Installation

Install Cisco DX Series Device

After you add devices to the Cisco Unified Communications Manager database, you can complete the device installation. You (or the users) can install the device at the user location.

Note Before you install a device, even if it is new, upgrade the device to the current firmware image. For information about upgrading, see the readme file for your device, which is located at:

http://software.cisco.com/download/release.html?mdfid=284721679&flowid=46173&softwareid=282074288

After the device connects to the network, the device startup process begins, and the device registers with Cisco Unified Communications Manager. To finish installation of the device, configure the network settings on the device depending on whether you enable or disable DHCP service.

If you used autoregistration, you need to update the specific configuration information for the device, such as associate the device with a user, or change the directory number.

The following steps provide an overview and checklist of installation tasks for Cisco DX Series devices. The steps present a suggested order to guide you through the device installation. Some tasks are optional, depending on your system and user needs.

Procedure

Step 1 Choose the power source.

- External power supply

- [Cisco DX650-only] Power over Ethernet (PoE)

  Note With PoE+ 802.3at, accessories that are plugged in to the device, such as mouse or keyboard, negotiate for power. If not enough power is available for the accessory, an error message appears on the screen. The device requires an external power supply when it is used in a WLAN environment.

Step 2 Assemble the device and connect the network cable. If you use the device in a WLAN environment, see Step 5.
This step locates and installs the device in the network.

Step 3 Monitor the device startup process. This step adds primary and secondary directory numbers and features that are associated with directory numbers to the device, and verifies that the device is configured properly.

Step 4 If you choose to deploy the device on a wireless network, skip to Step 5.
If you are configuring the Ethernet network settings on the device for an IP network, you can set up an IP address for the device either by use of DHCP or by manual entry of an IP address.

Step 5 If you choose to deploy the device on the wireless network, you must perform the following:

- Configure the wireless network.
- Enable wireless LAN for devices on Cisco Unified Communications Manager Administration.
- Configure a wireless network profile on the device.

Note The wireless LAN on the device does not activate when Ethernet cables are connected on the device.

Step 6 Make calls with the device to verify that the Call application and features work correctly.

Step 7 Provide information to end users about how to use and configure their devices.

Wireless LAN Setup

Ensure that the Wi-Fi coverage in the location where the wireless LAN is deployed is suitable for transmission of video and voice packets.

For complete wireless network configuration information, see the *Cisco DX Series Wireless LAN Deployment Guide*.

Wireless LAN Setup in Cisco Unified Communications Manager Administration

In Cisco Unified Communications Manager, you must enable a parameter called “Wi-Fi” for the device. You can enable this parameter in one of the following locations in Cisco Unified Communications Manager Administration:

- To enable wireless LAN on a specific device, choose **Enable** for the Wi-Fi parameter in the Product Specific Configuration Layout section (**Device** > **Phone**) for the specific device, and check **Override Common Settings**.
- To enable wireless LAN for a group of devices, choose **Enable** for the Wi-Fi parameter in a **Common Phone Profile Configuration** window (**Device** > **Device Settings** > **Common Phone Profile**), check

Override Common Settings, then associate the device (**Device** > **Phone**) with that common phone profile.

- To enable wireless LAN for all WLAN-capable devices in your network, choose **Enable** for the Wi-Fi parameter in the **Enterprise Phone Configuration** window (**System** > **Enterprise Phone Configuration**), and check **Override Common Settings**.

Note In the **Phone Configuration** window in Cisco Unified Communications Manager Administration (**Device** > **Phone**), use the Ethernet MAC address when you configure the MAC address. Cisco Unified Communications Manager registration does not use the wireless MAC address.

Provision Wireless LAN Profile

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Phone** > **Wireless LAN Profile**.

Step 2 Configure the Wireless LAN profile and click **Save**.

Provision Wireless LAN Profile Group

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Phone** > **Wireless LAN Profile Group**.

Step 2 Configure the Wireless LAN Profile Group and click **Save**.

Step 3 Choose **System** > **Device Pool** then add the Wireless LAN profile group to a device pool and click **Save**. Or, choose **Device** > **Phone** then add the Wireless LAN profile group to a specific device and click **Save**.

Network Settings Configuration

If you are not using DHCP in your network, you must configure these network settings on the device after you install the device on the network:

- IP address
- IP subnet information
- IPv6 addresses

- TFTP server IP address

If necessary, you may also configure the domain name and the DNS server settings.

Configure IPv4

Procedure

Step 1 In the Settings application, tap **Ethernet** > **IPv4 configuration**.

Step 2 Check **Use static IP**.

Step 3 Set the following options:

- IP address
- Gateway
- Netmask
- Domain name

  Note You can use option 15 to send multiple domain names to the device. Each domain name needs to be delimited by a space. Any other delimiter, such as a comma, is not supported. The domain names can also be entered manually if you are using a static IP address. Again, the space is the only valid delimiter. Currently, option 119 is not supported.
- DNS 1
- DNS 2

Renew IPv4

Procedure

In the Settings application, tap **Ethernet** > **Renew IPv4**.

Configure IPv6

Procedure

Step 1 In the Settings application, tap **Ethernet** > **IPv6 configuration**.

Step 2 Check **Use static IP**.

Step 3 Set the following options:

- IP address

- Default router
- Prefix length
- Domain name

  Note You can use option 15 to send multiple domain names to the device. Each domain name needs to be delimited by a space. Any other delimiter, such as a comma, is not supported. The domain names can also be entered manually if you are using a static IP address. Again, the space is the only valid delimiter. Currently, option 119 is not supported.

- DNS 1
- DNS 2

Renew IPv6

Procedure

In the Settings application, tap **Ethernet** > **Renew IPv6**.

Configure Ethernet Web Proxy

Procedure

Step 1 In the Settings application, tap **Ethernet** > **Proxy settings**.

Step 2 Choose the proxy setting type.

a) To set a manual proxy, enter the proxy hostname, proxy port, and any proxy bypasses. Check **Proxy requires authentication** if applicable.

b) To set an auto proxy, enter the PAC location, and any proxy bypasses. Check **Proxy requires authentication** if applicable.

Set Admin VLAN

Procedure

Step 1 In the Settings application, tap **Ethernet** > **Admin VLAN**.

Step 2 Enter an Admin VLAN ID value and tap **OK**.

Set SW Port Speed

Procedure

Step 1 In the Settings application, tap **Ethernet** > **SW port speed**.

Step 2 Select a port speed.
If the device is connected to a switch, configure the port on the switch to the same speed/duplex as the device, or configure both to autonegotiate. If you change the setting of this option, you must change the PC port speed to the same setting.

Set PC Port Speed

Procedure

Step 1 In the Settings application, tap **Ethernet** > **PC port speed**.

Step 2 Select a port speed.
If the device is connected to a switch, configure the port on the switch to the same speed/duplex as the device, or configure both to autonegotiate. If you change the setting of this option, you must change the SW port speed to the same setting.

Connect to Wi-Fi Network

Procedure

Step 1 In the Settings application, toggle **Wi-Fi** on.

Step 2 Tap **Wi-Fi**.

Step 3 Select a wireless network from the list of available networks.

Step 4 Enter the credentials and tap **Connect**.

Connect to Hidden Wi-Fi Network

Procedure

Step 1 In the Settings application, toggle **Wi-Fi** on.

Step 2 Tap **Wi-Fi**.

Step 3 Tap +.

Step 4 Enter the Network SSID, select the security type and credentials (if applicable).

Step 5 Tap **Save**.

Configure Wi-Fi Web Proxy

Procedure

Step 1 In the Settings application, tap **Wi-Fi**.

Step 2 Tap and hold a wireless network from the list of available networks.

Step 3 Tap **Modify network**.

Step 4 Check **Show advanced options**.

Step 5 Choose the proxy setting type.

a) To set a manual proxy, enter the proxy hostname, proxy port, and any proxy bypasses. Check **Proxy requires authentication** if applicable.

b) To set an auto proxy, enter the PAC location, and any proxy bypasses. Check **Proxy requires authentication** if applicable.

Step 6 Tap **Save**.

Configure Wi-Fi IP Settings

Procedure

Step 1 In the Settings application, tap **Wi-Fi**.

Step 2 Tap and hold a wireless network from the list of available networks.

Step 3 Tap **Modify network**.

Step 4 Check **Show advanced options**.

Step 5 Choose the IP settings type, and configure the following:

- IP address

- Gateway
- Network prefix length
- DNS 1
- DNS 2
- Domain name

Step 6 Tap **Save**.

Set Wi-Fi Frequency Band

Procedure

Step 1 In the Settings application, tap **Wi-Fi**.

Step 2 Tap **...**

Step 3 Tap **Wi-Fi frequency band** and choose a setting.

Mobile and Remote Access Through Expressway

Mobile and Remote Access through Expressway requires Cisco Expressway 8.6 or later and Cisco Unified Communications Manager 10.5.2 SU2 or Cisco Unified Communications Manager 11.0 or later.

Cisco Expressway provides a way for remote workers to easily and securely connect their Cisco DX Series devices into the corporate network without using a virtual private network (VPN) client tunnel. Expressway uses Transport Layer Security (TLS) to secure network traffic. For a DX Series device to authenticate an Expressway certificate and establish a TLS session, the Expressway certificate must be signed by a public Certificate Authority that is trusted by the DX Series firmware. It is not possible to install or trust other CA certificates on DX Series devices for authenticating an Expressway certificate. See Certificate Authority Trust List for the list of supported CA certificates.

To ensure that the users are able to use the Problem Report Tool, you must add the Problem Report Tool server address to the Expressway HTTP server allow list

When logging in to Expressway, the user is prompted for a Service Name, User ID, and Password. On first boot, off-premise users are prompted to log in to Expressway by the Setup Assistant. For devices that have previously been deployed, either on-premise or off-premise, you must convert the device to use Expressway.

With the **User Credentials Persistent for Expressway Sign In** parameter set in the Product Specific Options on Cisco Unified Communications Manager, the device stores a user's login credentials so that users do not need re-enter this information. User credentials stored on the device are encrypted.

For more information, see *Unified Communications Mobile and Remote Access via Cisco Expressway Deployment Guide*.

Mobile and Remote Access Limitations and Restrictions

- DX Series devices connected through Expressway cannot access web browsing, or email services hosted inside the enterprise network.
- The Off Hook/KPML Dialing, Mobility, DND, Call Back, and drop conference participants features are only supported with Expressway 8.6 and later.
- Busy Line Field features require Cisco Unified Communications Manager 11.0 or later.
- A device connected through Expressway cannot download APKs from an APK server inside the enterprise network. The device can download APKs from an APK server on a public network as long as the host is accessible.
- You do not have SSH access to the device from the corporate network.
- You do not have access to the device web page from the corporate network.
- Self-provisioning is not supported through Expressway.

Related Topics

http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html

Enable user Credential Persistence for Expressway

Procedure

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

Step 2 Set **User Credentials Persistent for Expressway Sign In** to On.

Convert a Device to Mobile and Remote Access through Expressway

Before You Begin

The device must have firmware 10.2(4) or later.

Procedure

Step 1 In the Settings application, tap **More...**.

Step 2 Tap **Reset network settings**.

Step 3 Uncheck **Enable automatic local telephony discovery** and tap **Reset**.

The network connection is reset. If the device is connected to a wired network, it will reconnect automatically. If the device is deployed wirelessly, you need to connect to a Wi-Fi network. When the device connects to a network, the **Enter TFTP server** screen displays.

Step 4 Tap **Expressway**.

Step 5 Fill in the **Service domain**, **Username**, and **Password** fields.

Step 6 Tap **Sign in**.

Convert an Expressway Device to VPN

Procedure

Step 1 In the Settings application, tap **More...**.

Step 2 Tap **Reset network settings**.

Step 3 Connect to a network.

Step 4 Enter TFTP server settings.

Step 5 Add a VPN profile and connect to it.

Convert an Off-Premise Device to On-Premise

Procedure

Connect a device to an enterprise network.
The enterprise network is detected, and the phone registers with Cisco Unified Communications Manager as it would normally.

Add Problem Report Tool Server to Expressway HTTP Allow List

Procedure

Step 1 On Expressway, go to **Configuration** > **Unified Communications** > **Configuration**.

Step 2 Click **HTTP server allow list**.

Step 3 Configure the hostname or IP address of the Problem Report Tool HTTP server.

Set the Allowed Authorization Request Rate

The rate of Mobile and Remote Access authorizations for a device is controlled by default. The default setting is 3 authorizations in 300 seconds. You may want to increase that rate if your Expressway server is issuing HTTP 429 “Too Many Requests” errors.

Procedure

Step 1 On Expressway, go to **Configuration** > **Unified Communications** > **Configuration** > **Advanced**.

Step 2 Set the **Authorization Rate Control**.

Enable Alternate TFTP Server

Procedure

Step 1 In the Settings application, tap **More**.

Step 2 Tap **TFTP Server Settings**.

Step 3 Check **Use Alternate TFTP Server**.

Set TFTP Server 1

Procedure

Step 1 In the Settings application, tap **More**.

Step 2 Tap **TFTP Server Settings**.

Step 3 Check **Use Alternate TFTP Server**.

Step 4 Tap **TFTP server 1**.

Step 5 Enter the TFTP server address and tap **OK**.

Set TFTP Server 2

Procedure

Step 1 In the Settings application, tap **More**.

Step 2 Tap **TFTP Server Settings**.

Step 3 Check **Use Alternate TFTP Server**.

Step 4 Tap **TFTP server 2**.

Step 5 Enter the TFTP server address and tap **OK**.

AnyConnect VPN

AnyConnect is a VPN client that provides remote users with secure VPN connections to the Cisco 5500 Series ASA running ASA Version 8.0, and later (with AnyConnect Mobile License) or Adaptive Security Device Manager (ASDM) 6.0 and later.

For more information about ASA, see http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

Add VPN Connection Profile

Procedure

Step 1 In the Settings application, tap **More**.

Step 2 Tap **VPN**.

Step 3 Tap **Add VPN profile**.

Step 4 Enter a description and the server address.

Step 5 Tap **Save**.

Connect to VPN

Procedure

Step 1 In the Settings application, tap **More**.

Step 2 Tap **VPN**.

Step 3 Tap and hold a VPN connection.

Step 4 If necessary, do either of the following in response to the appropriate prompts:

- Enter the credentials. If prompted to do so, also enter the secondary credentials to support double authentication.
- Tap **Get Certificate**, then enter the certificate enrollment credentials that your system administrator supplies. AnyConnect saves the certificate and reconnects to the VPN secure gateway to use the certificate for authentication.

Step 5 Tap **Connect**.

Optimize Video Call Experience Over VPN

Adjust video bandwidth settings to optimize the video call experience over VPN. A bandwidth of 1.5 Mbps is required for 720p video resolution. Lower bandwidth settings result in lower video resolution.

Note Throughput varies over time, due to factors like other traffic being shared on the network, or even time of day. These variations can affect the video experience.

Procedure

Step 1 Disconnect from VPN.

Step 2 Run a speed test for the device, and make a note of the upload speed in the test results.
Speed test applications, such as Internet Speed Test by Speed A.I. are available from Google Play.

Step 3 Reconnect to VPN.

Step 4 In the Call application, tap •••.

Step 5 Tap **Settings**.

Step 6 Tap **Video bandwidth**.

Step 7 Select a video bandwidth that is lower than the upload speed in the speed test results.

Configure VPN in Cisco Unified Communications Manager

The VPN Settings menu allows you to use the Secure Sockets Layer (SSL) to enable the VPN Client connection. Use the VPN connection when the device is located outside a trusted network or when network traffic between the device and Cisco Unified Communications Manager must cross untrusted networks.

Follow these steps from to configure VPN profiles. For more information, see the *Cisco Unified Communications Manager Security Guide* and the *Cisco Unified Communications Operating System Administration Guide*.

Procedure

Step 1 Set up VPN concentrators for each VPN gateway.

Step 2 Upload VPN certificates to a new Phone-VPN-Trust.

Step 3 Configure VPN gateways.

a) Choose **Advanced Features** > **VPN** > **VPN Gateway**.

b) Enter Gateway Name, Description, and URL.

Note You can assign up to ten certificates to a VPN Gateway. Assign at least one certificate to each gateway. Only certificates that are associated with the VPN role display in the available VPN certificates list.

The VPN Gateway URL is for the main concentrator in the gateway.

Step 4 Configure VPN Group. Choose **Advanced Features** > **VPN** > **VPN Group**.

Note You can add up to three VPN gateways to a VPN group. The total number of certificates in the VPN group cannot exceed ten.

Step 5 Configure VPN Profile. Choose **Advanced Features** > **VPN** > **VPN Profile**.

Note If **Enable Auto-Detect Network Connection** is enabled, the VPN client runs only if it detects that it is out of the corporate network.

If **Host ID Check** is enabled, the VPN Gateway certificate Common Name must match the URL to which the VPN client is connected.

If **Enable Password Persistence** is enabled, the user password is cached. If Store VPN Password on Device is also enabled, the user password is saved on the device until a sign-in failure occurs.

Step 6 Configure VPN Feature. Choose **Advanced Features** > **VPN** > **VPN Feature Configuration**.

Step 7 Assign a Common Phone Profile. Choose **Device** > **Device Settings** > **Common Phone Profile**.

VPN Configuration Settings

The following table describes the VPN configuration options for devices on Cisco Unified Communications Manager.

Table 1: VPN Configuration Options

Option	Description	To Change
Administrator Provisioned VPN Gateway	VPN enabled with VPN Group Configuration.	Display Only - Cannot change.

Option	Description	To Change
User Defined VPN Profiles	Shows whether option is enabled or disabled.	In the individual device configuration window or **Common Phone Profile** window (Product Specific Configuration layout area), set Allow User Defined Profiles to On or Off. **Note** Available for multilevel configurations. Administrator may change at device, common, or enterprise levels. If the feature is disabled on Cisco Unified Communications Manager, user-defined VPN profiles are removed from the list on the device and **Add New VPN Connection** is disabled.
Always Require VPN	Shows whether option is enabled or disabled.	Choose **Device** > **Device Settings** > **Common Phone Profile**. Choose the desired profile. Set Always Require VPN to On or Off. **Note** Always Require VPN setting overwrites enable and autoNetworkDetect values to True.
Store VPN Password on Device	Shows whether option is enabled or disabled.	Choose **Device** > **Device Settings** > **Common Phone Profile** or **Device** > **Phone** > **Phone Configuration**. Set Store VPN Password on Device to On or Off. **Note** Store VPN Password on Device only works if password persistence is enabled for the configured VPN profile, and if the client authentication method is “User and Password” or “Password only”.

Note Network configuration changes can potentially affect an active VPN connection.

If VPN is enabled, no proxy is configured or used for VPN.

VPN Authentication

Cisco DX Series devices support the following VPN authentication methods:

- Username and password
- Certificate only
- Password only

Note For password-only authentication, the device ID is prefilled as the username; Cisco Adaptive Security Appliance (ASA) configures the username.

The authentication that is specified on Cisco Unified Communications Manager must match authentication that is set on the ASA. If the authentication does not match that on the ASA, the user VPN is still allowed, but password persistence and autoconnect features are not applicable.

Startup Process

Upon connection to the network, Cisco DX Series devices go through a standard startup process. Depending on your specific network configuration, only some of these steps may occur on your devices.

1. Obtain power from the switch. If a device is not using external power, the switch provides inline power through the Ethernet cable that is attached to the device. The **Starting up...** screen appears for about 30 seconds.

   The device attempts to detect an Ethernet connection. If an Ethernet connection is detected but no IP address is assigned, the user is prompted to contact the administrator for assistance. If an Ethernet connection is not found, the device attempts to establish a wireless network connection.

2. (In a wireless LAN only) Scan for an access point. The device scans the RF coverage area. The device searches the network profiles and scans for access points that contain a matching Service Set Identifier (SSID) and authentication type. The device associates with the access point that matches the network profile configuration.

3. (In a wireless LAN only) Authenticate with the access point. The device begins the authentication process.

4. Load the stored device image. The device has nonvolatile flash memory in which the device stores firmware images and user-defined preferences. At startup, the device runs a bootstrap loader that loads a firmware image that is stored in flash memory. Using this image, the device initializes the software and hardware.

5. Configure the VLAN. If the device is connected to a Cisco Catalyst switch, the switch next informs the device of the voice VLAN that is defined on the switch. The device needs the VLAN membership information before it can proceed with the Dynamic Host Configuration Protocol (DHCP) request for an IP address.

6. Obtain an IP address. If the device is using DHCP to obtain an IP address, the device queries the DHCP server to obtain one. If you are not using DHCP in your network, you must assign static IP addresses to each device locally.

7 Access a TFTP server. In addition to assigning an IP address, the DHCP server directs the device to a TFTP Server. If the device has a statically defined IP address, you must configure the TFTP server locally on the device; the device then contacts the TFTP server directly.

If the TFTP server is not found, the user is prompted to sign in to Expressway.

Note You can also assign an alternate TFTP server to use instead of the server that DHCP assigns.

8 (A device connected to Expressway skips this step)

Request the CTL file. The TFTP server stores the CTL file. This file contains the certificates that are necessary to establish a secure connection between the device and Cisco Unified Communications Manager.

9 (A device connected to Expressway skips this step)

Request the ITL file. The device requests the ITL file after it requests the CTL file. The ITL file contains the certificates of the entities that the device can trust. The certificates are used to authenticate a secure connection with the servers or to authenticate a digital signature that is signed by the servers. Cisco Unified Communications Manager 8.5 and later supports the ITL file.

10 Request the configuration file. The TFTP server has configuration files, which define parameters for connecting to Cisco Unified Communications Manager and other information for the device.

11 Contact Cisco Unified Communications Manager. The configuration file defines how the device communicates with Cisco Unified Communications Manager and provides a device with the load ID. After it obtains the file from the TFTP server, the device attempts to make a connection to the highest-priority Cisco Unified Communications Manager on the list.

If the security profile of the device is configured for secure signaling (encrypted or authenticated) and the Cisco Unified Communications Manager is set to secure mode, the device makes a TLS connection. Otherwise, the device makes a nonsecure TCP connection.

If the device was manually added to the database, Cisco Unified Communications Manager identifies the device. If the device was not manually added to the database and autoregistration is enabled in Cisco Unified Communications Manager, the device attempts to autoregister in the Cisco Unified Communications Manager database.

Note Autoregistration is disabled when you configure the CTL client. In this case, you must add the device to the Cisco Unified Communications Manager database manually.

12 If the device is booting for the first time, display the **Welcome** screen and run the Setup Assistant.

Set TFTP Server Manually During Startup

Procedure

Step 1 While the screen shows `Starting up...`, tap the upper left corner of the screen three times..

Step 2 An extra period is added to the end of `Starting up...` to indicate that the key sequence was detected.

Step 3 The TFTP configuration screen appears. Enter the TFTP server address and tap **Confirm**.

Startup Verification

After the device has power connected to it, the device begins the startup diagnostic process by cycling through the following steps.

1. During the various stages of bootup as the device checks the hardware (Cisco DX650 only: the handset light and Mute button flash red and the Headset button and Speaker button flash green), the Lock/Power button is lit (white).
2. The Phone icon appears on the status bar.

If the device completes these stages successfully, it has started up properly, and the Lock/Power button stays lit.