



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

Deployment Guide

Cisco VCS X7.2

D14524.03

August 2012

Contents

Introduction	3
Example network deployment.....	3
Internal network elements.....	4
SIP and H.323 domain.....	4
Prerequisites and process summary	5
Prerequisites.....	5
Summary of process.....	5
Cisco VCS system configuration	6
Step 1: Initial configuration.....	6
Step 2: System name configuration.....	7
Step 3: DNS configuration.....	8
Local host name.....	8
Domain name.....	8
DNS servers.....	8
Step 4: Time configuration.....	10
Step 5: SIP domain configuration.....	11
Routing configuration	12
Pre-search transforms.....	12
Search rules.....	12
Step 6: Transform configuration.....	13
Step 7: Local zone search rules configuration.....	14
Endpoint registration	17
System checks	18
Registration status.....	18
Call signaling.....	18
Maintenance routine	19
System backup.....	19
Optional configuration steps	20
Cisco TMS configuration (optional).....	20
Logging server configuration (optional).....	22
Registration restriction configuration (optional).....	23
Restrict access to ISDN gateways (optional).....	24
Appendix 1 – Configuration details	27
Appendix 2 – DNS records configuration	29
Local DNS A record.....	29
Local DNS SRV records.....	29
Checking for updates and getting help	30
Document revision history	31
Disclaimer	31

Introduction

The Cisco TelePresence Video Communication Server (VCS) can be deployed as a VCS Control application or as a VCS Expressway™ application.

The VCS Expressway enables business to business communications, empowers remote and home based workers, and gives service providers the ability to provide video communications to customers. The VCS Control provides SIP proxy and call control as well as H.323 gatekeeper services within an organization's corporate network environment.

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

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

- Appendix 1 lists the configuration details used to configure the VCSs in the example network deployment.
- Appendix 2 includes details of the DNS records required for the system deployment to work as expected.

Descriptions of system configuration parameters can be found in the *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 VCSs running Device Provisioning 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*

These documents can be found at: <http://www.cisco.com/cisco/web/support/index.html>

Example network deployment

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

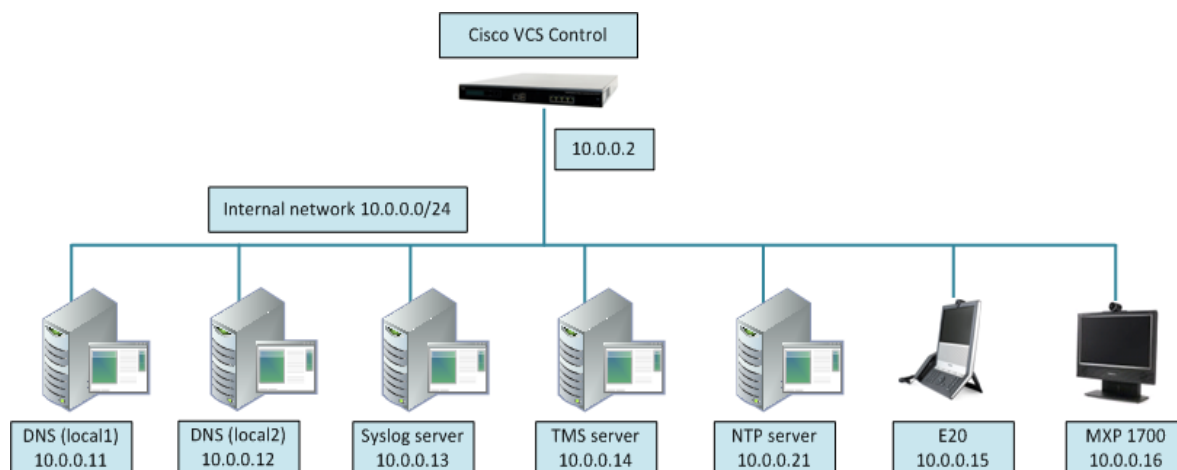


Figure 1: Example network deployment

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.

E20 and MXP1700

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.

Syslog server

A logging server for Syslog messages (see [Logging server configuration \(optional\) \[p.22\]](#)).

Cisco TMS server

A management and scheduling server (see [Cisco TMS configuration \(optional\) \[p.20\]](#)).

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 configuration \[p.29\]](#).

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)
- a VCS Control running version X5 or later
- 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 steps.

VCS system configuration:

- [Step 1: Initial configuration \[p.6\]](#)
- [Step 2: System name configuration \[p.7\]](#)
- [Step 3: DNS configuration \[p.8\]](#)
- [Step 4: Time configuration \[p.10\]](#)
- [Step 5: SIP domain configuration \[p.11\]](#)

Routing configuration:

- [Step 6: Transform configuration \[p.13\]](#)
- [Step 7: Local zone search rules configuration \[p.14\]](#)

Optional configuration steps:

- [Cisco TMS configuration \(optional\) \[p.20\]](#)
- [Logging server configuration \(optional\) \[p.22\]](#)
- [Registration restriction configuration \(optional\) \[p.23\]](#)
- [Restrict access to ISDN gateways \(optional\) \[p.24\]](#)

Cisco VCS system configuration

Step 1: Initial configuration

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

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

Note that VCSs require static IP addresses (they 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
- 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

Step 2: System name configuration

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 unit (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 the **System administration** page (**System > System**).
2. Configure the **System name** as follows:

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

3. Click **Save**.

The screenshot shows the Cisco VCS web interface. At the top, there is a navigation bar with tabs for Status, System, VCS configuration, Applications, and Maintenance. The 'System' tab is selected. Below the navigation bar, the page title is 'System administration' and the breadcrumb trail is 'You are here: System > System'. The main content area shows a form for configuring the 'System name'. The form has a label 'System name' and a text input field containing the value 'VCSc'. There is also an information icon (i) next to the input field.

Step 3: DNS configuration

Local host name

The **Local 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 <**Local host name**>.<**Domain name**> = FQDN of this VCS.

To configure the **Local host name**:

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

Local host name	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 the **DNS** page (**System > DNS**).
2. Configure the **Domain name** as follows:

Domain name	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 the **DNS** page (**System > DNS**).
2. Configure the DNS server **Address** fields as follows:

Address 1 Enter 10.0.0.11

Address 2 Enter 10.0.0.12

3. Click **Save**.

Status	System	VCS configuration	Applications	Maintenance
DNS				
DNS settings				
Local host name	<input type="text" value="vcsc"/>			
Domain name	<input type="text" value="internal-domain.net"/>			
DNS requests port range	<input type="text" value="Use the ephemeral port range"/>			
Default DNS servers				
Address 1	<input type="text" value="10.0.0.11"/>			
Address 2	<input type="text" value="10.0.0.12"/>			
Address 3	<input type="text"/>			
Address 4	<input type="text"/>			
Address 5	<input type="text"/>			
Per-domain DNS servers				
Address 1	<input type="text"/>		Domain names:	<input type="text"/>
Address 2	<input type="text"/>		Domain names:	<input type="text"/>
Address 3	<input type="text"/>		Domain names:	<input type="text"/>
Address 4	<input type="text"/>		Domain names:	<input type="text"/>
Address 5	<input type="text"/>		Domain names:	<input type="text"/>
<input type="button" value="Save"/>				

Step 4: Time configuration

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 the **Time** page (**System > Time**).
2. Configure the fields as follows:

NTP server 1	Enter 10.0.0.21
Time zone	Select GMT

3. Click **Save**.

The screenshot shows the 'Time' configuration page in the Cisco VCS web interface. The breadcrumb navigation at the top reads 'System > Time'. The page is divided into two main sections: 'NTP servers' and 'Time zone'.

NTP servers section: This section contains a table with five rows, each representing an NTP server. The first row is pre-filled with '10.0.0.21' in the 'Address' field and 'Disabled' in the 'Authentication' dropdown menu. The other four rows have empty 'Address' fields and 'Disabled' in the 'Authentication' dropdown menu. Each row has an information icon (i) to its right.

Time zone section: This section contains a single 'Time zone' dropdown menu, which is currently set to 'GMT'. It also has an information icon (i) to its right.

At the bottom left of the configuration area, there is a 'Save' button.

Step 5: SIP domain configuration

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.

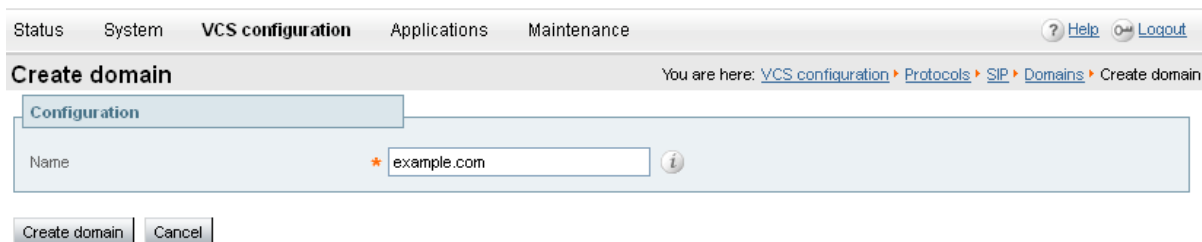
- Registration restriction (Allow or Deny) rules can be configured to limit acceptable registrations. See [Registration restriction configuration \(optional\) \[p.23\]](#).
- If authentication is enabled, only devices that can properly authenticate themselves will be allowed to register.

To configure a SIP domain:

1. Go to the **Domains** page (**VCS configuration > Protocols > SIP > Domains**).
2. Click **New**.
3. Enter the domain name into the **Name** field:

Name Enter `example.com`

4. Click **Create domain**.
5. The **Domains** page displays all configured SIP domain names.



The screenshot shows the Cisco VCS configuration interface. At the top, there are navigation tabs: Status, System, **VCS configuration**, Applications, and Maintenance. On the right, there are links for Help and Logout. Below the tabs, the page title is "Create domain" and the breadcrumb trail is "You are here: VCS configuration > Protocols > SIP > Domains > Create domain". The main content area is titled "Configuration" and contains a form with a "Name" field. The field contains the text "example.com" and has a red asterisk to its left and an information icon to its right. Below the form are two buttons: "Create domain" and "Cancel".

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.

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.

This is carried out to make the call searches the same for calls from H.323 endpoints and SIP endpoints.

- Pre-search transforms should be used with care because they apply to all signaling messages – if they match, they will affect the routing of 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

The search rules configuration defines 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 configuration described in this document is used to ensure 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 searching 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).

It is possible to 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 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.

Step 6: Transform configuration

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 configuration 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 form.

To configure the transform:

1. Go to the **Transforms** page (**VCS configuration > Dial plan > Transforms**).
2. Click **New**.
3. Configure the transform fields as follows:

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

4. Click **Create transform**.

The screenshot shows the 'Create transform' configuration page. At the top, there are navigation tabs: Status, System, **VCS configuration**, Applications, and Maintenance. On the right, there are links for Help and Logout. Below the navigation is a breadcrumb trail: You are here: [VCS configuration](#) > [Dial plan](#) > [Transforms](#) > Create transform.

The main configuration area is titled 'Configuration' and contains the following fields:

- Priority:** A text input field containing the value '1'.
- Description:** A text input field containing the value 'Transform destination aliases to URI format'.
- Pattern type:** A dropdown menu set to 'Regex'.
- Pattern string:** A text input field containing the value '*([^@]*)'.
- Pattern behavior:** A dropdown menu set to 'Replace'.
- Replace string:** A text input field containing the value '\1@example.com'.
- State:** A dropdown menu set to 'Enabled'.

At the bottom of the configuration area, there are two buttons: 'Create transform' and 'Cancel'.

Step 7: Local zone search rules configuration

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

1. Go to the **Search rules** page (**VCS 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:

Rule name	Enter <code>Local zone - no domain</code>
Description	Enter <code>Search local zone for H.323 devices (strip domain)</code>
Priority	Enter <code>48</code>
Protocol	Select <i>Any</i>
Source	Select <i>Any</i>
Request must be authenticated	Select <i>No</i>
Mode	Select <i>Alias pattern match</i>
Pattern type	Select <i>Regex</i>
Pattern string	Enter <code>(.+@example.com.*</code>
Pattern behavior	Select <i>Replace</i>
Replace string	Enter <code>\1</code>
On successful match	Select <i>Continue</i>
Target	Select <i>LocalZone</i>
State	Select <i>Enabled</i>

7. Click **Create search rule**.

Status System **VCS configuration** Applications Maintenance

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

Configuration

Rule name * Local zone – no domain ⓘ

Description Search local zone for H.323 devices (strip domain) ⓘ

Priority * 48 ⓘ

Protocol Any ⓘ

Source Any ⓘ

Request must be authenticated No ⓘ

Mode Alias pattern match ⓘ

Pattern type Regex ⓘ

Pattern string * (.+)@example.com.* ⓘ

Pattern behavior Replace ⓘ

Replace string \1 ⓘ

On successful match Continue ⓘ

Target * LocalZone ⓘ

State Enabled ⓘ

Create search rule Cancel

8. Click **New**.
9. Configure the search rule fields as follows:

Rule name	Enter Local zone – full URI
Description	Enter Search local zone for SIP and H.323 devices with a domain
Priority	Enter 50
Protocol	Select Any
Source	Select Any
Request must be authenticated	Select No
Mode	Select Alias pattern match
Pattern type	Select Regex
Pattern string	Enter (.+)@example.com.*
Pattern behavior	Select Leave
On successful match	Select Continue
Target	Select LocalZone
State	Leave as Enabled

10. Click **Create search rule**.

Status System **VCS configuration** Applications Maintenance

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

Configuration

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

Create search rule Cancel

Endpoint registration

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

Endpoint	IP address	Network
E20	10.0.0.15	Internal network
MXP1700	10.0.0.16	Internal network

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

E20 (uses SIP protocol)	
SIP URI	user.one.e20@example.com
SIP Proxy1	vcsc.internal-domain.net
MXP1700 (uses H.323 and SIP protocol)	
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 will be listed in the **Registrations by device** status page (**Status > Registrations > By device**).

If the expected endpoints are not registered:

- review the endpoint's registration configuration
- review the SIP domain configuration (Step 5)
- review any registration restriction configuration applied to the VCS (optional, see [Registration restriction configuration \(optional\) \[p.23\]](#))

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

System backup

To create a system backup:

1. Go to the **Backup and restore** page (**Maintenance > Backup and restore**).
2. Click **Create system backup file**.
3. Wait for file download dialog to appear.
4. Click **Save**, to save the backup file archive to your local PC.

For more information, see *VCS Administrator Guide*.

Optional configuration steps

Cisco TMS configuration (optional)

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

Further configuration steps are required on the Cisco TMS platform 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 the **SNMP** page (**System > SNMP**).
2. Configure the SNMP fields as follows:

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

3. Click **Save**.

Status **System** VCS configuration Applications Maintenance ? Logout

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: ⓘ

Save

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

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

Address	Enter 10.0.0.14
Path	Enter <code>tms/public/external/management/SystemManagementService.asmx</code>
Protocol	Select <i>HTTP</i> or <i>HTTPS</i>
Certificate verification mode	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**.

Status **System** VCS configuration Applications Maintenance ? [Help](#) Logout

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 ⓘ

Save

Logging server configuration (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 the **Logging** page (**Maintenance > Logging**).
2. Configure the fields as follows:

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

3. Click **Save**.

The screenshot shows the 'Logging' configuration page in the Cisco VCS Basic Configuration (Single VCS Control) Deployment Guide. The page is titled 'Logging' and is part of the 'Maintenance' section. It shows a 'Log level' dropdown set to '2' and a 'Remote syslog servers' section with four rows. The first row is configured with 'Address: 10.0.0.13' and 'Mode: IETF syslog format'. The other three rows are empty for address and set to 'Legacy BSD format' for mode. A 'Save' button is visible at the bottom left.

Registration restriction configuration (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 the **Allow List** page (**VCS configuration > Registration > Allow List**).
2. Click **New**.
3. Create an allow pattern by configuring the fields as the follows:

Description	Enter <code>Only allow registrations containing "@example.com"</code>
Pattern type	Select <code>Regex</code>
Pattern string	Enter <code>.*@example.com</code>

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

The screenshot shows the 'Create allow pattern' configuration page. The breadcrumb trail is: **VCS configuration > Registration > Allow List > Create allow pattern**. The form fields are:

- Description:** Only allow registrations containing "@example.com"
- Pattern type:** Regex
- Pattern string:** .*@example.com

Buttons: Add Allow List pattern, Cancel

To activate the registration restriction:

1. Go to the **Registration configuration** page (**VCS configuration > Registration > Configuration**).
2. Configure the **Restriction policy** as follows:

Restriction policy	Select <code>Allow List</code>
---------------------------	--------------------------------

3. Click **Save**.

The screenshot shows the 'Registration configuration' page. The breadcrumb trail is: **VCS configuration > Registration > Configuration**. The form field is:

- Restriction policy:** Allow List

Button: Save

Restrict access to ISDN gateways (optional)

Cisco 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 from 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*.

Create 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 are not allowed to 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 are not allowed to 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 are not allowed to hairpin and send calls 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 are not allowed to hairpin and send calls 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>
```

Load the CPL onto VCS Control

To configure the VCS Control to use the CPL:

1. Go to the [Call Policy configuration](#) page ([VCS 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**.

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

Call Policy configuration

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

Configuration

Call Policy mode i

Save

Policy files

Call policy file	CPL File	<input type="text" value="Show Call Policy file"/> i
CPL XSD file	XSD File	<input type="text" value="Show CPL XSD file"/> i
CPL extensions xsd file	XSD File	<input type="text" value="Show CPL extensions XSD file"/> i
Select the new Call Policy file	<input type="text"/>	<input type="button" value="Browse..."/> i

Upload 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	VCS	System > System
LAN1 IPv4 address	10.0.0.2	System > IP
IPv4 gateway	10.0.0.1	System > IP
LAN1 subnet mask	255.255.255.0	System > 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 Local 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	VCS configuration > Protocols > SIP > Domains

VCS Control transforms and search rules

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

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

Appendix 2 – DNS records configuration

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

Local DNS A record

Host	TTL	Type	Data
vcsc.internal-domain.net	86400	A	10.0.0.2

Local DNS SRV records

Service	Protocol	Host	Port	Notes
h323cs	tcp	_h323cs._tcp.internal-domain.net	1720	
h323ls	udp	_h323ls._udp.internal-domain.net	1719	
sip	tcp	_sip._tcp.internal-domain.net	5060	
sip	udp	_sip._udp.internal-domain.net	5060	
sips	tcp	_sips._tcp.internal-domain.net	5061	
sips	tls	_sips._tls.internal-domain.net	5061	For E20 TE2.1
sip	tls	_sip._tls.internal-domain.net	5061	For MXP F8.2, T150 L6.0, Movi prior to version 3.1

For each DNS SRV record the following values are common:

Name	internal-domain.net
TTL	86400
Type	SRV
Priority	10
Weight	10
Target	vcsc.internal-domain.net.

Checking for updates and getting help

If you experience any problems when configuring or using the product, consult the online help available from the user interface. The online help explains how the individual features and settings work.

If you cannot find the answer you need, check the web site at <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,
- find further relevant documentation, for example product user guides, printable versions of the online help, reference guides, and articles that cover many frequently asked questions,
- get help from the Cisco Technical Support team. Click on Technical Support Overview for information on Accessing Cisco Technical Services. Make sure you have the following information ready before raising a case:
 - the serial number and product model number of the unit (if applicable)
 - the software build number which can be found on the product user interface (if applicable)
 - your contact email address or telephone number
 - a full description of the problem

Document revision history

Revision	Date	Description
01	September 2009	Initial release.
02	October 2010	New document template applied.
03	Mmmmm 2012	Revised document structure and updated for X7.2.

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 NON-INFRINGEMENT 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.

© 2012 Cisco Systems, Inc. All rights reserved.