Cisco VCS Expressway Starter Pack

Deployment Guide

Cisco VCS X6.1

D14618.03

November 2011

Contents

Introduction 4

Purpose of this guide 4
Related documents 5

Configuring the Cisco VCS 6

Firewall ports 6
Check option key 6
Configure the routable address of the Cisco VCS 7
Ensure that Cisco VCS has a SIP domain configured 7
Enable FindMe 8
Configure device authentication 8
Enable presence server (optional) 10
Create user accounts 10
Create authentication credentials for the user 12
Configure bandwidths provisioned to Movi and other endpoints (optional) 12

Installing and configuring Movi 14

Making calls 15

Testing the Cisco VCS Expressway Starter Pack installation 16

Local system testing 16
Public network testing 16
Behind home, small business or hotel firewall testing 17

Appendix 1 – Basic Cisco VCS configuration 18

Appendix 2 – Troubleshooting 19

Movi sign in messaging 19
Login failed – Wrong username, domain, and / or password 19
Login failed – Out of licenses 19
Login failed – The server did not respond in time 19
Login failed – Could not find server in DNS 20
Login failed – Unable to connect to server 20
Call failed – The user could not be found. The user is offline or does not exist. 20
Call failed – The user could not be found 20
Call failed – The user could not be reached. Please try again later. 20
Call failed – An error was received from the server 21
Call failed – Not enough call licenses 21
Phone book searches do not return any entries 21
Failed to update presence 21
Signaling level troubleshooting 21

Appendix 3 – Comparison of Starter Pack provisioning and Cisco TMS provisioning 24

Appendix 4 – Known limitations 25

Modifying a user's display name 25

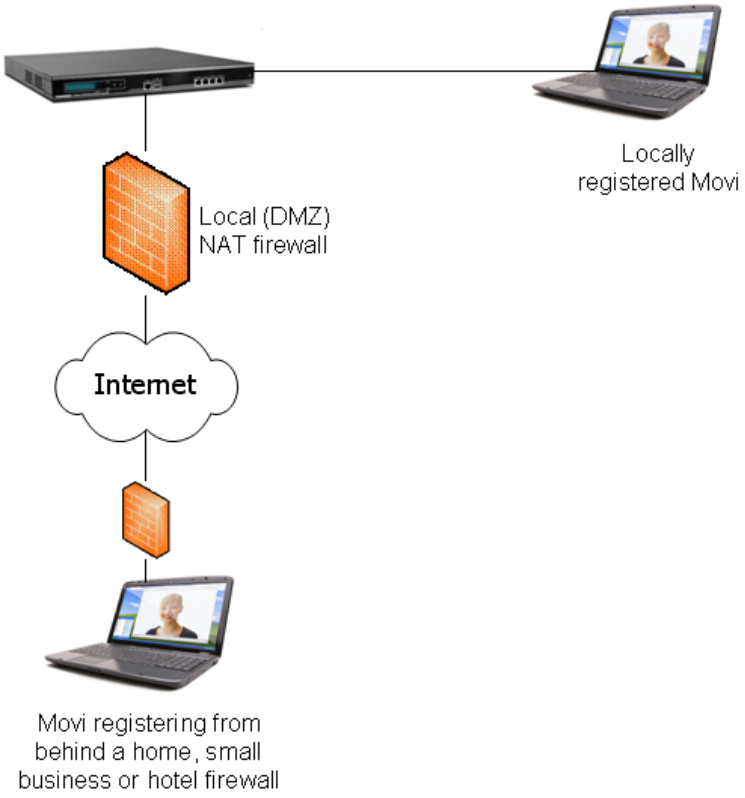
Appendix 5 – Characters allowed in SIP URIs 26

Appendix 6 – Determining the FindMe ID for a caller 27

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 endpoint devices, such as Movi.

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.

You must ensure that sufficient bandwidth is available when making calls through firewalls and other infrastructure. For example, five 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, device authentication 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 are 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.

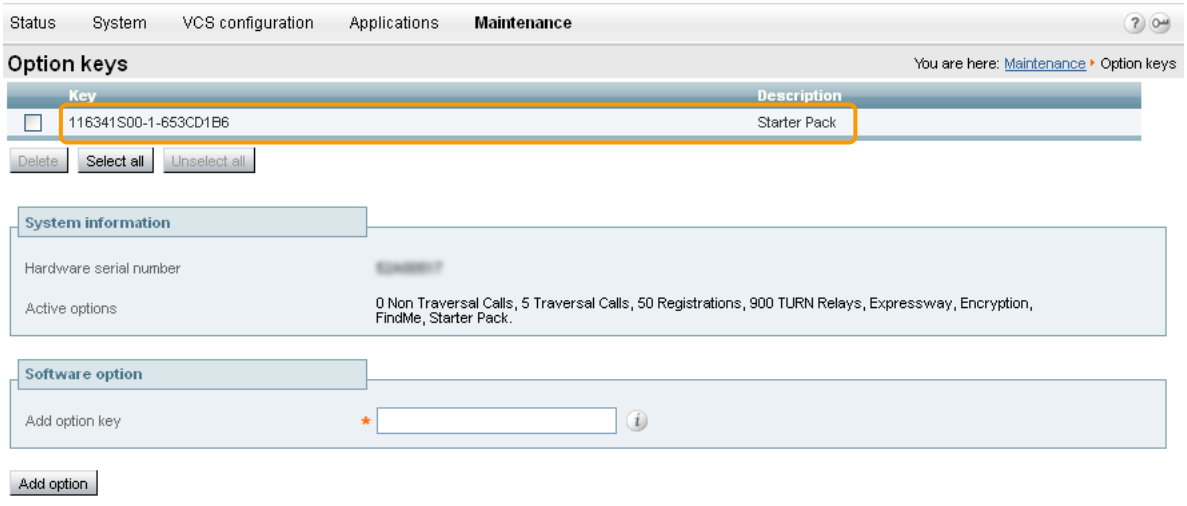
Firewall ports

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

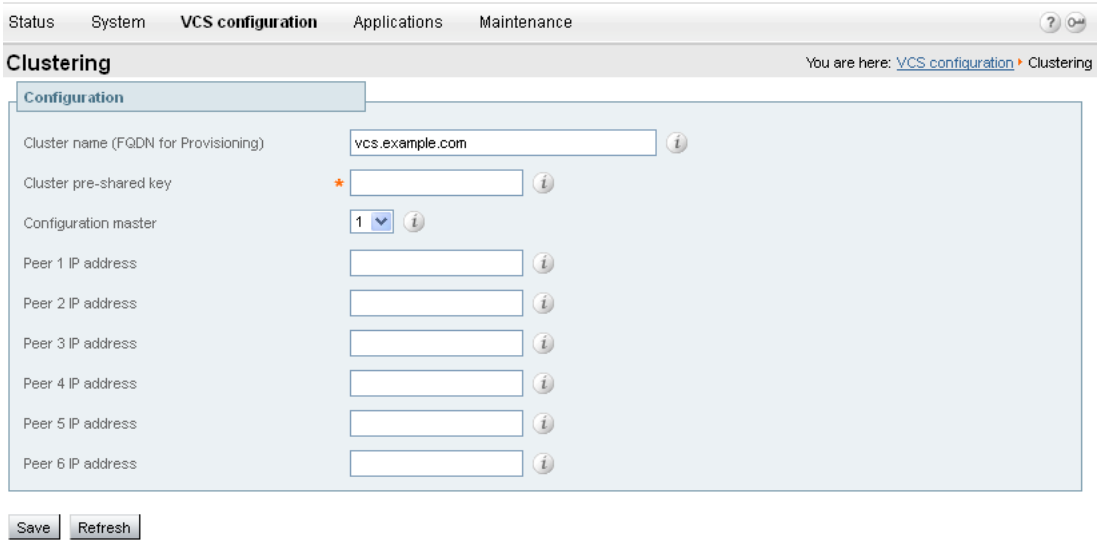
The routable address of the Cisco VCS (its FQDN) is the address supplied by the provisioning system to the provisioned device for it to use as its SIP registrar (the address to which it sends registration requests).

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**.

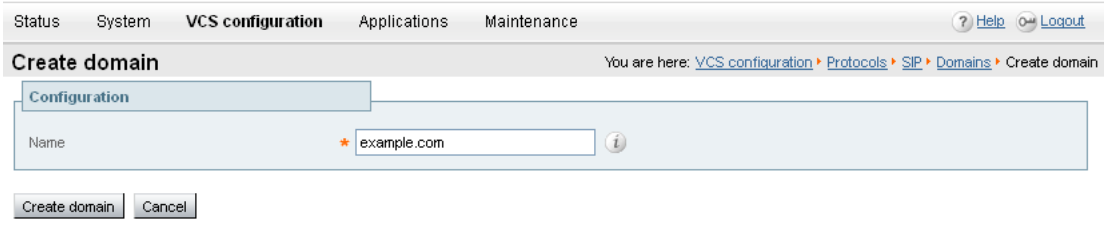


Ensure that Cisco VCS has a SIP domain configured

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, for example, example.com

3. Click **Create domain**.

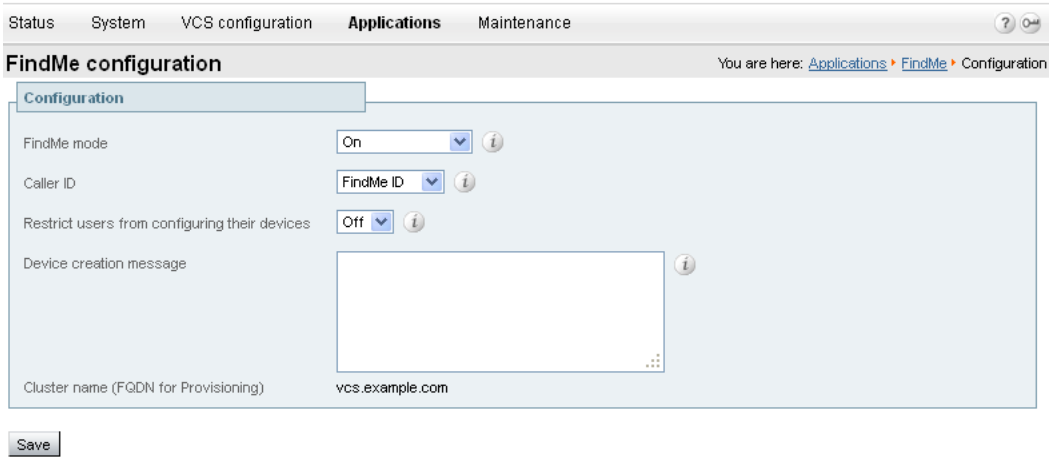


Enable FindMe

1. Go to the **FindMe configuration** page (**Applications > FindMe > Configuration**).
2. Configure the fields as follows:

FindMe mode	*On*
Caller ID	*FindMe ID*: the caller ID of a call being made through this Cisco VCS is replaced with the relevant FindMe ID.
Restrict users from configuring their devices	Controls if users are restricted from adding, deleting or modifying their own devices. The default is *Off*. By default FindMe users are allowed to configure further devices in addition to any principal or provisioned devices assigned to them by the system administrator. This setting can be used to stop users from adding their own devices and restrict them to being able to only maintain their locations and their associated devices.
Device creation message	Only visible when **FindMe mode** is *On*. The text entered here is displayed to users when they add a device to their FindMe configuration. A limited set of HTML markup is supported in the message which is previewed in the window at the bottom of the page when you click **Save**. Refer to the online help for more information on the tags supported. An example message might be: `Phone numbers: use the prefix <b>9</b>`

3. Click **Save**.



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.

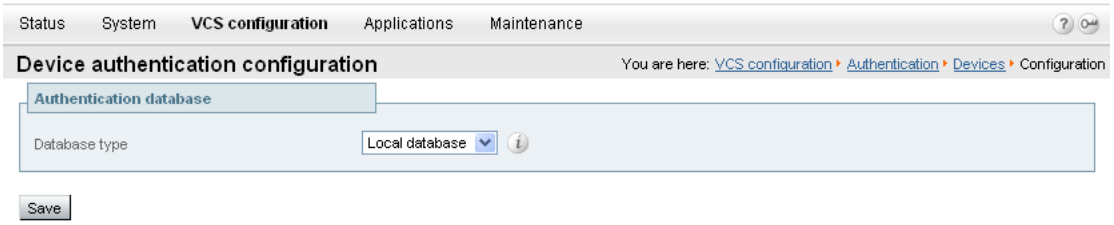
Configure device authentication

You are recommended to use device authentication – verifying that endpoints can identify themselves with a username and password known to the Cisco VCS.

Configure the authentication database

The authentication database setting determines which credential store is used by the Cisco VCS to check the credentials presented by the endpoint.

1. Go to the **Device authentication configuration** page (**VCS configuration > Authentication > Devices > Configuration**).
2. Configure the **Database type** to *Local database*.
3. Click **Save**.

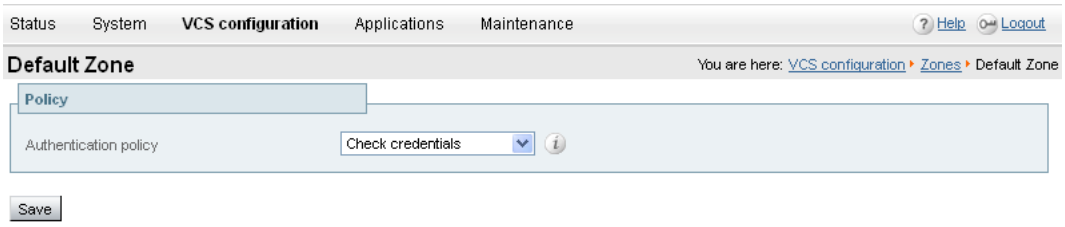


When *Local database* is selected, the appropriate prompts are given to set up the user's endpoint authentication credentials when configuring user accounts.

Configure the Default Zone to check credentials

This ensures that the Cisco VCS checks the credentials of provisioning requests, and call requests from unregistered endpoints.

1. Go to the **Zones** page (**VCS configuration > Zones**).
2. Click on **DefaultZone** to go to the **Default Zone** page.
3. Configure the **Authentication policy** setting to *Check credentials*.
   - Note that Movi users will not be able to log in if the **Authentication policy** setting is *Do not check credentials*.
4. Click **Save**.

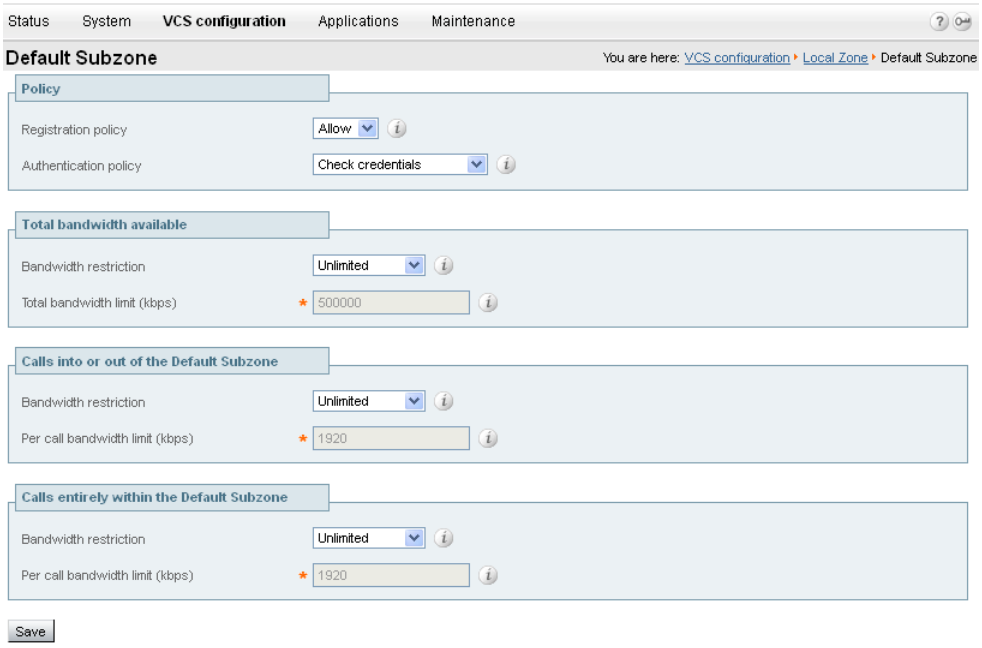


Configure the Default Subzone to check credentials

This ensures that the Cisco VCS checks the credentials of messages received through the Default Subzone. This includes registration requests, phone book requests and presence messages.

1. Go to the **Default Subzone** page (**VCS configuration > Local Zone > Default Subzone**).
2. Configure the **Authentication policy** setting to *Check credentials*.
   - Note that endpoints will not be able to publish presence or use phone books if the **Authentication policy** setting is *Do not check credentials*.
3. Click **Save**.

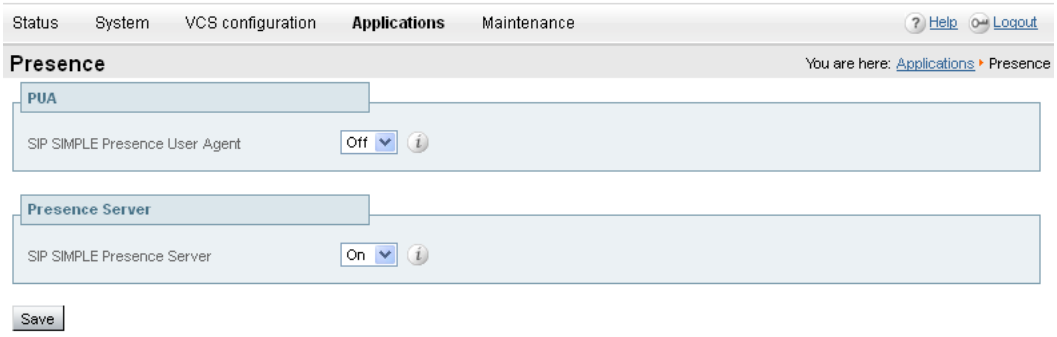
If you configure additional subzones, you are recommended to set the authentication policy of each of those subzones to also check credentials.



Enable presence server (optional)

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

1. Go to the **Presence** page (**Applications > Presence**).
2. Configure **SIP SIMPLE Presence Server** to *On*.
3. Click **Save**.



Create user accounts

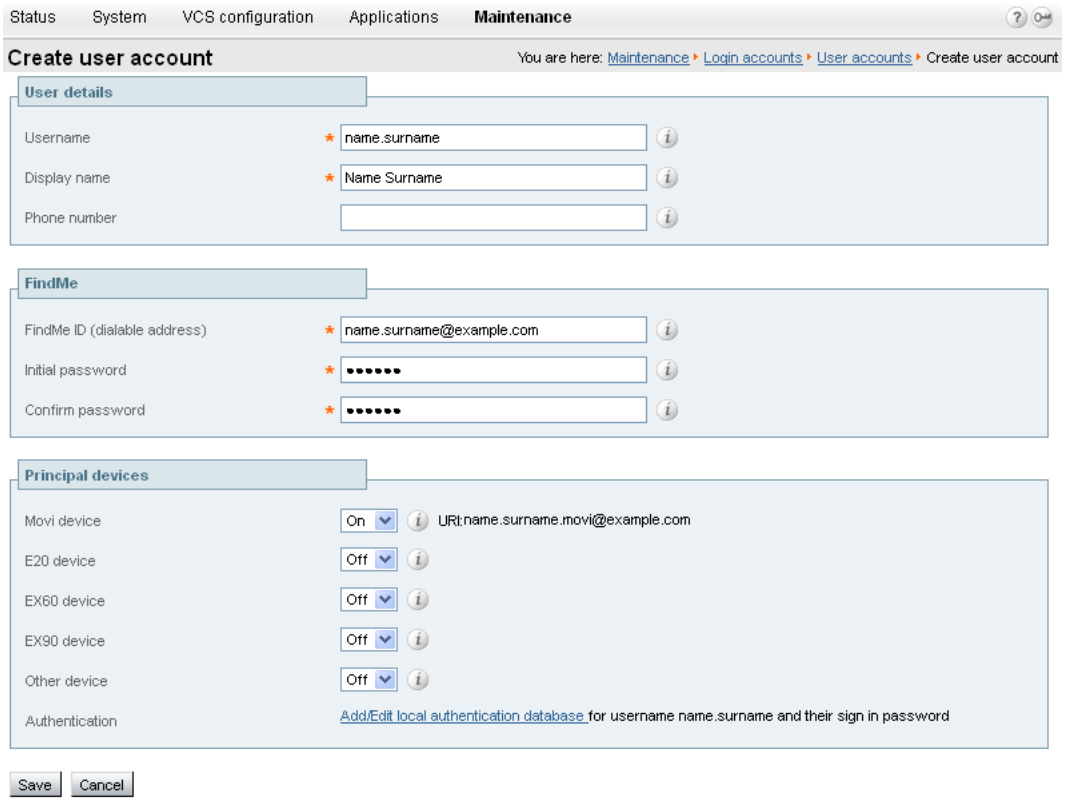
You must configure an account for each user:

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

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. If calls may be placed to an ISDN gateway, ensure that the format of this phone number matches the requirements of the ISDN provider.
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@example.com.
Initial and **Confirm password**	The password to log into the user's account on the Cisco VCS. The password entries are only displayed if **User authentication source** is set to *Local* (see "Enable FindMe™" on page 8.)
Principal devices	This section identifies the principal devices that can be provisioned for this user. These are also the devices that can be called when somebody dials the user's FindMe ID. Select (set to *On*) all of the device types that apply to this user. The URI of each selected device is generated automatically based on a combination of the **Username**, **FindMe ID** and device type. It takes the format <username>.<device type>@<domain portion of FindMe ID>. You can also specify the URI of an additional **Other device**, such as a cell phone, to include in the user's FindMe.

3. If the device authentication database type (**VCS configuration > Authentication > Devices > Configuration**) is configured to use the *Local database*, an **Authentication** field is displayed with a link to the **Local authentication database** page. Click on the link to add or edit the user's credentials in local authentication database. See "Create authentication credentials for the user" below for details.
4. Click **Save.**
5. 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

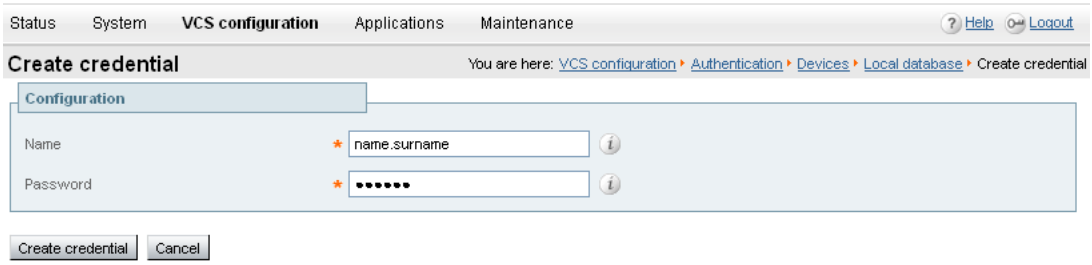
When device authentication has been enabled, the credentials entered into the Cisco VCS's local database must exactly match those used to sign on to Movi – otherwise provisioning requests, registration requests, call requests and phone book requests will be rejected.

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, click on Add/Edit local authentication database. 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 same as the Movi sign in username. All the names must match and are case sensitive.
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.

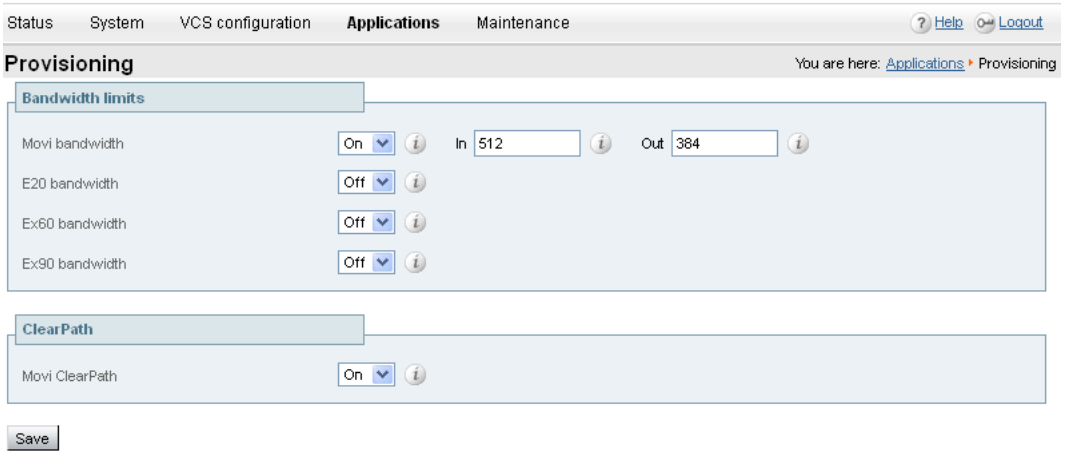


Configure bandwidths provisioned to Movi and other endpoints (optional)

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

1. Go to the **Provisioning** page (**Applications > Provisioning**).
2. Set **Movi bandwidth** to *On*.
   a. Check and set the maximum incoming bandwidth for Movi to, for example, 512kbps.
   b. Check and set the maximum outgoing bandwidth for Movi to, for example, 384kbps.
3. Enable bandwidth provisioning for other device types as required.
4. Set **Movi ClearPath** to *On*.

5. Click **Save**.



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

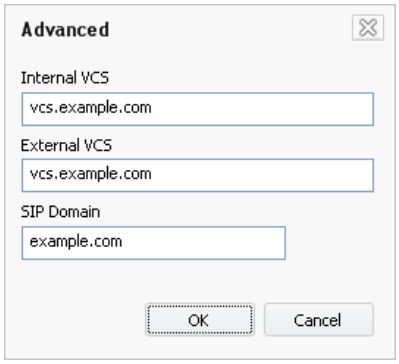
Installing and configuring Movi

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:

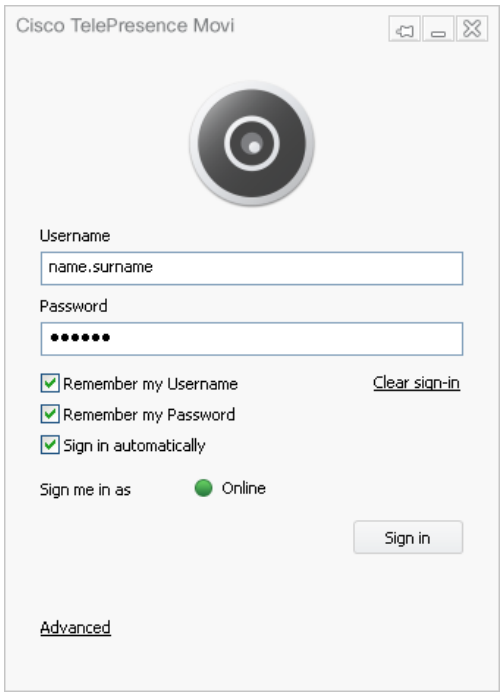
1. Start Movi.
2. Click **Advanced** (at the bottom of the Movi sign-in page).
3. Configure the fields as follows:

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**)



4. Click **OK** to return to the Movi sign in page.
5. Configure the fields as follows:

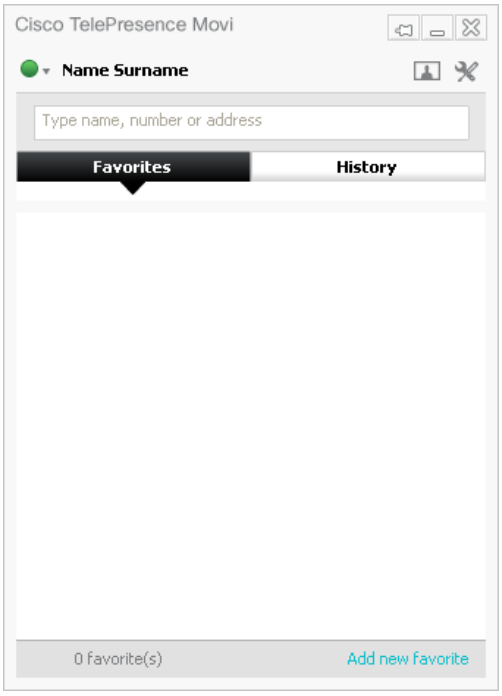
Username	The same username as entered on the Cisco VCS in the **Create user account** page (**Maintenance > Login accounts > User accounts**) and as stored in the local database (**VCS configuration > Authentication > Devices > Local database**).
Password	This must be the same password as the authentication 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, including their associated credentials.
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 > 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 that HTTP is just a redirect to HTTPS; turning off HTTPS will prevent web access to the Cisco VCS.

DNS

1. Go to **System > 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; 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 that <Local host name>.<DNS domain name> = FQDN of this Cisco VCS.

NTP

1. Go to **System > 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 **State** shows Active.

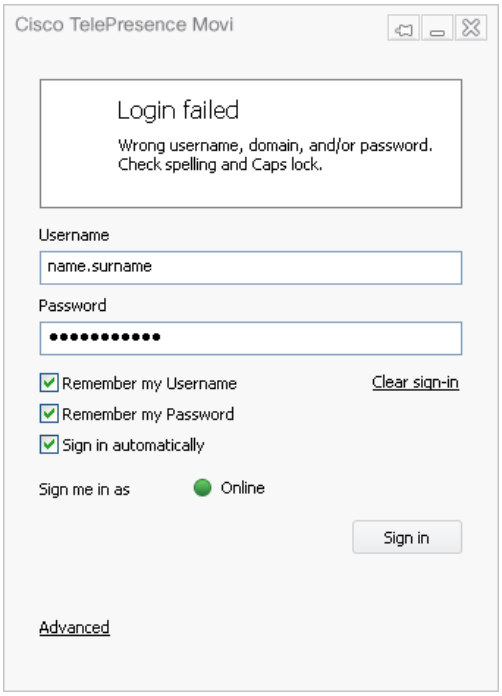
Further information

For further details on the configuration and operation of Cisco VCS, 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. Mistyped 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.
- Check that the Default Zone is configured with an **Authentication policy** of *Check credentials* or *Treat as authenticated*.
  - Movi logins will fail if the **Authentication policy** is *Do not check credentials*.
  - If authentication is set to *Check credentials* (recommended) the appropriate username and password must be configured in the local authentication database.

Login failed – Out of licenses

- Check the number of registered users; a maximum of 50 simultaneous registrations is supported.
- 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 be in use. Check the call licenses usage on the VCS **Overview** page.

Phone book searches do not return any entries

Phone book search requests are rejected if the Default Subzone is configured with an **Authentication policy** of *Do not check credentials*.

- You are recommended to set the Default Subzone authentication to *Check credentials* and configure the appropriate usernames and passwords in the local authentication database.

Failed to update presence

Movi displays a "Failed to update Presence" message if the Default Subzone is configured with an **Authentication policy** of *Do not check credentials*.

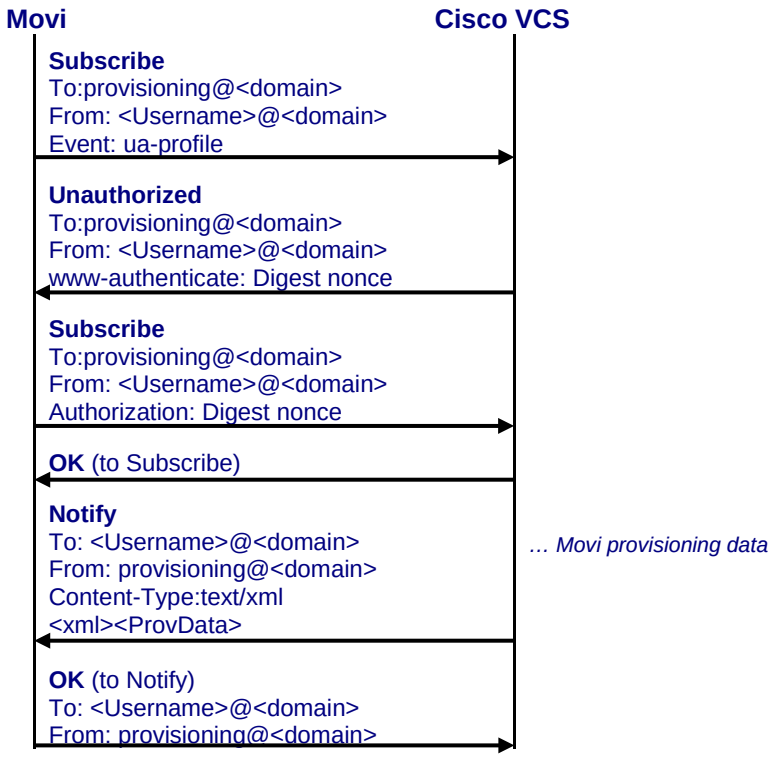
- You are recommended to set the Default Subzone authentication to *Check credentials* and configure the appropriate usernames and passwords in the local authentication database.

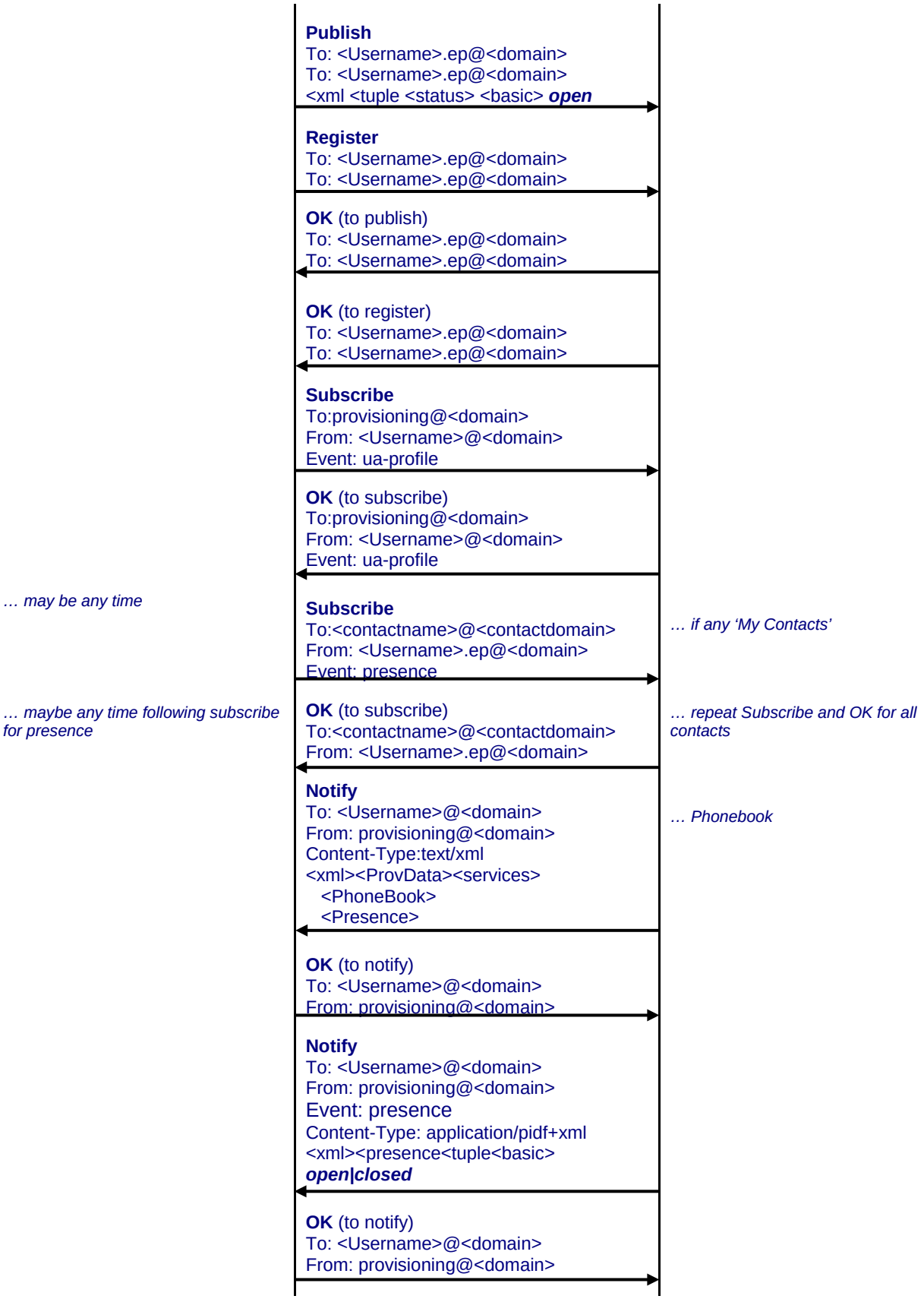
Signaling level troubleshooting

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.

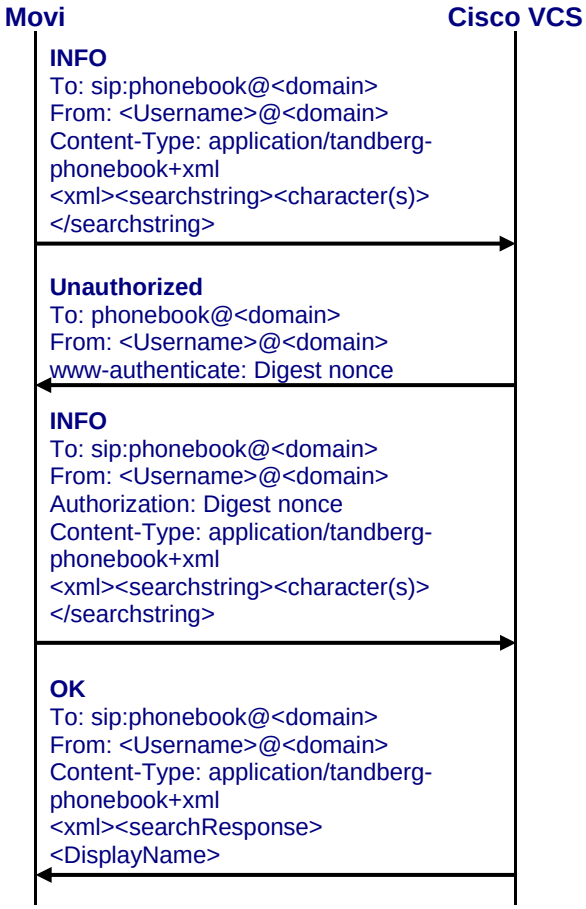
Note, however, that if Movi is communicating over TLS then messages will be encrypted and not decodable. If possible, turn off TLS or use SIP logging.

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




Publish
To: <Username>.ep@<domain>
To: <Username>.ep@<domain>
<xml <tuple <status> <basic> ***open***
Register
To: <Username>.ep@<domain>
To: <Username>.ep@<domain>
OK (to publish)
To: <Username>.ep@<domain>
To: <Username>.ep@<domain>
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 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	✓	✓
Ex60 provisioning	✓	✓
Ex90 provisioning	✓	✓
Architecture	Centralized	Centralized/Distributed
Registrations	50	2500 per Cisco VCS
Cluster support	✗	✓
Failover	✗	✓
No of concurrent calls	5 (but additional call licenses can be added)	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)
Phone books	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.

For example john%20doe@example.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 (or 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)

Principal devices

Note that principal devices are designed to be key devices for the user who owns them:

- A device is identified as a principal device if it has been configured by the Cisco VCS administrator in the **Principal devices** section of the user account page (**Maintenance > Login accounts > User accounts**, then select or create an account).
- Users cannot delete principal devices from the list of FindMe devices in an account.

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.

© 2011 Cisco Systems, Inc. All rights reserved.