Web ユーザ インターフェイスを使用したスイッチの設定

（注） マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。

- デイ 0 WebUI 設定の概要 （1 ページ）
- Cisco DNA Center クラウド導入準備デイ 0 ウィザード （2 ページ）
- クラシックデイ 0 ウィザード （5 ページ）

デイ 0 WebUI 設定の概要

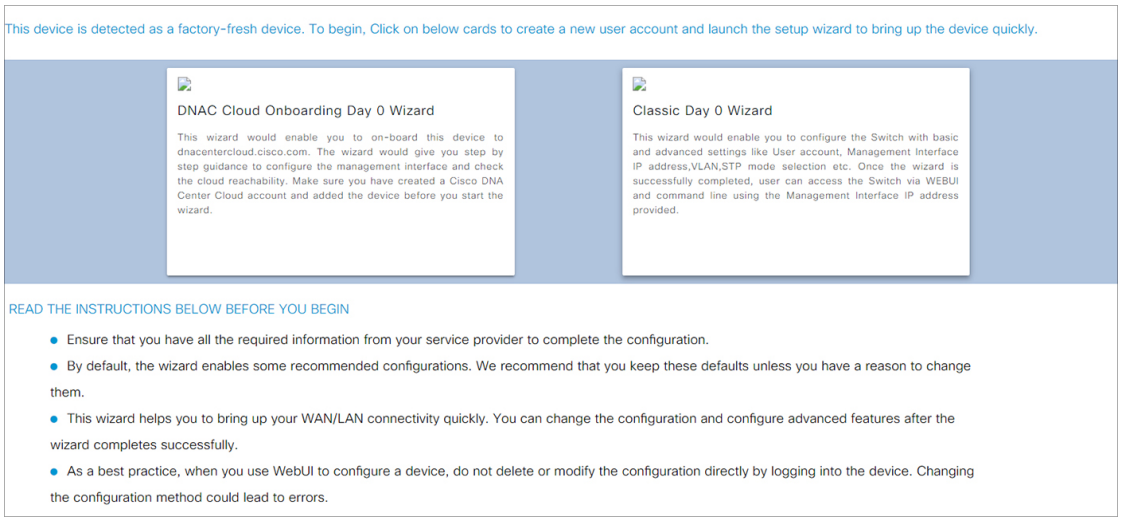
ハードウェアの取り付けが完了したら、トラフィックがネットワークを通過するのに必要な構成を使用してスイッチを設定する必要があります。新しいデバイスを使用する最初の日には、さまざまなタスクを実行することにより、デバイスがオンライン状態かつ到達可能で、簡単に設定されることを確認できます。

Web ユーザ インターフェイス（WebUI）は、組み込み GUI ベースのデバイス管理ツールです。デバイスをプロビジョニングしたり、デバイスの導入および管理性を簡素化したり、ユーザエクスペリエンスを向上したりする機能を提供します。WebUI を使用すれば、CLI の専門知識がなくても、設定を構築し、デバイスのモニタリングとトラブルシューティングを行うことができます。

WebUI を使用してスイッチを設定するには、2 つの方法があります。

- Cisco DNA Center クラウド導入準備デイ 0 ウィザード
- クラシックデイ 0 ウィザード

図 *1 : WebUI* デイ *0* ウィザード



Cisco DNA Center クラウド導入準備デイ 0 ウィザード

このウィザードを使用して、管理インターフェイスを設定し、クラウド経由で到達可能かどうかを確認します。

（注） このウィザードに進む前に、Cisco DNA Center クラウドアカウントにデバイスを追加する必要があります。

アカウント設定の構成

デバイスで実行する最初のタスクは、ユーザ名とパスワードの設定です。通常、ネットワーク管理者はデバイスへのアクセスを制御し、権限がないユーザがネットワーク設定を参照したり、設定を操作したりすることを防止します。

ステップ 1 デフォルトのユーザ名 **webui** とパスワード **cisco** を使用してログオンします。

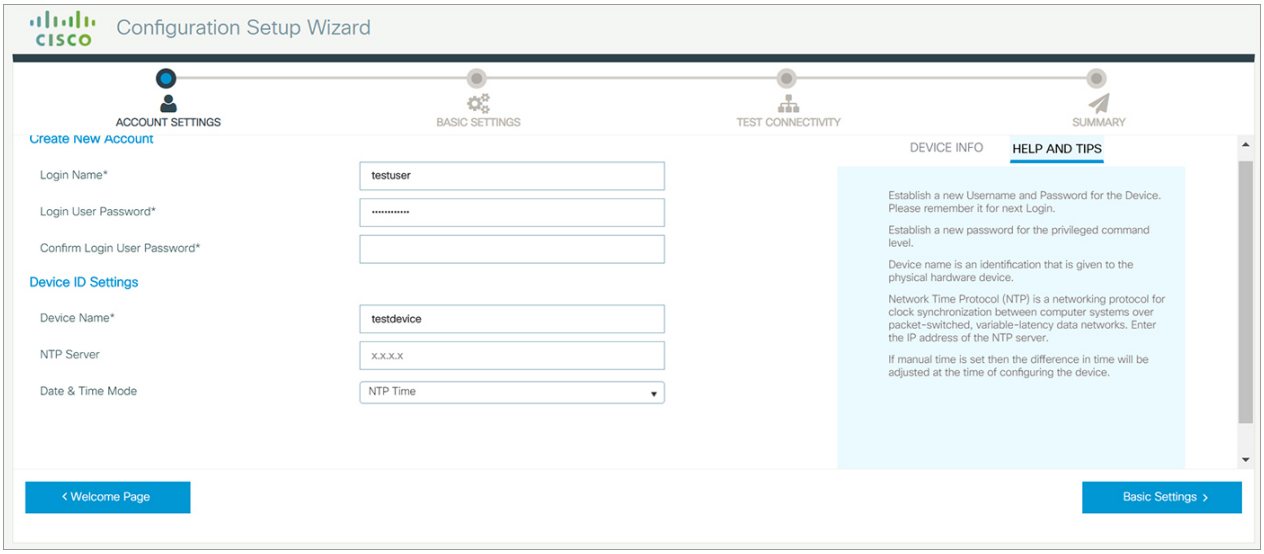
ステップ 2 最大 25 文字の英数字のパスワードを設定します。

設定したユーザ名とパスワードの組み合わせにより、特権 15 のアクセス権が与えられます。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。

ステップ 3 [Device ID Settings] セクションで、[Device Name] フィールドにネットワーク内のデバイスを識別する一意の名前を入力します。

ステップ 4 [Time & Device Mode] フィールドに、デバイスの日付と時刻を手動で入力します。デバイスを Network Time Protocol（NTP）クロックソースなどの外部タイミングメカニズムと同期するには、[NTP Server] フィールドに IP アドレスを入力します。

図 *2 : Account Settings*



基本デバイスの設定

[Basic Settings] ページで、次の情報を設定します。

ステップ 1 [Device Management Settings] セクションで、静的アドレスまたは DHCP アドレスを使用して管理インターフェイスに IP アドレスを割り当てます。

ステップ 2 [Static] を選択した場合は、次の手順を実行します。

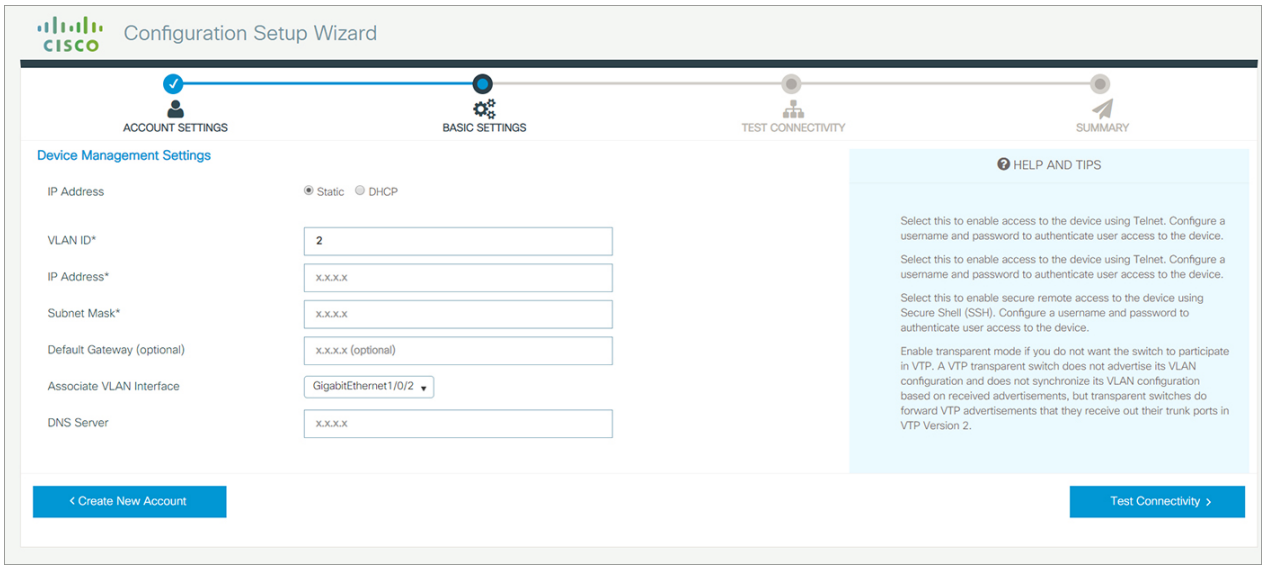
a) [Associate VLAN Interface] ドロップダウンリストで、インターフェイスに関連付ける VLAN ID を入力します。

b) 割り当てる IP アドレスが、入力したサブネット マスクの一部であることを確認してください。

c) デフォルト ゲートウェイの IP アドレスを入力します（オプション）。

d) DNS サーバのアドレスを入力します。

図 *3 :* 基本設定 - 静的構成



ステップ 3 [DHCP] を選択した場合は、次の手順を実行します。

a) [VLAN ID] フィールドに値を入力します。

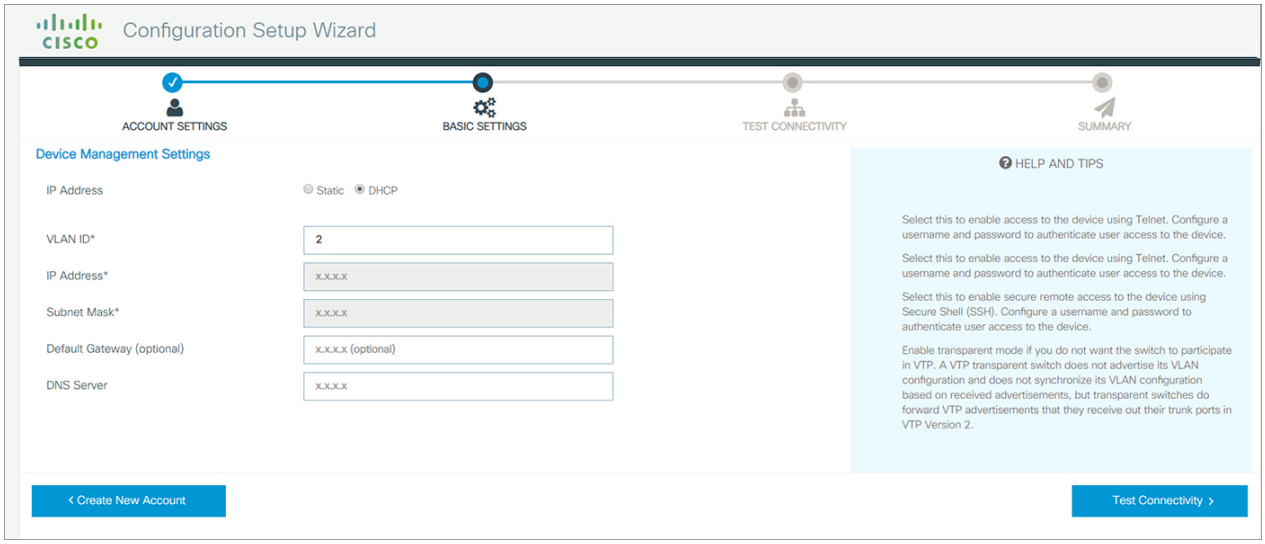
VLAN ID は 1 以外の値にする必要があります。

b) 割り当てる IP アドレスが、入力したサブネット マスクの一部であることを確認してください。

c) デフォルト ゲートウェイの IP アドレスを入力します（オプション）。

d) DNS サーバのアドレスを入力します。

図 *4 :* 基本設定 - *DHCP* 構成



接続のテストの設定

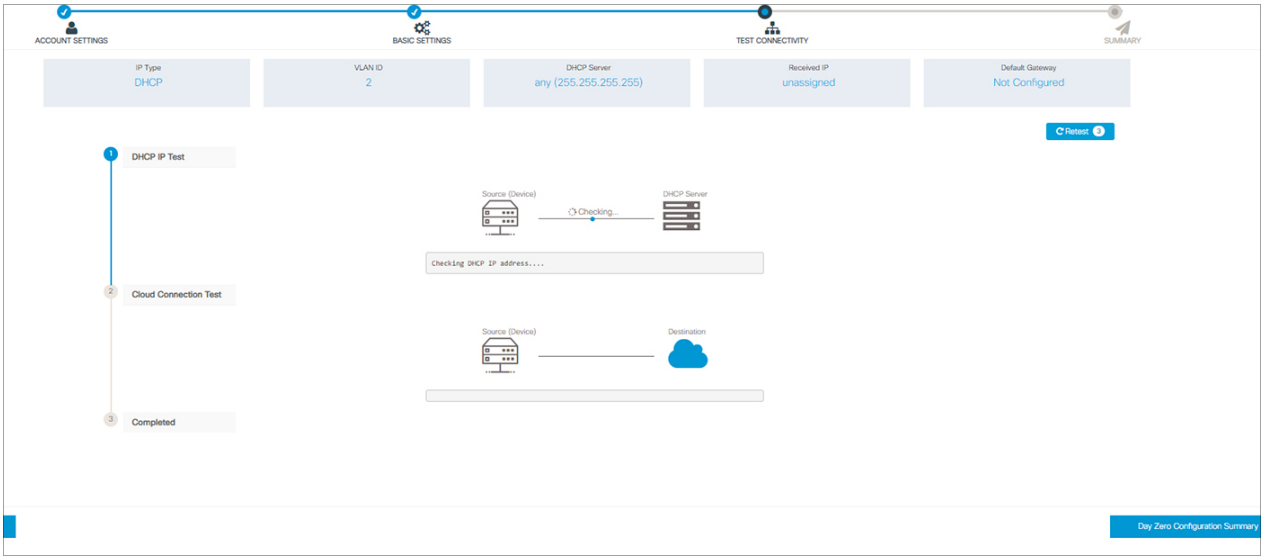
ステップ 1 デバイス間でCisco DNACクラウドへの接続が確立されていることを確認するには、[Test Connectivity/Retest] ボタンを使用します。

ステップ 2 接続が確立されていない場合は、[Retest] ボタンをクリックします。

それでも接続が失敗する場合は、前の [Basic Settings] ページに移動し、設定を変更して、接続のテストを再度確認してください。

ステップ 3 接続が確立されたら、[Day Zero Configuration Summary] に移動して設定を保存します。

図 *5 : Test Connectivity*



ステップ 4 設定が正常に適用され、デバイスが Cisco DNAC クラウドにリダイレクトされていることを確認します。

次のタスク

リダイレクションが成功しない場合は、デバイスが Cisco PnP 接続（devicehelper）のリダイレクション コントローラ プロファイルに関連付けられていることを確認します。

クラシックデイ 0 ウィザード

このウィザードを使用して、基本設定と詳細設定でデバイスを設定します。完了すると、管理インターフェイスの IP アドレスを使用して WebUI からデバイスにアクセスできます。

スイッチへの接続

始める前に

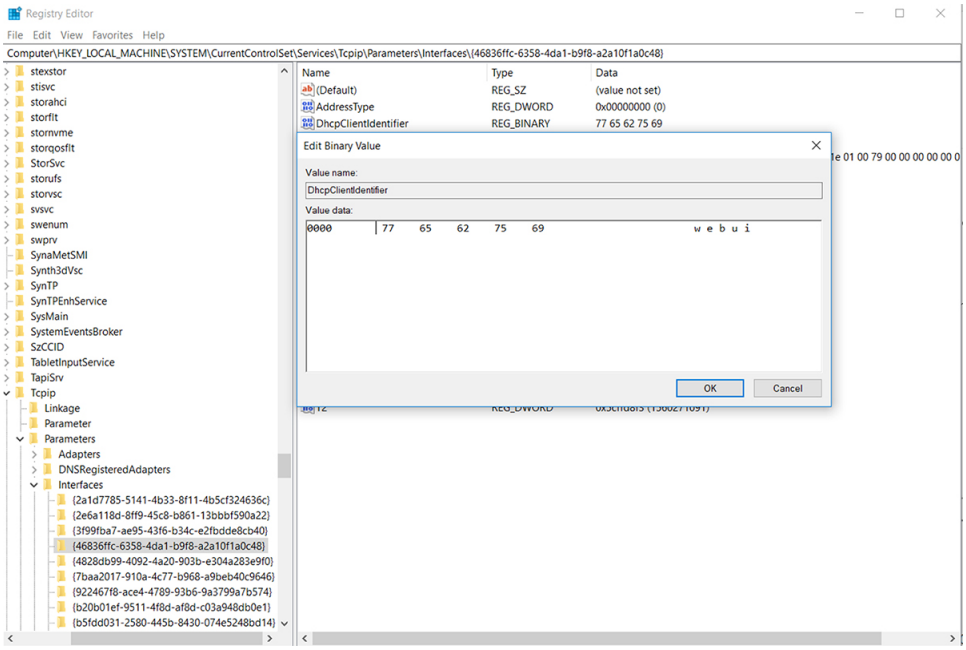
クライアントで DHCP クライアント識別子をセットアップして、スイッチから IP アドレスを取得し、Day 0 ログイン情報で認証できるようにします。

Windows クライアントでの DHCP クライアント識別子のセットアップ

1. タスクバーの Windows 検索ボックスに **regedit** と入力し、*Enter* キーを押します。
2. [User Account Contro] のメッセージが表示されたら、[Yes] をクリックしてレジストリエディタを開きます。
3. 次の場所に移動します。

   Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces（**イーサネットインターフェイス**のグローバル固有識別子（GUID）を見つけてください）
4. **webui** のデータ **77 65 62 75 69** を使用して新しい REG_BINARY の **DhcpClientIdentifier** を追加します。値は手動で入力する必要があります。

   図 *6 : Windows* での *DHCP* クライアント識別子のセットアップ

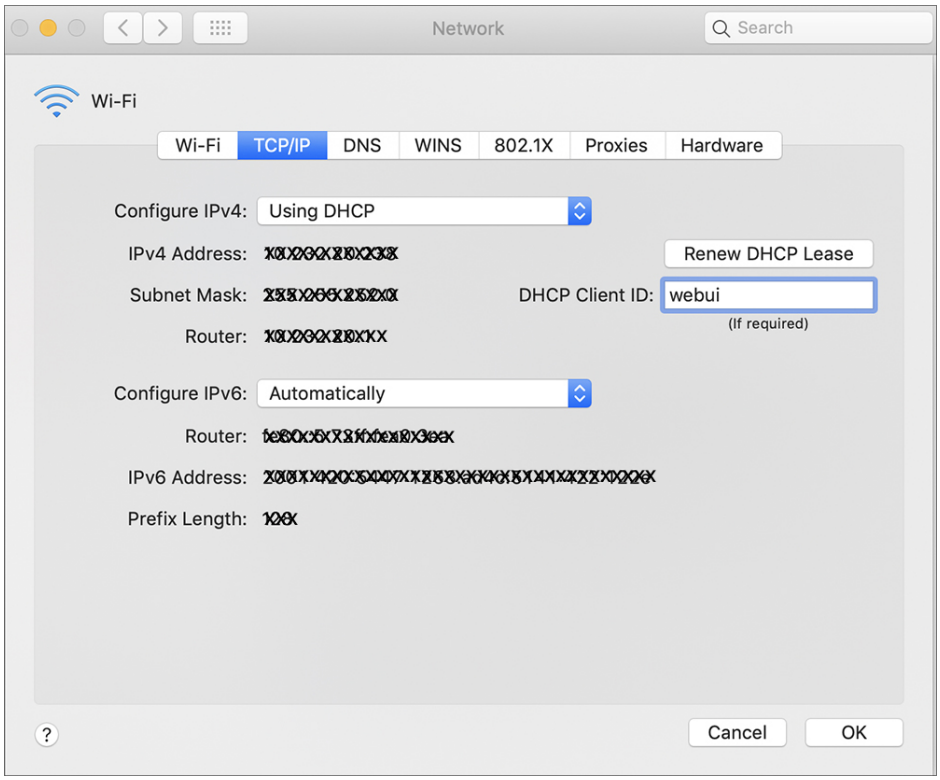


5. PC を再起動して設定を有効にします。

Mac クライアントでの DHCP クライアント識別子のセットアップ

1. [System Preferences] > [Network] > [Advanced] > [TCP] > DHCP Client ID] に移動し、**webui** と入力します。

図 *7 : Mac* での *DHCP* クライアント識別子のセットアップ



2. **[OK]** をクリックして変更を保存します。

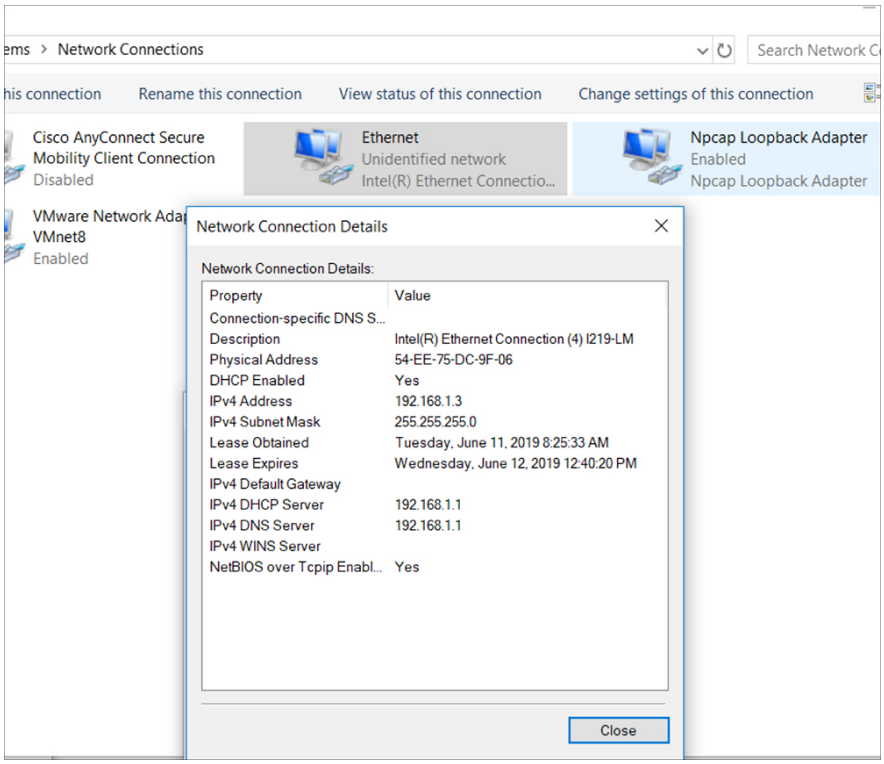
ブートアップスクリプトにより構成ウィザードが実行され、次の基本設定の入力を求められます（**Would you like to enter the initial configuration dialog? [yes/no]:**）。Web UI を使用して Day 0 設定を行うには、応答を入力しないでください。代わりに次のタスクを実行します。

ステップ 1 スイッチに何らかのデバイスが接続されていないことを確認します

ステップ 2 イーサネットケーブルの一方の端をアクティブなスーパーバイザのダウンリンク（非管理）ポートの 1 つに接続し、もう一方の端をホスト（PC/Mac）に接続します。

ステップ 3 PC/Mac を DHCP クライアントとして設定し、スイッチの IP アドレスを自動的に取得します。192.168.1.x/24 の範囲内の IP アドレスを取得する必要があります。

図 *8 : IP* アドレスの取得



最大で 3 分かかります。デバイスの端子を使用する前に、Web UI から Day 0 セットアップを完了させる必要があります。

ステップ 4 PC 上で Web ブラウザを起動し、デバイスの IP アドレス（**`https://192.168.1.1`**）をアドレスバーに入力します。

ステップ 5 Day 0 の [username] に **`webui`** と入力し、[password] に **`cisco`** を入力します。

次のタスク

ユーザ アカウントを作成します。

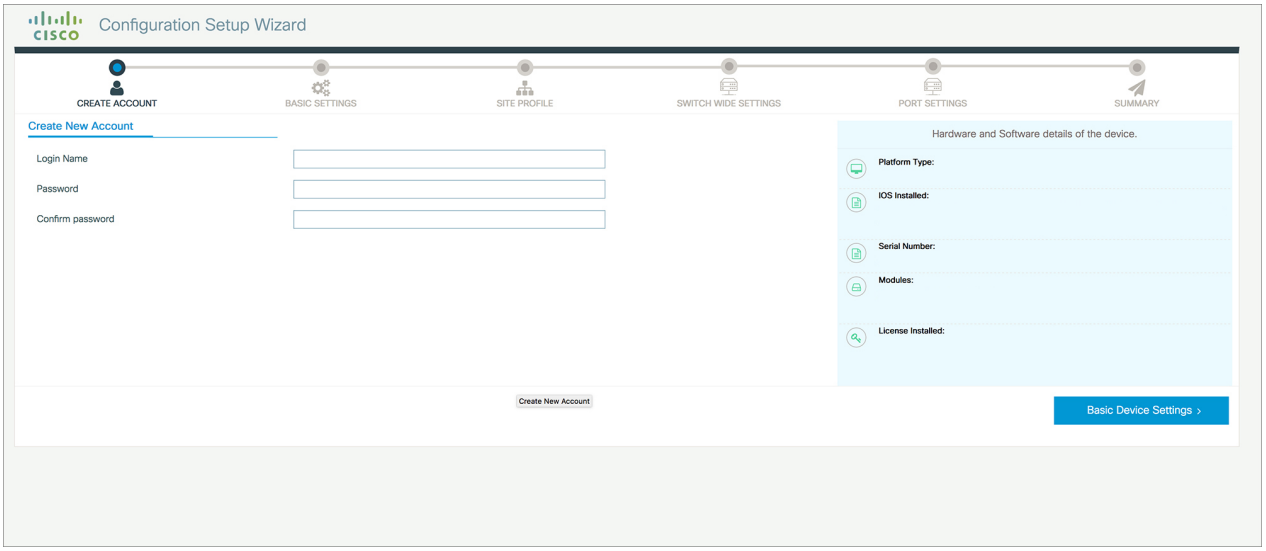
ユーザ アカウントの作成

デバイスで実行する最初のタスクは、ユーザ名とパスワードの設定です。通常、ネットワーク管理者はデバイスへのアクセスを制御し、権限がないユーザがネットワーク設定を参照したり、設定を操作したりすることを防止します。

ステップ 1 デバイスに付属のデフォルト ユーザ名とパスワードを使用してログオンします。

ステップ 2 最大25文字の英数字のパスワードを設定します。設定したユーザ名とパスワードの組み合わせにより、特権15のアクセス権が与えられます。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。

図 *9*:アカウントの作成



セットアップ オプションの選択

サイト プロファイルに基づいてデバイスを設定するには [Wired Network] を選択して、スイッチ全体の設定を続行します。それ以外の場合は、次の手順に進み、デバイスの基本設定のみを行います。

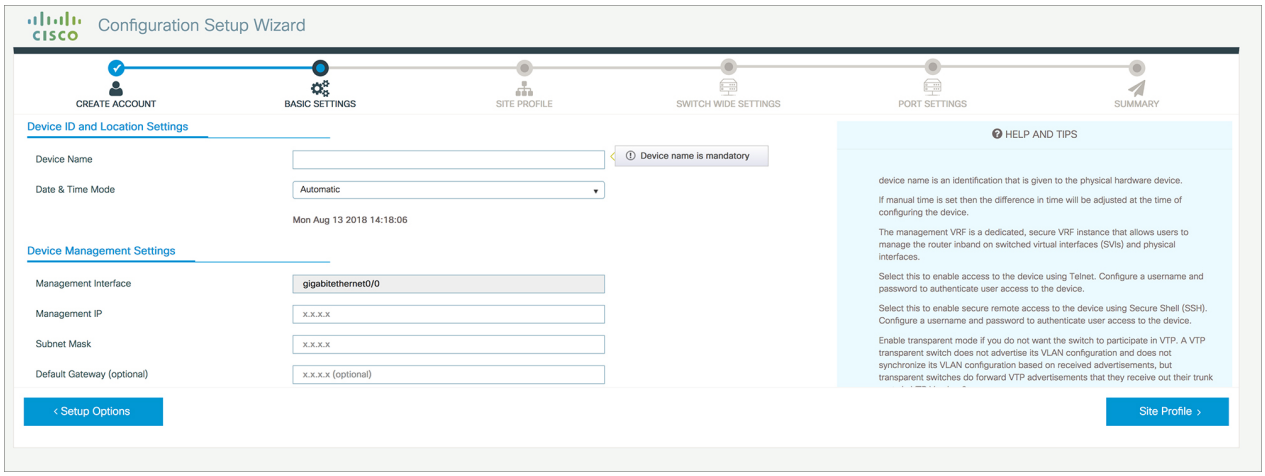
基本デバイスの設定

[Basic Device Settings] ページで、次の情報を設定します。

ステップ 1 [Device ID and Location Settings] セクションで、ネットワーク内のデバイスを識別する一意の名前を入力します。

ステップ 2 デバイスの日付と時刻の設定を選択します。デバイスをNTPクロック ソースなどの有効な外部タイミング メカニズムと同期させるには、[Automatic] を選択するか、[Manual] を選択して自分で設定します。

図 *10 : [Basic Device Settings] > [Device ID and Location Settings]*



ステップ 3 [Device Management Settings] セクションで、管理インターフェイスに IP アドレスを割り当てます。割り当てる IP アドレスが、入力したサブネット マスクの一部であることを確認してください。

ステップ 4 デフォルト ゲートウェイの IP アドレスを入力します（オプション）。

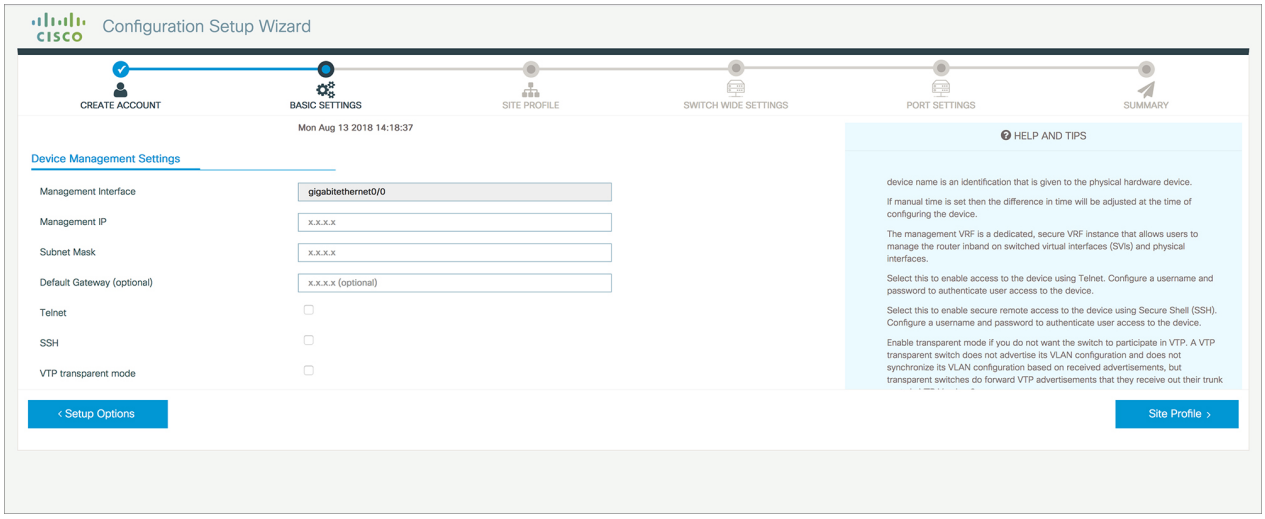
ステップ 5 Telnet によるデバイスへのアクセスを有効にするには、[Telnet] のチェック ボックスをオンにします。

ステップ 6 セキュア シェル（SSH）によるデバイスへのセキュアなリモート アクセスを有効にするには、[SSH] のチェック ボックスをオンにします。

ステップ 7 [VTP transparent mode] のチェック ボックスをオンにし、デバイスによる VTP への参加を無効化します。

前の手順で [Wired Network] を選択していない場合、次の画面に進み、[Day 0 Config Summary] 画面の設定を確認し、[Finish] をクリックします。サイトプロファイルに基づいてデバイスを自動的に設定するには、[Setup Options] をクリックして [Wired Network] を選択します。

図 *11 : [Basic Device Settings] > [Device Management Settings]*



サイト プロファイルに基づいたデバイスの設定

より簡単に設定作業を行い時間を節約するには、ネットワークでデバイスが設置および管理される場所に基づいて、サイトプロファイルを選択します。選択したサイトプロファイルに基づき、シスコのベストプラクティスに従ってデバイスが自動的に設定されます。該当する詳細設定画面から、このデフォルト設定を簡単に変更できます。

クイック セットアップの一環としてサイト プロファイルを選択すると、企業のビジネス ニーズに基づいてデバイスを設定できます。たとえば、デバイスをアクセス スイッチとして使用して、ネットワーク上のクライアント ノードとエンドポイントを接続したり、ディストリビューション スイッチとして使用して、サブネットと VLAN の間でパケットをルーティングしたりすることができます。

表 *1:* 各サイトプロファイルとともに読み込まれるデフォルト設定（アクセススイッチ）

設定	シングル アクセス スイッチ（シングルアップリンク）	シングル アクセス スイッチ（シングルポート チャネル アップリンク）	シングル アクセス スイッチ（冗長ポート チャネル アップリンク）
ホストネーム	クイックセットアップの一部として指定したホスト名またはデバイス名	クイックセットアップの一部として指定したホスト名またはデバイス名	クイックセットアップの一部として指定したホスト名またはデバイス名
スパニング ツリー モード	RPVST+	RPVST+	RPVST+
VTP	Mode Transparent	Mode Transparent	Mode Transparent
UDLD	イネーブル	イネーブル	イネーブル
エラーディセーブル回復	リカバリ モードを自動に設定	リカバリ モードを自動に設定	リカバリ モードを自動に設定
ポート チャネル ロード バランス	送信元/宛先 IP	送信元/宛先 IP	送信元/宛先 IP
SSH	Version 2	Version 2	Version 2
SCP	イネーブル	イネーブル	イネーブル
スイッチへの VTY アクセス	イネーブル	イネーブル	イネーブル
サービスタイムスタンプ	イネーブル	イネーブル	イネーブル

設定	シングル アクセス スイッチ（シングルアップリンク）	シングル アクセス スイッチ（シングルポート チャネル アップリンク）	シングル アクセス スイッチ（冗長ポート チャネル アップリンク）
VLAN	次のVLANが作成されます。 • Default VLAN • データ VLAN • 音声 VLAN • Management VLAN	次のVLANが作成されます。 • Default VLAN • データ VLAN • 音声 VLAN • Management VLAN	次のVLANが作成されます。 • Default VLAN • データ VLAN • 音声 VLAN • Management VLAN
管理インターフェイス	クイックセットアップに基づいて管理ポートに設定されたレイヤ 3 設定	クイックセットアップに基づいて管理ポートに設定されたレイヤ 3 設定	クイックセットアップに基づいて管理ポートに設定されたレイヤ 3 設定
IPv6 ホスト ポリシー	作成済みの IPv6 ホスト ポリシー	作成済みの IPv6 ホスト ポリシー	作成済みの IPv6 ホスト ポリシー
ダウンリンク ポートの QoS ポリシー	定義済みのアクセス用自動 QoS ポリシー	定義済みのアクセス用自動 QoS ポリシー	定義済みのアクセス用自動 QoS ポリシー
アップリンク ポートの QoS ポリシー	作成済みのディストリビューション用QoSポリシー	作成済みのディストリビューション用QoSポリシー	作成済みのディストリビューション用QoSポリシー
アップリンク インターフェイス	トランク ポートとして設定される、選択されたアップリンク インターフェイス（すべてのVLANを許可するように設定）	トランク モードで Port-channel として設定される、選択されたポート（すべてのVLANを許可するように設定）	トランク モードで Port-channel として設定される、選択されたポート（すべてのVLANを許可するように設定）
ダウンリンク インターフェイス	アクセスモードで設定されているダウンリンク ポート	アクセスモードで設定されているダウンリンク ポート	アクセスモードで設定されているダウンリンク ポート
Port-channel	設定なし	作成済みのディストリビューションへの Port-channel	作成済みのディストリビューションへの Port-channel

図 *12 : [Site Profile] > [Access Switches]*

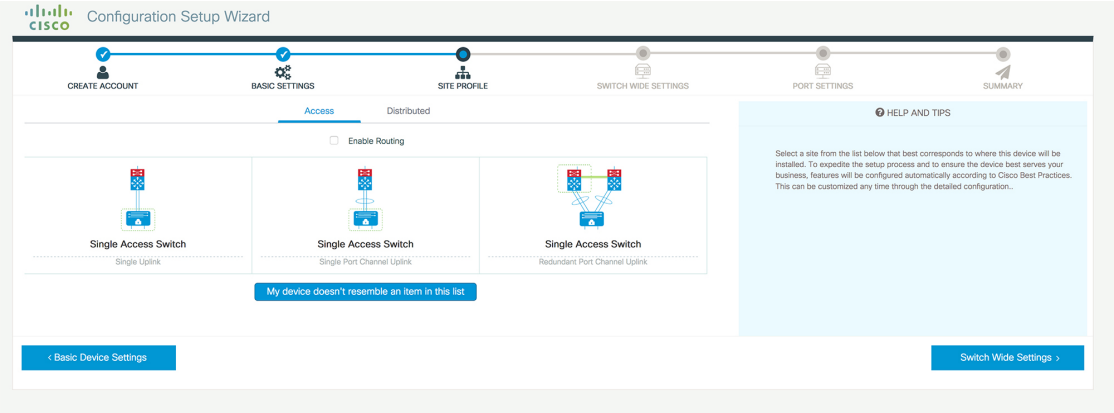
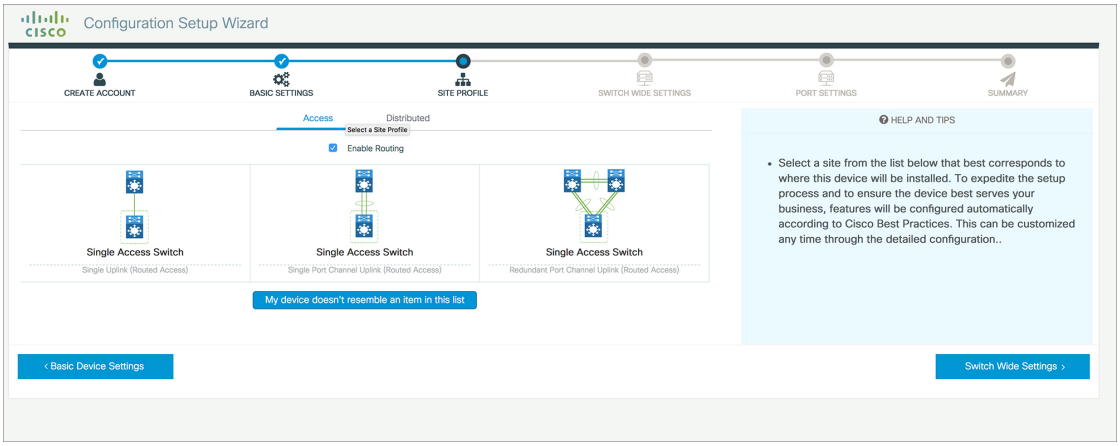


図 *13 : [Site Profile] > [Access Switches]*（ルーテッド アクセスの場合）



VLAN の設定

ステップ 1 [VLAN Configuration] セクションでは、データ VLAN と音声 VLAN の両方を設定できます。データ VLAN の名前を入力します。

ステップ 2 データ VLAN を設定するには、[Data VLAN] チェック ボックスがオンになっていることを確認し、VLAN の名前を入力して、VLAN ID を割り当てます。複数の VLAN を作成する場合は、VLAN の範囲のみを指定します。

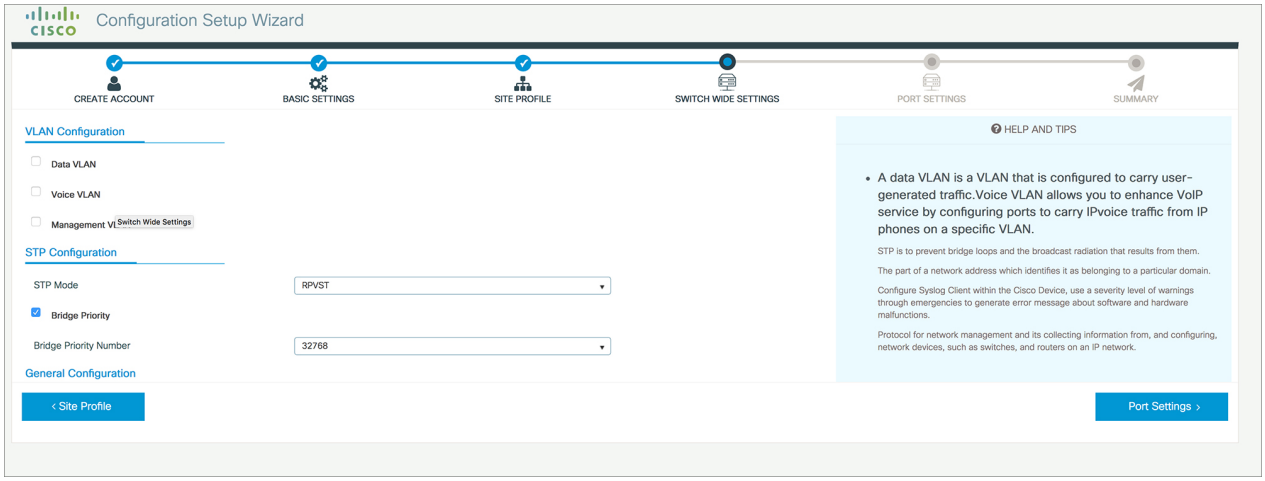
ステップ 3 音声 VLAN を設定するには、[Voice VLAN] チェック ボックスがオンになっていることを確認し、VLAN の名前を入力して、VLAN ID を割り当てます。複数の VLAN を作成する場合は、VLAN 範囲を指定します。

STP の設定

ステップ 1 RPVST はデバイスでデフォルトの STP モードです。[STP Mode] ドロップ ダウン リストでこれを PVST に変更できます。

ステップ 2 ブリッジプライオリティ番号をデフォルト値 32748 から変更するには、[Bridge Priority] を [Yes] に変更し、ドロップ ダウン リストからプライオリティ番号を選択します。

図 *14 : VLAN* と *STP* の設定



DHCP、NTP、DNS、SNMP の設定

ステップ 1 [Domain Details] セクションに、非修飾ホスト名を完成させるためにソフトウェアで使用されるドメイン名を入力します。

ステップ 2 DNS サーバを識別する IP アドレスを入力してください。このサーバは、デバイスでの名前とアドレスの解決に使用されます。

ステップ 3 [Server Details] セクションに、DHCP クライアントで使用可能にする DNS サーバの IP アドレスを入力します。

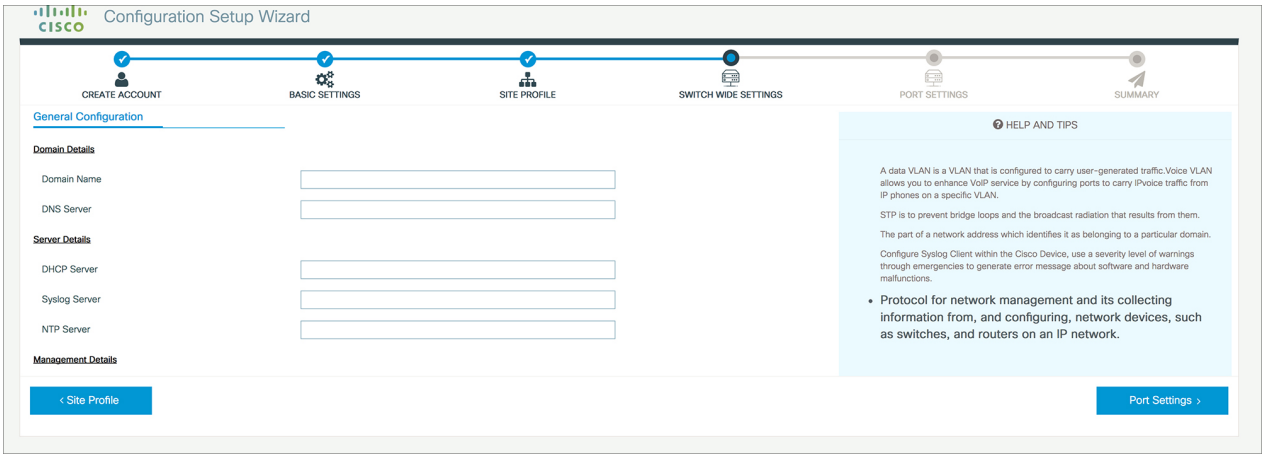
ステップ 4 [Syslog Server] フィールドに、syslog メッセージの送信先となるサーバの IP アドレスを入力します。

ステップ 5 正しい時刻、日付、およびタイムゾーンでデバイスが設定されるようにするには、デバイスの時間の同期相手となる NTP サーバの IP アドレスを入力します。

ステップ 6 [Management Details] セクションに、SNMP サーバを識別する IP アドレスを入力します。デバイスでは SNMPv1、SNMPv2、および SNMPv3 がサポートされています。

ステップ 7 SNMP プロトコルへのアクセスを許可する **SNMP コミュニティ** 文字列を指定します。

図 *15 : DHCP*、*NTP*、*DNS*、*SNMP* の設定



次のタスク

ポートを設定します。

ポート設定

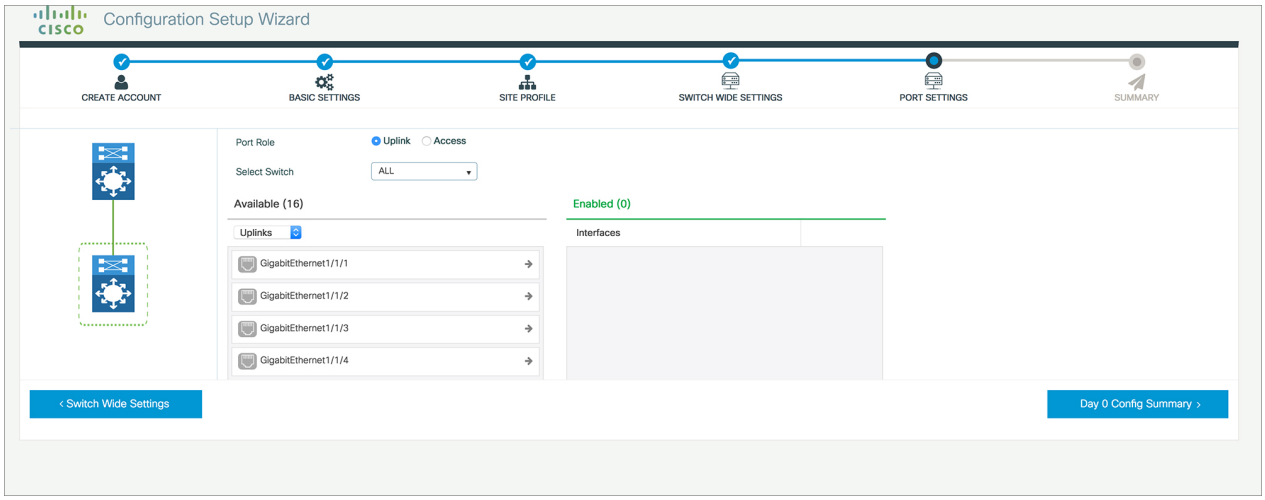
ステップ 1 前の手順で選択したサイトプロファイル（画面左側に表示）に基づいて、以下のオプションの中から [Port Role] を選択します。

- [Uplink]：ネットワークのコア方向にあるデバイスに接続します。
- [Downlink]：ネットワーク トポロジ内で下流にあるデバイスに接続します。
- [Access]：VLAN 未対応のゲスト デバイスに接続します。

ステップ 2 [Select Switch] ドロップダウン リストからオプションを選択します。

ステップ 3 有効化する方法に応じて [Available] インターフェイス リストから選択し、[Enabled] リストを開きます。

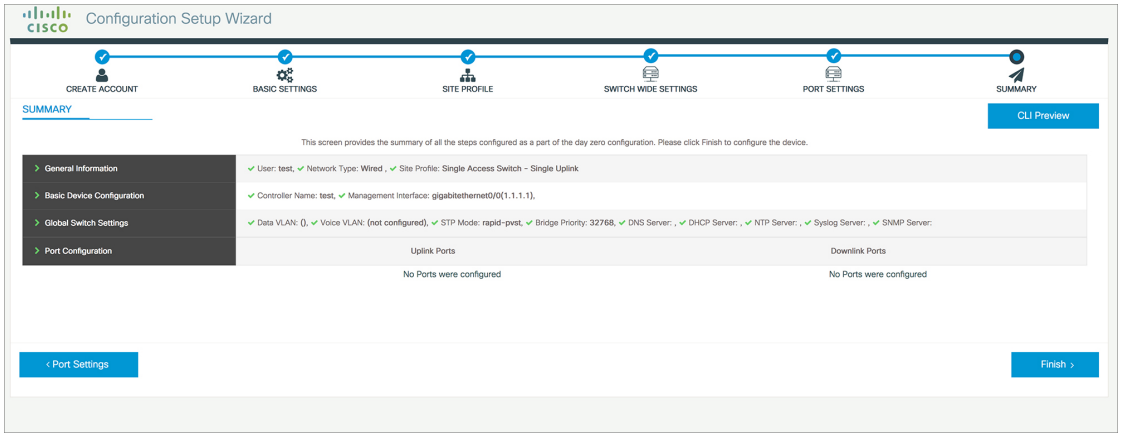
図 *16* : ポート設定



次のタスク

- [Day 0 Config Summary] をクリックして設定を確認します。
- [Finish] をクリックします。

図 *17 : Day 0 Config Summary*



VTY 回線の設定

Telnet または SSH を経由してデバイスに接続する場合は、仮想端末回線または仮想テレタイプ（VTY）が使用されます。VTY 回線の数は、リモートによるデバイスへの同時アクセス数の最大値に一致します。デバイスに十分な数の VTY 回線が設定されていない場合、ユーザが WebUI に接続する際に問題が発生することがあります。VTY 回線のデフォルト値は 0 ー 15 です。デバイスでは、最大 98 の同時セッションが可能です。

ステップ 1 WebUI から [Administration] > [Device] に移動し、[General] ページを選択します。

ステップ 2 [VTY Line] フィールドに、設定する VTY 回線の数に応じて **0 ～ xx** を入力します。

図 *18 : VTY* 回線の設定