Contents

Document revision history .................................................................................................................. 5
Introduction ............................................................................................................................................ 6
Prerequisites ........................................................................................................................................ 8
Upgrade Cisco VCS X1 / X2 Alternates to a Cisco VCS X5 cluster ................................................. 9
Upgrade a non-clustered X3/X4 Cisco VCS to a non-clustered X5 Cisco VCS ............................ 10
Upgrade a Cisco VCS X3 / X4 cluster to an X5 cluster (including Cisco TMS to 12.6 and non-clustered Cisco VCSs to X5) ...................................................................................... 11
  Upgrade Cisco TMS to 12.6 and Cisco VCS to X5 ................................................................. 11
  Upgrade Cisco TMS to 12.6 ................................................................................................. 11
  Upgrade Cisco VCS clusters to X5.2 .................................................................................. 12
  Upgrade non-clustered Cisco VCSs to X5.2 ........................................................................ 16
  Complete the Cisco TMS upgrade ..................................................................................... 17
Additional cluster configuration .......................................................................................................... 18
Upgrade an X5.0 cluster to an X5.2 cluster ............................................................................ 19
Before the upgrade ...................................................................................................................... 19
Upgrade Cisco TMS 12.5 to Cisco TMS 12.6 .......................................................................... 19
Restore TMS Agent data replication on non clustered Cisco VCSs .............................................. 20
Upgrade Cisco VCS clusters to X5.2 .................................................................................... 21
Create a new cluster of Cisco VCS X5 peers ............................................................................. 24
Prerequisites ................................................................................................................................. 24
Set up the cluster ....................................................................................................................... 24
No Cisco TMS .............................................................................................................................. 31
Additional cluster configuration ................................................................................................. 31
Add an X5 Cisco VCS to a Cisco VCS X5 cluster ................................................................. 32
Remove a live Cisco VCS from a Cisco VCS X5 cluster (permanently) ...................................... 37
Reconfigure Cisco TMS ............................................................................................................... 39
Remove an out-of-service Cisco VCS from a Cisco VCS X5 cluster (permanently) ................. 40
Reconfigure Cisco TMS ............................................................................................................... 40
Before you reconnect the out-of-service Cisco VCS back to the network .............................. 41
Disband a Cisco VCS X5 cluster ............................................................................................... 42
Reconfigure Cisco TMS ............................................................................................................... 44
Change the master peer of a Cisco VCS X5 cluster ............................................................... 45
Changing the master peer in a cluster where the old master Cisco VCS is accessible or is not
  accessible .............................................................................................................................. 45
Reconfigure Cisco TMS ............................................................................................................... 45
If the old master is not available ............................................................................................... 46
Contents

Change the IP address of a Cisco VCS X5 peer ................................................................. 47

Appendix 1 – Backing up a Cisco VCS ................................................................................. 48
Back up a pre X3.0 Cisco VCS .............................................................................................. 48
Back up an X3.0 or later Cisco VCS ....................................................................................... 48

Appendix 2 – Ensure that root access via SSH is enabled .............................................. 49

Appendix 3 – Adding a Cisco VCS to Cisco TMS .............................................................. 50

Appendix 4 – IP Port numbers ............................................................................................. 52

Appendix 5 – Impact of clustering on other Cisco VCS applications ............................. 53
Conference Factory (Multiway™) ......................................................................................... 53
Microsoft Office Communications Server 2007 (OCS) ...................................................... 53

Appendix 6 – Configuring endpoints to work with a Cisco VCS cluster ...................... 54
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 – DNS SRV (preferred) ......................................................................................... 55
  Option 2 – DNS Round-Robin (2nd choice) ...................................................................... 56
  Option 3 – Static IP (least preferred) .................................................................................. 56

Appendix 7 – Troubleshooting ......................................................................................... 57
Cisco VCS warnings ............................................................................................................. 57
  "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" ................................................................. 57
  "Cluster replication error: the Master peer is unreachable" .................................................. 57
  "Cluster replication error: there was an error during automatic replication of configuration" ................................................................. 57
  "Cluster replication error: <details> manual synchronization of configuration is required" .......... 57
  "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
Cluster script, option 5 .......................................................................................................... 59
  "WARNING: There are more Public Keys than there are alternates." .................................... 59
Cisco TMS warnings ............................................................................................................. 60
Cisco TMS Cluster Diagnostics ............................................................................................ 60
Conference factory template does not replicate ................................................................. 60
Cisco VCS’s External manager protocol keeps getting set to HTTPS .................................. 60
Why are Cisco VCS peers regularly doing reverse DNS lookups for one-another? .............. 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
Appendix 8 – Upgrading Cisco TMS to 12.6 .................................................................62
Appendix 9 – Upgrade Cisco VCS software to X5.........................................................63
Appendix 10 – Changing the cluster name (and keeping FindMe accounts) .............65
Appendix 11 – Cluster name and DNS SRV records....................................................66
Endpoints supporting SIP DNS SRV ........................................................................67
Looking up .SRV records.........................................................................................68
Nsllookup ..................................................................................................................68
Dig .........................................................................................................................68
Appendix 12 – NAPTR records ..................................................................................69
NAPTR record format ...............................................................................................69
Looking up NAPTR records ....................................................................................70
Looking up an ENUM NAPTR record .....................................................................70
Looking up a domain NAPTR record ......................................................................71
# Document revision history

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

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Up to December 2009</td>
<td>Releases for earlier versions of Cisco VCS.</td>
</tr>
<tr>
<td>2</td>
<td>December 2009</td>
<td>Updated for Cisco VCS X5.</td>
</tr>
<tr>
<td>3</td>
<td>May 2010</td>
<td>Updated for Cisco VCS X5.1.1 and Cisco TMS 12.6.</td>
</tr>
<tr>
<td>4</td>
<td>August 2010</td>
<td>Updated for Cisco VCS X5.2.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Replace previous Appendix 12 (Upgrading debian packages - only required for X5.1.1) with a new Appendix 12 - NAPTR records overview.</td>
</tr>
<tr>
<td>5</td>
<td>October 2010</td>
<td>New document styles applied.</td>
</tr>
</tbody>
</table>
Introduction

Cisco TelePresence Video Communication Server (Cisco VCS) clusters are designed to extend the resilience and capacity of a Cisco VCS installation. Cisco VCSs in the cluster share bandwidth usage, routing, zone, FindMe™ and other configuration among themselves. Endpoints can register to any of the Cisco VCSs 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-VCS peer basis, and so enough call licenses must be applied to each peer to support the number of calls that are needed on that peer, plus any additional calls that may be required when one or more other peers become inaccessible. The same number of licenses must be applied to each peer in the cluster.

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

This deployment guide describes how to create, modify and upgrade to X5 Cisco VCS clusters. It provides information on how to:

- upgrade an X1 Cisco VCS or X2 Cisco VCS set of Alternates to a Cisco VCS X5 cluster
- upgrade a Cisco VCS X3 / X4 cluster to a Cisco VCS X5 cluster
- upgrade a Cisco VCS X5 cluster to a Cisco VCS X5.2 cluster
- create a new cluster of Cisco VCS X5 peers
- add an X5 Cisco VCS as a new peer to an existing X5 cluster
- remove a peer from an X5 cluster
- disband an X5 cluster
- change the master peer of an X5 Cisco VCS cluster
- change the IP address of an X5 cluster peer

Note: In X3.x the use of Cisco TelePresence Management Suite (Cisco TMS) was essential to the correct operation of a Cisco VCS cluster because Cisco TMS was in control of copying configuration from the Master Cisco VCS to the non-master peers.

In X4.1 the Cisco VCS performs the replication of configuration from Master Cisco VCS to non-master peers and so use of Cisco TMS was optional for clustering. If provisioning was supported, Cisco TMS was needed.

In X5.x Cisco TMS is involved in initiating the environment for FindMe replication. Although not needed to replicate FindMe data throughout the cluster in a running environment, Cisco TMS is required to perform the initial distribution of the FindMe data throughout the cluster. Cisco TMS is also required if provisioning is to be supported on Cisco VCSs.

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

For creating and modifying clusters that will remain X4 and X3 clusters, see:
- Cisco VCS deployment guide - Cluster creation and maintenance (Cisco VCS X41)
- Cisco VCS deployment guide - Cluster creation and maintenance (Cisco VCS X3)
Prerequisites

Cisco VCS clusters peers should all run the same version of code, for example all X5.0, or all X5.2. 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 X5 Cisco VCS peers or adding an X5 Cisco VCS to a cluster, ensure that:

- each and every Cisco VCS peer in a cluster is within a 15ms hop (30ms round trip delay) of each and every other Cisco VCS in or to be added to the cluster
- each and every Cisco VCS peer in a cluster must be directly routable to each and every other Cisco VCS in or to be added to the cluster. (There must be no NAT between cluster peers.)
- all of the Cisco VCS peers have the same set of option keys installed
  - the Cisco VCS must be restarted after installing some option keys in order to fully activate them
  - the sum total of each type of option key must be the same on each peer, e.g. it is acceptable to have 1 peer with a 20 Traversal Calls option key and another with two 10 Traversal Calls option keys, as both add up to 20 Traversal Calls
- the Cisco TMS version being run is Cisco TMS 12.2 or later
  - at least Cisco TMS 12.2 if running an X3 or X4 cluster
  - Cisco TMS 12.6 if running X.5 code on the Cisco VCS
- each Cisco VCS has a different system name
- H.323 mode is enabled on each Cisco VCS (VCS Configuration > Protocols > H.323, and for H.323 mode select On) – H.323 communications are used between cluster peers
- root access via SSH is enabled on each Cisco VCS (see ‘Appendix 2 – Ensure that root access via SSH is enabled’)
- the Cisco VCS cluster has a DNS SRV record that defines all cluster peers
- the DNS servers used by both Cisco TMS and the Cisco VCSs support both forward and reverse DNS lookups for Cisco TMS and all Cisco VCSs, and any other DNS functionality required, (for example OCS FQDN lookup, LDAP server forward and reverse lookup); reverse lookups are frequently provided using PTR records
- the DNS servers used by the Cisco VCS peers must support both forward and reverse DNS lookups of Cisco TMS and all Cisco VCS peer addresses; the DNS servers must also provide address lookup for any other DNS functionality required by Cisco VCS, (for example: system servers like NTP and the external manager that are configured as DNS names, OCS FQDN lookup, LDAP server forward and reverse lookup); note that reverse lookups are frequently provided through PTR records
Upgrade Cisco VCS X1 / X2 Alternates to a Cisco VCS X5 cluster

Follow the steps below if you have a set of Cisco VCSs running software prior to X3 that are configured as Alternates.

There will be a Primary Cisco VCS handling the calls and one or more Alternates (which do not take calls) that are configured identically to the Primary Cisco VCS and are available to take calls should the Primary Cisco VCS become inaccessible.

In order to convert the group of Alternates into a Cisco VCS Cluster, you must first disband the Alternates and then create them into a new cluster with the Primary Alternate as the Master in the new cluster.

To do this, on each Cisco VCS:
1. Select VCS Configuration > Alternates.
2. Delete all entries listed under Alternate 1 IP Address .. Alternate 6 IP Address.
3. Click Save.
4. Repeat for the Primary and each Alternate Cisco VCS.

The Cisco VCSs are now individual Cisco VCSs.

5. Upgrade each individual Cisco VCS to X5, following the process defined in “Appendix 9 – Upgrade Cisco VCS software to X5”.
   - to clear the warning about the Cluster name not being set, put in a temporary name which is unique; it will be updated to the required name of the cluster in “Create a new cluster of Cisco VCS X5 peers”.

6. If FindMe accounts existed on the X1 / X2 Cisco VCS and these accounts are wanted in the new cluster, log in as root and at the command prompt, type:
   
   upgradefindmeaccounts
   
   This takes a while to complete – wait for the response OK, followed by the command prompt being re-displayed.
   
   If the OK response is not received after a short while, press ‘Enter’ (‘Carriage Return’).

7. Follow the procedure ”Create a new cluster of Cisco VCS X5 peers”, configuring what was the Primary Cisco VCS as the Master Cisco VCS in the new cluster.

Upgrading Alternates to a Cisco VCS X5 cluster is now complete.
Upgrade a non-clustered X3/X4 Cisco VCS to a non-clustered X5 Cisco VCS

Follow the steps below if you have a single non-clustered Cisco VCS to upgrade.

If provisioning is to be used with a non-clustered X5.x Cisco VCS, then use of Cisco TMS is essential. If provisioning is not to be used, then use of Cisco TMS is optional but recommended.

If FindMe is to be used on the Cisco VCS, use of Cisco TMS and replicating the FindMe data with Cisco TMS is strongly recommended. If Cisco VCS does not replicate FindMe data with Cisco TMS from the start, FindMe data on the Cisco VCS will be lost (overwritten by Cisco TMS’s blank database) when replication is enabled between Cisco TMS and Cisco VCS – replication is needed if a non-clustered Cisco VCS is ever to be made into a cluster and the FindMe data is to be kept.

- If the Cisco VCS is managed by a Cisco TMS and that Cisco TMS manages other Cisco VCSs which are clustered or manages Cisco VCSs that have provisioning enabled, use the process documented in “Upgrade a Cisco VCS X3 / X4 cluster to an X5 cluster”.

- If the Cisco VCS is to be used with Cisco TMS follow the upgrade procedure documented in “Upgrade a Cisco VCS X3 / X4 cluster to an X5 cluster”. Follow the sections of the upgrade procedure called “Upgrade Cisco TMS to 12.6” and “Upgrade non-clustered Cisco VCSs to X5”.

- If the Cisco VCS is not to use Cisco TMS follow the upgrade procedure documented in “Upgrade a Cisco VCS X3 / X4 cluster to an X5 cluster”. Follow the section of the upgrade procedure called “Upgrade non-clustered Cisco VCSs to X5”.
Upgrade a Cisco VCS X3 / X4 cluster to an X5 cluster (including Cisco TMS to 12.6 and non-clustered Cisco VCSs to X5)

Follow the steps below if you already have an X3.x or X4.x cluster.

Due to the close connection between Cisco VCS X5 and Cisco TMS 12.6 (or Cisco TMS 12.5) this procedure describes how to upgrade a whole network (including Cisco VCS clusters and non-clustered Cisco VCSs) to Cisco TMS 12.6 and Cisco VCS X5.x.

- Clusters will continue to handle calls when individual peers are upgraded to X5.x. However, the structure of the FindMe database is updated on upgrading from X3 and X4 to X5.x, so until the FindMe database is upgraded (after a whole cluster is upgraded) operation of FindMe on that cluster will be suspended.

- If Device Provisioning or FindMe is to be used with an X5.x Cisco VCS cluster, then use of Cisco TMS is essential. If neither Device Provisioning nor FindMe is to be used, then use of Cisco TMS is optional but recommended.

Upgrade Cisco TMS to 12.6 and Cisco VCS to X5

Upgrade Cisco TMS to 12.6

Follow this part of the procedure if Cisco TMS is not running version 12.6 software.

(This procedure assumes that the Cisco TMS is currently at version 12.2. If it is at version 12.5, see the section “Upgrade Cisco TMS 12.5 to Cisco TMS 12.6” on page 19.)

1. For each Cisco VCS cluster or non-clustered Cisco VCS managed by Cisco TMS:
   - Provisioning needs to be disabled in Cisco TMS
   - Configuration Replication by Cisco TMS must be disabled for clusters
   To configure this:
     a. For each cluster in Cisco TMS:
        i. Select Systems > Navigator (and any required sub folders).
        ii. Select the Master Cisco VCS of the cluster.
        iii. Select the Clustering tab.
        iv. Clear the Enable Provisioning check box (if it was set).
        v. Ensure that Enable Configuration Replication from TMS is not selected.
        vi. Click Save.
       Note: This disables database replication from Cisco TMS to each cluster peer.
       - Provisioning data will no longer be updated from Cisco TMS to the Cisco VCSs, however provisioning of endpoints from data cached on Cisco VCS will continue.
       - Cisco VCS cluster configuration replication will continue in X4 Cisco VCS clusters, but not X3 clusters.
       - Cisco VCS FindMe replication will continue in X3 and X4 clusters.
     Repeat for each Cisco VCS cluster in Cisco TMS.
     b. For each non-clustered Cisco VCS in Cisco TMS:
        i. Select Systems > Navigator (and any required sub folders).
        ii. Select the Cisco VCS.
        iii. Select the Clustering tab.
        iv. Clear the Enable Provisioning check box.
        v. Click Save.
       Note: This disables database replication from Cisco TMS to this Cisco VCS.
Upgrade a Cisco VCS X3 / X4 cluster to an X5 cluster (including Cisco TMS to 12.6 and non-clustered Cisco VCSs to X5)

- Provisioning data will no longer be updated from Cisco TMS to the Cisco VCS, however provisioning of endpoints from data cached on Cisco VCS will continue.
  
  Repeat for each Cisco VCS in Cisco TMS.

2. Make a note of which Cisco VCS clusters and non-clustered Cisco VCSs have had their provisioning disabled as this will have to be manually re-enabled later in this process.

3. Upgrade Cisco TMS to 12.6.
   Note: The upgrade will be blocked if provisioning is enabled on any Cisco VCS in Cisco TMS.
   a. Use Remote Desktop to connect to the server running Cisco TMS.
   b. On the Server that is running Cisco TMS, go to **Start > Shutdown** and select **Restart**.
      - Cisco TMS needs to be running from a clean boot-up in order for the upgrade to complete correctly
   c. Use Remote Desktop to connect to the server running Cisco TMS.
   d. Copy the Cisco TMS 12.6 **TMSSetup.exe** file onto the server.
   e. Run (double-click) the **TMSSetup.exe** file to start the upgrade.
   f. Follow the instructions of the installation wizard.
      You will need:
      - The Cisco TMS's SQL server username and password.
      - Release key for Cisco TMS 12.x *(if the Cisco TMS is not already 12.x)*.
      You are recommended to backup the database when given the opportunity to do so.
      (Note: Upgrading the LDAP server can take a while to complete.)
   Cisco TMS is now running 12.6.
   Provisioning and FindMe replication will be enabled on Cisco VCS clusters as they are upgraded to X5 *(see below)*

4. Verify the correct operation of the Local TMS Agent.
   When the Cisco TMS upgrade is complete, run the diagnostic tests within Cisco TMS to ensure that there are no issues with the Local TMS Agent:
   a. Log into Cisco TMS.
   b. Go to **Administrative Tools > TMS Agent Diagnostics**.
   c. In the **TMS Agent Browser** panel on the left hand side of the page, select **Local TMS Agent**.
   d. Click **Run All Diagnostics** to run the diagnostic tests on the Local TMS Agent.
   e. If all tests are successful (4 green check marks), proceed with upgrading your Cisco VCS clusters and non-clustered Cisco VCSs to X5.
      If any errors are found *(a red 'X' will appear against failing tests)*, do not proceed further with this upgrade, but contact your Authorized Service Provider for further assistance to resolve the issues identified.

Upgrade Cisco VCS clusters to X5.2

Follow this procedure for every Cisco VCS cluster managed by Cisco TMS.

**Upgrade master peer**

For the Master peer:
1. Backup the Cisco VCS (see "Appendix 1 – Backing up a Cisco VCS" for details).
2. Upgrade the master Cisco VCS peer to X5.2 following the process defined in 'Appendix 9 – Upgrade Cisco VCS software '  
   The upgrade process will disable Cisco VCS’s FindMe / provisioning functionality.
   - Provisioning is restored when **Enable TMS Agent Data Replication** is enabled.
   - **FindMe is restored on this Master Cisco VCS when the FindMe accounts are upgraded**.
3. A warning will be raised by Cisco VCS identifying that an X5 Cisco VCS cluster requires a cluster name.
   Go to **VCS Configuration > Clustering** and:
Upgrade a Cisco VCS X3 / X4 cluster to an X5 cluster (including Cisco TMS to 12.6 and non-clustered Cisco VCSs to X5)

1. Set **Cluster name** to be the routable Fully Qualified Domain Name used in SRV records that address this Cisco VCS cluster, for example "cluster1.example.com". (See Appendix 11 – Cluster name and DNS SRV records)

2. Ensure that **Configuration master** is set to the number of the peer which is annotated “This VCS”.

3. Click **Save**.

4. Go to **System configuration > DNS** and set the **Local host name** to be the DNS hostname for this Cisco VCS (typically the same as the **System name** in **System configuration > System**, but excluding spaces, and unique for each Cisco VCS in the cluster).

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

5. Click **Save**.

6. Log out and log back in to the web browser to activate the change.

7. Go to **VCS Configuration > Calls** and ensure that the **Call routed mode** is set to **Optimal**.

8. Click **Save**.

9. If FindMe or Device Provisioning is enabled.

   a. Ensure that the Host Name of the Cisco VCS is set up in Cisco TMS:
      i. Select **Systems > Navigator** (and any required sub folders).
      ii. Select the Master Cisco VCS of the cluster.
      iii. Select the **Connection** tab.
      iv. Set **Host Name** to be the FQDN of the Master peer, for example vcs1.uk.company.com.
      v. Click **Save/Try**.
         Do not worry about any error message like **"DNS config failure resolving <DNS name>: Did not find system IP address () in DNS: <Server IP>"**

   b. Ensure that Cisco TMS updates its DNS
      Select the **Settings** tab.
      i. Click **Force Refresh**.

10. Check for cluster name change
    - *in Cisco TMS 12.2 the cluster name in Cisco TMS was manually configured; in Cisco TMS 12.6, Cisco TMS picks up the name from the Cisco VCS Cluster name.*
    i. Select the **Clustering** tab.
    ii. If there is a warning that the Cluster name has changed
        Select **Update Cluster in TMS**.

Upgrading of the software on the master Cisco VCS is now complete.

**Note**: The upgrade process disables Cisco VCS’s provisioning functionality.

- Provisioning is restored when **Enable TMS Agent Data Replication** is enabled.

11. If FindMe or Device Provisioning is enabled, enable replication on this upgraded master Cisco VCS peer.
    On Cisco TMS enable replication on this upgraded Master Cisco VCS peer:
    a. Select the **TMS Agent** tab.
    b. Select **Enable TMS Agent Data Replication**.
    c. Select **Enable Authentication**
    d. Click **Save Settings**.

**Note**: This takes a while to complete (approximately 5 minutes); select the **Activity Status** page (see link at the top of the screen) to show you the list of activities, 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 until the Activity **Event completed successfully** is reported.
12. If FindMe is used in the cluster then the FindMe accounts need to be upgraded from their X4 format to the X5 format.
Log in to the Master peer Cisco VCS as root and at the command prompt, type:

```
upgradefindmeaccounts
```

This takes a while to complete – wait for the response OK, followed by the command prompt being re-displayed.

**Note:** If the OK response is not received after a short while, press ‘Enter’ (‘Carriage Return’).

13. Check that the expected FindMe entries still exist on this Master Cisco VCS (Maintenance > Login accounts > User accounts).

**Note:** If provisioning was enabled previously, provisioning records show up in the list with a FindMe name = N/A. DO NOT delete these entries if provisioning is required. Provisioning entries may be updated with FindMe information if required.

14. Check that other configuration (including Zone configuration, Transforms configuration and other configuration for items from the System Configuration, VCS Configuration and Application menus) is as expected.

Match patterns from Zones will have been converted to Search rules (See VCS Configuration > Search rules > Rules) – you may wish to edit these and give them better Rule names.

15. Backup the Cisco VCS (See “Appendix 1 – Backing up a Cisco VCS” for details).

### Upgrade non-master peers

For each non-master peer:

1. Upgrade the non-master Cisco VCS peer to X5.2 (the same code version as the Master was upgraded to) following the process defined in 'Appendix 9 – Upgrade Cisco VCS software'.

   The upgrade process will disable Cisco VCS’s FindMe / provisioning functionality

   - Provisioning is restored when **Enable TMS Agent Data Replication** is enabled.
   - **FindMe** is restored on this non-master Cisco VCS when **Enable TMS Agent Data Replication** is enabled.

2. Check that the cluster name has been updated on this non-master peer

   Go to VCS Configuration > Clustering and:
   a. Ensure that **Cluster name** is identical to the cluster name just configured on the master Cisco VCS.
   b. Ensure that **Configuration master** value is identical to that just configured on the master Cisco VCS.
   c. Ensure that the **Peer x IP address** entries are identical to those configured on the master Cisco VCS.

   If any are not, update them and click **Save**.

3. Go to System configuration > DNS and set the **Local host name** to be the DNS hostname for this Cisco VCS (typically the same as the **System name** in System configuration > System, but excluding spaces, and unique for each Cisco VCS in the cluster).

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

4. Click **Save**.

5. Log out and log back in to the web browser to activate the change

6. If FindMe or Device Provisioning is enabled:
   a. Ensure that the Host Name of the Cisco VCS is set up in Cisco TMS:
      i. Select Systems > Navigator (and any required sub folders).
      ii. Select this non-master Cisco VCS
      iii. Select the **Connection** tab.
iv. Set Host Name to be the FQDN of this non-master peer, for example vcs2.uk.company.com.

v. Click Save/Try.
   Do not worry about any error message like “DNS config failure resolving <DNS name>: Did not find system IP address () in DNS: <Server IP>”

b. Ensure that Cisco TMS updates its DNS.
   i. Select the Settings tab.
   ii. Click Force Refresh.

Upgrading of the software on the non-master Cisco VCS peers is now complete.

**Note:** The upgrade process disables Cisco VCS’s provisioning functionality.

- Provisioning is restored when **Enable TMS Agent Data Replication** is enabled.

7. If FindMe or Device Provisioning is enabled, enable replication on this upgraded non-master Cisco VCS peer.
   On Cisco TMS enable replication on this upgraded non-master Cisco VCS peer:
   a. Select the TMS Agent tab for this non-master Cisco VCS.
   b. Select Enable TMS Agent Data Replication.
   c. Select Enable Authentication
   d. Click Save Settings.

**Note:** This takes a while to complete (approximately 5 minutes); select the Activity Status page (see link at the top of the screen) to show you the list of activities, 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 until the Activity **Event completed successfully** is reported.

8. Check that the expected FindMe entries still exist on this Cisco VCS (Maintenance > Login accounts > User accounts).

9. Check that other configuration (including Zone configuration, Transforms configuration and other configuration for items from the System Configuration, Cisco VCS Configuration and Application menus) is as expected.
   Match patterns from Zones will have been converted to Search rules (See VCS Configuration > Search rules > Rules)

10. Repeat these steps for each non-master peer.

After all cluster peers have been upgraded:

1. If FindMe or Device Provisioning is to be used
   a. On Cisco TMS 12.6 enable **TMS Agent Data Replication on all Cluster Peers**:
      i. Select Systems > Navigator (and any required sub folders).
      ii. Select the Master Cisco VCS of the cluster.
      iii. Select the Clustering tab.
      iv. Select Enable TMS Agent Data Replication on all Cluster Peers.
      v. Click Save Cluster Settings.

For every Cisco VCS in the cluster (including the Master Cisco VCS):

1. To ensure that Cisco TMS has all the correct settings for this upgraded Cisco VCS, force a refresh of Cisco TMS. To do this:
   a. Select Systems > Navigator (and any required sub folders) and click on the name of the Cisco VCS.
   b. Select the Settings tab.
   c. Click Force Refresh.
2. Repeat for all Cisco VCS Clusters managed by Cisco TMS.

**Note:** If FindMe is enabled, but Device Provisioning is not, TMS Agent diagnostics may produce a Critical Error alarm ticket that the “Device Provisioning” option key is not installed, that SIP routes are wrong and that SIP domains may not be set up. This ticket should be ignored.

**Note:** If problems are observed with Cisco VCS peer configuration replication, ensure that all the functionality defined in “Create a new cluster of Cisco VCS X5 peers” has been performed on the cluster, especially the running of the relevant “cluster” script from the root login on each Cisco VCS in the cluster (including the Master).

---

**Upgrade non-clustered Cisco VCSs to X5.2**

Skip this section if there are no non-clustered (non-clustered) Cisco VCSs to upgrade.

For each Cisco VCS not in a cluster:
1. Backup the Cisco VCS (See Appendix 1 for details).
2. Upgrade the Cisco VCS to X5.x following the process defined in ‘Appendix 9 – Upgrade Cisco VCS software’.  
   *The upgrade process will disable Cisco VCS’s FindMe / provisioning functionality.*
   *Provisioning is restored when Enable TMS Agent Data Replication is enabled.*
   *FindMe is restored when the FindMe accounts are upgraded*
3. If FindMe is enabled, a warning will be raised by Cisco VCS identifying that an X5 Cisco VCS cluster requires a cluster name. 
   Go to VCS Configuration > Clustering and:
   a. Set **Cluster name** to be the routable Fully Qualified Domain Name used in SRV records that address this Cisco VCS cluster, for example "cluster1.example.com". (See Appendix 11 – Cluster name and DNS SRV records)
4. Click **Save**.
5. Go to System configuration > DNS and set the **Local host name** to be the DNS hostname for this Cisco VCS (typically the same as the **System name** in System configuration > System, but excluding spaces, and unique for each Cisco VCS).

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

6. Click **Save**.
7. If Device Provisioning or FindMe is to be used ensure that the Host Name of the Cisco VCS is set up in Cisco TMS:
   a. Select Systems > Navigator (and any required sub folders).
   b. Select this Cisco VCS
   c. Select the **Connection** tab.
   d. Set **Host Name** to be the FQDN of the Cisco VCS, for example vcs1.uk.company.com
   e. Click **Save/Try**.  
      Do not worry about any error message like “DNS config failure resolving <DNS name>: Did not find system IP address () in DNS: <Server IP>”
   f. Ensure that Cisco TMS updates its DNS.
   g. Select the **Settings** tab.
   h. Click **Force Refresh**.

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

**Note:** The upgrade process disables Cisco VCS’s provisioning functionality.

- Provisioning is restored when Enable TMS Agent Data Replication is enabled.
8. If FindMe or Device Provisioning is enabled, enable replication on this upgraded Cisco VCS. On Cisco TMS enable replication on this upgraded Cisco VCS:
   a. Select the TMS Agent tab.
   b. Select Enable TMS Agent Data Replication.
   c. Select Enable Authentication
   d. Click Save Settings.

   **Note:** This takes a while to complete (approximately 5 minutes); select the Activity Status page (see link at the top of the screen) to show you the list of activities, 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 until the Activity Event completed successfully is reported.

9. If FindMe is used then the FindMe accounts need to be upgraded from their X4 format to the X5 format.
   Log in as root and at the command prompt, type:
   
   ```bash
   upgradefindmeaccounts
   ```
   
   This takes a while to complete – wait for the response OK, followed by the command prompt being re-displayed.
   If the OK response is not received after a short while, press ‘Enter’ (‘Carriage Return’).

10. Check that the expected FindMe entries still exist on this Cisco VCS (Maintenance > Login accounts > User accounts).

   **Note:** If provisioning was enabled previously, provisioning records show up in the list with a FindMe name = N/A. DO NOT delete these entries if provisioning is required. Provisioning entries may be updated with FindMe information if required.

11. Check that other configuration (including Zone configuration, Transforms configuration and other configuration for items from the System Configuration, VCS Configuration and Application menus) is as expected.

**Complete the Cisco TMS upgrade**

On Cisco TMS

   In the Global (applied to all agents) section
   a. Set **Authentication Enabled** to Yes
   b. Set up the TMS Agent **LDAP Configuration Password**
   c. Set up the TMS Agent **LDAP Replication Password**

   **Note:** It is recommended that the LDAP Configuration Password and the LDAP Replication Password are set to different values.

   d. Click **Save**.

   *Cisco TMS will update the password on the local TMS Agent and all TMS Agents on connected Cisco VCSs*

2. To ensure that Cisco TMS has all the correct settings for this upgraded Cisco VCS, force a refresh of Cisco TMS. To do this:
   a. Select **Systems > Navigator** (and any required sub folders) then click on the name of the Cisco VCS.
   b. Select the **Settings** tab.
   c. Click **Force Refresh**.

3. Repeat step 2 for every Cisco VCS managed by Cisco TMS.
Additional cluster configuration

- If Conference Factory (Multiway™) is to be used, see the section ‘Conference Factory (Multiway™)’ in ‘Appendix 5 – Impact of clustering on other Cisco VCS applications’.
- If Microsoft Office Communications Server 2007 (OCS) is to be connected to this cluster, see the section ‘Microsoft Office Communications Server 2007 (OCS)’ in ‘Appendix 5 – Impact of clustering on other Cisco VCS applications’.

Upgrading a Cisco VCS X3 / X4 cluster to a Cisco VCS X5 cluster is now complete.
Upgrade an X5.0 cluster to an X5.2 cluster

This procedure assumes that Cisco TMS, if required for Device Provisioning or FindMe, is already running version 12.5 or 12.6 software and was made operational with the cluster as part of the upgrade or creation of the X5 cluster.

Non-clustered Cisco VCSs are not upgraded as part of this procedure.

Before the upgrade

Verify the correct operation of TMS Agent by running TMS agent diagnostics:

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 Diagnostics to run the diagnostic tests on the Local TMS Agent.
5. For each Cisco VCS peer:
   a. In the TMS Agent Browser panel on the left side of the page, select the peer.
   b. Click Run All Diagnostics to run the diagnostic tests on the Local TMS Agent.

   ▶ If all tests are successful (all green check marks), proceed with the "Upgrade Cisco VCS clusters to X5.2" 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 Authorized Service Provider for further assistance to resolve the issues identified.

Upgrade Cisco TMS 12.5 to Cisco TMS 12.6

If Cisco TMS is running 12.5, upgrade it to 12.6

1. For each Cisco VCS cluster or non-clustered Cisco VCS managed by the Cisco TMS:
   - Provisioning needs to be disabled in Cisco TMS
   - Configuration Replication by TMS must be disabled for clusters
   To configure this:
     a. For each cluster in Cisco TMS:
        i. Select Systems > Navigator (and any required sub folders).
        ii. Select the Master Cisco VCS of the cluster
        iii. Select the Clustering tab.
        iv. Clear the Enable TMS Agent Data Replication on all Cluster Peers check box (if it was set).
        v. Click Save Cluster Settings.
   Note: This disables database replication from Cisco TMS to each cluster peer.
   - Provisioning data will no longer be updated from Cisco TMS to the Cisco VCSs, however provisioning of endpoints from data cached on Cisco VCSs will continue.
   - Cisco VCS Cluster configuration replication will continue.
   - Cisco VCS FindMe replication will continue.
   Repeat for each Cisco VCS cluster in Cisco TMS
   b. For each non-clustered Cisco VCS in Cisco TMS:
      i. Select Systems > Navigator (and any required sub folders).
      ii. Select the Cisco VCS.
      iii. Select the TMS Agent tab.
      iv. Clear the Enable TMS Agent Data Replication check box.
v. Click **Save Settings**.

Note: This disables database replication from Cisco TMS to this Cisco VCS.

- Provisioning data will no longer be updated from Cisco TMS to the Cisco VCS, however provisioning of endpoints from data cached on Cisco VCS will continue.

Repeat for each non-clustered Cisco VCS in Cisco TMS

2. Make a note of which Cisco VCS clusters and non-clustered Cisco VCSs have had their provisioning disabled, these will have to be manually re-enabled later in this process.

3. Upgrade Cisco TMS to 12.6.

   Note: The upgrade will be blocked if provisioning is enabled on any Cisco VCS in Cisco TMS.

   a. Use Remote Desktop to connect to the server running Cisco TMS.

   b. On the Server that is running Cisco TMS, **Start > Shutdown** and select **Restart**.

   - **Cisco TMS needs to be running from a clean boot-up in order for the upgrade to complete correctly**

   c. Use Remote Desktop to connect to the server running Cisco TMS.

   d. Copy the Cisco TMS 12.6 **TMSSetup.exe** file onto the server.

   e. Double click on the **TMSSetup.exe** file to start the upgrade.

   f. Follow the instructions of the installation wizard.

   You will need:

   - The Cisco TMS's SQL server username and password.
   - Release key for Cisco TMS 12.x *(if the Cisco TMS is not already 12.x)*

   You are recommended to backup the database when given the opportunity to do so.

   (Note: Upgrading the LDAP server can take a while to complete.)

   **Cisco TMS is now running 12.6.**

   Provisioning and FindMe replication will be enabled on Cisco VCS clusters as they are upgraded to X5.2 *(see below)*

4. Verify the correct operation of the Local TMS Agent

   When the Cisco TMS upgrade is complete, run the diagnostic tests within Cisco TMS to ensure that there are no issues with the Local TMS Agent:

   a. Log into Cisco TMS.

   b. Go to **Administrative Tools > TMS Agent Diagnostics**.

   c. In the **TMS Agent Browser** panel on the left hand side of the page, select **Local TMS Agent**.

   d. Click **Run All Diagnostics** to run the diagnostic tests on the Local TMS Agent.

   e. If all tests are successful (4 green check marks), proceed with upgrading your Cisco VCS clusters and non-clustered Cisco VCSs to X5.2.

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

**Restore TMS Agent data replication on non clustered Cisco VCSs**

For each non-clustered Cisco VCS in Cisco TMS that previously had TMS Agent Data Replication enabled:

1. Select **Systems > Navigator** (and any required sub folders).

2. Select the Cisco VCS.

3. Select the **TMS Agent** tab.

4. Select the **Enable TMS Agent Data Replication** check box.

5. Click **Save Settings**.
Upgrade Cisco VCS clusters to X5.2

Upgrade master peer

For the master peer in the cluster:

1. Backup the Cisco VCS (see "Appendix 1 – Backing up a Cisco VCS" for details).

2. Enable maintenance mode. From the Cisco 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 (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 (Status > Registrations > By device, then select the check box next to the devices you want to remove and click Unregister).

5. Turn off Cisco TMS data replication.
   In Cisco TMS:
   a. Select Systems > Navigator (and any required sub folders).
   b. Select the Master Cisco VCS of the cluster.
   c. Select the Clustering tab.
   d. Clear the Enable TMS Agent Data Replication on all Cluster Peers check box.
   e. Click Save Cluster Settings.
   f. Select the TMS Agent tab
   g. Ensure that Enable Configuration Replication from TMS is not selected.
   h. Click Save Settings.
   Note: This disables database replication from Cisco TMS to each cluster peer.
   • Provisioning data will no longer be updated from Cisco TMS to the Cisco VCSs, however provisioning of endpoints from data cached on Cisco VCSs not in maintenance mode will continue.
   • Cisco VCS cluster configuration replication will continue.
   • Cisco VCS FindMe replication among Cisco VCS peers will continue.

6. Upgrade and restart the Cisco VCS (Maintenance > Upgrade).
   For any further details see the "Upgrading Software" section of the Cisco VCS Administrator Guide.

   Note: The web browser interface may timeout during the restart process, after the progress bar has reached the end. This may occur if:
   ▶ Cisco 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

Upgrading of the software on the master Cisco VCS is now complete.

   Note: The upgrade process disables Cisco VCS's provisioning functionality.
   ▶ Provisioning is restored when Enable TMS Agent Data Replication is enabled.

7. If FindMe or Device Provisioning is enabled, enable replication on this upgraded master Cisco VCS peer.
   On Cisco TMS:
   a. Select the TMS Agent tab for the master Cisco VCS.
   b. Select Enable TMS Agent Data Replication.
   c. Select Enable Authentication.
d. 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 until the activity **Event completed successfully** is reported.

8. Check that the expected FindMe entries still exist on this master Cisco VCS (**Maintenance > Login accounts > User accounts**).
9. Check that other configuration (including Zone configuration, Transforms configuration and other configuration for items from the System Configuration, VCS Configuration and Application menus) is as expected.
10. Disable maintenance mode. From the Cisco VCS command line type: `xconfiguration SystemUnit Maintenance Mode: Off`
11. Backup the master Cisco VCS (See “Appendix 1 – Backing up a Cisco VCS” for details).

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

### Upgrade non-master peers

For each non-master peer in the cluster:

1. **Enable maintenance mode.** From the Cisco 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 (**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** (**Status > Registrations > By device**, then select the check box next to the devices you want to remove and click **Unregister**).
4. **Turn off Cisco TMS data replication.**
   In Cisco TMS:
   a. **Select Systems > Navigator** (and any required sub folders).
   b. **Select the TMS Agent** tab for this non-master Cisco VCS.
   c. Ensure that **Enable Configuration Replication from TMS** is not selected.
   d. Click **Save Settings**.
5. **Upgrade and restart the Cisco VCS (**Maintenance > Upgrade**).**
   For any further details see the “Upgrading Software” section of the Cisco VCS Administrator Guide.

**Note:** The web browser interface may timeout during the restart process, after the progress bar has reached the end; this may happen if:

- Cisco 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

Upgrading the software on this Cisco VCS peer is now complete.

**Note:** The upgrade process disables Cisco VCS’s provisioning functionality.

- Provisioning is restored when **Enable TMS Agent Data Replication** is enabled.
6. If FindMe or Device Provisioning is enabled, enable replication on this upgraded non-master Cisco VCS peer.
   - On Cisco TMS:
     a. Select the TMS Agent tab for this non-master Cisco VCS.
     b. Select Enable TMS Agent Data Replication.
     c. Select Enable Authentication.
     d. 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 until the Activity Event completed successfully is reported.

7. Check that the expected FindMe entries exist on this Cisco VCS (Maintenance > Login accounts > User accounts).
8. Check that other configuration (including zone configuration, transforms configuration and other configuration for items from the System Configuration, VCS Configuration and Application menus) is as expected.
9. Disable maintenance mode – from the Cisco VCS command line type:
   ```
   xconfiguration SystemUnit Maintenance Mode: Off
   ```
10. Repeat these steps for each non-master peer.

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

**After the cluster peers have been upgraded**

After all cluster peers have been upgraded:
1. If FindMe or Device Provisioning is enabled, on Cisco TMS enable TMS Agent Data Replication on all Cluster Peers:
   a. Select Systems > Navigator (and any required sub folders).
   b. Select the Master Cisco VCS of the cluster.
   c. Select the Clustering tab.
   d. Select Enable TMS Agent Data Replication on all Cluster Peers.
   e. Click Save Cluster Settings.

   For every Cisco VCS in the cluster (including the Master Cisco VCS):
2. To ensure that Cisco TMS has all the correct settings for this upgraded Cisco VCS, force a refresh of Cisco TMS.
   To do this:
   a. Select Systems > Navigator (and any required sub folders) and click on the name of the Cisco VCS.
   b. Select the Settings tab.
   c. Click Force Refresh.
3. Repeat for all Cisco VCS peers in the cluster.

   **Note:** If problems are observed with Cisco VCS peer configuration replication, ensure that all the functionality defined in “Create a new cluster of Cisco VCS X5 peers” has been performed on the cluster, especially the running of the relevant “cluster” script from the root login on each Cisco VCS in the cluster (including the master).

Upgrading an X5.0 cluster to an X5.2 cluster is now complete.
Create a new cluster of Cisco VCS X5 peers

This process creates a new cluster from a set of X5.x Cisco VCSs. Do not use this process if the cluster already exists; instead, follow the instructions in “Add an X5 Cisco VCS to a Cisco VCS X5 cluster”.

**Note:** If Device Provisioning or FindMe is to be used with an X5 Cisco VCS cluster, then use of Cisco TMS is essential. If neither Device Provisioning nor FindMe is to be used, then use of Cisco TMS is optional but recommended.

If Cisco TMS is to be used with this Cisco VCS cluster, ensure that it is running version 12.6 – if an upgrade to Cisco TMS is required, see the process documented in “Upgrade a Cisco VCS X3 / X4 cluster to an X5 cluster”.

**Prerequisites**
- the Cisco VCSs to be included in the cluster must all be running the same version of software, and that version of software must be X5 or later
  - if any of the cluster peers have had their VCS Database and Device provisioning components upgraded, then all Cisco VCSs to be included in the cluster must have those components upgraded.
- if Device Provisioning and FindMe are configured, they have already been proven to be operational on the master Cisco VCS after its upgrade to X5
- if Cisco TMS is being used it is configured as specified in “Upgrade a Cisco VCS X3 / X4 cluster to an X5 cluster”

**Set up the cluster**
1. Determine which Cisco VCS will be the Master.

**Note:**
- The Master Cisco VCS will be the source of the configuration information for all Cisco VCS peers in the cluster. Non-master Cisco VCS peers will have their configuration deleted and replaced by that from the Master.
- During this upgrade process there will be the opportunity to merge each Cisco VCS’s FindMe accounts into the FindMe database for this cluster, provided that the Cisco VCS is already replicating its FindMe information with Cisco TMS.
- FindMe information can only be kept if the relevant Cisco VCS is already configured to operate with Cisco TMS and is configured with Enable TMS Agent Data Replication. (FindMe information is deleted and overwritten by the information from Cisco TMS when Enable TMS Agent Data Replication is first enabled.)

For every Cisco VCS to be added to the cluster (including the Master Cisco VCS):
2. Check that no other Cisco VCS (anywhere) has any of these Cisco VCSs’ IP addresses in its Alternates or Clustering Peers list.

On neighbor Gatekeepers (GKs) and Border Controllers (BCs):
3. If the Master Cisco 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.

For every Cisco VCS to be added to the cluster (including the Master Cisco VCS):
4. Check that the Cisco VCS is running X5 (or later) software.
5. Backup the Cisco VCS (See Appendix 1 for details).
6. On the web interface of the Cisco VCS being added, review the configuration to ensure that the Cisco VCS has:
   - A valid Ethernet speed (System Configuration > Ethernet).
   - Valid IP address and IP gateway (System Configuration > IP).
   - The same set of Option keys installed as those installed on the Master peer (Maintenance > Option Keys).
   - Root access via SSH enabled (see “Appendix 2 – Ensure that root access via SSH is enabled”).
   - 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 Configuration > DNS).

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

   - A valid and working NTP server configured (System Configuration > Time; in the Status section, the State should be “Active”).
   - 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.).

7. Repeat until each Cisco VCS has been backed up, had basic configuration and Option keys checked and has no Peers configured.

If Device Provisioning or FindMe is to be used with an X5 Cisco VCS cluster, then use of Cisco TMS is essential. If neither Device Provisioning nor FindMe is to be used, then use of Cisco TMS is optional but recommended.

If Cisco TMS is to be used, on each Cisco VCS:
1. Ensure that the Cisco VCS can see Cisco TMS.
   To do this, select System Configuration > External Manager and in the Status section, ensure that the State is Active.
   (If not, follow the process on ‘Appendix 3 – Adding a Cisco VCS to Cisco TMS’).
2. Ensure that Cisco TMS can communicate with this Cisco VCS. To do this, on Cisco TMS select Systems > Navigator (and any required sub folders) then click on the name of the Cisco VCS and ensure that it says:
   “✓ System has no open or acknowledged tickets”
   (If not, follow the process on ‘Appendix 3 – Adding a Cisco VCS to Cisco TMS’).
3. Repeat for each Cisco VCS.

On each Cisco VCS being added to the cluster:
   - Check the Warnings page of the Cisco VCS to be added (Status > Warnings). If there is a warning that the Cisco VCS must be restarted, select Maintenance > Restart and then click Restart System.
     - Warnings about TMS Agent passwords being default will be cleared when TMS Replication is enabled.

If Cisco TMS is to be used:
1. For each Cisco VCS, ensure that the Host Name of the Cisco VCS is set up in Cisco TMS:
   a. Select Systems > Navigator (and any required sub folders).
   b. Select this Cisco VCS.
   c. Select the Connection tab.
   d. Set Host Name to be the FQDN of this Cisco VCS, for example vcs3.uk.company.com.
Create a new cluster of Cisco VCS X5 peers

e. Click **Save/Try**. Do not worry about any error message like “DNS config failure resolving <DNS name>: Did not find system IP address () in DNS: <Server IP>”
f. Ensure that Cisco TMS updates its DNS.
g. Select the **Settings** tab.
h. Click **Force Refresh**.
Repeat on Cisco TMS for each Cisco VCS.

On the Master Cisco VCS:

1. Ensure that the Master Cisco VCS does not list any of the Cisco 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).

2. Set the H.323 **Time to live** to 60 (seconds) so that if a Cisco VCS becomes inaccessible to an endpoint, the endpoint will re-register quickly with another peer (**VCS Configuration > Protocols > H.323**).

3. Go to **System configuration > DNS** and ensure that the **Local host name** is the DNS hostname for this Cisco VCS (typically the same as the **System name** in **System configuration > System**, but excluding spaces, and unique for each Cisco VCS in the cluster); if not set it up appropriately and click **Save**.

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

4. If Cisco TMS is configured to **Enable TMS Agent Data Replication** with this Cisco VCS (to check: on Cisco TMS go to **Systems > Navigator** (and any required sub folders) select this Cisco VCS and select the TMS Agent tab) then any user accounts that existed on this Cisco 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.

   a. If the accounts held on this Cisco 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**.

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 Cisco VCS cluster, for example “cluster1.example.com”. (See Appendix 11 – Cluster name and DNS SRV records).

   b. If it is not, the **Cluster name** needs changing; follow the procedure in “Appendix 10 – Changing the cluster name”.

**Note:** If the Cluster name is changed without following the procedure “Appendix 10 – 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:

<table>
<thead>
<tr>
<th>Configuration master</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Peer 1 IP address</strong></td>
<td>Set to the IP address of this (the master peer) Cisco VCS</td>
</tr>
<tr>
<td><strong>Peer 2 IP address</strong></td>
<td>Set to the IP address of the 2nd Cisco VCS</td>
</tr>
<tr>
<td><strong>Peer 3 IP address</strong></td>
<td>Set to the IP address of the 3rd Cisco VCS (if there is a 3rd peer)</td>
</tr>
<tr>
<td><strong>Peer 4 IP address</strong></td>
<td>Set to the IP address of the 4th Cisco VCS (if there is a 4th peer)</td>
</tr>
<tr>
<td><strong>Peer 5 IP address</strong></td>
<td>Set to the IP address of the 5th Cisco VCS (if there is a 5th peer)</td>
</tr>
<tr>
<td><strong>Peer 6 IP address</strong></td>
<td>Set to the IP address of the 6th Cisco VCS (if there is a 6th peer)</td>
</tr>
</tbody>
</table>
Note: If the Cisco VCS peers have dual network interfaces, the Peer x IP address entries MUST specify LAN 1 interfaces.

8. Click **Save**.
   To the right of the **Peer 1 IP address** field the words “This VCS” should appear. Other peers may indicate “Unknown” and, after a refresh should indicate “Active”.

9. Go to **VCS Configuration > Calls** and set **Call routed mode** to **Optimal**.
10. Click **Save**.

On each non-master Cisco VCS:

1. If Cisco TMS is configured to **Enable TMS Agent Data Replication** with this Cisco VCS (to check: on Cisco TMS go to **Systems > Navigator** (and any required sub folders) select this Cisco VCS and select the TMS Agent tab) then any user accounts that existed on the Cisco VCS being added to the cluster may be merged to this cluster or they should be deleted. If **Enable TMS Agent Data Replication** is not enabled, no FindMe data will be available for merging.
   a. If the accounts held on this new peer 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**.
   b. If accounts are to be merged into the cluster’s FindMe database:
      i. Log in as root and at a command prompt, type:
         
         ```text
         transferfindmeaccounts <current Cluster name of this VCS> <Cluster name of the master VCS>
         ```

2. Log in as **admin** on an SSH or other CLI interface. At the Cisco VCS command prompt, type:
   ```text
   xcommand DefaultValuesSet Level: 2
   ```

   **Note**: This command will wipe any LDAP Authentication configuration – ensure that you have the web admin password before executing this command. DO NOT EXECUTE THIS COMMAND ON THE MASTER CISCO VCS

3. Go to **System configuration > DNS** and ensure that **Local host name** is the DNS hostname for this Cisco VCS (typically the same as the **System name** in **System configuration > System**, but excluding spaces, and unique for each Cisco VCS in the cluster); if not, set it up appropriately and click **Save**.

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

4. On the Clustering page (**VCS Configuration > Clustering**) configure the fields as follows:

<table>
<thead>
<tr>
<th>Cluster name</th>
<th>Identical to the Cluster name just configured on the master Cisco VCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration master</td>
<td>1</td>
</tr>
<tr>
<td>Peer 1 IP address ...</td>
<td>Identical to those just configured on the Master Cisco VCS</td>
</tr>
<tr>
<td>Peer 6 IP address</td>
<td></td>
</tr>
</tbody>
</table>

5. Click **Save**.
6. Repeat these steps for each non-master Cisco VCS.

On the Master Cisco VCS:

1. Log in to the Cisco VCS CLI as root and type:
   ```text
   cluster
   ```
   The following screen will appear:
2. Choose option 1 “Set this VCS to be the Configuration Master peer of a new cluster”.

**Note**: When the password is requested there is a 2 minute timeout. If you fail to enter the password within 2 minutes, exit the script (by holding down the ‘Ctrl’ key and pressing ‘c’ repeatedly until reaching the command line); then restart by typing ‘cluster’.

3. Follow the instructions until you are returned to the menu.
   Note: If the list of cluster peers is wrong:
   a. Exit this script by holding down the ‘Ctrl’ key and pressing ‘c’.
   b. Correct the list of peers on the Clustering page of the Master Cisco VCS.
   c. Re-run this cluster script file.

On the Master Cisco VCS web interface:

4. Check that the configuration (including Zone configuration, Transforms configuration, CPL and other configuration for items from the System Configuration, VCS Configuration and Application menus) is as expected.

5. Backup the Cisco VCS (See Appendix 1 for details).

On each non-master Cisco VCS:

1. Log in to the Cisco VCS CLI as root and type:
   
   ```
   cluster
   ```

2. Choose option 2 “Enable this VCS to replicate with an existing peer”.

**Note**: When the password is requested there is a 2 minute timeout. If you fail to enter the password within 2 minutes, exit the script (by holding down the ‘Ctrl’ key and pressing ‘c’ repeatedly until reaching the command line); then restart by typing ‘cluster’.

3. Follow the instructions until you are returned to the menu.
   You will be asked:
   a. to confirm that the Replicable data can be destroyed on this Cisco VCS
      (replicable data is Xconfiguration, Admin policy (cpl) and the login banner (not FindMe data))
   b. to confirm the list of peers
   c. to confirm the selection of the Master peer to receive the Replicable data from
   d. for passwords of the other cluster peers; enter the root password of the relevant Cisco VCS.
Create a new cluster of Cisco VCS X5 peers

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

The Cisco VCS configuration data replication starts immediately. (FindMe data is not replicated using this process, FindMe replication is controlled using **Enable TMS Agent Data Replication** on Cisco TMS).

4. Wait approximately 2 minutes – this is the frequency with which configuration data is copied from the Master.
5. Check the Warnings page of the newly added Cisco VCS (**Status > Warnings**).
   a. if there is a warning that the Cisco VCS must be restarted, select **Maintenance > Restart** and click **Restart System**
   b. if there is a cluster error, see the troubleshooting section below

At this stage ignore any other warnings - Warnings about TMS Agent passwords being default will be cleared when TMS Replication is enabled.

6. Check that the configuration (including zone configuration, transforms configuration, CPL and other configuration for items from the System Configuration, VCS Configuration and Application menus) is as expected (not FindMe — this will be replicated later) as per the Master Cisco VCS.
7. Repeat for each non-master Cisco VCS.

On each Cisco VCS in the cluster (including the master):
1. Log in to the Cisco VCS CLI as root and type:
   ```
   cluster
   ```
2. Choose option 5 “Check the replication state of this VCS”.
3. Check that the correct Cluster peers are reported and that it states “Replication is working”.
4. If there are problems, these need to be resolved.
   If a warning “**Replication process is not running**” is reported, this will right itself within one hour. Alternatively you can activate the replication immediately. To do so, either:
   - restart all Cisco VCSs reporting the problem, or
   - in the root login, at a command prompt, type:
     ```
     /etc/init.d/S80clusterd restart
     ```
   If there is a failure message **“ERROR: One or more Replicable directories /tandberg/persistent/oti/client/x5 /tandberg/persistent/oti/server/x5 do not exist”**
   i. Log in to the Cisco VCS as root and type:
      ```
      mkdir /tandberg/persistent/oti/client/x5
      mkdir /tandberg/persistent/oti/server/x5
      chown nobody:nobody /tandberg/persistent/oti/client/x5 -R
      chown nobody:nobody /tandberg/persistent/oti/server/x5 -R
      ```
   repeat these steps, choosing option 5 again, to make sure that this has cured the problem.
5. Repeat for each Cisco VCS in the cluster, including the Master, until all problems are resolved.

On other devices:

- If you have any other Cisco VCSs, Gatekeepers or Border controllers neighbored (or connected via a traversal zone) to this cluster of Cisco VCS peers, ensure that their zone configuration for this cluster is updated to include the addresses of all peers in the cluster.

If Cisco TMS is used, on Cisco TMS:
1. Go to **Systems > Navigator** (and any required sub folders) and select the Master Cisco VCS (listed as Peer 1 in the Cisco VCS cluster).
2. Select the **Clustering** tab.
3. Check the **Cluster name** field – it will have been populated from the Cisco VCS **Cluster name** (**VCS configuration > Clustering** page of the Cisco VCS).
4. If Device Provisioning or FindMe is to be used in this cluster, ensure that **Enable TMS Agent Data Replication on all Cluster Peers** is selected.

**Note:** If provisioning is to be supported by this cluster, follow the instructions in the Cisco TMS Provisioning Deployment Guide once the cluster has been completely set up and tested and shown to be working correctly.

5. Check that all the non-master cluster members are listed in addition to the Master Cisco VCS in the Cluster Peers section.
   - If they are not, go back to the Clustering page on the Master Cisco VCS (VCS Configuration > Clustering) and check the list of peers.

6. Click **Create Cluster**.

For the Master peer:

7. On Cisco TMS go to **Systems > Navigator** (and any required sub folders) and select the Master Cisco VCS (listed as Peer 1 in the Cisco VCS cluster).

8. Select the **TMS Agent** tab.

9. Ensure that **Enable TMS Agent Data Replication** is selected.

10. Ensure that **Enable Authentication** is selected.

11. Click **Save Settings**.

For each non-master peer:

12. On Cisco TMS go to **Systems > Navigator** (and any required sub folders) and select the non-master Cisco VCS.

13. Select the **TMS Agent** tab.

14. Ensure that **Enable TMS Agent Data Replication** is selected.

15. Ensure that **Enable Authentication** is selected.

16. Click **Save Settings**.

   Repeat for each non-master peer.

**Note:** If TMS Agent Data Replication reports Disabled then there is a problem. On Cisco 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 Cisco VCS peer (including the Master):

1. Log in to the web browser of the Cisco VCS.

2. Check the Warnings page (**Status > Warnings**):
   - If required, restart the Cisco VCS.
   - 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 7 – Troubleshooting’.

   repeat for the Master and each non-master peer.

On each non-master peer:

1. Check that the expected FindMe entries (from the Master Cisco VCS) exist on this Cisco VCS (**Maintenance > Login accounts > User accounts**).
No Cisco TMS

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

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

Additional cluster configuration

- If Conference Factory (Multiway™) is to be used, see the section “Conference Factory (Multiway™)” in “Appendix 5 – Impact of clustering on other Cisco VCS applications”.
- If Microsoft Office Communications Server 2007 (OCS) is to be connected to this cluster, see the section “Microsoft Office Communications Server 2007 (OCS)” in “Appendix 5 – Impact of clustering on other Cisco VCS applications”.

Creation of a new cluster of Cisco VCS peers is now complete.
Add an X5 Cisco VCS to a Cisco VCS X5 cluster

Follow this process if you have an existing X5 cluster to which you want to add a Cisco VCS. If you do not have an existing cluster, following the instructions in the section “Create a new cluster of Cisco VCS X5 peers”.

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

This process will add the X5.x Cisco VCS to the cluster and replicate the cluster Master’s configuration onto the Cisco VCS.

**Note:** Cisco VCS clusters peers should all run the same version of code, for example all X5.0, or all X5.2; also, if any Cisco VCS in the cluster has the upgraded VCS Database and VCS Provisioning components, all Cisco VCS peers must be upgraded – including the Cisco VCS being added to the cluster.

On the Master Cisco VCS:
1. Ensure that the Master Cisco VCS does not list this new Cisco VCS peer in any of its neighbor zones or traversal zones ([VCS Configuration > Zones](#)) then check each neighbor and traversal zone).

**Note:**
- The Master Cisco VCS will be the source of the configuration for this and all Cisco VCS peers in the cluster. After this Cisco VCS is added to the cluster, its configuration will be deleted and replaced by that from the Master.
- During this upgrade process there will be the opportunity to merge this new Cisco VCS’s FindMe accounts into the FindMe database for this cluster, provided that this Cisco VCS is already replicating its FindMe information with Cisco TMS. FindMe information can only be kept if the relevant Cisco VCS is already configured to operate with Cisco TMS and is configured with **Enable TMS Agent Data Replication**. (FindMe information is deleted and overwritten by the information from Cisco TMS when **Enable TMS Agent Data Replication** is first enabled.

On the Cisco VCS to be added to the cluster:
2. Check that no other Cisco VCS (anywhere) has this Cisco VCS’s IP address in their Alternates or Clustering Peers list.
3. Check that the Cisco VCS is running X5 (or later) software and that the software version is identical to the version running on the other cluster peers.
4. Backup the Cisco VCS (See Appendix 1 for details).

On the web interface of the Cisco VCS being added:
5. Review the configuration to ensure that the Cisco VCS has:
   - A valid Ethernet speed ([System Configuration > Ethernet](#)).
   - Valid IP address and IP gateway ([System Configuration > IP](#)).
   - The same set of Option keys as those installed on Master peer ([Maintenance > Option Keys](#)).
   - Root access via SSH enabled (see ‘Appendix 2 – Ensure that root access via SSH is enabled’).
   - 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 Configuration > DNS](#)).
Add an X5 Cisco VCS to a Cisco VCS X5 cluster

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

- A valid and working NTP server configured (**System Configuration > Time**; in the Status section, the State should be ‘Active’).
- 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 Cisco TMS, this Cisco VCS must also be managed by Cisco TMS.

**Note**: If Device Provisioning or FindMe is to be used with an X5 Cisco VCS cluster, then use of Cisco TMS is essential. If neither Device Provisioning nor FindMe is to be used, then use of Cisco TMS is optional but recommended.

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

1. Ensure that the Cisco VCS can see Cisco TMS.
   
   To do this, select **System Configuration > External Manager** and in the Status section, ensure that the State is **Active**.
   
   (If not, follow the process on ‘Appendix 3 – Adding a Cisco VCS to Cisco TMS’).

2. Ensure that Cisco TMS can communicate with this Cisco VCS. To do this, on Cisco TMS select **Systems > Navigator** (and any required sub folders) then click on the name of the Cisco VCS and ensure that it says:
   
   “✓ System has no open or acknowledged tickets”
   
   (If not, follow the process on ‘Appendix 3 – Adding a Cisco VCS to Cisco TMS’).

On the Cisco VCS being added to the cluster:

1. Check the Warnings page of the Cisco VCS to be added (**Status > Warnings**). If there is a warning that the Cisco VCS must be restarted, select **Maintenance > Restart** and then click **Restart System**.
   
   - Warnings about TMS Agent passwords being default will be cleared when TMS Replication is enabled.

If Cisco TMS is to be used:

1. For the Cisco VCS to be added to the cluster, ensure that the Host Name of the Cisco VCS is set up in Cisco TMS:
   
   a. Select **Systems > Navigator** (and any required sub folders).
   
   b. Select this Cisco 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**.
      
      Do not worry about any error message like "DNS config failure resolving <DNS name>: Did not find system IP address () in DNS: <Server IP>"
   
   f. Ensure that Cisco TMS updates its DNS.
   
   g. Select the **Settings** tab.
   
   h. Click **Force Refresh**.

On the Master Cisco 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 Cisco VCS.

2. Click **Save**.
   
   Peer 1 should indicate ‘This VCS’. The new peer may indicate ‘Unknown’ and then with a refresh should indicate ‘Active’.
Add an X5 Cisco VCS to a Cisco VCS X5 cluster

**Note:** Cluster replication is suspended at this point until the new Cisco VCS has been completely added. Any changes made to the configuration of the cluster will not be replicated until this Cisco VCS has been completely added.

On the Cisco VCS being added to the cluster:

1. If Cisco TMS is configured to **Enable TMS Agent Data Replication** with this Cisco VCS (to check: on Cisco TMS go to **Systems > Navigator** (and any required sub folders) select this Cisco VCS and select the TMS Agent tab) then any user accounts that existed on the Cisco VCS being added to the cluster may be merged to this cluster. Alternatively user accounts should be deleted.
   - **If Enable TMS Agent Data Replication** is not enabled, no FindMe data will be available for merging.
     a. If the accounts held on this new peer 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**.
     b. If accounts are to be merged into the cluster’s FindMe database:
        i. Log in as root and at a command prompt, type: `transferfindmeaccounts <current Cluster name of this VCS> <Cluster name of the master VCS>`

2. Log in as admin on an SSH or other CLI interface. At the Cisco VCS command prompt, type: `xcommand DefaultValuesSet Level: 2`
   
   **Note:** This command will wipe any LDAP Authentication configuration – ensure that you have the web admin password before executing this command.

3. Go to **System configuration > DNS** and ensure that **Local host name** is the DNS hostname for this Cisco VCS (typically the same as the **System name** in **System configuration > System**, but excluding spaces, and unique for each Cisco VCS in the cluster); if not set up appropriately and click **Save**.
   
   **Note:** `<Local host name>.<DNS domain name> = FQDN of this Cisco VCS.`

4. On the Clustering page (**VCS Configuration > Clustering**) configure the fields as follows:

<table>
<thead>
<tr>
<th>Cluster name</th>
<th>Identical to the Cluster name configured on the Master Cisco VCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration master</td>
<td>Identical to that configured on the Master Cisco VCS</td>
</tr>
<tr>
<td>Peer 1 IP address … Peer 6 IP address</td>
<td>Identical to those configured on the Master Cisco VCS</td>
</tr>
</tbody>
</table>

5. Click **Save**.

On every other non-master Cisco VCS in the cluster (including the Cisco VCS being added to the cluster):

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

<table>
<thead>
<tr>
<th>Cluster name</th>
<th>Identical to the Cluster name configured on the master Cisco VCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration master</td>
<td>Identical to that configured on the Master Cisco VCS</td>
</tr>
<tr>
<td>Peer 1 IP address … Peer 6 IP address</td>
<td>Identical to those configured on the Master Cisco VCS</td>
</tr>
</tbody>
</table>

2. Click **Save**.
Add an X5 Cisco VCS to a Cisco VCS X5 cluster

On the Cisco VCS being added to the cluster:

1. Log in to the Cisco VCS CLI as root.  
   Ignore warning messages that appear on login such as:
   ‘WARNING: Configuration Replication Error: Check that the Configuration Master Peer is reachable.’
   ‘WARNING: Security alert: the TMS Agent database has the default password set.’
   ‘WARNING: Security alert: the TMS Agent database has the default replication password set.’

2. On the command line type:
   `cluster`
   The following screen will appear:

   ![Cluster Menu Screen](image)

3. Choose option 2 “Enable this VCS to replicate with an existing Peer”.

   **Note:** When the password is requested there is a 2 minute timeout. If you fail to enter the password within 2 minutes, exit the script (by holding down the ‘Ctrl’ key and pressing ‘c’ repeatedly until reaching the command line); then restart by typing ‘cluster’.

4. Follow the instructions until you are returned to the menu.
   a. Ensure that you select the correct Master Cisco VCS from which to download the configuration and FindMe data
   b. When asked for a password, enter the root password of the relevant Cisco VCS.

   **Note:** The Master Cisco VCS will be the source of the configuration for this and all Cisco VCS peers in the cluster. This Cisco VCS will have its configuration deleted and replaced by that from the Master.

   The configuration will now be copied from the Master Cisco VCS to this Cisco VCS.

5. Wait approximately 2 minutes – this is the frequency with which configuration is copied from the Master.

6. Check the Warnings page of the newly added Cisco VCS (Status > Warnings). If there is a warning that the Cisco VCS must be restarted, select Maintenance > Restart and then click Restart System.
   - Warnings about TMS Agent passwords being default will be cleared when TMS Replication is enabled.

7. Check that the configuration (including Zone configuration, Transforms configuration, CPL and other configuration for items from the System Configuration, VCS Configuration and Application menus) is as expected (not FindMe — this will be replicated later) as per the Master Cisco VCS.
On each Cisco VCS now in the cluster (including the Master):

1. Log in to the Cisco VCS CLI as root and type:
   
   `cluster`

2. Choose option 5 “Check the replication state of this VCS”.

3. Check that the correct Cluster peers are reported and that it states “Replication is working”.
   
   If there are problems, they need to be resolved:
   
   - If a warning “**Replication process is not running**” is reported, this will right itself within one hour. Alternatively you can activate the replication immediately. To do so, either:
     
     i. Restart all Cisco VCSs reporting the problem, or
     
     ii. At the root login, at a command prompt, type:

     ```
     /etc/init.d/S80clusterd restart
     ```

   - If there is a failure message “**ERROR: One or more Replicable directories /tandberg/persistent/oti/client/x5 /tandberg/persistent/oti/server/x5 do not exist**”
     
     i. Log in to the Cisco VCS as root and type:

     ```
     mkdir /tandberg/persistent/oti/client/x5
     mkdir /tandberg/persistent/oti/server/x5
     chown nobody:nobody /tandberg/persistent/oti/client/x5 -R
     chown nobody:nobody /tandberg/persistent/oti/server/x5 -R
     ```

     repeat these steps, choosing option 5 again, to make sure that this has cured the problem.

4. Repeat for each Cisco VCS in the cluster, including the Master, until all problems are resolved.

On other devices:

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

IfCisco TMS is used:

1. Select **Systems > Navigator** (and any required sub folders) then select the Master Cisco VCS.

2. Select the **Clustering** tab and click **Update cluster in TMS**

3. Ensure that **Enable TMS Agent Data Replication on all Cluster Peers** is selected.
   - if not, select it and click **Save Cluster Settings**

4. Select **Systems > Navigator** (and any required sub folders) then select the new Cisco VCS to be added to this cluster.

5. Select the **TMS Agent** tab and ensure

   i. **Enable TMS Agent Data Replication** is selected

   ii. **Enable Authentication** is selected

6. If any changes need to be made, click **Save**.

On Cisco VCS:

7. Log in to the web browser of the new Cisco VCS peer.

8. Check the Warnings page (**Status > Warnings**) and if required, restart the Cisco VCS

9. Check that the expected FindMe entries (from the Master Cisco VCS) exist on this Cisco VCS **(Maintenance > Login accounts > User accounts)**

Adding a Cisco VCS to a cluster is now complete.
Remove a live Cisco VCS from a Cisco VCS X5 cluster (permanently)

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

- If the whole cluster is to be disbanded then use the procedure defined in “Disband a Cisco VCS X5 cluster”.
- If the cluster peer to be removed is not accessible, use the procedure defined in “Remove an out-of-service Cisco VCS from a Cisco VCS X5 cluster (permanently)”.

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

On Cisco TMS
2. Select **Systems > Navigator** (and any required sub folders) then click on the Cisco VCS to be removed.
3. Select the **TMS Agent** tab.
4. Clear the **Enable TMS Agent Data Replication** check box.
5. Click **Save Settings**.

On the Cisco VCS to be removed:
6. Log in to the CLI as root and type:
   ```
   cluster
   ```
   The following screen will appear:

7. Choose option 3 “Disable Replication on this VCS”.
8. Follow the instructions until you are returned to the menu.
9. Choose option q to Quit.

On the Cisco VCS that is being removed:
10. Log into the web interface.
11. Go to the Clustering page (VCS Configuration > Clustering):
   a. Change the Cluster name to a unique ID for this Cisco VCS (ideally to the routable Fully Qualified Domain Name used in SRV records that address this individual Cisco VCS, for example "vcs1.example.com". (See Appendix 11 – Cluster name and DNS SRV records.))
      Note: Do NOT use the process "Appendix 10 – Changing the cluster name (and keeping FindMe accounts)" because FindMe accounts are to be left with the cluster that this Cisco VCS is being removed from.
   b. Delete all entries in the Peer x IP address fields.
12. Click Save.

Note:

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

13. Go to the OCS Relay page (Applications > OCS Relay)
    if Mode = On change it to Mode = Off
    select Save
14. Restart the Cisco VCS (Maintenance > Restart and then click Restart System).

On the Master Cisco VCS:
1. Log into the web UI.
2. On the Clustering page (VCS Configuration > Clustering) delete the IP address of the Cisco VCS that has been removed.
3. If the Cisco VCS being removed is not the last in the list, move any other IP addresses up the list so that there are no empty fields between entries.
4. If the master Cisco 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 Cisco VCS peers:
1. Log into the web UI.
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 Cisco VCS.
3. Click Save.
4. Repeat for all remaining non-master Cisco VCS peers until they all have identical clustering configuration.

On other devices:
1. If you have any other Cisco VCSs, Gatekeepers or Border controllers neighbored (or connected via a traversal zone) to this cluster of Cisco 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 Cisco 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 Cisco VCS peers instead.

**Warning:** The removed Cisco VCS will retain its configuration at the time it is removed from the cluster, and will continue to function as a non-clustered Cisco VCS. It is recommended that after it has been removed from the cluster it is taken out of service (e.g. perform `xcommand DefaultValuesSet Level: 2` and `xcommand DefaultLinksAdd`) or the Cisco VCS is reconfigured with an alternative configuration, so that other devices no longer try to use it as a cluster peer.

---

**Reconfigure Cisco TMS**

**On Cisco TMS**

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

Removing a live Cisco VCS from a cluster is now complete.
Remove an out-of-service Cisco VCS from a Cisco VCS X5 cluster (permanently)

Use the following procedure if:

- the Cisco VCS is dead and needs to be RMAd, or
- the Cisco VCS cannot be accessed for some other reason

If the whole cluster is to be disbanded then use the procedure defined in “Disband a Cisco VCS X5 cluster”.

If the cluster peer to be removed is accessible, use the procedure defined in “Remove a live Cisco VCS from a Cisco VCS X5 cluster (permanently)” which clears up the removed Cisco VCS as well as its previous peers.

This procedure does not delete clustering configuration from the removed Cisco VCS. Once removed, you must not reconnect the out-of-service Cisco VCS without first deleting all of its peers and stopping FindMe and configuration replication (see the section below “Before you reconnect the out-of-service Cisco VCS back to the network”).

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

On Cisco TMS
1. Select Systems > Navigator (and any required sub folders) then click on the Cisco VCS to be removed.
2. Select the TMS Agent tab.
3. Clear the Enable TMS Agent Data Replication check box.
4. Click Save Settings.

On the Master Cisco VCS:
1. Log in to the CLI as root and type:
   ```
   cluster
   ```
   The following screen will appear:

   ![Cisco VCS CLI Screen]

2. Choose option 4 “Disable Replication on another Peer”.
3. Follow the instructions until you are returned to the menu (enter the IP address of the peer to remove when asked).
On the Master Cisco VCS:
4. Log into the web UI.
5. On the Clustering page (VCS Configuration > Clustering) delete the IP address of the Cisco VCS that has been removed.
6. If the Cisco 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
   a. If this results in the master Cisco VCS peer’s IP address moving up the list, alter the Configuration master value to match its new location.
7. Click Save.

On all the remaining non-master Cisco VCS peers:
1. Log into the web UI.
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 Cisco VCS.
3. Click Save.
4. Repeat for all remaining non-master Cisco VCS peers.

On other devices:
1. If you have any other Cisco VCSs, Gatekeepers or Border controllers neighbored (or connected via a traversal zone) to this cluster of Cisco 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 Cisco 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 Cisco VCS peers instead.

Reconfigure Cisco TMS

On Cisco TMS:
1. Select Systems > Navigator (and any required sub folders) then click on the Master Cisco VCS.
2. Select the Clustering tab.
3. Click Update Cluster in TMS.

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

Before you reconnect the out-of-service Cisco VCS back to the network

If the removed Cisco VCS is ever recovered, before you reconnect it you must:
1. Run the cluster script option 3 on the Cisco VCS (see steps 2 and 3 in the section “Remove a live Cisco VCS from a Cisco VCS X5 cluster (permanently)”)
2. Run the command xcommand DefaultValuesSet level: 2 from the CLI.

This will ensure that the configuration of the recovered Cisco VCS is returned to default and it will not interact with its ex-peers.
Disband a Cisco VCS X5 cluster

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

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

**Warning**: if any of the Cisco VCSs are left in operation after being removed from the cluster, calls between endpoints registered to different Cisco 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 Cisco VCSs over which calls can be routed. To overcome this, you must create neighbor relationships between the Cisco VCSs so that there are links between them.

- If any Cisco VCS is not accessible, firstly remove it using the procedure “Remove an out-of-service Cisco VCS from a Cisco VCS X5 cluster (permanently)”.

On Cisco TMS:
1. Select **Systems > Navigator** (and any required sub folders) then select the Master Cisco VCS.
2. Select the **Clustering** tab.
3. Un-select **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
7. Click **Save Settings**.

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

On each non-master Cisco VCS:
1. Log in to the Cisco VCS CLI as root and type:
   ```
   cluster
   ```
   The following screen will appear:
2. Choose option 3 “Disable Replication on this VCS”.
3. Follow the instructions until you are returned to the menu.
4. Choose option q to Quit.
5. Repeat for each non-master Cisco VCS.

On the Master Cisco VCS:
6. Log in to the Cisco VCS CLI as root and type:
   ```
close
   ```
7. Choose option 3 “Disable Replication on this VCS”.
8. Follow the instructions until you are returned to the menu.
9. Choose option q to Quit.

On each non-master Cisco VCS peer:
10. Log into the web interface.
11. From the Clustering page (VCS Configuration > Clustering):
   a. Change the Cluster name to a unique ID for this Cisco VCS (ideally to the routable Fully Qualified Domain Name used in SRV records that address this individual Cisco VCS, for example "vcs1.example.com", "vcs2.example.com". etc. (See Appendix 11 – Cluster name and DNS SRV records.))
   Note: Do NOT use the process "Appendix 10 – Changing the cluster name (and keeping FindMe accounts)" because FindMe accounts are to be left with the master peer of the cluster that this Cisco VCS is being removed from.
   b. Delete all entries in the Peer x IP address fields.
12. Click Save.

Note:

- FindMe users will not be available on this non-master Cisco VCS (they will only be left available on the master)
- A Warning similar to that shown below may appear on the web UI and CLI of the Cisco VCS being removed. This is not a problem, the warning will be cleared when the Cisco VCS is restarted:
13. Go to the OCS Relay page (Applications > OCS Relay) if Mode = On change it to Mode = Off select Save.

14. Restart the Cisco VCS (Maintenance > Restart and then click Restart System).

15. Repeat for each non-master Cisco VCS.

On the Master Cisco VCS:

16. Log into the web interface.

17. If the Cluster name is to be changed on this Master Cisco VCS, FindMe information must either be deleted, or changed to use the new Cluster name, so that the database is not left with unused user accounts. Either:
   a. Delete all FindMe entries:
      i. Go to Maintenance > Login accounts > User accounts.
      ii. Select each account and click Delete.
   b. Change the FindMe users held on this Cisco VCS to use the new Cluster name:
      i. Log in as root and at a command prompt, type:

         transferfindmeaccounts <current Cluster name of this VCS> <Cluster name that this VCS is being changed to>

18. Go to the Clustering page (VCS Configuration > Clustering).
   a. Optionally change the Cluster name to a unique ID for this Cisco VCS (ideally to the routable Fully Qualified Domain Name used in SRV records that address this individual Cisco VCS, for example "vcs1.example.com". (See Appendix 11 – Cluster name and DNS SRV records.))
   b. Delete all entries in the Peer x IP address fields.

19. Click Save.

Note: A Warning similar to that shown below may appear on the web UI and CLI of the Cisco VCS being removed. This is not a problem, the warning will be cleared when the Cisco VCS is restarted:

20. Restart the Cisco VCS (Maintenance > Restart and then click Restart System).

On other devices:

1. If you have any other Cisco VCSs, Gatekeepers or Border controllers neighbored (or connected via a traversal zone) to this cluster of Cisco VCS peers, ensure that they have those zones removed, or modified appropriately.

2. If you have any endpoints registering to this Cisco 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 Cisco VCS.

Reconfigure Cisco TMS

On Cisco TMS:

1. Select Systems > Navigator (and any required sub folders) then click on the Master Cisco 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. Cisco TMS will report “Cluster successfully deleted”.

Disband a cluster of Cisco VCSs is now complete.
Change the master peer of a Cisco VCS X5 cluster

Changing the master peer in a cluster where the old master Cisco VCS is accessible 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 Cisco VCSs which think they are cluster Master.

On the “new” Master Cisco 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 warnings on Cisco VCS that report ‘Cluster master mismatch’ or ‘Cluster replication error’ – they will be rectified as part of this procedure.**

If the “old” Master Cisco VCS is accessible, on the “old” Master Cisco VCS:
3. On the Clustering page (VCS Configuration > Clustering) from the Configuration master drop-down menu select the ID number of the “new” Master Cisco VCS.
4. Click **Save**.

For all other non-master Cisco VCS peers, on that Cisco VCS:
5. Go to the Clustering page (VCS Configuration > Clustering) and from the Configuration master drop-down menu select the ID number of the “new” Master Cisco VCS.
6. Click **Save**.

On each Cisco VCS in the cluster (including the master):
7. Confirm that the change to the Configuration master has been accepted by selecting VCS Configuration > Clustering and refreshing the page.
8. If any Cisco VCSs have not accepted the change, repeat steps 5 and 6.

On each Cisco VCS in the cluster (including the master):
9. Log in to the Cisco VCS CLI as root and type:
   
   ```
   cluster
   ```
10. Choose option 5 “Check the replication state of this VCS”.
11. Check that the correct Cluster peers are reported and that it states “Replication is working”.
   
   If any Cisco VCS reports a problem, ensure that no calls are in progress and then reboot the Cisco VCS.

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

Reconfigure Cisco TMS

No changes are required; Cisco TMS will see the master change on the Cisco VCS cluster and report this appropriately.
If the old master is not available

If the change of Master is being performed because the “old” Master is not accessible, remove the “old” Master using the “Remove an out-of-service Cisco VCS from a Cisco VCS X5 cluster (permanently)” procedure.

If the “old” Master was not accessible when changing the master peer of the Cisco VCS cluster, but later becomes available, you must bring it back into the cluster using the “Add an X5 Cisco VCS to a Cisco VCS X5 cluster” procedure.

Changing the master peer of a Cisco VCS cluster is now complete.
Change the IP address of a Cisco VCS X5 peer

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

The process is as follows:
1. Ensure that the Cisco VCS whose IP address is to be changed is not the Master Cisco VCS. If it is the Master Cisco VCS, follow the steps in the section “Change the master peer of a Cisco VCS X5 cluster” to make a different peer the Master.
2. Carry out the process documented in “Remove a live Cisco VCS from a Cisco VCS X5 cluster (permanently)”.  
3. Change the IP address of the Cisco VCS.
4. Carry out the process documented in “Add an X5 Cisco VCS to a Cisco VCS X5 cluster”.

Changing the IP address of a Cisco VCS peer is now complete.
Appendix 1 – Backing up a Cisco VCS

Backing up a pre X3.0 Cisco VCS

To save the configuration of a Cisco VCS running a version of code prior to X3.0:
1. Use SSH, Telnet or a serial link to log into the Cisco VCS CLI as an admin user.
2. Type:
   xconfiguration
3. Copy the results to a text file and save it.

To save the Cisco VCS FindMe data and certificates:
4. Log into the Cisco VCS CLI as root and save:
   a. persistent/policy/policy.xml
   b. persistent/oti/*.*
   c. persistent/certs/*.*

Backing up an X3.0 or later Cisco VCS

1. On the Cisco VCS web UI select Maintenance > Backup and restore.
2. Click Create System Backup File and save the file.
3. If Cisco VCS is X5 or later:
   a. Click Create TMS Agent backup file and save the file (this backs up FindMe entries that are in X5 FindMe database format).

Note:

- If the TMS Agent backup is restored (uploaded) to Cisco VCS then:
  from a root login run "tmsagent_reindex_database" to ensure the uploaded data is linked into the database correctly.

- A TMS Agent backup contains the whole of the Cisco TMS’s provisioning and FindMe database (for all clusters and non-clustered Cisco VCSs with which Cisco TMS is replicating). It is saved for emergency use only – if restored to a cluster it will only get overwritten by the Cisco TMS data. It can be restored to a non-clustered Cisco VCS that is not replicating with Cisco TMS.
Appendix 2 – Ensure that root access via SSH is enabled

To ensure that SSH is enabled:

1. Log in to the Cisco VCS CLI as root and type:
   \[ \text{rootaccess -d} \]
   This will display the current setting.

2. If “ssh off” is reported, type:
   \[ \text{rootaccess -s on} \]

3. On the web UI, from the System administration page (System Configuration > System) ensure that SSH service is set to On.
Appendix 3 – Adding a Cisco VCS to Cisco TMS

On the Cisco VCS:
1. Go to the SNMP page (System Configuration > SNMP) and ensure that:
   a. Enabled is set to On
   b. SNMP community name is set to public
      (If SNMP was previously disabled, a warning will appear indicating the need for a restart. To
      restart the Cisco VCS, go to Maintenance > Restart and click Restart System.)
2. Go to the External Manager page (System Configuration > External Manager) and ensure that:
   a. Address is set to the IP Address or FQDN of Cisco 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’.¹

On Cisco TMS:
1. Select Systems > Navigator.
2. Select (or create) an appropriate folder in which to put the Cisco 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 Cisco VCS.
5. Click Next.
   
If an error occurs, e.g. “✗ Wrong Password”, click on the Edit System link and correct the
problem (enter the root password of the Cisco VCS).

¹ 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 Cisco VCS password is not default, set this up in the **Connection** tab or in **Settings > Edit Settings**

   ▶ If the Cisco VCS was already configured in Cisco TMS, ensure that it has the correct IP address (in Cisco TMS, go to **Systems > Navigator** (and any required sub folders), select the Cisco VCS, and from the **Connection** tab check the **IP Address** field).

**On Cisco VCS:**

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

---

---
Appendix 4 – IP Port numbers

For cluster communications (between Cisco VCS peers / Cisco TMS):
- IP port 22 is used for Cisco VCS cluster configuration synchronization
- IP port 389 is used for diagnostics
- IP port 636 – is reserved, currently not used
- IP port 1719 is used for Bandwidth updates between Cisco VCS peers
- IP port 4444 is used for FindMe and provisioning data synchronization administration
- IP port 8989 is used for FindMe and provisioning data synchronization replication
- Standard SIP and H.323 ports are used for calls

It is unusual to have any sort of firewall between cluster peers, but if there is, all these IP ports must be open between each and every Cisco VCS peer in the cluster.
Appendix 5 – Impact of clustering on other Cisco VCS applications

Conference Factory (Multiway™)

- Conference Factory application configuration is NOT replicated across a cluster.
- The Conference Factory template MUST be DIFFERENT on each of the Cisco 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 Cisco 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 Cisco VCS serves the conference ID, it cannot serve a conference ID that any other Cisco VCS could have served.

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

Microsoft Office Communications Server 2007 (OCS)

If OCS is to be configured to operate with an X5 Cisco VCS cluster, see the "Cisco VCS deployment guide – Microsoft OCS 2007 (R1 and R2) and Cisco VCS Control (X5)".

Some parameters on Cisco VCS, such as:
- Call routed mode
- H.323 ↔ SIP interworking mode

need setting according to that guide rather than this clustering guide.
Appendix 6 – Configuring endpoints to work with a Cisco VCS cluster

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

Also see “Appendix 11 – 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 Cisco VCSs where 1 or more Cisco 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 Cisco 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 Cisco 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 Cisco VCS. On registering with the Cisco VCS, the Cisco VCS will respond with the H.323 “Alternate Gatekeepers” list containing the list of Cisco VCS Cluster peer members.

The endpoint will continue to use the first Cisco VCS that it registered to for re-registrations and for calls. If it ever loses connection to its Cisco 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 Cisco 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 Cisco 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 Cisco 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 Cisco VCS. On registering with the Cisco VCS, the Cisco VCS will respond with the H.323 ‘Alternate Gatekeepers’ list containing the list of Cisco VCS Cluster peer members.

The endpoint will continue to use the first Cisco 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 Cisco VCS at startup, the endpoint is quickly pointed at a different Cisco VCS.

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

Use this option if the Cisco 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 Cisco VCS peer

On startup the endpoint will try and register with the Cisco 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 Cisco VCS. On registering with the Cisco VCS, the Cisco VCS will respond with the H.323 “Alternate Gatekeepers” list containing the list of Cisco VCS Cluster peer members.

The endpoint will continue to use the first Cisco 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 Cisco VCSs where 1 or more Cisco 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 Cisco 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 Cisco 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 priority.

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

The endpoint will continue to use the first Cisco VCS that it registered to for re-registrations and for calls. If it ever loses connection to its Cisco VCS, it will use the DNS SRV entry to find a new Cisco 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 2 – DNS Round-Robin (2\textsuperscript{nd} choice)

To use this option, there must be a DNS A-record available for the DNS name of the Cisco 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 Cisco 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 Cisco 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 Cisco VCS.

The endpoint will continue to use the first Cisco VCS that it registered to for re-registrations and for calls. If it ever loses connection to its Cisco VCS it will perform another DNS lookup to find a new Cisco VCS to register to (the DNS server providing a Cisco 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 Cisco VCS is not accessible the endpoint is quickly pointed at a different Cisco VCS.

Option 3 – Static IP (least preferred)

Use this option if the Cisco 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 Cisco VCS peer

On startup the endpoint will try and register with the Cisco 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 Cisco VCS.

The endpoint will continue to use the first Cisco 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 Cisco VCS until it is accessible again.
Appendix 7 – Troubleshooting

Cisco VCS 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”

Follow the process defined in “Upgrade a Cisco VCS X3 / X4 cluster to an X5 cluster”.

“Cluster replication error: the Master peer is unreachable”

If Cisco VCS reports a warning: “Cluster replication error: the Master peer is unreachable”:

1. From a root login, check the directory /tmp/x5/peerconfiguration
2. It should have directories for each peer, e.g. if 2 peers it should have directories 1 and 2
3. It should also have a file ‘clustermaster’
4. cat clustermaster tells you the master

If the file clustermaster does not exist on any member of the cluster it must be created. This can be done by changing all Cisco VCSs in the cluster to use a new Cisco VCS as the cluster master and then returning them all to use the preferred master.

Do this on each Cisco VCS in the cluster using the web interface:

1. Go to VCS Configuration > Clustering.
2. From the Configuration master drop down select the a new cluster master (make sure that this is the same on all Cisco VCSs in the cluster).
3. Click Save.
4. Repeat for all Cisco VCSs in the cluster

then, on each Cisco VCS in the cluster:

1. From the Configuration master drop down select the preferred cluster master on all Cisco VCSs in the cluster.
2. Click Save.
3. Repeat for all Cisco VCSs in the cluster

“Cluster replication error: there was an error during automatic replication of configuration”

1. Check the event log.
   If it reports:
   
   <Date> logger: Event="Application Warning" Detail="Cluster watchdog had to terminate doFindMeReplication 10348." Level=1 Time=<Date/Time>

   then the base configuration file is too large for the automated process to copy. A manual copy can be carried out to fix this.
2. On the Cisco VCS reporting this issue, login to the Cisco VCS as root and type:
   
   cd /tmp/x5/peerconfiguration
   ls
   
   there should be a file ‘clustermaster’ plus one directory for each Cisco VCS in the cluster, labeled 1, 2, ..., 6
3. Type:
   
   ls 1
ls 2
ls 3 etc
the directories 1, 2, 3 etc should have a file "alternatesconfiguration.xml". If any is missing, it needs to be manually copied.

Note: Directory 1 relates to the configuration of the Cisco VCS listed in the Cisco VCS Clustering tab as Peer 1 IP address, directory 2 relates to the configuration of the Cisco VCS listed in the Cisco VCS Clustering tab as Peer 2 IP address etc.

4. Log in as root to the IP address of the Peer X IP address that is missing the "alternatesconfiguration.xml" file.
5. Scp the file /tmp/x5/peerconfiguration/X/alternatesconfiguration.xml to root@<IP of dest VCS>/tmp/x5/peerconfiguration/X
   where X is the directory ID missing the file.
   e. The relevant username and password of the receiving Cisco VCS will have to be entered to allow it to accept the file.

For example, if the Cisco VCS at 192.168.1.101 has directory 3 missing the alternatesconfiguration.xml file, and Peer 3 IP address is 192.168.1.103 then log in to 192.168.1.103 as root and type:
   scp /tmp/x5/peerconfiguration/3/alternatesconfiguration.xml root@<192.168.1.101>/tmp/x5/peerconfiguration/3

"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 Cisco VCS reports a warning: "Warning, cluster replication error – <details> manual sync of config is required"

On that non-master Cisco VCS:
   ▶ From an admin SSH or telnet login, type:
      xcommand ForceConfigUpdate

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

Warning: Never issue these commands on the Master Cisco VCS, otherwise all Cisco VCS configuration for the cluster will be lost.

"Cluster replication error: the NTP server is unreachable"
Configure an accessible NTP server on the Cisco VCS web page System configuration > Time.

"Cluster replication error: the local VCS does not appear in the list of peers"
Check and correct the list of peers for this Cisco VCS on the Master Cisco VCS, and copy to all other Cisco 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 Cisco VCS is being managed by Cisco TMS, on Cisco TMS:
1. Select 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 Cisco TMS and all Cisco VCSs and their TMS Agents managed by that Cisco TMS.

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

“Security alert: the TMS Agent database has the default replication password set”

If the Cisco VCS is being managed by Cisco TMS, on Cisco TMS:
1. Select 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 Cisco TMS and all Cisco VCSs and their TMS Agents managed by that Cisco TMS.

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

**Cluster script, option 5**

“WARNING: There are more Public Keys than there are alternates.”

If, when running Cluster script option 5 you receive a status: “WARNING: There are more Public Keys than there are alternates.” this means that the Cisco VCS has been a member of a cluster in the past and that cluster was not disbanded properly, or the Cisco VCS was not removed from the cluster properly.

- Cluster keys are kept in the directory /tandberg/.ssh.
- Cluster key looks like rsynch-aaa.bbb.ccc.ddd.pub
  - where aaa.bbb.ccc.ddd is the IP address of the Cisco VCS peer to which they belong.

Delete any keys (whose name starts rsynch) whose IP address does not match a Cisco VCS in the cluster.

Do not delete any other files in this directory.
Cisco TMS warnings

Cisco TMS Cluster Diagnostics

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

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

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

If HTTPS must be used for Cisco VCS to supply feedback to Cisco TMS, see details in “Appendix 3 – Adding a Cisco VCS to Cisco TMS” to see how to set up certificates etc.

Cisco TMS will force HTTPS on Cisco VCS if:

- **Administrative Tools > Configuration > Network Settings**, TMS Services > Enforce Management Settings on Systems = On

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

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

Why are Cisco VCS peers regularly doing reverse DNS lookups for one-another?

For Cisco VCS cluster peers to keep up to date, each Cisco VCS peer in a cluster logs in over SSH to every other peer in that cluster once per minute. The SSH process performs a reverse DNS lookup at every login to identify the connecting party.

Therefore in a cluster:

- (n-1) reverse DNS lookups per Cisco VCS per minute are expected
- n*(n-1) reverse DNS lookups per cluster per minute are expected
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.

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 8 – Upgrading Cisco TMS to 12.6

To upgrade Cisco TMS from 12.2 to 12.6, follow the procedures documented in “Upgrade a Cisco VCS X3 / X4 cluster to an X5 cluster”.

Appendix 9 – Upgrade Cisco VCS software to X5

To upgrade Cisco VCS Software to X5, follow the procedures documented in “Upgrade a Cisco VCS X3 / X4 cluster to an X5 cluster” – Cisco TMS and Cisco VCS have to be upgraded at the same time in many cases.

The process documented below is to be used in conjunction with, and where referenced by, “Upgrade a Cisco VCS X3 / X4 cluster to an X5 cluster” in order to perform the upgrade of code on a single Cisco VCS.

From release X4.1 onwards the Cisco VCS supports a maintenance mode. When placed in this mode, the Cisco VCS will eventually be left in a state where it has no calls or registrations, at which point it can be upgraded without affecting existing calls or registrations.

When maintenance mode is enabled, the Cisco VCS will ignore all further registration requests and will reject new call requests with a license limit exceeded indication. Where endpoints support the capability to register with a different Cisco VCS if the one that it is registering to fails (see “Appendix 6 – Configuring endpoints to work with a Cisco VCS cluster”) registrations will gradually migrate to other Cisco VCS peers in that cluster. Eventually all existing registrations on the Cisco VCS where maintenance mode has been enabled will expire and all ongoing calls will clear down. At this point the Cisco VCS can be upgraded and then maintenance mode disabled to bring it back into service.

When upgrading a cluster peer (master or non-master):
1. Enable maintenance mode. From the Cisco VCS command line type:
   xconfiguration SystemUnit Maintenance Mode: On
2. Wait for all calls to clear and registrations to timeout.
3. If necessary, manually remove any calls that do not clear automatically (Status > Calls, then check the box next to the calls you want to terminate and click Disconnect).
4. If necessary, manually remove any registrations that do not clear automatically (Status > Registrations > By device, then select the box next to the devices you want to remove and click Unregister).
5. Upgrade and restart the Cisco VCS (Maintenance > Upgrade).
   • ensure that you have the Release key for loading Cisco VCS X5 code onto this Cisco VCS
   • for any further details see the "Upgrading Software" section of the Cisco VCS Administrator Guide

Note: The web browser interface may timeout during the restart process, after the progress bar has reached the end; this may happen if:
   ▶ Cisco VCS carries out a disk file system check – which it does approximately once every 30 restarts
   ▶ Provisioning is enabled, and re-indexing the database takes a while
6. Disable maintenance mode. From the Cisco VCS command line type:
   xconfiguration SystemUnit Maintenance Mode: Off
7. At this stage do not worry about warnings reporting:
   • WARNING: Security alert: the TMS Agent database has the default password set.
   • WARNING: Cluster name not configured: if FindMe or clustering are in use a cluster name must be defined; see the Clustering section of the Cisco VCS Administrator Guide for more information
   • WARNING: Security alert: the TMS Agent database has the default replication password set.
   These are handled in the remainder of the process of upgrading the Cisco VCS X3 / X4 cluster to X5.
Note: It is recommended that while Cisco VCS peers are running different versions of code, configuration changes to any Cisco VCS in the cluster are limited to the changes needed to complete the upgrade. Configuration changes will not be replicated across Cisco VCS peers that are not running the same version of software as the Master Cisco VCS.

Upgrading the software on a Cisco VCS is now complete.
Appendix 10 – Changing the cluster name (and keeping FindMe accounts)

The cluster name specifies which data is to be used in 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 X5 Cisco VCS cluster is being created and the FindMe accounts are to be carried across from the Master Cisco 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 Cisco VCS cluster, for example "cluster1.example.com". (See Appendix 11 – Cluster name and DNS SRV records).

Note:

- If transferfindmeaccounts is executed on multiple Cisco VCSs with different <current Cluster name of this Cisco VCS> to the same <Cluster name of the cluster being created>, the FindMe accounts from each of the Cisco 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 Cisco VCS.

- If a Cisco VCS cluster has its name changed, go to Cisco TMS and select the Master Cisco VCS, select the clustering tab and 'Cluster name has changed' should be reported. Select 'Update Cluster in Cisco TMS'.
Appendix 11 – 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 Cisco VCS are:

- `_sips._tcp.<fully.qualified.domain>`
- `_sip._tcp.<fully.qualified.domain>`
- `_sip._udp.<fully.qualified.domain>` - not recommended for video calls, only 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 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 the Cisco VCS Administrator Guide and RFC 2782.

The Cisco 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 Cisco VCS cluster.
**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), Cisco 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 prior to 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

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 12 – 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 “Cisco VCS Deployment Guide - ENUM dialing on Cisco VCS”, 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 the “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" "!*mary.jones@tandberg.com!" .
IN NAPTR 10 100 "u" "mailto+E2U" "!*peter.archibald@myco.com!" .

$ORIGIN 1.2.1.7.5.5.enum.lookup.com.

IN NAPTR 10 100 "u" "E2U+sip" "!*john.smith@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:
;; 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 E20 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:
;; Got no failures.

;; 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

~ #