



Single Cisco VCS Control

Cisco TelePresence Deployment Guide

Cisco VCS Control X5

D14524.02

October 2010

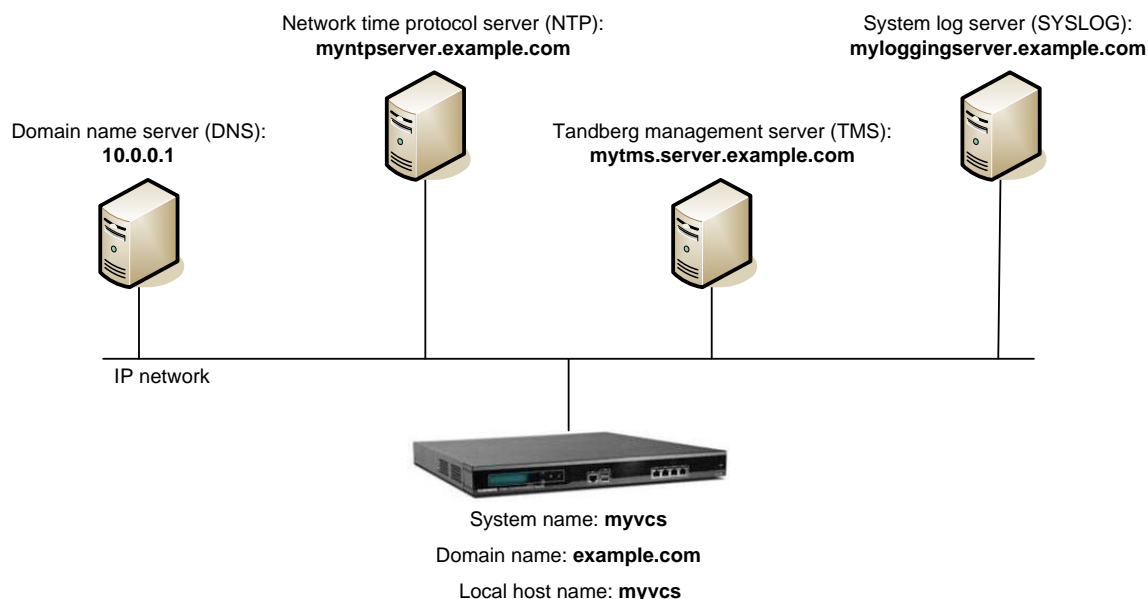
Contents

Introduction	3
Prerequisites.....	3
Summary of process.....	4
Getting started.....	5
Step 1: Complete the configuration checklist	5
Step 2: Perform initial configuration	6
Step 3: Access Cisco VCS using the web interface.....	7
Step 4: Change admin password	8
System configuration.....	9
Step 5: Configure System name (recommended).....	9
Step 6: Administration access – Session time-out (optional).....	10
Step 7: Administration access – Service access (optional).....	11
Step 8: DNS configuration - DNS address	12
Step 9: DNS configuration - DNS Domain name & Local host name	13
Step 10: Time configuration – NTP Server and time zone.....	14
Step 11: SNMP configuration (optional)	15
Step 12: External manager configuration (optional but recommended).....	16
Step 13: Logging configuration (optional).....	17
Enabling registrations and calls	18
Step 14: H.323 only configuration (optional)	19
Step 15: SIP only configuration (optional).....	20
Step 16: Mixed H.323 and SIP configuration	21
Appendix 1 – Configuration checklist.....	24

Introduction

This document describes how to configure a **single Cisco TelePresence Video Communication Server (Cisco VCS) control platform** for use in a basic video infrastructure deployment.

The following diagram represents an example network environment into which the Cisco VCS Control is being integrated. The example network names and addresses are used in the configuration steps throughout this document.



Prerequisites

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

- ▶ the Cisco VCS Administrator Guide and Cisco VCS Getting Started Guide (for reference purposes)
- ▶ a Cisco VCS Control running version X5 or later
- ▶ a PC connected via Ethernet to a LAN which can route HTTP(S) traffic to the Cisco VCS
- ▶ a web browser running on the PC
- ▶ a serial interface on the PC and cable (if the initial configuration (Step 2) is to be performed using the serial interface of the Cisco VCS)

Summary of process



The process of system configuration consists of the following steps. Each step is described in a separate section:


- ▶ Step 1: Complete the configuration checklist
- ▶ Step 2: Perform initial configuration
- ▶ Step 3: Access Cisco VCS using the web interface
- ▶ Step 4: Change admin password
- ▶ Step 5: Configure System name
- ▶ Step 6: Administration access – Session time-out
- ▶ Step 7: Administration access – Service access
- ▶ Step 8: DNS configuration - DNS Server address
- ▶ Step 9: DNS configuration - DNS Domain name & local hostname
- ▶ Step 10: Time configuration – NTP Server and time zone
- ▶ Step 11: SNMP configuration
- ▶ Step 12: External manager configuration
- ▶ Step 13: Logging configuration
- ▶ Step 14: H.323 only configuration
- ▶ Step 15: SIP only configuration
- ▶ Step 16: Mixed H.323 and SIP configuration

Getting started

Step 1: Complete the configuration checklist

It is important to collate all the necessary details to configure the Cisco VCS before starting the system configuration process. [Appendix 1](#) of this deployment guide contains a checklist that lets you collect the required details.

Detailed descriptions of system configuration parameters can be found in the Cisco VCS Administrator Guide and the Cisco VCS web application's online field  and page help .

Note: The Administrator Guide can be opened by clicking on the  Manual link, found at the top right of every Cisco VCS web interface page. It can also be download from www.tandberg.com.

To complete the configuration checklist:

1. Print out Appendix 1 of this guide.
2. Complete the checklist with as much detail as possible.

Step 2: Perform initial configuration

Assuming the Cisco VCS is in the initial configuration state; follow the Initial configuration steps described in the Video Communications Server Administrator Guide (Version X5) to configure the Cisco VCS basic network parameters:

- ▶ LAN1 IP (v4 or v6) address
- ▶ Subnet mask (if using IPv4)
- ▶ Default Gateway IP address (v4 or v6)

Note: Cisco VCSs require static IP addresses (not dynamic i.e. served via DHCP),

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

- ▶ using a serial cable
- ▶ via the front panel of the Cisco VCS

Refer to the “Initial configuration” section in the Cisco VCS Getting Started Guide for details.

Step 3: Access Cisco VCS using the web interface

After the basic network parameters have been configured (and as long as the network access policy permits it) the Cisco VCS web interface (login screen) should be reachable using a web browser — after entering the Cisco VCS's IP address (or FQDN) into the browser's address bar, the Web interface login screen should be displayed.


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

To log in to the Cisco VCS using the web interface:

1. Enter the IP address of the Cisco VCS into the web browser's address bar.
The Cisco VCS web interface login screen should be displayed in the browser.
2. Click **Administrator login**.
3. Enter the following (default) access credentials:

Username	admin
Password	TANDBERG

4. Click **Login**.
The Cisco VCS **Overview** page should be displayed.

Note: Next to each configuration parameter on the web interface there is an information icon . Clicking the icon opens an information box in the browser containing information, usage notes and the default value of the related parameter.

Refer to “Web interface” in the “Using the Cisco VCS” section of the Cisco VCS Administrator Guide for more details regarding using the web interface.

Step 4: Change admin password

By default (on system initialization) a single Administrator account is defined in the system. It is recommended that the default admin password is changed (from TANDBERG).

To change the administrator user password:

1. Go to the **Administrator accounts** page (**Maintenance > Login accounts > Administrator accounts**).
2. Select the **admin** account.
3. Enter and confirm the new admin account password for the Cisco VCS.
4. Click **Save**.

Note: The password strength (security level) of the entered password string is displayed. The strength is based on the variation of characters in the string, especially by the inclusion of non-alphanumeric characters such as \$%^&.

The best password strength is given for passwords which contain character combinations of at least two lower case letters (**a-z**), two upper case letters (**A-Z**), two digits (**0-9**), two non-alphanumeric characters (i.e. **!"£\$%^&***) and which are the maximum length (14 characters).

Refer to the "System administration access" section of the Cisco VCS Administrator Guide for more details regarding Administration access.

System configuration

Refer to the “System configuration” section of the Cisco VCS Administrator Guide for more details about each configuration section.

Step 5: Configure System name (recommended)

To configure the **System name** (recommended):

1. Go to the **System administration** page (**System configuration > System**).
2. Enter the required name in the **System name** field.
3. Click **Save**.

Overview Status **System configuration** VCS configuration Applications Maintenance

System administration

System name

System name

Administration access

Session time out (minutes) *

Telnet service

SSH service

HTTP service

HTTPS service

Note: It is recommended that the **System name** should be unique within an organization or network and should be limited to a maximum of 16 characters in length (as the LCD panel on the server can only display a maximum of 16 characters).

Step 6: Administration access – Session time-out (optional)

The **Session time-out** value determines the length of time an inactive administrative session is kept open (before the session is automatically closed), in minutes.

A **Session time-out** value of 0 (zero) keeps inactive administrative sessions open indefinitely (until it is ended manually – by closing a browser, or terminates due to a network condition – loss of transmission).

It is recommended to use the default value of 0 while initially configuring a Cisco VCS, then a finite time (for example: 15 minutes) when the platform is in production.

To configure the **Session time-out** value (optional):

1. Go to the **System administration** page (**System configuration > System**).
2. Change the **Session time-out** value (set in minutes).
3. Click **Save**.

The screenshot shows the 'System administration' configuration page. At the top, there are navigation tabs: Overview, Status, System configuration (selected), VCS configuration, Applications, and Maintenance. Below the tabs is the 'System administration' section. Under 'System name', the 'System name' field is set to 'myvcs'. Under 'Administration access', the 'Session time out (minutes)' field is set to '0' and is circled in red. The other services are: Telnet service (Off), SSH service (On), HTTP service (On), and HTTPS service (On). At the bottom, there are 'Save' and 'Restart' buttons.

System name	Value
System name	myvcs

Administration access	Value
Session time out (minutes)	0
Telnet service	Off
SSH service	On
HTTP service	On
HTTPS service	On

Buttons: Save, Restart

Step 7: Administration access – Service access (optional)

By default, administrative access is permitted using SSH, HTTP and HTTPS and denied using Telnet.

Unless there are specific security requirements, it is recommended that you do not change the services that can be used for administrative access.

To configure which services can be used for administrative access:

1. Go to the **System administration** page (**System configuration > System**).
2. Modify the permitted access by changing the value (*On* or *Off*) of the drop-down menu for the relevant service (Telnet, SSH, HTTP and HTTPS).
3. Click **Save**.
4. A system restart is required, click **Restart** (the **Restart** page will appear, click **Restart system**).

The screenshot shows the 'System administration' configuration page. At the top, there are navigation tabs: Overview, Status, System configuration (selected), VCS configuration, Applications, and Maintenance. Below the tabs, the page title is 'System administration'. There are two main sections: 'System name' and 'Administration access'. In the 'System name' section, the 'System name' field contains 'myvcs'. In the 'Administration access' section, there are five rows of settings: 'Session time out (minutes)' with a value of '0', 'Telnet service' with a dropdown set to 'Off', 'SSH service' with a dropdown set to 'On', 'HTTP service' with a dropdown set to 'On', and 'HTTPS service' with a dropdown set to 'On'. A red oval highlights the 'Telnet service', 'SSH service', 'HTTP service', and 'HTTPS service' dropdown menus. At the bottom of the page, there are two buttons: 'Save' and 'Restart'.

Note: HTTP enabled access allows the Cisco VCS to redirect the session started as HTTP to an HTTPS session. It does not allow non-secure access to the Cisco VCS.

Step 8: DNS configuration - DNS address

The Cisco VCS must have at least one domain name server address defined if it is using FQDNs (Fully Qualified Domain Names) instead of IP addresses when specifying external addresses (for example for LDAP and NTP servers, neighbor zones and alternates), or when using features such as URI dialing or ENUM dialing.

1. Go to the **DNS** page (**System configuration > DNS**).
2. Enter a valid DNS server IP address (IPv4 if the Cisco VCS is using IPv4, IPv6 if the Cisco VCS is using IPv6) in the **Address 1** field.
3. Click **Save**.

Overview Status **System configuration** VCS configuration Applications Maintenance

DNS

Saved: DNS settings have been saved.

DNS server

Address 1	<input type="text" value="10.0.0.1"/>
Address 2	<input type="text"/>
Address 3	<input type="text"/>
Address 4	<input type="text"/>
Address 5	<input type="text"/>

Domain name

Domain name	<input type="text" value="example.com"/>
-------------	--

Note: Addresses 2-5 can be used for alternate DNS server addresses (for resilience purposes), or alternatively for DNS server addresses which serve different types of lookup data (for example, ENUM lookups).

Step 9: DNS configuration - DNS Domain name & Local host name

The **Domain name** is used when attempting to resolve server addresses configured on the Cisco VCS that are without any form of qualification (e.g. **myserver** or **my_server** but not **my.server.com**). It applies only to the following:

- ▶ LDAP server
- ▶ NTP server
- ▶ External Manager server
- ▶ Remote logging (syslog) server

The DNS Domain name is appended to the unqualified server address before a query to the DNS server is executed.

To configure the **Domain name**:

1. Go to the **DNS** page (**System configuration > DNS**).
2. Enter the **Domain name**.
3. Click **Save**.

The **Local host name** defines the local DNS host name of this Cisco VCS.

To configure the **Local host name**:

1. Go to the **DNS** page (**System configuration > DNS**).
2. Enter the **Local host name** (a string comprising of only letters, digits, hyphens and underscores (no spaces) – where the first and last characters are letters or digits).
3. Click **Save**.

Overview	Status	System configuration	VCS configuration	Applications	Maintenance
DNS					
DNS server					
Address 1				10.0.0.1	<i>i</i>
Address 2					<i>i</i>
Address 3					<i>i</i>
Address 4					<i>i</i>
Address 5					<i>i</i>
DNS settings					
Local host name				myvcs	<i>i</i>
Domain name				example.com	<i>i</i>
Save					

Step 10: Time configuration – NTP Server and time zone

An NTP server is required for H323 systems and systems with traversal zone relationships. It is also strongly recommend that an NTP server is configured to maintain accurate Cisco VCS log message timestamps.

The **Time zone** setting provides log messages in local time format. The time derived from the NTP server is UTC time (coordinated universal time). The **Time zone** setting provides the system with the local offset to UTC.

Note: Event log entries are prefixed with a local time value and suffixed with a UTC time value.

To configure the NTP server address and time zone:

1. Go to the **Time** page (**System configuration > Time**).
2. Enter the NTP server's address into the **NTP server** field. It can take any of the following formats:
 - IP address
 - FQDN (fully qualified domain name)
 - Unqualified server name to which the DNS Domain name will be appended (for example, myntp_server would be appended with the DNS_domain_name to fully qualify it as myntp_server.DNS_domain_name)
3. Select the relevant local **Time zone** for your region.
4. Click **Save**.

The screenshot shows the Cisco VCS Administrator web interface. At the top, there is a navigation bar with the following tabs: Overview, Status, System configuration (selected), VCS configuration, Applications, and Maintenance. Below the navigation bar, the page title is 'Time'. Underneath, there is a 'Configuration' tab. The configuration area contains two fields: 'NTP server' with the value 'myntp_server' and 'Time zone' with the value 'GMT'. Both fields have an information icon (i) to their right. Below the configuration area, there is a 'Save' button.

Refer to “Time” in the “System configuration” section of the Cisco VCS Administrator Guide for more details regarding NTP server and time zone configuration.

Note: The local time is displayed in the bottom left corner of the Cisco VCS web user interface.

Step 11: SNMP configuration (optional)

Note: SNMP is required when integrating with Cisco TMS.

To enable and configure SNMP:

1. Go to the **SNMP** page (**System configuration > SNMP**).
2. Set **Enabled** to *On*.
3. Enter the **SNMP community name**. By default this is set to *public*. This value is used as an industry standard for SNMP community names.

Note: When integrating with Cisco TMS the **SNMP community name** must be the same as the name configured in Cisco TMS; both the Cisco VCS and Cisco TMS have a default name of *public*.

4. Enter the **System contact** and **location** details. These optional settings can be retrieved via SNMP managers to identify persons responsible to perform local maintenance.
5. Click **Save**.
6. A system restart is required, click **Restart** (the **Restart** page will appear, click **Restart system**).

Overview Status **System configuration** VCS configuration Applications Maintenance

Configuration

Enabled *i*

SNMP community name *i*

System contact *i*

Location *i*

Refer to “SNMP” in the “System configuration” section of the Cisco VCS Administrator Guide for more details regarding SNMP usage.

Step 12: External manager configuration (optional but recommended)

External manager configuration is required to enable the Cisco VCS to communicate with an external manager (Cisco TMS).

To configure the necessary **External manager** parameters:

1. Go to the **External manager** page (**System configuration > External manager**).
2. Enter the FQDN or IP Address of the external manager (Cisco TMS) in the **Address** field. Alternatively an unqualified domain name can be entered as long as the **DNS Domain name** has been entered as described in Step 9 of this document.
3. Configure the external manager **Path**. The default path (which also must be used when using Cisco TMS) is **tms/public/external/management/SystemManagementService.asmx**. Configure the **External manager protocol** by selecting **HTTP** or **HTTPS** from the drop-down menu (this is the protocol the Cisco VCS will use to provide feedback to Cisco TMS).

Note: Cisco TMS may automatically configure the Cisco VCS's **External manager protocol** to **HTTPS**. See below for more details.

4. Configure the **External manager Certificate verification mode** by selecting *On* or *Off* from the drop-down menu. The certificate is only verified if the value is *On* and the protocol is set to *https*.

Note: If the **External manager protocol** is set to **HTTPS** and **Certificate verification mode** is set to *On*, then relevant certificates need loading before the External Manager connection can become active (see document D50520 "Implementing Secure Management" for details).

If either **External manager protocol** is set to **HTTP** or **Certificate verification mode** is set to *Off*, then no certificates need to be loaded.

5. Click **Save**.

The screenshot shows the 'External manager' configuration page in the Cisco VCS interface. The 'Configuration' tab is active. The fields are as follows:

- Address:** mytms.server.example.com
- Path:** tms/public/external/management/systemmanagementservice.asmx
- Protocol:** HTTP
- Certificate verification mode:** On

A 'Save' button is located at the bottom left of the configuration area.

Automatic configuration of external manager protocol in Cisco TMS

Cisco TMS automatically sets the Cisco VCS's **External manager protocol** to **HTTPS** if Cisco TMS is configured as follows:

- ▶ **Administrative Tools > Configuration > Network Settings, TMS Services > Enforce Management Settings on Systems = On** and
- ▶ **Administrative Tools > Configuration > Network Settings, Secure-Only Device Communication > Secure-Only Device Communication = On**

If you do not want Cisco TMS to force the management settings on the Cisco VCS, turn **Enforce Management Settings on Systems** to *Off*.

If it is sufficient for the Cisco VCS to use HTTP (rather than HTTPS) when providing feedback to Cisco TMS, turn **Secure-Only Device Communication** to *Off*.

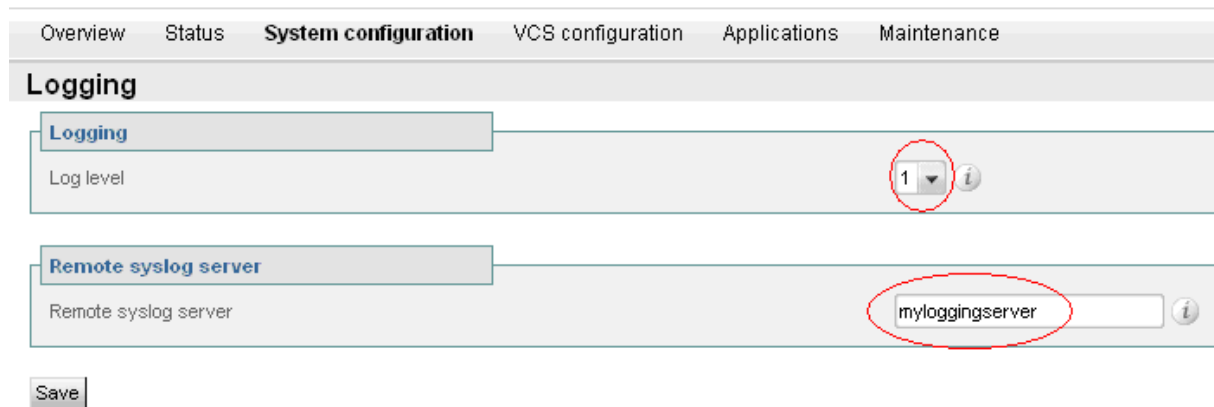
Step 13: Logging configuration (optional)

The Cisco VCS collates and stores system log messages locally. Log messages can (optionally) be sent to a remote syslog server.

To configure a syslog server address:

1. Go to the **Logging** page (**System configuration > Logging**).
2. Enter the address into the **Remote syslog server** field. It can take any of the following formats:
 - IP address
 - FQDN (fully qualified domain name)
 - Unqualified server name to which the DNS Domain name will be appended (for example, `mysyslog_server` would be appended with the `DNS_domain_name` to fully qualify it as `mysyslog_server.DNS_domain_name`)
3. Click **Save**.

Note: By default the system log level is set to level 1. This configures the Cisco VCS to output high level (easily readable) events in system log and syslog messages.



The screenshot shows the Cisco VCS Administrator GUI. The top navigation bar includes 'Overview', 'Status', 'System configuration', 'VCS configuration', 'Applications', and 'Maintenance'. The 'System configuration' tab is active. Below the navigation bar, the 'Logging' section is displayed. It contains two main configuration areas: 'Logging' and 'Remote syslog server'. In the 'Logging' area, the 'Log level' is set to 1, indicated by a dropdown menu with a red circle around it. In the 'Remote syslog server' area, the text 'myloggingserver' is entered into the input field, also circled in red. A 'Save' button is located at the bottom left of the configuration area.

For more information on log levels refer to “Logging” in the “System configuration” section of the Cisco VCS Administrator Guide.

Enabling registrations and calls

The Cisco VCS platform supports two different signaling protocols: H.323 and SIP.

The Cisco VCS also supports interworking functionality. Interworking enables calls initiated from one signaling protocol to be made to destinations which use the other signaling protocol (i.e. from a SIP registered endpoint to a H.323 registered endpoint and vice versa).

All endpoints which are required to make calls via the Cisco VCS must first be registered to the Cisco VCS.

The registration process (at high level) requires that the endpoint first makes its address (identity) known to the Cisco VCS. The Cisco VCS then accepts (or rejects) the registration. After the endpoint is successfully registered, the Cisco VCS will attempt to route all signaling messages received for the endpoint address (identity) to the endpoint.

Some endpoints support a single signaling protocol (i.e. H.323 or SIP); some endpoints support dual protocol registration (i.e. H.323 and SIP).

Endpoints registering using H.323 can register the following address types to the Cisco VCS:

- ▶ H323 ID – for example: **user1** or **user1@example.com**
- ▶ E.164 number – for example: **0123456789**

Endpoints registering using SIP can register the following address type to the Cisco VCS:

- ▶ SIP URI – for example: **user1@example.com**

Step 14: H.323 only configuration (optional)

By default H.323 endpoints can register with the Cisco VCS and make calls to one another using their registered addresses (H.323 id or E.164 number).

Note: To check which endpoints are registered to a Cisco VCS go to the **Registration by alias page** on the Cisco VCS (**Status > Registrations > By alias**).

Step 15: SIP only configuration (optional)

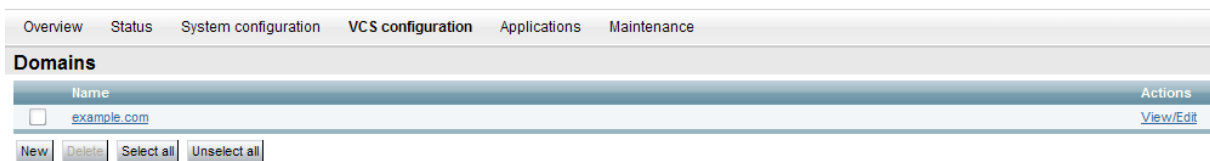
SIP endpoints register SIP URI (Uniform Resource Identifier) addresses to the Cisco VCS.

SIP URIs are made up of the user information @ domain name (for which the Cisco VCS has authority).

The domain name must be configured on the Cisco VCS to allow SIP endpoint to register, using the domain name as part of the URI.

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



Overview		Status	System configuration	VCS configuration	Applications	Maintenance
Domains						
Name						Actions
<input type="checkbox"/> example.com						View/Edit
New Delete Select all Unselect all						

Note: After the domain name has been configured (on the Cisco VCS), SIP endpoints will be able to register using this domain name, for example: a Cisco VCS is configured with the domain name of **example.com** will accept registrations from an endpoint registering using SIP URI of **user1@example.com**.

Note: After SIP endpoints have registered, they can make and receive calls using their SIP URIs.

Step 16: Mixed H.323 and SIP configuration

The following configuration recommendation assumes that the Cisco VCS Control is authoritative for a single SIP domain (i.e. has only one SIP domain configured).

Perform the following instructions after completing steps 14 and 15.

The following steps describe how to configure the Cisco VCS to:

- ▶ check if a called address contains a '@' character – if it does not, then '@' and the Cisco VCS SIP domain name is appended to the dialed address.

For example, if the called address is '01234' the Cisco VCS will automatically append the configured domain name (in this case example.com) to the called address (i.e. 01234@example.com), before attempting to set up the call.

Note: The purpose of appending the valid SIP domain is to standardize called addresses originating from both H.323 and SIP devices.

Note: The Cisco VCS will only attempt to search for addresses which match valid SIP URIs (i.e. using valid SIP domain).

- ▶ strip off the SIP domain portion of the called address, and attempt to find a locally registered H.323 device.
- ▶ if no device is located, attempt a second search (without stripping off the SIP domain portion of the called address) to attempt to find a locally registered SIP device.

To configure the **Transform** which appends '@' and the configured SIP domain to the called addresses (which does not already contain an '@' and a domain):

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

Pattern string	Enter <code>[^@]*</code>
Pattern type	Select Regex
Pattern behavior	Select Replace
Replace string	Enter <code>\1@<i>sip.domain</i></code>

4. Click **Create transform**.

Overview Status System configuration **VCS configuration** Applications Maintenance

Create transform

Configuration

Pattern string * ⓘ

Priority ⓘ

Pattern type **Regex** ⓘ

Pattern behavior **Replace** ⓘ

Replace string ⓘ

To configure the **Search rules** required to locate the locally registered H.323 or SIP device:

1. Go to the **Search rules** page (**VCS configuration > Search rules > Rules**).
2. Click **New**.
3. Configure the fields as follows:

Rule name	Enter a name (for example: h323search)
Zone name	Select LocalZone

4. Click **Create rule**.
5. Configure the fields as follows:

Priority	Enter 48
Source	Select Any
Mode	Select AliasPatternMatch
Pattern type	Select Regex
Pattern string	Enter (.+)@sip.domain.* (for example (.+)@example.com.*)
Pattern behavior	Select Replace
Replace string	Enter \1
On successful match	Select Continue
Target zone	Select LocalZone

6. Click **Save**.

Overview Status System configuration **VCS configuration** Applications Maintenance

Edit search rule

Configuration

Rule name	<input type="text" value="h323search"/>
Priority	<input type="text" value="48"/>
Source	<input type="text" value="Any"/>
Mode	<input type="text" value="AliasPatternMatch"/>
Pattern type	<input type="text" value="Regex"/>
Pattern string	<input type="text" value="(.)@example.com."/>
Pattern behavior	<input type="text" value="Replace"/>
Replace string	<input type="text" value="\1"/>
On successful match	<input type="text" value="Continue"/>
Target zone	<input type="text" value="LocalZone"/>

7. Go to the **Search rules** page (**VCS configuration > Search rules > Rules**).
8. Click **New**.
9. Configure the fields as follows:

Rule name	Enter a name (for example: urisearch)
Zone name	Select LocalZone

10. Click **Create rule**.

11. Configure the fields as follows:

Priority	Enter 50
Source	Select Any
Mode	Select AliasPatternMatch
Pattern type	Select Regex
Pattern string	Enter (.+)@sip.domain.* (for example (.+)@example.com.*)
Pattern behavior	Select Leave
On successful match	Select Continue
Target zone	Select LocalZone

12. Click **Save**.

Overview Status System configuration **VCS configuration** Applications Maintenance

Edit search rule

Configuration

Rule name: * urisearch ⓘ

Priority: * 50 ⓘ

Source: Any ⓘ

Mode: AliasPatternMatch ⓘ

Pattern type: Regex ⓘ

Pattern string: (.*)@example.com.* ⓘ

Pattern behavior: Leave ⓘ

On successful match: Continue ⓘ

Target zone: LocalZone ⓘ

Save **Delete** **Cancel**

Related tasks

[Test whether a pattern match or transform has the expected result](#)

[Perform a test search for an alias](#)

Note: It should now be possible for:

- ▶ an H.323 device registered as H.323id = “user1” to call a SIP device registered as SIP URI = “user2@example.com” by calling address “user2” from the H.323 endpoint
- ▶ a SIP device registered as SIP URI = user2@example.com to call an H.323 device registered as “user1” by calling address “user1@example.com” from the SIP endpoint

Note: Some SIP devices will automatically append the SIP domain to a dialed address, for example it may be possible for the user to enter “user1” and the device will actually call user1@example.com.

Appendix 1 – Configuration checklist

Item	Required, recommended or optional	Make a note for your reference			
Cisco VCS Administrator guide version X5	Recommended	See http://www.tandberg.com			
Cisco VCS Getting Started guide	Recommended	See http://www.tandberg.com			
IP version	Required	<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td style="text-align: center;">4</td> <td style="text-align: center;">6</td> <td style="text-align: center;">Both</td> </tr> </table> <p style="text-align: center;">(Circle one)</p>	4	6	Both
4	6	Both			
IPv4 default gateway	Required (if using IPv4)	<p style="text-align: center;">____.____.____.____</p> <p style="text-align: center;">(Fill in IPv4 address)</p>			
IPv6 default gateway	Required (if using IPv6)	<p style="text-align: center;">____:____:____:____:____:____</p> <p style="text-align: center;">(Fill in IPv6 address)</p>			
LAN1 IPv4 address	Required (if using IPv4)	<p style="text-align: center;">____.____.____.____</p> <p style="text-align: center;">(Fill in IPv4 address)</p>			
LAN1 IPv4 subnet mask	Required (if using IPv4)	<p style="text-align: center;">____.____.____.____</p> <p style="text-align: center;">(Fill in IPv4 address)</p>			
LAN1 IPv6 address	Required (if using IPv6)	<p style="text-align: center;">____:____:____:____:____:____</p> <p style="text-align: center;">(Fill in IPv6 address)</p>			

System name	Recommended	_____				
		(Write system name)				
Administration access time-out	Optional	<table border="1"> <tr> <td>_____ Minutes</td> <td>No time-out</td> </tr> </table>	_____ Minutes	No time-out		
_____ Minutes	No time-out					
		(Fill in and / or circle one)				
Administration access services	Recommended	<table border="1"> <tr> <td>Telnet</td> <td>SSH</td> <td>HTTP</td> <td>HTTPS</td> </tr> </table>	Telnet	SSH	HTTP	HTTPS
Telnet	SSH	HTTP	HTTPS			
		(Circle allowed access methods)				
DNS server address	Recommended	<p>_____</p> <p>_____ : _____ : _____ : _____ : _____ : _____</p>				
		(Fill in IPv4 or IPv6 address)				
DNS local host name	Optional	_____				
		(Write host name)				
DNS domain name	Optional	_____				
		(Write domain name)				
NTP server	Recommended (Required) for systems using H323, or to maintain accurate log message timestamps in SIP only deployments).	_____				
		(Write server name or IP address)				
Time zone	Recommended	_____				
		(Write time zone, e.g.: GMT)				

SNMP enabled	Optional (Recommended when integrating with Cisco TMS as an external manager).	<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td style="padding: 2px 10px;">On</td> <td style="padding: 2px 10px;">Off</td> </tr> </table> <p style="text-align: center;">(Circle one)</p>	On	Off
On	Off			
SNMP community name	Required (if SNMP is enabled)	<p style="text-align: center;">_____</p> <p style="text-align: center;">(Write community name, normally: public)</p>		
SNMP system contact	Optional	<p style="text-align: center;">_____</p> <p style="text-align: center;">(Write contact name)</p>		
SNMP location	Optional	<p style="text-align: center;">_____</p> <p style="text-align: center;">(Write location)</p>		
External manager (Cisco TMS) Address	Optional	<p style="text-align: center;">_____</p> <p style="text-align: center;">(Write server name (FQDN) or IP address)</p>		
External manager (Cisco TMS) protocol	Required (if using an external manager such as Cisco TMS)	<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td style="padding: 2px 10px;">HTTP</td> <td style="padding: 2px 10px;">HTTPS</td> </tr> </table> <p style="text-align: center;">(Circle one)</p>	HTTP	HTTPS
HTTP	HTTPS			
External manager (Cisco TMS) certificate verification mode	Required (if using an external manager, such as Cisco TMS)	<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td style="padding: 2px 10px;">On</td> <td style="padding: 2px 10px;">Off</td> </tr> </table> <p style="text-align: center;">(Circle one)</p>	On	Off
On	Off			
Remote syslog server	Optional	<p style="text-align: center;">_____</p> <p style="text-align: center;">(Write server name or IP address)</p>		

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.