

# Configuration de l'authentification MAC sur un commutateur

## Objectif

802.1X est un outil d'administration qui permet d'autoriser les périphériques de liste, sans accès non autorisé à votre réseau. Ce document explique comment configurer l'authentification basée sur MAC sur un commutateur à l'aide de l'interface utilisateur graphique (GUI). Pour savoir comment configurer l'authentification basée sur MAC à l'aide de l'interface de ligne de commande (CLI), cliquez [ici](#).

**Note:** Ce guide est long en 9 sections et 1 section pour vérifier qu'un hôte a été authentifié. Prenez du café, du thé ou de l'eau et assurez-vous de disposer de suffisamment de temps pour examiner et exécuter les étapes en jeu.

[Pour plus d'informations, reportez-vous au glossaire.](#)

## Fonctionnement de RADIUS

L'authentification 802.1X comporte trois composants principaux : un demandeur (client), un authenticateur (périphérique réseau tel qu'un commutateur) et un serveur d'authentification (RADIUS). Le service RADIUS (Remote Authentication Dial-In User Service) est un serveur d'accès qui utilise le protocole AAA (Authentication, Authorization and Accounting) qui permet de gérer l'accès au réseau. RADIUS utilise un modèle client-serveur dans lequel des informations d'authentification sécurisées sont échangées entre le serveur RADIUS et un ou plusieurs clients RADIUS. Il valide l'identité du client et indique au commutateur si le client est autorisé ou non à accéder au réseau local.

Un authenticateur fonctionne entre le client et le serveur d'authentification. Tout d'abord, il demandera des informations d'identité au client. En réponse, l'authenticateur vérifierait les informations avec le serveur d'authentification. Enfin, il relaie une réponse au client. Dans cet article, l'authenticateur serait un commutateur qui inclut le client RADIUS. Le commutateur pourrait encapsuler et décapsuler les trames EAP (Extensible Authentication Protocol) pour interagir avec le serveur d'authentification.

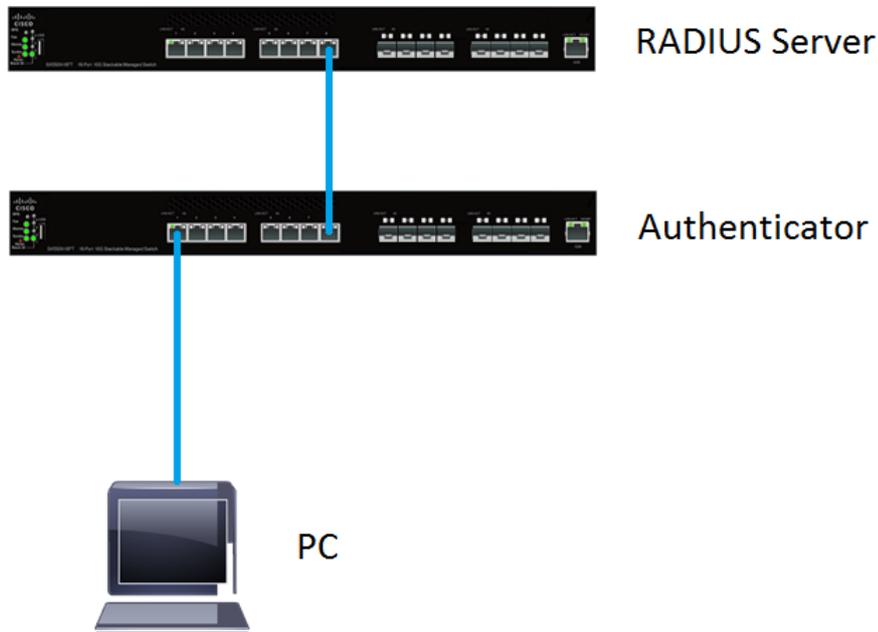
## Qu'en est-il de l'authentification basée sur MAC ?

Dans l'authentification basée sur MAC, lorsque le demandeur ne comprend pas comment parler à l'authenticateur ou est incapable de le faire, il utilise l'adresse MAC de l'hôte pour s'authentifier. Les demandeurs basés sur MAC sont authentifiés à l'aide de RADIUS pur (sans utiliser EAP). Le serveur RADIUS possède une base de données hôte dédiée qui contient uniquement les adresses MAC autorisées. Au lieu de traiter la demande d'authentification basée sur MAC comme une authentification PAP (Password Authentication Protocol), les serveurs reconnaissent une telle demande par l'attribut 6 [Service-Type] = 10. Ils compareront l'adresse MAC de l'attribut Calling-Station-Id aux adresses MAC stockées dans la base de données hôte.

La version 2.4 ajoute la possibilité de configurer le format du nom d'utilisateur envoyé pour les supplicants basés sur MAC et d'être défini soit par la méthode d'authentification EAP, soit par RADIUS pur. Dans cette version, vous pouvez également configurer le format du nom d'utilisateur ainsi qu'un mot de passe spécifique, différent du nom d'utilisateur, pour les demandes basées sur

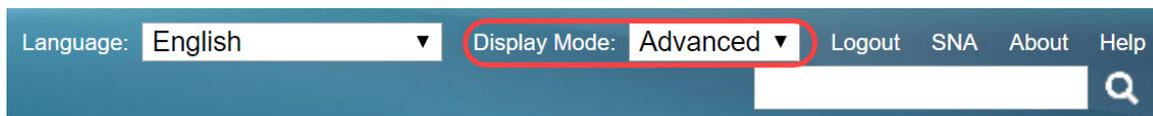
MAC.

Topologie:



**Note:** Dans cet article, nous allons utiliser le SG550X-24 pour le serveur RADIUS et l'authentificateur. Le serveur RADIUS a l'adresse IP statique 192.168.1.100 et l'authentificateur a l'adresse IP statique 192.168.1.101.

Les étapes de ce document sont exécutées en mode d'affichage **avancé**. Pour passer du mode avancé, accédez au coin supérieur droit et sélectionnez **Avancé** dans la liste déroulante *Mode affichage*.



## Table des matières

1. [Paramètres globaux du serveur RADIUS](#)
2. [Clés de serveur RADIUS](#)
3. [Groupes de serveurs RADIUS](#)
4. [Utilisateurs du serveur RADIUS](#)
5. [Client RADIUS](#)
6. [Propriétés d'authentification 802.1X](#)
7. [Paramètres d'authentification 802.1X basée sur MAC](#)
8. [Authentification 802.1X Authentification d'hôte et de session](#)
9. [Authentification du port d'authentification 802.1X](#)
10. [Conclusion](#)

# Périphériques pertinents

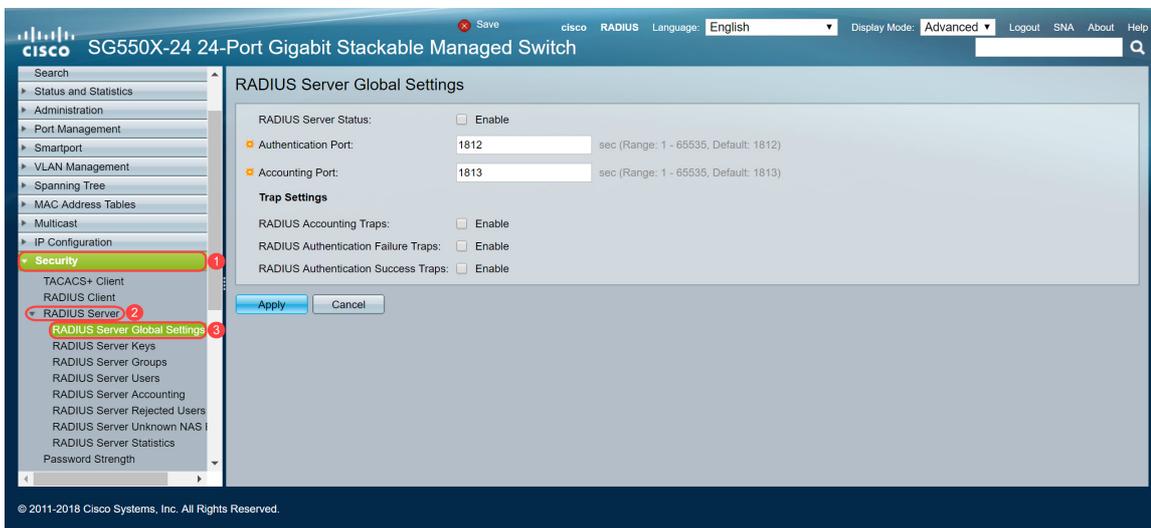
- Série Sx350X
- Série SG350XG
- Gamme Sx550X
- Série SG550XG

## Version du logiciel

- 2.4.0.94

## Paramètres globaux du serveur RADIUS

Étape 1. Connectez-vous à l'utilitaire Web de votre commutateur qui sera configuré en tant que serveur RADIUS et accédez à **Security > RADIUS Server > RADIUS Server Global Settings**.



Étape 2. Pour activer l'état de la fonctionnalité du serveur RADIUS, cochez la case **Enable** dans le champ *RADIUS Server Status*.



Étape 3. Pour générer des interruptions pour les événements de comptabilité RADIUS, les connexions ayant échoué ou les connexions ayant réussi, cochez la case **Activer** souhaitée pour générer des interruptions. Les interruptions sont des messages d'événements système générés via le protocole SNMP (Simple Network Management Protocol). Un déroutement est envoyé au gestionnaire SNMP du commutateur en cas de violation. Les paramètres de déroutement suivants

sont les suivants :

- RADIUS Accounting Traps : cochez cette case pour générer des interruptions pour les événements de comptabilité RADIUS.
- Blocs d'échec d'authentification RADIUS : cochez cette case pour générer des interruptions pour les connexions qui ont échoué.
- Blocs de réussite de l'authentification RADIUS : cochez cette case pour générer des interruptions pour les connexions qui ont réussi.

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

Étape 4. Cliquez sur **Apply** pour enregistrer vos paramètres.

## Clés de serveur RADIUS

Étape 1. Accédez à **Security > RADIUS Server > RADIUS Server Keys**. La page *RADIUS Server Key* s'ouvre.

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.

Étape 2. Dans la section *Table des clés secrètes*, cliquez sur **Ajouter...** pour ajouter une clé secrète.

## 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

Étape 3. La page *Ajouter une clé secrète* s'ouvre. Dans le champ *Adresse NAS*, saisissez l'adresse du commutateur qui contient le client RADIUS. Dans cet exemple, nous utiliserons l'adresse IP 192.168.1.101 comme client RADIUS.

NAS Address: 192.168.1.101 (IPv4 or IPv6 Address)

Secret Key:  Use default key  
 Encrypted   
 Plaintext  (0/128 characters used)

Apply

Close

Étape 4. Sélectionnez l'une des cases d'option utilisées comme *clé secrète*. Les options suivantes sont disponibles :

- Use default key : pour les serveurs spécifiés, le périphérique tente d'authentifier le client RADIUS à l'aide de la chaîne de clé par défaut existante.
- Encrypted : pour chiffrer les communications à l'aide de l'algorithme MD5 (Message-Digest Algorithm 5), saisissez la clé sous forme chiffrée.
- Texte clair : saisissez la chaîne de clé en mode texte clair.

Dans cet exemple, nous allons sélectionner *Texte clair* et utiliser l'**exemple** de mot comme *Clé secrète*. Après avoir appuyé sur Appliquer, votre clé sera chiffrée.

**Note:** Nous ne recommandons pas d'utiliser le mot **exemple** comme clé secrète. Veuillez utiliser une clé plus forte. Vous pouvez utiliser jusqu'à 128 caractères. Si votre mot de passe est trop complexe à retenir, c'est un bon mot de passe, mais mieux encore si vous pouvez transformer le mot de passe en une phrase de passe mémorable avec des caractères spéciaux et des chiffres remplaçant les voyelles — "P@55w0rds@reH@rdT0Remember« . Il est préférable de ne pas utiliser un mot qui se trouve dans un dictionnaire. Il est préférable de choisir une phrase et d'échanger certaines lettres contre des caractères et des chiffres spéciaux. Pour plus de détails, reportez-vous à ce billet [de blog Cisco](#).

NAS Address: 192.168.1.101 (IPv4 or IPv6 Address)

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

Étape 5. Cliquez sur **Apply** pour enregistrer votre configuration. La clé secrète est maintenant chiffrée avec MD5. MD5 est une fonction de hachage cryptographique qui prend un morceau de données et crée une sortie hexadécimale unique qui n'est généralement pas reproductible. MD5 utilise une valeur de hachage de 128 bits.

### 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	1a79a4d60de6718e8e5b326e338ae533

## Groupes de serveurs RADIUS

Étape 1. Accédez à **Security > RADIUS Server > RADIUS Server Groups**.

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

Étape 2. Cliquez sur **Add...** pour ajouter un nouveau groupe de serveurs RADIUS.

# 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"/>						

Étape 3. La page *Add RADIUS Server Group* s'affiche. Entrez un nom pour le groupe. Dans cet exemple, nous utiliserons **MAC802** comme nom de groupe.

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)

Étape 4. Entrez le niveau de privilège d'accès de gestion du groupe dans le champ *Niveau de privilège*. La plage est comprise entre 1 et 15, 15 étant le plus privilégié et la valeur par défaut est 1. Dans cet exemple, nous allons laisser le niveau de privilège 1.

**Note:** Nous ne configurerons pas *Time Range* ni *VLAN* dans cet article.

Group Name:  (6/32 characters used)

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

Time Range:  Enable

Time Range Name:

VLAN:

None

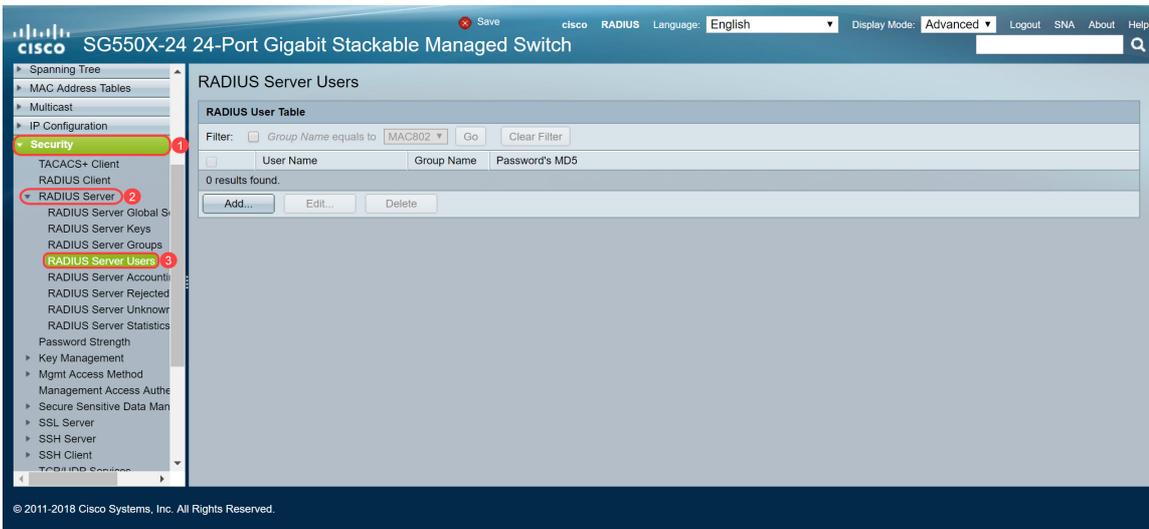
VLAN ID  (Range: 1 - 4094)

VLAN Name  (0/32 characters used)

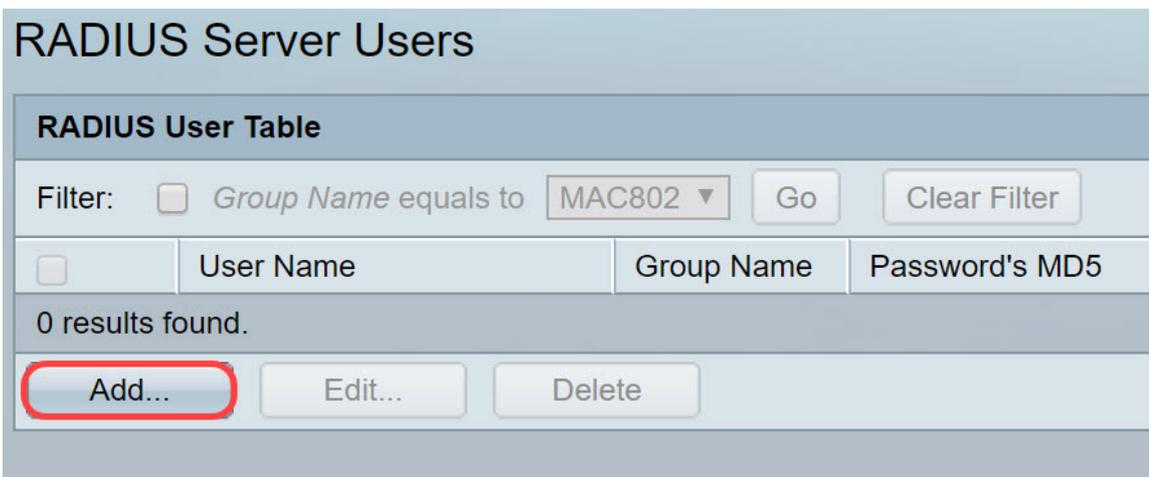
Étape 5. Cliquez sur **Apply** pour enregistrer vos paramètres.

# Utilisateurs du serveur RADIUS

Étape 1. Accédez à **Security > RADIUS Server > RADIUS Server Users** pour configurer les utilisateurs RADIUS.



Étape 2. Cliquez sur **Add...** pour ajouter un nouvel utilisateur.



Étape 3. La page *Add RADIUS Server User* s'ouvre. Dans le champ *Nom d'utilisateur*, saisissez l'adresse MAC d'un utilisateur. Dans cet exemple, nous utiliserons notre adresse MAC Ethernet sur notre ordinateur.

**Note:** Une partie de l'adresse MAC a été effacée.

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

Group Name: MAC802 ▼

Password:  Encrypted   
 Plaintext (0/32 characters used)

Apply Close

Étape 4. Sélectionnez un groupe dans la liste déroulante *Nom du groupe*. Comme indiqué à l'[étape 3](#) de la section [Groupe de serveurs RADIUS](#), nous allons sélectionner **MAC802** comme nom de groupe pour cet utilisateur.

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

Group Name: MAC802 ▼

Password:  Encrypted   
 Plaintext (0/32 characters used)

Apply Close

Étape 5. Sélectionnez l'une des cases d'option suivantes :

- Encrypted : une clé est utilisée pour chiffrer les communications à l'aide de MD5. Pour utiliser le chiffrement, entrez la clé sous forme chiffrée.
- Texte clair : si vous n'avez pas de chaîne de clé chiffrée (provenant d'un autre périphérique), entrez la chaîne de clé en mode texte clair. La chaîne de clé chiffrée est générée et affichée.

Nous sélectionnerons *Texte en clair* comme mot de passe pour cet utilisateur et nous taperons **par exemple** notre mot de passe en clair.

**Note:** Il n'est pas recommandé d'utiliser **exemple** comme mot de passe en texte clair. Nous vous recommandons d'utiliser un mot de passe plus fort.

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

Group Name: MAC802 ▼

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

Apply Close

Étape 6. Cliquez sur **Apply** une fois la configuration terminée.

Vous avez maintenant terminé la configuration du serveur RADIUS. Dans la section suivante, nous allons configurer le deuxième commutateur pour qu'il devienne authentificateur.

## Client RADIUS

Étape 1. Connectez-vous à l'utilitaire Web de votre commutateur qui sera configuré comme authentificateur et accédez à **Security > RADIUS Client**.

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

Étape 2. Faites défiler jusqu'à la section *Table RADIUS*, puis cliquez sur **Ajouter...** pour ajouter un serveur RADIUS.

**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.

Étape 3. (Facultatif) Indiquez si le serveur RADIUS doit être spécifié par adresse IP ou par nom dans le champ *Définition du serveur*. Dans cet exemple, nous allons conserver la sélection par défaut de **By IP address**.

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface:

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

Étape 4. (Facultatif) Sélectionnez la version de l'adresse IP du serveur RADIUS dans le champ *Version IP*. Nous allons conserver la sélection par défaut de **la version 4** pour cet exemple.

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface:

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

Étape 5. Saisissez l'adresse IP ou le nom du serveur RADIUS. Nous allons entrer l'adresse IP **192.168.1.100** dans le champ *Adresse IP/Nom du serveur*.

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

Étape 6. Saisissez la priorité du serveur. La priorité détermine l'ordre dans lequel le périphérique tente de contacter les serveurs pour authentifier un utilisateur. Le périphérique commence par le serveur RADIUS de priorité la plus élevée. Zéro est la priorité la plus élevée.

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

Étape 7. Entrez la chaîne de clé utilisée pour authentifier et chiffrer la communication entre le périphérique et le serveur RADIUS. Cette clé doit correspondre à la clé configurée sur le serveur RADIUS. Il peut être entré au format **Chiffré** ou **Texte clair**. Si **Use Default** est sélectionné, le périphérique tente de s'authentifier auprès du serveur RADIUS à l'aide de la chaîne de clé par défaut. Nous utiliserons le **texte défini par l'utilisateur (texte clair)** et saisirons l'**exemple** clé.

**Note:** Nous allons laisser le reste de la configuration par défaut. Vous pouvez les configurer si vous le souhaitez.

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface:

Server IP Address/Name:

Priority:  (Range: 0 - 65535)

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

Étape 8. Cliquez sur **Apply** pour enregistrer la configuration.

## Propriétés d'authentification 802.1X

La page des propriétés est utilisée pour activer globalement l'authentification des ports/périphériques. Pour que l'authentification fonctionne, elle doit être activée à la fois globalement et individuellement sur chaque port.

Étape 1. Accédez à **Sécurité > Authentification 802.1X > Propriétés**.

The screenshot shows the Cisco configuration interface for a SG550X-24 24-Port Gigabit Stackable Managed Switch. The left sidebar shows the navigation menu with 'Security' expanded and '802.1X Authentication' selected. The main area displays 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 shows various traps for 802.1X authentication, all of which are currently disabled.

Étape 2. Cochez la case **Activer** pour activer l'authentification basée sur les ports.

## 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

Étape 3. Sélectionnez les méthodes d'authentification des utilisateurs. Nous choisirons RADIUS comme méthode d'authentification. Les options suivantes sont disponibles :

- RADIUS, None : exécutez d'abord l'authentification de port à l'aide du serveur RADIUS. Si aucune réponse n'est reçue de RADIUS (par exemple, si le serveur est en panne), aucune authentification n'est effectuée et la session est autorisée. Si le serveur est disponible mais que les informations d'identification de l'utilisateur sont incorrectes, l'accès est refusé et la session est interrompue.
- RADIUS : authentifie l'utilisateur sur le serveur RADIUS. Si aucune authentification n'est effectuée, la session n'est pas autorisée.
- Aucun : ne pas authentifier l'utilisateur. Autoriser la session.

## 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

Étape 4. (Facultatif) Cochez la case **Activer** pour les *interruptions d'échec d'authentification MAC* et les interruptions de *réussite d'authentification MAC*. Cela génère un déroutement si l'authentification MAC échoue ou réussit. Dans cet exemple, nous allons activer les interruptions d'*échec d'authentification MAC* et les *interruptions d'authentification MAC*.

## 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

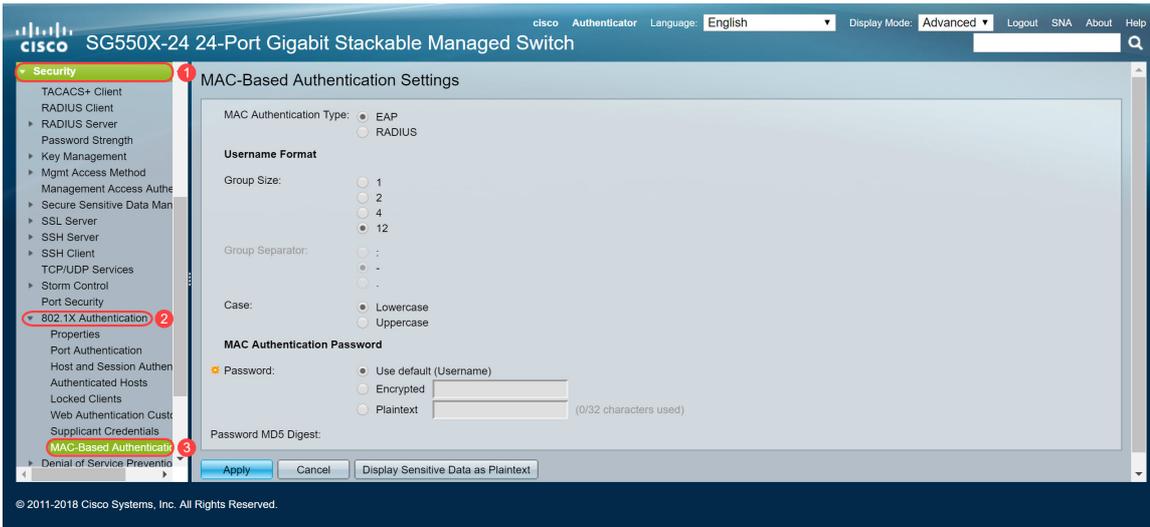
Étape 5. Cliquez sur Apply.

## Paramètres d'authentification 802.1X basée sur MAC

Cette page vous permet de configurer différents paramètres applicables à l'authentification basée

sur MAC.

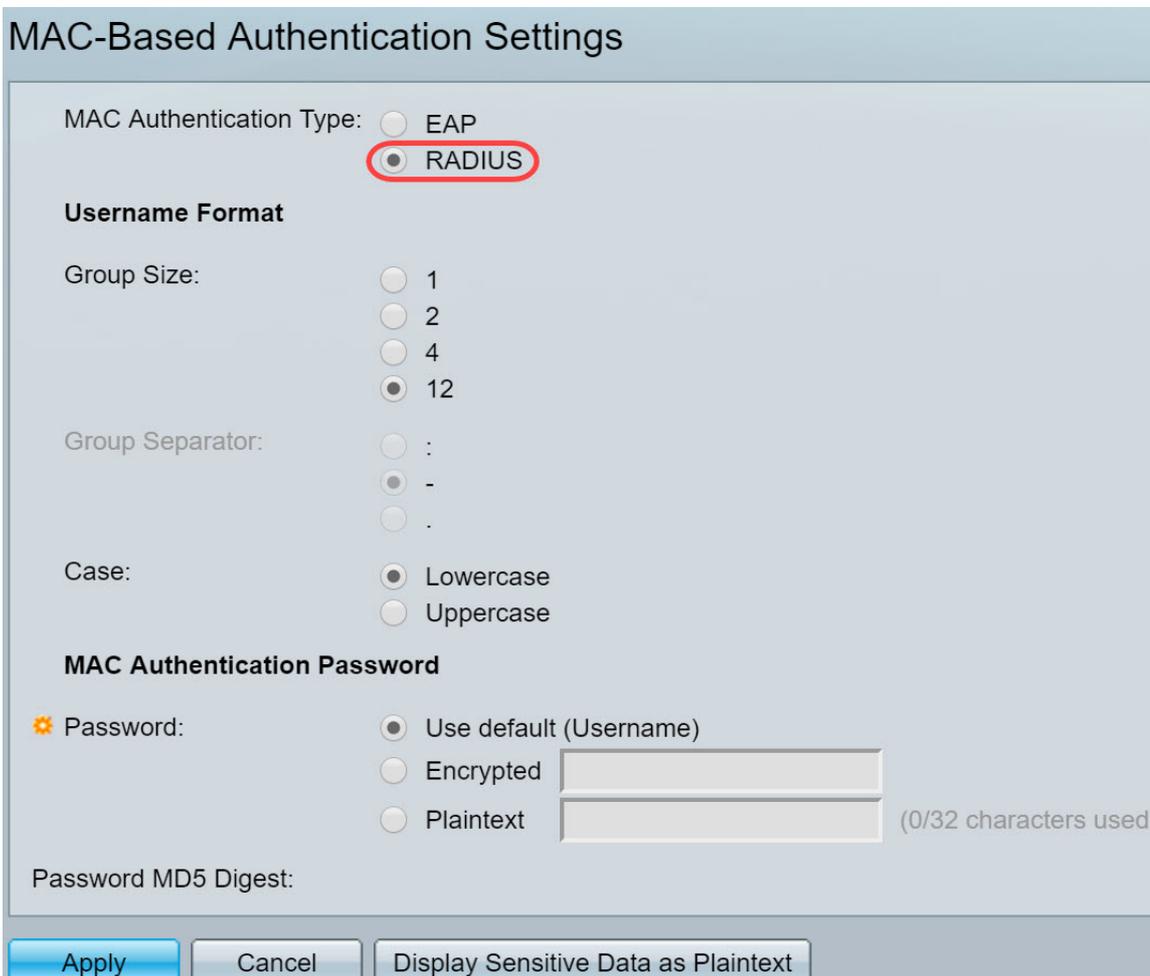
Étape 1. Accédez à **Security > 802.1X Authentication > MAC-Based Authentication Settings**.



Étape 2. Dans le *type d'authentification MAC*, sélectionnez l'une des options suivantes :

- EAP : utilisez RADIUS avec encapsulation EAP pour le trafic entre le commutateur (client RADIUS) et le serveur RADIUS, qui authentifie un demandeur basé sur MAC.
- RADIUS : utilisez RADIUS sans encapsulation EAP pour le trafic entre le commutateur (client RADIUS) et le serveur RADIUS, qui authentifie un demandeur basé sur MAC.

Dans cet exemple, nous allons choisir RADIUS comme type d'authentification MAC.



Étape 3. Dans le *format Username*, sélectionnez le nombre de caractères ASCII entre les

délimiteurs de l'adresse MAC envoyée sous forme de nom d'utilisateur. Dans ce cas, nous choisirons 2 comme taille de groupe.

**Note:** Assurez-vous que le format du nom d'utilisateur est identique à celui de l'entrée de l'adresse MAC dans la section [Utilisateurs du serveur Radius](#).

### 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:

Étape 4. Sélectionnez le caractère utilisé comme séparateur entre les groupes de caractères définis dans l'adresse MAC. Dans cet exemple, nous allons sélectionner : comme séparateur de groupe.

## 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:

Étape 5. Dans le champ *Cas*, sélectionnez **Minuscules** ou **Majuscules** pour envoyer le nom d'utilisateur en minuscules ou en majuscules.

## 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:

Étape 6. Le mot de passe définit la manière dont le commutateur va utiliser pour l'authentification via le serveur RADIUS. Sélectionnez l'une des options suivantes :

- Use default (Username) : sélectionnez cette option pour utiliser le nom d'utilisateur défini comme mot de passe.
- Encrypted : définit un mot de passe au format chiffré.
- Texte clair : définit un mot de passe en texte clair.

### 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:

**Remarque :** *Password Message-Digest Algorithm 5 (MD5) Digest* affiche le mot de passe MD5 Digest. MD5 est une fonction de hachage cryptographique qui prend un morceau de données et crée une sortie hexadécimale unique qui n'est généralement pas reproductible. MD5 utilise une valeur de hachage de 128 bits.

Étape 7. Cliquez sur **Apply** et les paramètres sont enregistrés dans le fichier de configuration en cours.

## Authentification 802.1X Authentification d'hôte et de session

La page *Host and Session Authentication* permet de définir le mode dans lequel 802.1X fonctionne sur le port et l'action à effectuer si une violation a été détectée.

Étape 1. Accédez à **Security > 802.1X Authentication > Host and Session Authentication**.

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

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

SG550X-24 24-Port Gigabit Stackable Managed Switch

Security

- TACACS+ Client
- RADIUS Client
- RADIUS Server
- Password Strength
- Key Management
- Mgmt Access Method
- Management Access Authen
- Secure Sensitive Data Man
- SSL Server
- SSH Server
- SSH Client
- TCP/UDP Services
- Storm Control
- Port Security
- 802.1X Authentication
- Properties
- Port Authentication
- Host and Session Authen
- Authenticated Hosts
- Locked Clients
- Web Authentication Cust
- Supplicant Credentials
- MAC-Based Authenticatio
- Denial of Service Preventio

### 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 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)				

Étape 2. Sélectionnez le port que vous voulez configurer l'authentification de l'hôte. Dans cet exemple, nous allons configurer GE1 lorsqu'il est connecté à un hôte final.

### 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)				

Étape 3. Cliquez sur **Modifier...** pour configurer le port.

<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...

Étape 4. Dans le champ *Authentification de l'hôte*, sélectionnez l'une des options suivantes :

#### 1. Mode hôte unique

- Un port est autorisé s'il existe un client autorisé. Un seul hôte peut être autorisé sur un port.
- Lorsqu'un port est non autorisé et que le VLAN invité est activé, le trafic non étiqueté est remappé au VLAN invité. Le trafic étiqueté est abandonné, sauf s'il appartient au VLAN invité ou à un VLAN non authentifié. Si un VLAN invité n'est pas activé sur le port, seul le trafic étiqueté appartenant aux VLAN non authentifiés est ponté.
- Lorsqu'un port est autorisé, le trafic non étiqueté et étiqueté de l'hôte autorisé est ponté en fonction de la configuration du port d'appartenance au VLAN statique. Le trafic provenant d'autres hôtes est abandonné.
- Un utilisateur peut spécifier que le trafic non étiqueté de l'hôte autorisé sera remappé sur un VLAN qui est attribué par un serveur RADIUS au cours du processus d'authentification. Le trafic étiqueté est abandonné, sauf s'il appartient au VLAN attribué par RADIUS ou aux VLAN non authentifiés. L'affectation de VLAN Radius sur un port est définie dans la page *Port Authentication*.

#### 2. Mode multihôte

- Un port est autorisé s'il existe au moins un client autorisé.
- Lorsqu'un port est non autorisé et qu'un VLAN invité est activé, le trafic non étiqueté est remappé au VLAN invité. Le trafic étiqueté est abandonné, sauf s'il appartient au VLAN invité ou à un VLAN non authentifié. Si le VLAN invité n'est pas activé sur un port, seul le trafic étiqueté appartenant à des VLAN non authentifiés est ponté.

- Lorsqu'un port est autorisé, le trafic non étiqueté et étiqueté de tous les hôtes connectés au port est ponté, en fonction de la configuration du port d'appartenance au VLAN statique.
- Vous pouvez spécifier que le trafic non étiqueté du port autorisé sera remappé sur un VLAN qui est attribué par un serveur RADIUS au cours du processus d'authentification. Le trafic étiqueté est abandonné, sauf s'il appartient au VLAN attribué par RADIUS ou aux VLAN non authentifiés. L'affectation de VLAN Radius sur un port est définie dans la page *Port Authentication*.

### 3. Mode multisessions

- Contrairement aux modes hôte unique et hôte multiple, un port en mode multisession n'a pas d'état d'authentification. Cet état est attribué à chaque client connecté au port.
- Le trafic étiqueté appartenant à un VLAN non authentifié est toujours ponté, que l'hôte soit autorisé ou non.
- Le trafic étiqueté et non étiqueté provenant d'hôtes non autorisés n'appartenant pas à un VLAN non authentifié est remappé au VLAN invité s'il est défini et activé sur le VLAN, ou est abandonné si le VLAN invité n'est pas activé sur le port.
- Vous pouvez spécifier que le trafic non étiqueté du port autorisé sera remappé sur un VLAN qui est attribué par un serveur RADIUS au cours du processus d'authentification. Le trafic étiqueté est abandonné, sauf s'il appartient au VLAN attribué par RADIUS ou aux VLAN non authentifiés. L'affectation de VLAN Radius sur un port est définie dans la page *Port Authentication*.

Interface: Unit  Port

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

Étape 5. Cliquez sur **Apply** pour enregistrer votre configuration.

**Note:** Utiliser *les paramètres de copie...* pour appliquer la même configuration de GE1 à plusieurs ports. Laissez le port connecté au serveur RADIUS en tant que *multihôte (802.1X)*.

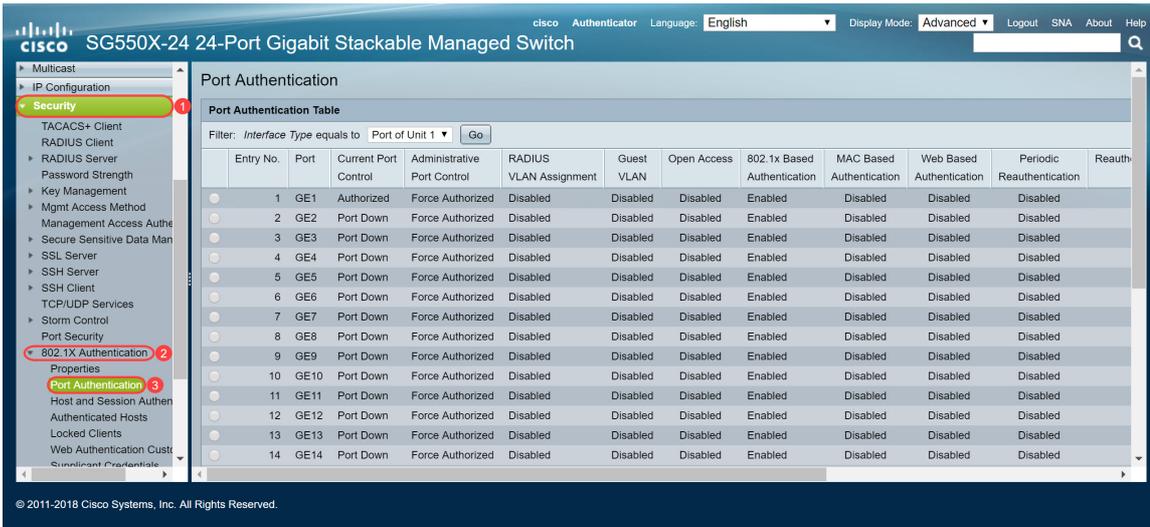
## Authentification du port d'authentification 802.1X

La page *Port Authentication* active la configuration des paramètres pour chaque port. Étant donné que certaines des modifications de configuration ne sont possibles que lorsque le port est à l'état Autorisé en vigueur, par exemple l'authentification de l'hôte, il est recommandé de modifier le contrôle de port en Forcer Autorisé avant d'apporter des modifications. Une fois la configuration terminée, remettez le contrôle de port à son état précédent.

**Note:** Nous configurerons uniquement les paramètres requis pour l'authentification basée sur

MAC. Le reste de la configuration sera laissé par défaut.

### Étape 1. Accédez à **Security > 802.1X Authentication > Port Authentication**.



### Étape 2. Sélectionnez le port que vous voulez configurer l'autorisation de port.

**Note:** Ne configurez pas le port auquel le commutateur est connecté. Le commutateur est un périphérique de confiance et laissez ce port comme *Autorisé forcé*.

Port Authentication

Port Authentication Table

Filter: Interface Type equals to Port of Unit 1 Go

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	

### Étape 3. Ensuite, faites défiler la page vers le bas et cliquez sur **Modifier...** pour configurer le port.

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	

Copy Settings... Edit...

Dans la page *Edit Port Authentication*, le champ *Current Port Control* affiche l'état d'autorisation de port actuel. Si l'état est *Autorisé*, le port est authentifié ou le *contrôle de port administratif* est *Autorisé*. Inversement, si l'état est *Non autorisé*, alors le port n'est pas authentifié ou le *contrôle de port administratif* est *Force Unallowed*. Si le demandeur est activé sur une interface, le contrôle de

port actuel est Suppliquant.

Étape 4. Sélectionnez l'état d'autorisation du port administratif. Configurez le port sur **Auto**. Les options disponibles sont les suivantes :

- **Forced Unallowed** : refuse l'accès à l'interface en déplaçant l'interface dans l'état non autorisé. Le périphérique ne fournit pas de services d'authentification au client via l'interface.
- **Auto** : active l'authentification et l'autorisation basées sur les ports sur le périphérique. L'interface se déplace entre un état autorisé ou non autorisé en fonction de l'échange d'authentification entre le périphérique et le client.
- **Forced Authorized** : autorise l'interface sans authentification.

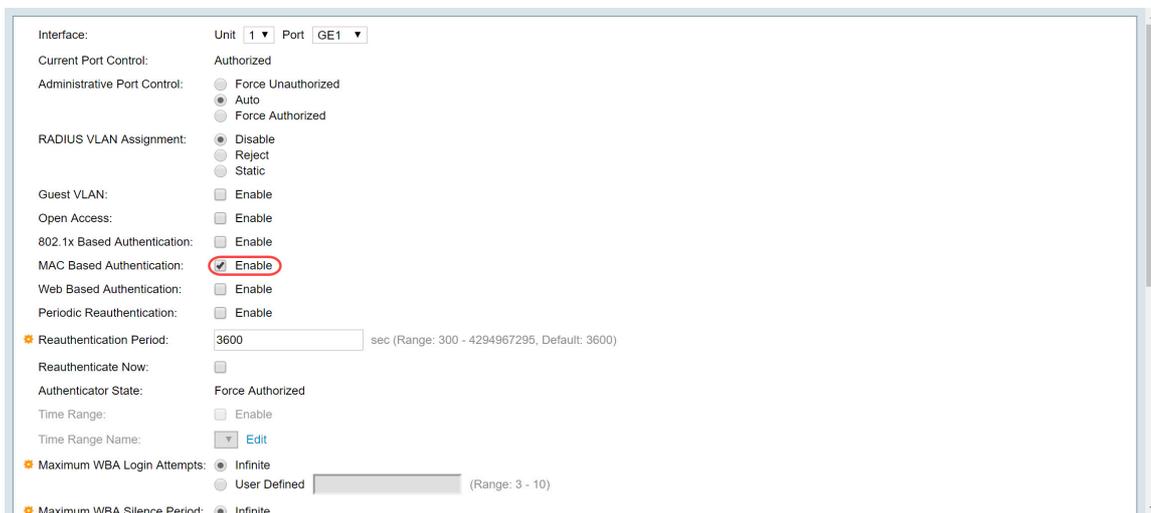
**Remarque** : *Forced Authorized* est la valeur par défaut.

The screenshot shows a configuration window for an interface. The 'Administrative Port Control' section has three radio buttons: 'Force Unauthorized', 'Auto' (which is selected and circled in red), and 'Force Authorized'. Other sections include 'RADIUS VLAN Assignment' with 'Disable' selected, 'Guest VLAN' with 'Enable' unchecked, 'Open Access' with 'Enable' unchecked, '802.1x Based Authentication' with 'Enable' checked, 'MAC Based Authentication' with 'Enable' unchecked, 'Web Based Authentication' with 'Enable' unchecked, and 'Periodic Reauthentication' with 'Enable' unchecked. The 'Reauthentication Period' is set to 3600 seconds. The 'Authenticator State' is set to 'Force Authorized'. The 'Maximum WBA Login Attempts' is set to 'Infinite' and the 'Maximum WBA Silence Period' is also set to 'Infinite'.

Étape 5. Dans le champ *Authentification basée sur 802.1X*, décochez la case **Activer** car nous n'utiliserons pas la norme 802.1X comme authentification. La valeur par défaut de l'*authentification basée sur 802.1x* est activée.

The screenshot shows the same configuration window as in Step 4. In the '802.1x Based Authentication' section, the 'Enable' checkbox is now unchecked and circled in red. All other settings remain the same as in the previous screenshot.

Étape 6. Cochez la case **Activer** pour l'*authentification basée sur MAC* comme nous voulons activer l'authentification de port basée sur l'adresse MAC du demandeur. Seules 8 authentifications MAC peuvent être utilisées sur le port.



Étape 7. Cliquez sur **apply** pour enregistrer vos modifications.

Pour enregistrer votre configuration, appuyez sur le bouton **Enregistrer** en haut de l'écran.



## Conclusion

Vous avez maintenant correctement configuré l'authentification basée sur MAC sur votre commutateur. Pour vérifier que l'authentification basée sur MAC fonctionne, procédez comme suit.

Étape 1. Accédez à **Sécurité > Authentification 802.1X > Hôtes authentifiés** pour afficher des détails sur les utilisateurs authentifiés.



Étape 2. Dans cet exemple, vous pouvez voir que notre adresse MAC Ethernet a été authentifiée dans la *table des hôtes authentifiés*. Les champs suivants définissent comme suit :

- User Name : noms de demandeur authentifiés sur chaque port.
- Port : numéro du port.
- Session Time (DD:HH:MM:SS) : durée pendant laquelle le demandeur a été authentifié et autorisé à accéder au port.
- Authentication Method : méthode par laquelle la dernière session a été authentifiée.
- Serveur authentifié — Serveur RADIUS.
- MAC Address : affiche l'adresse MAC du demandeur.
- VLAN ID : VLAN du port.

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:...	GE1/1	00:00:06:56	MAC	Remote	54:ee:75:...	

Étape 3. (Facultatif) Accédez à **Status and Statistics > View Log > RAM Memory**. La page *Mémoire vive* affiche tous les messages enregistrés dans la mémoire vive (cache) dans l'ordre chronologique. Les entrées sont stockées dans le journal de la mémoire vive en fonction de la configuration de la page *Paramètres du journal*.

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

Étape 4. Dans la *table de journalisation de la mémoire vive*, vous devriez voir un message de journal informatif indiquant que votre adresse MAC est autorisée sur le port gi1/0/1.

**Note:** Une partie de l'adresse MAC est floue.

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

[Voir la version vidéo de cet article...](#)

[Cliquez ici pour afficher d'autres présentations techniques de Cisco](#)