



# Cisco TelePresence Conductor Clustering with Cisco VCS (Policy Service)

## Deployment Guide

---

TelePresence Conductor XC3.0  
Cisco VCS X8.x

Revised March 2015

---

# Contents

|  |           |
|--|-----------|
| <b>Introduction</b> .....  | <b>4</b>  |
| About Cisco TelePresence Conductor clustering .....  | 4         |
| About this document .....  | 4         |
| Related documentation .....  | 4         |
| <b>Example network deployment</b> .....  | <b>5</b>  |
| Cisco VCS .....  | 5         |
| Conference bridges .....   | 5         |
| Endpoints .....  | 6         |
| <b>Creating a TelePresence Conductor cluster</b> .....   | <b>7</b>  |
| Prerequisites .....  | 7         |
| Integration overview .....   | 7         |
| Creating an initial cluster peer .....   | 8         |
| Task 1: Checking configuration .....   | 8         |
| Task 2: Configuring IP addresses .....   | 9         |
| Adding a peer to a cluster .....   | 10        |
| Task 3: Configuring the cluster to accept the new peer .....                                       | 10        |
| Task 4: Checking configuration .....   | 10        |
| Task 5: Configuring the new peer to join the cluster .....   | 11        |
| Task 6: Configuring the Cisco VCS to use the new cluster peer .....                                | 11        |
| <b>Creating a system backup</b> .....  | <b>13</b> |
| <b>Removing a TelePresence Conductor peer</b> .....  | <b>14</b> |
| Task 1: Placing the peer in standalone mode .....  | 14        |
| Task 2: Updating all other peers in the cluster .....  | 14        |
| <b>Upgrading a cluster of TelePresence Conductors</b> .....  | <b>15</b> |
| Task 1: Reconfiguring the policy service on the Cisco VCS .....                                    | 15        |
| Task 2: Removing the peers from the cluster .....  | 15        |
| Task 3: Upgrading the peers that have been removed from the cluster .....                          | 15        |
| Task 4: Re-clustering the upgraded peer(s) .....   | 15        |
| Task 5: Configuring the Cisco VCS(s) to point at the upgraded TelePresence Conductor peer(s) ..... | 16        |
| Task 6: Upgrading the remaining cluster peer .....   | 16        |
| Task 7: Adding the remaining peer back into the cluster .....                                      | 16        |
| <b>Peer-specific configuration</b> .....   | <b>17</b> |
| Cluster configuration .....  | 17        |
| Ethernet .....   | 17        |
| IP .....   | 17        |
| System host name and domain .....  | 17        |
| DNS servers .....  | 17        |
| Time .....   | 17        |
| SNMP .....   | 18        |
| Logging .....  | 18        |
| Security certificates .....  | 18        |
| Administration access .....  | 18        |
| Root account password .....  | 18        |
| Locations .....  | 18        |

---

|  |           |
|--|-----------|
| <b>Troubleshooting</b> .....                       | <b>19</b> |
| Unable to cluster the TelePresence Conductor ..... | 19        |
| <b>Appendix 1: IP ports and protocols</b> .....    | <b>20</b> |
| IPSec communications .....                         | 20        |
| MTU size .....                                     | 20        |
| <b>Document revision history</b> .....             | <b>21</b> |

# Introduction

## About Cisco TelePresence Conductor clustering

Clusters of Cisco TelePresence Conductors are used to provide redundancy in the rare case of the failure of an individual TelePresence Conductor (for example, due to a network or power outage). Each TelePresence Conductor is a peer of the other TelePresence Conductors in the cluster.

The process to create clusters of TelePresence Conductors depends upon whether the TelePresence Conductor cluster is communicating with a Cisco Video Communications Server (Cisco VCS) or a Cisco Unified Communications Manager (Unified CM).

If the call control platform is the Cisco VCS and this has been configured to use the TelePresence Conductor, the configuration and conference status data is shared between all peers in the TelePresence Conductor cluster. When the Cisco VCS detects that one TelePresence Conductor has failed, it automatically contacts a different TelePresence Conductor, which responds exactly as the failed one would. This process is transparent to the user and offers virtually no interruption in service.

Connections between a TelePresence Conductor cluster and Cisco TMSPE behave differently. In Cisco TMS you can specify only a single TelePresence Conductor peer. If that peer fails you must manually add a different TelePresence Conductor peer.

## About this document

This document assumes that one standalone TelePresence Conductor has already been configured to work with a Cisco VCS and conference bridges according to the [Cisco TelePresence Conductor with Cisco VCS \(Policy Service\) Deployment Guide](#). This document provides details on how to extend the deployment with Cisco VCS using the Cisco VCS's external policy server interface to use a cluster of up to three TelePresence Conductors.

The topics covered in this document are:

- [Creating an initial cluster peer](#)
- [Adding a peer to a cluster](#)
- [Removing a TelePresence Conductor peer](#)
- [Upgrading a cluster of TelePresence Conductors](#)

## Related documentation

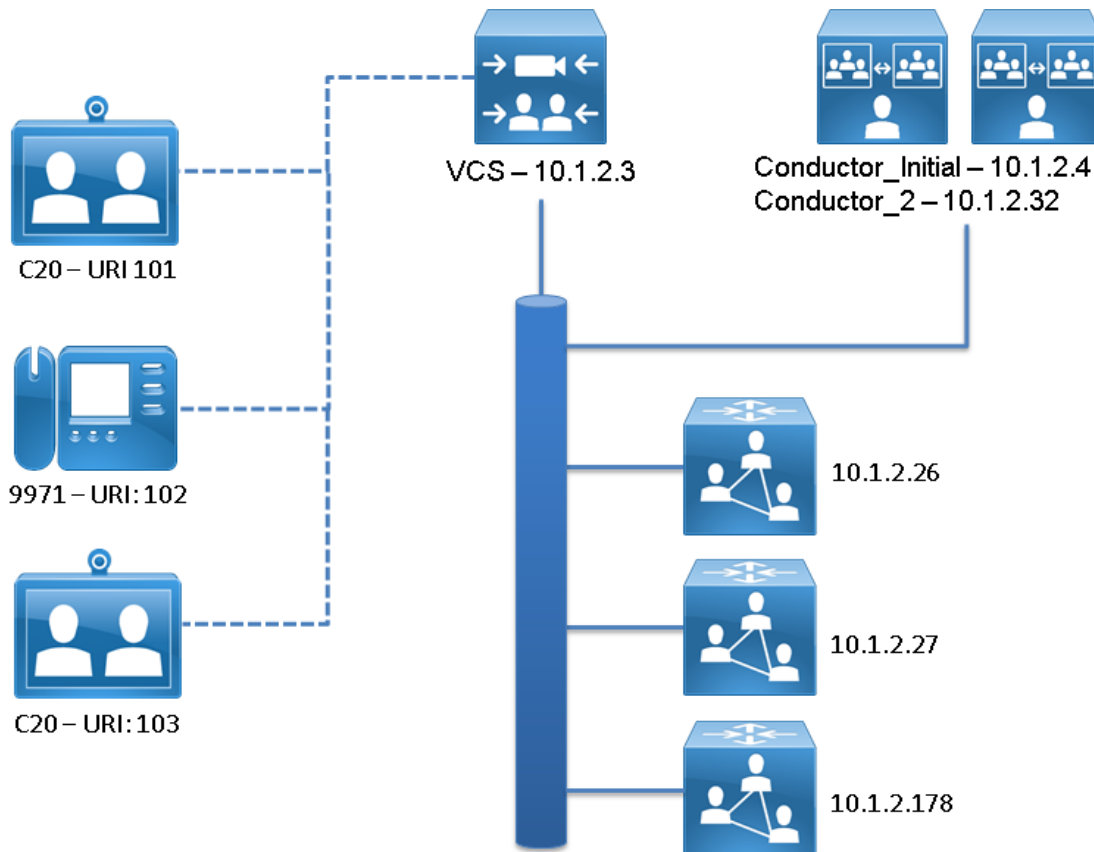
For more information on how to integrate a TelePresence Conductor cluster with a Cisco VCS in a deployment using the TelePresence Conductor's back-to-back user agent (B2BUA) see [Cisco TelePresence Conductor Clustering with Cisco VCS \(B2BUA\) Deployment Guide](#).

For more information on how to integrate a TelePresence Conductor cluster with Unified CM see [Cisco TelePresence Conductor Clustering with Cisco Unified CM Deployment Guide](#).

For more information on how to deploy Cisco VCS, TelePresence Conductor, and the conference bridges in an end-to-end secure network see [Cisco TelePresence Conductor with Cisco VCS \(Policy Service\) Deployment Guide](#).

## Example network deployment

This document uses the example network shown in the diagram below as the basis for the deployment configuration described.



## Cisco VCS

The Cisco Video Communications Server (Cisco VCS) acts as a call processor for video devices. It has a built in Gatekeeper, SIP Registrar, performs IPv4 to IPv6 conversions, performs H323 to SIP and SIP to H323 interworking, and provides H460 firewall traversal support. The Cisco VCS works with other infrastructure devices in the network to process the calling requests and direct or route them to the appropriate destination.

## Conference bridges

Conference bridges are network devices that enable multipoint conferences for endpoints by decoding and re-encoding the streams from the different endpoints and sending a single stream to each endpoint. This version of the TelePresence Conductor supports the conference bridge types TelePresence MCU and TelePresence Server.

## Endpoints

Endpoints are devices that receive and make video calls. They can be software clients on PCs and Macs such as Jabber Video, desktop endpoints such as the 9971 and EX90, or room systems such as the MX300.

# Creating a TelePresence Conductor cluster

## Prerequisites

Before starting the configuration, ensure you have met the following criteria:

- Each TelePresence Conductor that is supposed to be added to the cluster must be running the same version of XC software. See [Cisco TelePresence Conductor Administrator Guide](#) for information on upgrading a TelePresence Conductor.
- If using full capacity TelePresence Conductors, up to three peers can be clustered and all peers must be full capacity versions.
- If using TelePresence Conductor Select, up to two peers can be clustered and both peers must be a TelePresence Conductor Select.
- One TelePresence Conductor, the Cisco VCS and the conference bridges must be configured according to the [Cisco TelePresence Conductor with Cisco VCS \(Policy Service\) Deployment Guide](#).
- The remaining TelePresence Conductor peers must be configured according to the tasks in section "Configuring the TelePresence Conductor" in the *Cisco TelePresence Conductor with Cisco VCS (Policy Service) Deployment Guide*.
- All TelePresence Conductor cluster peers must be configured to use either the same NTP servers, or NTP servers that are very closely synchronized. The NTP servers can be viewed and configured on the **Time** page (**System > Time**).
- All TelePresence Conductor cluster peers must have a unique IP address.
- If peers are deployed on different LANs, there must be sufficient connectivity between the networks to ensure a low degree of latency between the peers - a maximum delay of 15ms one way, 30ms round-trip.
- For information on the ports that must be open between the TelePresence Conductor peers see [Appendix 1: IP ports and protocols \[p.20\]](#).
- All TelePresence Conductor cluster peers must be reachable using HTTPS from the Cisco VCS(s) from which they are going to receive conferencing requests.
- Conference bridges in use by TelePresence Conductor must be reachable over HTTPS and/or HTTP on a per-conference-bridge basis.
- We highly recommend that you take a [backup](#) on the initial cluster peer before adding it to the cluster.

## Integration overview

The Cisco TelePresence Conductor integrates tightly with the Cisco TelePresence Video Communication Server (Cisco VCS).

The Cisco VCS uses the TelePresence Conductor as a policy server for calls. The Cisco VCS configuration can assign a policy server to a search rule match and ask that policy server to allow or deny the request when that search rule is matched.

Within the policy server configuration of the Cisco VCS, up to three IP addresses or FQDNs can be specified as servers that are available to use for policy requests. These three IP addresses can point to a single TelePresence Conductor or a single TelePresence Conductor cluster.

The diagram below explains the call flow including the relationship between the Cisco VCS and TelePresence Conductor:



The following tasks in this document will focus on what needs to be configured on the TelePresence Conductor to create the initial peer of a cluster, add an additional peer to the cluster, and how to remove a peer from the cluster.

## Creating an initial cluster peer

### Task 1: Checking configuration

1. Decide which TelePresence Conductor is to be the initial peer. For the purposes of this example, we shall refer to this peer as **Conductor\_Initial**.  
**Note:** The configuration of this system will be shared with all other peers as they are added to the cluster, unless the configuration is peer-specific. For information on which configuration is peer-specific see [Peer-specific configuration \[p. 17\]](#).
2. Ensure that no other TelePresence Conductor is using **Conductor\_Initial**'s IP address in their clustering peers list. To do this:
  - a. Log into every TelePresence Conductor as a user with administrator rights.
  - b. Go to **System > Clustering**.
  - c. Ensure that all **Peer X IP address** fields (x = 1, 2, and 3) on this page do not have **Conductor\_Initial**'s IP address. If they do, delete that Peer IP address.
  - d. Click **Save**.
  - e. Go to **Maintenance > Restart options**.
  - f. Click **Restart**.
3. Log into **Conductor\_Initial** as a user with administrator rights.
4. Ensure that **Conductor\_Initial** has a valid and working NTP server configured:
  - a. Go to **System > Time**.
  - b. In the **Status** section at the bottom of the page, the **State** should be *Synchronized*:



5. Ensure that **Conductor\_Initial** has at least one valid DNS server configured. Go to **System > DNS** to verify DNS settings.
6. Ensure that **Conductor\_Initial** has the correct **Domain name** and **System host name** configured.

---

**Note:** <System host name>.<domain name> = FQDN of this TelePresence Conductor.

---

Go to **System > DNS** to verify DNS settings.

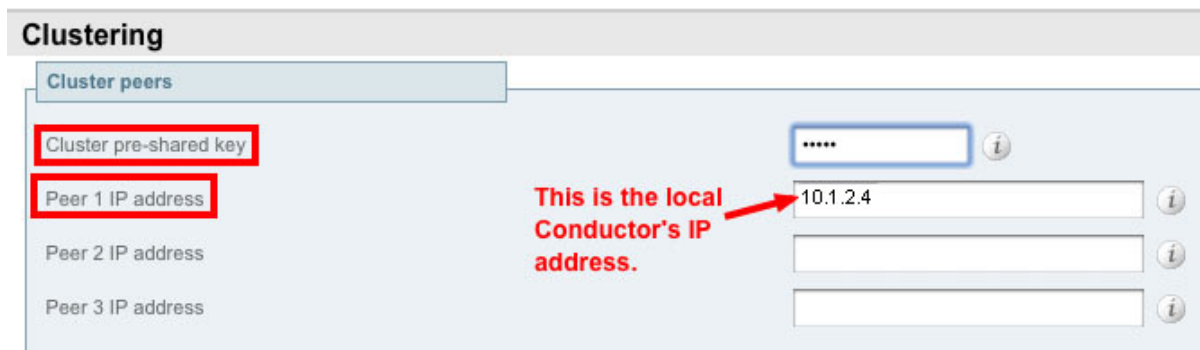


7. Ensure that **Conductor\_Initial** has no other TelePresence Conductor peers configured on this system:
  - a. Go to **System > Clustering**.
  - b. Ensure that all **Peer x IP address** fields (x = 1, 2, and 3) on this page are blank. If not, delete any entries.
  - c. Click **Save**.
8. Ensure that **Conductor\_Initial** has no Cluster pre-shared key configured:
  - a. Go to **System > Clustering**.
  - b. If a value is in **Cluster pre-shared key** field, delete the entry.
  - c. Click **Save**.
  - d. Go to **Maintenance > Restart options**.
  - e. Click **Restart**.

## Task 2: Configuring IP addresses

1. On **Conductor\_Initial**, go to **System > Clustering**.
2. Enter the following values in the relevant fields:

| Field                  | Values  |
|------------------------|---|
| Cluster pre-shared key | Enter a password (this will be the same for all peers).   |
| Peer 1 IP address      | Enter the IP address of this Conductor peer, <b>Conductor_Initial</b> (this is the initial peer in the cluster from which the initial configuration will be replicated from to all other peers in the cluster). |
| Peer 2 IP address      | Leave blank at this point in the configuration.   |
| Peer 3 IP address      | Leave blank at this point in the configuration.   |



3. Click **Save**.
4. Go to **Maintenance > Restart options**.
5. Click **Restart**.
6. Log into **Conductor\_Initial** as a user with administrator rights.
7. Go to **System > Clustering**.
8. Verify that it says 'This system' in green next to the peer 1 IP address.

## Adding a peer to a cluster

### Task 3: Configuring the cluster to accept the new peer

On each existing cluster peer (i.e. the initial peer and any other peer that has already been added to the cluster):

1. Log into the initial TelePresence Conductor, **Conductor\_Initial**, as a user with administrator rights.
2. Go to **System > Clustering**.
3. In the **Peer 2 IP address** field, enter the new peer's IP address. For the purposes of this example we shall refer to this peer as **Conductor\_2**.
4. Click **Save**.
5. It is normal for the peer to not show as 'Active' yet at this stage of the configuration process.
6. Go to **Maintenance > Restart options**.
7. Click **Restart**.

### Task 4: Checking configuration

1. Log into the new peer, **Conductor\_2**, as a user with administrator rights.
2. Ensure that **Conductor\_2** has a valid and working NTP server configured:
  - a. Go to **System > Time**.
  - b. In the **Status** section at the bottom of the page, the **State** should be *Synchronized*:



3. Ensure that **Conductor\_2** has at least one valid DNS server configured. Go to **System > DNS** to verify DNS settings.
4. Ensure that **Conductor\_2** has the correct **Domain name** and **System host name** configured:
 

---

**Note:** <System host name>.<domain name> = FQDN of this TelePresence Conductor.

---

 Go to **System > DNS** to verify DNS settings.
5. Ensure that **Conductor\_2** has no other TelePresence Conductor peers configured on this system:
  - a. Go to **System > Clustering**.
  - b. Ensure that all **Peer x IP address** fields on this page are blank. If not, delete any entries and click **Save**.
6. Ensure that **Conductor\_2** has no **Cluster pre-shared key** configured:
  - a. Go to the **Clustering** page (**System > Clustering**).
  - b. If a value is in **Cluster pre-shared key** field, delete the entry.
  - c. Click **Save**.
  - d. Go to **Maintenance > Restart options**.
  - e. Click **Restart**.

## Task 5: Configuring the new peer to join the cluster

1. On this peer, go to the **Clustering** page (**System > Clustering**).
2. In the **Cluster pre-shared key** field, enter the same password that was used for the initial peer, **Conductor\_Initial**.
3. In the **Peer 1 IP address** field, enter the IP address of the initial peer, **Conductor\_Initial**.
4. In the **Peer 2 IP address** field, enter the IP addresses of the local TelePresence Conductor, **Conductor\_2**.

**Clustering**

**Saved:** Saved peer address.

**Cluster peers**

Cluster pre-shared key: [password field]

Peer 1 IP address: **Conductor\_Initial** → 10.1.2.4 This system

Peer 2 IP address: **Conductor\_2** → 10.1.2.32 Active as X032

Peer 3 IP address: [empty field]

**Save**

5. Click **Save**.
6. Go to **Maintenance > Restart options**.
7. Click **Restart**.
8. Log into **Conductor\_2** as a user with administrator rights.
9. Go to **System > Clustering**.
10. Verify that it says 'This system' in green next to peer 1 and 'Active as xxx' in green next to peer 2.

**Clustering**

**Saved:** Saved peer address.

**Cluster peers**

Cluster pre-shared key: [password field]

Peer 1 IP address: 10.1.2.4 This system

Peer 2 IP address: 10.1.2.32 Active as X032

Peer 3 IP address: [empty field]

**Save**

## Task 6: Configuring the Cisco VCS to use the new cluster peer

For every Cisco VCS that communicates with the TelePresence Conductor cluster directly:

1. Log into the Cisco VCS (or if the Cisco VCS is clustered, the master Cisco VCS in the cluster) as a user with administrator privileges.
2. Go to **Configuration > Dial plan > Policy services**.
3. Click on the policy service for the TelePresence Conductor cluster.

4. In the uppermost blank **Server x address** field (x = 1, 2, or 3), enter the IP address of the TelePresence Conductor peer you have added to the cluster.

|                  |            |
|------------------|------------|
| Server 1 address | ★ 10.1.2.4 |
| Server 2 address | 10.1.2.32  |
| Server 3 address |            |

5. Click **Save**. You will be taken back to the **Policy services** page.
6. Wait for about a minute and then click on the policy service again.
7. If there is proper connectivity between the Cisco VCS and each TelePresence Conductor in the cluster, next to each peer IP address a green message will appear saying *Active*.

**Active. Last communication: 2012-10-25 11:00:41**

If the message is in red and says *Failed*, then:

- a. check the IP address used in the **Server x address** field (x = 1, 2, or 3)
- b. check the user credentials
- c. ensure that the default admin and root passwords have been changed on that TelePresence Conductor

## Creating a system backup

To create a backup of TelePresence Conductor system data:

1. Go to **Maintenance > Backup and restore**.
2. Optionally, enter an **Encryption password** with which to encrypt the backup file.  
If a password is specified, the same password will be required to restore the file.
3. Click **Create system backup file**.
4. After the backup file has been prepared, a pop-up window appears and prompts you to save the file (the exact wording depends on your browser). The default name is in the format:  
**<software version>\_<hardware serial number>\_<date>\_<time>\_backup.tar.gz**.  
(The file extension is normally **.tar.gz.enc** if an encryption password is specified. However, if you use Internet Explorer to create an encrypted backup file, the filename extension will be **.tar.gz.gz** by default. These different filename extensions have no operational impact; you can create and restore encrypted backup files using any supported browser.)  
The preparation of the system backup file may take several minutes. Do not navigate away from this page while the file is being prepared.
5. Save the file to a designated location.

Log files are not included in the system backup file.

**Note:** A system backup can only be restored to the peer from which the backup was taken.

For more information see [Cisco TelePresence Conductor Administrator Guide](#) or the TelePresence Conductor's online help.

# Removing a TelePresence Conductor peer

## Task 1: Placing the peer in standalone mode

Before removing a live peer from a cluster, you must place the peer in standalone mode so that it no longer communicates with other peers in the cluster. If the peer is out of service and can no longer be accessed, you do not need to place it in standalone mode. However, you must still follow the instructions to remove it from the cluster in the next section: [Task 2: Updating all other peers in the cluster \[p. 14\]](#).

To place a peer into standalone mode:

1. Log in to the peer to be removed from the cluster as a user with administrator privileges.
2. Go to **System > Clustering**.
3. Delete the **Cluster pre-shared keyvalue**.
4. Delete all entries from the **Peer IP address** fields.
5. Click **Save**.
6. Go to **Maintenance > Restart options**.
7. Click **Restart**. When the TelePresence Conductor has restarted, it will be in standalone mode.
8. Log in to the TelePresence Conductor as a user with administrator privileges.
9. Go to **Conference configuration > Conference bridges**.
10. Delete all conference bridge entries.
11. Log into the Cisco VCS (or if the Cisco VCS is clustered the master Cisco VCS in the cluster) as a user with administrator privileges.
12. Go to **Configuration > Dial plan > Policy services**.
13. Click on the policy service for the TelePresence Conductor cluster.
14. From the relevant **Server x address** (x = 1, 2, or 3) field, delete the IP address of the TelePresence Conductor that is being placed in standalone mode.
15. Click **Save**.

## Task 2: Updating all other peers in the cluster

After the peer to be removed has been placed in standalone mode (or if the peer is out of service and cannot be contacted), you must update all other peers in the cluster so they no longer consider the removed peer to be part of their cluster.

To do this, on each remaining peer in the TelePresence Conductor cluster:

1. Go to **System > Clustering**.
2. From the relevant **Peer x IP address** field (x = 1, 2, or 3), delete the IP address of the peer that has been removed from the cluster.
3. Click **Save**.
4. Repeat these steps on each remaining peer.

# Upgrading a cluster of TelePresence Conductors

The process described here is essentially disbanding, upgrading and then re-clustering a cluster of TelePresence Conductors. In order to prevent downtime, one peer in the cluster is upgraded separately to the others, so that there is always at least one peer active and able to service conference requests from the Cisco VCSs until all peers have been upgraded and re-clustered.

## Task 1: Reconfiguring the policy service on the Cisco VCS

This task involves choosing one peer in the cluster to be the last to be upgraded. This cluster peer will service conference requests from the Cisco VCSs until the other peers have been upgraded and re-clustered.

For every Cisco VCS that communicates directly with TelePresence Conductor:

1. Go to the Cisco VCS web interface and log in as a user with administrator privileges.
2. Go to **Configuration > Dial plan > Policy services**.
3. Click **View/Edit** for the TelePresence Conductor policy service.
4. Delete all but one of the **Server x addresses** (x = 1, 2, and 3), leaving only the address of the peer to be upgraded last.
5. Click **Save**.

## Task 2: Removing the peers from the cluster

The purpose of this task is to remove from the cluster all the TelePresence Conductor peers that are going to be upgraded first.

For each peer in the cluster that is to be upgraded first, complete the steps outlined in [Task 1: Placing the peer in standalone mode \[p.14\]](#) and [Task 2: Updating all other peers in the cluster \[p.14\]](#).

## Task 3: Upgrading the peers that have been removed from the cluster

For each TelePresence Conductor peer that has been removed from the cluster:

1. Log in as a user with administrator privileges.
2. Go to **Maintenance > Upgrade**.
3. Click **Browse** and select the TelePresence Conductor software image.
4. Click **Upgrade**.
5. Follow the onscreen prompts.

## Task 4: Re-clustering the upgraded peer(s)

If you have only one upgraded peer (i.e. you started with a cluster of two) follow the tasks outlined in [Creating an initial cluster peer \[p.8\]](#).

If you have two upgraded peers (i.e. you started with a cluster of three):

1. For the first peer, follow the tasks outlined in [Creating an initial cluster peer \[p.8\]](#), then
2. For the second peer, follow the tasks outlined in [Adding a peer to a cluster \[p.10\]](#).

## Task 5: Configuring the Cisco VCS(s) to point at the upgraded TelePresence Conductor peer(s)

For every Cisco VCS that communicates directly with TelePresence Conductor:

1. Go to the Cisco VCS web interface and log in as a user with administrator privileges.
2. Go to **Configuration > Dial plan > Policy services**.
3. Click on the TelePresence Conductor cluster policy service.
4. Delete the **Server x address** (x =1, 2, or 3) of the peer that has not been upgraded, and insert the addresses of the peers that have been upgraded.
5. Click **Save**.

## Task 6: Upgrading the remaining cluster peer

On the TelePresence Conductor peer that has not been upgraded:

1. Go to the web interface and log in as a user with administrator privileges.
2. Go to the **Clustering** page (**System > Clustering**).
3. Delete the **Cluster pre-shared key** value.
4. Delete all entries from the **Peer IP address** fields.
5. Click **Save**.
6. Go to **Maintenance > Restart options**.
7. Click **Restart**. When the TelePresence Conductor has restarted, it will be in standalone mode.
8. Log in as user with administrator privileges.
9. Go to **Maintenance > Upgrade**.
10. Click **Browse** and select the TelePresence Conductor software image.
11. Click **Upgrade**.
12. Follow the onscreen prompts.

## Task 7: Adding the remaining peer back into the cluster

Follow the tasks outlined in [Adding a peer to a cluster \[p.10\]](#).



# Peer-specific configuration

Most items of configuration are applied to all peers in a cluster. However, the following items must be specified separately on each cluster peer.

## Cluster configuration

The list of Peer IP addresses (including the peer's own IP address) that make up the cluster has to be specified on each peer and they **must** be identical on each peer (the order in which they appear is not important).

The cluster pre-shared key has to be specified on each peer and **must** be identical for all peers.

## Ethernet

The Ethernet speed is specific to each peer. Each peer may have slightly different requirements for the connection to their Ethernet switch.

## IP

---

**Note:** Never change the Primary LAN 1 IP address of a TelePresence Conductor that is part of a cluster. The only IP settings that can be changed when the system is part of a cluster are the additional IPv4 addresses.

---

The IPv4 address is specific to each peer. It **must** be different for each peer in the cluster.

The IPv4 subnet mask is specific to each peer. It can be different for each peer in the cluster.

The IPv4 gateway is specific to each peer. Each peer can use a different gateway.

Any additional IPv4 addresses added for use with Unified CM must be different for each peer in the cluster.

## System host name and domain

The system host name is specific to each peer. We recommend that it is different for each peer in the cluster so that you can easily identify each system.

The DNS domain name is specific to each peer.

## DNS servers

DNS servers are specific to each peer. Each peer can use a different set of DNS servers.

## Time

The NTP servers are specific to each peer. Each peer may use one or more different NTP servers.

The time zone is specific to each peer. Each peer may have a different local time.

## SNMP

SNMP settings are specific to each peer. They can be different for each peer.

## Logging

The **Event Log** and **Configuration Log** on each peer will only report activity for the local TelePresence Conductor.

The list of remote syslog servers is specific to each peer. We recommend that you set up a remote syslog server to which the logs of all peers can be sent. This will allow you to have a global view of activity across all peers in the cluster.

## Security certificates

The Trusted CA Certificate and Server Certificate used by the TelePresence Conductor are specific to each peer. They must be uploaded individually on each peer.

## Administration access

The SSH service and LCD panel settings are specific to each peer. They can be different for each peer.

## Root account password

The password for the root account is specific to each peer. Each peer may have a different password, and for security reasons we recommend that they do.

---

**Note:** The username and password for the administrator account is shared across peers.

---

## Locations

All ad hoc or rendezvous IP addresses assigned to Locations must be different for each peer in the cluster.

# Troubleshooting

## Unable to cluster the TelePresence Conductor

When running a TelePresence Conductor without a valid release key (as TelePresence Conductor Essentials) clustering is not supported. Contact your Cisco account representative to obtain release key and option keys.

## Appendix 1: IP ports and protocols

It is unusual to have any sort of firewall between cluster peers, but if there is, the IP protocols and ports that must be open between each and every TelePresence Conductor peer in the cluster are listed below.

For cluster communications between TelePresence Conductor peers:

- UDP port 500 (ISAKMP) is used for PKI (Public Key Infrastructure) key exchange
- Standard SIP and H.323 signaling ports are used for calls
- UDP port 1719 is used for bandwidth updates between TelePresence Conductor peers
- IP protocol 51 (IPSec AH) is used for database synchronization

If you are using the TelePresence Conductor's built-in **Firewall rules** feature then you must ensure that it is not configured to drop or reject traffic sent to UDP ports 4369 – 4380.

### IPSec communications

For IPSec between TelePresence Conductor cluster peers:

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

### MTU size

The default MTU size on the TelePresence Conductor is 1500 bytes. Under normal conditions this has no effect on the cluster. However, if there are network elements between the cluster peers (which is not recommended), you must ensure consistent MTU size throughout the path. Cluster replication could fail if the MTU is lower on the path between peers, because the synchronization packets are not allowed to fragment.

Determine which network element in the paths between peers has the lowest MTU value, then adjust each peer's cluster interface to use that value.

## Document revision history

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

| <b>Date</b>    | <b>Description</b>   |
|----------------|--|
| March 2015     | Added information about connections between Cisco TMSPE and TelePresence Conductor                                   |
| January 2015   | Updated for release XC3.0. Added information on MTU size.  |
| September 2014 | Updated for XC2.4  |
| April 2014     | Updated for XC2.3  |
| December 2013  | Updated the IP ports and protocols section   |
| October 2013   | Updated the Prerequisites section with changes introduced in XC2.2.1   |
| August 2013    | Updated for XC2.2  |
| May 2013       | Updated for XC2.1  |
| December 2012  | Updated for XC2.0. Information regarding clustering with Cisco Unified Communications Manager split out into D15000. |
| May 2012       | Updated for XC1.2  |
| May 2012       | Updated for XC1.1  |

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

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

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

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

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

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

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

© 2015 Cisco Systems, Inc. All rights reserved.