

Cisco Sx220シリーズスマートスイッチでの802.1Xポート認証の設定

目的

この記事の目的は、Sx220シリーズスマートスイッチでポート認証を設定する方法を示すことです。

802.1Xポート認証を使用すると、デバイスの各ポートに802.1Xパラメータを設定できます。認証を要求するポートはサブリカントと呼ばれます。オーセンティケータは、サブリカントに対してネットワークガードとして機能するスイッチまたはアクセスポイントです。オーセンティケータは認証メッセージをRADIUSサーバに転送して、ポートの認証と情報の送受信を可能にします。

適用可能なデバイス

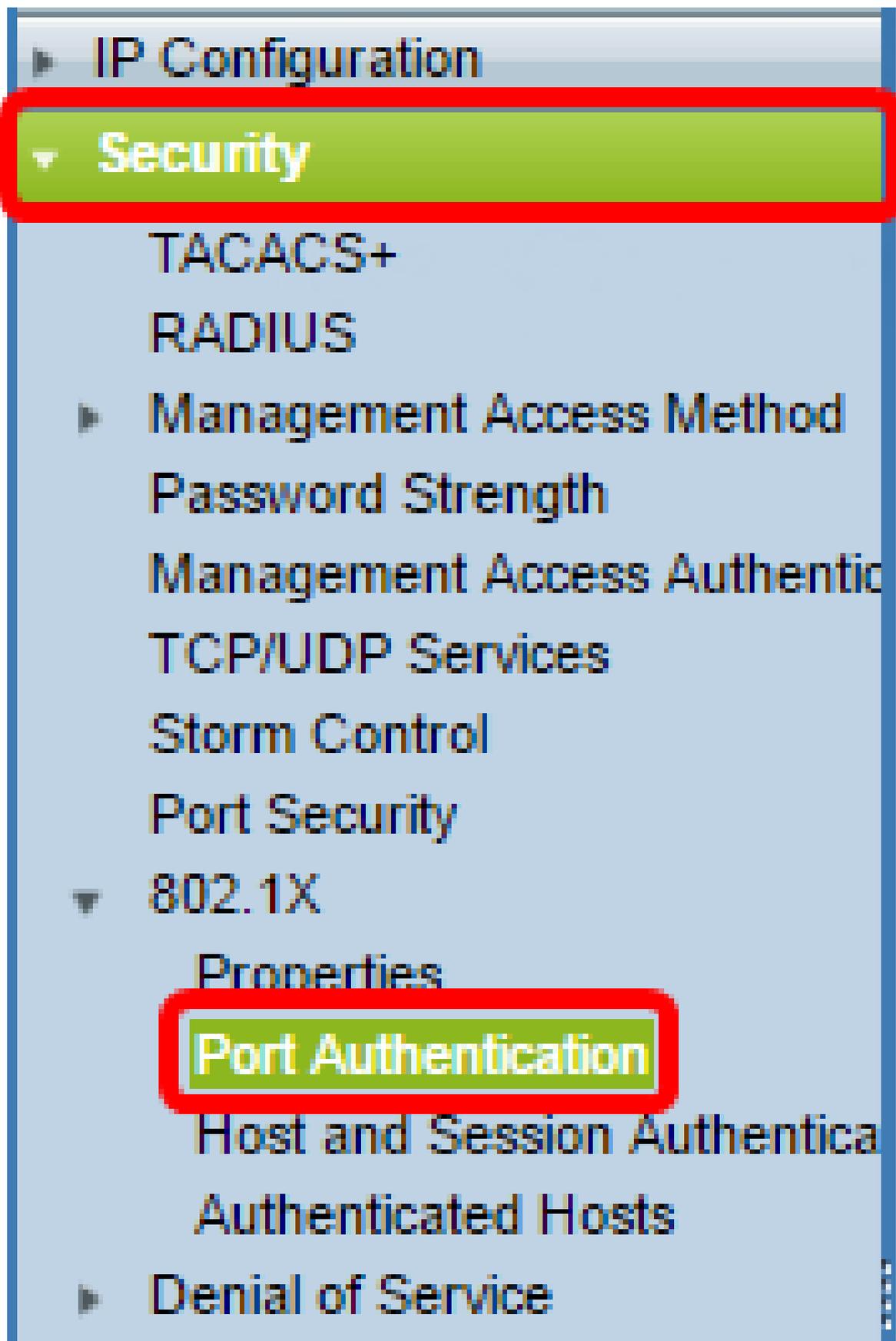
- Sx220シリーズ

[Software Version]

- 1.1.0.14

ポート認証の設定

ステップ 1：スイッチのWebベースユーティリティにログインし、Security > 802.1X > Port Authenticationの順に選択します。



ステップ 2 : 設定するポートのオプションボタンをクリックし、Editをクリックします。

<input type="radio"/>	3	GE3	N/A	Disabled	Disabled	Disabled	Enabled
<input checked="" type="radio"/>	4	GE4	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	5	GE5	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	6	GE6	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	7	GE7	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	8	GE8	N/A	Auto	Disabled	Enabled	Enabled
<input type="radio"/>	9	GE9	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	10	GE10	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	11	GE11	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	12	GE12	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	13	GE13	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	14	GE14	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	15	GE15	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	16	GE16	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	17	GE17	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	18	GE18	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	19	GE19	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	20	GE20	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	21	GE21	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	22	GE22	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	23	GE23	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	24	GE24	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	25	GE25	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	26	GE26	N/A	Disabled	Disabled	Disabled	Enabled

Copy Settings... Edit...

注：この例では、ポートGE4が選択されています。

ステップ 3：Edit Port Authenticationウィンドウが表示されます。Interfaceドロップダウンリストから、指定したポートが手順2で選択したポートであることを確認します。それ以外の場合は、ドロップダウン矢印をクリックして適切なポートを選択します。

Interface:

Port GE4 ▼

Administrative Port Control:

- Disabled
- Force Unauthorized
- Auto
- Force Authorized

RADIUS VLAN Assignment:

- Disabled
- Reject
- Static

Guest VLAN:

- Enable

ステップ 4 : Administrative Port Controlのオプションボタンを選択します。これにより、ポートの許可状態が決まります。次のオプションがあります。

- Disabled:802.1Xを無効にします。これはデフォルトの状態です。
- Force Unauthorized : インターフェイスを無許可の状態に移行することで、インターフェイスへのアクセスを拒否します。スイッチは、インターフェイスを介してクライアントに認証サービスを提供しません。
- Auto : スイッチでポートベースの認証と認可を有効にします。インターフェイスは、スイッチとクライアント間の認証交換に基づいて、許可または不正な状態の間を移動します。
- Force Authorized : 認証なしでインターフェイスを許可します。

Interface:

Port GE4 ▼

Administrative Port Control:

- Disabled
- Force Unauthorized
- Auto
- Force Authorized

RADIUS VLAN Assignment:

- Disabled
- Reject
- Static

Guest VLAN:

- Enable

注：この例では、Autoが選択されています。

ステップ5: (オプション) RADIUS VLAN割り当てのオプションボタンを選択します。これにより、指定したポートでダイナミックVLAN割り当てが有効になります。次のオプションがあります。

- Disabled: VLAN許可結果を無視し、ホストの元のVLANを保持します。これはデフォルトのアクションです。
- Reject : 指定されたポートがVLANで許可された情報を受信した場合、その情報を使用します。ただし、VLANで許可された情報がない場合、ホストは拒否され、許可されません。
- Static : 指定されたポートがVLANで許可された情報を受信すると、その情報が使用されます。ただし、VLANで許可された情報がない場合は、ホストの元のVLANが保持されます。

注: RADIUSからのVLAN認証情報があるが、VLANがDevice Under Test(DUT)で管理上作成されていない場合、VLANは自動的に作成されます。この例では、Staticが選択されています。

Interface:	Port	GE4 ▼
Administrative Port Control:	<input type="radio"/>	Disabled
	<input type="radio"/>	Force Unauthorized
	<input checked="" type="radio"/>	Auto
	<input type="radio"/>	Force Authorized
RADIUS VLAN Assignment:	<input type="radio"/>	Disabled
	<input type="radio"/>	Reject
	<input checked="" type="radio"/>	Static
Guest VLAN:	<input type="checkbox"/>	Enable

ヒント: ダイナミックVLAN割り当て機能を動作させるには、スイッチでRADIUSサーバから次のVLAN属性を送信する必要があります。

- [64] Tunnel-Type = VLAN (タイプ13)
- [65] Tunnel-Medium-Type = 802 (タイプ6)
- [81] Tunnel-Private-Group-Id = VLAN ID

ステップ6: (オプション) 不正なポートにゲストVLANを使用するには、ゲストVLANのEnableチェックボックスにチェックマークを入れます。

Interface:	Port	GE4 ▼
Administrative Port Control:	<input type="radio"/> Disabled	<input type="radio"/> Force Unauthorized
	<input checked="" type="radio"/> Auto	<input type="radio"/> Force Authorized
RADIUS VLAN Assignment:	<input type="radio"/> Disabled	<input type="radio"/> Reject
	<input checked="" type="radio"/> Static	
Guest VLAN:	<input checked="" type="checkbox"/> Enable	

手順 7 : Periodic ReauthenticationのEnableチェックボックスにチェックマークを入れます。これにより、指定された再認証期間の後にポートの再認証の試行が有効になります。

Interface:	Port	GE4 ▼
Administrative Port Control:	<input type="radio"/> Disabled	<input type="radio"/> Force Unauthorized
	<input checked="" type="radio"/> Auto	<input type="radio"/> Force Authorized
RADIUS VLAN Assignment:	<input type="radio"/> Disabled	<input type="radio"/> Reject
	<input checked="" type="radio"/> Static	
Guest VLAN:	<input checked="" type="checkbox"/> Enable	
Periodic Reauthentication:	<input checked="" type="checkbox"/> Enable	

注 : この機能はデフォルトで有効になっています。

ステップ 8 : Reauthentication Periodフィールドに値を入力します。これは、ポートを再認証する時間 (秒) です。

Interface:	Port	GE4 ▼
Administrative Port Control:	<input type="radio"/>	Disabled
	<input type="radio"/>	Force Unauthorized
	<input checked="" type="radio"/>	Auto
	<input type="radio"/>	Force Authorized
RADIUS VLAN Assignment:	<input type="radio"/>	Disabled
	<input type="radio"/>	Reject
	<input checked="" type="radio"/>	Static
Guest VLAN:	<input checked="" type="checkbox"/>	Enable
Periodic Reauthentication:	<input checked="" type="checkbox"/>	Enable
Reauthentication Period:	<input type="text" value="3600"/>	
Reauthenticate Now:	<input type="checkbox"/>	

注：この例では、デフォルト値の3600が使用されています。

ステップ9: (オプション) Reauthenticate Nowチェックボックスをオンにして、即時のポート再認証を有効にします。

注:Authenticator Stateフィールドには、認証の現在の状態が表示されます。

Interface:	Port	GE4 ▼
Administrative Port Control:	<input type="radio"/> Disabled	<input type="radio"/> Force Unauthorized
	<input checked="" type="radio"/> Auto	<input type="radio"/> Force Authorized
RADIUS VLAN Assignment:	<input type="radio"/> Disabled	<input type="radio"/> Reject
	<input checked="" type="radio"/> Static	
Guest VLAN:	<input checked="" type="checkbox"/> Enable	
Periodic Reauthentication:	<input checked="" type="checkbox"/> Enable	
⚙️ Reauthentication Period:	<input type="text" value="3600"/>	
Reauthenticate Now:	<input checked="" type="checkbox"/>	
Authenticator State:	N/A	

注：ポートがForce AuthorizedまたはForce Unauthorized状態でない場合は、Autoモードであり、認証者は進行中の認証の状態を表示します。ポートが認証されると、状態はAuthenticatedと表示されます。

ステップ 10：Max Hostsフィールドに、特定のポートで許可される認証済みホストの最大数を入力します。この値は、マルチセッションモードでのみ有効です。

Interface:	Port	GE4 ▼
Administrative Port Control:	<input type="radio"/> Disabled	<input type="radio"/> Force Unauthorized
	<input checked="" type="radio"/> Auto	<input type="radio"/> Force Authorized
RADIUS VLAN Assignment:	<input type="radio"/> Disabled	<input type="radio"/> Reject
	<input checked="" type="radio"/> Static	
Guest VLAN:	<input checked="" type="checkbox"/> Enable	
Periodic Reauthentication:	<input checked="" type="checkbox"/> Enable	
⚙️ Reauthentication Period:	<input type="text" value="3600"/>	
Reauthenticate Now:	<input checked="" type="checkbox"/>	
Authenticator State:	N/A	
⚙️ Max Hosts:	<input type="text" value="256"/>	

注：この例では、デフォルト値の256が使用されています。

ステップ 11 Quiet Periodフィールドには、認証の交換に失敗した後にスイッチがクワイエット状態を維持する秒数を入力します。スイッチがQuiet状態の場合は、スイッチがクライアントからの新しい認証要求をリッスンしていないことを意味します。

⚙️ Reauthentication Period:	<input type="text" value="3600"/>
Reauthenticate Now:	<input checked="" type="checkbox"/>
Authenticator State:	N/A
⚙️ Max Hosts:	<input type="text" value="256"/>
⚙️ Quiet Period:	<input type="text" value="60"/>

注：この例では、デフォルト値の60が使用されています。

ステップ 12 Resending EAPフィールドに、スイッチが要求を再送信する前にサブリカント（クライアント）からの拡張認証プロトコル(EAP)要求またはアイデンティティフレームへの応答を待機する秒数を入力します。

⚙️ Reauthentication Period:	<input type="text" value="3600"/>
Reauthenticate Now:	<input checked="" type="checkbox"/>
Authenticator State:	N/A
⚙️ Max Hosts:	<input type="text" value="256"/>
⚙️ Quiet Period:	<input type="text" value="60"/>
⚙️ Resending EAP:	<input type="text" value="30"/>

注：この例では、デフォルト値の30が使用されます。

ステップ 13 Max EAP Requestsフィールドに、送信できるEAP要求の最大数を入力します。定義された期間（サブリカントタイムアウト）後に応答が受信されない場合、認証プロセスが再起動されます。

⚙️ Reauthentication Period:	<input type="text" value="3600"/>
Reauthenticate Now:	<input checked="" type="checkbox"/>
Authenticator State:	N/A
⚙️ Max Hosts:	<input type="text" value="256"/>
⚙️ Quiet Period:	<input type="text" value="60"/>
⚙️ Resending EAP:	<input type="text" value="30"/>
⚙️ Max EAP Requests:	<input type="text" value="2"/>

注：この例では、デフォルト値の2が使用されます。

ステップ 14： Supplicant Timeoutフィールドに、EAP要求がサブリカントに再送信されるまでの経過時間を秒数で入力します。

⚙️ Max Hosts:	<input type="text" value="256"/>
⚙️ Quiet Period:	<input type="text" value="60"/>
⚙️ Resending EAP:	<input type="text" value="30"/>
⚙️ Max EAP Requests:	<input type="text" value="2"/>
⚙️ Supplicant Timeout:	<input type="text" value="30"/>

注：この例では、デフォルト値の30が使用されます。

ステップ 15： Server Timeoutフィールドに、スイッチが認証サーバに要求を再送信するまでの経過時間を秒数で入力します。

⚙ Max Hosts:	<input type="text" value="256"/>
⚙ Quiet Period:	<input type="text" value="60"/>
⚙ Resending EAP:	<input type="text" value="30"/>
⚙ Max EAP Requests:	<input type="text" value="2"/>
⚙ Supplicant Timeout:	<input type="text" value="30"/>
⚙ Server Timeout:	<input type="text" value="30"/>

注：この例では、デフォルト値の30が使用されます。

ステップ 16：[APPLY] をクリックします。

これで、スイッチのポート認証が正常に設定されました。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。