

# スイッチでのMACベース認証の設定

## 目的

802.1Xは、リストデバイスを許可し、ネットワークへの不正アクセスを防止するための管理ツールです。このドキュメントでは、グラフィカルユーザインターフェイス(GUI)を使用してスイッチにMACベースの認証を設定する方法を説明します。コマンドラインインターフェイス(CLI)を使用してMACベースの認証を設定する方法については、[ここをクリックしてください](#)。

注：このガイドは、ホストが認証されたことを確認するために、9つのセクションと1のセクションで長い時間を費やします。コーヒー、紅茶、または水を手に入れ、必要な手順を確認して実行するのに十分な時間があることを確認します。

[詳細については、用語集を参照してください。](#)

## RADIUS はどのように動作しますか。

802.1X認証には、サブリカント（クライアント）、オーセンティケータ（スイッチなどのネットワークデバイス）、および認証サーバ(RADIUS)の3つの主要コンポーネントがあります。

Remote Authentication Dial-In User Service(RADIUS)は、ネットワークアクセスの管理に役立つ認証、許可、アカウントिंग(AAA)プロトコルを使用するアクセスサーバです。RADIUSは、RADIUSサーバと1つ以上のRADIUSクライアント間でセキュアな認証情報が交換されるクライアントサーバモデルを使用します。クライアントのIDを検証し、クライアントがLANへのアクセスを許可されているかどうかをスイッチに通知します。

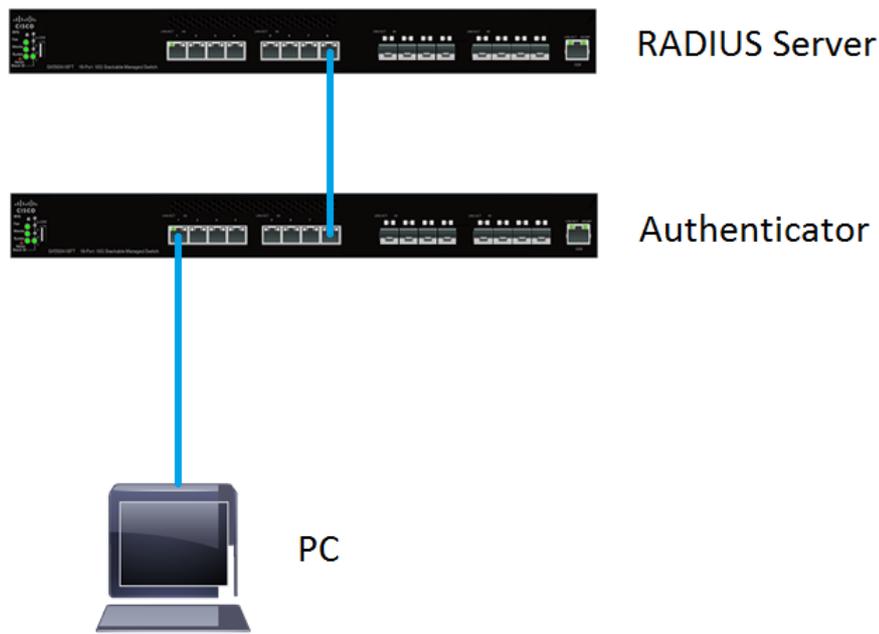
オーセンティケータは、クライアントと認証サーバの間で動作します。まず、クライアントからID情報を要求します。応答として、オーセンティケータは認証サーバで情報を確認します。最後に、クライアントに応答をリレーします。この記事では、オーセンティケータはRADIUSクライアントを含むスイッチです。スイッチは、Extensible Authentication Protocol(EAP)フレームをカプセル化およびカプセル解除して、認証サーバと対話できます。

## MACベース認証について

MACベースの認証では、サブリカントがオーセンティケータと通信する方法を理解していない場合、またはオーセンティケータと通信できない場合は、ホストのMACアドレスを使用して認証します。MACベースのサブリカントは、純粋なRADIUSを使用して（EAPを使用せずに）認証されます。RADIUSサーバには、許可されたMACアドレスだけを含む専用のホストデータベースがあります。MACベースの認証要求をPassword Authentication Protocol(PAP)認証として扱う代わりに、サーバは属性6 [Service-Type] = 10でこのような要求を認識します。これらの要求は、Calling-Station-Id属性のMACアドレスとホストデータベースに格納されているMACアドレスを比較します。

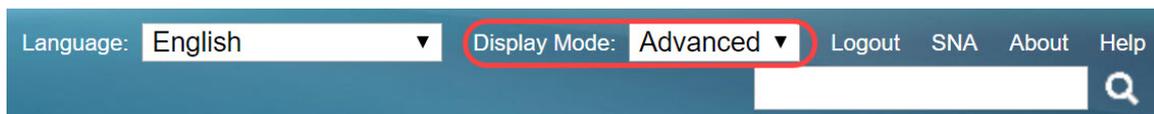
バージョン2.4リリースでは、MACベースのサブリカントに送信され、EAP認証方式または純粋なRADIUSのいずれかを定義するユーザ名の形式を設定する機能が追加されています。このバージョンでは、ユーザ名の形式を設定したり、MACベースのサブリカントに対してユーザ名とは異なる特定のパスワードを設定することもできます。

トポロジ：



注：この記事では、RADIUSサーバとオーセンティケータの両方にSG550X-24を使用します。RADIUSサーバのスタティックIPアドレスは192.168.1.100で、オーセンティケータのスタティックIPアドレスは192.168.1.101です。

このドキュメントの手順は、詳細表示モードで実行されます。モードを詳細モードに変更するには、右上隅の[表示モード(*Display Mode*)]ドロップダウンリストの[詳細(*Advanced*)]を選択します。



## 目次

1. [RADIUSサーバのグローバル設定](#)
2. [RADIUSサーバキー](#)
3. [RADIUSサーバグループ](#)
4. [RADIUSサーバユーザ](#)
5. [RADIUSクライアント](#)
6. [802.1X認証プロパティ](#)
7. [802.1X認証MACベースの認証設定](#)
8. [802.1X認証ホストおよびセッション認証](#)
9. [802.1X認証ポート認証](#)
10. [結論](#)

## 該当するデバイス

- Sx350Xシリーズ

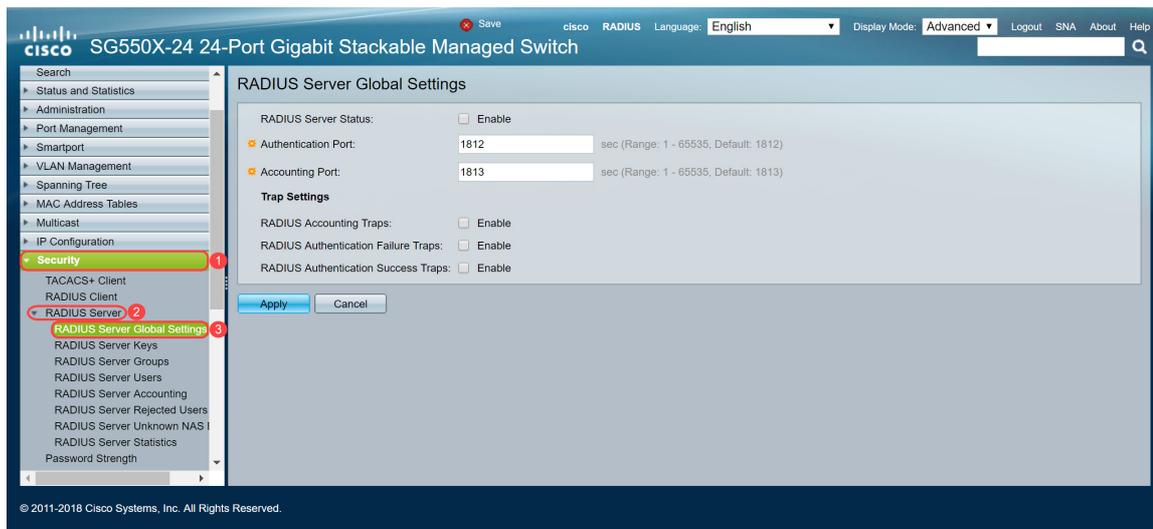
- SG350XGシリーズ
- Sx550Xシリーズ
- SG550XGシリーズ

## [Software Version]

- 2.4.0.94

## RADIUSサーバのグローバル設定

ステップ1:RADIUSサーバとして設定するスイッチのWebベースユーティリティにログインし、[Security] > [RADIUS Server] > [RADIUS Server Global Settings]に移動します。



ステップ2:RADIUSサーバ機能のステータスを有効にするには、[RADIUS Server Status]フィールドの[Enable]チェックボックスをオンにします。



ステップ3:RADIUSアカウントイベント、失敗したログイン、成功したログインに対してトラップを生成するには、目的の[Enable]チェックボックスをオンにしてトラップを生成します。トラップは、Simple Network Management Protocol (SNMP ; 簡易ネットワーク管理プロトコル) によって生成されるシステムイベントメッセージです。違反が発生すると、トラップがスイッチのSNMPマネージャに送信されます。次のトラップ設定は次のとおりです。

- [RADIUS Accounting Traps]:RADIUSアカウントイベントのトラップを生成する場合にオンにします。

- [RADIUS Authentication Failure Traps] : 失敗したログインのトラップを生成するには、このチェックボックスをオンにします。
- [RADIUS Authentication Success Traps] : 成功したログインのトラップを生成するには、このチェックボックスをオンにします。

RADIUS Server Global Settings

RADIUS Server Status:  Enable

Authentication Port:  sec (Range: 1 - 65535, Default: 1812)

Accounting Port:  sec (Range: 1 - 65535, Default: 1813)

**Trap Settings**

RADIUS Accounting Traps:  Enable

RADIUS Authentication Failure Traps:  Enable

RADIUS Authentication Success Traps:  Enable

ステップ4:[Apply]をクリックして設定を保存します。

## RADIUSサーバキー

ステップ1:[Security] > [RADIUS Server] > [RADIUS Server Keys]に移動します。 [RADIUS Server Key]ページが開きます。

cisco RADIUS Language: English Display Mode: Advanced Logout SNA About Help

SG550X-24 24-Port Gigabit Stackable Managed Switch

MAC Address Tables

Multicast

IP Configuration

Security 1

TACACS+ Client

RADIUS Client

RADIUS Server 2

RADIUS Server Global Settings

RADIUS Server Keys 3

RADIUS Server Groups

RADIUS Server Users

RADIUS Server Accounts

RADIUS Server Rejected

RADIUS Server Unknown

RADIUS Server Statistics

Password Strength

Key Management

Mgmt Access Method

Management Access Authentication

Secure Sensitive Data Management

SSL Server

SSH Server

SSH Client

TCP/UDP Services

RADIUS Server Keys

Default Key:  Keep existing default key  
 Encrypted   
 Plaintext  (0/128 characters used)

MD5 Digest:

Secret Key Table

NAS Address	Secret Key's MD5
0 results found.	

© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

ステップ2:[Secret Key Table]セクションで、[Add...]をクリックします。 秘密キーを追加します。

## RADIUS Server Keys

Default Key:  Keep existing default key

Encrypted

Plaintext

(0/128 characters used)

MD5 Digest:

Apply

Cancel

### Secret Key Table

<input type="checkbox"/>	NAS Address	Secret Key's MD5
--------------------------	-------------	------------------

0 results found.

Add...

Edit...

Delete

ステップ3:[秘密キーの追加(Add Secret Key)]ウィンドウが開きます。[NAS Address]フィールドに、RADIUSクライアントを含むスイッチのアドレスを入力します。この例では、IPアドレス192.168.1.101をRADIUSクライアントとして使用します。

★ NAS Address: 192.168.1.101 (IPv4 or IPv6 Address)

Secret Key:  Use default key

Encrypted

Plaintext

(0/128 characters used)

Apply

Close

ステップ4：秘密キーとして使用するオプションボタンを1つ選択します。次のオプションがあります。

- Use default key：指定されたサーバでは、デバイスは既存のデフォルトのキー文字列を使用してRADIUSクライアントの認証を試みます。
- [暗号化(Encrypted)]:Message-Digest Algorithm 5(MD5)を使用して通信を暗号化するには、暗号化された形式でキーを入力します。
- 「プレーンテキスト」 - プレーンテキストモードでキー文字列を入力します。

この例では、[Plaintext]を選択し、[Secret Key]に[example]という語を使用します。[apply]を押すと、キーは暗号化された形式になります。

注：秘密キーとしてexampleという単語を使用することはお勧めしません。もっと強い鍵を使ってください。最大128文字を使用できます。パスワードが複雑すぎて覚えにくい場合は、パスワードは良いパスワードですが、パスワードを暗記可能なパスフレーズに変え、母音を置き換える特殊文字や数字を使う方が良いでしょう。辞書に載っている単語を使わないのが一番です。フレーズを選択し、特殊文字や数字の一部の文字を入れ替えることをお勧めします。詳細については、このシスコの[ブログ](#)記事を参照してください。

\* NAS Address:  (IPv4 or IPv6 Address)

Secret Key:
   
 Use default key
   
 Encrypted 
  
 Plaintext  (128 characters used)

ステップ5:[Apply]をクリックして設定を保存します。秘密キーはMD5で暗号化されます。MD5は、データを取得し、通常は再生可能ではない一意の16進数出力を作成する暗号化ハッシュ関数です。MD5は128ビットハッシュ値を使用します。

### RADIUS Server Keys

Default Key:
   
 Keep existing default key
   
 Encrypted 
  
 Plaintext  (0/128 characters used)

MD5 Digest:

#### Secret Key Table

<input type="checkbox"/>	NAS Address	Secret Key's MD5
<input type="checkbox"/>	192.168.1.101	1a79a4d60de6718e8e5b3226e338ae533

## RADIUSサーバグループ

ステップ1:[Security] > [RADIUS Server] > [RADIUS Server Groups]に移動します。

The screenshot shows the Cisco configuration interface for a SG550X-24 switch. The left-hand navigation pane is expanded to show the 'Security' section, with 'RADIUS Server' and 'RADIUS Server Groups' highlighted. The main configuration area displays the 'RADIUS Server Groups' configuration page, which currently shows '0 results found' and buttons for 'Add...', 'Edit...', and 'Delete'.

ステップ2:[Add...]をクリックします。新しいRADIUSサーバグループを追加します。

# RADIUS Server Groups

## RADIUS Server Group table

<input type="checkbox"/>	Group Name	Privilege Level	Time Range		VLAN ID	VLAN Name
			Name	State		
0 results found.						
<input type="button" value="Add..."/> <input type="button" value="Edit..."/> <input type="button" value="Delete"/>						

ステップ3:[Add RADIUS Server Group]ページが開きます。グループの名前を入力します。この例では、グループ名としてMAC802を使用します。

✱ Group Name:  (6/32 characters used)

✱ Privilege Level:  (Range: 1 - 15, Default: 1)

Time Range:  Enable

Time Range Name:

VLAN:  None

VLAN ID  (Range: 1 - 4094)

VLAN Name  (0/32 characters used)

ステップ4:[Privilege Level]フィールドにグループの管理アクセス特権レベルを入力します。範囲は1 ~ 15、15が最も特権で、デフォルト値は1です。この例では、特権レベルは1のままにします。

注：この記事では、時間範囲やVLANを設定しません。

✱ Group Name:  (6/32 characters used)

✱ Privilege Level:  (Range: 1 - 15, Default: 1)

Time Range:  Enable

Time Range Name:

VLAN:  None

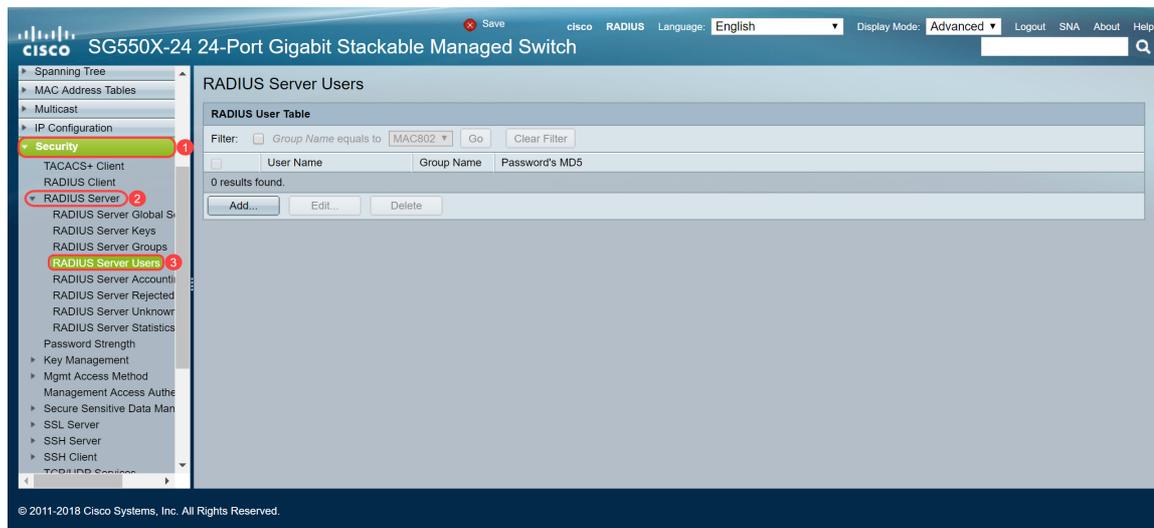
VLAN ID  (Range: 1 - 4094)

VLAN Name  (0/32 characters used)

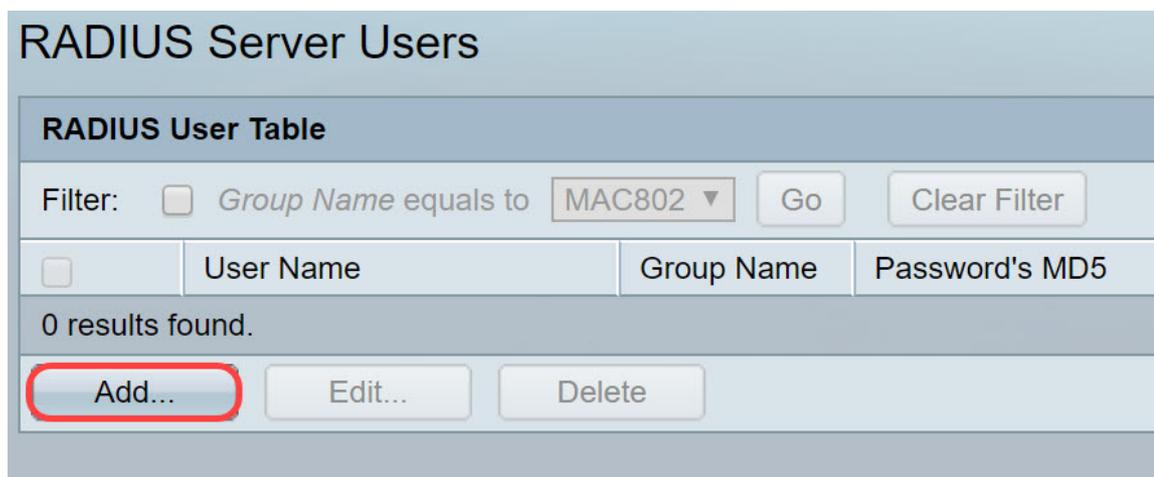
ステップ5:[Apply]をクリックして設定を保存します。

# RADIUSサーバユーザ

ステップ1:[Security] > [RADIUS Server] > [RADIUS Server Users]に移動し、RADIUSのユーザーを設定します。



ステップ2:[Add...]をクリックします。新しいユーザを追加します。



ステップ3:[Add RADIUS Server User]ページが開きます。[User Name]フィールドに、ユーザのMACアドレスを入力します。この例では、コンピュータのイーサネットMACアドレスを使用します。

注：MACアドレスの一部がぼやけている。

User Name: 54:EE:75: (17/32 characters used)

Group Name: MAC802 ▼

Password:  Encrypted   
 Plaintext (0/32 characters used)

Apply Close

ステップ4:[グループ名]ドロップダウンリストでグループを選択します。「[RADIUS Server Group](#)」[セクション](#)の[ステップ3](#)で強調した通り、このユーザのグループ名として**MAC802**を選択します

User Name: 54:EE:75: (17/32 characters used)

Group Name: MAC802 ▼

Password:  Encrypted   
 Plaintext (0/32 characters used)

Apply Close

ステップ5：次のいずれかのオプションボタンを選択します。

- 暗号化：MD5を使用して通信を暗号化するためにキーが使用されます。暗号化を使用するには、暗号化された形式でキーを入力します。
- プレーンテキスト：暗号化されたキー文字列（別のデバイスから）がない場合は、プレーンテキストモードでキー文字列を入力します。暗号化されたキー文字列が生成され、表示されます。

このユーザのパスワードとしてPlaintextを選択し、プレーンテキストのパスワードとして**example**を入力します。

注：プレーンテキストのパスワードとしてexampleを使用することはお勧めしません。より強力なパスワードを使用することをお勧めします。

User Name: 54:EE:75: (17/32 characters used)

Group Name: MAC802 ▼

Password:  Encrypted  Plaintext example (2/32 characters used)

Apply Close

ステップ6：設定が完了したら、[Apply]をクリックします。

これで、RADIUSサーバの設定が完了しました。次のセクションでは、2番目のスイッチをオーセンティケータとして設定します。

## RADIUSクライアント

ステップ1：オーセンティケータとして設定するスイッチのWebベースのユーティリティにログインし、[Security] > [RADIUS Client]に移動します。

SG550X-24 24-Port Gigabit Stackable Managed Switch

RADIUS Client

RADIUS Accounting for Management Access can only be enabled when TACACS+ Accounting is disabled. TACACS+ Accounting is currently Disabled.

RADIUS Accounting:  Port Based Access Control (802.1X, MAC Based, Web Authentication)  Management Access  Both Port Based Access Control and Management Access  None

Use Default Parameters

Retries: 3 (Range: 1 - 15, Default: 3)

Timeout for Reply: 3 sec (Range: 1 - 30, Default: 3)

Dead Time: 0 min (Range: 0 - 2000, Default: 0)

Key String:  Encrypted  Plaintext (0/128 characters used)

Source IPv4 Interface: Auto

Source IPv6 Interface: Auto

Apply Cancel

ステップ2:[RADIUS Table]セクションまで下にスクロールし、[Add...]をクリックします。RADIUSサーバを追加します。

**Use Default Parameters**

Retries:  (Range: 1 - 15, Default: 3)

Timeout for Reply:  sec (Range: 1 - 30, Default: 3)

Dead Time:  min (Range: 0 - 2000, Default: 0)

Key String:  Encrypted   
 Plaintext  (0/128 characters used)

Source IPv4 Interface: Auto ▼

Source IPv6 Interface: Auto ▼

**RADIUS Table**

<input type="checkbox"/>	Server	Priority	Key String (Encrypted)	Timeout for Reply	Authentication Port	Accounting Port	Retries	Dead Time	Usage Type
0 results found.									

An \* indicates that the parameter is using the default global value.

ステップ3: ( オプション ) [Server Definition]フィールドで、RADIUSサーバをIPアドレスまたは名前で指定するかどうかを選択します。この例では、[By IP address]のデフォルトの選択を維持します。

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1 ▼

Server IP Address/Name:

Priority:  (Range: 0 - 65535)

Key String:  Use Default  
 User Defined (Encrypted)   
 User Defined (Plaintext)  (0/128 characters used)

Timeout for Reply:  Use Default  
 User Defined  sec (Range: 1 - 30, Default: 3)

Authentication Port:  (Range: 0 - 65535, Default: 1812)

Accounting Port:  (Range: 0 - 65535, Default: 1813)

Retries:  Use Default  
 User Defined  (Range: 1 - 15, Default: 3)

Dead Time:  Use Default  
 User Defined  min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  
 802.1x  
 All

ステップ4: ( オプション ) [IP Version]フィールドで、RADIUSサーバのIPアドレスのバージョンを選択します。この例では、バージョン4のデフォルトの選択を維持します。

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1 ▼

Server IP Address/Name:

Priority:  (Range: 0 - 65535)

Key String:  Use Default  
 User Defined (Encrypted)   
 User Defined (Plaintext)  (0/128 characters used)

Timeout for Reply:  Use Default  
 User Defined  sec (Range: 1 - 30, Default: 3)

Authentication Port:  (Range: 0 - 65535, Default: 1812)

Accounting Port:  (Range: 0 - 65535, Default: 1813)

Retries:  Use Default  
 User Defined  (Range: 1 - 15, Default: 3)

Dead Time:  Use Default  
 User Defined  min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  
 802.1x  
 All

ステップ5: RADIUSサーバでIPアドレスまたは名前を入力します。[Server IP Address/Name]フィールドに192.168.1.100のIPアドレスを入力します。

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.100

Priority:  (Range: 0 - 65535)

Key String:  Use Default  User Defined (Encrypted)   User Defined (Plaintext)  (0/128 characters used)

Timeout for Reply:  Use Default  User Defined Default  sec (Range: 1 - 30, Default: 3)

Authentication Port: 1812 (Range: 0 - 65535, Default: 1812)

Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

Retries:  Use Default  User Defined Default  (Range: 1 - 15, Default: 3)

Dead Time:  Use Default  User Defined Default  min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  802.1x  All

Apply Close

ステップ6：サーバの優先度を入力します。優先順位によって、デバイスがユーザを認証するためにサーバに接続する順序が決まります。デバイスは、最初に最も優先度の高いRADIUSサーバから開始します。ゼロが最も高い優先順位です。

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.100

Priority: 0 (Range: 0 - 65535)

Key String:  Use Default  User Defined (Encrypted)   User Defined (Plaintext)  (0/128 characters used)

Timeout for Reply:  Use Default  User Defined Default  sec (Range: 1 - 30, Default: 3)

Authentication Port: 1812 (Range: 0 - 65535, Default: 1812)

Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

Retries:  Use Default  User Defined Default  (Range: 1 - 15, Default: 3)

Dead Time:  Use Default  User Defined Default  min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  802.1x  All

Apply Close

ステップ7：デバイスとRADIUSサーバ間の通信の認証および暗号化に使用するキー文字列を入力します。このキーは、RADIUSサーバで設定されているキーと一致している必要があります。暗号化またはプレーンテキスト形式で入力できます。[Use Default]が選択されている場合、デバイスはデフォルトのキー文字列を使用してRADIUSサーバへの認証を試みます。ここでは、ユーザ定義(Plaintext)を使用し、キーの例を入力します。

注：残りの設定はデフォルトのままにします。必要に応じて設定できます。

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.100

Priority: 0 (Range: 0 - 65535)

Key String:  Use Default  
 User Defined (Encrypted)   
 User Defined (Plaintext) example (7/128 characters used)

Timeout for Reply:  Use Default  
 User Defined Default sec (Range: 1 - 30, Default: 3)

Authentication Port: 1812 (Range: 0 - 65535, Default: 1812)

Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

Retries:  Use Default  
 User Defined Default (Range: 1 - 15, Default: 3)

Dead Time:  Use Default  
 User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  
 802.1x  
 All

Apply Close

ステップ8:[Apply]をクリックして、設定を保存します。

## 802.1X認証プロパティ

[Properties]ページは、ポート/デバイス認証をグローバルに有効にするために使用します。認証を機能させるには、各ポートでグローバルおよび個別にアクティブにする必要があります。

ステップ1:[Security] > [802.1X Authentication] > [Properties]に移動します。

The screenshot shows the Cisco configuration interface for a switch. The left sidebar has 'Security' expanded, and '802.1X Authentication' is selected. The main panel shows the 'Properties' page for 802.1X Authentication. The 'Port-Based Authentication' checkbox is checked. The 'Authentication Method' is set to 'RADIUS'. The 'Guest VLAN' is set to '1'. The 'Guest VLAN Timeout' is set to 'Immediate'. The 'Trap Settings' section has several checkboxes for enabling failure and success traps for 802.1X, MAC, and Web authentication.

ステップ2:[Enable] チェックボックスをオンにして、ポートベース認証を有効にします。

## Properties

Port-Based Authentication:	<input checked="" type="checkbox"/> Enable
Authentication Method:	<input type="radio"/> RADIUS, None <input checked="" type="radio"/> RADIUS <input type="radio"/> None
Guest VLAN:	<input type="checkbox"/> Enable
Guest VLAN ID:	1 ▾
✱ Guest VLAN Timeout:	<input checked="" type="radio"/> Immediate <input type="radio"/> User Defined <input type="text"/> sec (Range: 30 - 180)
<b>Trap Settings</b>	
802.1x Authentication Failure Traps:	<input type="checkbox"/> Enable
802.1x Authentication Success Traps:	<input type="checkbox"/> Enable
MAC Authentication Failure Traps:	<input type="checkbox"/> Enable
MAC Authentication Success Traps:	<input type="checkbox"/> Enable
Supplicant Authentication Failure Traps:	<input type="checkbox"/> Enable
Supplicant Authentication Success Traps:	<input type="checkbox"/> Enable
Web Authentication Failure Traps:	<input type="checkbox"/> Enable
Web Authentication Success Traps:	<input type="checkbox"/> Enable
Web Authentication Quiet Traps:	<input type="checkbox"/> Enable

ステップ3：ユーザ認証方法を選択します。認証方式としてRADIUSを選択します。次のオプションがあります。

- RADIUS, None: RADIUSサーバを使用して、最初にポート認証を実行します。RADIUSから応答が受信されない場合（サーバがダウンしている場合など）、認証は実行されず、セッションは許可されます。サーバは使用可能であるが、ユーザのクレデンシャルが正しくない場合、アクセスは拒否され、セッションは終了します。
- RADIUS: RADIUSサーバでユーザを認証します。認証が実行されない場合、セッションは許可されません。
- [None]：ユーザを認証しません。セッションを許可します。

## Properties

Port-Based Authentication:	<input checked="" type="checkbox"/> Enable
Authentication Method:	<input type="radio"/> RADIUS, None <input checked="" type="radio"/> RADIUS <input type="radio"/> None
Guest VLAN:	<input type="checkbox"/> Enable
Guest VLAN ID:	1 ▾
✦ Guest VLAN Timeout:	<input checked="" type="radio"/> Immediate <input type="radio"/> User Defined <input type="text"/> sec (Range: 30 - 180)
<b>Trap Settings</b>	
802.1x Authentication Failure Traps:	<input type="checkbox"/> Enable
802.1x Authentication Success Traps:	<input type="checkbox"/> Enable
MAC Authentication Failure Traps:	<input type="checkbox"/> Enable
MAC Authentication Success Traps:	<input type="checkbox"/> Enable
Supplicant Authentication Failure Traps:	<input type="checkbox"/> Enable
Supplicant Authentication Success Traps:	<input type="checkbox"/> Enable
Web Authentication Failure Traps:	<input type="checkbox"/> Enable
Web Authentication Success Traps:	<input type="checkbox"/> Enable
Web Authentication Quiet Traps:	<input type="checkbox"/> Enable

ステップ4: ( オプション ) *MAC Authentication Failure Traps*および*MAC Authentication Success Traps*の**Enable**チェックボックスをオンにします。これにより、MAC認証が失敗または成功した場合にトラップが生成されます。この例では、*MAC Authentication Failure Traps*と*MAC Authentication Success Traps*の両方を有効にします。

## Properties

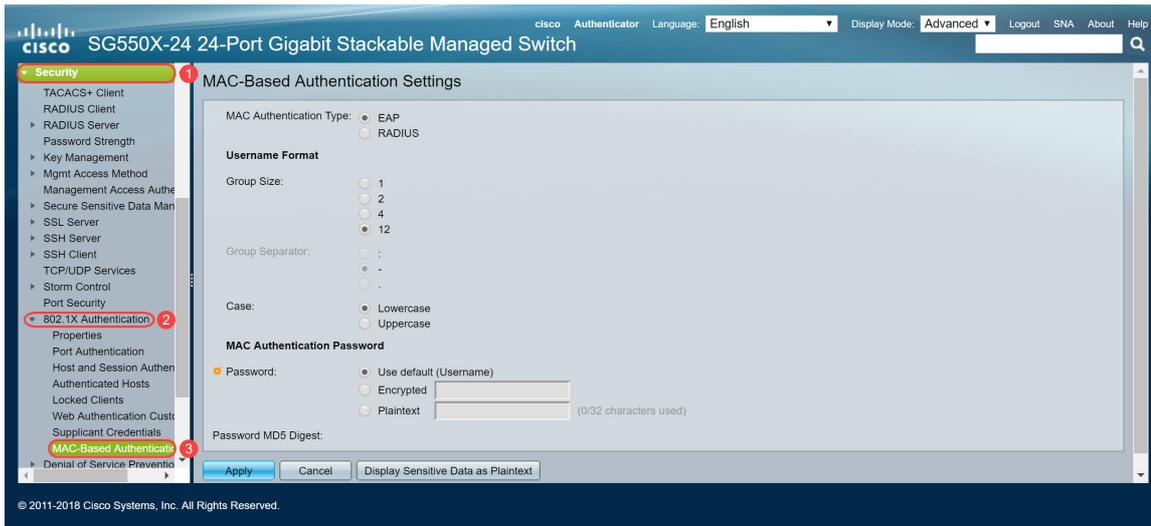
Port-Based Authentication:	<input checked="" type="checkbox"/> Enable
Authentication Method:	<input type="radio"/> RADIUS, None <input checked="" type="radio"/> RADIUS <input type="radio"/> None
Guest VLAN:	<input type="checkbox"/> Enable
Guest VLAN ID:	1 ▾
✦ Guest VLAN Timeout:	<input checked="" type="radio"/> Immediate <input type="radio"/> User Defined <input type="text"/> sec (Range: 30 - 180)
<b>Trap Settings</b>	
802.1x Authentication Failure Traps:	<input type="checkbox"/> Enable
802.1x Authentication Success Traps:	<input type="checkbox"/> Enable
MAC Authentication Failure Traps:	<input checked="" type="checkbox"/> Enable
MAC Authentication Success Traps:	<input checked="" type="checkbox"/> Enable
Supplicant Authentication Failure Traps:	<input type="checkbox"/> Enable
Supplicant Authentication Success Traps:	<input type="checkbox"/> Enable
Web Authentication Failure Traps:	<input type="checkbox"/> Enable
Web Authentication Success Traps:	<input type="checkbox"/> Enable
Web Authentication Quiet Traps:	<input type="checkbox"/> Enable

ステップ5:[Apply]をクリックします。

## 802.1X認証MACベースの認証設定

このページでは、MACベースの認証に適用できるさまざまな設定を設定できます。

ステップ1:[Security] > [802.1X Authentication] > [MAC-Based Authentication Settings]に移動します。



ステップ2:[MAC Authentication Type]で、次のいずれかを選択します。

- EAP : スイッチ ( RADIUSクライアント ) とRADIUSサーバ間のトラフィックにEAPカプセル化されたRADIUSを使用します。RADIUSサーバはMACベースのサブリカントを認証します。
- RADIUS:MACベースのサブリカントを認証するスイッチ ( RADIUSクライアント ) とRADIUSサーバ間のトラフィックに対して、EAPカプセル化なしでRADIUSを使用します。

この例では、MAC認証タイプとしてRADIUSを選択します。

### MAC-Based Authentication Settings

MAC Authentication Type:  EAP  RADIUS

**Username Format**

Group Size:  1  2  4  12

Group Separator:  :  -  .

Case:  Lowercase  Uppercase

**MAC Authentication Password**

✱ Password:  Use default (Username)  Encrypted   (0/32 characters used)  
 Plaintext

Password MD5 Digest:

Apply Cancel Display Sensitive Data as Plaintext

ステップ3:[ユーザ名の形式]で、ユーザ名として送信されるMACアドレスの区切り記号の間の

ASCII文字の数を選択します。この場合、グループサイズとして2を選択します。

注：ユーザ名の形式が、[[Radius Server Users](#)]セクションでMACアドレスを入力する方法と同じであることを確認します。

### MAC-Based Authentication Settings

MAC Authentication Type:  EAP  
 RADIUS

**Username Format**

Group Size:  1  
 2  
 4  
 12

Group Separator:  :  
 -  
 .

Case:  Lowercase  
 Uppercase

**MAC Authentication Password**

✦ Password:  Use default (Username)  
 Encrypted   
 Plaintext  (0/32 characters used)

Password MD5 Digest:

ステップ4:MACアドレスで定義された文字グループ間の区切り文字として使用する文字を選択します。この例では、次の項目を選択します。グループ区切り記号として使用します

## MAC-Based Authentication Settings

MAC Authentication Type:  EAP  
 RADIUS

### Username Format

Group Size:  1  
 2  
 4  
 12

Group Separator:  :  
 -  
 .

Case:  Lowercase  
 Uppercase

### MAC Authentication Password

✱ Password:  Use default (Username)  
 Encrypted   
 Plaintext  (0/32 characters used)

Password MD5 Digest:

Apply

Cancel

Display Sensitive Data as Plaintext

ステップ5:[大文字]フィールドで、[小文]または[大文]を選択し、ユーザー名を小文字または大文字で送信します。

## MAC-Based Authentication Settings

MAC Authentication Type:  EAP  
 RADIUS

**Username Format**

Group Size:  1  
 2  
 4  
 12

Group Separator:  :  
 -  
 .

Case:  Lowercase  
 Uppercase

**MAC Authentication Password**

✱ Password:  Use default (Username)  
 Encrypted   
 Plaintext  (0/32 characters used)

Password MD5 Digest:

ステップ6 : パスワードは、スイッチがRADIUSサーバを介して認証に使用する方法を定義します。次のオプションのいずれかを選択します。

- [デフォルトを使用 ( ユーザ名 ) (Use default (Username))] : 定義されたユーザ名をパスワードとして使用する場合に選択します。
- [Encrypted] : 暗号化された形式でパスワードを定義します。
- プレーンテキスト : プレーンテキスト形式でパスワードを定義します。

## MAC-Based Authentication Settings

MAC Authentication Type:  EAP  
 RADIUS

**Username Format**

Group Size:  1  
 2  
 4  
 12

Group Separator:  :  
 -  
 .

Case:  Lowercase  
 Uppercase

**MAC Authentication Password**

✱ Password:  Use default (Username)  
 Encrypted   
 Plaintext  (7/32 characters used)

Password MD5 Digest:

注：Password Message-Digest Algorithm 5 (MD5) Digestは、MD5ダイジェストパスワードを表示しません。MD5は暗号化ハッシュ関数で、データの一部を取得し、通常は再生可能ではない一意の16進数出力を作成します。MD5は128ビットハッシュ値を使用します。

ステップ7:[Apply]をクリックし、設定が実行コンフィギュレーションファイルに保存されます。

## 802.1X認証ホストおよびセッション認証

[Host and Session Authentication]ページでは、802.1Xがポートで動作するモードと、違反が検出された場合に実行するアクションを定義できます。

ステップ1:[Security] > [802.1X Authentication] > [Host and Session Authentication]に移動します

。

Save Cisco Authenticator Language: English Display Mode: Advanced Logout SNA About Help

**Security** 1 Host and Session Authentication

Host and Session Authentication Table Showing 1-28 of 28 All per page

Filter: Interface Type equals to Port of Unit 1 Go

Entry No.	Port	Host Authentication	Single Host			
			Action on Violation	Traps	Trap Frequency	Number of Violations
<input type="radio"/>	1	GE1	Multiple Host (802.1X)			
<input type="radio"/>	2	GE2	Multiple Host (802.1X)			
<input type="radio"/>	3	GE3	Multiple Host (802.1X)			
<input type="radio"/>	4	GE4	Multiple Host (802.1X)			
<input type="radio"/>	5	GE5	Multiple Host (802.1X)			
<input type="radio"/>	6	GE6	Multiple Host (802.1X)			
<input type="radio"/>	7	GE7	Multiple Host (802.1X)			
<input type="radio"/>	8	GE8	Multiple Host (802.1X)			
<input type="radio"/>	9	GE9	Multiple Host (802.1X)			
<input type="radio"/>	10	GE10	Multiple Host (802.1X)			
<input type="radio"/>	11	GE11	Multiple Host (802.1X)			
<input type="radio"/>	12	GE12	Multiple Host (802.1X)			
<input type="radio"/>	13	GE13	Multiple Host (802.1X)			
<input type="radio"/>	14	GE14	Multiple Host (802.1X)			
<input type="radio"/>	15	GE15	Multiple Host (802.1X)			

© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

ステップ2: ホスト認証を設定するポートを選択します。この例では、GE1をエンドホストに接続するように設定します。

Host and Session Authentication

Host and Session Authentication Table

Filter: Interface Type equals to Port of Unit 1 Go

Entry No.	Port	Host Authentication	Single Host			
			Action on Violation	Traps	Trap Frequency	Number of Violations
<input checked="" type="radio"/>	1	GE1	Multiple Host (802.1X)			
<input type="radio"/>	2	GE2	Multiple Host (802.1X)			
<input type="radio"/>	3	GE3	Multiple Host (802.1X)			
<input type="radio"/>	4	GE4	Multiple Host (802.1X)			
<input type="radio"/>	5	GE5	Multiple Host (802.1X)			
<input type="radio"/>	6	GE6	Multiple Host (802.1X)			
<input type="radio"/>	7	GE7	Multiple Host (802.1X)			
<input type="radio"/>	8	GE8	Multiple Host (802.1X)			
<input type="radio"/>	9	GE9	Multiple Host (802.1X)			
<input type="radio"/>	10	GE10	Multiple Host (802.1X)			
<input type="radio"/>	11	GE11	Multiple Host (802.1X)			
<input type="radio"/>	12	GE12	Multiple Host (802.1X)			
<input type="radio"/>	13	GE13	Multiple Host (802.1X)			
<input type="radio"/>	14	GE14	Multiple Host (802.1X)			

ステップ3:[Edit...]をクリックします。ポートを設定します。

<input type="radio"/>	10	GE10	Multiple Host (802.1X)
<input type="radio"/>	11	GE11	Multiple Host (802.1X)
<input type="radio"/>	12	GE12	Multiple Host (802.1X)
<input type="radio"/>	13	GE13	Multiple Host (802.1X)
<input type="radio"/>	14	GE14	Multiple Host (802.1X)
<input type="radio"/>	15	GE15	Multiple Host (802.1X)
<input type="radio"/>	16	GE16	Multiple Host (802.1X)
<input type="radio"/>	17	GE17	Multiple Host (802.1X)
<input type="radio"/>	18	GE18	Multiple Host (802.1X)
<input type="radio"/>	19	GE19	Multiple Host (802.1X)
<input type="radio"/>	20	GE20	Multiple Host (802.1X)
<input type="radio"/>	21	GE21	Multiple Host (802.1X)
<input type="radio"/>	22	GE22	Multiple Host (802.1X)
<input type="radio"/>	23	GE23	Multiple Host (802.1X)
<input type="radio"/>	24	GE24	Multiple Host (802.1X)
<input type="radio"/>	25	XG1	Multiple Host (802.1X)
<input type="radio"/>	26	XG2	Multiple Host (802.1X)
<input type="radio"/>	27	XG3	Multiple Host (802.1X)
<input type="radio"/>	28	XG4	Multiple Host (802.1X)

Copy Settings... Edit...

ステップ4:[Host Authentication ( ホスト認証 )]フィールドで、次のいずれかのオプションを選択します。

#### 1. シングルホストモード

- 許可されたクライアントがある場合、ポートは許可されます。1つのポートで許可できるホストは1つだけです。
- ポートが不正で、ゲストVLANが有効になっている場合、タグなしトラフィックはゲストVLANに再マップされます。タグ付きトラフィックは、ゲストVLANまたは認証されていないVLANに属していない限り、ドロップされます。ゲストVLANがポートで有効になっていない場合、非認証VLANに属するタグ付きトラフィックだけがブリッジされます。
- ポートが承認されると、承認されたホストからのタグなしトラフィックおよびタグ付きトラフィックは、スタティックVLANメンバーシップポート設定に基づいてブリッジされます。他のホストからのトラフィックはドロップされます。
- ユーザは、認証プロセス中にRADIUSサーバによって割り当てられたVLANに、許可されたホストからのタグなしトラフィックが再マッピングされるように指定できます。タグ付きトラフィックは、RADIUSによって割り当てられたVLANまたは認証されていないVLANに属していない限り、ドロップされます。ポートでのRADIUS VLAN割り当ては、[ポート認証]ページで設定されます。

#### 2. マルチホストモード

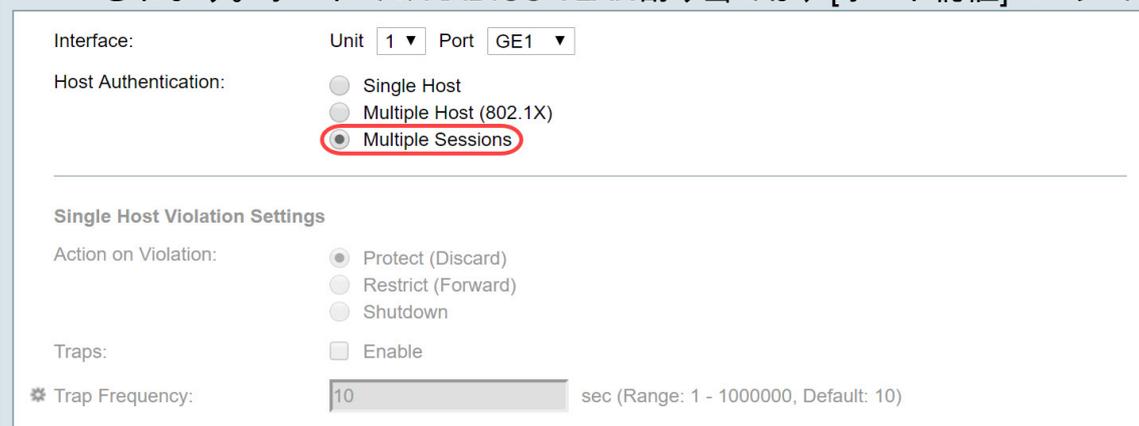
- 許可されたクライアントが少なくとも1つ存在する場合、ポートは許可されます。
- ポートが不正で、ゲストVLANが有効になっている場合、タグなしトラフィックはゲストVLANに再マップされます。タグ付きトラフィックは、ゲストVLANまたは認証されていない

いVLANに属していない限り、ドロップされます。ゲストVLANがポートで有効になっていない場合、非認証VLANに属するタグ付きトラフィックだけがブリッジされます。

- ポートが承認されると、スタティックVLANメンバーシップポート設定に基づいて、ポートに接続されているすべてのホストからのタグなしトラフィックとタグ付きトラフィックがブリッジされます。
- 認証プロセス中に、RADIUSサーバによって割り当てられたVLANに、認可ポートからのタグなしトラフィックが再マップされるように指定できます。タグ付きトラフィックは、RADIUSが割り当てたVLANまたは認証されていないVLANに属していない限り、ドロップされます。ポートでのRADIUS VLAN割り当ては、[ポート認証]ページで設定されます。

### 3. マルチセッションモード

- シングルホストモードとマルチホストモードとは異なり、マルチセッションモードのポートには認証ステータスはありません。このステータスは、ポートに接続された各クライアントに割り当てられます。
- 認証されていないVLANに属するタグ付きトラフィックは、ホストが許可されているかどうかにかかわらず、常にブリッジされます。
- 非認証VLANに属していない不正ホストからのタグ付きトラフィックおよびタグなしトラフィックは、VLANで定義および有効になっている場合はゲストVLANに再マップされ、ポートでゲストVLANが有効になっていない場合はドロップされます。
- 認証プロセス中に、RADIUSサーバによって割り当てられたVLANに、認可ポートからのタグなしトラフィックが再マップされるように指定できます。タグ付きトラフィックは、RADIUSが割り当てたVLANまたは認証されていないVLANに属していない限り、ドロップされます。ポートでのRADIUS VLAN割り当ては、[ポート認証]ページで設定します。



Interface: Unit 1 Port GE1

Host Authentication:

- Single Host
- Multiple Host (802.1X)
- Multiple Sessions

---

Single Host Violation Settings

Action on Violation:

- Protect (Discard)
- Restrict (Forward)
- Shutdown

Traps:  Enable

Trap Frequency: 10 sec (Range: 1 - 1000000, Default: 10)

Apply Close

ステップ5:[Apply]をクリックして設定を保存します。

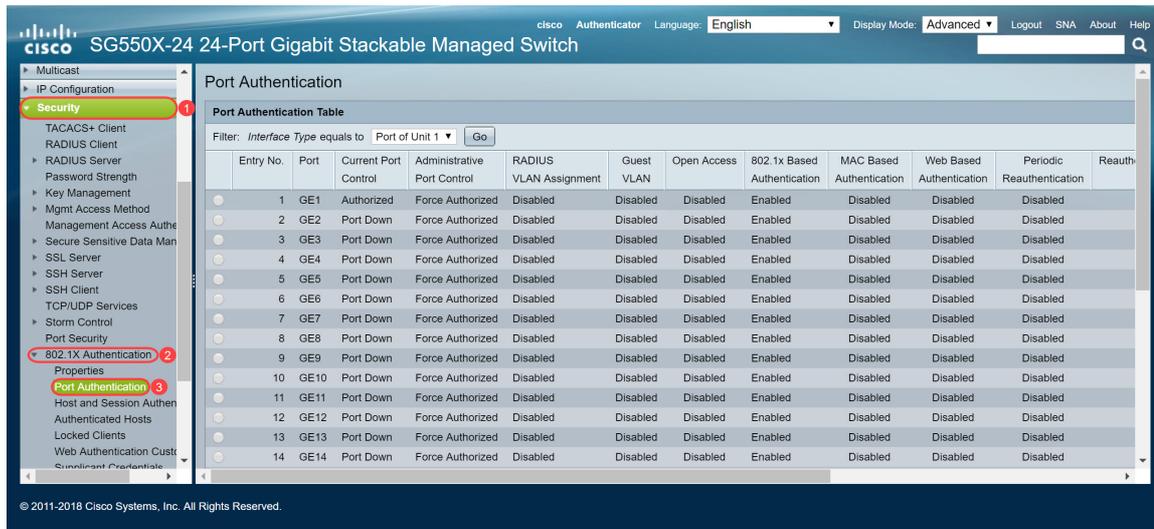
注：設定のコピーを使用... GE1の同じ設定を複数のポートに適用します。RADIUSサーバに接続されているポートはMultiple Host (802.1X)のままにします。

## 802.1X認証ポート認証

「ポート認証」ページでは、各ポートのパラメータを設定できます。設定の変更の一部は、ホスト認証など、ポートが強制承認済み状態である場合にのみ可能であるため、変更を行う前にポート制御を[強制承認済み(Force Authorized)]に変更することをお勧めします。設定が完了したら、ポート制御を以前の状態に戻します。

注：ここでは、MACベースの認証に必要な設定だけを設定します。残りの設定はデフォルトのままになります。

ステップ1:[Security] > [802.1X Authentication] > [Port Authentication]に移動します。



ステップ2：ポート許可を設定するポートを選択します。

注：スイッチが接続されているポートは設定しないでください。スイッチは信頼できるデバイスであるため、そのポートは[強制承認]のままにします。

Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment	Guest VLAN	Open Access	802.1x Based Authentication	MAC Based Authentication	Web Based Authentication	Periodic Reauthentication	Reauth
1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
2	GE2	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
3	GE3	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
4	GE4	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
6	GE6	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
7	GE7	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
8	GE8	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
9	GE9	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
10	GE10	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
11	GE11	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
12	GE12	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
13	GE13	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
14	GE14	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	

ステップ3：下にスクロールし、[Edit...]をクリックします。ポートを設定します。

11	GE11	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
12	GE12	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
13	GE13	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
14	GE14	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
15	GE15	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
16	GE16	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
17	GE17	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
18	GE18	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
19	GE19	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
20	GE20	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
21	GE21	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
22	GE22	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
23	GE23	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
24	GE24	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
25	XG1	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
26	XG2	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
27	XG3	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
28	XG4	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	

[ポート認証の編集]ページで、[現在のポート制御]フィールドに現在のポート認証状態が表示されます。状態がAuthorizedの場合は、ポートが認証されるか、管理ポート制御がForce Authorizedになります。逆に、状態がUnauthorizedの場合、ポートは認証されていないか、管理ポート制御は

*Force Unauthorized*になります。サブリカントがインターフェイスで有効になっている場合、現在のポート制御はサブリカントになります。

ステップ4：管理ポートの許可状態を選択します。ポートを自動的に設定します。使用可能なオプションは次のとおりです。

- **Forced Unauthorized**：インターフェイスを不正な状態に移行することによって、インターフェイスアクセスを拒否します。デバイスは、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]**：デバイスでポートベースの認証と許可を有効にします。インターフェイスは、デバイスとクライアント間の認証交換に基づいて、許可された状態または不正な状態の間を移動します。
- **Forced Authorized**：認証なしでインターフェイスを承認します。

注：**[強制承認]**は既定値です。

Interface: Unit 1 Port GE1  
Current Port Control: Authorized  
Administrative Port Control:  Force Unauthorized  Auto  Force Authorized  
RADIUS VLAN Assignment:  Disable  Reject  Static  
Guest VLAN:  Enable  
Open Access:  Enable  
802.1x Based Authentication:  Enable  
MAC Based Authentication:  Enable  
Web Based Authentication:  Enable  
Periodic Reauthentication:  Enable  
Reauthentication Period: 3600 sec (Range: 300 - 4294967295, Default: 3600)  
Reauthenticate Now:   
Authenticator State: Force Authorized  
Time Range:  Enable  
Time Range Name: Edit  
Maximum WBA Login Attempts:  Infinite  User Defined (Range: 3 - 10)  
Maximum WBA Silence Period:  Infinite

ステップ5:[802.1X Based Authentication]フィールドで、[Enable]チェックボックスをオフにします。これは、認証に802.1Xを使用しないためです。802.1x Based Authenticationのデフォルト値は有効です。

Interface: Unit 1 Port GE1  
Current Port Control: Authorized  
Administrative Port Control:  Force Unauthorized  Auto  Force Authorized  
RADIUS VLAN Assignment:  Disable  Reject  Static  
Guest VLAN:  Enable  
Open Access:  Enable  
802.1x Based Authentication:  Enable  
MAC Based Authentication:  Enable  
Web Based Authentication:  Enable  
Periodic Reauthentication:  Enable  
Reauthentication Period: 3600 sec (Range: 300 - 4294967295, Default: 3600)  
Reauthenticate Now:   
Authenticator State: Force Authorized  
Time Range:  Enable  
Time Range Name: Edit  
Maximum WBA Login Attempts:  Infinite  User Defined (Range: 3 - 10)  
Maximum WBA Silence Period:  Infinite

ステップ6：サブリカントのMACアドレスに基づいてポート認証を有効にする場合は、[MAC Based Authentication]の[Enable]チェックボックスをオンにします。ポートで使用できるMACベースの認証は8つだけです。

Interface: Unit 1 Port GE1

Current Port Control: Authorized

Administrative Port Control:
 

- Force Unauthorized
- Auto
- Force Authorized

RADIUS VLAN Assignment:
 

- Disable
- Reject
- Static

Guest VLAN:  Enable

Open Access:  Enable

802.1x Based Authentication:  Enable

MAC Based Authentication:  Enable

Web Based Authentication:  Enable

Periodic Reauthentication:  Enable

Reauthentication Period: 3600 sec (Range: 300 - 4294967295, Default: 3600)

Reauthenticate Now:

Authenticator State: Force Authorized

Time Range:  Enable

Time Range Name: Edit

Maximum WBA Login Attempts:
 

- Infinite
- User Defined

Maximum WBA Silence Period:  Infinite

ステップ7:[Apply]をクリックして、変更を保存します。

設定を保存する場合は、画面の上部にある[保存]ボタンを押します。



## 結論

これで、スイッチでMACベースの認証が正常に設定されました。MACベースの認証が機能していることを確認するには、次の手順を実行します。

ステップ1:[Security] > [802.1X Authentication] > [Authenticated Hosts]に移動し、認証されたユーザに関する詳細を表示します。

Authenticated Hosts

User Name	Port	Session Time (DD:HH:MM:SS)	Authentication Method	Authentication Server	MAC Address	VLAN ID
	GE1/1	00:00:06:56	MAC	Remote	54:ee:75:	

ステップ2：この例では、イーサネットMACアドレスが認証済みホストテーブルで認証されたことを確認できます。次のフィールドは次のように定義されます。

- [User Name]：各ポートで認証されたサブリカント名。
- Port：ポートの番号。
- Session Time(DD:HH:MM:SS)：サブリカントが認証され、ポートでアクセスが許可された時間。
- [Authentication Method]：最後のセッションが認証された方式。
- [Authenticated Server]:RADIUSサーバ。
- [MAC Address]：サブリカントのMACアドレスを表示します。
- VLAN ID：ポートのVLAN。

Authenticated Hosts

Authenticated Host Table						
User Name	Port	Session Time (DD:HH:MM:SS)	Authentication Method	Authentication Server	MAC Address	VLAN ID
54:EE:75: [redacted]	GE1/1	00:00:06:56	MAC	Remote	54:ee:75: [redacted]	

ステップ3: ( オプション ) [Status and Statistics] > [View Log] > [RAM Memory]に移動します。  
 [RAMメモリ]ページには、RAM ( キャッシュ ) に保存されたすべてのメッセージが時系列で表示されます。エントリは、[ログの設定]ページの設定に従ってRAMログに保存されます。

The screenshot shows the Cisco SG550X-24 24-Port Gigabit Stackable Managed Switch interface. The left sidebar has 'Status and Statistics' selected, with 'View Log' and 'RAM Memory' highlighted. The main content area displays the 'RAM Memory Log Table' with the following data:

Log Index	Log Time	Severity	Description
2147483573	2018-May-31 04:33:00	Warning	%AAA-EAP-W-RADIUSREPLY: Invalid attribute 26 ignored - vendor id is not Microsoft
2147483574	2018-May-31 04:33:00	Warning	%STP-W-PORTSTATUS: gi1/0/1: STP status Forwarding
2147483575	2018-May-31 04:32:56	Informational	%LINK-I-Up: gi1/0/1
2147483576	2018-May-31 04:32:53	Warning	%LINK-W-Down: gi1/0/1
2147483577	2018-May-31 04:31:56	Informational	%SEC-I-SUPPLICANTAUTHORIZED: MAC 54:ee:75: [redacted] is authorized on port gi1/0/1
2147483578	2018-May-31 04:31:56	Warning	%AAA-EAP-W-RADIUSREPLY: Invalid attribute 26 ignored - vendor id is not Microsoft
2147483579	2018-May-31 04:31:56	Warning	%STP-W-PORTSTATUS: gi1/0/1: STP status Forwarding
2147483580	2018-May-31 04:31:51	Informational	%LINK-I-Up: gi1/0/1
2147483581	2018-May-31 04:31:48	Warning	%LINK-W-Down: gi1/0/1
2147483582	2018-May-31 04:30:55	Notice	%COPY-N-TRAP: The copy operation was completed successfully
2147483583	2018-May-31 04:30:53	Informational	%COPY-I-FILECOPY: Files Copy - source URL running-config destination URL flash://system/configuration/startup-config
2147483584	2018-May-31 04:13:26	Informational	%SEC-I-SUPPLICANTAUTHORIZED: MAC 54:ee:75: [redacted] is authorized on port gi1/0/1
2147483585	2018-May-31 04:13:26	Warning	%AAA-EAP-W-RADIUSREPLY: Invalid attribute 26 ignored - vendor id is not Microsoft

ステップ4: RAMメモリログテーブルに、ポートgi1/0/1でMACアドレスが許可されていることを示す情報ログメッセージが表示されます。

注 : MACアドレスの一部がぼやけている。

2147483584 2018-May-31 04:13:26 Informational %SEC-I-SUPPLICANTAUTHORIZED: MAC 54:ee:75: [redacted] is authorized on port gi1/0/1

[この記事のビデオ版を表示...](#)

[シスコのその他のテクニカルトークを表示するには、ここをクリックしてください](#)