CHAPTER 3

デバイス コミュニティ

Cisco Configuration Professional（Cisco CP）では、管理者がログインして管理できるデバイスのコミュニティを作成できます。コミュニティ情報が保存されると、コミュニティ内の各デバイスの IP アドレスとクレデンシャルが Cisco CP で記憶されます。管理者は、コミュニティを選択してからログイン先のデバイスを選択するだけで、コミュニティ内のデバイスにログインできます。

この章の内容は、次のとおりです。

コミュニティの作成

Cisco CP には、画面に示される手順に従ってコミュニティを作成できるウィザードが用意されています。ここでは、このウィザードの使用方法とウィザードの個々の画面について説明します。各セクションの内容は、次のとおりです。

- コミュニティ ウィザードを使用したコミュニティの作成
- コミュニティ ウィザード画面のリファレンス

コミュニティ ウィザードを使用したコミュニティの作成

コミュニティ ウィザードを使用してコミュニティを作成するには、次の手順に従ってください。

ステップ 1　［コミュニティの選択 / 作成］ボタンをクリックして［コミュニティの選択 / 作成］画面を表示します。［コミュニティの選択 / 作成］画面は、Cisco CP の起動時にも表示されます。

ステップ 2　［コミュニティの選択 / 作成］画面の［作成］をクリックします。［コミュニティ名の入力］ウィザード画面が表示されます。

ステップ 3　［コミュニティ名の入力］画面で、コミュニティ名を入力します。次に、［次へ］をクリックします。

ステップ 4　［コミュニティ メンバの追加 / 編集］ウィザード画面の［作成］をクリックします。［コミュニティ エントリの作成］画面が表示されます。

ステップ 5　［コミュニティ エントリの作成］画面で、コミュニティ メンバの IP アドレス、ユーザ名、およびパスワードの情報を入力します。次に、［OK］をクリックします。この画面の詳細については、「コミュニティ ウィザード画面のリファレンス」の項（P. 3-3）の「［コミュニティ エントリの作成］または［コミュニティ エントリの編集］」を参照してください。

ステップ 6　別のコミュニティ メンバを追加するには、［作成］をもう一度クリックして、そのコミュニティ メンバの IP アドレスと認証情報を入力します。

ステップ 7　コミュニティのメンバの追加が完了したら、［次へ］をクリックします。コミュニティが作成されたことを示す［完了］画面が表示されます。この画面から、別のコミュニティを作成することもできます。

ステップ 8　［完了］画面で、別のコミュニティを作成するかコミュニティ ウィザードを終了するかを選択します。

a.　別のコミュニティを作成するには、［他のコミュニティの作成］をクリックして［OK］をクリックします。次に、ステップ 3 以降をもう一度実行します。

b.　コミュニティ ウィザードを終了するには、［完了 - ウィザードを終了］をクリックします。

コミュニティ ウィザード画面のリファレンス

次の各トピックで、コミュニティ ウィザードの画面について説明します。

コミュニティ名の入力

［コミュニティ名の入力］画面では、デバイスのコミュニティの名前を入力します。

この画面へのアクセス方法

- ツールバーの［コミュニティの選択 / 作成］>［作成］をクリックします。
- ［アプリケーション］>［コミュニティの選択 / 作成］>［作成］をクリックします。

フィールド リファレンス

表 3-1　コミュニティ名

要素	説明
新しいコミュニティ名の入力	コミュニティ名を入力します。この名前は、このコミュニティ内にあるデバイスにアクセスするときに使用します。名前には、スペースを含めることができます。たとえば、「comm 1」という名前を使用できます。

コミュニティ メンバの追加 / 編集

［コミュニティ メンバの追加 / 編集］画面では、コミュニティ メンバの作成、コミュニティ メンバの設定の編集、および作成しているコミュニティの全メンバの一覧表示が可能です。

この画面へのアクセス方法

- ツールバーの［コミュニティの選択 / 作成］>［作成］>［次へ］をクリックします。
- ［アプリケーション］>［コミュニティの選択 / 作成］>［作成］>［次へ］をクリックします。

関連リンク

- コミュニティ情報

フィールド リファレンス

表 3-2　コミュニティ メンバの追加 / 編集

要素	説明
コミュニティ名	［コミュニティ名の入力］画面で入力したコミュニティ名です。
フィルタ	指定のテキストが含まれているエントリだけを表示するには、そのテキストをフィルタ ボックスに入力します。表示は、1 文字入力するたびに更新されます。
IP アドレス	コミュニティに追加されたデバイスの IP アドレスです。デバイスが 1 つも追加されていない場合は、このカラムに IP アドレスは表示されません。

表 3-2　コミュニティ メンバの追加 / 編集（続き）

要素	説明
作成	コミュニティにデバイスを追加するには、[作成] をクリックしてからデバイスの IP アドレスを入力し、そのデバイス上で設定されているユーザ名とパスワードを入力します。
編集	コミュニティ メンバの情報を編集するには、コミュニティ メンバのエントリを選択して［編集］をクリックし、表示されたダイアログで IP アドレス、ユーザ名、およびパスワードの情報を編集します。
削除	メンバをコミュニティから削除するには、コミュニティ メンバのエントリを選択して［削除］をクリックします。
ルータのステータス	コミュニティ メンバのハードウェア、ソフトウェア、および機能の詳細情報を表示するには、そのメンバのエントリを選択して［ルータのステータス］をクリックします。

［コミュニティ エントリの作成］または［コミュニティ エントリの編集］

［コミュニティ エントリの作成］画面と［コミュニティ エントリの編集］画面では、コミュニティ内のデバイスの IP アドレス、ユーザ名、およびパスワードを入力します。

この画面へのアクセス方法

- ツールバーの［コミュニティの選択 / 作成］>［作成］>［次へ］>［作成］をクリックします。
- ［アプリケーション］>［コミュニティの選択 / 作成］>［作成］>［次へ］>［作成］をクリックします。
- ［アプリケーション］>［コミュニティの選択 / 作成］>＜ *コミュニティ名* ＞>［OK］>［作成］をクリックします。
- ［アプリケーション］>［コミュニティの選択 / 作成］>＜ *コミュニティ名* ＞>［OK］>＜ *コミュニティ メンバ エントリ* ＞>［編集］をクリックします。

フィールド リファレンス

表 3-3　コミュニティ情報

要素	説明
IP アドレス	デバイスの IP アドレスをドット区切り 10 進表記で入力します（たとえば、192.168.233.332）。
ルータのログイン名	ルータへのログインに使用するユーザ名を入力します。
ルータのパスワード	入力したユーザ名に対応するパスワードを入力します。
認証の有効化	
ルータのパスワードと同じ	enable パスワードと［ルータのパスワード］フィールドに入力されたルータ パスワードが同一の場合は、このチェック ボックスを選択します。
イネーブル パスワード	enable パスワードと［ルータのパスワード］フィールドに入力されたルータ パスワードが異なる場合は、このフィールドに enable パスワードを入力します。

完了

コミュニティ ウィザードの［完了］画面では、ウィザードをもう一度起動して別のコミュニティを作成することも、ウィザードを終了することもできます。

この画面へのアクセス方法

- ツールバーの［コミュニティの選択 / 作成］>［作成］>［次へ］>［次へ］をクリックします。
- ［アプリケーション］>［コミュニティの選択 / 作成］>［作成］>［次へ］>［次へ］をクリックします。

フィールド リファレンス

表 3-4　［完了］画面のボタン

要素	説明
他のコミュニティの作成	他のコミュニティを作成するには、［他のコミュニティの作成］をクリックして［OK］をクリックします。
完了 - ウィザードを終了	別のコミュニティを作成しない場合は、［完了 - ウィザードを終了］をクリックして［完了］をクリックします。

コミュニティの保守

コミュニティ メンバは、追加したり削除したりできます。また、コミュニティ メンバの情報を編集することもできます。このセクションの内容は、次のとおりです。

- コミュニティ情報の編集
- コミュニティ保守画面のリファレンス

コミュニティ情報の編集

コミュニティの情報を編集するには、次の手順に従ってください。

ステップ 1　［アプリケーション］>［コミュニティの選択 / 作成］をクリックします。［コミュニティの選択 / 作成］画面が表示されます。［コミュニティの選択 / 作成］画面は、Cisco CP の起動時にも表示されます。

ステップ 2　［コミュニティの選択 / 作成］画面で、コミュニティの名前を選択します。

ステップ 3　下部のボタン バーの［OK］をクリックします。［コミュニティ情報］画面が表示されます。詳細については、「コミュニティ保守画面のリファレンス」の「コミュニティ情報」を参照してください。

ステップ 4　［コミュニティ情報］画面で、必要な変更を加えます。

- 新しいコミュニティ メンバを追加するには、［作成］をクリックし、コミュニティ メンバの情報を入力します。
- メンバをコミュニティから削除するには、削除するメンバのエントリを選択して［削除］をクリックします。
- コミュニティ メンバの情報を編集するには、メンバのエントリを選択して［編集］をクリックします。次に、［コミュニティエントリの編集］画面で情報を編集します。詳細については、「コミュニティ ウィザード画面のリファレンス」の「［コミュニティ エントリの作成］または［コミュニティ エントリの編集］」を参照してください。

変更した情報はすべて自動的に保存されます。

コミュニティ保守画面のリファレンス

次の各セクションで、コミュニティの保守に使用する画面について説明します。

- コミュニティの選択 / 作成
- コミュニティ情報
- ［コミュニティ エントリの作成］または［コミュニティ エントリの編集］

コミュニティの選択 / 作成

［コミュニティの選択 / 作成］画面は、管理対象の既存のコミュニティを選択するとき、または新しいコミュニティを作成するときに使用します。

この画面へのアクセス方法

- ［コミュニティの選択 / 作成］画面は、Cisco CP の起動時に自動的に表示されます。
- ツールバーの［コミュニティの選択 / 作成］をクリックします。
- ［アプリケーション］>［コミュニティの選択 / 作成］をクリックします。

フィールド リファレンス

表 3-5　コミュニティの選択または作成

要素	説明
フィルタ	指定のテキストが含まれているエントリだけを表示するには、そのテキストをフィルタ ボックスに入力します。表示は、1 文字入力するたびに更新されます。
名前	コミュニティの名前（たとえば「comm 1」）です。
メンバの数	コミュニティ内のメンバの数です。
作成	コミュニティ ウィザードを起動するには、［作成］をクリックします。
削除	コミュニティの情報を削除するには、コミュニティのエントリを選択して［削除］をクリックします。
OK	管理対象のコミュニティを選択するには、コミュニティのエントリを選択して［OK］をクリックします。
キャンセル	［コミュニティの選択 / 作成］ウィンドウを閉じるには、［キャンセル］をクリックします。

コミュニティ情報

［コミュニティ情報］画面には、コミュニティの情報の要約が表示されます。この画面では、各コミュニティ メンバの検出、作成、編集、およびステータスの確認が可能です。

この画面へのアクセス方法

- ツールバーの［コミュニティの選択 / 作成］>< *コミュニティ名* >>［OK］をクリックします。
- ［アプリケーション］>［コミュニティの選択 / 作成］>< *コミュニティ名* >>［OK］をクリックします。

関連リンク

- コミュニティ メンバの追加 / 編集

フィールド リファレンス

表 3-6　コミュニティ情報

要素	説明
コミュニティ情報	
コミュニティ名	コミュニティの名前です。
コミュニティ内のデバイスの数	コミュニティ内のデバイスの数です。
コミュニティ メンバ	
フィルタ	指定のテキストが含まれているエントリだけを表示するには、そのテキストをフィルタ ボックスに入力します。表示は、1 文字入力するたびに更新されます。
IP アドレス	コミュニティ メンバの IP アドレスです。
ホスト名	IP アドレスに対応するホスト名がある場合は、その名前。
検出のステータス	このカラムには、次のいずれかの値が表示されます。 • ［検出済み］：デバイスは検出済みで、使用可能です。 • ［未検出］：デバイスは検出されていません。

表 3-6　コミュニティ情報（続き）

要素	説明
ボタン	
作成	コミュニティにメンバを追加するには、［作成］をクリックして、表示されたダイアログで IP アドレス、ユーザ名、およびパスワードの情報を入力します。
編集	コミュニティ メンバの情報を編集するには、コミュニティ メンバのエントリを選択して［編集］をクリックし、表示されたダイアログで IP アドレス、ユーザ名、およびパスワードの情報を編集します。
削除	メンバをコミュニティから削除するには、コミュニティ メンバのエントリを選択して［削除］をクリックします。
検出	コミュニティ メンバを検出するには、検出する各メンバのエントリを選択して［検出］をクリックします。
検出の詳細	デバイスのコミュニティ ステータスに関する詳細情報を表示するには、メンバのエントリを選択して［検出の詳細］をクリックします。
ルータのステータス	コミュニティ メンバのハードウェア、ソフトウェア、および機能の詳細情報を表示するには、そのメンバのエントリを選択して［ルータのステータス］をクリックします。

デバイスの検出

デバイスにログインして設定を変更するには、デバイスが属するコミュニティを選択してからそのデバイスを検出する必要があります。ここでは、その方法を説明します。各セクションの内容は、次のとおりです。

- コミュニティの選択とコミュニティ メンバの検出
- 検出されたデバイスに関する情報の表示
- デバイス検出に関する参考情報

コミュニティの選択とコミュニティ メンバの検出

コミュニティを選択してコミュニティ メンバを選択するには、次の手順に従ってください。

ステップ 1　［アプリケーション］>［コミュニティの選択 / 作成］をクリックして［コミュニティの選択 / 作成］画面を表示します。［コミュニティの選択 / 作成］画面は、Cisco CP の起動時にも表示されます。

ステップ 2　［コミュニティの選択 / 作成］画面で、コミュニティの名前を選択します。詳細については、「コミュニティ保守画面のリファレンス」の「コミュニティの選択 / 作成」を参照してください。

ステップ 3　下部のボタン バーの［OK］をクリックします。［コミュニティ情報］画面が表示されます。

ステップ 4　［コミュニティ情報］画面で、検出するデバイスのエントリを選択します。詳細については、「コミュニティ保守画面のリファレンス」の「コミュニティ情報」を参照してください。

ステップ 5　［検出］をクリックします。

［コミュニティ エントリの作成］画面または［コミュニティ エントリの編集］画面で指定された情報を使用して Cisco CP がデバイスにログインすると、［検出のステータス］フィールドが［検出済み］に変更されます。

（注）　検出プロセスが完了までには、数分間かかることがあります。

デバイスが検出されると、Cisco CP を使用してそのデバイスの設定を表示および変更できるようになります。

検出されたデバイスに関する情報の表示

検出されたデバイスに関して検出プロセスで取得された情報、およびそれらのデバイスに関するハードウェアとソフトウェアの情報を表示できます。

検出されたデバイスに関する情報を表示するには、次の手順に従ってください。

ステップ 1　［コミュニティ情報］ウィンドウで、情報を表示する検出済みデバイスを選択します。

ステップ 2　次のいずれの方法で、このデバイスに関する情報を取得します。

- 検出プロセスによって生成された情報を取得するには、［検出の詳細］をクリックします。
- デバイスに関するハードウェアとソフトウェアの情報を取得するには、［ルータのステータス］をクリックします。

ステップ 3　現在の情報ウィンドウを閉じるには、［OK］をクリックします。

検出情報画面のリファレンス

次の各セクションで、検出済みデバイスに関する情報の表示に使用する画面について説明します。

- ［検出の詳細］画面
- ［ルータのステータス］画面

［検出の詳細］画面

デバイスの検出に成功すると、この画面にデバイスの検出プロセスのパフォーマンス情報が表示されます。検出に失敗した場合は、この画面に失敗の理由が表示されます。

この画面へのアクセス方法

- ツールバーの［コミュニティの選択 / 作成］>< *コミュニティ名* >>［OK］をクリックします。
- ［アプリケーション］>［コミュニティの選択 / 作成］>< *コミュニティ名* >>［OK］><*IP アドレス*>>［検出の詳細］をクリックします。

関連リンク

- デバイス検出に関する参考情報

フィールド リファレンス

表 3-7　検出の詳細

要素	説明
検出成功	検出に成功したときは、検出のパフォーマンス データと、検出されたソフトウェア機能に関する情報が表示されます。
ハードウェア検出	このフィールドには、デバイスの検出に使用された方法が表示されます。表示される方法は次のとおりです。 • ［Telnet］: 非セキュア オプションを選択した場合に、デバイス検出時に使用される方法です。 • ［SSH］: セキュア オプションを選択した場合に、デバイス検出時に使用される方法です。
ハードウェア検出に要した時間	ハードウェア機能（インターフェイスやネットワーク モジュールなど）の検出に要した時間の長さです。時間はミリ秒単位で表示されます。
セキュリティ機能使用可能	Cisco CP のセキュリティ機能が使用可能な状態になるのに要した時間の長さです。時間はミリ秒単位で表示されます。
すべての機能検出に要した時間	Cisco CP の全機能が使用可能になるのに要した時間の長さです。時間はミリ秒単位で表示されます。

表 3-7　検出の詳細（続き）

要素	説明
すべての検出に要した時間	ハードウェアとソフトウェアの全機能の検出に要した合計時間の長さです。時間はミリ秒単位で表示されます。
要約	ハードウェアとソフトウェアの全機能が正常に検出された場合は、この行に「すべての機能が正常に検出されました。」と表示されます。
検出失敗	デバイスを検出できなかったときは、失敗の理由が表示されます。
失敗メッセージの例	Ping が失敗しました。 Ping エラー : 10.78.237.105 へは接続できません。ネットワークの接続性を確認してください。

［ルータのステータス］画面

この画面には、検出されたデバイスに関するハードウェアとソフトウェアの詳細情報が表示されます。

この画面へのアクセス方法

- ツールバーの［コミュニティの選択 / 作成］> *< コミュニティ名 >* > ［OK］> *<IP アドレス >* > ［ルータのステータス］をクリックします。
- ［アプリケーション］>［コミュニティの選択 / 作成］> *< コミュニティ名 >* > ［OK］> *<IP アドレス >* > ［ルータのステータス］をクリックします。

フィールド リファレンス

表 3-8　［ルータのステータス］のフィールド

要素	説明
ハードウェアの詳細	
モデル タイプ	デバイスのモデル タイプ（たとえば Cisco 3825）です。
使用可能メモリ / 合計メモリ	使用可能なメモリの大きさと合計メモリの大きさがメガバイト単位で表示されます（たとえば「109/256 MB」）。
フラッシュの合計容量	フラッシュ メモリの容量がメガバイト単位で表示されます（たとえば「61 MB」）。
ソフトウェアの詳細	
IOS バージョン	Cisco IOS のバージョンです（たとえば「12.4(11)T」）。
IOS イメージ	Cisco IOS イメージの名前です（たとえば「c3825-adventerprisek9-mz.124-11.T」）。
ホスト名	ホスト名が設定されている場合は表示されます。たとえば、「c3825-1」です。
機能の可用性	
IP	IP ルーティング機能が使用可能な場合は、緑色のアイコンが表示されます。 IP ルーティング機能が使用不可能な場合は、赤色のアイコンが表示されます。

表 3-8　［ルータのステータス］のフィールド（続き）

要素	説明
ファイアウォール	ファイアウォール機能が使用可能な場合は、緑色のアイコンが表示されます。 ファイアウォール機能が使用不可能な場合は、赤色のアイコンが表示されます。
VPN	仮想プライベート ネットワーク（VPN）機能が使用可能な場合は、緑色のアイコンが表示されます。 仮想プライベート ネットワーク（VPN）機能が使用不可能な場合は、赤色のアイコンが表示されます。
IPS	侵入防止システム（IPS）機能が使用可能な場合は、緑色のアイコンが表示されます。 侵入防止システム（IPS）機能が使用不可能な場合は、赤色のアイコンが表示されます。
NAC	ネットワーク アクセス コントロール（NAC）機能が使用可能な場合は、緑色のアイコンが表示されます。 ネットワーク アクセス コントロール（NAC）機能が使用不可能な場合は、赤色のアイコンが表示されます。

デバイス検出に関する参考情報

ここでは、デバイスを検出できない場合の参考となるように、検出プロセスについて説明します。各セクションの内容は、次のとおりです。

- Cisco CP 設定の要件
- セキュア シェル（SSH）のバージョンが正しくない場合の検出の失敗
- デバイスがファイアウォールによって保護されている場合の検出の失敗
- Cisco CP による既存のクレデンシャルの上書き

Cisco CP 設定の要件

検出が正常に実行されるようにするには、デバイスを正しく設定する必要があります。以下の設定項目に問題がないかどうかを確認してください。

- サポートされるデバイス：検出するデバイスは、Cisco CP によってサポートされているデバイスでなければなりません。『*Release Notes for Cisco Configuration Professional*』を参照してください。このリリース ノートへのリンクは、このヘルプ トピックの終わりに記載されています。
- 正しいユーザ名とパスワード：デバイス上で設定されているユーザ名とパスワードを使用する必要があります。
- 正しい権限レベル：［コミュニティ メンバの追加］画面または［コミュニティ メンバの編集］画面で入力されるユーザ アカウントの権限レベルは 15 でなければなりません。
- vty 回線：Cisco CP とデバイスとの間で確立されるセッションごとに 1 本の vty 回線が使用可能でなければなりません。Cisco CP からデバイスに接続するには、少なくとも 1 本の vty 回線が必要です。CP を使用してデバイス上で別のアプリケーションを起動する場合は、追加のセッションごとに 1 本の vty 回線が必要です。
- vty 回線のトランスポート入力：vty トランスポート入力が、セキュア接続の場合は ssh、非セキュア接続の場合は telnet に設定されている必要があります。

- セキュリティ設定：次のようにセキュリティが設定されている必要があります。
  - ip http server：非セキュア アクセスの場合
  - ip http secure-server：セキュア アクセスの場合
  - ip http authentication local
- プロトコルおよび暗号化の設定：その他の設定、たとえばネットワークへのアクセスを制限するためのファイアウォールやネットワーク アクセス コントロールなどの機能が、検出の妨げとなっていないことを確認してください。

Cisco CP の設定の要件は、『*Release Notes for Cisco Configuration Professional*』に記載されています。また、Cisco CP と共に購入するデバイスに付属しているデフォルトのコンフィギュレーション ファイルには基本的設定が定義されており、この設定を使用すれば検出は正常に実行されます。

リリース ノートを入手するには、次のリンクにアクセスしてください。

http://www.cisco.com/go/ciscocp

［Support］ボックスの［General Information］>［Release Notes］をクリックします。［Release Notes］ページに、最新のリリース ノートがあります。

セキュア シェル（SSH）のバージョンが正しくない場合の検出の失敗

検出するデバイスで使用されているセキュア シェル（SSH）のバージョンが 1.99 や 2.0 ではない場合は、検出に失敗することがあります。この問題を解消するには、バージョンをアップデートする必要があります。デバイスで使用されている SSH のバージョンを確認し、必要に応じて、バージョンをアップデートして RSA キーを再生成するには、次の手順に従ってください。

ステップ 1　デバイスで使用されている SSH のバージョンを確認するために、EXEC モード コマンド **show ip ssh** を入力します。コマンドの入力と出力の例を次に示します。

```
c3845-1(config)# show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
c3845-1(config)#
```

（注）　表示されたバージョンが 1.99 の場合は、SSH のバージョンを 2.0 にアップデートする必要はありません。

ステップ 2　SSH をバージョン 2 にアップデートするには、Exec モードで **ip ssh version 2** コマンドを入力します。次に例を示します。

```
c3845-1(config)# ip ssh version 2
```

ステップ 3　新しい RSA キーを生成するには、グローバル コンフィギュレーション モードで **crypto key generate rsa** コマンドを入力します。次に例を示します。

```
c3845-1(config)# crypto key generate rsa
The name for the keys will be name.domain.com
Choose the size of the key modulus in the range of 360 to 2048 for your General
Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 768
% Generating 768 bit RSA keys, keys will be non-exportable...[OK]
c3845-1(config)# end
c3845-1# wr
```

この手順を完了すると、設定の変更が実行コンフィギュレーションに反映され、スタートアップ コンフィギュレーションに保存されます。これで、SSH のバージョンの問題による検出の失敗は解消されます。

デバイスがファイアウォールによって保護されている場合の検出の失敗

検出するデバイスがファイアウォールの背後に配置されている場合は、Cisco CP からデバイスへの ping（デバイスにログオンする前に実行するテスト）を実行できないため、検出に失敗することがあります。

検出するデバイスがファイアウォールで保護されており、検出に失敗する場合は、次のいずれかの方法で対処してください。

- ネットワーク内の PC を、ファイアウォールの背後ではない場所に移動する。
- Cisco CP を実行する PC にネットワーク内の現在位置からのアクセスを許可するように、ファイアウォールの設定を修正する。
- Cisco IOS を使用してこのデバイスを管理する。

Cisco CP による既存のクレデンシャルの上書き

デバイスをコミュニティに追加するときに、デフォルトのユーザ名 cisco とパスワード cisco を入力した場合は、セキュリティの問題を回避するために新しいクレデンシャルの作成が必要であることを通知するメッセージが表示されます。指定した新しいクレデンシャルを使用して管理用ユーザが作成され、権限レベル 15 が与えられます。入力したクレデンシャルが設定済みのものである場合は、Cisco CP によってそのクレデンシャルが上書きされ、デバイス検出時に権限レベル 15 が与えられます。既存のユーザ アカウントやデフォルトのクレデンシャル cisco/cisco が上書きされるのを避けたい場合は、Cisco CP によるログインに使用するクレデンシャルとして別のものを入力してください。