



## Cisco IOS XE Amsterdam 17.2.x (Catalyst 9200 スイッチ) ソフトウェア コンフィギュレーション ガイド

初版：2020年3月30日

### シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター  
0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>



## 目次

はじめに :	はじめに vii
	表記法 vii
	関連資料 ix
	マニュアルの入手方法およびテクニカル サポート x
第 1 章	目次 1
第 2 章	Web ユーザ インターフェイスを使用したスイッチの設定 3
	デイ 0 WebUI 設定の概要 3
	Cisco DNA Center クラウド導入準備デイ 0 ウィザード 4
	アカウント設定の構成 4
	基本デバイスの設定 5
	接続のテストの設定 7
	クラシックデイ 0 ウィザード 7
	スイッチへの接続 8
	ユーザ アカウントの作成 10
	セットアップ オプションの選択 11
	基本デバイスの設定 11
	サイト プロファイルに基づいたデバイスの設定 13
	VLAN の設定 15
	STP の設定 16
	DHCP、NTP、DNS、SNMP の設定 16
	ポート設定 17

VTY 回線の設定 18



【注意】シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.





## はじめに

ここでは、このマニュアルの表記法、および他資料の入手方法について説明します。また、シスコ製品のマニュアルの最新情報についても説明します。



(注) この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFPのドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

- [表記法](#) (vii ページ)
- [関連資料](#) (ix ページ)
- [マニュアルの入手方法およびテクニカルサポート](#) (x ページ)

## 表記法

このマニュアルでは、以下の表記法を使用しています。

表記法	説明
^ または Ctrl	^ 記号と Ctrl は両方ともキーボードの Control (Ctrl) キーを表します。たとえば、^D または Ctrl+D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します (ここではキーを大文字で表記していますが、小文字で入力してもかまいません)。
太字	コマンド、キーワード、およびユーザーが入力するテキストは太字で記載されます。
<i>italic</i> フォント	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、イタリック体で示しています。

表記法	説明
Courier フォント	システムが表示する端末セッションおよび情報は、courier フォントで示しています。
太字の courier フォント	太字の Courier フォントは、ユーザが入力しなければならないテキストを示します。
[x]	角カッコの中の要素は、省略可能です。
...	構文要素の後の省略記号（3つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。
	パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示します。
[x y]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
{x y}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x {y z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めてstring とみなされます。
<>	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[]	システムプロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!, #	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。

### 読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。



(注) 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。





ヒント 「問題解決に役立つ情報」です。



注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。



ワンポイントアドバイス

時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。



警告 安全上の重要な注意事項

この警告マークは「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。ステートメント 1071

これらの注意事項を保存しておいてください

## 関連資料



(注) device をインストールまたはアップグレードする前に、device のリリースノートを参照してください。



(注) スイッチの設置またはアップグレードを実施する前に、スイッチのリリースノートを参照してください。

- 次の URL にある Cisco Catalyst 9400 シリーズ スイッチのマニュアル：

<http://www.cisco.com/go/c9400>

## マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカルサポート、その他の有用な情報について、毎月更新される『更新情報』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

<http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>

『更新情報』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。



# 第 1 章

## 目次

---

Cisco TrustSec

Bonjour 向け DNA サービス

インターフェイスおよびハードウェアコンポーネント

IP アドレッシングサービス

IP マルチキャストルーティング

レイヤ 2

Network Management

プログラマビリティ

Quality of Service

IP ルーティング

セキュリティ

スタック構成と高可用性

システム管理

VLAN





## 第 2 章

# 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 \(3 ページ\)](#)
- [Cisco DNA Center クラウド導入準備デイ 0 ウィザード \(4 ページ\)](#)
- [クラシックデイ 0 ウィザード \(7 ページ\)](#)

## デイ 0 WebUI 設定の概要

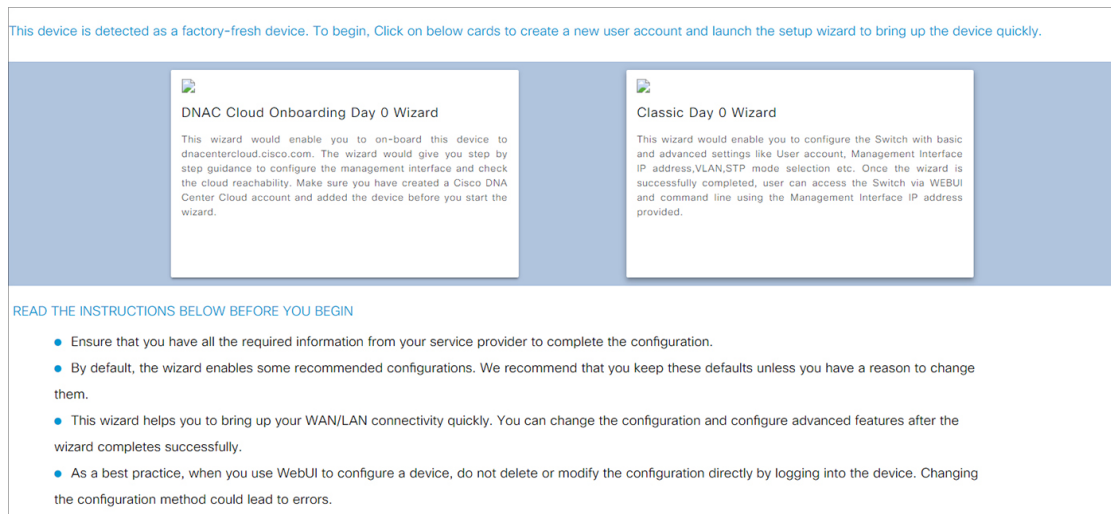
ハードウェアの取り付けが完了したら、トラフィックがネットワークを通過するのに必要な構成を使用してスイッチを設定する必要があります。新しいデバイスを使用する最初の日には、さまざまなタスクを実行することにより、デバイスがオンライン状態かつ到達可能で、簡単に設定されることを確認できます。

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、ユーザー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

The screenshot shows the 'Configuration Setup Wizard' interface. At the top, there are four tabs: ACCOUNT SETTINGS, BASIC SETTINGS, TEST CONNECTIVITY, and SUMMARY. The 'ACCOUNT SETTINGS' tab is active. Below the tabs, there are two main sections: 'Create New Account' and 'Device ID Settings'. The 'Create New Account' section has three input fields: 'Login Name\*' (containing 'testuser'), 'Login User Password\*' (containing '.....'), and 'Confirm Login User Password\*'. The 'Device ID Settings' section has three input fields: 'Device Name\*' (containing 'testdevice'), 'NTP Server' (containing 'x.x.x.x'), and 'Date & Time Mode' (a dropdown menu set to 'NTP Time'). On the right side, there is a 'HELP AND TIPS' section with a light blue background. It contains the following text: 'Establish a new Username and Password for the Device. Please remember it for next Login. Establish a new password for the privileged command level. Device name is an identification that is given to the physical hardware device. Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. Enter the IP address of the NTP server. If manual time is set then the difference in time will be adjusted at the time of configuring the device.' At the bottom of the wizard, there are two buttons: '< Welcome Page' and 'Basic Settings >'. The 'Basic Settings >' button is highlighted in blue.

## 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。

- [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。
- 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。
- 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)。
- 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

Configuration Setup Wizard

ACCOUNT SETTINGS    BASIC SETTINGS    TEST CONNECTIVITY    SUMMARY

**Device Management Settings**

IP Address     Static     DHCP

VLAN ID\*   

IP Address\*   

Subnet Mask\*   

Default Gateway (optional)   

Associate VLAN Interface   

DNS Server   

< Create New Account    Test Connectivity >

**HELP AND TIPS**

Select this to enable access to the device using Telnet. Configure a username and password to authenticate user access to the device.

Select this to enable access to the device using Telnet. Configure a username and password to authenticate user access to the device.

Select this to enable secure remote access to the device using Secure Shell (SSH). Configure a username and password to authenticate user access to the device.

Enable transparent mode if you do not want the switch to participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements, but transparent switches do forward VTP advertisements that they receive out their trunk ports in VTP Version 2.

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

Configuration Setup Wizard

ACCOUNT SETTINGS    BASIC SETTINGS    TEST CONNECTIVITY    SUMMARY

**Device Management Settings**

IP Address     Static     DHCP

VLAN ID\*   

IP Address\*   

Subnet Mask\*   

Default Gateway (optional)   

DNS Server   

< Create New Account    Test Connectivity >

**HELP AND TIPS**

Select this to enable access to the device using Telnet. Configure a username and password to authenticate user access to the device.

Select this to enable access to the device using Telnet. Configure a username and password to authenticate user access to the device.

Select this to enable secure remote access to the device using Secure Shell (SSH). Configure a username and password to authenticate user access to the device.

Enable transparent mode if you do not want the switch to participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements, but transparent switches do forward VTP advertisements that they receive out their trunk ports in VTP Version 2.



## 接続のテストの設定

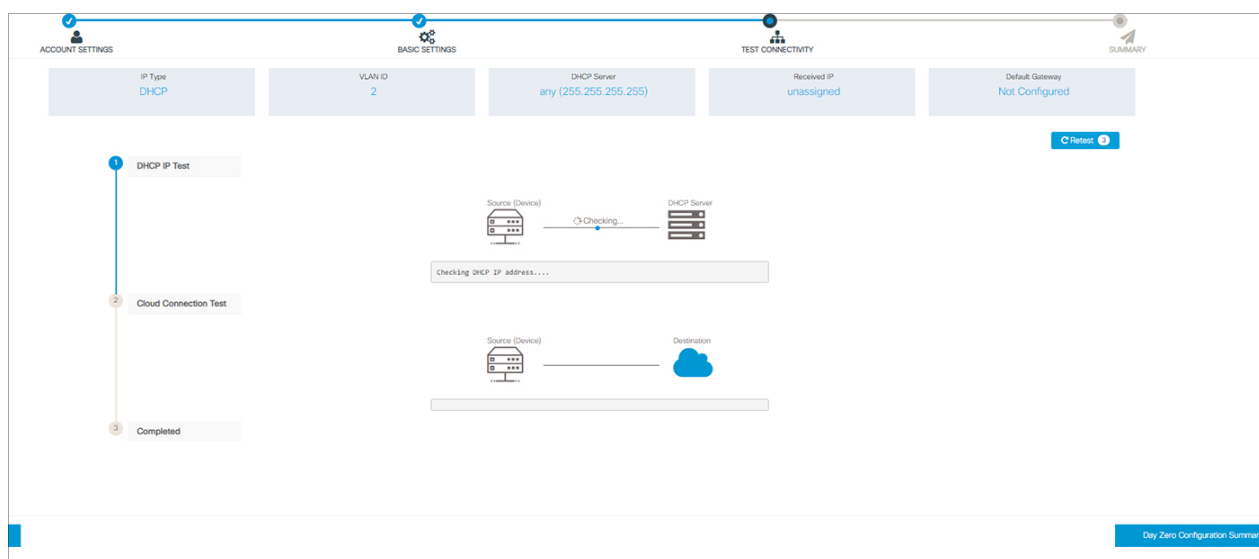
**ステップ 1** デバイス間で Cisco DNAC クラウドへの接続が確立されていることを確認するには、[Test Connectivity/Retest] ボタンを使用します。

**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。

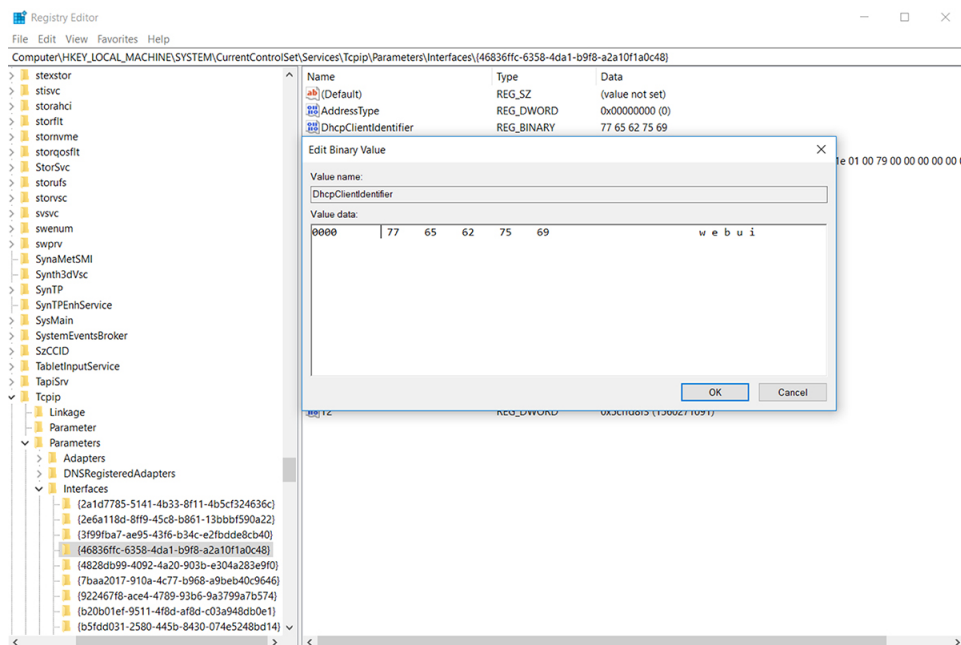
### Windows クライアントでの DHCP クライアント識別子のセットアップ

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 Control] 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

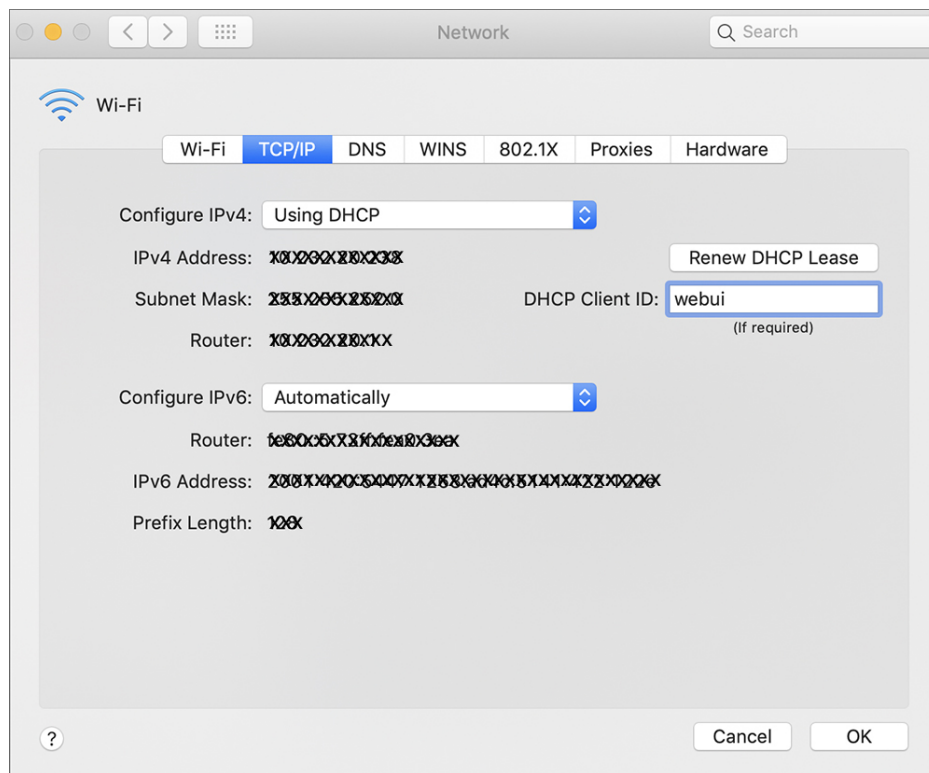


5. PC を再起動して設定を有効にします。

### 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

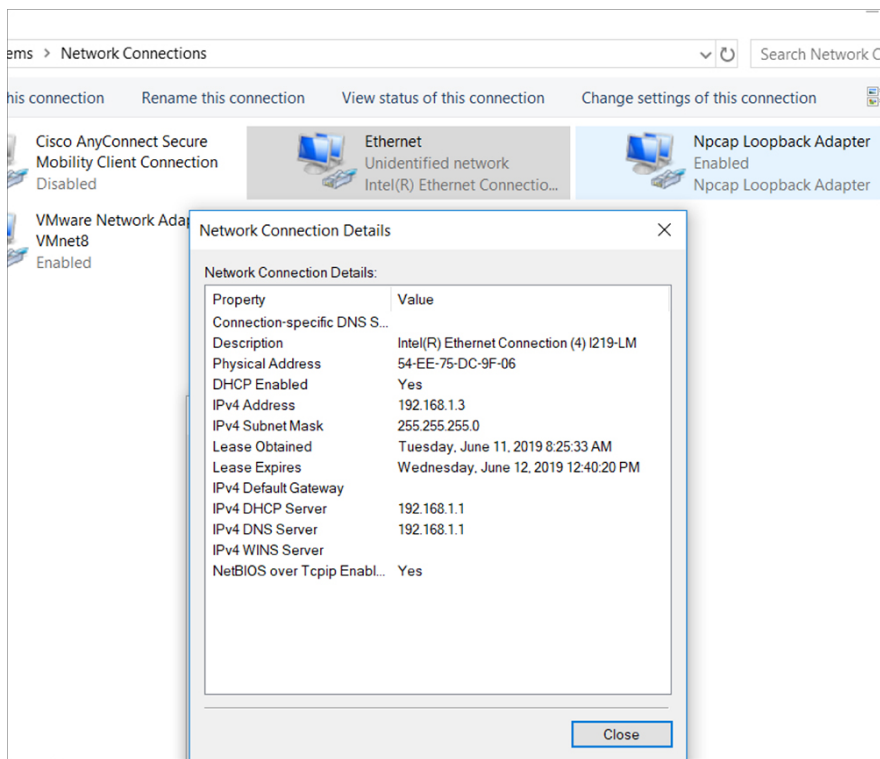


2. [OK] をクリックして変更を保存します。

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

The screenshot displays the 'Configuration Setup Wizard' interface for creating a new account. The progress bar indicates the current step is 'CREATE ACCOUNT'. The form contains three input fields for 'Login Name', 'Password', and 'Confirm password'. To the right, there are sections for 'Platform Type', 'IOS Installed', 'Serial Number', 'Modules', and 'License Installed'. A 'Create New Account' button is located at the bottom center, and a 'Basic Device Settings >' button is at the bottom right.

## 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] &gt; [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] &gt; [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ンネルアップリンク)	シングル アクセス スイッチ (冗長ポートチャンネルアップリンク)
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的に設定	リカバリモードを自動的に設定	リカバリモードを自動的に設定
ポートチャン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。 <ul style="list-style-type: none"> <li>• Default VLAN</li> <li>• データ VLAN</li> <li>• 音声 VLAN</li> <li>• Management VLAN</li> </ul>	次の VLAN が作成されます。 <ul style="list-style-type: none"> <li>• Default VLAN</li> <li>• データ VLAN</li> <li>• 音声 VLAN</li> <li>• Management VLAN</li> </ul>	次の VLAN が作成されます。 <ul style="list-style-type: none"> <li>• Default VLAN</li> <li>• データ VLAN</li> <li>• 音声 VLAN</li> <li>• Management VLAN</li> </ul>
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] &gt; [Access Switches]

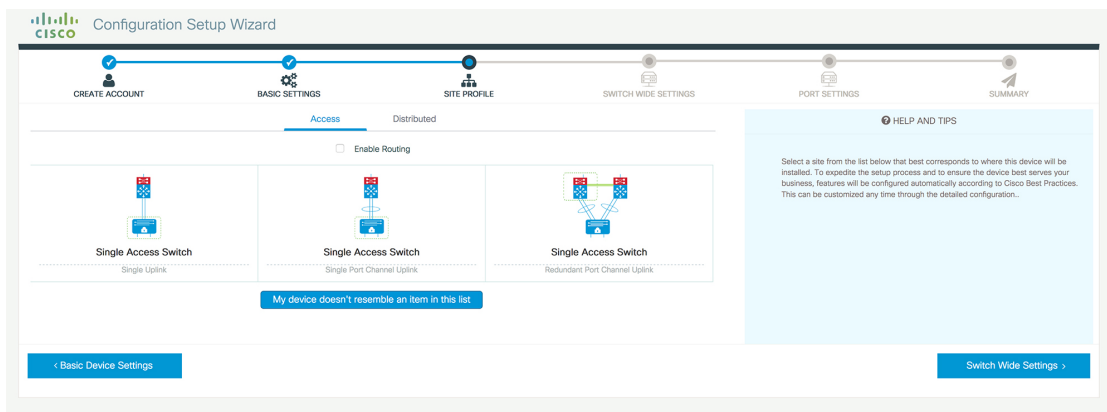
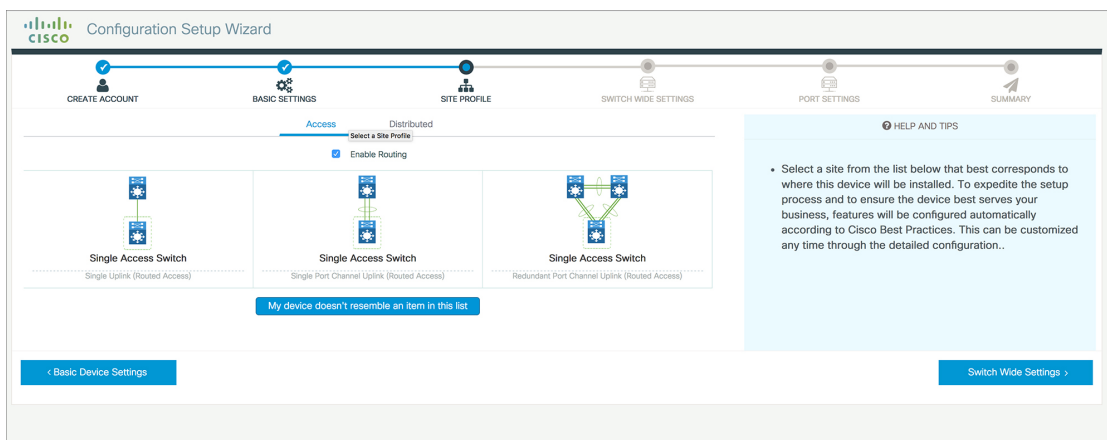


図 13 : [Site Profile] &gt; [Access Switches] (ルーテッドアクセスの場合)



## 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

The screenshot shows the 'Configuration Setup Wizard' interface for a Cisco switch. The progress bar at the top indicates the current step is 'SWITCH WIDE SETTINGS'. The main content area is divided into three sections:

- VLAN Configuration:** Contains three checkboxes: 'Data VLAN', 'Voice VLAN', and 'Management VLAN (Switch Wide Settings)'. All are currently unchecked.
- STP Configuration:** Contains a dropdown menu for 'STP Mode' set to 'RPVST', a checked checkbox for 'Bridge Priority', and a dropdown menu for 'Bridge Priority Number' set to '32768'.
- General Configuration:** Contains a '< Site Profile' button.

On the right side, there is a 'HELP AND TIPS' panel with the following text:

- A data VLAN is a VLAN that is configured to carry user-generated traffic. Voice VLAN allows you to enhance VoIP service by configuring ports to carry IP voice traffic from IP phones on a specific VLAN.
- STP is to prevent bridge loops and the broadcast radiation that results from them.
- The part of a network address which identifies it as belonging to a particular domain.
- Configure Syslog Client within the Cisco Device, use a severity level of warnings through emergencies to generate error message about software and hardware malfunctions.
- Protocol for network management and its collecting information from, and configuring, network devices, such as switches, and routers on an IP network.

At the bottom right, there is a 'Port Settings >' button.

## 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。

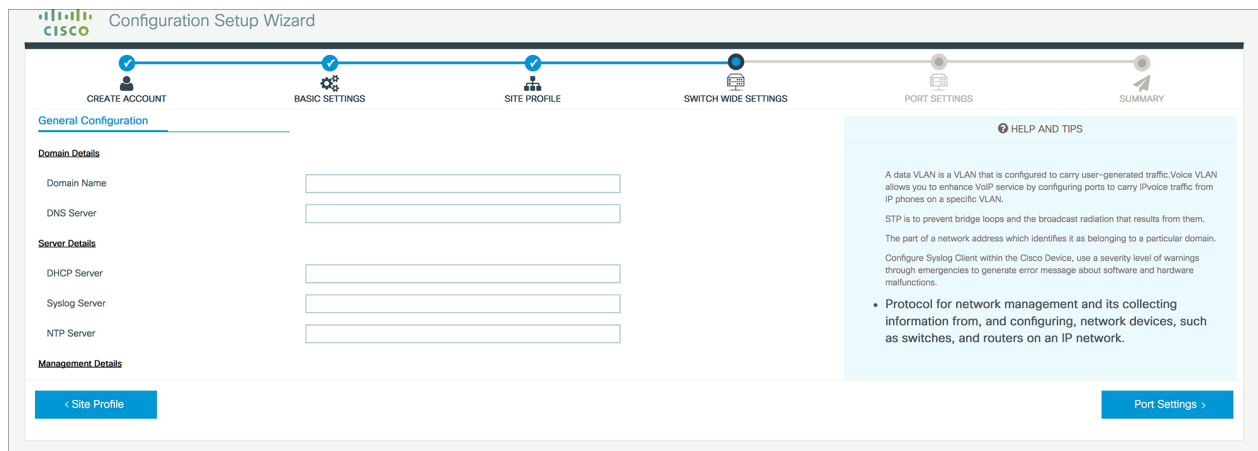
**ステップ 4** [Syslog Server] フィールドに、syslog メッセージの送信先となるサーバの IP アドレスを入力します。

**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

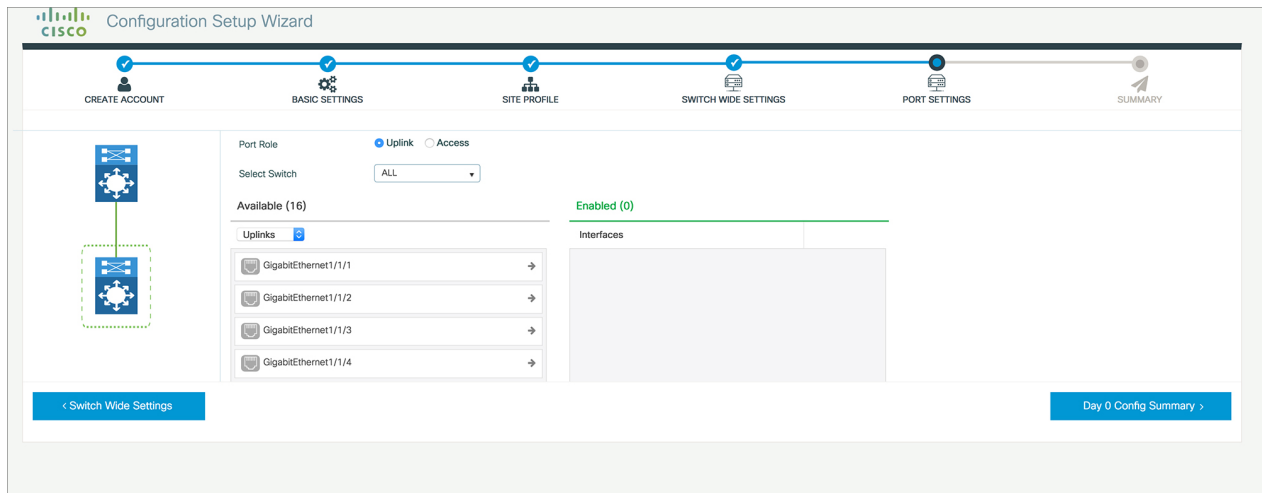
**ステップ 1** 前の手順で選択したサイトプロファイル（画面左側に表示）に基づいて、以下のオプションの中から [Port Role] を選択します。

- [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。

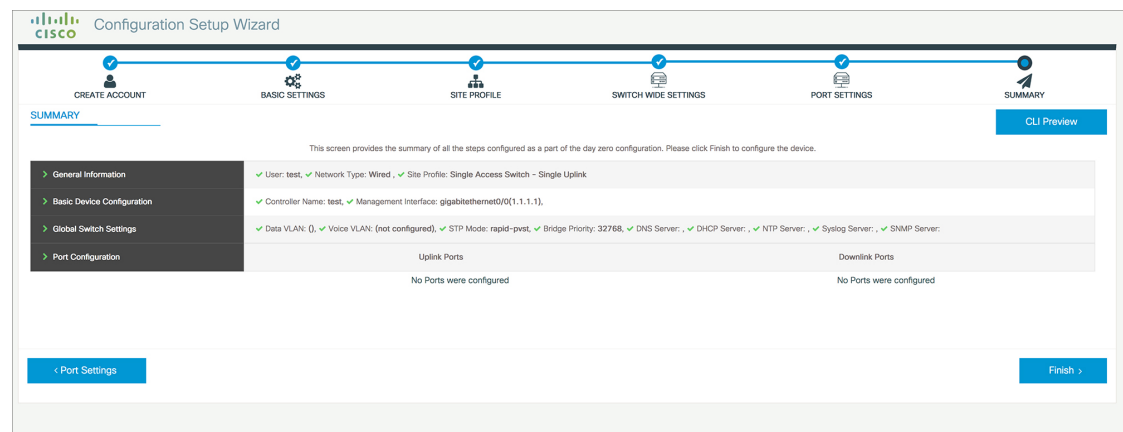
図 16: ポート設定



### 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 ~ 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

The screenshot shows the Cisco WebUI configuration page for VTY lines. The breadcrumb navigation is Administration > Device. The left sidebar contains a search bar and menu items: Dashboard, Monitoring, Configuration, Administration (selected), Licensing, and Troubleshooting. The main content area is titled 'Administration > Device' and has a 'General' tab selected. The configuration fields are as follows:

Field	Value
IP Routing	DISABLED
Host Name*	SW-9200
Banner	
Management Interface	GigabitEthernet0/0
IP Address*	
Subnet Mask*	
System MTU(Bytes)	1500
VTY Line	0-30
VTY Transport Mode	Select a value

There is a link 'View VTY options' next to the VTY Line field.

