



# Backing Up and Restoring Security for Cisco Unified CallManager

If you configured security in your Cisco Unified CallManager 4.0 or 4.1 cluster, the following information applies for backups and restorations:

- Use the latest version of BARS to back up data.
- BARS 4.0(7) and later backs up the CTL file and security-related configuration that exists in the database.
- Unless specifically stated otherwise, all guidelines in this manual apply.
- All CTL operations depend on the Cisco CTL Provider service in Cisco Unified CallManager Serviceability. Ensure that the service is activated and running when you use the CTL client after restorations complete.
- Any time that you update the CTL file, always run BARS, as described in this manual.

This section contains the following topics:

- [Backing Up and Restoring Security for Cisco Unified CallManager 4.0, page 5-1](#)
- [Backing Up and Restoring Security for Cisco Unified CallManager 4.1, page 5-6](#)

## Backing Up and Restoring Security for Cisco Unified CallManager 4.0

If you implemented the CTL client and CAPF functionality in Cisco Unified CallManager 4.0, use the following procedures for backups and restorations:

- [Backing Up CAPF 1.0\(1\) Files for Cisco Unified CallManager 4.0, page 5-2](#)
- [Restoring Data Only When Security Exists in the Cisco Unified CallManager 4.0 Cluster, page 5-2](#)
- [Replacing a Secure 4.0 Publisher Database Server Where CAPF Utility 1.0\(1\) Was Installed, page 5-2](#)
- [Replacing a Secure 4.0 Subscriber Server Where CAPF Utility 1.0 \(1\) Was Installed, page 5-3](#)
- [Replacing a Secure 4.0 Publisher Database Server Where CAPF Was Not Installed, page 5-4](#)
- [Replacing a Secure 4.0 Subscriber Server Where CAPF Was Not Installed, page 5-5](#)

*FINAL REVIEW DRAFT - Cisco Confidential***Backing Up CAPF 1.0(1) Files for Cisco Unified CallManager 4.0**

If you use CAPF utility 1.0(1) with Cisco Unified CallManager 4.0, perform the following procedure to back up the CAPF files.

**Procedure**

- 
- Step 1** Use the latest version of BARS to back up the Cisco Unified CallManager data on the publisher database server.
- Step 2** Locate the server in the cluster where you installed CAPF utility 1.0(1). Copy **capf.phone** and all **.0 files** from the CAPF installation directory to a directory on a remote computer.
- The default location for the CAPF installation specifies C:\Program Files\Cisco\capf.
- 

**Restoring Data Only When Security Exists in the Cisco Unified CallManager 4.0 Cluster**

To restore 4.0 data when security exists in your Cisco Unified CallManager 4.0 cluster, perform the following procedure:

**Procedure**

- 
- Step 1** Restore the data, as described in this manual.
- Step 2** Update the CTL file; sign the CTL file with a token that exists in the file and that the phone trusts.
- Step 3** In Cisco Unified CallManager Serviceability, restart the Cisco CallManager and Cisco TFTP services.
- Step 4** Reset the devices.
- 


**Replacing a Secure 4.0 Publisher Database Server Where CAPF Utility 1.0(1) Was Installed**

To replace a secure Cisco Unified CallManager 4.0 publisher database server where CAPF Utility 1.0(1) was installed, perform the following procedure:

**Procedure**

- 
- Step 1** Obtain at least one token that exists in the current CTL file and that the phone trusts. You must use the token later in this procedure.
- Step 2** On the new or rebuilt server, perform the following operating system tasks:
- a. Use the Cisco-provided disks to install the Windows 2000 or 2000 or 2003 operating system.
  - b. Upgrade the operating system to match the version that currently runs in the cluster.
  - c. Apply operating system service releases to match the version that runs in the cluster.

*FINAL REVIEW DRAFT - Cisco Confidential*

- Step 3** On the new or rebuilt server, perform the following Cisco Unified CallManager installation tasks:
- Use Cisco-provided disks to install Cisco Unified CallManager.
  - Upgrade Cisco Unified CallManager to match the version that runs in the cluster.
  - Apply Cisco Unified CallManager service releases and engineering specials to match the version that runs in the cluster.
  - Identify the location where you previously installed CAPF on the publisher database server. Reinstall CAPF utility 1.0(1) to the same location on the new or rebuilt server, as described in *Cisco Unified IP Phone Authentication and Encryption for Cisco Unified CallManager 4.0*.
  - If the CTL client previously existed on the publisher database server, go to Cisco Unified CallManager Administration and install the CTL client.
  - On the new or rebuilt server, install the version of BARS that created the BARS backup file in the [“Backing Up CAPF 1.0\(1\) Files for Cisco Unified CallManager 4.0”](#) section on page 5-2.
- Step 4** Use BARS to restore the data on the new or rebuilt publisher database server; verify that the restored data exists on the publisher database server.
- Step 5** Copy the files that were backed up in [Step 2](#) in the [“Backing Up CAPF 1.0\(1\) Files for Cisco Unified CallManager 4.0”](#) section on page 5-2 to the CAPF installation directory on the new or rebuilt publisher database server.
- Step 6** Run the CTL client to update the CTL file; make sure that you click the **Update CTL file** radio button and sign the file with a token that exists in the file and that the phone trusts.
-  **Tip** Because the CTL file gets restored, do not choose the Mixed Mode or Non-Secure Mode options after you launch and run the CTL client.
- Step 7** In Cisco Unified CallManager Serviceability, restart the Cisco TFTP and Cisco CallManager services.
- Step 8** Reset all devices.


## Replacing a Secure 4.0 Subscriber Server Where CAPF Utility 1.0 (1) Was Installed

To replace a secure Cisco Unified CallManager 4.0 subscriber server where CAPF utility 1.0(1) was installed, performed the following procedure:

### Procedure

- Step 1** Obtain at least one token that exists in the current CTL file and that the phone trusts. You must use the token later in this procedure.
- Step 2** Verify that you performed the tasks in the [“Backing Up CAPF 1.0\(1\) Files for Cisco Unified CallManager 4.0”](#) section on page 5-2.
- Step 3** On the new or rebuilt server, perform the following operating system tasks:
- Use the Cisco-provided disks to install the Windows 2000 or 2000 or 2003 operating system.
  - Upgrade the operating system to match the version that currently runs in the cluster.
  - Apply operating system service releases to match the version that runs in the cluster.

*FINAL REVIEW DRAFT - Cisco Confidential*

- Step 4** On the new or rebuilt server, perform the following Cisco Unified CallManager installation tasks:
- Use Cisco-provided disks to install Cisco Unified CallManager.
  - Upgrade Cisco Unified CallManager to match the version that runs in the cluster.
  - Apply Cisco Unified CallManager service releases and engineering specials to match the version that runs in the cluster.
  - Identify the location where you previously installed CAPF on the subscriber server. Reinstall CAPF utility 1.0(1) to the same location on the new or rebuilt server, as described in *Cisco Unified IP Phone Authentication and Encryption for Cisco Unified CallManager 4.0*.
  - If the CTL client previously existed on the subscriber server, go to Cisco Unified CallManager Administration and install the CTL client.
- Step 5** Copy all **.0 files** from C:\Program Files\Cisco\Certificates on the publisher database server to the C:\Program Files\Cisco\Certificates on the new or rebuilt subscriber server.
- Step 6** Copy the files that were backed up in **Step 2** in the [“Backing Up CAPF 1.0\(1\) Files for Cisco Unified CallManager 4.0”](#) section on page 5-2 to the CAPF installation directory on the new or rebuilt subscriber server.
- Step 7** Run the CTL client to update the CTL file; make sure that you click the **Update CTL file** radio button and sign the file with a token that exists in the file and that the phone trusts.
-  **Tip** Because the CTL file gets restored, do not choose the Mixed Mode or Non-Secure Mode options after you launch and run the CTL client.
- Step 8** In Cisco Unified CallManager Serviceability, restart the Cisco CallManager and Cisco TFTP services.
- Step 9** Reset all devices.
- 

**Replacing a Secure 4.0 Publisher Database Server Where CAPF Was Not Installed**

To replace a secure Cisco Unified CallManager 4.0 publisher database where CAPF utility 1.0(1) was not installed, perform the following procedure:

**Procedure**

- 
- Step 1** Obtain at least one token that exists in the current CTL file and that the phone trusts. You must use the token later in this procedure.
- Step 2** On the new or rebuilt server, perform the following operating system tasks:
- Use the Cisco-provided disks to install the Windows 2000 or 2003 operating system.
  - Upgrade the operating system to match the version that currently runs in the cluster.
  - Apply operating system service releases to match the version that runs in the cluster.
- Step 3** On the new or rebuilt server, perform the following Cisco Unified CallManager installation tasks:
- Use Cisco-provided disks to install Cisco Unified CallManager.
  - Upgrade Cisco Unified CallManager to match the version that runs in the cluster.
  - Apply Cisco Unified CallManager service releases and engineering specials to match the version that runs in the cluster.

*FINAL REVIEW DRAFT - Cisco Confidential*

- Step 4** If the CTL client previously existed on the publisher database server, go to Cisco Unified CallManager Administration and install the CTL client on the new or rebuilt server.
- Step 5** On the new or rebuilt server, install the version of BARS that created the BARS backup file in the “[Backing Up CAPF 1.0\(1\) Files for Cisco Unified CallManager 4.0](#)” section on page 5-2.
- Step 6** Use BARS to restore the data on the new or rebuilt publisher database server; verify that the restored data exists on the publisher database server.
- Step 7** Run the CTL client to update the CTL file; make sure that you click the **Update CTL file** radio button and sign the file with a token that exists in the file and that the phone trusts.




---

**Tip** Because the CTL file gets restored, do not choose the Mixed Mode or Non-Secure Mode options after you launch and run the CTL client.

---

- Step 8** In Cisco Unified CallManager Serviceability, restart the Cisco TFTP and Cisco CallManager services.
- Step 9** Reset all devices.
- 

## Replacing a Secure 4.0 Subscriber Server Where CAPF Was Not Installed

To replace a secure Cisco Unified CallManager 4.0 subscriber server where CAPF utility 1.0(1) was not installed, perform the following procedure:

### Procedure

---

- Step 1** Obtain at least one token that exists in the current CTL file and that the phone trusts. You must use the token later in this procedure.
- Step 2** On the new or rebuilt server, perform the following operating system tasks:
- Use the Cisco-provided disks to install the Windows 2000 or 2003 operating system.
  - Upgrade the operating system to match the version that currently runs in the cluster.
  - Apply operating system service releases to match the version that runs in the cluster.
- Step 3** On the new or rebuilt server, perform the following Cisco Unified CallManager installation tasks:
- Use Cisco-provided disks to install Cisco Unified CallManager.
  - Upgrade Cisco Unified CallManager to match the version that runs in the cluster.
  - If the CTL client previously existed on the subscriber server, go to Cisco Unified CallManager Administration and install the CTL client on the new or rebuilt server.
  - Apply Cisco Unified CallManager service releases and engineering specials to match the version that runs in the cluster.
- Step 4** Copy all **.0 files** from C:\Program Files\Cisco\Certificates on the publisher database server to C:\Program Files\Cisco\Certificates on the new or rebuilt subscriber server.

*FINAL REVIEW DRAFT - Cisco Confidential*

- Step 5** Run the CTL client to update the CTL file; make sure that you click the **Update CTL file** radio button and sign the file with a token that exists in the file and that the phone trusts.



**Tip** Because the CTL file gets restored, do not choose the Mixed Mode or Non-Secure Mode options after you launch and run the CTL client.

- Step 6** In Cisco Unified CallManager Serviceability, restart the Cisco CallManager and Cisco TFTP services on the subscriber server.

- Step 7** Reset all devices.

## Backing Up and Restoring Security for Cisco Unified CallManager 4.1

If you implemented the CTL client and CAPF functionality in Cisco Unified CallManager 4.1, use the following procedures for backups and restorations:

- [Restoring Data Only, page 5-6](#)
- [Replacing an Existing or Failed Secure 4.1 Publisher Database Server, page 5-6](#)
- [Replacing an Existing/Failed Secure 4.1 Subscriber Server, page 5-7](#)
- [Restoring the 4.1 Cisco Unified CallManager Cluster That Uses Security, page 5-8](#)

### Restoring Data Only

If you implemented security, you must update the CTL file after you restore the data; sign the CTL file with a token that exists in the file and that the phone trusts.

For data restorations, you do not need to re-create the Cisco Unified CallManager self-signed certificate/keys or the CAPF certificate/keys. If you copied the Cisco Unity certificate to all servers in the cluster prior to the data restoration, you do not need to copy the certificate again.

### Replacing an Existing or Failed Secure 4.1 Publisher Database Server

When you replace an existing/failed publisher database server, the Cisco Unified CallManager installation automatically installs the Cisco Unified CallManager self-signed certificate/keys and the CAPF certificate/keys on the server.

If you need to replace or rebuild an existing/failed publisher database server and you configured security prior to the replacement/rebuild, perform the following procedure:

#### Procedure

- Step 1** Obtain at least one token that exists in the current CTL file and that the phone trusts. You must use the token in [Step 9](#).
- Step 2** Use the latest version of BARS to back up the Cisco Unified CallManager data on the existing publisher database server.

*FINAL REVIEW DRAFT - Cisco Confidential*

- Step 3** On the new or rebuilt server, perform the following operating system tasks:
- Use the Cisco-provided disks to install the Windows 2000 or 2003 operating system.
  - Upgrade the operating system to match the version that currently runs in the cluster.
  - Apply operating system service releases to match the version that runs in the cluster.
- Step 4** On the new or rebuilt server, perform the following Cisco Unified CallManager installation tasks:
- Use Cisco-provided disks to install Cisco Unified CallManager.
  - Upgrade Cisco Unified CallManager to match the version that runs in the cluster.
  - Apply Cisco Unified CallManager service releases and engineering specials to match the version that runs in the cluster.
- Step 5** On the new or rebuilt server, install the version of BARS that created the backup file in [Step 2](#).
- Step 6** Use BARS to restore the data on the new or rebuilt publisher database server.
- Step 7** Verify that the restored data exists on the publisher database server.
- Step 8** If the CTL client exists on a subscriber server or a PC/workstation, go to [Step 9](#). If the CTL client existed on the failed publisher database server, go to Cisco Unified CallManager Administration and install the CTL client.




---

**Tip** Because the CTL file gets restored, do not choose the Mixed Mode or Non-secure cluster security option after you launch and run the CTL client.

---

- Step 9** Run the CTL client to update the CTL file; make sure that you click the **Update CTL file** radio button and sign the file with a token that exists in the file and that the phone trusts.
- Step 10** Restart the Cisco TFTP and Cisco CallManager services.
- Step 11** Reset all devices.
- 

## Replacing an Existing/Failed Secure 4.1 Subscriber Server


If you are replacing an existing/failed secure subscriber server and you configured security prior to the replacement/rebuild, perform the following tasks:

### Procedure

---

- Step 1** Obtain at least one token that exists in the current CTL file and that the phone trusts. You must use the token in [Step 5](#).
- Step 2** On the new or rebuilt subscriber server, perform the following operating system tasks:
- Use the Cisco-provided disks to install the Windows 2000 or 2003 operating system.
  - Upgrade the operating system to match the version that currently runs in the cluster.
  - Apply operating system service releases to match the version that currently runs in the cluster.

*FINAL REVIEW DRAFT - Cisco Confidential*

- Step 3** On the new or rebuilt subscriber server, perform the following Cisco Unified CallManager installation tasks:
- Use Cisco-provided disks to install Cisco Unified CallManager.
  - Upgrade Cisco Unified CallManager to match the version that runs in the cluster.
  - Apply Cisco Unified CallManager service releases and engineering specials to match the version that runs in the cluster.
- Step 4** If the CTL client exists on the publisher database server or a PC/workstation, go to [Step 5](#). If the CTL client existed on the failed subscriber server, browse to Cisco Unified CallManager Administration and install the CTL client.
-  **Tip** Because the CTL file gets restored, do not choose the Mixed Mode or Non-secure cluster security option after you launch and run the CTL client.
- Step 5** Run the CTL client to update the CTL file; click the **Update CTL File** radio button and sign the file with a token that existed in the file and is trusted by the phones.
- Step 6** Restart the Cisco CallManager and Cisco TFTP services.
- Step 7** Reset all devices.
- 

**Restoring the 4.1 Cisco Unified CallManager Cluster That Uses Security**

Before you restore a secure cluster, ensure that your situation meets all of the following criteria:

- Every server in the cluster crashed.
- You configured security prior to the restoration.
- The phones and the backup file contain a valid CTL file.

If your situation meets the preceding criteria, perform the following tasks:

1. Obtain at least one token that exists in the current CTL file and that the phone trusts.
2. Restore the entire cluster, as described in the BARS documentation. Start with the publisher database server. After you complete the restoration on the publisher database server, restore the subscriber servers one at a time.
3. If the CTL client existed on a failed server in the cluster, reinstall the CTL client on the new or rebuilt server.
4. Run the CTL client. Click the **Update CTL file** radio button and make sure that you sign the file with a token that exists in the CTL file and that the phone trusts.



**Tip** Because the CTL file gets restored, do not choose the Mixed Mode or Non-secure cluster security option after you launch and run the CTL client.

---

5. Restart the Cisco TFTP and Cisco CallManager services.
  6. Reset all devices.
-