 domain

The example deployment is configured to route SIP (and H.323) signaling messages for calls made to URIs which use the domain `example.com`.

The DNS SRV configurations are described in [Appendix 2: DNS records \[p.27\]](#).

# Prerequisites and process summary

## Prerequisites

Before starting the system configuration, make sure you have access to:

- the [VCS Administrator Guide](#) and [VCS Getting Started Guide](#) (for reference purposes)
- your VCS system
- a PC connected via Ethernet to a LAN which can route HTTP(S) traffic to the VCS
- a web browser running on the PC
- a serial interface on the PC and cable (if the initial configuration is to be performed over the serial interface)

## Summary of process

The configuration process consists of the following tasks.

VCS system configuration:

- [Task 1: Performing initial configuration \[p.6\]](#)
- [Task 2: Setting the system name \[p.6\]](#)
- [Task 3: Configuring DNS \[p.7\]](#)
- [Task 4: Replacing the default server certificate \[p.8\]](#)
- [Task 5: Configuring NTP servers \[p.9\]](#)
- [Task 6: Configuring SIP domains \[p.10\]](#)

Routing configuration:

- [Task 7: Configuring transforms \[p.11\]](#)
- [Task 8: Configuring Local Zone search rules \[p.12\]](#)

Optional configuration tasks:

- [Task 9: Configuring Cisco TMS \(optional\) \[p.18\]](#)
- [Task 10: Configuring logging \(optional\) \[p.20\]](#)
- [Task 11: Configuring registration restriction policy \(optional\) \[p.20\]](#)
- [Task 12: Configuring device authentication policy \(optional\) \[p.21\]](#)
- [Task 13: Restricting access to ISDN gateways \(optional\) \[p.22\]](#)

# VCS system configuration

## Task 1: Performing initial configuration

Assuming the VCS is in the factory delivered state, follow the Initial configuration steps described in the *VCS Getting Started Guide* to configure the basic network parameters:

- LAN1 IP (IPv4 or IPv6) address
- Subnet mask (if using IPv4)
- Default Gateway IP address (IPv4 or IPv6)

Note that VCS requires a static IP address (it will not pick up an IP address from a DHCP server).

The initial configuration can be performed in one of three ways:

- using a serial cable
- via the front panel of the VCS appliance
- via the default IP address of 192.168.0.100

See the “Initial configuration” section in *VCS Getting Started Guide* for details.

This deployment guide is based on configuration using the web interface. If you cannot access the VCS using the web interface after completing the initial configuration (assigning the IP address), speak to your network administrator.

The follow configuration values are used in the example deployment:

LAN1 IPv4 address	10.0.0.2
IPv4 gateway	10.0.0.1
LAN1 subnet mask	255.255.255.0

## Task 2: Setting the system name

The **System name** defines the name of the VCS.

The **System name** appears in various places in the web interface, and in the display on the front panel of the appliance (so that you can identify it when it is in a rack with other systems). The system name is also used by Cisco TMS.

You are recommended to give the VCS a name that allows you to easily and uniquely identify it. If the system name is longer than 16 characters, only the last 16 characters will be shown in the display on the front panel.

To configure the **System name**:

1. Go to **System > Administration**.
2. Configure the **System name** as follows:

<b>System name</b>	Enter <code>vcsc</code>
--------------------	-------------------------

3. Click **Save**.

**System administration**
You are here: [System](#) > Administration

System name

System name

?

## Task 3: Configuring DNS

### System host name

The **System host name** defines the DNS hostname that this system is known by. Note that this is not the fully-qualified domain name, just the host label portion.

Note that **<System host name>.<Domain name>** = FQDN of this VCS.

To configure the **System host name**:

1. Go to **System > DNS**.
2. Configure the **System host name** as follows:

<b>System host name</b>	Enter <code>vcsc</code>
-------------------------	-------------------------

3. Click **Save**.

### Domain name

The **Domain name** is the name to append to an unqualified host name before querying the DNS server.

To configure the **Domain name**:

1. Go to **System > DNS**.
2. Configure the **Domain name** as follows:

<b>Domain name</b>	Enter <code>internal-domain.net</code>
--------------------	--

3. Click **Save**.

### DNS servers

The DNS server addresses are the IP addresses of up to 5 domain name servers to use when resolving domain names. You must specify at least one default DNS server to be queried for address resolution if you want to either:

- use FQDNs (Fully Qualified Domain Names) instead of IP addresses when specifying external addresses (for example for LDAP and NTP servers, neighbor zones and peers)
- use features such as URI dialing or ENUM dialing

The VCS only queries one server at a time; if that server is not available the VCS will try another server from the list.

In the example deployment 2 DNS servers are configured for each VCS, which provides a level of DNS server redundancy. The VCS Control is configured with DNS servers which are located on the internal network.

To configure the **Default DNS server** addresses:

1. Go to **System > DNS**.
2. Configure the DNS server **Address** fields as follows:

<b>Address 1</b>	Enter 10.0.0.11
<b>Address 2</b>	Enter 10.0.0.12

3. Click **Save**.

### DNS

#### DNS settings

Local host name  ⓘ

Domain name  ⓘ

DNS requests port range  ⓘ

#### Default DNS servers

Address 1  ⓘ

Address 2  ⓘ

Address 3  ⓘ

Address 4  ⓘ

Address 5  ⓘ

## Task 4: Replacing the default server certificate

For extra security, you may want to have the VCS communicate with other systems (such as LDAP servers, neighbor VCSs, or clients such as SIP endpoints and web browsers) using TLS encryption.

For this to work successfully in a connection between a client and server:

- The server must have a certificate installed that verifies its identity. This certificate must be signed by a Certificate Authority (CA).
- The client must trust the CA that signed the certificate used by the server.

The VCS allows you to install appropriate files so that it can act as either a client or a server in connections using TLS. The VCS can also authenticate client connections (typically from a web browser) over HTTPS. You can also upload certificate revocation lists (CRLs) for the CAs used to verify LDAP server and HTTPS client certificates.

The VCS can generate server certificate signing requests (CSRs). This removes the need to use an external mechanism to generate and obtain certificate requests.

For secure communications (HTTPS and SIP/TLS) we recommend that you replace the VCS default certificate with a certificate generated by a trusted certificate authority.



Note that in connections:

- to an endpoint, the VCS acts as the TLS server
- to an LDAP server, the VCS is a client
- between two VCS systems, either VCS may be the client with the other VCS being the TLS server
- via HTTPS, the web browser is the client and the VCS is the server

TLS can be difficult to configure. For example, when using it with an LDAP server we recommend that you confirm that your system is working correctly before you attempt to secure the connection with TLS. You are also recommended to use a third party LDAP browser to verify that your LDAP server is correctly configured to use TLS.

---

**Note:** be careful not to allow your CA certificates or CRLs to expire as this may cause certificates signed by those CAs to be rejected.

---

To load the trusted CA list, go to **Maintenance > Security certificates > Trusted CA certificate**.

To generate a CSR and/or upload the VCS's server certificate, go to **Maintenance > Security certificates > Server certificate**.

For full information, see [VCS Certificate Creation and Use Deployment Guide](#).

## Task 5: Configuring NTP servers

The **NTP server** address fields set the IP addresses or Fully Qualified Domain Names (FQDNs) of the NTP servers to be used to synchronize system time.

The **Time zone** sets the local time zone of the VCS.

To configure the NTP server address and Time zone:

1. Go to **System > Time**.
2. Configure the fields as follows:

<b>NTP server 1</b>	Enter 10.0.0.21
<b>Time zone</b>	GMT in this example

3. Click **Save**.

**Time** You are here: [System](#) ▶ Time

**NTP servers**

NTP server 1	Address	<input type="text" value="10.0.0.21"/>		Authentication	<input type="text" value="Disabled"/>	
NTP server 2	Address	<input type="text"/>		Authentication	<input type="text" value="Disabled"/>	
NTP server 3	Address	<input type="text"/>		Authentication	<input type="text" value="Disabled"/>	
NTP server 4	Address	<input type="text"/>		Authentication	<input type="text" value="Disabled"/>	
NTP server 5	Address	<input type="text"/>		Authentication	<input type="text" value="Disabled"/>	

**Time zone**

Time zone

## Task 6: Configuring SIP domains

The VCS acts as a SIP Registrar for configured SIP domains, accepting registration requests for any SIP endpoints attempting to register with an alias that includes these domains.

- Registration restriction (Allow or Deny) rules can be configured to limit acceptable registrations. See [Task 11: Configuring registration restriction policy \(optional\) \[p.20\]](#).
- If authentication is enabled, only devices that can properly authenticate themselves will be allowed to register.

To configure a SIP domain:

1. Go to **Configuration > Domains**.
2. Click **New**.
3. Enter the domain name into the **Name** field, such as **example.com**.
4. Click **Create domain**.
5. The **Domains** page displays all configured SIP domain names.

**Domains** You are here: [Configuration](#) ▶ [Domains](#) ▶ New

**Configuration**

Domain name

# Routing configuration

## Pre-search transforms

Pre-search transform configuration allows the destination alias (called address) in an incoming search request to be modified. The transformation is applied by the VCS before any searches take place, either locally or to external zones.

The pre-search transform configuration described in this document is used to standardize destination aliases originating from both H.323 and SIP devices. This means that the same call searches will work for calls from both H.323 and SIP endpoints.

For example, if the called address is an H.323 E.164 alias “01234”, the VCS will automatically append the configured domain name (in this case example.com) to the called address (that is, 01234@example.com making it into a URI), before attempting to set up the call.

- Pre-search transforms should be used with care because they apply to all signaling messages – if they match, they will affect the routing of Unified Communications messages, provisioning and presence requests as well as call requests.
- Transformations can also be carried out in search rules – consider whether it is best to use a pre-search transform or a search rule to modify the called address to be looked up.

## Search rules

Search rules define how the VCS routes calls (to destination zones) in specific call scenarios. When a search rule is matched, the destination alias can be modified according to the conditions defined in the search rule.

The search rules described in this document are used to ensure that SIP (and H.323) endpoints can dial H.323 devices that have registered E.164 numbers or H.323 IDs without a domain portion. The search rules first search for received destination aliases without the domain portion of the URI, and then search with the full URI.

The routing configuration in this document searches for destination aliases that have valid SIP URIs (that is, using a valid SIP domain, such as id@domain).

You can configure routing which enables calls to unregistered devices on an internal network (routing to the addresses of IP of the devices) by configuring a search rule with a mode of *Any IP address* with target Local Zone. However this is not recommended (and not described in this document). The best practice is to register all devices and route using destination aliases.

## Task 7: Configuring transforms

The pre-search transform configuration described in this document is used to standardize destination aliases originating from both H.323 and SIP devices.

The following transform modifies the destination alias of all call attempts made to destination aliases which do not contain an '@'. The old destination alias has @example.com appended to it. This has the effect of standardizing all called destination aliases into a SIP URI format.

To configure the transform:

1. Go to **Configuration > Dial plan > Transforms**.
2. Click **New**.
3. Configure the transform fields as follows:

<b>Priority</b>	Enter 1
<b>Description</b>	Enter <code>Transform destination aliases to URI format</code>
<b>Pattern type</b>	<i>Regex</i>
<b>Pattern string</b>	Enter <code>([^\@]*)</code>
<b>Pattern behavior</b>	<i>Replace</i>
<b>Replace string</b>	Enter <code>\1@example.com</code>
<b>State</b>	<i>Enabled</i>

4. Click **Create transform**.

**Create transform** You are here: [Configuration](#) > [Dial plan](#) > [Transforms](#) > Create transform

**Configuration**

Priority:  ⓘ

Description:  ⓘ

Pattern type: Regex ⓘ

Pattern string: \*  ⓘ

Pattern behavior: Replace ⓘ

Replace string:  ⓘ

State: Enabled ⓘ

## Task 8: Configuring Local Zone search rules

To configure the search rules to route calls to the Local Zone (to locally registered endpoint aliases):

1. Go to **Configuration > Dial plan > Search rules**.
2. Select the check box next to the default search rule (**LocalZoneMatch**).
3. Click **Delete**.  
(The default search rule is being deleted and replaced with a more specific configuration.)
4. Click **OK**.
5. Click **New**.
6. Configure the search rule fields as follows:

<b>Rule name</b>	Enter <code>Local zone - no domain</code>
<b>Description</b>	Enter <code>Search local zone for H.323 devices (strip domain)</code>
<b>Priority</b>	Enter 48

<b>Protocol</b>	<i>Any</i>
<b>Source</b>	<i>Any</i>
<b>Request must be authenticated</b>	<i>No</i>
<b>Mode</b>	<i>Alias pattern match</i>
<b>Pattern type</b>	<i>Regex</i>
<b>Pattern string</b>	Enter <code>(.+ )@example.com.*</code>
<b>Pattern behavior</b>	<i>Replace</i>
<b>Replace string</b>	Enter <code>\1</code>
<b>On successful match</b>	<i>Continue</i>
<b>Target</b>	<i>LocalZone</i>
<b>State</b>	<i>Enabled</i>

7. Click **Create search rule**.

**Create search rule** You are here: [Configuration](#) > [Dial plan](#) > [Search rules](#) > Create search rule

**Configuration**

Rule name \*  ⓘ

Description  ⓘ

Priority \*  ⓘ

Protocol  ⓘ

Source  ⓘ

Request must be authenticated  ⓘ

Mode  ⓘ

Pattern type  ⓘ

Pattern string \*  ⓘ

Pattern behavior  ⓘ

Replace string  ⓘ

On successful match  ⓘ

Target \*  ⓘ

State  ⓘ

8. Click **New**.

9. Configure the search rule fields as follows:

<b>Rule name</b>	Enter <code>Local zone – full URI</code>
------------------	--

<b>Description</b>	Enter <code>Search local zone for SIP and H.323 devices with a domain</code>
<b>Priority</b>	Enter 50
<b>Protocol</b>	<i>Any</i>
<b>Source</b>	<i>Any</i>
<b>Request must be authenticated</b>	<i>No</i>
<b>Mode</b>	<i>Alias pattern match</i>
<b>Pattern type</b>	<i>Regex</i>
<b>Pattern string</b>	Enter <code>(.+)@example.com.*</code>
<b>Pattern behavior</b>	<i>Leave</i>
<b>On successful match</b>	<i>Continue</i>
<b>Target</b>	<i>LocalZone</i>
<b>State</b>	<i>Enabled</i>

10. Click **Create search rule**.

**Create search rule** You are here: [Configuration](#) > [Dial plan](#) > [Search rules](#) > Create search rule

**Configuration**

Rule name	* Local zone – full URI <span style="float: right;">?</span>
Description	local zone for SIP and H.323 devices with a domain <span style="float: right;">?</span>
Priority	* 50 <span style="float: right;">?</span>
Protocol	Any <span style="float: right;">?</span>
Source	Any <span style="float: right;">?</span>
Request must be authenticated	No <span style="float: right;">?</span>
Mode	Alias pattern match <span style="float: right;">?</span>
Pattern type	Regex <span style="float: right;">?</span>
Pattern string	* (.+)@example.com.* <span style="float: right;">?</span>
Pattern behavior	Leave <span style="float: right;">?</span>
On successful match	Continue <span style="float: right;">?</span>
Target	* LocalZone <span style="float: right;">?</span>
State	Enabled <span style="float: right;">?</span>

Create search rule
Cancel

## Endpoint registration

There are two endpoints shown in the example network configuration diagram.

Endpoint	IP address	Network
EX90	10.0.0.15	Internal network
EX60	10.0.0.16	Internal network

Following the system configuration, endpoint registration should be possible using the following endpoint configuration details:

<b>EX90 (uses SIP protocol)</b>	
SIP URI	user.one.ex90@example.com
SIP Proxy1	vcsc.internal-domain.net
<b>EX60 (uses H.323 and SIP protocol)</b>	
H.323 ID	user.two.mxp@example.com
H.323 E.164	7654321
Gatekeeper IP Address	vcsc.internal-domain.net
SIP URI	user.two.mxp@example.com
SIP Proxy1	vcsc.internal-domain.net

# System checks

## Registration status

Check that all endpoints which are expected to be registered are actually registered to the relevant VCS, and that they are registering the expected aliases. All successfully registered endpoints are listed on **Status > Registrations > By device**.

If the expected endpoints are not registered:

- Review the endpoint's registration configuration: is it configured to register with the VCS Expressway if located on the external network / internet, and to register with the VCS Control if located on the internal network?
- Review the SIP domains ([Task 6: Configuring SIP domains \[p.10\]](#)).
- Review any registration restriction configuration applied to the VCS (optional, see [Task 11: Configuring registration restriction policy \(optional\) \[p.20\]](#)).

## Call signaling

If calls do not complete, despite the endpoints being successfully registered to a VCS:

- Review the VCS Control search rule configuration.
- Check the search history page for search attempts and failures (**Status > Search history**).
- Check the Event Log for call connection failure reasons (**Status > Logs > Event Log**).



# Maintenance routine

## Creating a system backup

To create a backup of VCS system data:

1. Go to **Maintenance > Backup and restore**.
2. Optionally, enter an **Encryption password** with which to encrypt the backup file.  
If a password is specified, the same password will be required to restore the file.
3. Click **Create system backup file**.
4. After the backup file has been prepared, a pop-up window appears and prompts you to save the file (the exact wording depends on your browser). The default name is in the format:  
**<software version>\_<hardware serial number>\_<date>\_<time>\_backup.tar.gz**.  
(The file extension is normally **.tar.gz.enc** if an encryption password is specified. However, if you use Internet Explorer to create an encrypted backup file, the filename extension will be **.tar.gz.gz** by default. These different filename extensions have no operational impact; you can create and restore encrypted backup files using any supported browser.)  
The preparation of the system backup file may take several minutes. Do not navigate away from this page while the file is being prepared.
5. Save the file to a designated location.

Log files are not included in the system backup file.

# Optional configuration tasks

## Task 9: Configuring Cisco TMS (optional)

The following configuration enables the VCS systems to be integrated to a Cisco TelePresence Management Server (Cisco TMS).

Further configuration tasks are required on Cisco TMS to fully integrate the VCS with the Cisco TMS server – see *Cisco TMS Administrator Guide*.

- Enabling SNMP speeds up the VCS - Cisco TMS integration process but is not essential.

To enable and configure SNMP:

1. Go to **System > SNMP**.
2. Configure the SNMP fields as follows:

<b>SNMP mode</b>	<i>v3 plus TMS support</i>
<b>Community name</b>	Check that it is <b>public</b>
<b>System contact</b>	Enter <b>IT administrator</b>
<b>Location</b>	Enter <b>example.com head office</b>
<b>Username</b>	Enter <b>vcs</b>
<b>Authentication mode</b>	<i>On</i>
<b>Type</b>	<i>SHA</i>
<b>Password</b>	Enter <b>ex4mp13.c0m</b>
<b>Privacy mode</b>	<i>On</i>
<b>Type</b>	<i>AES</i>
<b>Password</b>	Enter <b>ex4mp13.c0m</b>

3. Click **Save**.

**SNMP** You are here: [System](#) > SNMP

**Configuration**

SNMP mode: v3 plus TMS support ⓘ

Community name: public ⓘ

System contact: IT administrator ⓘ

Location: example.com head office ⓘ

Username: VCS ⓘ

**Authentication**

Authentication mode: On ⓘ

Type: SHA ⓘ

Password: ..... ⓘ

**Privacy**

Privacy mode: On ⓘ

Type: AES ⓘ

Password: ..... ⓘ

To configure the necessary external manager (Cisco TMS) parameters:

1. Go to **System > External manager**.
2. Configure the fields as follows:

<b>Address</b>	Enter 10.0.0.14
<b>Path</b>	Enter <code>tms/public/external/management/SystemManagementService.asmx</code>
<b>Protocol</b>	Select <i>HTTP</i> or <i>HTTPS</i>
<b>Certificate verification mode</b>	Select <i>On</i> or <i>Off</i> (see Note below)

Note that the certificate is only verified if the value is *On* and the protocol is set to *HTTPS*. If you switch this on then Cisco TMS and VCS must have appropriate certificates.

3. Click **Save**.

**External manager** You are here: [System](#) > External manager

**Configuration**

Address: 10.0.0.14 ⓘ

Path: tms/public/external/management/SystemManagementService.asmx ⓘ

Protocol: HTTP ⓘ

Certificate verification mode: On ⓘ

## Task 10: Configuring logging (optional)

The following configuration will enable event logs to be sent to an external logging server (using the SYSLOG protocol).

- The **Log level** controls the granularity of event logging. 1 is the least verbose, 4 the most.
- A minimum log level of 2 is recommended, as this level provides both system and basic signaling message logging.

To configure a logging server:

1. Go to **Maintenance > Logging**.
2. Configure the fields as follows:

<b>Log level</b>	2
<b>Remote syslog server 1: Address</b>	Enter 10.0.0.13
<b>Remote syslog server 1: Mode</b>	IETF syslog format

3. Click **Save**.

**Logging** You are here: [Maintenance](#) > [Logging](#)

**Logging**

Log level:  ⓘ

**Remote syslog servers**

Remote syslog server 1	Address: <input type="text" value="10.0.0.13"/>	Mode: <input type="text" value="IETF syslog format"/>
Remote syslog server 2	Address: <input type="text"/>	Mode: <input type="text" value="Legacy BSD format"/>
Remote syslog server 3	Address: <input type="text"/>	Mode: <input type="text" value="Legacy BSD format"/>
Remote syslog server 4	Address: <input type="text"/>	Mode: <input type="text" value="Legacy BSD format"/>

## Task 11: Configuring registration restriction policy (optional)

The aliases that endpoints can register can be limited using either an Allow (white) list or a Deny (black) list.

The following configuration will limit registrations to endpoints which register with an identity that contains "@example.com".

To configure Allow List registration restrictions:

1. Go to **Configuration > Registration > Allow List**.
2. Click **New**.
3. Create an allow pattern by configuring the fields as the follows:

<b>Description</b>	Enter <b>only</b> allow registrations containing "@example.com"
--------------------	---

<b>Pattern type</b>	<i>Regex</i>
<b>Pattern string</b>	Enter <code>.*@example.com</code>

4. Click **Add Allow List pattern**.

**Create allow pattern** You are here: [Configuration](#) > [Registration](#) > [Allow List](#) > Create allow pattern

**Configuration**

Description  ⓘ

Pattern type  ⓘ

Pattern string  ⓘ

To activate the registration restriction:

1. Go to **Configuration > Registration > Configuration**.
2. Configure the **Restriction policy** as follows:

<b>Restriction policy</b>	<i>Allow List</i>
---------------------------	-------------------

3. Click **Save**.

**Registration configuration** You are here: [Configuration](#) > [Registration](#) > Configuration

**Configuration**

Restriction policy  ⓘ

## Task 12: Configuring device authentication policy (optional)

Authentication policy is applied by the VCS at the zone and subzone levels. It controls how the VCS challenges incoming messages (for provisioning, registration, presence, phone books and calls) from that zone or subzone and whether those messages are rejected, treated as authenticated, or treated as unauthenticated within the VCS.

Each zone and subzone can set its **Authentication policy** to either *Check credentials*, *Do not check credentials*, or *Treat as authenticated*.

- Registration authentication is controlled by the Default Subzone (or relevant alternative subzone) configuration.
- Initial provisioning subscription request authentication is controlled by the Default Zone configuration.
- Call, presence, and phone book request authentication is controlled by the Default Subzone (or relevant alternative subzone) if the endpoint is registered, or by the Default Zone if the endpoint is not registered.

By default, zones and subzones are configured as *Do not check credentials*.

## Task 13: Restricting access to ISDN gateways (optional)

VCS users are recommended to take appropriate action to restrict unauthorized access to any ISDN gateway resources (also known as toll-fraud prevention). This optional step shows some methods in which this can be achieved.

In these examples, an ISDN gateway is registered to the VCS Control with a prefix of 9 (and/or has a neighbour zone specified that routes calls starting with a 9).

This example shows how to configure the VCS Control to stop calls coming in via the gateway from being able to route calls back out of the gateway. This is done by loading some specially constructed CPL onto the VCS Control and configuring its **Call policy mode** to use *Local CPL*.

### Creating a CPL file

The CPL file to be uploaded onto the VCS can be created in a text editor.

Here are 2 example sets of CPL. In these examples:

- “GatewayZone” is the neighbour zone to the ISDN gateway
- “GatewaySubZone” is the subzone to the ISDN gateway (required if the gateway registers the 9 prefix to the VCS)
- Calls coming into the ISDN gateway and hitting a FindMe will not ring devices that use the gateway – for example, calls forwarded to a mobile phone will be disallowed

This example CPL excludes any checking of whether the calling party is authenticated or not:

```
<?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>
  <taa:rule-switch>
    <!--Check that gateway is not hairpinning call - Neighbor zone -->
    <taa:rule originating-zone="GatewayZone" destination="9.*">
      <!-- Calls coming from the gateway may not send calls back out of this gateway -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="ISDN hairpin call denied"/>
    </taa:rule>
    <!-- Check that gateway is not hairpinning call - Subzone for registered gateway -->
    <taa:rule originating-zone="GatewaySubZone" destination="9.*">
      <!-- Calls coming from the gateway may not send calls back out of this gateway -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="ISDN hairpin call denied"/>
    </taa:rule>
    <taa:rule origin=".*" destination=".*">
      <!-- All other calls allowed -->
      <proxy/>
    </taa:rule>
  </taa:rule-switch>
</taa:routed>
</cpl>
```

This example CPL also ensures that the calling party is authenticated:

```

<?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>
  <taa:rule-switch>
    <!-- Check that calling party is authenticated -->
    <taa:rule authenticated-origin="" destination="9.*">
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="ISDN call denied as unauthenticated caller"/>
    </taa:rule>
    <!-- Check that gateway is not hairpinning call - Neighbor zone -->
    <taa:rule originating-zone="GatewayZone" destination="9.*">
      <!-- Calls coming from the gateway may not hairpin and send calls back out -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="ISDN hairpin call denied"/>
    </taa:rule>
    <!-- Check that gateway is not hairpinning call - Subzone for registered gateway -->
    <taa:rule originating-zone="GatewaySubZone" destination="9.*">
      <!-- Calls coming from the gateway may not hairpin and send calls back out -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="ISDN hairpin call denied"/>
    </taa:rule>
    <taa:rule origin=".*" destination=".*">
      <!-- All other calls allowed -->
      <proxy/>
    </taa:rule>
  </taa:rule-switch>
</taa:routed>
</cpl>

```

## Loading the CPL onto VCS Control

To configure the VCS Control to use the CPL:

1. Go to **Configuration > Call Policy > Configuration**.
2. Click **Browse...** and select your CPL file (created above) from your file system.
3. Click **Upload file**.
  - You should receive a "File upload successful" message.
  - If you receive an "XML invalid" message then you must correct the problems with the CPL file and upload it again.
4. Select a **Call policy mode** of *Local CPL*.
5. Click **Save**.

## Call Policy configuration

You are here: [Configuration](#) > [Call Policy](#) > Configuration

### Configuration

Call Policy mode

Local CPL

### Policy files

Call policy file

CPL File

CPL XSD file

XSD File

CPL extensions xsd file

XSD File

Select the new Call Policy file



# Appendix 1: Configuration details

This appendix summarizes the configuration required for the VCS Control.

## VCS Control system configuration

Configuration item	Value	VCS page
System configuration		
System name	VCSc	System > Administration
LAN1 IPv4 address	10.0.0.2	System > Network interfaces > IP
IPv4 gateway	10.0.0.1	System > Network interfaces > IP
LAN1 subnet mask	255.255.255.0	System > Network interfaces > IP
DNS server address 1	10.0.0.11	System > DNS
DNS server address 2	10.0.0.12	System > DNS
DNS Domain name	internal-domain.net	System > DNS
DNS System host name	vcsc	System > DNS
NTP server 1	10.0.0.21	System > Time
Time zone	GMT	System > Time
Protocol configuration		
SIP domain name	example.com	Configuration > Domains

## VCS Control transforms and search rules

Configuration item	Value	VCS page
Transform		
Pattern string	([^\@]*)	Configuration > Dial plan > Transforms
Pattern type	Regex	Configuration > Dial plan > Transforms
Pattern behavior	Replace	Configuration > Dial plan > Transforms
Replace string	\1@example.com	Configuration > Dial plan > Transforms
Local search rule 1		
Rule name	Local zone – no domain	Configuration > Dial plan > Search rules
Priority	48	Configuration > Dial plan > Search rules
Source	Any	Configuration > Dial plan > Search rules
Mode	Alias pattern match	Configuration > Dial plan > Search rules
Pattern type	Regex	Configuration > Dial plan > Search rules
Pattern string	(.+ )@example.com.*	Configuration > Dial plan > Search rules
Pattern behavior	Replace	Configuration > Dial plan > Search rules
Replace string	\1	Configuration > Dial plan > Search rules
On successful match	Continue	Configuration > Dial plan > Search rules

---

Configuration item	Value	VCS page
Target	LocalZone	Configuration > Dial plan > Search rules
Local search rule 2		
Rule name	Local zone – full URI	Configuration > Dial plan > Search rules
Priority	50	Configuration > Dial plan > Search rules
Source	Any	Configuration > Dial plan > Search rules
Mode	Alias pattern match	Configuration > Dial plan > Search rules
Pattern type	Regex	Configuration > Dial plan > Search rules
Pattern string	(.+)@example.com.*	Configuration > Dial plan > Search rules
Pattern behavior	Leave	Configuration > Dial plan > Search rules
On successful match	Continue	Configuration > Dial plan > Search rules
Target	LocalZone	Configuration > Dial plan > Search rules

---

## Appendix 2: DNS records

The following records are required in the local DNS which hosts the internally routable domain: internal-domain.net to allow internal messages to be routed to the VCS Control.

### Local DNS A record

Host	Host IP address
vcsc.internal-domain.net	10.0.0.2

### Local DNS SRV records

Name	Service	Protocol	Priority	Weight	Port	Target host
internal-domain.net.	h323cs	tcp	10	10	1720	vcsc.internal-domain.net.
internal-domain.net.	h323ls	udp	10	10	1719	vcsc.internal-domain.net.
internal-domain.net.	h323rs	udp	10	10	1719	vcsc.internal-domain.net.
internal-domain.net.	sip	tcp	10	10	5060	vcsc.internal-domain.net.
internal-domain.net.	sip	udp *	10	10	5060	vcsc.internal-domain.net.
internal-domain.net.	sips	tcp	10	10	5061	vcsc.internal-domain.net.

\* SIP UDP is disabled on VCS by default.

For example, the DNS records would be:

```
_h323cs._tcp.internal-domain.net. 86400 IN SRV 10 10 1720 vcsc.internal-domain.net.
_h323ls._udp.internal-domain.net. 86400 IN SRV 10 10 1719 vcsc.internal-domain.net.
_h323rs._udp.internal-domain.net. 86400 IN SRV 10 10 1719 vcsc.internal-domain.net.
_sip._tcp.internal-domain.net.      86400 IN SRV 10 10 5060 vcsc.internal-domain.net.
_sip._udp.internal-domain.net.      86400 IN SRV 10 10 5060 vcsc.internal-domain.net.
_sips._tcp.internal-domain.net.     86400 IN SRV 10 10 5061 vcsc.internal-domain.net.
vcsc.internal-domain.net.           86400 IN A 10.0.0.2
```

## Technical support

If you cannot find the answer you need in the documentation, check the website at [www.cisco.com/cisco/web/support/index.html](http://www.cisco.com/cisco/web/support/index.html) where you will be able to:

- Make sure that you are running the most up-to-date software.
- Get help from the Cisco Technical Support team.

Make sure you have the following information ready before raising a case:

- Identifying information for your product, such as model number, firmware version, and software version (where applicable).
- Your contact email address or telephone number.
- A full description of the problem.

To view a list of Cisco TelePresence products that are no longer being sold and might not be supported, visit: [www.cisco.com/en/US/products/prod\\_end\\_of\\_life.html](http://www.cisco.com/en/US/products/prod_end_of_life.html) and scroll down to the TelePresence section.

## Document revision history

<b>Date</b>	<b>Description</b>
April 2015	Menu path changes for X8.5. Republished with X8.5.2.
December 2014	Republished for X8.5.
June 2014	Republished for X8.2.
December 2013	Updated for X8.1.
August 2012	Revised document structure and updated for X7.2.
October 2010	New document template applied.
September 2009	Initial release.

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](http://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.

© 2015 Cisco Systems, Inc. All rights reserved.