Maintenance

Reset Device

A device reset provides a way to reset or restore various configuration and security settings or provides a way to recover the device if the device encounters an error.

The following procedure describes the types of resets that you can perform.

Note All three reset methods cause deletion of all user data and reset all settings from the device.

The following occurs on a device when you perform a reset:

- User configuration settings - Reset to default values.
- Network configuration settings - Reset to default values.
- Call histories - Get erased.
- Locale information - Reset to default values.
- Security settings - Reset to default values; this includes deletion of the CTL file and change of the 802.1x Device Authentication parameter to Disabled.

Note Do not power down the device until it completes the factory reset process.

Procedure

You can reset the device with any of these operations. Choose the operation that is appropriate for your situation.

- Method 1: Cisco Unified Communications Manager Administrator Web GUI

  1. From the Product Specific Configuration Layout area of the device configuration window, enable **Wipe Device**.
  2. Issue an Apply Config, Restart, or Reset command from the Admin GUI to push the wipe to the device.

- Method 2: Settings application

  1. In the Settings application, choose **Backup & reset** > **Factory data reset**.

     Note If a PIN or Password is configured on the device, it will need to be entered before the reset can proceed.

- Method 3: Key-press sequences

  This method should be used if the device is secured with a PIN or Password lock and the PIN/password has been lost.

  Follow these steps to reset a Cisco DX70 on boot up:

  1. Power on the device and wait for the Mute LED to blink.
  2. Press and hold the **Volume Up** button until the **Mute** button is lit red.
  3. Release the **Volume Up** button, then press and hold the **Mute** button for 3 seconds.

  Follow these steps to reset a Cisco DX80 on boot up:

  1. Press and hold the **Volume Up** button and power on the device.
  2. Release the **Volume Up** button when the **Mute** button is lit red, then press the **Mute** button.

  Follow these steps to reset a Cisco DX650 on boot up:

  1. Press and hold the # key and power on the device.
  2. When the Message Waiting Indicator (MWI) flashes red once then stays lit, release the # key.

Reset Options and Load Upgrades

Cisco DX Series devices receive configuration changes and load upgrades from Cisco Unified Communications Manager. The following protocol describes how the device handles change requests:

- Reset waits for active call to end.

- If the device screen is on, user receives a popup dialog box that notifies the user about the changes and the need for restart. The dialog box provides the following options:
  - Restart: Dismisses the popup dialog box and restarts the device (default action).
  - Snooze: Dismisses the popup dialog box for an hour. The user can set the device to snooze for a maximum of 24 hours, after which the device will restart.

    Note The popup dialog box has a countdown timer of 60 seconds. The default action begins if the user does not act.

    After the user sets the device to snooze, the user has the option to manually reset the device at any time from the notifications list.

  - If the device screen is off, active audio keeps the request waiting.

Remote Lock

This feature allows you to lock a device from the Device Configuration window in Cisco Unified Communications Manager.

When the device receives a remote lock request, the device immediately terminates any active calls, and the device locks. If the device is not registered with the system at the time of the request, the device is locked the next time that it registers to the system.

Note After you issue a remote lock request, the request cannot be canceled.

Remote Lock Device

Procedure

Step 1 In the **Phone Configuration** window for the device, click **Lock**.

Step 2 Click **Lock** to accept the Lock confirmation message.
You can view the Lock status in the Device Lock/Wipe Status section of the **Phone Configuration** window for the device.

Remote Wipe

This feature allows you to erase the data on a device from the Device Configuration window in Cisco Unified Communications Manager.

When the device receives a remote wipe request, the device immediately terminates any active calls and erases the device data. If the device is not registered with the system at the time of the request, the data is erased the next time that the device registers to the system.

Note After you issue a remote wipe request, the request cannot be canceled.

Remote Wipe Device

Procedure

Step 1 In the **Phone Configuration** window for the device, click **Wipe**.

Step 2 Click **Wipe** to accept the Wipe confirmation message.
You can view the Wipe status in the Device Lock/Wipe Status section of the **Phone Configuration** window for the device.

Boot Alternate Image for Cisco DX70

Procedure

Step 1 Power on the device and wait for the Mute LED to blink.

Step 2 Press and hold the **Volume Down** button until the **Mute** button is lit red.

Step 3 Release the **Volume Down** button, then press and hold the **Mute** button for 3 seconds.

Boot Alternate Image for Cisco DX80

Procedure

Step 1 Press and hold the **Volume Down** button and power on the device.

Step 2 Release the **Volume Down** button when the **Mute** button is lit red, then press the **Mute** button.

Boot Alternate Image for Cisco DX650

Procedure

Step 1 Disconnect the power to turn the device off.

Step 2 Press and hold the * key, then connect the power supply.

Step 3 Keep the * key held until the message LED becomes solid.

Step 4 When the message LED flashes 3 times, release the * key.
The device uses the alternate image to boot.

Data Migration

The data migration feature ensures that a factory reset is not required when data incompatibility exists after a firmware upgrade.

Note Data may still be lost upon downgrade to an earlier release of firmware. If you upgrade to a newer firmware release, you may not be able to revert to an earlier release without losing data.

If you downgrade to earlier firmware and the device is not able to migrate data, you receive an alarm. Instruct the user to back up the user data or perform a remote wipe of the device. When the device registers to Cisco Unified Communications Manager, the device detects prior factory resets, overrides migration, downgrades, and reboots. When the device reboots, it loads the downgraded firmware.

Debugging Log Profiles

You can turn on debugging log profiles remotely for a device or group of devices.

Set Debugging Log Profile for Call Processing

Procedure

Step 1 Go to the Product Specific Configuration Layout area of the individual device configuration window or Common Phone Profile window.

Step 2 Check **Log Profile**, and choose Telephony.

Step 3 Save your changes.

Step 4 The user is notified that debug logging is enabled in the notification area. The user can expand the message for more information, but cannot dismiss the notification.

Reset Debugging Log Profile to Default

Procedure

Step 1 Go to the Product Specific Configuration Layout area of the individual device configuration window or Common Phone Profile window.

Step 2 Check **Log Profile**, and select **Default** to reset all debugs to the default values. This includes debugs that have been set manually from Android Debug Bridge.

Step 3 Save and apply your changes.

Step 4 Choose **Preset** to keep the current debug levels.

Step 5 Save your changes.

User Support

To successfully use some of the features on their devices, users must receive information from you or from your network team or be able to contact you for assistance. Make sure to provide end users with the names of people to contact for assistance and with instructions for contacting those people.

Cisco recommends that you create a web page on your internal support site that provides users with important information about their device.

Problem Report Tool

Users submit problem reports to you with the Problem Report Tool.

Note The Problem Report Tool logs are required by Cisco TAC when troubleshooting problems.

To issue a problem report, users access the Problem Report Tool and provide the date and time that the problem occurred, and a description of the problem.

You must add a server address to the **Customer Support Upload URL** field on Cisco Unified Communications Manager.

If you are deploying devices with Mobile and Remote Access through Expressway, you must also add the PRT server address to the HTTP Server Allow list on the Expressway server.

Configure Customer Support Upload URL

You must use a server with an upload script to receive PRT files. The PRT uses an HTTP POST mechanism, with the following parameters included in the upload (utilizing multipart MIME encoding):

- devicename (example: “SEP001122334455”)
- serialno (example: “FCH12345ABC”)
- username (the username configured in CUCM, the device owner)
- prt_file (example: “probrep-20141021-162840.tar.gz”)

A sample script is shown below. This script is provided for reference only. Cisco does not provide support for the upload script installed on a customer's server.

```
<?php

// NOTE: you may need to edit your php.ini file to allow larger
// size file uploads to work.
// Modify the setting for upload_max_filesize
// I used:  upload_max_filesize = 20M

// Retrieve the name of the uploaded file
$filename = basename($_FILES['prt_file']['name']);

// Get rid of quotes around the device name, serial number and username if they exist
$devicename = $_POST['devicename'];
$devicename = trim($devicename, "'\"");

$serialno = $_POST['serialno'];
$serialno = trim($serialno, "'\"");

$username = $_POST['username'];
$username = trim($username, "'\"");

// where to put the file
$fullfilename = "/var/prtuploads/".$filename;

// If the file upload is unsuccessful, return a 500 error and
// inform the user to try again

if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
        header("HTTP/1.0 500 Internal Server Error");
        die("Error: You must select a file to upload.");
}

?>
```

Procedure

Step 1 Set up a server that can run your PRT upload script.

Step 2 Write a script that can handle the parameters listed above, or edit the provided sample script to suit your needs.

Step 3 Upload your script to your server.

Step 4 In Cisco Unified Communications Manager, go to the Product Specific Configuration Layout area of the individual device configuration window, Common Phone Profile window, or Enterprise Phone Configuration window.

Step 5 Check **Customer support upload URL** and enter your upload server URL.

Example:

http://example.com/prtscript.php

Step 6 Save your changes.

Take Screenshot From Web Browser

Procedure

Use your browser to go to this URL:http://<Endpoint IP Address>/CGI/Screenshot
You receive a prompt that asks for authentication. Use the associated user ID name and password.

Take Screenshot From Device

Procedure

Press the **Vol Down** button and **Power/Lock** button for three seconds.

Application Support

Evaluate whether the issue is a device issue or a problem with the application. If the problem is application related, contact the application support center directly.