Cisco VCS Expressway Starter Pack

Cisco TelePresence Deployment Guide

Cisco VCS X5.1

D14618.02

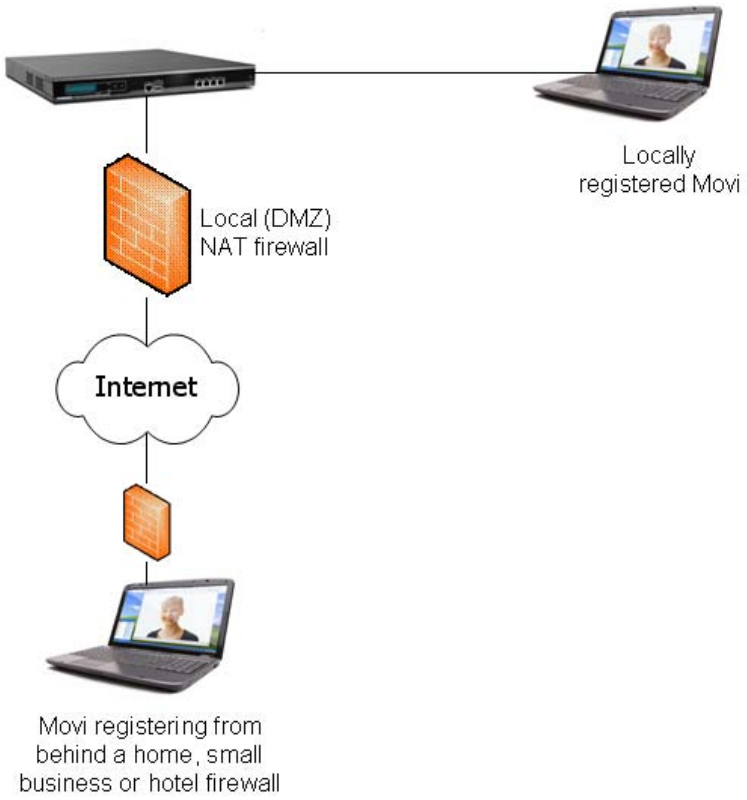
November 2010

Contents

Introduction

A Cisco TelePresence Video Communications Server (Cisco VCS) with the Starter Pack option key creates a Cisco VCS Expressway Starter Pack which acts as a standalone provisioning server, registrar and proxy server for Movi endpoints.

The Cisco VCS Expressway Starter Pack may have endpoints register to it locally or register to it from behind a home, small business or hotel firewall.



If the Cisco VCS Expressway Starter Pack services Movi users that are behind a firewall, the Cisco VCS must have a public IP address – the local (DMZ) firewall must pass the specific public IP address traffic to the Cisco VCS.

The Dual Network interface option may be used on the Cisco VCS Expressway Starter Pack. When enabled, the Cisco VCS can be deployed behind a local static NAT firewall; the Cisco VCS is configured with the public IP address of the local (DMZ) NAT firewall so that when the Cisco VCS communicates with other devices it appears as an Internet routable device despite being behind the local NAT firewall.

Note: Ensure sufficient bandwidth is available when making calls through firewalls and other infrastructure. For example, 5 simultaneous calls using 512kbps in each direction will require 2.5Mbps bandwidth for this video traffic on top of its normal operation.

Purpose of this guide

This deployment guide describes the configuration steps required to configure a Cisco VCS Expressway Starter Pack, including basic configuration, provisioning, and also how to configure user accounts so that Movi clients are provisioned when users sign on to them.

Related documents

Document number	Title
D14049	Cisco VCS Administrator Guide
D14088	FindMe™ User Guide
D14427	Provisioning troubleshooting guide
D14525	Cisco VCS Deployment Guide – FindMe™

Configuring the Cisco VCS

This deployment guide assumes that the Cisco VCS is accessible on an IP network and has had a basic configuration implemented. This means that the Cisco VCS has been configured with:

- IP details
- DNS details
- NTP server details

Note: Brief instructions on how to carry out this configuration is available in 'Appendix 1 – Basic Cisco VCS configuration' on page 18.

If the system is required to support calling to non-registered endpoints, a DNS zone should be configured together with a search rule that sends any calls to it that are not for the Cisco VCS's local SIP domain.

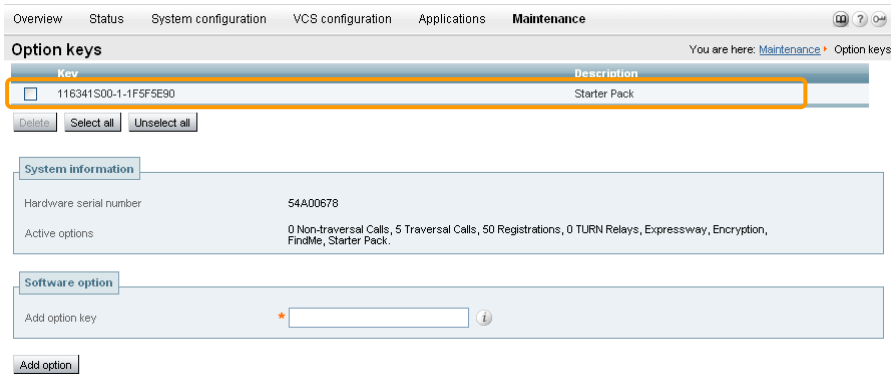
Firewall ports

If the Cisco VCS is placed in a DMZ, to enable SIP calls to be received the following IP ports must be open to the Cisco VCS through the firewall:

- 5060 (if basic SIP connection is required)
- 5061 (for SIP over TLS)
- 50000 to 52399 (for media)

Check option key

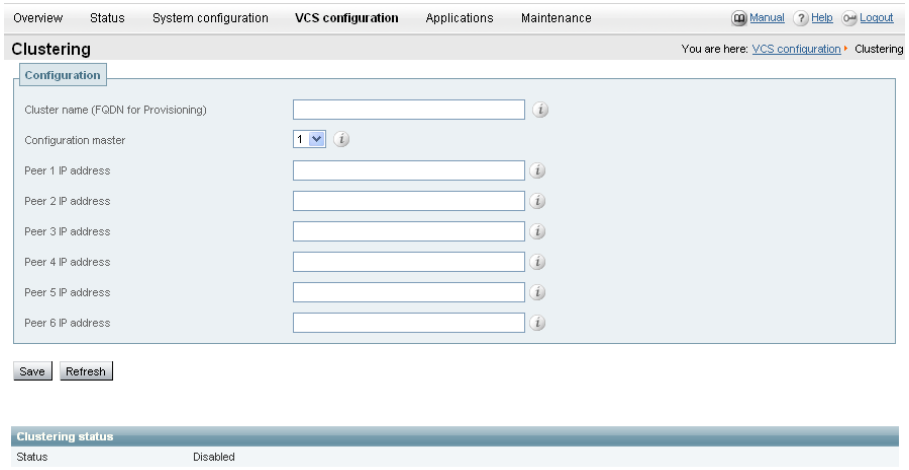
- Ensure that Starter Pack is enabled: check that the **Starter Pack** option key is listed on the **Option keys** page (**Maintenance > Option keys**):



Configure the routable address of the Cisco VCS

The routable address of the Cisco VCS (its FQDN) is the address supplied by the provisioning system to the provisioned device (Movi) for it to use as its SIP registrar (the address to which it sends registration requests).

1. Go to the **Clustering** page (**VCS configuration > Clustering**).



2. Configure the fields as follows:

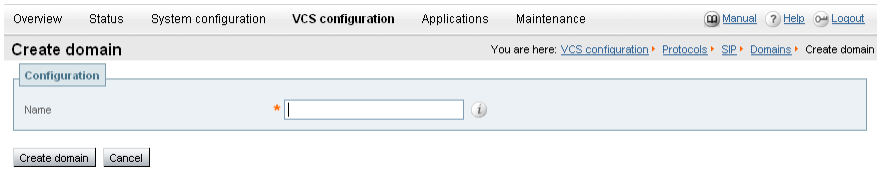
Cluster name (FQDN for Provisioning)	Routable address of the Cisco VCS, ideally the DNS SRV address of the Cisco VCS, alternatively a DNS A record or an IP address. Typically your IT department will supply the FQDN for this Cisco VCS and ensure that the network is configured to route SIP calls, HTTPS and other IP traffic to this Cisco VCS when addressed to the FQDN.

No other field on this page needs to be configured.

3. Click **Save**.

Ensure that Cisco VCS has a SIP domain configured

1. On the **Domains** page (**VCS Configuration > Protocols > SIP > Domains**) if no domain is configured, click **New**.



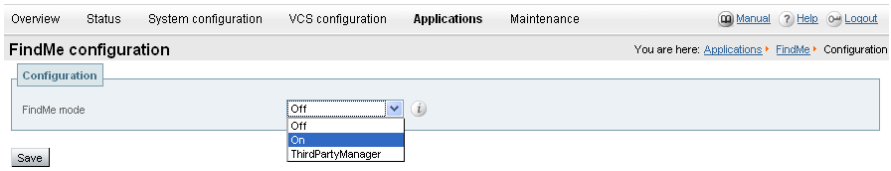
2. Configure the fields as follows:

Name	The SIP domain to be used for this installation, e.g. company.com

3. Click **Create domain**.

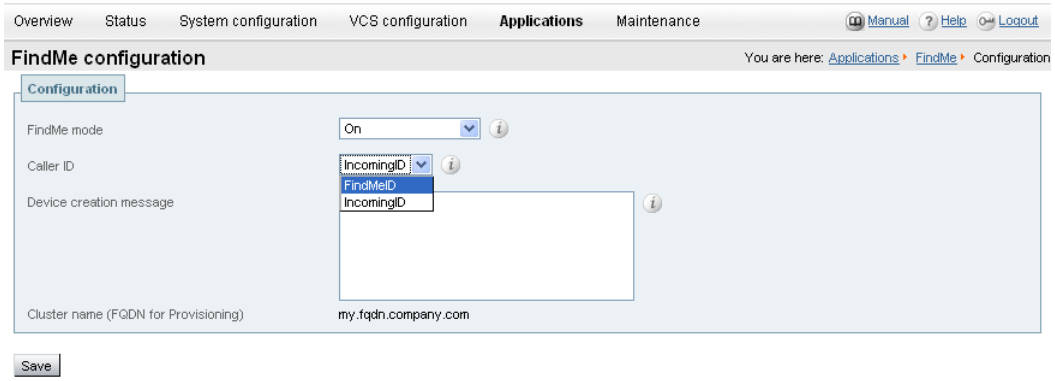
Enable FindMe™

1. Go to the **FindMe configuration** page (**Applications > FindMe > Configuration**).



2. Configure the fields as follows:

FindMe mode	**On**



3. Configure the fields as follows:

Caller ID	**FindMe ID**: the caller ID of a call being made through this Cisco VCS is replaced with the relevant FindMe ID.

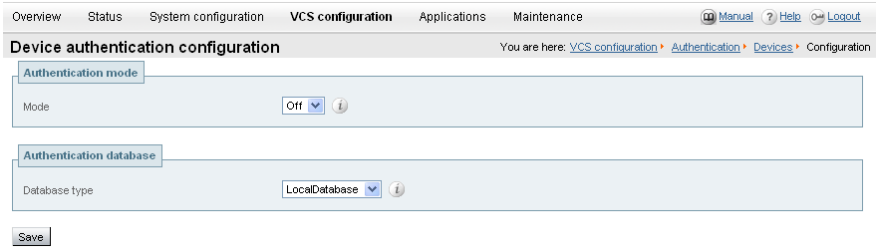
Note: For more details on the use of Caller ID and FindMe ID, see “Appendix 6 – Determining the FindMe ID for a caller” on page 27.

4. Click **Save**.

Enable device authentication (recommended)

If device authentication is to be used – verifying that endpoints can identify themselves with a username and password known to the Cisco VCS – it should be enabled now so that when users are created the appropriate prompts are given to set up the user’s endpoint authentication credentials.

1. Go to the **Device authentication configuration** page (**VCS Configuration > Authentication > Devices > Configuration**) and click **New**.



2. Configure the fields as follows:

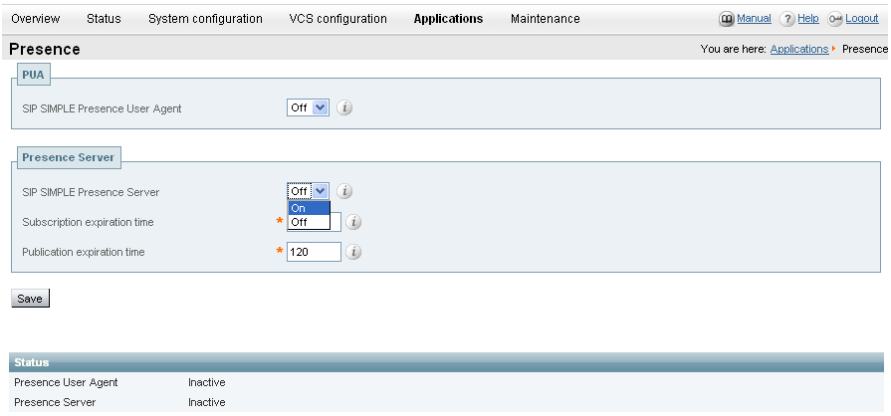
Mode	**On**
Database type	**LocalDatabase**

3. Click **Save**.

Enable presence server (optional)

The presence server allows Movi clients to see the presence status (Online, Away, Busy in a call and Offline) of other Movi clients.

1. Go to the **Presence** page (**Applications > Presence**).



2. Configure the fields as follows:

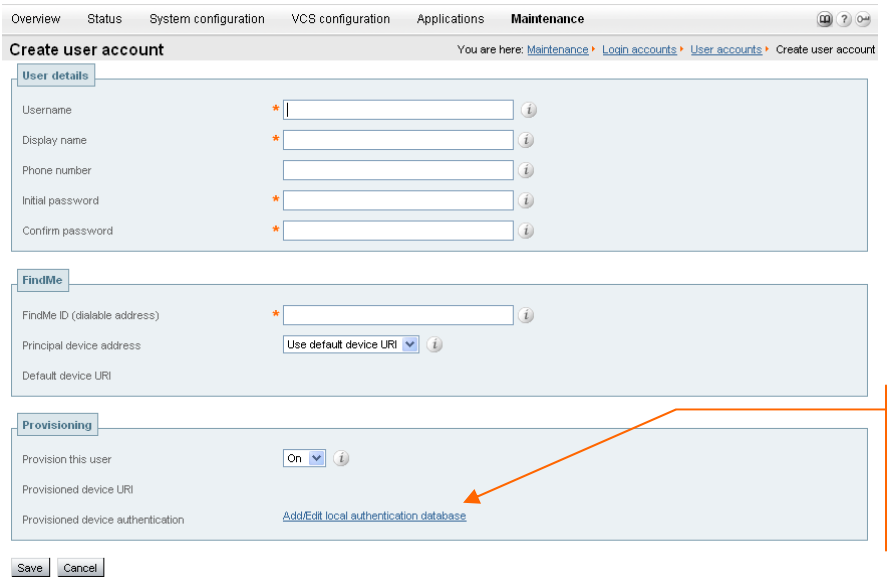
SIP SIMPLE Presence Server	**On**

3. Click **Save**.

Create user accounts

You must configure an account for each user:

1. Go to the **User accounts** page (**Maintenance > Login accounts > User accounts**) and click **New**.



This link is only displayed if device authentication is enabled.

Right-click this link to avoid losing the data already entered on this screen – see instructions below.

2. Configure the fields as follows:

Username	The username for logging into this user account, for example **name.surname**. Note that the username is case sensitive. This same username must be used as the name in the local authentication database if device authentication is enabled. This username is also used to create the FindMe default device URI and the provisioned device URI. To create these as a valid SIP URI, the username must consist of alphanumeric characters but not spaces, the @ sign or extended characters (such as ö or â). For the full set of allowed characters, see ”Appendix 5 – Characters allowed in SIP URIs”. Note: the **Username** must be different from the **FindMe ID**.
Display name	The user’s name without formatting restrictions. It is displayed on the user search page and used in phone books. For example **Name Surname**
Phone number (optional)	The E.164 caller ID to be presented on outdialed H.323 calls, e.g. to ISDN gateways. It must only contain digits – do not include any spaces, hyphens or brackets. Note: If calls may be placed to an ISDN gateway, ensure that the format of this phone number matches the requirements of the ISDN provider.
Initial password**	The password to log into the user’s account on the Cisco VCS.
Confirm password**	Repeat the password entered above.
FindMe ID	The FindMe ID is a unique alias through which the user can be contacted on all of their endpoints. It can be a URI, an H.323 ID or an E.164 number. For use with Movi, a FindMe ID in the form of a SIP URI is recommended. For example **name.surname@company.com** Note: the **FindMe ID** must be different from the **Username** (but it can, for example, be in the format username@domain).
Principal device address	The principal device address identifies the user’s main device. It is the ID of a device that is called when somebody dials the user’s FindMe ID. **Use default device URI**: this is the recommended configuration. The default principal device URI is the same as the device URI that will be provisioned for this user. **Specify a device URI:** select this only if a URI other than that of the device being provisioned is required for this user. In which case you must then enter a **Principal device URI** as the URI, H.323 ID or E164 number of the primary device for this user. Note 1: Principal devices cannot be deleted by users. Note 2: The principal device address must be different from the FindMe ID.
Provision this user	**On**
Add/Edit local authentication database	This link is only displayed if device authentication is enabled. **TAKE CARE**: If you select this link while adding or changing user account details you will lose the data already entered on this screen. You should either select this link after the user account details have been saved (by editing this user) or by right-clicking on the link and selecting “Open in New Window” (or equivalent depending on your browser version).

	See “Create authentication credentials for the user (optional)” below for more details.

** The password entries are only displayed if **User authentication source** is set to **Local** (see “Enable FindMe™“ on page 8.)

3. Click **Save.**
4. Repeat these steps to create accounts for all users.

Additional users can be added later, as and when required, by returning to the **User accounts** page and selecting **New**.

Note: Cisco VCS Expressway Starter Pack supports a maximum of 50 registered users.

After an account has been set up, its details (except the **Username**) can be edited by selecting the user on the **User accounts** page (**Maintenance > Login accounts > User accounts**) and then clicking **View/Edit**.

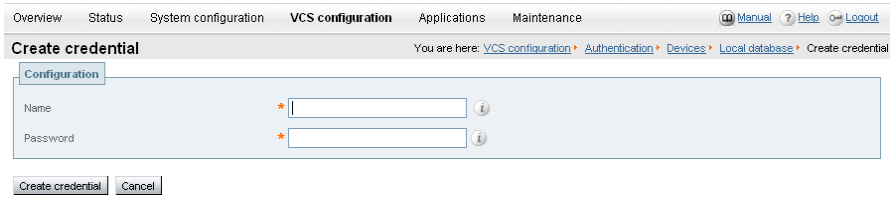
Create authentication credentials for the user (optional)

If device authentication has been enabled, the credentials entered into the Cisco VCS must exactly match those used to sign on to Movi – otherwise provisioning requests, registration requests, call requests and phone book requests will be rejected.

In a typical installation you are recommended to use the same password for both the user’s Movi authentication credentials and for their user account login (where users access their FindMe details).

1. From near the bottom of the **Create user account** or **Edit user account** pages right-click on the Add/Edit local authentication database link and select ‘Open in New Window’ (or equivalent depending on your browser version).

   Alternatively using the menu go to the **Local authentication database** page (**VCS Configuration > Authentication > Devices > Local database**).
2. Click **New**.



3. Configure the fields as follows:

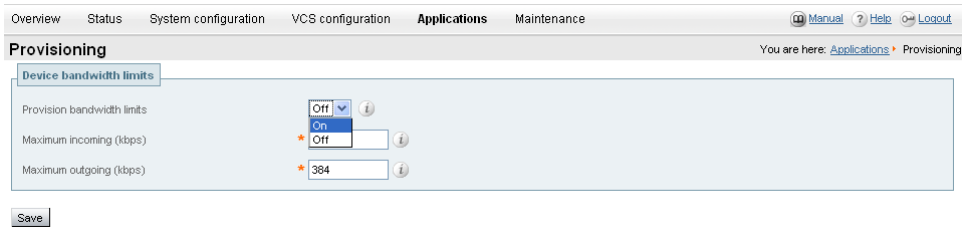
Name	The credential name must be the same as the user account username – as indicated by the link on the **Create user account** and **Edit user account** pages. It is also the Movi sign in username.
Password	The password must be the same as the Movi sign in password. (Typically this is also the same as the user account password used for accessing FindMe details.)

4. Click **Create credential**.
5. If appropriate, close any new window or tab that was opened to create this credential.

Configure bandwidths provisioned to Movi clients (optional)

The Cisco VCS can provision bandwidth limits to Movi clients. These are used to configure Movi with default values for it to use for incoming and outgoing bandwidth control.

1. Go to the **Provisioning** page (**Applications > Provisioning**).
2. Set **Provision bandwidth limits** to **On**.



3. Check and set the **Maximum incoming** bandwidth for Movi (e.g. 512kbps).
4. Check and set the **Maximum outgoing** bandwidth for Movi (e.g. 384kbps).
5. Click **Save**.

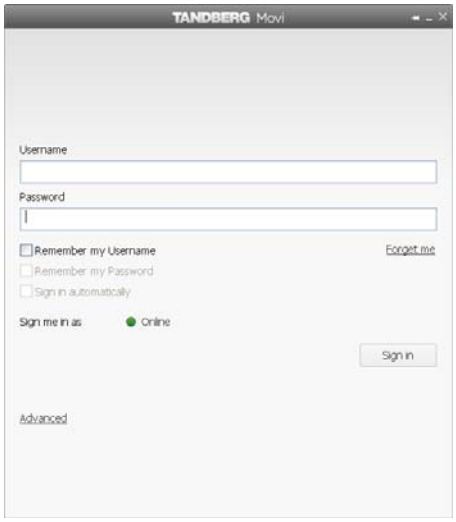
Note: Cisco VCS links and pipes can also be used for more advanced bandwidth control.

Installing and configuring Movi

As part of the Cisco TelePresence Movi Starter Pack – Express Edition solution, a Movi software client installation pack will be supplied. Movi can be installed by IT administrators, or more typically will be supplied to end users for them to install.

After Movi has been installed, it must be configured with user credentials and connection details for the Cisco VCS Expressway Starter Pack:

1. Start Movi.

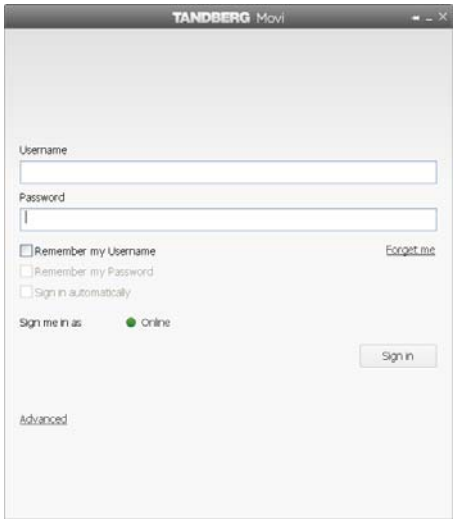


2. Click **Advanced**.

3. Configure the fields as follows:

Internal VCS	The DNS name or IP address of the private side of the Cisco VCS.
External VCS	The DNS name or IP address of the public side of the Cisco VCS.
SIP Domain	The SIP Domain should be the same as configured on the Cisco VCS's **Domains** page (**VCS Configuration > Protocols > SIP > Domain**)
Transport	**Auto**

4. Click **OK** to return to the Movi sign in page.



5. Configure the fields as follows:

Username	The same username as entered on the Cisco VCS in the **Create user account** page (**Maintenance > Login accounts > User accounts**).
Password	If device authentication is enabled this must be the same password as the authentication credential password entered for this user (**VCS configuration > Authentication > Devices > Local database**). Typically this will be the same as the user's account password on the Cisco VCS.
Remember my Username	Select this to save you from typing in your username every time you start Movi.
Remember my Password	Select this if you are the only user of the PC that Movi is installed on and you are happy to have the password automatically applied.
Sign in automatically	Select this if Movi should start and sign in automatically when you log in to your computer.
Sign me in as	Select the initial presence status to display to other users when you sign in.

6. Click **Sign in**.

Making calls

- When you are signed in to Movi, calls can be made by entering the FindMe ID of another user in the **Type name, number or address** field and then pressing **Enter**.

Testing the Cisco VCS Expressway Starter Pack installation

Local system testing

Start by testing Movi devices locally registered to the Cisco VCS Expressway Starter Pack.

1. Configure three users.
2. Install three Movi clients.
3. Connect the three Movi PCs to the same network as the Cisco VCS Expressway Starter Pack.
4. With each of the Movi clients sign in as a different user (for example User1, User2 and User3):
   - Ensure that sign in is successful.
   - Ensure that each Movi user can call the others by entering another user's FindMe ID in the **Type name, number or address** field and then pressing **Enter**.

Result Matrix – local only		Receiving Movi		
		User1 (local)	User2 (local)	User3 (local)
Calling Movi	User1 (local)			
	User2 (local)			
	User3 (local)			

Public network testing

When local system testing is successful, test Movi in the public network.

1. Sign out of two of the Movi clients (User2 and User3) and connect these two Movi PCs to the public internet.
2. With the public internet Movi clients, sign in as User2 and User3:
   - Ensure that sign in is successful.
   - Ensure that each Movi user can call the others by entering another user's FindMe ID in the **Type name, number or address** field and then pressing **Enter**.

Result Matrix – local and internet		Receiving Movi		
		User1 (local)	User2 (internet)	User3 (internet)
Calling Movi	User1 (local)			
	User2 (internet)			
	User3 (internet)			

Behind home, small business or hotel firewall testing

When public network testing is successful, test Movi behind a firewall.

1. Sign out of the two Movi clients in the public network and connect them behind a home, small business or hotel firewall.
2. With the Movi clients sign connected behind the firewall, sign in as User2 and User3:
   - Ensure that sign in is successful.
   - Ensure that each Movi user can call the others by entering another user's FindMe ID in the **Type name, number or address** field and then pressing **Enter**.

Result Matrix – local and behind firewall		Receiving Movi		
		User1 (local)	User2 (firewall)	User3 (firewall)
Calling Movi	User1 (local)			
	User2 (firewall)			
	User3 (firewall)			

Appendix 1 – Basic Cisco VCS configuration

Follow the process specified in the "Cisco VCS Getting Started Guide" to connect, power up, configure the IP address, change passwords and gain access to the Cisco VCS via the web browser.

System name

1. Go to **System configuration > System** and set **System name** to a name that represents this Cisco VCS, for example "VCS Movi server".
2. Enable or disable Telnet, SSH, HTTP and HTTPS as required.

Note: HTTP is just a redirect to HTTPS – turning off HTTPS will prevent web access to the Cisco VCS.

DNS

1. Go to **System configuration > DNS** and configure a DNS server address in the **DNS server Address 1** field. If other DNS servers are available, others can be added for DNS server resilience.
2. Set **Local host name** to be the DNS hostname for this Cisco VCS – note this name must not have any spaces in it.
3. Set **Domain name** to be the suffix which when added to an unqualified DNS name makes it into an FQDN.

Note: <Local host name>.<DNS domain name> = FQDN of this Cisco VCS.

NTP

1. Go to **System configuration > Time** and configure the **NTP server** address and **Time zone** in which the Cisco VCS is located.
2. Check that after clicking **Save** and returning to this page the NTP **State** shows Active.

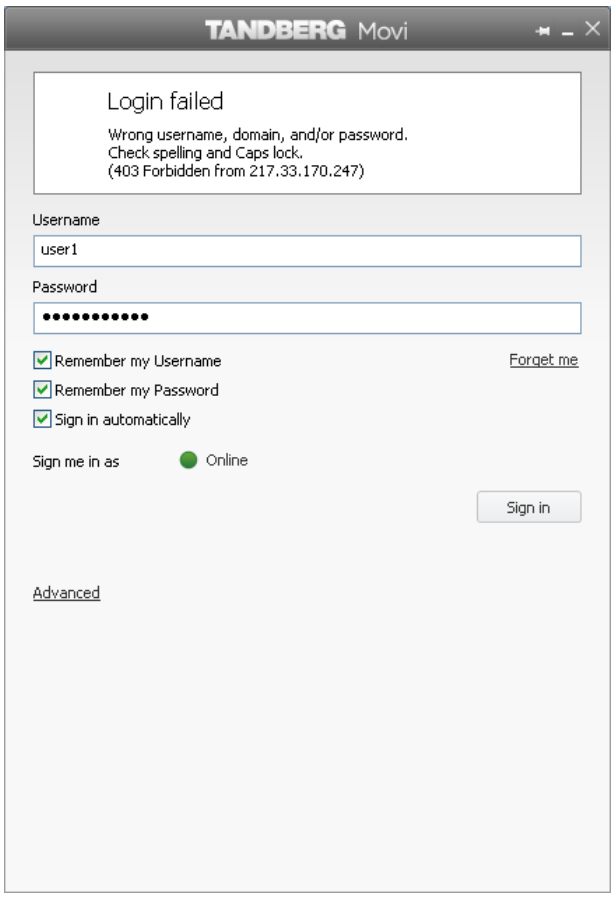
Further information

For further details on the configuration and operation of Cisco VCS, please see the Cisco VCS Administrator Guide.

Appendix 2 – Troubleshooting

Movi sign in messaging

If there are problems signing in to Movi, a status message will be displayed, for example:



Possible messages include:

Login failed – Wrong username, domain, and / or password

- Check and correct these items either at the Movi login, or on the Cisco VCS.
  - Mis-typed domain names are a common cause of this problem (see **VCS Configuration > Protocols > SIP > Domains**). The Movi SIP domain must match a SIP domain on the Cisco VCS that is provisioning the Movi and that Movi will register to.
- Check that Cisco VCS allow / deny lists are not preventing the registration.

Login failed – Out of licenses

- Check the number of registered users – Cisco VCS Expressway Starter Pack supports a maximum of 50 simultaneous registrations.
- Make sure that Movi is trying to connect to the correct IP address for the Cisco VCS Expressway Starter Pack.

Login failed – The server did not respond in time

This means the provisioning request was acknowledged by the server, but no provisioning message was received by Movi.

- Make sure that no firewalls are blocking communication from the Cisco VCS to Movi.
- Make sure that the Cisco VCS can contact the IP address of the Movi (or if behind a home, small business or hotel firewall, the outside IP address of that firewall).

Login failed – Could not find server in DNS

The term "server" refers to the provisioning server before the Movi is provisioned, and the Cisco VCS after Movi is provisioned.

- Check that the **Internal VCS** and **External VCS** names on the Movi **Advanced** dialog are resolvable by the Movi PC, for example by attempting to ping the DNS names. (These are the addresses Movi uses when requesting to be provisioned.)
- Check that the **Cluster name (FQDN for provisioning)** on the **VCS configuration > Clustering** page of Cisco VCS is resolvable by the Movi PC, for example by attempting to ping the DNS name.

Login failed – Unable to connect to server

The term "server" refers to the provisioning server before the Movi is provisioned, and the Cisco VCS after Movi is provisioned.

- Check that the **Internal VCS** and **External VCS** names on the Movi **Advanced** dialog are resolvable by the Movi PC and resolve to the Cisco VCS Expressway Starter Pack address, for example by attempting to ping the DNS names. (These are the addresses Movi uses when requesting to be provisioned.)
- Check that the **Cluster name (FQDN for provisioning)** on the **VCS configuration > Clustering** page of Cisco VCS is resolvable by the Movi PC and resolves to the Cisco VCS Expressway Starter Pack address, for example by attempting to ping the DNS name.
- Check that **TCP mode** and **TLS mode** are both set to **On**. (Check this on the **VCS configuration > Protocols > SIP > Configuration** page.)
- Make sure the Cisco VCS is configured to listen on the ports Movi is trying to access, by default **TCP port** = 5060 and **TLS port** = 5061. (Check this on the **VCS configuration > Protocols > SIP > Configuration** page.)

Call failed – The user could not be found. The user is offline or does not exist.

Check the called ID entered in the **Type name, number or address** field (past entries are available under the **Recent calls** tab).

If this is correct, check:

- Is the called party offline?
- Is the called party dialable on this network?

Call failed – The user could not be found

Check the called ID entered in the **Type name, number or address** field (past entries are available under the **Recent calls** tab).

If this is correct, check:

- Is the called party offline?
- Is the called party dialable on this network?

Call failed – The user could not be reached. Please try again later.

The user did not respond.

Call failed – An error was received from the server

The call was rejected by the Cisco VCS. The error message received from the server is in the user's Audit.log. See the Movi troubleshooting section in the Cisco TMS Provisioning troubleshooting guide.

Call failed – Not enough call licenses

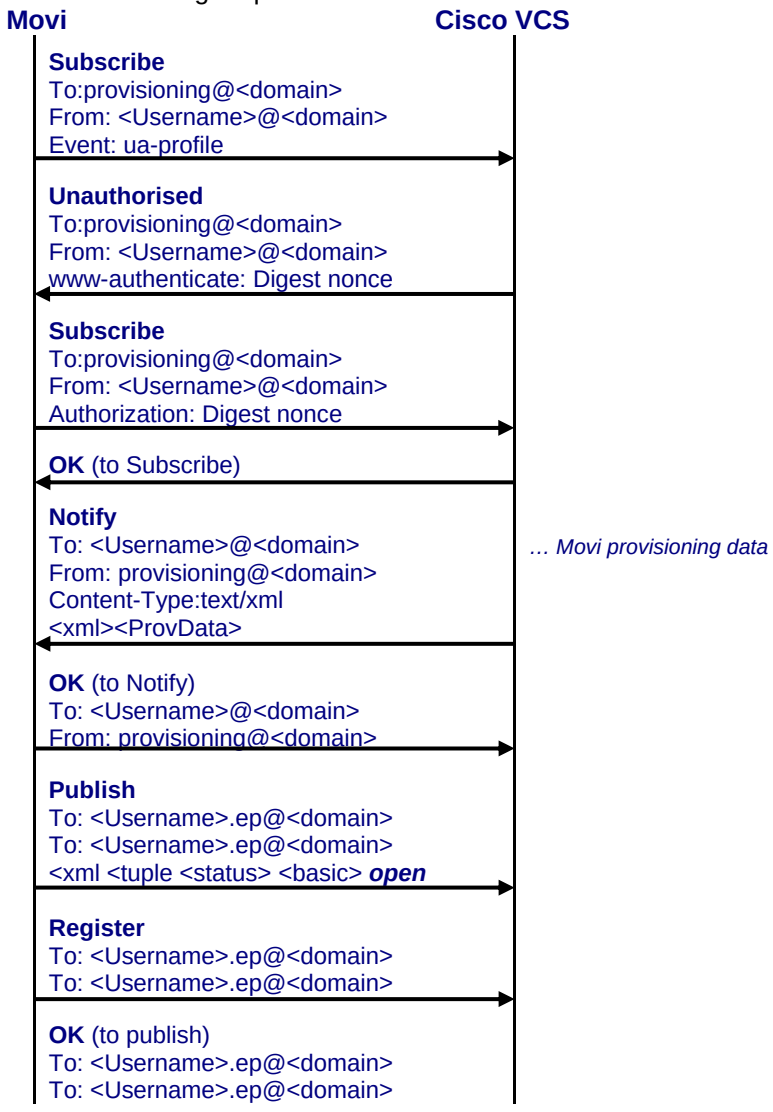
All available licenses may already be in use. Check the call licenses used on the VCS **Overview** page.

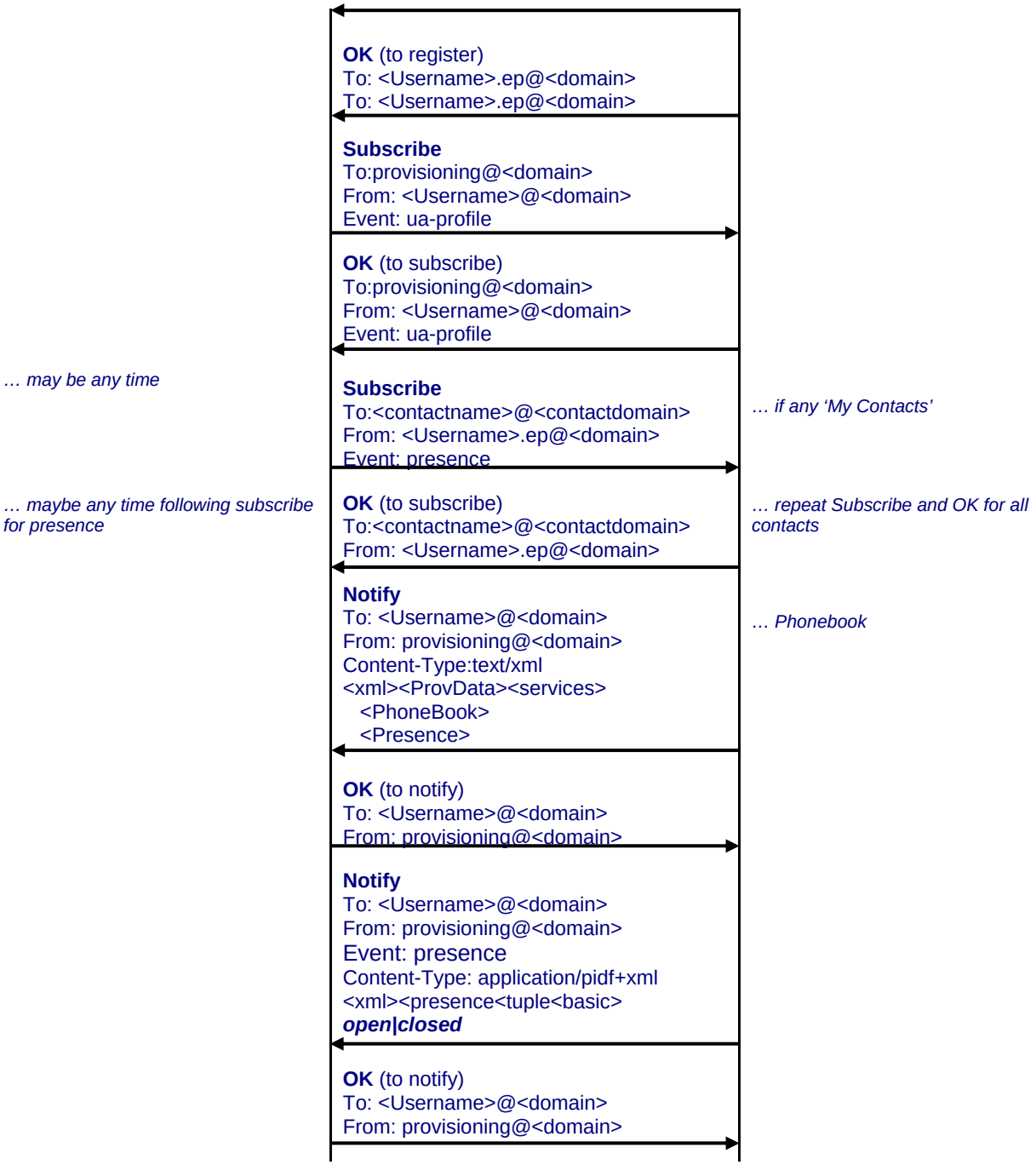
Signaling level troubleshooting

Troubleshooting is usually best carried out in the first instance by taking a Wireshark (a free, open-source packet analyzer) trace on the PC running Movi.

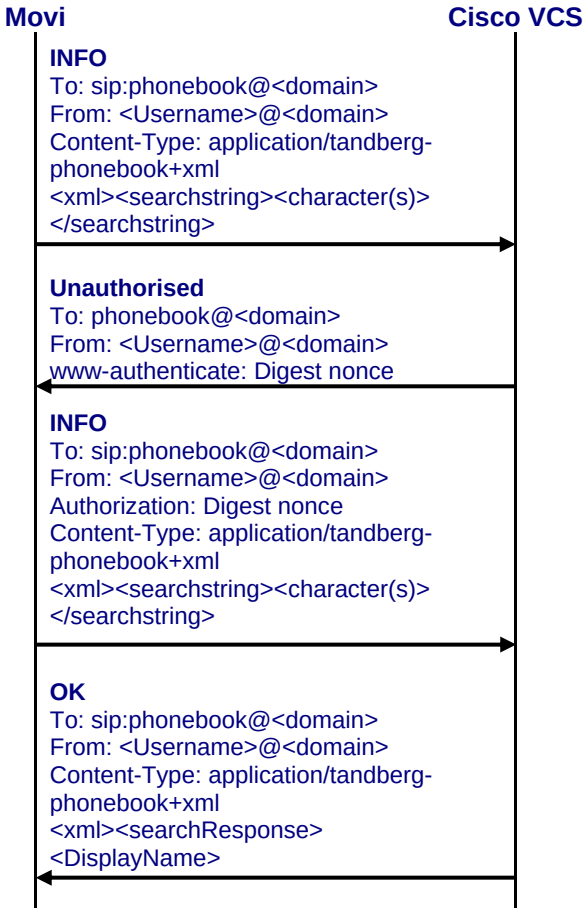
Note: If Movi has Auto or TLS transport selected, sign out of Movi, go to the **Advanced** page and reconfigure Movi to use TCP. Using TLS causes messages to be encrypted and not decodable.

On the Wireshark trace check that the following sequence is observed:




OK (to register)
To: <Username>.ep@<domain>
To: <Username>.ep@<domain>
Subscribe
To:provisioning@<domain>
From: <Username>@<domain>
Event: ua-profile
OK (to subscribe)
To:provisioning@<domain>
From: <Username>@<domain>
Event: ua-profile
… may be any time
Subscribe
To:<contactname>@<contactdomain>
From: <Username>.ep@<domain>
Event: presence
… if any 'My Contacts'
… maybe any time following subscribe for presence
OK (to subscribe)
To:<contactname>@<contactdomain>
From: <Username>.ep@<domain>
… repeat Subscribe and OK for all contacts
Notify
To: <Username>@<domain>
From: provisioning@<domain>
Content-Type:text/xml
<xml><ProvData><services>
<PhoneBook>
<Presence>
… Phonebook
OK (to notify)
To: <Username>@<domain>
From: provisioning@<domain>
Notify
To: <Username>@<domain>
From: provisioning@<domain>
Event: presence
Content-Type: application/pidf+xml
<xml><presence<tuple<basic>
open|closed
OK (to notify)
To: <Username>@<domain>
From: provisioning@<domain>

When Movi looks for phone book information the message flow is:



As more characters are typed in Movi's **Type name, number or address** field, further INFO messages (with Authorization header) are sent with more searchstring characters specified. For each INFO message an OK comes back with the first 10 phone book entries that match that searchstring.

Note: Note 401 Unauthorized or 407 Proxy authentication required may extend the trace.

- **Failure to get any response to the initial subscribe**: the wrong Internal VCS / External VCS values may have been configured (or DNS is wrongly converting the name to IP address).
- **401 Unauthorized for a second time to the initial subscribe**: the Username / Password credentials on Movi do not match those configured in the authentication page of Cisco VCS.
- **No OK to Register**: check that the SIP domain configured in Movi matches the SIP domain configured on Cisco VCS
  - check that Allow and Deny lists are not blocking this registration
  - check the VCS Event Log (**Status > Logs > Event Log**)

Appendix 3 – Comparison of Cisco VCS Expressway Starter Pack provisioning and Cisco TMS provisioning

	Cisco VCS Expressway Starter Pack Provisioning	Cisco VCS with Cisco TMS Provisioning and Management
Movi provisioning	✓	✓
E20 provisioning	×	✓
Architecture	Centralized	Centralized/Distributed
Registrations	50	2500 per Cisco VCS
Cluster support	×	✓
Failover	×	✓
No of concurrent calls	5	Up to 500 non-traversal and 100 traversal calls per Cisco VCS
Registration capacity	50	2,500 per Cisco VCS, 10,000 per Cluster
Presence server	50 registrations	10,000 registrations
Interworking gateway	×	✓
FindMe™	50 users	Optional
Group FindMe™	×	✓
Multiway support	×	✓
SIP support	✓	✓
ICE support	×	✓
Provisioning of Movi	Basic	Advanced
Cisco TMS management	×	✓
AD import of user details	×	✓
Individual settings per user (bandwidth, phone books, encryption setting)	×	✓ (Global, Group and/or User)
Phonebooks	Local only	✓
Multiple user groups	×	✓
Reporting	×	✓
Scheduling and booking	×	✓
Endpoint management	×	✓
Automatic Movi Software update alert	×	✓

Appendix 4 – Known limitations

Modifying a user's display name

Any change to a user account **Display name** is immediately reflected in phone books and the display name returned in FindMe searches.

However, the caller ID display name in SIP messaging is only updated after the relevant Movi is re-provisioned (for example, after signing out and signing back in again).

Appendix 5 – Characters allowed in SIP URIs

The following character set is allowed in SIP URIs (further details may be found in RFC 3261):

```
a-z / A-Z / 0-9 / "-" / "_" / "." / "!" / "~" / "*" / "'"/ "(" / ")" "&" /
"=" / "+" / "$" / "," / ";" / "?" / "/"
```

If other characters are needed they must be “escaped” using "%" HexDigit HexDigit

where HexDigit HexDigit is the ASCII value for the required character.

e.g. steve%20hight@company.com - %20 is the space character

Appendix 6 – Determining the FindMe ID for a caller

Cisco VCS can only overwrite the Caller ID with a FindMe ID if:

- the call signaling passes through the Cisco VCS / Cisco VCS cluster where the FindMe data is held
- the Cisco VCS can identify a FindMe as the owner of the endpoint caller ID

If either of these conditions are not met, the incoming caller ID will be passed through unchanged.

The Cisco VCS identifies a FindMe as the owner of the endpoint caller ID if the incoming caller ID provided in the call:

- matches a FindMe device which is only found in a single FindMe account

or

- matches a single principal FindMe device (if the same device address is associated with more than one FindMe profile)

Note:

Principal devices are designed to be key devices for the user who owns them:

- A device is identified as a principal device if it is the initially configured device for the FindMe created on Cisco VCS, or the device is a FindMe device created by Cisco TMS.
- A principal device may not be deleted from the list of FindMe devices in an account – first it must have its principal device status unset on the **Edit principal devices** page (**Maintenance > Login accounts > User accounts**, select an account, then select **Edit principal devices**).