インストール

Cisco DX シリーズ デバイスの設置

Cisco Unified Communications Manager データベースにデバイスを追加したら、デバイスのインストールを完了できます。管理者（またはユーザー）は、ユーザーの場所にデバイスを設置できます。

（注） デバイスを設置する前に、新しいデバイスであっても、デバイスを最新のファームウェア イメージにアップグレードします。アップグレードの詳細については、次の場所にあるデバイスの Readme ファイルを参照してください。

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

デバイスをネットワークに接続すると、デバイスの起動プロセスが開始され、デバイスがCisco Unified Communications Manager に登録されます。デバイスの設置を完了するには、DHCP サービスを有効にするかどうかに応じて、デバイス上でネットワーク設定値を構成します。

自動登録を使用した場合は、デバイスをユーザーに関連付ける、ディレクトリ番号を変更するなど、デバイスの特定の構成情報をアップデートする必要があります。

次の手順では、Cisco DX シリーズデバイスの設置タスクの概要とチェックリストを示します。この手順では、デバイスの設置を推奨する順序を示します。一部のタスクは、システムおよびユーザーのニーズによっては省略できます。

手順

ステップ 1 電源を次の中から選択します。

- 外部電源
- [Cisco DX650-のみ] Power over Ethernet（PoE）

（注） PoE+ 802.3at では、マウスやキーボードなどのデバイスに接続されているアクセサリが電力をネゴシエートします。アクセサリに十分な電力が供給されていない場合は、エラー メッセージが画面に表示されます。デバイスを WLAN 環境で使用する場合は、外部電源が必要です。

ステップ 2 デバイスを組み立て、ネットワーク ケーブルを接続します。WLAN 環境でデバイスを使用する場合は、ステップ 5 を参照してください。
この手順では、ネットワーク内のデバイスを見つけてインストールします。

ステップ 3 デバイスの起動プロセスをモニタします。この手順では、プライマリとセカンダリのディレクトリ番号、およびディレクトリ番号に関連付ける機能をデバイスに追加し、デバイスが正しく構成されていることを確認します。

ステップ 4 ワイヤレス ネットワークにデバイスを展開する場合は、ステップ 5 に進みます。

IP ネットワークに対してデバイスでイーサネット ネットワーク設定を構成する場合、DHCP を使用するか、IP アドレスを手動で入力してデバイスの IP アドレスを設定できます。

ステップ 5 ワイヤレスネットワークにデバイスを展開する場合は、次の手順を実行する必要があります。

- ワイヤレス ネットワークを構成します。
- Cisco Unified Communications Manager 管理でデバイスのワイヤレス LAN を有効にします。
- デバイスでワイヤレス ネットワーク プロファイルを構成します。

（注） イーサネット ケーブルがデバイスに接続されている場合、デバイスのワイヤレス LAN はアクティブになりません。

ステップ 6 デバイスを使用してコールを発信し、コールアプリケーションと機能が正常に動作することを確認します。

ステップ 7 エンド ユーザーに対して、デバイスの使用方法および構成方法を通知します。

ワイヤレス LAN の設定

ワイヤレス LAN が導入されている場所の Wi-Fi カバレッジがビデオおよび音声パケットの送信に最適であることを確認します。

ワイヤレス ネットワークの完全な設定情報については、「『*Cisco DX Series Wireless LAN Deployment Guide*』」を参照してください。

Cisco Unified Communications Manager 管理のワイヤレス LAN 設定

Cisco Unified Communications Manager で、デバイスの 「Wi-Fi」 と呼ばれるパラメータを有効にする必要があります。 Cisco Unified Communications Manager 管理の次のいずれかの場所で、このパラメータを有効にできます。

- 特定のデバイスでワイヤレス LAN を有効にするには、特定のデバイスの [製品固有の設定レイアウト（Product Specific Configuration Layout）] セクション（**[デバイス（Device）]** > **[電話（Phone）]**）で Wi-Fi パラメータの **[有効（ Enable）]** を選択し、**[共通設定のオーバーライド（ Override Common Settings）]** をオンにします。
- デバイスのグループに対してワイヤレス LAN を有効にするには、**[共通の電話プロファイルの構成（Common Phone Profile Configuration ）]** ウィンドウ（**[[デバイス（Device）]** > **[デバイス設定（Device Settings）]** > **[共通の電話プロファイル（Common Phone Profile）]**）で Wi-Fi パラメータの **[有効化（Enable）]** を選択し、**[共通設定のオーバーライド（Override Common Settings）]** をオンにしてから、デバイス（**[デバイス（Device）]** > **[電話（Phone）]** をその共通の電話プロファイルに関連付けます。
- ネットワーク内のすべての WLAN 対応デバイスでワイヤレス LAN を有効にするには、**[エンタープライズ電話 の構成（Enterprise Phone Configuration）]** ウィンドウ（**[システム（System）]** > **[エンタープライズ電話の構成]（Enterprise Phone Configuration）]**）で、Wi-Fi パラメータの **[有効化（Enable）]** を選択し、**[共通設定のオーバーライド（Override Common Settings）]** をオンにします。

（注） Cisco Unified Communications Manager 管理（**[デバイス（Device）]** > **[電話（Phone）]**）の **[電話構成（Phone Configuration）]** ウィンドウで、MAC アドレスを構成するときにイーサネット MAC アドレスを使用します。Cisco Unified Communications Manager の登録では、無線 MAC アドレスを使用しません。

ワイヤレス LAN プロファイルのプロビジョニング

手順

ステップ 1 Cisco Unified Communications Manager 管理で、**[デバイス（Device）]** > **[電話（Phone）]** > **[ワイヤレス LAN プロファイル（Wireless LAN Profile）]** を選択します。

ステップ 2 ワイヤレス LAN プロファイルを構成し、**[保存（Save）]** をクリックします。

ワイヤレス LAN プロファイル グループのプロビジョニング

手順

ステップ 1 Cisco Unified Communications Manager 管理で、**[デバイス > 電話 > ワイヤレス LAN プロファイル グループ（DevicePhoneWireless LAN Profile Group）]** を選択します。

ステップ 2 ワイヤレス LAN プロファイル グループを構成し、**[保存（Save）]** をクリックします。

ステップ 3 **[システム > デバイス プール（System Device Pool）]** を選択し、ワイヤレス LAN プロファイル グループをデバイス プールに追加し、**[保存（Save）]** をクリックします。または、**[デバイス > 電話（Device Phone）]** を選択し、ワイヤレス LAN プロファイル グループを特定のデバイスに追加して、**[保存（Save）]** をクリックします。

ネットワーク設定構成

ネットワークで DHCP を使用していない場合、ネットワークでデバイスをインストールした後、デバイスでこれらのネットワーク設定を構成する必要があります。

- IP アドレス
- IP サブネット情報
- IPv6 アドレス
- TFTP サーバの IP アドレス

必要に応じて、ドメイン名と DNS サーバ設定値も設定できます。

IPv4の設定

手順

ステップ 1 [設定（Settings）] アプリケーションで、**[イーサネット（Ethernet）] > [IPv4 構成（IPv4 configuration）]** をタップします。

ステップ 2 **[静的 IP を使用する（Use static IP）]** をオンにします。

ステップ 3 次のオプションを設定します。

- [IP アドレス（IP Address）]
- ゲートウェイ
- ネットマスク
- ドメイン名

（注） オプション 15 を使用して、複数のドメイン名をデバイスに送信できます。各ドメイン名はスペースで区切る必要があります。カンマなどの他のデリミタはサポートされていません。静的 IP アドレスを使用している場合は、ドメイン名を手動で入力することもできます。繰り返しますが、スペースは唯一の有効なデリミタです。現在、オプション 119 はサポートされていません。

- DNS 1
- DNS 2

IPv4 の更新

手順

設定アプリケーションで、**[イーサネット（Ethernet）]** > **[IPv4 の更新（Renew IPv4）]** をタップします。

IPv6 を設定する

手順

ステップ 1 [設定（Settings）] アプリケーションで、[**イーサネット** > **IPv6 構成（ EthernetIPv6 configuration**）**]** をタップします。

ステップ 2 **[静的 IP を使用する（Use static IP）]** をオンにします。

ステップ 3 次のオプションを設定します。

- IP アドレス
- デフォルト ルータ
- プレフィックス長
- ドメイン名

（注） オプション 15 を使用して、複数のドメイン名をデバイスに送信できます。各ドメイン名はスペースで区切る必要があります。カンマなどの他のデリミタはサポートされていません。静的 IP アドレスを使用している場合は、ドメイン名を手動で入力することもできます。繰り返しますが、スペースは唯一の有効なデリミタです。現在、オプション 119 はサポートされていません。

- DNS 1
- DNS 2

IPv6 の更新

手順

設定アプリケーションで、**[イーサネット（Ethernet）]** > **[IPv6 の更新（Renew IPv6）]** をタップします。

イーサネット Web プロキシの構成

手順

ステップ 1 設定アプリケーションで、**[イーサネット（Ethernet）]** > **[プロキシ設定（Proxy settings）]** をタップします。

ステップ 2 プロキシ設定タイプを選択します。

a) 手動プロキシを設定するには、プロキシのホスト名、プロキシ ポート、およびプロキシ バイパスを入力します。該当する場合は、**[プロキシは認証が必要（Proxy require authentication）]** を オンにします。

b) 自動プロキシを設定するには、PACの場所とプロキシバイパスを入力します。該当する場合は、**[プロキシは認証が必要（Proxy require authentication）]** を オンにします。

管理 VLAN の設定

手順

ステップ 1 [設定（Settings）] アプリケーションで、**[イーサネット（Ethernet）]** > **[管理 VLAN（ Admin VLAN）]** をタップします。

ステップ 2 管理 VLAN ID の値を入力し、**[OK]** をタップします。

SW ポートの速度の設定

手順

ステップ 1 [設定（Settings）] アプリケーションで、**[イーサネット** > **SW ポート速度（EthernetSW port speed）]** をタップします。

ステップ 2 ポートの速度を選択します。

デバイスがスイッチに接続されている場合は、スイッチ上のポートをデバイスと同じ速度および二重化方式に構成するか、両方を自動ネゴシエーションに設定します。このオプションの設定値を変更する場合は、[PC ポートの構成（PC Port config）] オプションを同じ設定値に変更する必要があります。

PC ポートの速度の設定

手順

ステップ 1 [設定（Settings）] アプリケーションで、**[イーサネット（Ethernet）]** > **[PC ポート速度（PC port speed）]** をタップします。

ステップ 2 ポートの速度を選択します。

デバイスがスイッチに接続されている場合は、スイッチ上のポートをデバイスと同じ速度および二重化方式に構成するか、両方を自動ネゴシエーションに設定します。このオプションの設定値を変更する場合は、[SW ポートの構成（SW Port config）] オプションを同じ設定値に変更する必要があります。

Wi-Fi ネットワークへの接続

手順

ステップ 1 設定アプリケーションで、[Wi-Fi（Wi-Fi）] をオンに切り替えます。

ステップ 2 **[Wi-Fi]** をタップします。

ステップ 3 使用可能なネットワークのリストからワイヤレス ネットワークを選択します。

ステップ 4 認証情報を入力し、**[接続（Connect）]** をタップします。

非表示の Wi-Fi ネットワークに接続

手順

ステップ 1 設定アプリケーションで、[Wi-Fi（Wi-Fi）] をオンに切り替えます。

ステップ 2 **[Wi-Fi]** をタップします。

ステップ 3 [+] をタップします。

ステップ 4 ネットワーク SSID を入力し、セキュリティ タイプとログイン情報（該当する場合）を選択します。

ステップ 5 [保存（Save）] をタップします。

Wi-Fi Web プロキシの構成

手順

ステップ 1 設定アプリケーションで、**[Wi-Fi]** をタップします。

ステップ 2 使用可能なネットワークのリストからワイヤレス ネットワークを長押しします。

ステップ 3 **[ネットワークを変更（Modify Network）]** をタップします。

ステップ 4 **[詳細オプションの表示（Show advanced options）]**をチェックします。

ステップ 5 プロキシ設定タイプを選択します。

a) 手動プロキシを設定するには、プロキシのホスト名、プロキシ ポート、およびプロキシ バイパスを入力します。該当する場合は、**[プロキシは認証が必要（Proxy require authentication）] を** オンにします。

b) 自動プロキシを設定するには、PAC の場所とプロキシバイパスを入力します。該当する場合は、**[プロキシは認証が必要（Proxy require authentication）] を** オンにします。

ステップ 6 [保存（Save）] をタップします。

Wi-Fi IP 設定の構成

手順

ステップ 1 設定アプリケーションで、**[Wi-Fi]** をタップします。

ステップ 2 使用可能なネットワークのリストからワイヤレス ネットワークを長押しします。

ステップ 3 **[ネットワークを変更（Modify Network）]** をタップします。

ステップ 4 **[詳細オプションの表示（Show advanced options）]**をチェックします。

ステップ 5 IP 設定タイプを選択し、以下を構成します。

- [IP アドレス（IP Address）]
- ゲートウェイ
- ネットワーク プレフィックス長
- DNS 1
- DNS 2

- ドメイン名

ステップ 6 [保存（Save）] をタップします。

Wi-Fi 周波数バンドの設定

手順

ステップ 1 設定アプリケーションで、**[Wi-Fi]** をタップします。

ステップ 2 **[...]** をタップします

ステップ 3 **[Wi-Fi 周波数帯（Wi-Fi Frequency Band）]** をタップし、設定を選択します。

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 www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-technical-reference-list.html 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.

Expressway 用ユーザー ログイン情報の有効化

手順

ステップ 1 個別デバイスの構成ウィンドウまたは **[共通の電話プロファイル（Common Phone Profile）]** ウィンドウの [製品固有構成レイアウト（Product Specific Configuration Layout）] 領域に移動します。

ステップ 2 **[Expressway ログイン用ユーザ クレデンシャル パーシステント（User Credentials Persistent for Expressway Sign In）]** をオンにします。

Expressway を介してデバイスをモバイル & リモート アクセスに変換

始める前に

デバイスのファームウェアは 10.2(4) 以降である必要があります。

手順

ステップ 1 設定アプリケーションで、**[詳細...（More....）]** をタップします。。

ステップ 2 [ネットワーク設定のリセット（Reset network settings）] をタップします。

ステップ 3 **[ローカル テレフォニーの自動検出を有効にする（Enable automatic local telephony discovery ）]** をオフにし、**[リセット（Reset）]** をタップします。
ネットワーク接続をリセットします。デバイスが有線ネットワークに接続されている場合は、自動的に再接続されます。デバイスがワイヤレスで導入されている場合は、Wi-Fi ネットワークに接続する必要があります。デバイスがネットワークに接続すると、**[TFTP サーバの入力（Enter TFTP server ）]** 画面が表示されます。

ステップ 4 **[Expressway]** をタップします。

ステップ 5 **[サービス ドメイン（Service domain）]**、**[ユーザー名（ Username）]**、および **[パスワード（ Password ）]** フィールドに入力します。

ステップ 6 [ログイン（Sign in）] をタップします。

Expressway デバイスを VPN に変換

手順

ステップ 1 設定アプリケーションで、**[詳細...（More....）]** をタップします。。
ステップ 2 [ネットワーク設定のリセット（Reset network settings）] をタップします。
ステップ 3 ネットワークに接続します。
ステップ 4 TFTP サーバーの設定を入力します。
ステップ 5 VPN プロファイルを追加して接続します。

オフプレミス デバイスからオンプレミスに変換

手順

デバイスをエンタープライズ ネットワークに接続します。
企業ネットワークが検出され、電話機が Cisco Unified Communications Manager に正常に登録されます。

Expressway HTTP 許可リストに問題報告ツール サーバーの追加

手順

ステップ 1 Expressway で、**[構成（Configuration）]** > **[Unified Communications]** > **[構成（Configuration）]** に移動します。
ステップ 2 **[HTTP サーバー許可リスト（HTTP server allow list）]** をクリックします。
ステップ 3 Problem Report Tool HTTP サーバーのホスト名または IP アドレスを構成します。

許可済み認証リクエスト レートの設定

デバイスのモバイルおよびリモートアクセス認証のレートは、デフォルトで制御されます。デフォルト設定は、300 秒で 3 認証です。Expressway サーバーが HTTP 429 「Too many Requests」エラーを発行している場合は、このレートを増やすことができます。

手順

ステップ 1 Expressway で、**[構成（Configuration）]** > **[Unified Communications]** > **[構成（Configuration）]** > **[詳細（Advanced）]** に移動します。
ステップ 2 **[認証レート制御（Authorization Rate Control）]** を設定します。

代替 TFTP サーバの有効化

手順

ステップ 1 設定アプリケーションで、**[詳細（More）]** をタップします。
ステップ 2 [TFTPサーバの設定（TFTP Server Settings）] をタップします。
ステップ 3 **[代替 TFTP サーバの使用（Use Alternate TFTP Server）]** をタップします。

TFTP サーバ 1 の設定

手順

ステップ 1 設定アプリケーションで、**[詳細（More）]** をタップします。
ステップ 2 [TFTPサーバの設定（TFTP Server Settings）] をタップします。
ステップ 3 **[代替 TFTP サーバーの使用（Use Alternate TFTP Server）]** をタップします。
ステップ 4 **[TFTP サーバー 1（TFTP Server1）]** をタップします。
ステップ 5 TFTP サーバ アドレスを入力し、[OK] をタップします。

TFTP サーバー 2 の設定

手順

ステップ 1 設定アプリケーションで、**[詳細（More）]** をタップします。
ステップ 2 [TFTPサーバの設定（TFTP Server Settings）] をタップします。
ステップ 3 **[代替 TFTP サーバーの使用（Use Alternate TFTP Server）]** をタップします。
ステップ 4 **[TFTP サーバー 2（TFTP Server 2）]** をタップします。
ステップ 5 TFTP サーバ アドレスを入力し、[OK] をタップします。

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 https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

VPN 接続プロファイルの追加

手順

ステップ 1 設定アプリケーションで、**[詳細（More）]** をタップします。
ステップ 2 [VPN（VPN）] をタップします。
ステップ 3 [VPN プロファイルの追加（ **Add VPN profile**）] をタップします。
ステップ 4 サーバ アドレスの説明を入力します。
ステップ 5 [保存（Save）] をタップします。

VPN への接続

手順

ステップ 1 設定アプリケーションで、**[詳細（More）]** をタップします。
ステップ 2 [VPN（VPN）] をタップします。
ステップ 3 VPN 接続をタップしたままにします。
ステップ 4 必要に応じて、適切なプロンプトへの応答として次のいずれかを行います。

- クレデンシャルを入力します。入力を求められたら、二重認証をサポートするセカンダリ ログイン情報も入力します。
- [証明書を取得（Get Certificate）] をタップし、次にシステム管理者により提供される証明書登録の認証情報を入力します。AnyConnect は、証明書を保存し、VPN セキュア ゲートウェイに再接続して、認証にその証明書を使用します。

ステップ 5 [接続（Connect）] をタップします。

VPN 経由のビデオ コール体験の最適化

ビデオ帯域幅の設定を調整して、VPN を介したビデオ コール エクスペリエンスを最適化します。720p のビデオ解像度には、1.5 Mbps の帯域幅が必要です。帯域幅の設定を低くすると、ビデオ解像度が低くなります。

（注） スループットは、ネットワーク上で共有されている他のトラフィックや時刻などの要因により、時間の経過とともに変化します。これらのバリエーションは、ビデオエクスペリエンスに影響を与える可能性があります。

手順

ステップ 1 VPN から接続解除します。

ステップ 2 デバイスの速度テストを実行し、テスト結果のアップロード速度をメモします。

Speed A.I. によるインターネット速度テストなどの速度テスト アプリケーションは、Google Play から入手できます。

ステップ 3 VPN に再接続します。

ステップ 4 通話アプリケーションで、  をタップします。

ステップ 5 [設定（Settings）] をタップします。

ステップ 6 [動画帯域幅（Video bandwidth）] をタップします。

ステップ 7 速度テストの結果のアップロード速度よりも低いビデオ帯域幅を選択します。

Cisco Unified Communications Manager で VPN の構成

[VPN 設定（VPN Settings）] メニューでは、Secure Sockets Layer（SSL）を使用して VPN クライアント接続を有効にすることができます。デバイスが信頼できるネットワークの外部にある場合、またはデバイスと Cisco Unified Communications Manager 間のネットワーク トラフィックが信頼できないネットワークを通過する必要がある場合は、VPN 接続を使用します。

これらのステップに従い、VPNプロファイルを構成します。詳細については、『『*Cisco Unified Communications Manager Security Guide*』』および『*Cisco Unified Communications* オペレーティング システム管理ガイド』を参照してください。

手順

ステップ 1 VPN ゲートウェイごとに VPN コンセントレータをセットアップします。

ステップ 2 VPN 証明書を新しい Phone-VPN-Trust にアップロードします。

ステップ 3 VPN ゲートウェイを構成します。

a) **[拡張機能（Advanced Features）]** > **[VPN]** > **[VPN ゲートウェイ（VPN Gateway）]** を選択します。

b) ゲートウェイ名、説明、および URL を入力します。

（注） VPN ゲートウェイには最大 10 個の証明書を割り当てることができます。各ゲートウェイに少なくとも 1 つの証明書を割り当てます。利用可能な VPN 証明書リストに、VPN ロールに関連付けられた証明書のみが表示されます。

VPN ゲートウェイ URL は、ゲートウェイのメイン コンセントレータ用です。

ステップ 4 VPN グループを構成します。**[拡張機能（Advanced Features）]** > **[VPN]** > **[VPN グループ（VPN Group）]** を選択します。

（注） 1 つの VPN グループに 3 つの VPN ゲートウェイを追加できます。VPN グループ内の証明書の合計数は 10 以下にする必要があります。

ステップ 5 VPN プロファイルを構成します。**[拡張機能（Advanced Features）]** > **[VPN]** > **[VPN プロファイル（VPN Profile）]** を選択します。

（注） **[ネットワーク接続の自動検出を有効にする（ Enable Auto-Detect Network Connection ）]** が有効になっている場合、VPN クライアントは、企業ネットワークの外にあることを検出した場合にのみ実行されます。

[ホスト ID チェック（Host ID Check）] が有効になっている場合、VPN ゲートウェイ証明書の共通名は、VPN クライアントが接続されている URL と一致する必要があります。

[パスワードの永続化を有効にする（Enable Password Persistence）] が有効になっている場合、ユーザー パスワードはキャッシュされます。[VPNパスワードをデバイスに保存（Store VPN Password on Device）] も有効になっている場合、サインインが失敗するまで、ユーザーパスワードがデバイスに保存されます。

ステップ 6 VPN 機能を構成します。**[拡張機能（Advanced Features）]** > **[VPN]** > **[VPN 機能構成（VPN Feature Configuration）]** を選択します。

ステップ 7 [共通の電話プロファイル（Common Phone Profile）] を割り当てます。**[デバイス（Device）]** > **[デバイス設定（Device Settings）]** > **[共通の電話プロファイル（Common Phone Profile）]** の順に選択します。

VPN 構成設定

次の表に、Cisco Unified Communications Manager でデバイスの VPN 構成オプションを説明します。

表 *1 : VPN* 構成オプション

オプション	説明	変更の手順
管理者がプロビジョニングした VPN ゲートウェイ	VPNグループ構成でVPNが有効になっています。	[表示のみ（Display Only）]：変

オプション	説明	変更の手順
ユーザー定義 VPN プロファイル	オプションが有効か無効かを示します。	個々のデバイス構成ウィンドウま **電話プロファイル（Common Pho** ウィンドウ（[製品固有の構成レ （Product Specific Configuration lay で、[ユーザー定義プロファイルの User Defined Profiles）] を [オン（ [オフ（Off）] に設定します。 （注） マルチレベル構成で使用で 理者は、デバイス、共通、 タープライズ レベルで変更 Cisco Unified Communicatio でこの機能が無効になって ユーザー定義の VPN プロ デバイスのリストから削除 **い VPN 接続の追加（ Add** **Connection ）]** は無効にな
常に VPN が必要	オプションが有効か無効かを示します。	**[デバイス（Device）]>[デバイス設** **Settings）] > [共通の電話プロファ** **（Common Phone Profile）]** の順に す。 目的のプロファイルを選択します [常にVPNが必要（Always Require [オン（On）] または [オフ（Off） す。 （注） [常に VPN が必要（Always VPN）] 設定により、enabl autoNetworkDetect 値が True れます。

オプション	説明	変更の手順
[デバイス上に VPN パスワードを保存（Store VPN Password on Device）]	オプションが有効か無効かを示します。	**[デバイス（Device）]>[デバイ Settings）] > [共通の電話プロ（Common Phone Profile）]** ま **（Device）] > [電話（Phone）] （Phone Configuration）[** また [デバイス上に VPN パスワード VPN Password on Device）] を [または [オフ（Off）] に設定しま （注） [VPN パスワードをデバ （Store VPN Password on 構成された VPN プロフ ワードの永続化が有効に クライアント認証方式が とパスワード（User and または 「[パスワードの only）]」 の場合にのみ

（注） ネットワーク構成の変更は、アクティブな VPN 接続に影響を与える可能性があります。

VPN が有効になっている場合、プロキシは構成されず、VPN に使用されません。

VPN 認証

Cisco DX シリーズ デバイスは、次の VPN 認証方法をサポートします。

- ユーザ名とパスワード
- 証明書のみ
- パスワードのみ

（注） パスワードのみの認証の場合、デバイス ID がユーザー名として事前に入力されます。 Cisco 適応型セキュリティ アプライアンス（ASA）がユーザー名を設定します。

Cisco Unified Communications Manager で指定されている認証は、ASA で設定されている認証と一致する必要があります。認証が ASA の認証と一致しない場合、ユーザー VPN は引き続き許可されますが、パスワードの永続性と自動接続機能は適用されません。

起動プロセス

ネットワークに接続すると、Cisco DX シリーズデバイスは標準の起動プロセスを実行します。実際のネットワークの設定によっては、次の手順のうち、デバイスで実行されるのは一部だけになる場合があります。

1. スイッチからの電力の取得。デバイスが外部電源を使用していない場合、デバイスに接続されているイーサネット ケーブル経由でスイッチからのインライン パワーが供給されます。**[起動中...（ Starting up...）]** 画面が約 30 秒間表示されます。

   デバイスはイーサネット接続の検出を試みます。イーサネット接続が検出されたが、IP アドレスが割り当てられていない場合、ユーザーは管理者に問い合わせるように求められます。イーサネット接続が見つからない場合、デバイスはワイヤレス ネットワーク接続の確立を試みます。

2. （ワイヤレス LAN のみ）アクセス ポイントのスキャン。デバイスは、RF カバレッジ エリアをスキャンします。デバイスはネットワーク プロファイルを検索し、一致する Service Set Identifier (SSID) と認証タイプを含むアクセス ポイントをスキャンします。デバイスは、ネットワーク プロファイル構成に一致するアクセス ポイントに関連付けられます。

3. （ワイヤレス LAN のみ）アクセス ポイントの認証。デバイスは認証プロセスを開始します。

4. 保存されているデバイス イメージをロードします。デバイスには不揮発性フラッシュ メモリがあり、ファームウェア イメージやユーザー定義の設定値が保存されます。起動時に、デバイスはブートストラップ ローダーを実行して、フラッシュ メモリに保存されているファームウェア イメージをロードします。このイメージを使用して、デバイスはソフトウェアとハードウェアを初期化します。

5. VLAN の設定。デバイスe を Cisco Catalyst スイッチに接続している場合、スイッチは、スイッチ上に定義されているボイス VLAN をデバイスに通知します。デバイスは、Dynamic Host Configuration Protocol（DHCP）要求を使用して IP アドレスの取得を開始するには、VLAN メンバーシップ情報をあらかじめ把握している必要があります。

6. IP アドレスの取得. デバイスで DHCP を使用して IP アドレスを取得する場合、デバイスは DHCP サーバーにクエリを発行してアドレスを取得します。ネットワーク内で DHCP を使用しない場合は、各デバイスにスタティック IP アドレスをローカルに割り当てる必要があります。

7. TFTP サーバへのアクセス. DHCP サーバは、IP アドレスを割り当てる以外に、デバイスを TFTP サーバに転送します。デバイスの IP アドレスを静的に定義した場合は、デバイスがある場所で TFTP サーバーを構成する必要があります。構成すると、デバイスは TFTP サーバに直接アクセスします。

   TFTP サーバが見つからない場合、ユーザーは Expressway にサインインするように求められます。

（注） DHCP で割り当てられるサーバの代わりに、代替 TFTP サーバーを割り当てて使用することもできます。

8. （Expressway に接続されているデバイスはこの手順をスキップします）

CTL ファイルの要求。TFTP サーバに、CTL ファイルが保管されています。このファイルには、デバイスと Cisco Unified Communications Manager との間にセキュアな接続を確立するために必要な証明書が含まれています。

9. （Expressway に接続されているデバイスはこの手順をスキップします）

ITL ファイルの要求。デバイスは、まず CTL ファイルを要求し、次に ITL ファイルを要求します。ITL ファイルはデバイスが信頼できるエンティティの証明書を含んでいます。証明書がサーバーとのセキュア接続の認証、またはサーバーによるデジタル署名の認証に使用されます。Cisco Unified Communications Manager 8.5 以降では、ITL ファイルがサポートされています。

10. 設定ファイルの要求。TFTP サーバーは、構成ファイルを保持しています。このファイルは、Cisco Unified Communications Manager に接続するためのパラメータに加え、デバイスに関するその他の情報を定義しています。

11. Cisco Unified Communications Manager にお問い合わせください。構成ファイルは、デバイスと Cisco Unified Communications Manager との間の通信方法、およびロード ID をデバイスに提供する方法を定義します。TFTP サーバーからファイルを取得した後、リストで優先順位が最も高い Cisco Unified Communications Manager に接続を試みます。

デバイスのセキュリティ プロファイルがセキュアな信号（暗号化または認証）に構成され、Cisco Unified Communications Manager がセキュア モードに設定されている場合、デバイスは TLS 接続を行います。それ以外の場合は、デバイスは非セキュア TCP 接続を実行します。

デバイスがデータベースに手動で追加された場合、 Cisco Unified Communications Manager はデバイスを識別します。デバイスがデータベースに手動で追加されておらず、 Cisco Unified Communications Managerで自動登録が有効になっている場合、デバイスは Cisco Unified Communications Manager データベースへの自動登録を試行します。

（注） CTL クライアントを設定している場合、自動登録は無効になっています。この場合、デバイスを Cisco Unified Communications Manager データベースに手動で追加する必要があります。

12. デバイスを初めて起動する場合は、**[ようこそ（Welcome）]** 画面を表示し、セットアップ アシスタントを実行します。

起動中の TFTP サーバーを手動で設定

手順

ステップ 1 画面に [起動中...（Starting up...）] と表示されている間に、画面の左上隅を 3 回タップします。

ステップ 2 [起動中...（ Starting up... ）] の末尾に追加のピリオドが追加され、キー シーケンスが検出されたことを示します。

ステップ 3 TFTP 構成画面が表示されます。TFTP サーバー アドレスを入力し、**[確認（Confirm）]** をタップします。

起動確認22-02-2018 09:42

デバイスが電源に接続されると起動診断プロセスを開始し、次の一連の手順を実行します。

1. 起動のさまざまな段階で、デバイスがハードウェアをチェックしている間（Cisco DX650 のみ：ハンドセットのライトとミュート ボタンが赤く点滅し、ヘッドセット ボタンとスピーカー ボタンが緑に点滅します）、[ロック/電源（Lock/Power）] ボタンが点灯します（白）。
2. [電話（Phone）] アイコンがステータス バーに表示されます。

デバイスがこれらのステージを適切に完了すると、正常に起動し、[ロック/電源（Lock/Power）] ボタンが点灯したままになります。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。