



## Working with TAPS

---

Use the Tool for Auto-Registered Phones Support (TAPS) in conjunction with BAT to provide two features:

- Update MAC addresses and download predefined configuration for new phones
- Reload configuration for replacement phones

When adding new phones to Cisco CallManager, TAPS works in conjunction with BAT to update phones that were added to BAT using dummy MAC addresses. After the phones with dummy MAC addresses have been bulk-added to Cisco CallManager Administration using BAT, you can plug the phones into the network. You or the phone's user can dial a TAPS directory number that causes the phone to download its configuration. At the same time, the phone is updated in Cisco CallManager Administration with the correct MAC address. Auto-registration must be enabled in Cisco CallManager Administration (**System > Cisco CallManager**) for TAPS to function.

For example, you have 100 new hires starting on Monday. You must add these users and their new phones to Cisco CallManager Administration. You can use BAT to create a phone template for these 100 users and a CSV file for phones and users. By using the dummy MAC address option in the CSV file, you do not need to input the individual MAC addresses for the 100 new phones. Now, as long as auto-registration is enabled, the phones can be plugged directly into the network, and configured by simply dialing the TAPS directory number (by you or the new hire) and following the voice prompt instructions.

When replacing an existing phone (due to damage, for example), use Configure TAPS so that the user can receive a new phone, plug it into the network, and dial the TAPS directory number to download the configuration used by the previous

phone. Auto-registration must be enabled for Configure TAPS to work. No configuration changes need to be made by the user or in Cisco CallManager Administration.

For example, John's Cisco IP Phone 7940 gets short-circuited during a lightning storm. He receives a new Cisco IP Phone 7940 and plugs it into the network. John can dial the TAPS directory number, and the new phone will download the configuration previously used for the damaged phone. No need exists to change directory numbers or update device information in Cisco CallManager Administration — TAPS does it automatically. See the [“Configuring TAPS” section on page 6-3](#) for more information.

You must enable auto-registration in Cisco CallManager Administration (**System > Cisco CallManager**) for TAPS to function. If auto-registration is not enabled in Cisco CallManager Administration (**System > Cisco CallManager**), TAPS will not function.

Because TAPS can replace a directory number, you may want to protect certain directory numbers from being overwritten. You can protect important numbers by using the Secure TAPS application. See the [“Securing TAPS” section on page 6-7](#) for more information.

The TAPS application, which is installed on a Cisco CRA server, also requires components to be installed on the server running the Cisco CallManager Publisher database.

**Note**

---

TAPS requires the Cisco IP Interactive Voice Response (IP IVR) application that runs on the Cisco Customer Response Application (Cisco CRA) server. You must purchase an IP IVR for TAPS to work.

---

Do not use TAPS if you are specifying each phone's MAC address during the bulk-add.

**Related Topics**

- [Configuring TAPS, page 6-3](#)
- [Securing TAPS, page 6-7](#)
- [Starting TAPS, page 6-6](#)
- [Stopping TAPS, page 6-7](#)
- [TAPS for End Users, page 6-12](#)

# Configuring TAPS

You must configure TAPS by adding a CTI route point, CTI ports, and users in Cisco CallManager Administration. Like any other application in the Cisco IP telephony system, TAPS requires configuring. See the Cisco CRA Release Notes for complete information. You can review the Application Server documentation by browsing to <http://www.cisco.com> and clicking **Software Center > Voice Software > Cisco CRA**. Open the documentation for instructions on how to configure an application.

You need only one CTI route point for TAPS. You will need at least one CTI port, but you can configure as many ports as you would like to make available to TAPS users.

In Cisco CallManager Administration

- Create a CTI route point and assign it a unique directory number.
- Set call forward busy, call forward no answer, and call forward on failure to the operator number on the TAPS CTI route point.
- Create one or more CTI ports with consecutive directory numbers. You can create CTI ports in BAT or Cisco CallManager Administration.

TAPS supports a maximum number of sessions equal to the number of CTI ports configured for TAPS. For example, if you have configured five CTI ports, up to five users can dial into TAPS at any time. The sixth caller cannot connect to TAPS.

- Create a user. The TAPS route point and ports should be in the user's control devices list.
- Create an auto-registration partition/calling search space to prevent phones that have auto-registered from dialing any directory number other than the directory number assigned to the TAPS CTI route point. Restricting access to this directory number ensures that users download the proper configuration information for their phones.
- Upload **TAPS.aef** using the Repository Manager on the Cisco CRA server. See Step 2 in the [“Installing TAPS” section on page 2-4](#) for instructions.

For information about how to add or assign these values, see the *Cisco CallManager Administration System Guide*.

**Related Topics**

- [Allowing TAPS to Update Any Cisco IP Phone Added Using Auto-Registration, page 6-4](#)
- [Restricting TAPS to Update Only Cisco IP Phones Added Using the Dummy MAC Address Option in BAT, page 6-5](#)

## Allowing TAPS to Update Any Cisco IP Phone Added Using Auto-Registration

The Configure TAPS feature allows you to use TAPS to update phones that auto-registered regardless of whether they were entered into the Cisco CallManager database via Cisco CallManager Administration or via BAT using a dummy MAC address. By default, use of TAPS is limited to only those phones added using the dummy MAC address option in BAT. Phones with dummy MAC addresses have a device name that starts with the prefix 'BAT'. But you can use Configure TAPS to allow any phone that auto-registered in the Cisco CallManager system to be updated, including phones that have a MAC address that is not preceded by 'BAT'. This is useful when you need to replace one phone with a same model phone. As long as auto-registration is enabled in Cisco CallManager Administration, the user can plug in the new phone and then dial the TAPS directory number to retrieve the configuration previously used by the old phone.

Use the following steps to configure TAPS so that the device profile of any phone on the system can be updated, not just phones added to BAT using the dummy MAC address option.

**Procedure**

- 
- Step 1** On the Cisco CRA server, clicking **Start > Programs > Cisco CallManager > Bulk Admin Tool > Configure TAPS**.

The Configure TAPS window displays.

- Step 2** Click the second button, **Allow Auto-Registered phones to be reset with any phone**.

- Step 3** Click **Set**.

A prompt asks you whether you wish to save the new setting.

**Step 4** Click **Yes**.

Another prompt confirms that TAPS will allow any phone that auto-registered to be updated using TAPS (not just phones that were added using the dummy MAC address option).

**Step 5** Click **OK**.

TAPS allows any phone added to the Cisco CallManager database using auto-registration to be updated by TAPS. The Configure TAPS window automatically closes.

---

**Related Topics**

- [Restricting TAPS to Update Only Cisco IP Phones Added Using the Dummy MAC Address Option in BAT, page 6-5](#)

## Restricting TAPS to Update Only Cisco IP Phones Added Using the Dummy MAC Address Option in BAT

By default, use of TAPS is limited to only those phones added using the dummy MAC address option in BAT. Phones added to the Cisco CallManager database with dummy MAC addresses always have a device name that starts with the prefix 'BAT'. However, if you have changed the configuration of TAPS to allow any phone that was added to the system using auto-registration (as explained in the section, [Allowing TAPS to Update Any Cisco IP Phone Added Using Auto-Registration, page 6-4](#)), then you must follow these steps to restore the default setting so that TAPS can only be used to update phones with the 'BAT' prefix.

**Procedure**

---

**Step 1** On the Cisco CRA server, clicking **Start > Programs > Cisco CallManager > Bulk Admin Tool > Configure TAPS**.

The Configure TAPS window displays.

**Step 2** Click the first button, **Allow Auto-Registered phones to be reset with a profile that has 'BAT' prefix in the device**.

**Step 3** Click **Set**.

A prompt asks you whether you wish to save the new setting.

**Step 4** Click **Yes**.

Another prompt confirms that TAPS will allow only phones that were added using the dummy MAC address option in BAT to be updated.

**Step 5** Click **OK**.

TAPS allows only phones added to the Cisco CallManager database using the dummy MAC address option to be updated by TAPS. The Configure TAPS window automatically closes.

---

#### Related Topics

- [Allowing TAPS to Update Any Cisco IP Phone Added Using Auto-Registration, page 6-4](#)

## Starting TAPS

You must manually start the TAPS service. Perform the following steps to start TAPS.

Procedure

---

**Step 1** On the server running the Publisher database for Cisco CallManager, click **Start > Programs > Administrative Tools > Services**.

The Services window displays.

**Step 2** Double-click **Cisco TAPS**.

The TAPS service is now running. If the server should fail, you must manually start TAPS again.

---

#### Related Topics

- [Stopping TAPS, page 6-7](#)

# Stopping TAPS

Stop the TAPS service from the Services window on the Publisher server (where BAT is installed).

## Procedure

---

- Step 1** On the server running the Publisher database for Cisco CallManager, click **Start > Programs > Administrative Tools > Services**.
- The Services window displays.
- Step 2** In the list of services, right-click Cisco TAPS and choose **Stop**.
- 

## Related Topics

- [Starting TAPS, page 6-6](#)

# Securing TAPS

The Secure TAPS feature lets you specify directory numbers that the TAPS feature cannot access. Use this capability when you want to protect directory numbers from being accidentally assigned.

For example, in your system, the directory number 5000 provides voice mail access. You do not want a new user to mistakenly configure 5000 on the new phone. Secure TAPS allows you to specify the directory numbers that TAPS cannot access.

## Related Topics

- [Restricting Directory Numbers, page 6-8](#)
- [Lifting the Restriction on a Directory Number, page 6-9](#)
- [Resetting Directory Numbers, page 6-10](#)
- [Viewing a List of Restricted Directory Numbers, page 6-11](#)

## Restricting Directory Numbers

Use the following steps to block TAPS from using directory numbers that you specify.

### Procedure

---

**Step 1** On the Cisco CRA server, click **Start > Programs > Cisco CallManager > Bulk Admin Tool > Secure TAPS**.

The Secure TAPS Directory Numbers window displays.

**Step 2** In the field, enter the directory number you want to protect from TAPS.

**Step 3** Click **Add**.

A prompt indicates the directory number has been secured from use with TAPS.

**Step 4** Click **OK**.

**Step 5** Continue to add directory numbers by repeating Steps 2 through 4. When you've finished adding directory numbers, click **View Secure DN**.

A list box displays the directory numbers you have protected. The directory numbers shown in this list cannot be used by TAPS. If a user tries to update a device profile by entering one of the directory numbers in this list, TAPS will refuse the request.



### Note

The View Secure DN list box does not automatically refresh. If you want to see the latest list of secured directory numbers, you must close the list box and then click **View Secure DN** to redisplay an updated list.

---

**Step 6** Click **Exit**.

A prompt asks you to confirm that you want to exit Secure TAPS.

**Step 7** Click **Yes** to exit.

---

### Related Topics

- [Securing TAPS, page 6-7](#)
- [Lifting the Restriction on a Directory Number, page 6-9](#)

- [Resetting Directory Numbers, page 6-10](#)
- [Viewing a List of Restricted Directory Numbers, page 6-11](#)

## Lifting the Restriction on a Directory Number

Use the following steps to remove a directory number from the list of directory numbers that TAPS cannot access.

### Procedure

---

**Step 1** On the Cisco CRA server, click **Start > Programs > Cisco CallManager > Bulk Admin Tool > Secure TAPS**.

The Secure TAPS Directory Numbers window displays.

**Step 2** In the field, enter the directory number you want to unprotect from TAPS.

**Step 3** Click **Remove**.

A prompt indicates the directory number has been removed from the list of secured directory numbers.

**Step 4** Click **OK**.

**Step 5** Continue to remove directory numbers by repeating Steps 2 through 4. When you've finished removing directory numbers, click **View Secure DN**.

A list box displays the directory numbers that are protected. The directory numbers shown in this list cannot be used by TAPS. If a user tries to update a device profile by entering one of the directory numbers in this list, TAPS will refuse the request.



### Note

---

The View Secure DN list box does not automatically refresh. If you want to see the latest list of secured directory numbers, you must close the list box and then click **View Secure DN** to redisplay an updated list.

---

**Step 6** Click **Exit**.

A prompt asks you to confirm that you want to exit Secure TAPS.

**Step 7** Click **Yes** to exit.

---

#### Related Topics

- [Securing TAPS, page 6-7](#)
- [Restricting Directory Numbers, page 6-8](#)
- [Resetting Directory Numbers, page 6-10](#)
- [Viewing a List of Restricted Directory Numbers, page 6-11](#)

## Resetting Directory Numbers

Use the following steps to reset the list of secured directory numbers. TAPS cannot use any directory number that has been specified in the list of secured directory numbers.

#### Procedure

---

**Step 1** On the Cisco CRA server, click **Start > Programs > Cisco CallManager > Bulk Admin Tool > Secure TAPS**.

The Secure TAPS Directory Numbers window displays.

**Step 2** Click **Resetting DN**.

A prompt indicates that no directory numbers will be secured from TAPS.

**Step 3** Click **Yes** to clear all directory numbers or click **No** to cancel the reset operation.

A prompt advises you that the list of directory numbers protected from TAPS has been cleared.

**Step 4** Click **OK**.

All directory numbers in the system can be updated using TAPS. If you want to protect directory numbers so they cannot be updated using TAPS, see [Restricting Directory Numbers, page 6-8](#).

---

**Related Topics**

- [Securing TAPS, page 6-7](#)
- [Restricting Directory Numbers, page 6-8](#)
- [Lifting the Restriction on a Directory Number, page 6-9](#)
- [Viewing a List of Restricted Directory Numbers, page 6-11](#)

## Viewing a List of Restricted Directory Numbers

Use these steps to view a list of directory numbers that TAPS cannot access.

**Procedure**

---

**Step 1** On the Cisco CRA server, click **Start > Programs > Cisco CallManager > Bulk Admin Tool > Secure TAPS**.

The Secure TAPS Directory Numbers window displays.

**Step 2** Click **View Secure DN**.

A list box displays. The directory numbers shown in this list cannot be used by TAPS. If a user tries to update a device profile by entering one of the directory numbers in this list, TAPS will refuse the request.

**Step 3** Close the list box.

**Step 4** Click **Exit**.

A prompt asks you to confirm that you want to exit Secure TAPS.

**Step 5** Click **Yes** to exit.

---

**Related Topics**

- [Securing TAPS, page 6-7](#)
- [Restricting Directory Numbers, page 6-8](#)
- [Lifting the Restriction on a Directory Number, page 6-9](#)
- [Resetting Directory Numbers, page 6-10](#)

# TAPS for End Users

Follow these steps to configure your new phone.

## Procedure

---

- Step 1** Plug the phone into a port.  
The phone automatically registers and displays a number.
- Step 2** Dial the TAPS extension provided by your system administrator.
- Step 3** Dial your personal extension number, provided by your system administrator, followed by #.



---

**Note** You may be instructed to enter the complete telephone number (including area code).

---

- Step 4** To confirm, enter your personal extension number again, followed by #.  
A confirmation displays.
- Step 5** Hang up the phone.  
The phone resets and displays your extension number.
- 

Contact your system administrator if you experience any problems.