



# **VCS cluster creation and maintenance**

## **Deployment Guide**

---

**Cisco VCS X7.2**  
**Cisco TMS 12.6 or later**

D14367.15

November 2012

# Contents

<b>Introduction .....</b>	<b>5</b>
<b>Prerequisites .....</b>	<b>7</b>
<b>Upgrade an X6.0, X6.1, X7.0 or X7.0.n or X7.1 cluster to an X7.2 cluster .....</b>	<b>8</b>
Before the upgrade .....	8
Upgrade VCS cluster peers to X7.2 .....	8
Upgrade the Master peer .....	8
Upgrade non-master peers .....	11
After all the cluster peers have been upgraded .....	12
After the upgrade .....	13
Check cluster status .....	13
<b>Upgrade an X7.1 cluster to an X7.2 cluster (Provisioning Extension mode).....</b>	<b>14</b>
Before the upgrade .....	14
Upgrade VCS cluster peers to X7.2 .....	14
Upgrade the Master peer .....	14
Upgrade non-master peers .....	15
After all the cluster peers have been upgraded check cluster status.....	16
<b>Create a new cluster of VCS X7.2 peers (Provisioning Extension mode – preferred) ...</b>	<b>17</b>
Prerequisites.....	17
Set up the master peer of the cluster .....	17
After the master peer configuration .....	19
Additional cluster configuration .....	19
<b>Create a new cluster of VCS X7.2 peers (TMS Agent legacy mode) .....</b>	<b>20</b>
Prerequisites.....	20
Set up the master peer of the cluster .....	20
After the master peer configuration .....	24
No Cisco TMS .....	24
Additional cluster configuration .....	24
<b>Add an X7.2 VCS to a VCS X7.2 cluster (Provisioning Extension mode) .....</b>	<b>25</b>
Prerequisites.....	25
After adding the VCS peer to the cluster.....	29
Additional cluster configuration .....	29
<b>Add an X7.2 VCS to a VCS X7.2 cluster (TMS Agent legacy mode).....</b>	<b>30</b>
After adding the VCS peer to the cluster.....	35
Additional cluster configuration .....	36
<b>Remove a live VCS from a VCS X7.2 cluster (permanently) .....</b>	<b>37</b>
Reconfigure TMS.....	38
After the removal .....	38
<b>Remove an out-of-service VCS from a VCS X7.2 cluster (permanently) .....</b>	<b>40</b>

Reconfigure TMS.....	41
After the removal .....	41
Before reconnecting the out-of-service VCS back to the network.....	41
<b>Disband a VCS X7.2 cluster .....</b>	<b>43</b>
Reconfigure TMS.....	45
<b>Change the master peer of a VCS X7.2 cluster .....</b>	<b>46</b>
Changing the master peer where the old master is or is not accessible.....	46
Reconfigure TMS .....	46
If the old master is not available.....	46
<b>Change the IP address of a VCS X7.2 peer.....</b>	<b>47</b>
<b>Upgrading VCS X5.2 or earlier versions to X7.2.....</b>	<b>48</b>
Upgrade VCS X1 / X2 Alternates to a VCS X7.2 cluster.....	48
Upgrade an X3 / X4 / X5.0 cluster to an X7.2 cluster.....	48
Upgrade an X5.1, X5.1.1 or X5.2 cluster to an X7.2 cluster .....	48
<b>Appendix 1 – Backing up a VCS.....</b>	<b>49</b>
Backing up an X5.0 or later VCS.....	49
<b>Appendix 2 – Adding a VCS to TMS.....</b>	<b>50</b>
<b>Appendix 3 – IP ports and protocols .....</b>	<b>52</b>
IPSEC communications.....	52
<b>Appendix 4 – Impact of clustering on other VCS applications.....</b>	<b>53</b>
Conference Factory (Multiway™).....	53
Microsoft Office Communications Server 2007 (OCS) and Lync Server 2010 .....	53
<b>Appendix 5 – Configuring endpoints to work with a VCS cluster .....</b>	<b>54</b>
H.323 endpoints .....	54
Option 1 – DNS SRV (preferred).....	54
Option 2 – DNS Round-Robin (2nd choice) .....	54
Option 3 – Static IP (least preferred).....	55
SIP endpoints .....	55
Option 1 – SIP Outbound (preferred) .....	55
Option 2 – DNS SRV (2 <sup>nd</sup> choice) .....	56
Option 3 – DNS Round-Robin (3 <sup>rd</sup> choice) .....	56
Option 4 – Static IP (least preferred).....	56
<b>Appendix 6 – Troubleshooting .....</b>	<b>58</b>
Cisco VCS alarms and warnings.....	58
"Cluster name not configured: if FindMe or clustering are in use a cluster name must be defined; see the Clustering section of the VCS Administrator Guide for more information".....	58
"Cluster replication error: <details> manual synchronization of configuration is required" .....	58
"Cluster replication error: the NTP server is unreachable" .....	58
"Cluster replication error: the local VCS does not appear in the list of peers" .....	58
"Cluster replication error: automatic replication of configuration has been temporarily disabled because an upgrade is in progress" .....	59

---

"Invalid clustering configuration: H.323 mode must be turned On - clustering uses H.323 communications between peers" .....	59
"Security alert: the TMS Agent database has the default LDAP password set" .....	59
"Security alert: the TMS Agent database has the default replication password set" .....	59
"VCS database failure: Please contact your Cisco support representative" .....	59
Cisco TMS .....	60
No TMS Agent tabs .....	60
Cisco TMS warnings.....	60
TMS Cluster Diagnostics.....	60
Conference Factory template does not replicate .....	60
VCS's External manager protocol keeps getting set to HTTPS.....	60
My cluster of Cisco VCS Expressways with dual network interfaces is not replicating correctly .....	61
My cluster of Cisco VCS Expressways with static NAT is not replicating correctly .....	61
<b>Appendix 7 – Changing the cluster name (and keeping FindMe accounts).....</b>	<b>62</b>
Provisioning Extension mode .....	62
TMS Agent legacy mode .....	62
<b>Appendix 8 – Cluster name and DNS SRV records.....</b>	<b>63</b>
Endpoints supporting SIP DNS SRV .....	64
Looking up .SRV records.....	65
Web browser checking of DNS SRV settings .....	65
Nslookup.....	66
Dig .....	66
<b>Appendix 9 – NAPTR records.....</b>	<b>67</b>
NAPTR record format.....	67
Looking up NAPTR records.....	68
Looking up an ENUM NAPTR record.....	68
Looking up a domain NAPTR record .....	69
<b>Document revision history .....</b>	<b>70</b>

# Introduction

Cisco TelePresence Video Communication Server (Cisco VCS) clusters are designed to extend the resilience and capacity of a Cisco VCS installation. VCS peers in a cluster share bandwidth usage as well as routing, zone, FindMe™ and other configuration amongst themselves. Endpoints can register to any of the peers in the cluster; if they lose connection to their initial peer, they can re-register to another peer in the cluster.

Call licensing is carried out on a per-cluster basis. Any traversal or non-traversal call licenses that have been installed on a cluster peer are available for use by any peer within the cluster. If a cluster peer becomes unavailable, the call licenses installed on that peer will remain available to the rest of the cluster peers for two weeks from the time the cluster lost contact with the peer. This will maintain the overall license capacity of the cluster — however, note that each peer is limited by its physical capacity (500 non-traversal calls and 100 traversal calls).

Every VCS peer in the cluster must have the same routing capabilities — if any VCS can route a call to a destination it is assumed that all VCS peers in that cluster can route a call to that destination. If the routing is different on different VCS peers, then separate VCSs / VCS clusters must be used.

This deployment guide describes how to create, modify and upgrade to X7.2 VCS clusters. It provides information on how to:

- Upgrade an X6.0, X6.1, X7.0 or X7.0.n or X7.1 cluster to an X7.2 cluster
- Upgrade an X7.1 cluster to an X7.2 cluster (Provisioning Extension mode)
- Create a new cluster of VCS X7.2 peers (Provisioning Extension mode – preferred)
- Create a new cluster of VCS X7.2 peers (TMS Agent legacy mode)
- Add an X7.2 VCS to a VCS X7.2 cluster (Provisioning Extension mode)
- Add an X7.2 VCS to a VCS X7.2 cluster (TMS Agent legacy mode)
- Remove a live VCS from a VCS X7.2 cluster (permanently)
- Remove an out-of-service VCS from a VCS X7.2 cluster (permanently)
- Disband a VCS X7.2 cluster
- Change the master peer of a VCS X7.2 cluster
- Change the IP address of a VCS X7.2 peer
- Upgrading VCS X5.2 or earlier versions to X7.2

---

**Note:**

In X5.x, X6.x, X7.0.n, X7.1 and X7.2 in TMS Agent Legacy mode, TMS is involved in initiating the environment for FindMe replication. Although not needed to replicate FindMe data throughout the cluster in a running environment, TMS is required to perform the initial distribution of the FindMe data throughout the cluster. TMS is also required if provisioning is to be supported on VCSs.

X7.1 or later in Provisioning Extension mode: TMS is required if FindMe configuration is to be sourced from TMS and also if endpoints are to be provisioned. TMS is not needed to set up cluster, and FindMe can be configured locally on the VCS cluster if required. (If FindMe is stored locally on the VCS cluster and not sourced by TMS, there is no way at a later date to move that FindMe information to TMS.)

---

**Note:** Enabling provisioning and creating a cluster are two separate processes. If you intend to enable provisioning on your cluster, either:

- ▶ follow the instructions in this guide to create the cluster of VCSs (without provisioning enabled), and then follow the instructions in *Cisco TMS Provisioning Deployment Guide* to enable provisioning across the cluster, or
  - ▶ follow the instructions in *Cisco TMS Provisioning Deployment Guide* to enable provisioning on what will be the Master VCS, and then follow the instructions in this guide to create the cluster of VCSs
- 

For creating, modifying, and troubleshooting clusters that will remain X7.0.n / X6.1 / X6.0 / X5 / X4.3 / X4.1 clusters, see:

- Cisco VCS Cluster Creation and Maintenance Deployment Guide (X7.0.n)
- Cisco VCS Cluster Creation and Maintenance Deployment Guide (X6.1)
- Cisco VCS deployment guide - Cluster creation and maintenance (X6)
- Cisco VCS deployment guide - Cluster creation and maintenance (X5)
- TANDBERG VCS deployment guide - Cluster creation and maintenance (VCS X4.3)
- TANDBERG VCS deployment guide - Cluster creation and maintenance (VCS X4.1)

## Prerequisites

VCS clusters peers must all run the same version of code, for example all X7.2, all X7.0.2 or all X6.1. The only occasion where different peers should be allowed to run different versions of code is for the short period of time while a cluster is being upgraded from one version of code to another.

Before setting up a cluster of X7.2 VCS peers or adding an X7.2 VCS to a cluster, ensure that:

- a DNS SRV record is available for the cluster which contains A or AAA records for each peer of the cluster
- each and every VCS peer in a cluster is within a 15ms hop (30ms round trip delay) of each and every other VCS in or to be added to the cluster
- each and every VCS peer in a cluster must be directly routable to each and every other VCS in or to be added to the cluster. (There must be no NAT between cluster peers – if there is a firewall ensure that the required ports are opened.)
- all VCS peers have the same set of option keys installed
  - the number of call license keys may be different on different peers; all other license keys must be identical on each peer
  - the VCS must be restarted after installing some option keys in order to fully activate them
- the Cisco TMS version being run is TMS 12.6 or later (TMS 13.2 or later is required if using Provision Extension mode)
- each VCS has a different system name
- H.323 mode is enabled on each VCS ([VCS configuration > Protocols > H.323](#), and for H.323 mode select On) – H.323 communications are used between cluster peers
- the VCS cluster has a DNS SRV record that defines all cluster peers
- the DNS servers used by the VCS peers must support both forward and reverse DNS lookups of TMS and all VCS peer addresses; the DNS servers must also provide address lookup for any other DNS functionality required (for example: system servers like NTP and the external manager that are configured using DNS names, Microsoft OCS/Lync Server FQDN lookup, LDAP server forward and reverse lookup); note that reverse lookups are frequently provided through PTR records
- If TMS is to be used for replicating FindMe and/or Provisioning data, ensure that TMS Agent Legacy mode or Provisioning Extension mode functionality has been enabled on TMS (see *TMS provisioning deployment guide* for details).

# Upgrade an X6.0, X6.1, X7.0 or X7.0.n or X7.1 cluster to an X7.2 cluster

This procedure assumes that TMS, if used, is already running version 12.6 or later software and is operational with the X6.0, X6.1, X7.0.n or X7.1 cluster.

If TMS replication is enabled, the cluster will be upgraded to a state where it remains running TMS Agent Legacy mode. To change to running Provisioning Extension mode, after this upgrade of the cluster to X7.2, perform the steps in *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide*.

---

**Note:**

- ▶ Use of TMS is required if Device Provisioning or FindMe is to be used with this cluster.
  - ▶ If the VCS is downgraded back to X6.0 or earlier from X6.1 or later, or to X7.0.n or earlier from X7.1 or later, even after restoring the relevant backup the VCSs will require re-clustering as the technique for sharing configuration data changes in both X6.1 and X7.1.
- 

## Before the upgrade

For each VCS peer (including the Master):

1. Check the **Alarms** page (**Status > Alarms**) and ensure that all alarms are acted upon and cleared.

If TMS is being used, verify the correct operation of TMS Agent by running TMS agent diagnostics as follows:

1. Log into TMS.
2. Go to **Administrative Tools > TMS Agent Diagnostics**.
3. In the **TMS Agent Browser** panel on the left side of the page, select **Local TMS Agent**.
4. Click **Run All Diagnoses** to run the diagnostic tests on the Local TMS Agent.
5. For each VCS peer:
  - a. In the **TMS Agent Browser** panel on the left side of the page, expand the Clustered VCSs folder and cluster folder and select the VCS peer.
  - b. Click **Run All Diagnoses** to run the diagnostic tests on the VCS peer.

---

**Note:** If device authentication is intentionally enabled on the VCS, ignore the warning 'verify that authentication is disabled on the VCS'

---

- If all tests are successful (all green check marks), proceed with the instructions below.
- If any errors are found (a red 'X' will appear against failing tests), do not proceed further with this upgrade, but contact your Cisco Authorized Service Provider for further assistance to resolve the issues identified first.

## Upgrade VCS cluster peers to X7.2

### Upgrade the Master peer

For the Master peer in the cluster:

1. Backup the VCS:



- a. If the VCS being backed up is version X.61: log in as root on an SSH or other CLI interface. At the VCS command prompt, type:  
`mkdir /tandberg/persistent/oti`  
`mkdir /tandberg/persistent/management`
- b. Then perform a backup as described in “Appendix 1 – Backing up a VCS”.

---

**Note:** You should backup your system before upgrading. If at a later date you need to downgrade to an earlier version, to restore the configuration you will need to restore a backup made against that previous release.

---

2. Log in to the Master peer as admin via SSH or other CLI interface. Enable maintenance mode. This will stop the Master peer processing any new calls (existing calls will not be dropped until a restart; other cluster peers will continue processing calls). Log in as admin on an SSH or other CLI interface. At the VCS command line type:  
`xconfiguration SystemUnit Maintenance Mode: On`
3. Log in to the Master peer as admin on the web interface.
4. Wait for all calls to clear and registrations to timeout on this master peer.  
 If necessary, manually remove any calls on this peer that do not clear automatically (using the web browser go to **Status > Calls**, then select the check box next to the calls you want to terminate and click **Disconnect**).
5. If necessary, manually remove any registrations from this peer that do not clear automatically (using the web browser go to **Status > Registrations > By device**, then select the check box next to the devices you want to remove and click **Unregister**).  
 You can leave the registration for the Conference Factory – this will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own Conference Factory registration (if enabled).
6. If TMS Agent Data Replication is enabled on TMS (for FindMe or Device Provisioning replication), then on **Cisco TMS**:
  - a. Select **Systems > Navigator** (and any required sub folders), then click on the Master VCS of the cluster.
  - b. Select the **Clustering** tab.
  - c. Ensure that all expected peers are shown in the **Cluster Peers** list.
  - d. Clear the **Enable TMS Agent Data Replication on all Cluster Peers** check box.
  - e. Click **Save Cluster Settings**.
  - f. Review the status shown in **Administrative Tools > Activity Status** to ensure these tasks have completed successfully.

---

**Note:** This disables database replication from TMS to each cluster peer.

---

- ▶ Provisioning data will no longer be updated from TMS to the VCSs, however provisioning of endpoints from data cached on VCSs not in maintenance mode will continue.
  - ▶ VCS cluster configuration replication will continue.
  - ▶ VCS FindMe replication among VCS peers will STOP.
- 

On the Master VCS peer web interface:

1. Upgrade and restart the Master VCS (**Maintenance > Upgrade**).  
 For any further details see the "Upgrading Software" section of the VCS Administrator Guide.  
 Note that the web browser interface may timeout during the restart process, after the progress bar has reached the end. This may occur if:
  - VCS carries out a disk file system check – which it does approximately once every 30 restarts

- Provisioning is enabled, and database re-indexing is in progress – this may take up to 30 minutes if there is a large amount of user data

Upgrading of the software on the Master VCS is now complete.

---

**Note:** Do not worry about a “Cluster communication failure” alarm on the Master or any non-master peers – this is expected.

- The upgrade process disables the VCS’s provisioning functionality — provisioning will be restored later when Provisioning is re-enabled.
- 

If TMS is used, ensure that TMS has all the correct settings for this upgraded VCS by forcing a refresh of TMS.

On TMS:

1. Go to **Systems > Navigator** (and any required sub folders) and select the Master VCS.
2. Select the **Settings** tab.
3. Click **Force Refresh**.

If TMS is used and FindMe or Device Provisioning is required, enable replication on this upgraded master VCS peer.

On TMS:

4. Go to **Systems > Navigator** (and any required sub folders) then click on the master VCS.
5. Select the **TMS Agent** tab.
6. Select **Enable TMS Agent Data Replication**.
7. Ensure that **Authentication Scheme** is set to **Digest**.
8. Click **Save Settings**.

---

**Note:** This may take a while to complete (approximately 5 minutes); select the **Activity Status** page (see link at the top of the screen) to show the list of activities that are active, scheduled or in progress. Select the activity **Enable TMS Agent Data Replication for system(s) <name of system>**. This displays an activity log. Refresh this web page (button bottom left of this page) until the Activity Event completed successfully is reported.

- Do not worry about a message “Cluster replication error: cannot find master or this slave’s peer configuration file, manual synchronization of configuration is required” – this is expected while the cluster starts up. It should clear within 10 minutes.
  - Similarly do not worry about TMS warnings and emails about cluster problems created during this upgrade.
- 

On the Master VCS peer:

1. Check that the expected FindMe entries still exist on this master VCS (**Maintenance > Login accounts > User accounts**).
2. Check that other configuration (including zone configuration, transforms and other configuration for items from the System, VCS Configuration and Application menus) is as expected.
3. Backup the master VCS (See “Appendix 1 – Backing up a VCS” for details).

---

**Note:** It is recommended that while VCS peers are running different versions of code, configuration changes to any VCS in the cluster are limited to the changes needed to complete the upgrade. Configuration changes will not be replicated across VCS peers that are not running the same version of software as the master VCS.

---

## Upgrade non-master peers

---

**Note:** Do not worry about a “Cluster communication failure” alarm – this is expected.

---

For each non-master peer in the cluster:

1. Backup the VCS:
  - a. If the VCS being backed up is version X6.1: log in as root on an SSH or other CLI interface. At the VCS command prompt, type:
 

```
mkdir /tandberg/persistent/oti
mkdir /tandberg/persistent/management
```
  - b. Then perform backup as described in “Appendix 1 – Backing up a VCS”.

---

**Note:** You should backup your system before upgrading. If at a later date you need to downgrade to an earlier version, to restore the configuration you will need to restore a backup made against that previous release.

---

2. Log in to the non-master peer as admin on an SSH or other CLI interface. Enable maintenance mode; from the VCS command line type:
 

```
xconfiguration SystemUnit Maintenance Mode: On
```
3. Log in to the non-master peer as admin on the web interface.
4. Wait for all calls to clear and registrations to timeout on this non-master peer. If necessary, manually remove any calls on this peer that do not clear automatically (using the web browser go to **Status > Calls**, then select the check box next to the calls you want to terminate and click **Disconnect**).
5. If necessary, manually remove any registrations from this peer that do not clear automatically (using the web browser go to **Status > Registrations > By device**, then select the check box next to the devices you want to remove and click **Unregister**). You can leave the registration for the conference factory – this will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own conference factory registration (if enabled).

On the non-master peer:

6. Upgrade and restart the VCS (**Maintenance > Upgrade**). If multiple peers need restarting, restart each peer in turn, waiting for the peer to be accessible through the web interface before restarting the next. For any further details see the "Upgrading Software" section of the VCS Administrator Guide. Note that the web browser interface may timeout during the restart process, after the progress bar has reached the end. This may occur if:
  - VCS carries out a disk file system check – which it does approximately once every 30 restarts
  - Provisioning is enabled, and database re-indexing is in progress – this may take up to 30 minutes if there is a large amount of user data

Upgrading the software on this non-master VCS peer is now complete.

---

**Note:** If TMS is used, the upgrade process disables the VCS's provisioning functionality — provisioning will be restored later when Provisioning is re-enabled.

---

If TMS is used, ensure that TMS has all the correct settings for this upgraded VCS by forcing a refresh of TMS.

On TMS:

1. Go to **Systems > Navigator** (and any required sub folders) and select the Master VCS.
2. Select the **Settings** tab.

### 3. Click **Force Refresh**.

If Cisco TMS is used and FindMe or Device Provisioning is required, enable replication on this upgraded non-master VCS peer.

On TMS:

4. Go to **Systems > Navigator** (and any required sub folders) then click on this non-master VCS.
5. Select the **TMS Agent** tab.
6. Select **Enable TMS Agent Data Replication**.
7. Ensure that **Authentication Scheme** is set to **Digest**.
8. Click **Save Settings**.

---

**Note:** This may take a while to complete (approximately 5 minutes); select the **Activity Status** page (see link at the top of the screen) to show the list of activities that are active, scheduled or in progress. Select the activity **Enable TMS Agent Data Replication for system(s) <name of system>**. This displays an activity log. Refresh this web page (button bottom left of this page) until the Activity Event completed successfully is reported.

- ▶ Do not worry about a message “Cluster replication error: cannot find master or this slave’s peer configuration file, manual synchronization of configuration is required” – this is expected while the cluster starts up. It should clear within 10 minutes.
  - ▶ Similarly do not worry about TMS warnings and emails about cluster problems created during this upgrade.
- 

On this non-master VCS peer:

1. Check the **Alarms** page (**Status > Alarms**) and ensure that all Alarms are acted upon and cleared.
2. Check that the expected FindMe entries exist on this VCS (**Maintenance > Login accounts > User accounts**).
3. Check that other configuration (including zone configuration, transforms and other configuration for items from the System, VCS Configuration and Application menus) is as expected.
4. Repeat these steps for each non-master peer.

## After all the cluster peers have been upgraded

After all cluster peers have been upgraded:

1. If TMS is used and FindMe or Device Provisioning is required, on TMS enable **TMS Agent Data Replication on all Cluster Peers**:
  - a. Go to **Systems > Navigator** (and any required sub folders), then click on the Master VCS of the cluster.
  - b. Select the **Clustering** tab.
  - c. Select **Enable TMS Agent Data Replication on all Cluster Peers**.
  - d. Click **Save Cluster Settings**.

---

**Note:** This may take a while to complete (approximately 5 minutes); select the **Activity Status** page (see link at the top of the screen) to show the list of activities that are active, scheduled or in progress. Select the activity **Enable TMS Agent Data Replication for system(s) <name of system>**. This displays an activity log. Refresh this web page (button bottom left of this page) until the Activity Event completed successfully is reported.

---

## After the upgrade

If TMS is being used, verify the correct operation of TMS Agent by running TMS Agent diagnostics as follows:

1. Log into TMS.
2. Go to **Administrative Tools > TMS Agent Diagnostics**.
3. In the **TMS Agent Browser** panel on the left side of the page, select **Local TMS Agent**.
4. Click **Run All Diagnoses** to run the diagnostic tests on the Local TMS Agent.
5. For each VCS peer:
  - a. In the **TMS Agent Browser** panel on the left side of the page, expand the Clustered VCSs folder and cluster folder and select the VCS peer.
  - b. Click **Run All Diagnoses** to run the diagnostic tests on the VCS peer.

---

**Note:** If device authentication is intentionally enabled on the VCS, ignore the warning 'verify that authentication is disabled on the VCS'

---

- If all tests are successful (all green check marks), proceed with the instructions below.
- If any errors are found (a red 'X' will appear against failing tests), do not proceed further with this upgrade, but contact your Cisco Authorized Service Provider for further assistance to resolve the issues identified.

## Check cluster status

On each VCS (including the master):

1. Go to the **Clustering** page (**VCS Configuration > Clustering**).
  - Cluster database status should show **SUCCEEDED**.
  - VCS system configuration replication status should show **Last synchronization result SUCCEEDED**.
2. If replication with Cisco TMS is enabled:
  - a. Select the link "**View TMS Agent replication status**".
  - b. Check that the top line of the TMS Agent replication status report reports **Replication Enabled**.

Upgrading an X6.0, X6.1 X7.0, X7.0.n or X7.1 cluster to an X7.2 cluster is now complete.

If TMS replication is enabled, the cluster will be running TMS Agent Legacy mode – see *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide* to upgrade from TMS Agent legacy mode to Provisioning Extension mode.

# Upgrade an X7.1 cluster to an X7.2 cluster (Provisioning Extension mode)

This procedure assumes that TMS is already running version 13.2 or later software and is operational with the X7.1 cluster. The VCS cluster and TMS must also be configured and operating using TMS Provisioning Extension mode.

If Provisioning Extension mode is not already operational, upgrade to Provisioning Extension mode, using the steps in *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide* before performing this upgrade.

---

**Note:** If the VCS is downgraded back to X6.0 or earlier from X6.1 or later, or to X7.0.n or earlier from X7.1 or later, even after restoring the relevant backup the VCSs will require re-clustering as the technique for sharing configuration data changes in both X6.1 and X7.1.

---

## Before the upgrade

For each VCS peer (including the Master):

1. Check the **Alarms** page (**Status > Alarms**) and ensure that all alarms are acted upon and cleared.

## Upgrade VCS cluster peers to X7.2

### Upgrade the Master peer

For the Master peer in the cluster:

1. Backup the VCS:
  - a. Details of how to perform a backup are described in “Appendix 1 – Backing up a VCS”.

---

**Note:** You should backup your system before upgrading. If at a later date you need to downgrade to an earlier version, to restore the configuration you will need to restore a backup made against that previous release.

---

2. On the Master peer, login as admin via SSH or other CLI interface and enable maintenance mode. This will stop the Master peer processing any new calls (existing calls will not be dropped until a restart; other cluster peers will continue processing calls).  
Log in as admin on an SSH or other CLI interface. At the VCS command line type:  
`xconfiguration SystemUnit Maintenance Mode: On`
3. Log in to the Master peer as admin on the web interface.
  - a. Wait for all calls to clear and registrations to timeout on this master peer.  
If necessary, manually remove any calls on this peer that do not clear automatically (using the web browser go to **Status > Calls**, then select the check box next to the calls you want to terminate and click **Disconnect**).
  - b. If necessary, manually remove any registrations from this peer that do not clear automatically (using the web browser go to **Status > Registrations > By device**, then select the check box next to the devices you want to remove and click **Unregister**).  
You can leave the registration for the Conference Factory – this will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own Conference Factory registration (if enabled).

On the Master VCS peer web interface:

1. Upgrade and restart the Master VCS (**Maintenance > Upgrade**).  
For any further details see the "Upgrading Software" section of the VCS Administrator Guide.  
Note that the web browser interface may timeout during the restart process, after the progress bar has reached the end. This may occur if VCS carries out a disk file system check – which it does approximately once every 30 restarts

Upgrading of the software on the Master VCS is now complete.

---

**Note:** Do not worry about cluster-related alarms that occur during the upgrade process, for example

- ▶ "Cluster communication failure" alarm on the Master or any non-master peers – this is expected.
- ▶ "Cluster replication error: cannot find master or this slave's peer configuration file, manual synchronization of configuration is required"

Similarly do not worry about TMS warnings and emails about cluster problems created during this upgrade.

These alarms and warnings are expected and will clear when all cluster peers are upgraded and cluster data synchronization has occurred (they should clear within 10 minutes of the complete upgrade).

---

On the Master VCS peer:

1. Check that the expected FindMe entries still exist on this master VCS (**Status > Applications > TMS Provisioning Extension Services > FindMe > Accounts**).
2. Check that other configuration (including zone configuration, transforms and other configuration for items from the System, VCS Configuration and Application menus) is as expected.
3. Backup the master VCS (See "Appendix 1 – Backing up a VCS" for details).

---

**Note:** It is recommended that while VCS peers are running different versions of code, configuration changes to any VCS in the cluster are limited to the changes needed to complete the upgrade. Configuration changes will not be replicated across VCS peers that are not running the same version of software as the master VCS.

---

## Upgrade non-master peers

---

**Note:** Do not worry about cluster-related alarms that occur during the upgrade process – these are expected.

---

For each non-master peer in the cluster:

1. Backup the VCS:
  - a. Details of how to perform a backup are described in "Appendix 1 – Backing up a VCS".

---

**Note:** You should backup your system before upgrading. If at a later date you need to downgrade to an earlier version, to restore the configuration you will need to restore a backup made against that previous release.

---

2. Log in to the non-master peer as admin on an SSH or other CLI interface. Enable maintenance mode; from the VCS command line type:  
`xconfiguration SystemUnit Maintenance Mode: On`
3. Log in to the non-master peer as admin on the web interface.



- a. Wait for all calls to clear and registrations to timeout on this non-master peer.  
If necessary, manually remove any calls on this peer that do not clear automatically (using the web browser go to **Status > Calls**, then select the check box next to the calls you want to terminate and click **Disconnect**).
- b. If necessary, manually remove any registrations from this peer that do not clear automatically (using the web browser go to **Status > Registrations > By device**, then select the check box next to the devices you want to remove and click **Unregister**).  
You can leave the registration for the conference factory – this will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own conference factory registration (if enabled).

On the non-master peer:

1. Upgrade and restart the VCS (**Maintenance > Upgrade**).  
If multiple peers need restarting, restart each peer in turn, waiting for the previously reset peer to be accessible through the web interface before restarting the next.  
For any further details see the "Upgrading Software" section of the VCS Administrator Guide.  
Note that the web browser interface may timeout during the restart process, after the progress bar has reached the end; this may happen if VCS carries out a disk file system check – which it does approximately once every 30 restarts

Upgrading the software on this non-master VCS peer is now complete.

---

**Note:** Do not worry about cluster-related alarms that occur during the upgrade process, for example

- ▶ "Cluster communication failure" alarm on the Master or any non-master peers – this is expected.
- ▶ "Cluster replication error: cannot find master or this slave's peer configuration file, manual synchronization of configuration is required"

Similarly do not worry about TMS warnings and emails about cluster problems created during this upgrade.

These alarms and warnings are expected and will clear when all cluster peers are upgraded and cluster data synchronization has occurred (they should clear within 10 minutes of the complete upgrade).

---

On this non-master VCS peer:

1. Check the **Alarms** page (**Status > Alarms**) and ensure that all Alarms are acted upon and cleared.
2. Check that the expected FindMe entries exist on this VCS (**Status > Applications > TMS Provisioning Extension Services > FindMe > Accounts**).
3. Check that other configuration (including zone configuration, transforms and other configuration for items from the System, VCS Configuration and Application menus) is as expected.
4. Repeat these steps for each non-master peer.

## After all the cluster peers have been upgraded check cluster status

On each VCS (including the master):

1. Go to the **Clustering** page (**VCS configuration > Clustering**).
  - Cluster database status should show **SUCCEEDED**.
  - VCS system configuration replication status should show **Last synchronization result SUCCEEDED**.

Upgrading an X7.1 cluster to an X7.2 cluster is now complete.



## Create a new cluster of VCS X7.2 peers (Provisioning Extension mode – preferred)

---

**Note:** This procedure will require a period of downtime for the VCS service. Ensure that these instructions are followed in a scheduled maintenance window.

---

This process creates a cluster of a single VCS.

To complete the cluster containing multiple VCSs, when this section is complete, follow the instructions in “Add an X7.2 VCS to a VCS X7.2 cluster (Provisioning Extension mode)” to add the non-master peers to the cluster.

Do not use this section if the cluster already exists; instead, follow the instructions in “Add an X7.2 VCS to a VCS X7.2 cluster (Provisioning Extension mode)”.

---

**Note:** If Device Provisioning is to be used with an X7.2 VCS cluster, then use of TMS is essential. Also if FindMe is to be managed by TMS, then use of TMS is essential. If neither Device Provisioning nor FindMe managed by TMS is to be used, then use of TMS is optional but recommended.

---

### Prerequisites

- If TMS is to be used, it must be version 13.2 or later.
- If Device Provisioning or FindMe are managed by TMS, this VCS and TMS must be operating in Provisioning Extension mode, and this mode proven to be operational.
- All VCSs to be included in the cluster must be running the same version of VCS software, and that version of software must be X7.2.
- If a firewall exists between cluster peers, it must be configured to permit the traffic documented in Appendix 3.

### Set up the master peer of the cluster

This process sets up the first (Master) peer of this new cluster – additional peers are added afterwards using the “Add an X7.2 VCS to a VCS X7.2 cluster (Provisioning Extension mode)” process.

Before proceeding, the VCS that will be the master must be determined.

---

**Note:** The Master VCS will be the source of the configuration information for all VCS peers in the cluster. Non-master VCS peers will have their configuration deleted and replaced by that from the Master.

---

On neighbor Gatekeepers (GKs) and Border Controllers (BCs):

1. If the Master VCS has a traversal zone configured to connect with any GK or BC, upgrade these systems to N6.1 or Q6.1 or later code.

On other VCSs:

1. Check that no other VCS (anywhere) has this VCS's IP address in its Alternates or Clustering Peers list.

On this Master VCS:

1. Check that the VCS is running X7.2 software.
2. Backup the VCS (See Appendix 1 for details).
3. On the web interface of this Master VCS, review the configuration to ensure that the VCS has:
  - A valid Ethernet speed (**System > Ethernet**).

- Valid IP address and IP gateway (**System > IP**).
- The same set of option keys installed as those that will be installed on all other peers of the cluster (**Maintenance > Option Keys**).

---

**Note:** the number of call license keys may be different on different peers; all other license keys must be identical on each peer.

---

- At least one valid DNS server configured, and that if unqualified DNS names are used elsewhere (e.g. for the NTP server), that the correct **Domain name** is also configured (**Domain name** is added as a suffix to an unqualified DNS name to make it into an FQDN) (**System > DNS**).

---

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

---

- A valid and working NTP server configured (**System > Time**; in the Status section, the State should be “**Synchronized**”).
  - No peers configured (**VCS configuration > Clustering** – all Peer x IP address fields on this page should be blank. If not, delete any entries and click **Save**).
4. Ensure that this VCS does not list any of the VCSs that are to be peers in this new cluster in any of its neighbor zones or traversal zones (**VCS configuration > Zones** then check each neighbor and traversal zone).
  5. Set the H.323 **Time to live** to 60 (seconds) so that if a VCS becomes inaccessible to an endpoint, the endpoint will re-register quickly with another peer (**VCS configuration > Protocols > H.323**).
  6. Go to **System > DNS** and ensure that the **Local host name** is the DNS hostname for this VCS (typically the same as the **System name** in **System > System**, but excluding spaces, and unique for each VCS in the cluster); if it is not configured correctly, set it up appropriately and click **Save**.

---

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

---

7. Go to **VCS configuration > Calls** and set **Call routed mode** to *Optimal*.
8. Click **Save**.
9. Enable maintenance mode. Log in as admin on an SSH or other CLI interface. At the VCS command line type:  

```
xconfiguration SystemUnit Maintenance Mode: On
```
10. Wait for all calls to clear and registrations to timeout.  
 If necessary, manually remove any calls that do not clear automatically (using the web browser go to **Status > Calls**, then select the check box next to the calls you want to terminate and click **Disconnect**).
11. If necessary, manually remove any registrations that do not clear automatically (using the web browser go to **Status > Registrations > By device**, then select the check box next to the devices you want to remove and click **Unregister**).  
 You can leave the registration for the Conference Factory – this will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own Conference Factory registration (if enabled).
12. Go to **VCS configuration > Clustering** and:
  - a. Check that **Cluster name** is the routable Fully Qualified Domain Name used in SRV records that address this VCS cluster, for example "cluster1.example.com". (See Appendix 8 – Cluster name and DNS SRV records).
  - b. If it is not, change the **Cluster name**.
13. Click **Save**.
14. On the Clustering page (**VCS configuration > Clustering**) configure the fields as follows:

<b>Configuration master</b>	1
-----------------------------	---

<b>Cluster pre-shared key</b>	Enter a password (any characters)
<b>Peer 1 IP address</b>	Set to the IP address of this (the master peer) VCS

---

**Note:** If the VCS has dual network interfaces, the Peer IP address **MUST** specify the LAN 1 interface address – also this interface must not have NAT enabled on it.

---

15. Click **Save**.  
To the right of the **Peer 1 IP address** field the words “*This VCS*” should appear (though this may require the page to be refreshed before they appear).
16. Restart the VCS (select **Maintenance > Restart**, then select **Restart system** and confirm **OK**).

After the restart, on the Master VCS web interface:

1. Check that the configuration (including zone configuration, transforms and other configuration for items from the System, VCS Configuration and Application menus) is as expected.
2. Backup the VCS (see Appendix 1 for details).

On other devices:

- If you have any other VCSs, Gatekeepers or Border Controllers neighbored (or connected via a traversal zone) to this Master VCS peer, ensure that their zone configuration for this cluster is updated to only include the address of this Master VCS.

On this Master VCS peer:

1. Log in to the web browser of this VCS.
2. Check the Alarms page (**Status > Alarms**):
  - a. If required, restart the VCS.
3. If the VCS did not need to be restarted, ensure that maintenance mode is disabled. Log in as admin on an SSH or other CLI interface. At the VCS command line type:

```
xconfiguration SystemUnit Maintenance Mode: Off
```

## After the master peer configuration

Check the Alarms page on the VCS (**Status > Alarms**) and ensure that all Alarms are acted upon and cleared.

## Additional cluster configuration

- If Microsoft Office Communications Server 2007 (OCS) or Lync 2010 is to be connected to this cluster, see the section “Microsoft Office Communications Server 2007 (OCS) and Lync Server 2010” in “Appendix 4 – Impact of clustering on other VCS applications”.

Creation of the new cluster (of one VCS) is complete; add other VCSs to the cluster using “Add an X7.2 VCS to a VCS X7.2 cluster (Provisioning Extension mode)”.

## Create a new cluster of VCS X7.2 peers (TMS Agent legacy mode)

**Note:** This procedure will require a period of downtime for the VCS service. Ensure that these instructions are followed in a scheduled maintenance window.

This process creates a cluster of a single VCS, and if TMS replication is enabled, it will be enabled using the old TMS Agent legacy mode.

Only use this process rather than "Create a new cluster of VCS X7.2 peers (Provisioning Extension mode – preferred)" if there are good reasons not to switch to the new Provisioning Extension mode, for example existing clusters connected to TMS that cannot be updated yet.

To complete the cluster containing multiple VCSs, when this section is complete, follow the instructions in "Add an X7.2 VCS to a VCS X7.2 cluster (TMS Agent legacy mode)" to add the non-master peers to the cluster.

Do not use this section if the cluster already exists; instead, follow the instructions in "Add an X7.2 VCS to a VCS X7.2 cluster (TMS Agent legacy mode)".

**Note:** If Device Provisioning or FindMe is to be used with an X7.2 VCS cluster, then use of TMS is essential. If neither Device Provisioning nor FindMe is to be used, then use of TMS is optional but recommended.

### Prerequisites

- All VCSs to be included in the cluster must be running the same version of VCS software, and that version of software must be X7.2.
- If Device Provisioning and FindMe are configured, they must have already been proven to be operational on the master VCS after its upgrade to X7.2.
- If TMS is to be used with this VCS cluster, ensure that it is running version 12.6 or later.
- If a firewall exists between cluster peers, it must be configured to permit the traffic documented in Appendix 3.

### Set up the master peer of the cluster

This process sets up the first (Master) peer of this new cluster – additional peers are added afterwards using the "Add an X7.2 VCS to a VCS X7.2 cluster (Provisioning Extension mode)" process.

Before proceeding, the VCS that will be the Master peer must be determined.

**Note:**

- ▶ The Master VCS will be the source of the configuration information for all VCS peers in the cluster. Non-master VCS peers will have their configuration deleted and replaced by that from the Master.
- ▶ FindMe information can only be kept if the relevant VCS is already configured to replicate with TMS. (FindMe information for clusters is stored on TMS; it is deleted on VCS and overwritten by the information from TMS when replication with TMS is enabled.)

On neighbor Gatekeepers (GKs) and Border Controllers (BCs):

1. If the Master VCS has a traversal zone configured to connect with any GK or BC, upgrade these systems to N6.1 or Q6.1 or later code.

On other VCSs:

1. Check that no other VCS (anywhere) has this VCS's IP address in its Alternates or Clustering Peers list.

On this Master VCS:

1. Check that the VCS is running X7.2 software.
2. Backup the VCS (See Appendix 1 for details).
3. On the web interface of this Master VCS, review the configuration to ensure that the VCS has:
  - A valid Ethernet speed (**System > Ethernet**).
  - Valid IP address and IP gateway (**System > IP**).
  - The same set of option keys installed as those that will be installed on all other peers of the cluster (**Maintenance > Option Keys**).

---

**Note:** the number of call license keys may be different on different peers; all other license keys must be identical on each peer.

---

- At least one valid DNS server configured, and that if unqualified DNS names are used elsewhere (e.g. for the NTP server), that the correct **Domain name** is also configured (**Domain name** is added as a suffix to an unqualified DNS name to make it into an FQDN) (**System > DNS**).

---

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

---

- A valid and working NTP server configured (**System > Time**; in the Status section, the State should be "**Synchronized**").
  - No peers configured (**VCS configuration > Clustering** – all Peer x IP address fields on this page should be blank. If not, delete any entries and click **Save**).
4. Ensure that this VCS does not list any of the VCSs that are to be peers in this new cluster in any of its neighbor zones or traversal zones (**VCS configuration > Zones** then check each neighbor and traversal zone).
  5. Set the H.323 **Time to live** to 60 (seconds) so that if a VCS becomes inaccessible to an endpoint, the endpoint will re-register quickly with another peer (**VCS configuration > Protocols > H.323**).
  6. Go to **System > DNS** and ensure that the **Local host name** is the DNS hostname for this VCS (typically the same as the **System name** in **System > System**, but excluding spaces, and unique for each VCS in the cluster); if it is not configured correctly, set it up appropriately and click **Save**.

---

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

---

7. Go to **VCS configuration > Calls** and set **Call routed mode** to *Optimal*.
8. Click **Save**.

---

**Note:** If Device Provisioning or FindMe is to be used with this X7.2 VCS cluster, then use of TMS is essential. If neither Device Provisioning nor FindMe is to be used, then use of TMS is optional but recommended.

---

If TMS is to be used, on the Master VCS:

1. Ensure that the VCS can see TMS.  
To do this, select **System > External Manager** and in the Status section, ensure that the **State** is **Active**.  
(If not, follow the process on 'Appendix 2 – Adding a VCS to TMS').
2. Ensure that TMS can communicate with this VCS.  
To do this, on TMS select **Systems > Navigator** (and any required sub folders) then click on the name of the VCS and ensure that it says:

“✓ System has no open or acknowledged tickets”

(If not, follow the process on ‘Appendix 2 – Adding a VCS to TMS’).

On this Master VCS:

1. Check the **Alarms** page of the VCS to be added (**Status > Alarms**). If there is an alarm that the VCS must be restarted, select **Maintenance > Restart** and then click **Restart System**.
  - Ignore any alarms about TMS Agent passwords being default; these will be cleared when TMS Replication is enabled.

If TMS is to be used:

1. Ensure that the Host Name of this Master VCS is set up in TMS:
  - a. Select **Systems > Navigator** (and any required sub folders).
  - b. Select this VCS.
  - c. Select the **Connection** tab.
  - d. Set **Host Name** to be the FQDN of this VCS, for example vcs3.uk.company.com.
  - e. Click **Save/Try**.  
You can ignore any error messages like “DNS config failure resolving <DNS name>: Did not find system IP address ( ) in DNS: <Server IP>”
  - f. Ensure that TMS updates its DNS.
    - i. Select the **Settings** tab.
    - ii. Click **Force Refresh**.

For this Master VCS:

1. If TMS is configured to **Enable TMS Agent Data Replication** with this VCS (to check: on TMS go to **Systems > Navigator** (and any required sub folders) select this VCS and select the TMS Agent tab) then any user accounts that existed on this VCS can be kept for use in the new cluster – if they are not wanted, they should be deleted.

If **Enable TMS Agent Data Replication** is not enabled, no FindMe data will be available for merging.

If data is replicating with TMS:

- a. If the user accounts held on this VCS are not wanted, delete any that exist:
  - i. Go to **Maintenance > Login accounts > User accounts**.
  - ii. Select all of the accounts shown and click **Delete**.
2. Enable maintenance mode. Log in as admin on an SSH or other CLI interface. At the VCS command line type:  
`xconfiguration SystemUnit Maintenance Mode: On`
3. Wait for all calls to clear and registrations to timeout.  
If necessary, manually remove any calls that do not clear automatically (using the web browser go to **Status > Calls**, then select the check box next to the calls you want to terminate and click **Disconnect**).
4. If necessary, manually remove any registrations that do not clear automatically (using the web browser go to **Status > Registrations > By device**, then select the check box next to the devices you want to remove and click **Unregister**).  
You can leave the registration for the Conference Factory – this will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own Conference Factory registration (if enabled).
5. Go to **VCS configuration > Clustering** and:
  - a. Check that **Cluster name** is the routable Fully Qualified Domain Name used in SRV records that address this VCS cluster, for example "cluster1.example.com". (See Appendix 8 – Cluster name and DNS SRV records).

- b. If it is not, the **Cluster name** needs changing; follow the procedure in “Appendix 7 – Changing the cluster name”.

---

**Note:** If the Cluster name is changed without following the procedure “Appendix 7 – Changing the cluster name” then any FindMe entries will be lost.

---

6. Click **Save**.
7. On the Clustering page (**VCS configuration > Clustering**) configure the fields as follows:

<b>Configuration master</b>	1
<b>Cluster pre-shared key</b>	Enter a password (any characters)
<b>Peer 1 IP address</b>	Set to the IP address of this (the master peer) VCS

---

**Note:** If the VCS has dual network interfaces, the Peer IP address **MUST** specify the LAN 1 interface address – also this interface must not have NAT enabled on it.

---

8. Click **Save**.  
To the right of the **Peer 1 IP address** field the words “*This VCS*” should appear (though this may require the page to be refreshed before they appear).
9. Restart the VCS (select **Maintenance > Restart**, then select **Restart system** and confirm **OK**).

After the restart, on the Master VCS web interface:

10. Check that other configuration (including zone configuration, transforms and other configuration for items from the System, VCS Configuration and Application menus) is as expected.
11. Backup the VCS (See Appendix 1 for details).

On other devices:

- If you have any other VCSs, Gatekeepers or Border Controllers neighbored (or connected via a traversal zone) to this Master VCS peer, ensure that their zone configuration for this cluster is updated to only include the address of this Master VCS.

If TMS is used, on TMS:

1. Go to **Systems > Navigator** (and any required sub folders) and select this Master VCS.
2. Select the **TMS Agent** tab:
  - a. Ensure that **Enable TMS Agent Data Replication** is selected.
  - b. Ensure that **Authentication Scheme** is set to **Digest**.
3. If any changes need to be made, click **Save Settings**.

---

**Note:** If TMS Agent Data Replication reports Disabled then there is a problem. On TMS select **Administrative Tools > Activity Status** and look for the Description ‘Enable TMS Agent Data Replication for system(s): <VCS name(s)>’. Click on the description for a full listing of the Activity log associated with this action. Identify and fix any reported problems.

---

On this Master VCS peer:

4. Log in to the web browser of this VCS.
5. Check the Alarms page (**Status > Alarms**):
  - a. If required, restart the VCS.
  - b. If “Security Alert: the TMS agent database has the default LDAP password set” or “Security Alert: the TMS agent database has the default replication password set” appear, see the relevant section in ‘Appendix 6 – Troubleshooting’.
6. If the VCS did not need to be restarted, ensure that maintenance mode is disabled. Log in as admin on an SSH or other CLI interface. At the VCS command line type:



xconfiguration SystemUnit Maintenance Mode: Off

## After the master peer configuration

If TMS is being used, verify the correct operation of TMS Agent by running TMS agent diagnostics as follows:

1. Log into TMS.
2. Go to **Administrative Tools > TMS Agent Diagnostics**.
3. In the **TMS Agent Browser** panel on the left side of the page, select **Local TMS Agent**.
4. Click **Run All Diagnoses** to run the diagnostic tests on the Local TMS Agent.
5. For this master VCS peer:
  - a. In the **TMS Agent Browser** panel on the left side of the page, expand the Un-clustered VCSs folder and the relevant sub folder and select the VCS peer.
  - b. Click **Run All Diagnoses** to run the diagnostic tests on the VCS peer.

---

**Note:** If authentication is intentionally enabled on the VCS, ignore the warning 'verify that authentication is disabled on the VCS'

---

- If all tests are successful (all green check marks), proceed with the "Additional cluster configuration" instructions below.
- If any errors are found (a red 'X' will appear against failing tests), do not proceed further with this upgrade, but contact your Cisco Authorized Service Provider for further assistance to resolve the issues identified.

## No Cisco TMS

If TMS is not used to monitor / manage VCS then check the Alarms page on the VCS (**Status > Alarms**) and ensure that all Alarms are acted upon and cleared.

---

**Note:** Use of TMS is required if Device Provisioning or FindMe is to be used with this cluster.

---

## Additional cluster configuration

- If Microsoft Office Communications Server 2007 (OCS) or Lync 2010 is to be connected to this cluster, see the section "Microsoft Office Communications Server 2007 (OCS) and Lync Server 2010" in "Appendix 4 – Impact of clustering on other VCS applications".

Creation of the new cluster (of one VCS) is complete, with TMS replication using the old TMS Agent legacy mode if enabled; add other VCSs to the cluster using "Add an X7.2 VCS to a VCS X7.2 cluster (TMS Agent legacy mode)".



## Add an X7.2 VCS to a VCS X7.2 cluster (Provisioning Extension mode)

Follow this process if you have an existing X7.2 cluster (of one or more peers) to which you want to add another VCS peer. If you do not have an existing cluster, following the instructions in the section “Create a new cluster of VCS X7.2 peers (Provisioning Extension mode – preferred)”.

---

**Note:** You can have up to 6 VCSs, including the master VCS, in a cluster.

---

This process will add an X7.2 VCS to the cluster and replicate the cluster Master's configuration onto the VCS.

### Prerequisites

- If Device provisioning is enabled, or FindMe is managed by TMS the existing cluster of 1 or more peers must already be running using Provisioning Extension mode.
- VCS clusters peers must all run the same version of code as the master, for example all X7.2.

---

**Note:** Only one VCS must be added to the cluster at a time.

---

On the Master VCS:

1. Ensure that the Master VCS does not list this new VCS peer in any of its neighbor zones or traversal zones (**VCS configuration > Zones** then check each neighbor and traversal zone).

---

**Note:** The Master VCS will be the source of the configuration for this new VCS peer and all other VCS peers in the cluster. When a VCS is added to the cluster, its configuration will be deleted and replaced by that from the Master.

---

On the VCS to be added to the cluster:

1. Check that no other VCS (anywhere) has this VCS's IP address in its Alternates or Clustering Peers list.
2. Check that the VCS software version is identical to the version running on the Master and any other cluster peers of the existing cluster (X7.2).
3. Backup the VCS (See Appendix 1 for details).

On the web interface of the VCS being added:

4. Review the configuration to ensure that the VCS has:
  - A valid Ethernet speed (**System > Ethernet**).
  - Valid IP address and IP gateway (**System > IP**).
  - The same set of Option keys as those installed on Master peer (**Maintenance > Option Keys**).

---

**Note:** The number of call license keys may be different on different peers; all other license keys must be identical on each peer.

---

- At least one valid DNS server configured, and that if unqualified DNS names are used elsewhere (e.g. for the NTP server), that the correct **Domain name** is also configured (**Domain name** is added as a suffix to an unqualified DNS name to make it into an FQDN) (**System > DNS**).

---

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

---

- A valid and working NTP server configured (**System > Time**; in the Status section, the State should be 'Synchronized').
- No peers configured (**VCS configuration > Clustering** – all Peer x IP address fields on this page should be blank. If not, delete any entries and click **Save**).

If the cluster is managed by TMS, this VCS being added to the cluster must also be managed by TMS.

---

**Note:** If Device Provisioning or FindMe is to be used with an X7.2 VCS cluster, then use of TMS is essential. If neither Device Provisioning nor FindMe is to be used, then use of TMS is optional but recommended.

---

If TMS is to be used, on the VCS to be added to the cluster:

1. Ensure that the VCS can see TMS.  
To do this, select **System > External Manager** and in the Status section, ensure that the State is **Active**.  
(If not, follow the process on 'Appendix 2 – Adding a VCS to TMS').
2. Ensure that TMS can communicate with this VCS. To do this, on TMS select **Systems > Navigator** (and any required sub folders) then click on the name of the VCS and ensure that it says:  
“✓ System has no open or acknowledged tickets”  
(If not, follow the process on 'Appendix 2 – Adding a VCS to TMS').

On the VCS being added to the cluster:

1. Check the **Alarms** page of the VCS to be added (**Status > Alarms**). If there is an alarm that the VCS must be restarted, select **Maintenance > Restart** and then click **Restart System**.
  - If multiple peers need restarting: restart each peer in turn, waiting for the peer to be accessible through the web interface before restarting the next peer.

If TMS is to be used:

1. For the VCS to be added to the cluster, ensure that the Host Name of the VCS is set up in TMS:
  - a. Select **Systems > Navigator** (and any required sub folders).
  - b. Select this VCS
  - c. Select the **Connection** tab.
  - d. Set **Host Name** to be the FQDN of this non-master peer, for example vcs3.uk.company.com.
  - e. Click **Save/Try**.  
You can ignore any error messages like “DNS config failure resolving <DNS name>: Did not find system IP address ( ) in DNS: <Server IP>”
  - f. Ensure that TMS updates its DNS.
    - i. Select the **Settings** tab.
    - ii. Click **Force Refresh**.

If TMS is configured to replicate FindMe information with this VCS being added to the cluster (to check: on TMS go to **Systems > Navigator** (and any required sub folders) select this VCS and select the Provisioning tab – see if the FindMe services tick box is selected), then any user accounts that existed on the VCS should be deleted.

If FindMe replication is not enabled, no FindMe data will be stored on TMS, and so the FindMe entries do not need to be deleted.

If FindMe data is provisioned from TMS:

- a. Delete any user accounts that exist. On the VCS being added to the cluster:
  - i. Go to **Maintenance > Login accounts > User accounts**.
  - ii. Select all of the accounts shown and click **Delete**.

On the VCS being added to the cluster:

1. Enable maintenance mode.  
Log in as admin on an SSH or other CLI interface. At the VCS command line type:  
`xconfiguration SystemUnit Maintenance Mode: On`
2. Wait for all calls to clear and registrations to timeout.  
If necessary, manually remove any calls that do not clear automatically (using the web browser go to **Status > Calls**, then select the check box next to the calls you want to terminate and click **Disconnect**).
3. If necessary, manually remove any registrations that do not clear automatically (using the web browser go to **Status > Registrations > By device**, then select the check box next to the devices you want to remove and click **Unregister**).  
You can leave the registration for the Conference Factory – this will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own Conference Factory registration (if enabled).

On the Master VCS:

1. On the Clustering page (**VCS configuration > Clustering**), one or more of the **Peer x IP address** fields should be empty.  
In the first empty field, enter the IP address of the new VCS peer.

---

**Note:**

- ▶ Only one VCS must be added to the cluster at a time (repeat the whole process if multiple VCS peers are being added).
  - ▶ If the new VCS peer has dual network interfaces, the Peer IP address **MUST** specify the LAN 1 interface address – also this interface must not have NAT enabled on it.
- 

2. Click **Save**.

Peer 1 should indicate 'This VCS'. The new peer may indicate '**Unknown**' and then with a refresh should indicate '**Failed**' as the VCS is not completely added to the cluster.

---

**Note:**

- ▶ A cluster communication failure alarm will be raised on the master and on other non-master peers already in the cluster advising that this new VCS peer is not communicating – this will clear later.
  - ▶ Cluster configuration replication is suspended at this point until the new VCS has been completely added. Any changes made to the configuration of the cluster will not be replicated until this VCS has been completely added
- 

On every other non-master VCS already in the cluster (not the VCS being added):

1. On the Clustering page (**VCS configuration > Clustering**) configure the fields as follows:

<b>Cluster name</b>	Identical to the <b>Cluster name</b> configured on the master VCS
<b>Cluster pre-shared key</b>	Identical to that configured on the master VCS
<b>Configuration master</b>	Identical to that configured on the master VCS
<b>Peer 1 IP address ... Peer 6 IP address</b>	Identical to those configured on the master VCS

---

2. Click **Save**.

On the additional non-master VCS being added to the cluster:

1. Log in as admin on an SSH or other CLI interface. At the VCS command prompt, type:  
`xcommand DefaultValueSet Level: 2`  
`xcommand DefaultLinksAdd`

---

**Note:** This command will wipe any LDAP authentication configuration – ensure that you have the web admin password before executing this command.

---

2. Go to the **Administrator accounts** page (**Maintenance > Login accounts > Administrator accounts**).
3. Delete all entries except the default admin account.
4. Go to **System > DNS** and ensure that **Local host name** is the DNS hostname for this VCS (typically the same as the **System name** in **System > System**, but excluding spaces, and unique for each VCS in the cluster); if it is not configured correctly, set it up appropriately and click **Save**.

---

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

---

5. On the Clustering page (**VCS configuration > Clustering**) configure the fields as follows:

<b>Cluster name</b>	Identical to the <b>Cluster name</b> configured on the master VCS
<b>Cluster pre-shared key</b>	Identical to that configured on the master VCS
<b>Configuration master</b>	Identical to that configured on the master VCS
<b>Peer 1 IP address ... Peer 6 IP address</b>	Identical to those configured on the master VCS

6. Click **Save**.

---

**Note:** A cluster communication failure alarm will be raised on this VCS peer advising that this new VCS is not communicating – this will clear after the restart.

---

7. Restart the VCS:
  - a. On the **Maintenance > Restart** page, click **Restart system**.
  - b. Confirm the restart by clicking **OK**.  
If multiple peers need restarting: restart each peer in turn, waiting for the peer to be accessible through the web interface before restarting the next peer.
8. After the restart, wait approximately 2 minutes – this is the frequency with which configuration is copied from the Master.
9. Check the **Alarms** page of the newly added VCS (**Status > Alarms**). If there is an alarm that the VCS must be restarted, select **Maintenance > Restart** and then click **Restart System**.
  - If multiple peers need restarting: restart each peer in turn, waiting for the peer to be accessible through the web interface before restarting the next peer.
10. Check that the configuration (including zone configuration, transforms configuration, CPL and other configuration for items from the System, VCS configuration and Application menus) is as expected (not FindMe — this will be replicated later) as per the Master VCS.

On other devices:

- If you have any other VCSs, Gatekeepers or Border Controllers neighbored (or connected via a traversal zone) to this cluster of VCS peers, ensure that their zone configuration for this cluster is updated to include the address of this new peer.

On each VCS peer (including the master and this new VCS peer):

1. Log in to the web browser of the new VCS peer.
2. Check the **Alarms** page (**Status > Alarms**):
  - a. If required, restart the VCS.
  - b. If multiple peers need restarting: restart each peer in turn, waiting for the peer to be accessible through the web interface before restarting the next peer.
3. Check that the expected FindMe entries (from the Master VCS) exist on this VCS (**Status > Applications > TMS Provisioning Extension services > FindMe > Accounts**).

Check replication status:

---

**Note:** It can take 5 or so minutes before VCS reports the successful status. If problems are seen, refresh the screen after waiting 5 minutes.

---

On VCS:

1. Go to the **Clustering** page (**VCS configuration > Clustering**):
  - Clustering status should show Status Enabled.
  - VCS system configuration replication status should show Last synchronization result SUCCEEDED.

If TMS is being used, ensure that TMS has all the correct settings for this upgraded VCS by forcing a refresh of TMS.

On TMS:

1. For every VCS in the cluster (including the Master VCS):
  - a. Select **Systems > Navigator** (and any required sub folders) and click on the name of the VCS.
  - b. Select the **Settings** tab.
  - c. Click **Force Refresh**.
2. Repeat for all VCS peers in the cluster.

## After adding the VCS peer to the cluster

Check the Alarms page on the VCS (**Status > Alarms**) and ensure that all Alarms are acted upon and cleared.

## Additional cluster configuration

- If Conference Factory (Multiway™) is to be used, see the section “Conference Factory (Multiway™)” in “Appendix 4 – Impact of clustering on other VCS applications”.
- If the cluster has non-default Trusted CA certificate and / or non default Server certificate ensure that the added peer is configured with the required Trusted CA certificate and an appropriate Server certificate.

Add an X7.2 VCS to a VCS X7.2 cluster is now complete.

## Add an X7.2 VCS to a VCS X7.2 cluster (TMS Agent legacy mode)

Follow this process if you have an existing X7.2 cluster (of one or more peers) to which you want to add another VCS peer. If you do not have an existing cluster, following the instructions in the section “Create a new cluster of VCS X7.2 peers (TMS Agent legacy mode)”.

---

**Note:** You can have up to 6 VCSs, including the master VCS, in a cluster.

---

This process will add an X7.2 VCS to the cluster and replicate the cluster Master’s configuration onto the VCS.

If TMS replication is enabled:

- the existing cluster of 1 or more peers must already be running using TMS Agent legacy mode.
- the added peer will be enabled using the old TMS Agent legacy mode.

---

**Note:**

- ▶ VCS clusters peers must all run the same version of code as the master, for example all X7.2.
  - ▶ Only one VCS must be added to the cluster at a time.
- 

On the Master VCS:

1. Ensure that the Master VCS does not list this new VCS peer in any of its neighbor zones or traversal zones (**VCS configuration > Zones** then check each neighbor and traversal zone).

---

**Note:** The Master VCS will be the source of the configuration for this new VCS peer and all other VCS peers in the cluster. When a VCS is added to the cluster, its configuration will be deleted and replaced by that from the Master.

---

On the VCS to be added to the cluster:

2. Check that no other VCS (anywhere) has this VCS’s IP address in its Alternates or Clustering Peers list.
3. Check that the VCS software version is identical to the version running on the Master and any other cluster peers of the existing cluster (X7.2).
4. Backup the VCS (See Appendix 1 for details).

On the web interface of the VCS being added:

5. Review the configuration to ensure that the VCS has:
  - A valid Ethernet speed (**System > Ethernet**).
  - Valid IP address and IP gateway (**System > IP**).
  - The same set of Option keys as those installed on Master peer (**Maintenance > Option Keys**).

---

**Note:** The number of call license keys may be different on different peers; all other license keys must be identical on each peer.

---

- At least one valid DNS server configured, and that if unqualified DNS names are used elsewhere (e.g. for the NTP server), that the correct **Domain name** is also configured (**Domain name** is added as a suffix to an unqualified DNS name to make it into an FQDN) (**System > DNS**).

---

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

---

- A valid and working NTP server configured (**System > Time**; in the Status section, the State should be **Synchronized**).
- No peers configured (**VCS configuration > Clustering** – all Peer x IP address fields on this page should be blank. If not, delete any entries and click **Save**).

If the cluster is managed by TMS, this VCS being added to the cluster must also be managed by TMS.

---

**Note:** If Device Provisioning or FindMe is to be used with an X7.2 VCS cluster, then use of TMS is essential. If neither Device Provisioning nor FindMe is to be used, then use of TMS is optional but recommended.

---

If TMS is to be used, on the VCS to be added to the cluster:

6. Ensure that the VCS can see TMS.  
To do this, select **System > External Manager** and in the Status section, ensure that the State is **Active**.  
(If not, follow the process on 'Appendix 2 – Adding a VCS to TMS').
7. Ensure that TMS can communicate with this VCS. To do this, on TMS select **Systems > Navigator** (and any required sub folders) then click on the name of the VCS and ensure that it says:  
“✓ System has no open or acknowledged tickets”  
(If not, follow the process on 'Appendix 2 – Adding a VCS to TMS').

On the VCS being added to the cluster:

8. Check the **Alarms** page of the VCS to be added (**Status > Alarms**). If there is an alarm that the VCS must be restarted, select **Maintenance > Restart** and then click **Restart System**.
  - Ignore any alarms about TMS Agent passwords being default; these will be cleared when TMS Replication is enabled.
  - If multiple peers need restarting: restart each peer in turn, waiting for the peer to be accessible through the web interface before restarting the next peer.

If TMS is to be used:

9. For the VCS to be added to the cluster, ensure that the Host Name of the VCS is set up in TMS:
  - a. Select **Systems > Navigator** (and any required sub folders).
  - b. Select this VCS
  - c. Select the **Connection** tab.
  - d. Set **Host Name** to be the FQDN of this non-master peer, for example vcs3.uk.company.com.
  - e. Click **Save/Try**.  
You can ignore any error messages like “DNS config failure resolving <DNS name>: Did not find system IP address ( ) in DNS: <Server IP>”
  - f. Ensure that TMS updates its DNS.
    - i. Select the **Settings** tab.
    - ii. Click **Force Refresh**.

If TMS is configured to replicate with this VCS being added to the cluster (to check this on TMS go to **Systems > Navigator** - and any required sub folders - select this VCS and select the TMS Agent tab) then any user accounts that existed on the VCS should be deleted.

If TMS is not configured to replicate with this VCS no FindMe data will be stored on TMS.

If TMS is replicating with VCS:

- g. Delete any user accounts that exist. On the VCS being added to the cluster:
  - i. Go to **Maintenance > Login accounts > User accounts**.
  - ii. Select all of the accounts shown and click **Delete**.



If TMS is used, for the master VCS in the cluster:

1. Select **Systems > Navigator** (and any required sub folders), then click on the Master VCS of the cluster.
2. Select the **Clustering** tab.
3. Clear the **Enable TMS Agent Data Replication on all Cluster Peers** check box (if it was set).
4. Click **Save Cluster Settings**.

---

**Note:** This disables database replication from TMS to each cluster peer.

- ▶ Provisioning data will no longer be updated from TMS to the VCSs, however provisioning of endpoints from data cached on VCSs will continue.
  - ▶ VCS cluster configuration replication will continue.
  - ▶ VCS FindMe replication among VCS peers will STOP.
- 

If TMS is used, for each VCS in the cluster (including the Master and the VCS being added to the cluster), in TMS:

1. Select **Systems > Navigator** (and any required sub folders).
2. Select the VCS.
3. Select the **TMS Agent** tab.
4. Clear the **Enable TMS Agent Data Replication** check box (if it was set).
5. Click **Save Settings**.

On the VCS being added to the cluster:

6. Enable maintenance mode.  
Log in as admin on an SSH or other CLI interface. At the VCS command line type:  
`xconfiguration SystemUnit Maintenance Mode: On`
7. Wait for all calls to clear and registrations to timeout.  
If necessary, manually remove any calls that do not clear automatically (using the web browser go to **Status > Calls**, then select the check box next to the calls you want to terminate and click **Disconnect**).
8. If necessary, manually remove any registrations that do not clear automatically (using the web browser go to **Status > Registrations > By device**, then select the check box next to the devices you want to remove and click **Unregister**).  
You can leave the registration for the Conference Factory – this will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own Conference Factory registration (if enabled).

On the Master VCS:

1. On the Clustering page (**VCS configuration > Clustering**), one or more of the **Peer x IP address** fields should be empty.  
In the first empty field, enter the IP address of the new VCS peer.

---

**Note:**

- ▶ Only one VCS must be added to the cluster at a time (repeat the whole process if multiple VCS peers are being added).
  - ▶ If the new VCS peer has dual network interfaces, the Peer IP address MUST specify the LAN 1 interface address – also this interface must not have NAT enabled on it.
- 

2. Click **Save**.

Peer 1 should indicate 'This VCS'. The new peer may indicate '**Unknown**' and then with a refresh should indicate '**Failed**' as the VCS is not completely added to the cluster.



**Note:**

- ▶ A cluster communication failure alarm will be raised on the master and on other non-master peers already in the cluster advising that this new VCS peer is not communicating – this will clear later.
- ▶ Cluster configuration replication is suspended at this point until the new VCS has been completely added. Any changes made to the configuration of the cluster will not be replicated until this VCS has been completely added

On every other non-master VCS already in the cluster (not the VCS being added):

1. On the Clustering page (**VCS configuration > Clustering**) configure the fields as follows:

<b>Cluster name</b>	Identical to the <b>Cluster name</b> configured on the master VCS
<b>Cluster pre-shared key</b>	Identical to that configured on the master VCS
<b>Configuration master</b>	Identical to that configured on the master VCS
<b>Peer 1 IP address ... Peer 6 IP address</b>	Identical to those configured on the master VCS

2. Click **Save**.

On the additional non-master VCS being added to the cluster:

1. Log in as admin on an SSH or other CLI interface. At the VCS command prompt, type:

```
xcommand DefaultValueSet Level: 2
xcommand DefaultLinksAdd
```

**Note:** This command will wipe any LDAP Authentication configuration – ensure that you have the web admin password before executing this command.

2. Go to the **Administrator accounts** page (**Maintenance > Login accounts > Administrator accounts**).
3. Delete all entries except the default admin account.
4. Go to **System > DNS** and ensure that **Local host name** is the DNS hostname for this VCS (typically the same as the **System name** in **System > System**, but excluding spaces, and unique for each VCS in the cluster); if it is not configured correctly, set it up appropriately and click **Save**.

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

5. On the Clustering page (**VCS configuration > Clustering**) configure the fields as follows:

<b>Cluster name</b>	Identical to the <b>Cluster name</b> configured on the master VCS
<b>Cluster pre-shared key</b>	Identical to that configured on the Master VCS
<b>Configuration master</b>	Identical to that configured on the Master VCS
<b>Peer 1 IP address ... Peer 6 IP address</b>	Identical to those configured on the Master VCS

6. Click **Save**.

**Note:** A cluster communication failure alarm will be raised on this VCS peer advising that this new VCS is not communicating – this will clear after the restart.

7. Restart the VCS:
  - a. On the **Maintenance > Restart** page, click **Restart system**.

- b. Confirm the restart by clicking **OK**.  
If multiple peers need restarting: restart each peer in turn, waiting for the peer to be accessible through the web interface before restarting the next peer.
8. After the restart, wait approximately 2 minutes – this is the frequency with which configuration is copied from the Master.
9. Check the **Alarms** page of the newly added VCS (**Status > Alarms**). If there is an alarm that the VCS must be restarted, select **Maintenance > Restart** and then click **Restart System**.
  - Ignore any alarms about TMS Agent passwords being default; these will be cleared when TMS Replication is enabled.
  - If multiple peers need restarting: restart each peer in turn, waiting for the peer to be accessible through the web interface before restarting the next peer.
10. Check that the configuration (including zone configuration, transforms configuration, CPL and other configuration for items from the System, VCS configuration and Application menus) is as expected (not FindMe — this will be replicated later) as per the Master VCS.

On other devices:

- If you have any other VCSs, Gatekeepers or Border Controllers neighbored (or connected via a traversal zone) to this cluster of VCS peers, ensure that their zone configuration for this cluster is updated to include the address of this new peer.

If TMS is used, and if Device Provisioning or FindMe are to be used in this cluster, on TMS:

1. Select **Systems > Navigator** (and any required sub folders) then select the Master VCS.
2. Select the **Clustering** tab
  - a. Ensure that **Enable TMS Agent Data Replication on all Cluster Peers** is selected, if it is not, select it and click **Save Cluster Settings** or **Create Cluster** as appropriate.
3. Go to **Systems > Navigator** (and any required sub folders) then select the new VCS to be added to this cluster.
4. Select the **TMS Agent** tab
  - a. Ensure that **Enable TMS Agent Data Replication** is selected.
  - b. Ensure that **Authentication Scheme** is set to **Digest**.
5. If any changes need to be made, click **Save Settings**.

---

**Note:** If TMS Agent Data Replication reports Disabled then there is a problem. On TMS select **Administrative Tools > Activity Status** and look for the Description 'Enable TMS Agent Data Replication for system(s): <VCS name(s)>'. Click on the description for a full listing of the Activity log associated with this action. Identify and fix any reported problems.

---

On each VCS peer (including the master and this new VCS peer):

6. Log in to the web browser of the new VCS peer.
7. Check the **Alarms** page (**Status > Alarms**):
  - a. If required, restart the VCS.
  - b. If "Security Alert: the TMS agent database has the default LDAP password set" or "Security Alert: the TMS agent database has the default replication password set" appear, see the relevant section in 'Appendix 6 – Troubleshooting'.  
If multiple peers need restarting: restart each peer in turn, waiting for the peer to be accessible through the web interface before restarting the next peer.
8. Check that the expected FindMe entries (from the Master VCS) exist on this VCS (**Maintenance > Login accounts > User accounts**).

Check replication status:

---

**Note:** It can take 5 or so minutes before VCS reports the successful status. If problems are seen, refresh the screen after waiting 5 minutes.

---

On VCS:

9. Go to the **Clustering** page (**VCS configuration > Clustering**):
  - Clustering status should show Status Enabled.
  - VCS system configuration replication status should show Last synchronization result SUCCEEDED.
10. If replication with TMS is enabled:
  - a. Select the link "View TMS Agent replication status".
  - b. Check that the top line of the TMS Agent replication status report reports Replication Enabled.

If TMS is being used, ensure that TMS has all the correct settings for this upgraded VCS by forcing a refresh of TMS.

On TMS:

11. For every VCS in the cluster (including the Master VCS):
  - a. Select **Systems > Navigator** (and any required sub folders) and click on the name of the VCS.
  - b. Select the **Settings** tab.
  - c. Click **Force Refresh**.
12. Repeat for all VCS peers in the cluster.

## After adding the VCS peer to the cluster

If TMS is being used, verify the correct operation of TMS Agent by running TMS agent diagnostics as follows:

1. Log into Cisco TMS.
2. Go to **Administrative Tools > TMS Agent Diagnostics**.
3. In the **TMS Agent Browser** panel on the left side of the page, select **Local TMS Agent**.
4. Click **Run All Diagnoses** to run the diagnostic tests on the Local TMS Agent.
5. For each VCS peer:
  - a. In the **TMS Agent Browser** panel on the left side of the page, expand the Clustered VCSs folder and cluster folder and select the VCS peer.
  - b. Click **Run All Diagnoses** to run the diagnostic tests on the VCS peer.

---

**Note:** If authentication is intentionally enabled on the VCS, ignore the warning 'verify that authentication is disabled on the VCS'.

---

If all tests are successful (all green check marks), proceed with the "Check the Alarms page on the VCS (**Status > Alarms**) and ensure that all Alarms are acted upon and cleared.

- Additional cluster configuration" instructions below.
- If any errors are found (a red 'X' will appear against failing tests), do not proceed further with this upgrade, but contact your Cisco Authorized Service Provider for further assistance to resolve the issues identified.

## Additional cluster configuration

- If Conference Factory (Multiway™) is to be used, see the section “Conference Factory (Multiway™)” in “Appendix 4 – Impact of clustering on other VCS applications”.
- If the cluster has non-default Trusted CA certificate and / or non default Server certificate ensure that the added peer is configured with the required Trusted CA certificate and an appropriate Server certificate.

Add an X7.2 VCS to a VCS X7.2 cluster is now complete.

## Remove a live VCS from a VCS X7.2 cluster (permanently)

This process will remove one VCS peer from an existing cluster. FindMe and configuration replication to this VCS will be stopped and the VCS will no longer be included in the list of peers in the cluster. Provisioning will also be disabled on the removed VCS.

- If the whole cluster is to be disbanded then use the procedure defined in “Disband a VCS X7.2 cluster”.
- If the cluster peer to be removed is not accessible, use the procedure defined in “Remove an out-of-service VCS from a VCS X7.2 cluster (permanently)”.

Before starting:

1. Ensure that the VCS to be removed from the cluster is not indicated as the Master peer. If it is the Master, see the section “Change the master peer of a VCS X7.2 cluster” for instructions on how to make a different peer the master.

If TMS is in TMS Agent Legacy mode, on TMS:

(no change is required if TMS is in Provisioning Extension mode)

1. Select **Systems > Navigator** (and any required sub folders) then select the VCS to be removed.
2. Select the **TMS Agent** tab.
3. If TMS is in TMS Agent Legacy mode
  - a. Clear the **Enable TMS Agent Data Replication** check box
  - b. Click **Save Settings**.

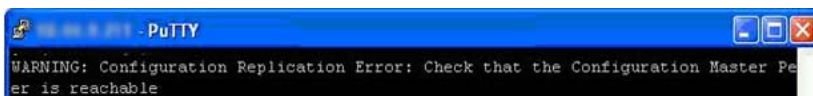
On the VCS that is being removed:

1. Log into the web interface.
2. Go to the **Clustering** page ( **VCS configuration > Clustering**):
  - a. Change the **Cluster name** to a unique ID for this VCS (ideally to the routable Fully Qualified Domain Name used in SRV records that address this individual VCS, for example "vcs1.example.com". (See Appendix 8 – Cluster name and DNS SRV records.))  
Note: Do NOT use the process “Appendix 7 – Changing the cluster name (and keeping FindMe accounts)” because FindMe accounts are to be left with the cluster that this VCS is being removed from.
  - b. Delete the **Cluster pre-shared key**.
  - c. Delete all entries in the **Peer x IP address** fields.
3. Click **Save**.

---

### Note:

- ▶ FindMe users will not be available on this removed VCS (they will be left available on the cluster).
- ▶ An alarm similar to that shown below may appear on the web interface and CLI of the VCS being removed. This is not a problem, the alarm will be cleared when the VCS is restarted:



4. If OCS Relay was used in the cluster, go to the OCS Relay page (**Applications > OCS Relay**).
  - If Mode = *On* change it to Mode = *Off* and click **Save**.

5. If Microsoft OCS/Lync B2BUA was used in the cluster, go to the Microsoft OCS/Lync B2BUA configuration page (**Applications > B2BUA > Microsoft OCS/Lync > Configuration**).
  - If Microsoft OCS/Lync B2BUA = *Enabled* change it to Microsoft OCS/Lync B2BUA = *Disabled* and click **Save**.
6. Restart the VCS (**Maintenance > Restart** and then click **Restart System**).

On the Master VCS:

1. Log into the web interface.
2. On the Clustering page (**VCS configuration > Clustering**) delete the IP address of the VCS that has been removed.
3. If the VCS being removed is not the last field in the list, move any other IP addresses up the list so that there are no empty fields between entries.
4. If the master VCS peer's IP address has been moved up the list in the previous step, alter the **Configuration master** value to match its new location.
5. Click **Save**.

On all the remaining non-master VCS peers:

1. Log into the web interface.
2. On the Clustering page (**VCS configuration > Clustering**) edit the **Peer x IP address** and **Configuration master** fields so that they are identical to those configured on the Master VCS.
3. Click **Save**.
4. Repeat for all remaining non-master VCS peers until they all have identical clustering configuration.

On other devices:

1. If you have any other VCSs, Gatekeepers or Border Controllers neighbored (or connected via a traversal zone) to this cluster of VCS peers, ensure their zone configuration for this cluster is updated to exclude the address of the removed peer.
2. If you have any endpoints registering to the VCS that has now been removed, change the configuration of the endpoint (or the configuration of the DNS server entry that points to the cluster peers) so that they register to one of the remaining clustered VCS peers instead.

---

**Caution:** The removed VCS will retain its configuration at the time it is removed from the cluster, and will continue to function as a non-clustered VCS. It is recommended that after it has been removed from the cluster it is taken out of service (e.g. perform a factory reset – as documented in "Before reconnecting the out-of-service VCS back to the network" later in this document, or perform `xcommand DefaultValueSet Level: 2` and `xcommand DefaultLinksAdd`) or the VCS is reconfigured with an alternative configuration, so that other devices no longer try to use it as a cluster peer.

---

## Reconfigure TMS

If TMS is used and TMS Agent is in Legacy mode, on TMS:

1. Select **Systems > Navigator** (and any required sub folders) then select the Master VCS.
2. Select the **Clustering** tab.
3. Click **Update Cluster in TMS**.

## After the removal

If TMS is not used or TMS is in Provisioning Extension mode, skip this section, there are no diagnostic checks to run

If TMS is being used and TMS Agent is in Legacy mode: verify the correct operation of TMS Agent by running TMS agent diagnostics as follows:

1. Log into TMS.
2. Go to **Administrative Tools > TMS Agent Diagnostics**.
3. In the **TMS Agent Browser** panel on the left side of the page, select **Local TMS Agent**.
4. Click **Run All Diagnoses** to run the diagnostic tests on the Local TMS Agent.
5. For each VCS peer:
  - a. In the TMS Agent Browser panel on the left side of the page, expand the Clustered VCSs folder and cluster folder and select the VCS peer.
  - b. Click **Run All Diagnoses** to run the diagnostic tests on the VCS peer.

---

**Note:** If authentication is intentionally enabled on the VCS, ignore the warning 'verify that authentication is disabled on the VCS'.

---

- If all tests are successful (all green check marks), removing an out-of-service VCS from a cluster is now complete.
- If any errors are found (a red 'X' will appear against failing tests), do not proceed further with this upgrade, but contact your Cisco Authorized Service Provider for further assistance to resolve the issues identified.

Removing a live VCS from a cluster is now complete.

## Remove an out-of-service VCS from a VCS X7.2 cluster (permanently)

Use the following procedure if:

- the VCS is dead and needs to be RMA'd, or
- the VCS cannot be accessed for some other reason

If the whole cluster is to be disbanded then use the procedure defined in "Disband a VCS X7.2 cluster".

If the cluster peer to be removed is accessible, use the procedure defined in "Remove a live VCS from a VCS X7.2 cluster (permanently)" which clears up the removed VCS as well as its previous peers.

---

**Note:** This procedure does not delete clustering configuration from the removed VCS. When removed, you must not reconnect the out-of-service VCS without first deleting all of its peers and stopping FindMe and configuration replication (see the section below "Before reconnecting the out-of-service VCS back to the network").

---

Before starting:

1. Ensure that the VCS to be removed from the cluster is not indicated as the Master VCS on TMS. If it is the Master VCS, see the section "Change the master peer of a VCS X7.2 cluster" for instructions on how to make a different peer the master.

If TMS is in TMS Agent Legacy mode, on TMS:

(no change is required if TMS is in Provisioning Extension mode)

1. Select **Systems > Navigator** (and any required sub folders) then select the VCS to be removed.
2. Select the **TMS Agent** tab.
3. If TMS is in TMS Agent Legacy mode
  - a. Clear the **Enable TMS Agent Data Replication** check box.
  - b. Click **Save Settings**.

On the Master VCS:

1. Log into the web interface.
2. On the Clustering page (**VCS configuration > Clustering**) delete the IP address of the VCS that has been removed.
3. If the VCS being removed was not the last in the list, move any other IP addresses up the list so that there are no empty fields between entries
  - If this results in the master VCS peer's IP address moving up the list, alter the **Configuration master** value to match its new location.
4. Click **Save**.

On all the remaining non-master VCS peers:

1. Log into the web interface.
2. On the Clustering page (**VCS configuration > Clustering**) edit the **Peer x IP address** and **Configuration master** fields so that they are identical to that set on the Master VCS.
3. Click **Save**.
4. Repeat for all remaining non-master VCS peers.

On other devices:

1. If you have any other VCSs, Gatekeepers or Border Controllers neighbored (or connected via a traversal zone) to this cluster of VCS peers, ensure their zone configuration for this cluster is updated to exclude the address of the removed peer.



2. If you have any endpoints registering to the VCS that has now been removed, change the configuration of the endpoint (or the configuration of the DNS server entry that points to the cluster peers) so that they register to one of the remaining clustered VCS peers instead.

## Reconfigure TMS

If TMS is used and TMS Agent is in Legacy mode, on TMS:

1. Select **Systems > Navigator** (and any required sub folders) then select the Master VCS.
2. Select the **Clustering** tab.
3. Click **Update Cluster in TMS**.

## After the removal

If TMS is not used or TMS is in Provisioning Extension mode, skip this section, there are no diagnostic checks to run

If TMS is being used and TMS Agent is in Legacy mode: verify the correct operation of TMS Agent by running TMS agent diagnostics as follows:

1. Log into TMS.
2. Go to **Administrative Tools > TMS Agent Diagnostics**.
3. In the **TMS Agent Browser** panel on the left side of the page, select **Local TMS Agent**.
4. Click **Run All Diagnoses** to run the diagnostic tests on the Local TMS Agent.
5. For each VCS peer:
  - a. In the TMS Agent Browser panel on the left side of the page, expand the Clustered VCSs folder and cluster folder and select the VCS peer.
  - b. Click **Run All Diagnoses** to run the diagnostic tests on the VCS peer.

---

**Note:** If authentication is intentionally enabled on the VCS, ignore the warning 'verify that authentication is disabled on the VCS'.

---

- If all tests are successful (all green check marks), removing an out-of-service VCS from a cluster is now complete.
- If any errors are found (a red 'X' will appear against failing tests), do not proceed further with this upgrade, but contact your Cisco Authorized Service Provider for further assistance to resolve the issues identified.

Removing an out-of-service VCS from a cluster is now complete.

## Before reconnecting the out-of-service VCS back to the network

If the removed VCS is ever recovered, before you reconnect it you must clear out its configuration. This is most easily implemented as follows:

1. Log into the VCS as root (over serial or SSH – serial connection will show more details as the factory reset progresses).
2. Type:  
`factory-reset`  
then press **enter**
  - a. Keep option Keys = YES

- b. Keep IP configuration = YES or NO ... depends on whether the VCS has been replaced with another at the same IP address
- c. Keep SSH keys = NO
- d. Keep root and admin passwords = YES or NO ... as desired
- e. Save log files = NO ... unless specifically requested for analysis purposes
- f. Replace hard disk = NO
- g. Are you sure you want to continue = YES

Some messages will be displayed, then connection over serial / SSH will be lost.  
It may take some 20 or more minutes before VCS is available to access again.

3. Log into the VCS as Admin over SSH

4. Type:

```
xcommand DefaultLinksAdd
```

This ensures that the configuration of the recovered VCS is returned to default and it will not interact with its ex-peers.

## Disband a VCS X7.2 cluster

This process will remove all VCS peers from an existing cluster. FindMe and configuration replication will be stopped, as will provisioning, and the cluster will be deleted from TMS.

Each VCS will retain its configuration at the time the cluster was disbanded, and will function as a stand-alone VCS.

---

**Caution:** If any of the VCSs are left in operation after being removed from the cluster, calls between endpoints registered to different VCSs that were once part of the same cluster will not succeed. This is because after the cluster has been disbanded, the Cluster Subzone will no longer exist and there will not be any link between the two VCSs over which calls can be routed. To overcome this, you must create neighbor relationships between the VCSs so that there are links between them.

---

- If any VCS is not accessible, firstly remove it using the procedure “Remove an out-of-service VCS from a VCS X7.2 cluster (permanently)”.

If TMS is used and TMS is in **TMS Agent Legacy mode**, on TMS:

1. Select **Systems > Navigator** (and any required sub folders) then select the Master VCS.
2. Select the **Clustering** tab.
3. Clear the **Enable TMS Agent Data Replication on all Cluster Peers**.
4. Click **Save Cluster Settings**.
5. Select the **TMS Agent** tab.
6. Ensure that **Enable TMS Agent Data Replication** is not selected; if this needs changing, change it and click **Save Settings**.

If TMS is used and TMS is in **TMS Agent Legacy mode**, on TMS, for every non-master VCS peer:

1. Select **Systems > Navigator** (and any required sub folders) then click on the non-master VCS.
2. Select the **TMS Agent** tab.
3. Ensure that **Enable TMS Agent Data Replication** is not selected; if this needs changing, change it and click **Save Settings**.
4. Repeat for all non-master VCS peers –TMS may require you to pause between disabling each peer.

If TMS is used and TMS is in **Provisioning Extension mode**:

1. Select **Systems > Navigator** (and any required sub folders), then click on any VCS in the cluster.
2. Select the **Provisioning** tab.
3. Disable all 4 services (clear tick boxes).
4. Click **Save**.

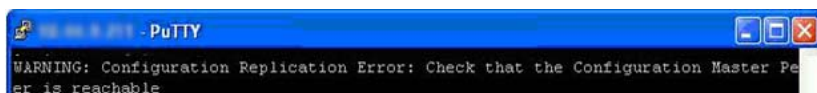
On each non-master VCS peer:

1. Log into the web interface.
2. From the Clustering page ( **VCS configuration > Clustering**):
  - a. Change the **Cluster name** to a unique ID for this VCS (ideally to the routable Fully Qualified Domain Name used in SRV records that address this individual VCS, for example "vcs1.example.com", "vcs2.example.com". etc. (See Appendix 8 – Cluster name and DNS SRV records.))  
 Note: Do NOT use the process “Appendix 7 – Changing the cluster name (and keeping FindMe accounts)” because FindMe accounts are to be left with the master peer of the cluster that this VCS is being removed from.
  - b. Delete the **Cluster pre-shared key**.

- c. Delete all entries in the **Peer x IP address** fields.
3. Click **Save**.

**Note:**

- ▶ FindMe users will not be available on non-master VCSs (they will only be left available on the master).
- ▶ An alarm similar to that shown below may appear on the web interface and CLI of the VCS being removed. This is not a problem, the alarm will be cleared when the VCS is restarted:

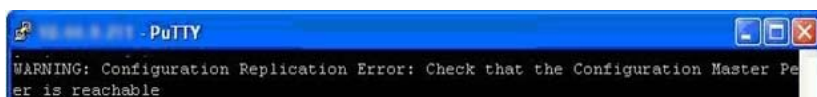


4. If OCS Relay was used in the cluster, go to the OCS Relay page (**Applications > OCS Relay**).
  - If Mode = *On* change it to Mode = *Off* and click **Save**.
5. If Microsoft OCS/Lync B2BUA was used in the cluster, go to the Microsoft OCS/Lync B2BUA configuration page (**Applications > B2BUA > Microsoft OCS/Lync > Configuration**).
  - If Microsoft OCS/Lync B2BUA = *Enabled* change it to Microsoft OCS/Lync B2BUA = *Disabled* and click **Save**.
6. Restart the VCS (**Maintenance > Restart** and then click **Restart System**).  
If multiple peers need restarting, restart each peer in turn, waiting for the peer to be accessible through the web interface before restarting the next.
7. Repeat for each non-master VCS.

## On the Master VCS:

1. Log into the web interface.
2. If the **Cluster name** is to be changed on this Master VCS, FindMe information should be deleted, so that the database is not left with unused user accounts.
  - a. Delete all FindMe entries:
    - i. Go to **Maintenance > Login accounts > User accounts**.
    - ii. Select each account and click **Delete**.
3. Go to the Clustering page (**VCS configuration > Clustering**).
  - a. Optionally change the **Cluster name** to a unique ID for this VCS (ideally to the routable Fully Qualified Domain Name used in SRV records that address this individual VCS, for example "vcs1.example.com". (See Appendix 8 – Cluster name and DNS SRV records.))  
Use the process "Appendix 7 – Changing the cluster name (and keeping FindMe accounts)" if FindMe accounts are to be kept with this VCS.
  - b. Delete the **Cluster pre-shared key**.
  - c. Delete all entries in the **Peer x IP address** fields.
4. Click **Save**.

**Note:** An alarm similar to that shown below may appear on the web interface and CLI of the VCS being removed. This is not a problem; the alarm will be cleared when the VCS is restarted:



5. Restart the VCS (**Maintenance > Restart** and then click **Restart System**).

On other devices:

1. If you have any other VCSs, Gatekeepers or Border Controllers neighbored (or connected via a traversal zone) to this cluster of VCS peers, ensure that they have those zones removed, or modified appropriately.
2. If you have any endpoints registering to this VCS cluster, change the configuration of the endpoints (or the configuration of the DNS server entry that points to the cluster peers) so that they now register with an appropriate VCS.

## Reconfigure TMS

If TMS is used and TMS is in TMS Agent Legacy mode: on TMS:

1. Select **Systems > Navigator** (and any required sub folders) then select the Master VCS.
2. Select the **Clustering** tab.
3. In the Cluster Settings section click **Delete Cluster**.
4. Confirm that you really want to delete the cluster by clicking **Delete**.  
TMS will report "Cluster successfully deleted".

Disband a cluster of VCSs is now complete.

# Change the master peer of a VCS X7.2 cluster

## Changing the master peer where the old master is or is not accessible

---

**Note:** The operations in this process should be performed in one go so that the cluster is not left in a state where there are multiple VCSs which think they are cluster Master.

---

On the “new” Master VCS:

1. Go to the **Clustering** page (**VCS configuration > Clustering**) and from the **Configuration master** drop-down menu select the ID number of the Peer entry that says ‘This VCS’.
2. Click **Save**.

*While performing this change of master peer, ignore any alarms on VCS that report ‘Cluster master mismatch’ or ‘Cluster replication error’ – they will be rectified as part of this procedure.*

If the “old” Master VCS is accessible, on the “old” Master VCS:

1. On the **Clustering** page (**VCS configuration > Clustering**) from the **Configuration master** drop-down menu select the ID number of the “new” Master VCS.
2. Click **Save**.

For all other non-master VCS peers, on that VCS:

1. Go to the **Clustering** page (**VCS configuration > Clustering**) and from the **Configuration master** drop-down menu select the ID number of the “new” Master VCS.
2. Click **Save**.

On each VCS in the cluster (including the master):

1. Confirm that the change to the **Configuration master** has been accepted by going to **VCS configuration > Clustering** and refreshing the page.
2. If any VCSs have not accepted the change, repeat the steps above.
3. Check the Status section:
  - Clustering status should show Status Enabled
  - VCS system configuration replication status should show Last synchronization result SUCCEEDED

---

**Note:** After approximately 2 minutes any alarms raised on the VCS peers that relate to ‘Cluster master mismatch’ and ‘Cluster replication error’ should automatically clear.

---

## Reconfigure TMS

No changes are required; TMS will see the master change on the VCS cluster and report this appropriately.

## If the old master is not available

If you are changing the Master because the “old” Master is not accessible, remove the “old” Master using the “Remove an out-of-service VCS from a VCS X7.2 cluster (permanently)” procedure.

If the “old” Master was not accessible when changing the master peer of the VCS cluster, but later becomes available, you must bring it back into the cluster using the “Add an X7.2 VCS to a VCS X7.2 cluster (Provisioning Extension mode)” procedure.

Changing the master peer of a VCS cluster is now complete.

## Change the IP address of a VCS X7.2 peer

To change the IP address of a VCS peer you must remove the VCS from the cluster, change its IP address, and then add the VCS back into the cluster.

The process is as follows:

1. Ensure that the VCS whose IP address is to be changed is not the Master VCS.  
If it is the Master VCS, follow the steps in the section “Change the master peer of a VCS X7.2 cluster” to make a different peer the Master.
2. Carry out the process documented in “Remove a live VCS from a VCS X7.2 cluster (permanently)”.
3. Change the IP address of the VCS.
4. Carry out the process documented in “Add an X7.2 VCS to a VCS X7.2 cluster (Provisioning Extension mode)”.

Changing the IP address of a VCS peer is now complete.

# Upgrading VCS X5.2 or earlier versions to X7.2

This section describes how to upgrade VCS version X5.2 or earlier to X7.2.

## Upgrade VCS X1 / X2 Alternates to a VCS X7.2 cluster

An upgrade from X1 / X2 alternates direct to an X7.2 cluster is not possible. An upgrade from X1 / X2 to X5.2 must be performed first, then upgrade from X5.2 to X6.1, then upgrade to X7.2.

Follow the steps in “Upgrade VCS X1 / X2 Alternates to a VCS X5 cluster” in *Cluster creation and maintenance guide (X5)*, upgrading the VCSs to X5.2, then follow the steps “Upgrade and X5.1, X5.1.1 or X5.2 cluster to an X6.1 cluster” in *Cluster creation and maintenance deployment guide (X6.1)* and then return to this guide and follow the steps “Upgrade an X6.0, X6.1, X7.0 or X7.0.n or X7.1 cluster to an X7.2 cluster”.

## Upgrade an X3 / X4 / X5.0 cluster to an X7.2 cluster

An upgrade from an X3 / X4 / X5.0 cluster direct to an X7.2 cluster is not possible, an upgrade from X3 / X4 / X5.0 to X5.2 must be performed first, then upgrade from X5.2 to X6.1, then upgrade to X7.2.

Follow the steps in “Upgrade a Cisco VCS X3 / X4 cluster to an X5 cluster (including Cisco TMS to 12.6)”, or the “Upgrade an X5.0 cluster to an X5.2 cluster” in *Cluster creation and maintenance guide (X5)* to get to an X5.2 cluster, then follow the steps “Upgrade and X5.1, X5.1.1 or X5.2 cluster to an X6.1 cluster” in *Cluster creation and maintenance deployment guide (X6.1)* and then return to this guide and follow the steps “Upgrade an X6.0, X6.1, X7.0 or X7.0.n or X7.1 cluster to an X7.2 cluster”.

## Upgrade an X5.1, X5.1.1 or X5.2 cluster to an X7.2 cluster

An upgrade from an X5.1 / X5.1.1 / X5.2 cluster direct to an X7.2 cluster is not possible, an upgrade from X5.1 / X5.1.1 / X5.2 to X6.1 must be performed first, then upgrade from X6.1 to X7.2.

Follow the steps ““Upgrade and X5.1, X5.1.1 or X5.2 cluster to an X6.1 cluster”” in *Cluster creation and maintenance deployment guide (X6.1)* and then return to this guide and follow the steps “Upgrade an X6.0, X6.1, X7.0 or X7.0.n or X7.1 cluster to an X7.2 cluster”.



# Appendix 1 – Backing up a VCS

## Backing up an X5.0 or later VCS

To backup the data:

1. On the VCS web interface go to **Maintenance > Backup and restore**.
2. Click **Create System Backup File** and save the file.
3. If the option exists, click **Create TMS Agent backup file** and save the file (this backs up FindMe entries on Legacy systems).

---

**Note:**

- ▶ TMS Agent backup is not used for Provisioning Extension mode or VCS Starter Pack Express.
  - ▶ If the TMS Agent backup is restored (uploaded) to VCS then:  
from a root login run “tmsagent\_reindex\_database” to ensure the uploaded data is linked into the database correctly.
  - ▶ If TMS is in TMS Agent Legacy mode, a TMS Agent backup contains the whole of the TMS’s provisioning and FindMe database (for all clusters and non-clustered VCSs with which TMS is replicating). It is saved for emergency use only – if restored to a cluster it will only get overwritten by the TMS data. It can be restored to a non-clustered VCS that is not replicating with TMS.
- 

To save the VCS certificates:

4. Use SCP (log in as root) to copy the following files from the VCS:
  - a. persistent/policy/policy.xml
  - b. persistent/certs/\*.\*

## Appendix 2 – Adding a VCS to TMS

On the VCS:

1. Go to the SNMP page (**System > SNMP**) and ensure that:

- a. **SNMP mode** is set to *v3 plus TMS support* or *v2c*.
- b. **Community name** is set to *public*.

(If SNMP was previously disabled, an alarm may appear indicating the need for a restart. If a restart is required, go to **Maintenance > Restart** and click **Restart System**.)

If multiple peers need restarting: restart each peer in turn, waiting for the peer to be accessible through the web interface before restarting the next peer.

2. Go to the External Manager page (**System > External Manager**) and ensure that:

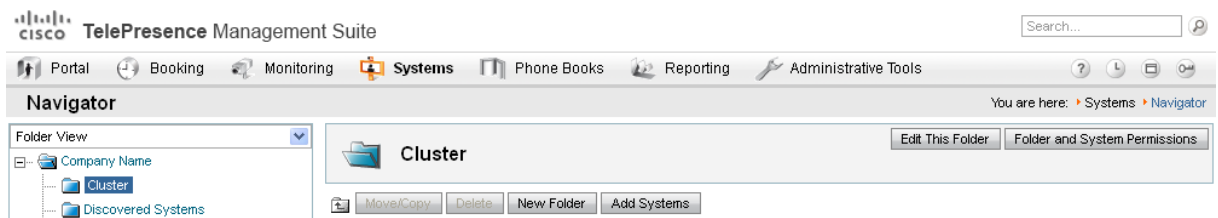
- a. **Address** is set to the IP Address or FQDN of TMS.
- b. **Path** is set to *tms/public/external/management/SystemManagementService.asmx*.
- c. If the **Protocol** is *HTTPS* and **Certificate verification mode** is *On* then you must load the relevant certificates before the connection can become 'Active'. See document "D50520 Implementing Secure Management" for details.
- d. If the **Protocol** is *HTTP* or **Certificate verification mode** is *Off*, no certificates need to be loaded.

3. Click **Save**.

The **Status** section of the **External Manager** page should show a **State** 'Active' or 'Initialising'.<sup>1</sup>

On TMS:

1. Select **Systems > Navigator**.
2. Select (or create) an appropriate folder in which to put the VCS (in the example below the folder has been called "Cluster"):



3. Click **Add Systems**.
4. In section "1. Specify Systems by IP addresses or DNS names", enter the IP address or DNS name of the VCS.
5. Click **Next**.
6. Look for ✓ System added.

If an error occurs, e.g. "✗ Wrong Password", click on the **Edit System** link and correct the problem (enter the root password of the VCS).

<sup>1</sup> TMS may force protocol to be HTTPS. The configuration for this is found in TMS **Administrative Tools > Configuration > Network settings**. The protocol will be forced to HTTPS if, in the **TMS Services** section **Enforce Management Settings on Systems** is set to **On** and in the **Secure-Only Device Communication** section **Secure-Only Device Communication** is set to **On**.

7. Click **Finish Adding Systems**, **Add System despite warnings** or **Add More Systems** as appropriate.
8. If 'Could not connect to system. Details: No SNMP response' is reported, go to the **Connection** tab and type 'public' into the SNMP Get Community Name and select **Save/Try**.
9. If the VCS password is not default, set this up in the Connection tab or in **Settings > Edit Settings**.
  - If the VCS was already configured in TMS, ensure that it has the correct IP address (in TMS, go to **Systems > Navigator** (and any required sub folders), select the VCS, and from the **Connection** tab check the **IP Address** field).

On VCS:

1. Go to the **External Manager** page (**System > External Manager**). The State should now show State **Active**.

## Appendix 3 – IP ports and protocols

It is unusual to have any sort of firewall between cluster peers, but if there is, the following lists document the IP protocols and ports that must be open between each and every VCS peer in the cluster.

For cluster communications between VCS peers:

- UDP port 500 (ISAKMP) for PKI (Public Key Infrastructure) key exchange
- Standard SIP and H.323 signaling and media ports are used for calls (see *X4 to X7 VCS Port Usage for Firewall Traversal* for more information)
- UDP port 1719 is used for bandwidth updates between VCS peers
- IP protocol 51 (IPSec AH) is used for database synchronization
- UDP ephemeral ports are used for cluster management

For cluster communications between VCS peers and a TMS when running in Provisioning Extension mode:

- VCS ephemeral port to port 443 on TMS (secure) or
- VCS ephemeral port to port 80 on TMS

Note that port 443 or 80 are the default values; they can be configured in the TMS IIS, and VCS if different ports are required.

For cluster communications between VCS peers and a TMS when running in TMS Agent Legacy mode:

- TCP port 389 (LDAP) is used for directory lookup services
- TCP port 636 is reserved, currently not used
- TCP port 8989 is used for FindMe and provisioning data synchronization replication
- TCP port 4444 is used for FindMe and provisioning data synchronization administration from TMS to VCS

## IPSEC communications

For IPSEC between VCS cluster peers:

- AES256 is used for encryption, SHA256 (4096 bit key length) is used for authentication. Peers are identified by their IP address and are authenticated using a pre-shared key.
- Main mode is used during the IKE exchange.
- diffie-hellman group 'modp4096' is being used.

## Appendix 4 – Impact of clustering on other VCS applications

### Conference Factory (Multiway™)

- The Conference Factory application configuration is NOT replicated across a cluster.
- The Conference Factory template MUST be DIFFERENT on each of the VCS peers.

When configuring a cluster to support Multiway:

1. Set up the **same** Conference Factory alias (the alias called by the endpoint to initiate a Multiway conference) on each peer.
2. Set up a **different** Conference Factory template on each peer (so that each peer generates unique Multiway conference IDs).

For example, if the MCU service prefix for ad hoc conferences is **775** then the Master VCS may have a template of **775001%%@domain**, peer 2 a template of **775002%%@domain**, and peer 3 a template of **775003%%@domain**. In this way whichever VCS serves the conference ID, it cannot serve a conference ID that any other VCS could have served.

The same applies across a network. If there is more than one VCS or VCS cluster that provides Conference Factory functionality in a network, each and every VCS must provide values in a unique range, so that no two VCSs can serve the same conference ID.

### Microsoft Office Communications Server 2007 (OCS) and Lync Server 2010

If Lync Server is to be configured to operate with an X7.2 VCS cluster, see *Microsoft Lync 2010 and VCS deployment guide*.

For OCS, see *Microsoft OCS 2007, Lync 2010 and VCS deployment guide*.

If the VCS cluster is an “OCS/Lync gateway” VCS cluster and the Microsoft OCS/Lync B2BUA is turned off, and OCS Relay is used, some parameters on the VCS cluster, such as:

- Call routed mode
- H.323 ↔ SIP interworking mode

may need setting according to the OCS/Lync deployment guide rather than the values specified in this cluster deployment guide.

## Appendix 5 – Configuring endpoints to work with a VCS cluster

When configuring endpoints it is desirable for them to know about all the VCS peers in a cluster, so that at initial registration or later, if they lose connection to their VCS peer, they have the ability to register with and use another peer in the VCS cluster.

SIP and H.323 endpoints behave differently – the following sections show the methods that can be used, and order them in preferred order.

For additional details about DNS SRV and round-robin DNS see the URI dialling section in the VCS Administrator Guide.

Also see “Appendix 8 – Cluster name and DNS SRV records”.

### H.323 endpoints

The options below are listed in preference order for providing resilience of connectivity of endpoints to a cluster of VCSs where 1 or more VCS cluster peers become inaccessible. The choice of option will depend on what functionality the endpoint you are using supports.

#### Option 1 – DNS SRV (preferred)

To use this option, there must be a DNS SRV record available for the DNS name of the VCS cluster that defines an equal weighting and priority for each cluster peer.

On each H.323 endpoint, configure the Gatekeeper Settings as:

- Discovery = Manual
- IP Address = DNS name of the VCS cluster

If the endpoint supports DNS SRV, on startup the endpoint issues a DNS SRV request and receives a DNS SRV record back defining an equal weighting and priority for each cluster peer. It may also receive a list of lower priority entries pointing at a fallback cluster.

The endpoint then tries to register with a relevant cluster peer (having taken into account the priority / weightings). If that peer is not available, the endpoint will try and register to another listed peer at the same priority, or if all peers at that priority have been tried, a peer at the next lower (higher numbered) priority.

This will be repeated until the endpoint can register with a VCS. On registering with the VCS, the VCS will respond with the H.323 “Alternate Gatekeepers” list containing the list of VCS cluster peer members.

The endpoint will continue to use the first VCS that it registered to for re-registrations and for calls. If it ever loses connection to its VCS then it will select an “Alternate Gatekeeper” from the list it was supplied with.

DNS SRV cache timeout should be set to a fairly long time (e.g. 24 hours) to minimize DNS traffic.

#### Option 2 – DNS Round-Robin (2nd choice)

To use this option, there must be a DNS A-record available for the DNS name of the VCS cluster that supplies a round-robin list of IP addresses.

On each H.323 endpoint configure the Gatekeeper Settings as:

- Discovery = Manual
- IP Address = DNS name of the VCS cluster

If the endpoint does not support DNS SRV, on startup the endpoint will perform a DNS A-record lookup. The DNS server will have been configured to support round-robin DNS, with each of the cluster peer members defined in the round-robin list.

The endpoint will take the address given by the DNS lookup and will then try and register with the relevant cluster peer. If that peer is not available, then the endpoint will perform another DNS lookup and will try to connect to the new VCS peer that it is given. (The DNS server will have supplied the next cluster peer's IP address.)

This will be repeated until the endpoint can register with a VCS. On registering with the VCS, the Cisco will respond with the H.323 'Alternate Gatekeepers' list containing the list of VCS cluster peer members.

The endpoint will continue to use the first VCS that it registered to for re-registrations and for calls. If it ever loses connection then it will select an "Alternate Gatekeeper" from the list it was supplied with.

DNS cache timeout should be set to a fairly short time (e.g. 1 minute or less) so that on failure to reach a VCS at startup, the endpoint is quickly pointed at a different VCS.

### Option 3 – Static IP (least preferred)

Use this option if the VCS cluster does not have a DNS name.

On each H.323 endpoint configure the Gatekeeper Settings as:

- Discovery = Manual
- IP Address = IP address of a VCS peer

On startup the endpoint will try and register with the VCS at the specified IP address. If that is not available, then the endpoint will continue trying at regular intervals.

This will be repeated until the endpoint can register with the VCS. On registering with the VCS, the VCS will respond with the H.323 "Alternate Gatekeepers" list containing the list of VCS cluster peer members.

The endpoint will continue to use the first VCS that it registered to for re-registrations and for calls. If it ever loses connection then it will select an "Alternate Gatekeeper" from the list it was supplied with.

## SIP endpoints

The options below are listed in preference order for providing resilience of connectivity of endpoints to a cluster of VCSs where 1 or more VCS cluster peers become inaccessible. The choice of option will depend on what functionality the endpoint you are using supports.

### Option 1 – SIP Outbound (preferred)

SIP outbound allows an endpoint to be configured to register to 2 or more VCS peers simultaneously. The benefit of this is that if the connection between one peer and the endpoint gets broken, then a connection from the endpoint to the other peer remains. With the endpoint registering to both peers simultaneously, there is no break in service while the endpoint realizes that its registration has failed, before it registers to a different peer. Thus, at no time is the endpoint unreachable.

Configuration of SIP outbound is endpoint specific, but typically will be:

- Proxy 1
  - Server discovery = Manual
  - Server Address =  
    DNS name of cluster peer or  
    IP address of cluster peer
- Proxy 2

- Server discovery = Manual
- Server Address =
  - DNS name of a different cluster peer or
  - IP address of a different cluster peer
- Outbound = On

## Option 2 – DNS SRV (2<sup>nd</sup> choice)

To use this option, there must be a DNS SRV record available for the DNS name of the VCS cluster that defines an equal weighting and priority for each cluster peer.

On each SIP endpoint configure the SIP Settings as:

- Server discovery = Manual
- Server Address = DNS name of the VCS cluster

If the endpoint supports DNS SRV, on startup the endpoint issues a DNS SRV request and receives a DNS SRV record back defining an equal weighting and priority for each cluster peer.

The endpoint then tries to register with a relevant cluster peer (having taken into account the priority / weightings). If that peer is not available, the endpoint will try and register to another listed peer at the same priority, or if all peers at that priority have been tried, a peer at the next lower priority.

This will be repeated until the endpoint can register with a VCS.

The endpoint will continue to use the first VCS that it registered to for re-registrations and for calls. If it ever loses connection to its VCS, it will use the DNS SRV entry to find a new VCS to register to, starting at the highest priority.

DNS SRV cache timeout should be set to a fairly long time (e.g. 24 hours) to minimize DNS traffic.

## Option 3 – DNS Round-Robin (3<sup>rd</sup> choice)

To use this option, there must be a DNS A-record available for the DNS name of the VCS cluster that supplies a round-robin list of IP addresses.

On each SIP endpoint configure the SIP Settings as:

- Server discovery = Manual
- Server Address = DNS name of the VCS cluster

If the endpoint does not support DNS SRV, on startup the endpoint will perform a DNS A-record lookup. The DNS server will have been configured to support round-robin DNS, with each of the cluster peer members defined in the round-robin list.

The endpoint will take the address given by the DNS lookup and will then try and register with the relevant cluster peer. If that is not available, then the endpoint will perform another DNS lookup and will try to connect to the new VCS peer that it is given. (The DNS server will have supplied the next cluster peer's IP address.)

This will be repeated until the endpoint can register with a VCS.

The endpoint will continue to use the first VCS that it registered to for re-registrations and for calls. If it ever loses connection to its VCS it will perform another DNS lookup to find a new VCS to register to (the DNS server providing a VCS in the round-robin sequence).

DNS cache timeout should be set to a fairly short time (e.g. 1 minute or less) so that if a VCS is not accessible the endpoint is quickly pointed at a different VCS.

## Option 4 – Static IP (least preferred)

Use this option if the VCS cluster does not have a DNS name.



On each SIP endpoint configure the SIP Settings as:

- Server discovery = Manual
- Server Address = IP address of a VCS peer

On startup the endpoint will try and register with the VCS at the specified IP address. If that is not available, then the endpoint will continue trying at regular intervals.

This will be repeated until the endpoint can register with the VCS.

The endpoint will continue to use the first VCS that it registered to for re-registrations and for calls. If it ever loses connection then it will keep on trying to register to that VCS until it is accessible again.

## Appendix 6 – Troubleshooting

### Cisco VCS alarms and warnings

**“Cluster name not configured: if FindMe or clustering are in use a cluster name must be defined; see the Clustering section of the VCS Administrator Guide for more information”**

Ensure that the same cluster name is configured on each VCS in the cluster.

The **Cluster name** should be the routable Fully Qualified Domain Name used in SRV records that address this Cisco VCS cluster, for example "cluster1.example.com". (See Appendix 8 – Cluster name and DNS SRV records).

**“Cluster replication error: <details> manual synchronization of configuration is required”**

This may be:

- “Cluster replication error: manual synchronization of configuration is required”
- "Cluster replication error: cannot find master or this slave's peer configuration file, manual synchronization of configuration is required"
- "Cluster replication error: configuration master ID is inconsistent, manual synchronization of configuration is required"
- "Cluster replication error: this peer's configuration conflicts with the master's configuration, manual synchronization of configuration is required"

If a non-master VCS reports an alarm: “Cluster replication error – <details> synchronization of configuration”

On that non-master VCS:

- Log in as admin on an SSH or other CLI interface. At the command prompt type:  
`xcommand ForceConfigUpdate`

This will delete the non-master VCS configuration and then force it to update its configuration from the master VCS.

---

**Caution:** Only use this command if the configuration on the Master VCS is known to be in a good state.

---

**"Cluster replication error: the NTP server is unreachable"**

Configure an accessible NTP server on the VCS web page **System > Time**.

**"Cluster replication error: the local VCS does not appear in the list of peers"**

Check and correct the list of peers for this VCS on the Master VCS, and copy to all other VCS peers (**VCS configuration > Clustering**).

## "Cluster replication error: automatic replication of configuration has been temporarily disabled because an upgrade is in progress"

Wait until the upgrade has completed.

## "Invalid clustering configuration: H.323 mode must be turned On - clustering uses H.323 communications between peers"

Ensure that H.323 mode is on (see **VCS configuration > Protocols > H.323**).

## "Security alert: the TMS Agent database has the default LDAP password set"

If the VCS is being managed by TMS, on TMS:

1. Go to **Administrative Tools > Configuration > TMS Agent Settings**. In the Global (applied to all agents) section:
  - a. Set up the **TMS Agent LDAP Configuration Password**.
  - b. Click **Save**.

---

**Note:** This will configure the LDAP Configuration password on the TMS and all VCSs and their TMS Agents managed by that TMS.

---

If the VCS is a non-clustered VCS, follow the instructions in the Action link associated with the alarm.

## "Security alert: the TMS Agent database has the default replication password set"

If the VCS is being managed by TMS, on TMS:

1. Go to **Administrative Tools > Configuration > TMS Agent Settings**. In the Global (applied to all agents) section:
  - a. Set up the **TMS Agent LDAP Replication Password**.
2. Click **Save**.

---

**Note:** This will configure the LDAP Configuration password on the TMS and all VCSs and their TMS Agents managed by that TMS.

---

If the VCS is a non-clustered VCS, follow the instructions in the Action link associated with the alarm.

## "VCS database failure: Please contact your Cisco support representative"

They will help you work through the following steps:

1. Take a system snapshot and provide to TAC.
2. Remove the VCS from the cluster using: "Remove a live VCS from a VCS X7.2 cluster (permanently)".
3. Restore that VCS's database by restoring a VCS backup taken on that VCS previously.
4. Add the VCS back to the cluster using "Add an X7.2 VCS to a VCS X7.2 cluster (Provisioning Extension mode)".

A second method is possible if the database does not recover:

1. Take a system snapshot and provide to TAC.

2. Remove the VCS from the cluster using: “Remove a live VCS from a VCS X7.2 cluster (permanently)”.
3. Log in as root and run “clusterdb\_destroy\_and\_purge\_data.sh”.
4. Restore that VCS’s database by restoring a VCS backup taken on that VCS previously.
5. Add the VCS back to the cluster using “Add an X7.2 VCS to a VCS X7.2 cluster (Provisioning Extension mode)”.

---

**Note:** clusterdb\_destroy\_and\_purge\_data.sh is as dangerous as it sounds – only use this command in conjunction with instructions from TAC.

---

## Cisco TMS

### No TMS Agent tabs

If there are no TMS Agent tabs, TMS Agent has to be enabled in TMS. See *TMS Provisioning deployment guide* for details about how to do this.

## Cisco TMS warnings

### TMS Cluster Diagnostics

If TMS cluster diagnostics reports a difference in configuration on VCS peers, it is comparing the output of `https://<ip address>/alternatesconfiguration.xml` for each VCS.

To manually check the differences, on a Unix / Linux system, run:

```
wget --user=admin --password=<password> --no-check-certificate https://<IP
    or FQDN of VCS>/alternatesconfiguration.xml
```

for each of the VCS peers, then use `diff` to check for differences.

### Conference Factory template does not replicate

This is by design; the Conference Factory %% value is NOT shared between cluster peers and the Conference Factory application configuration is NOT replicated across a cluster.

See the section “Conference Factory (Multiway™)” above.

### VCS’s External manager protocol keeps getting set to HTTPS

TMS can be configured to force specific management settings on connected systems. This includes ensuring that a VCS uses HTTPS for feedback. If enabled, TMS will (on a time period defined by TMS) re-configure the VCS’s **System > External manager** Protocol to HTTPS.

If HTTPS must be used for VCS to supply feedback to TMS, see details in “Appendix 2 – Adding a VCS to TMS” to see how to set up certificates etc.

TMS will force HTTPS on VCS if:

- **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*

Set **Enforce Management Settings on Systems** to *Off* if TMS does not need to force the management settings.

Set **Secure-Only Device Communication** to *Off* if it is unnecessary for VCS to provide feedback to TMS using HTTPS (if HTTP is sufficient).

## My cluster of Cisco VCS Expressways with dual network interfaces is not replicating correctly

Cisco VCS Expressways with Dual Network interfaces are only designed to replicate through their LAN 1 interface. Ensure that the Peer x IP Address entries specified in **VCS configuration > Clustering** all refer to LAN 1 interfaces.

Also this replicating interface (LAN 1) must not have NAT enabled on it.

## My cluster of Cisco VCS Expressways with static NAT is not replicating correctly

When using Cisco VCS Expressways with static NAT the cluster replication must occur on the LAN interface which is not behind the NAT device. Therefore LAN interface 1 must be the non NAT interface and the Peer x IP Address entries specified in **VCS configuration > Clustering** must all refer to LAN 1 interfaces. LAN interface 2 must be configured for static NAT.

# Appendix 7 – Changing the cluster name (and keeping FindMe accounts)

## Provisioning Extension mode

Cluster name changing needs no special handling when using Provisioning Extension mode.

Be aware though that the cluster name is the FQDN provided as part of provisioning as the FQDN for the endpoint to send registration requests to.

## TMS Agent legacy mode

The cluster name specifies which data is to be used from the replicated database.

Follow this process to change the cluster name in order to retain the data associated with the previous cluster name. e.g. when a new VCS cluster is being created and the FindMe accounts are to be carried across from the Master VCS to the new cluster.

1. In the **root login**, at a command prompt, type:  
`transferfindmeaccounts <current Cluster name of this VCS> <Cluster name of the cluster being created>`
2. Go to **VCS configuration > Clustering** and:
  - Set **Cluster name** to be <Cluster name of the cluster being created>, where <Cluster name of the cluster being created> is the routable fully qualified domain name used in SRV records that address this VCS cluster, for example "cluster1.example.com". (See Appendix 8 – Cluster name and DNS SRV records).

---

**Note:**

- ▶ If transferfindmeaccounts is executed on multiple VCSs with different <current Cluster name of this VCS> to the same <Cluster name of the cluster being created>, the FindMe accounts from each of the VCSs will be merged into the new <Cluster name of the cluster being created> database.
  - ▶ If a whole cluster is having its cluster name changed, the transferfindmeaccounts only needs to be run on the master VCS.
  - ▶ If a VCS cluster has its name changed, go to TMS and select the Master VCS, select the clustering tab and 'Cluster name has changed' should be reported. Select 'Update Cluster in TMS'.
-

## Appendix 8 – Cluster name and DNS SRV records

Using DNS SRV to convert a domain to an IP address has a number of benefits:

- The structure of the lookup includes service type and protocol as well as the domain, so that a common domain can be used to reference multiple different services which are hosted on different machines (e.g. html, sip, h.323).
- The DNS SRV response includes priority and weighting values which allow the specification of primary, secondary, tertiary etc groups of servers, and within each priority group, the weighting defines the proportion of accesses that should use each server.
- Because the DNS SRV response contains details about priorities and weights of multiple servers, the receiving device can use a single lookup to search for an in-service server (where some servers are in-accessible) without the need to repeatedly query the DNS server (this is in contrast to using round robin DNS which does require repeated lookups into the DNS server if initial servers are found to be in-accessible).

The generic format of a DNS SRV query is:

- `_service._protocol.<fully.qualified.domain>`

The format of DNS SRV queries for sip (RFC 3263) and h.323 used by VCS are:

- `_sips._tcp.<fully.qualified.domain>`
- `_sip._tcp.<fully.qualified.domain>`
- `_sip._udp.<fully.qualified.domain>` - not recommended for video calls, only use for audio-only calls
- `_h323ls._udp.<fully.qualified.domain>` - for udp RAS messaging, e.g LRQ
- `_h323cs._tcp.<fully.qualified.domain>` - for H.323 call signaling

The format of DNS SRV queries for sip (RFC 3263) and h.323 typically used by an endpoint are:

- `_sips._tcp.<fully.qualified.domain>`
- `_sip._tcp.<fully.qualified.domain>`
- `_sip._udp.<fully.qualified.domain>` - not recommended for video calls, only use for audio-only calls
- `_h323ls._udp.<fully.qualified.domain>` - for udp RAS messaging, e.g LRQ
- `_h323cs._tcp.<fully.qualified.domain>` - for H.323 call signaling
- `_h323rs._udp.<fully.qualified.domain>` - for H.323 registrations

The DNS SRV response is a set of records in the format:

- `_ service. _ protocol.<fully.qualified.domain>. TTL Class SRV Priority Weight Port Target`

where Target is an A-record defining the destination.

---

**Note:** UDP is not a good transport medium for video – SIP messaging for video systems is too large to be carried on a packet based (rather than stream based) transport. UDP is often used for audio only devices.

---

Further details on DNS SRV can be found in *Cisco VCS Administrator Guide* and RFC 2782.

The VCS **Cluster name** (configured on the **VCS configuration > Clustering** page) should be the <fully.qualified.domain> specified in the DNS SRV records that point to the VCS cluster.

Example: DNS SRV records for 2 peers of a VCS Expressway cluster for company.com

Where:

- FQDN of VCS Expressway peer 1: vcse1.company.com
- FQDN of VCS Expressway peer 2: vcse2.company.com
- FQDN of VCS Expressway cluster: company.com

```
_sips._tcp.company.com. 86400 IN SRV 1 1 5061 vcse1.company.com.  
_sips._tcp.company.com. 86400 IN SRV 1 1 5061 vcse2.company.com.  
  
_sip._tcp.company.com. 86400 IN SRV 1 1 5060 vcse1.company.com.  
_sip._tcp.company.com. 86400 IN SRV 1 1 5060 vcse2.company.com.  
  
_h323ls._udp.company.com. 86400 IN SRV 1 1 1719 vcse1.company.com.  
_h323ls._udp.company.com. 86400 IN SRV 1 1 1719 vcse2.company.com.  
  
_h323cs._tcp.company.com. 86400 IN SRV 1 1 1720 vcse1.company.com.  
_h323cs._tcp.company.com. 86400 IN SRV 1 1 1720 vcse2.company.com.  
  
_h323rs._udp.company.com. 86400 IN SRV 1 1 1719 vcse1.company.com.  
_h323rs._udp.company.com. 86400 IN SRV 1 1 1719 vcse2.company.com.
```

---

**Note:**

- ▶ Priorities are all the same – only use different priorities if you have different clusters allowing failover from one primary cluster to another (secondary) cluster  
- in that case the primary cluster's peers should have one value and the other (secondary) cluster's peers a (larger) value
  - ▶ Weights should be the same – so that there is equal use of each peer
- 

## Endpoints supporting SIP DNS SRV

Movi versions prior to 4.0 supports:

- \_sip.\_tls.<fully.qualified.domain>
- \_sip.\_tcp.<fully.qualified.domain>

Movi version 4.0 and later supports:

- \_sips.\_tcp.<fully.qualified.domain>
- \_sip.\_tcp.<fully.qualified.domain>

E20 version TE2.1 supports:

- \_sips.\_tls.<fully.qualified.domain>
- \_sip.\_tcp.<fully.qualified.domain>

MXP version F8.2 supports:

- \_sip.\_tls.<fully.qualified.domain>



- `_sip._tcp.<fully.qualified.domain>`

T150 version L6.0 supports:

- `_sip._tls.<fully.qualified.domain>`
- `_sip._tcp.<fully.qualified.domain>`

C-Series versions prior to TC4.0 supports:

- `_sip._tls.<fully.qualified.domain>`
- `_sip._tcp.<fully.qualified.domain>`

C-Series from version TC4.0 supports:

- `_sips._tcp.<fully.qualified.domain>`
- `_sip._tcp.<fully.qualified.domain>`

Cisco TelePresence MCU supports:

- `_sips._tcp.<fully.qualified.domain>`
- `_sip._tcp.<fully.qualified.domain>`

SIP DNS SRV records required:

- `_sips._tcp.<fully.qualified.domain>` Movi (4.0 and later), C-Series (TC4.0 and later), VCS, MCU
- `_sips._tls.<fully.qualified.domain>` E20 to TE2.1
- `_sip._tls.<fully.qualified.domain>` MXP to F8.2, T150 to L6.0, Movi prior to 4.0, C-Series prior to TC4.0
- `_sip._tcp.<fully.qualified.domain>` All products for TCP

---

#### Note:

- ▶ UDP is not a good transport medium for video – SIP messaging for video systems is too large to be carried on a packet based (rather than stream based) transport. UDP is often used for audio only devices.
  - ▶ `_sip._tls,<fully.qualified.domain>` is an SRV record also used by Microsoft OCS Edge servers.
- 

## Looking up .SRV records

### Web browser checking of DNS SRV settings

Go to **Maintenance > Tools > Network utilities > DNS lookup**.

Enter the SRV path in the Host field and click **Lookup**.

## Nslookup

```
nslookup -query=SRV _sip._tcp.example.com
```

## Dig

```
dig _sip._tcp.example.com SRV
```

```
; <<>> DiG 9.4.1 <<>> _sip._tcp.example.com SRV
;; global options: printcmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 44952
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 4

;; QUESTION SECTION:
_sip._tcp.example.com.      IN      SRV

;; ANSWER SECTION:
_sip._tcp.example.com. 1183    IN      SRV      1 0 5060 sbc1.example.com.
_sip._tcp.example.com. 1183    IN      SRV      1 0 5060 sbc2.example.com.

;; AUTHORITY SECTION:
example.com.           87450    IN      NS       ns1.mydyndns.org.
example.com.           87450    IN      NS       ns2.mydyndns.org.

;; ADDITIONAL SECTION:
sbc1.example.com.      1536     IN      A        194.73.59.53
sbc2.example.com.      1376     IN      A        194.73.59.54
ns1.mydyndns.org.      75       IN      A        204.13.248.76
ns2.mydyndns.org.      10037    IN      A        204.13.249.76

;; Query time: 0 msec
;; SERVER: 10.44.8.11#53(10.44.8.11)
;; WHEN: Mon Jul 26 11:09:59 2010
;; MSG SIZE rcvd: 243

~ #
```

## Appendix 9 – NAPTR records

NAPTR records are typically used to specify various methods to connect to a destination URI, for example by email, by SIP, by H.323. They can also be used to specify the priority to use for those connection types, for example to use SIP tls in preference over using SIP tcp or SIP udp.

NAPTR records are also used in ENUM, when converting a telephone number into a dialable URI.

(For further details on ENUM see *ENUM dialing on VCS deployment guide*, document reference D14465).

E20 video endpoints use NAPTR records to identify whether they are inside a private network (and so should request provisioning data for the internal network) or are outside in the public internet (where they should request provisioning data for devices in the public network). The flag “s” is extended to “se” to indicate to the E20 that it is “external”.

(For further details see *Cisco TMS Provisioning Deployment Guide*, document reference D14368.)

### NAPTR record format

Example: SIP access to example.com, and for enum lookups for 557120, 557121, and 557122.

\$ORIGIN example.com.

IN	NAPTR	10	100	"s"	"SIPS+D2T"	"	_sips._tcp.example.com.
IN	NAPTR	12	100	"s"	"SIP+D2T"	"	_sip._tcp.example.com.
IN	NAPTR	14	100	"s"	"SIP+D2U"	"	_sip._udp.example.com.

\$ORIGIN www.example.com.

IN	NAPTR	10	100	"s"	"http+I2R"	"	_http._tcp.example.com.
IN	NAPTR	10	100	"s"	"ftp+I2R"	"	_ftp._tcp.example.com.

\$ORIGIN 0.2.1.7.5.5.enum.lookup.com.

IN	NAPTR	10	100	"u"	"E2U+sip"	"!^.*\$!john.smith@tandberg.com!"	.
IN	NAPTR	12	100	"u"	"E2U+h323"	"!^.*\$!john.smith@tandberg.com!"	.
IN	NAPTR	10	100	"u"	"mailto+E2U"	"!^.*\$!mailto:john.smith@tandberg.com!"	.

\$ORIGIN 1.2.1.7.5.5.enum.lookup.com.

IN	NAPTR	10	100	"u"	"E2U+sip"	"!^.*\$!mary.jones@tandberg.com!"	.
----	-------	----	-----	-----	-----------	-----------------------------------	---

\$ORIGIN 2.2.1.7.5.5.enum.lookup.com.

IN	NAPTR	10	100	"u"	"E2U+h323"	"!^.*\$!peter.archibald@myco.com!"	.
----	-------	----	-----	-----	------------	------------------------------------	---

IN = Internet routing

NAPTR = record type

10 = order value (use lowest order value first)

100 = preference value if multiple entries have the same order value

"u" = the result is a routable URI

"s" = the result is a DNS SRV record

"a" = the result is an 'A' or 'AAAA' record

"E2U+sip" to make SIP call

"E2U+h323" to make h.323 call

Regular expression:

! = delimiter

" = no expression used

... usual Regex expressions can be used

Replace field; . = not used

## Looking up NAPTR records

### Looking up an ENUM NAPTR record

**dig 4.3.7.8.enum4.example.com. NAPTR**

```

; <<>> ;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38428
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 2

;; QUESTION SECTION:
4.3.7.8.enum4.example.com. IN    NAPTR

;; ANSWER SECTION:
4.3.7.8.enum4.example.com. 60 IN NAPTR 10 100 "u" "E2U+sip" "!.^.*$!steve.hight@example.com!" .
4.3.7.8.enum4.example.com. 60 IN NAPTR 10 100 "u" "E2U+h323" "!.^.*$!steve.hight@example.com!"
.

;; AUTHORITY SECTION:
enum4.example.com. 60      IN      NS      int-server1.example.com.

;; ADDITIONAL SECTION:
int-server1.example.com. 3600 IN A      10.44.9.144
int-server1.example.com. 3600 IN AAAA   3ffe:80ee:3706::9:144

;; Query time: 0 msec
;; SERVER: 10.44.8.11#53(10.44.8.11)
;; WHEN: Tue Jul 13 16:51:41 2010
;; MSG SIZE rcvd: 251

#

```

## Looking up a domain NAPTR record

Example: NAPTR record allowing E2O endpoints to detect that they are in the public (external) network.

```
~ # dig -t NAPTR example.com
```

```
;; <<>> DiG 9.4.1 <<>> -t NAPTR example.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1895
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 6, ADDITIONAL: 4

;; QUESTION SECTION:
example.com.                IN      NAPTR

;; ANSWER SECTION:
example.com.                2      IN      NAPTR    50 50 "se" "SIPS+D2T" "" _sips._tcp.example.com.
example.com.                2      IN      NAPTR    90 50 "se" "SIP+D2T" "" _sip._tcp.example.com.
example.com.                2      IN      NAPTR   100 50 "se" "SIP+D2U" "" _sip._udp.example.com.

;; AUTHORITY SECTION:
example.com.                320069 IN      NS       nserver2.example.com.
example.com.                320069 IN      NS       nserver.euro.example.com.
example.com.                320069 IN      NS       nserver.example.com.
example.com.                320069 IN      NS       nserver3.example.com.
example.com.                320069 IN      NS       nserver4.example.com.
example.com.                320069 IN      NS       nserver.asia.example.com.

;; ADDITIONAL SECTION:
nserver.example.com.       56190  IN      A        17.111.10.50
nserver2.example.com.     57247  IN      A        17.111.10.59
nserver3.example.com.     57581  IN      A        17.22.14.50
nserver4.example.com.     57452  IN      A        17.22.14.59

;; Query time: 11 msec
;; SERVER: 10.44.8.11#53(10.44.8.11)
;; WHEN: Tue Jul 13 17:08:40 2010
;; MSG SIZE rcvd: 385

~ #
```

## Document revision history

The following table summarizes the changes that have been applied to this document.

Revision	Date	Description
1	Up to December 2009	Releases for earlier versions of Cisco VCS.
2	December 2009	Updated for VCS X5.
3	May 2010	Updated for VCS X5.1.1 and TMS 12.6.
4	August 2010	Updated for VCS X5.2. Replace previous Appendix 12 (Upgrading debian packages - only required for X5.1.1) with a new Appendix 12 - NAPTR records overview.
5	October 2010	New document styles applied.
6	December 2010	Updated for VCS X6.
7	February 2011	Clarify this document refers to VCS X6.0 only, and to TMS 12.6 or later.
8	May 2011	Updated for VCS X6.1.
9	August 2011	Updated for VCS X7.0.
10	September 2011	Updated Appendix 3 – IP port and protocol numbers.
11	October 2011	Updated for X7.0.n.
12	January 2012	Various minor revisions and clarifications applied.
13	March 2012	Updated for X7.1.
14	August 2012	Updated for X7.2.
15	November 2012	Removed recommendation to use DNS name of the VCS cluster for endpoint SIP outbound configuration.

---

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.