

MAC-gebaseerde verificatie op een switch configureren

Doel

802.1X is een beheergereedschap om lijstapparaten toe te staan, zodat u geen onbevoegde toegang tot uw netwerk hebt. Dit document toont u hoe u op MAC-gebaseerde verificatie op een switch kunt configureren met behulp van de grafische gebruikersinterface (GUI). Om te leren hoe u MAC-gebaseerde verificatie kunt configureren met behulp van de Opdracht Line Interface (CLI), klikt u [hier](#).

Opmerking: Deze gids is lang bij 9 delen en 1 sectie om te controleren of een host echt is bevonden. Grab koffie, thee of water en controleer of u voldoende tijd hebt om de stappen die erin zitten te bekijken en uit te voeren.

[Zie de woordenlijst voor aanvullende informatie.](#)

Hoe werkt Radius?

Er zijn drie hoofdcomponenten voor 802.1X-verificatie, een smeekbede (client), een authenticator (netwerkapparaat zoals een switch) en een authenticatieserver (RADIUS). De Remote Authentication Dial-On User Service (RADIUS) is een toegangsserver die gebruik maakt van verificatie, autorisatie en accounting (AAA) protocol dat netwerktoegang helpt beheren. RADIUS gebruikt een client-server model waarin beveiligde authenticatie informatie wordt uitgewisseld tussen de RADIUS-server en een of meer RADIUS-clients. Dit bevestigt de identiteit van de client en stelt de switch in kennis van de vraag of de client al dan niet is geautoriseerd om toegang te krijgen tot het LAN.

Een authenticator werkt tussen de client en de authenticatieserver. Ten eerste zal zij de cliënt om identiteitsinformatie verzoeken. Als reactie hierop zou de authenticator de informatie bij de authenticatieserver verifiëren. Tot slot zou zij een antwoord aan de cliënt doorgeven. In dit artikel zou de authenticator een schakelaar zijn die de RADIUS-client omvat. De switch zou de MAP-frames (Extensible Authentication Protocol) kunnen inkapselen decapsuleren om met de authenticatieserver te communiceren.

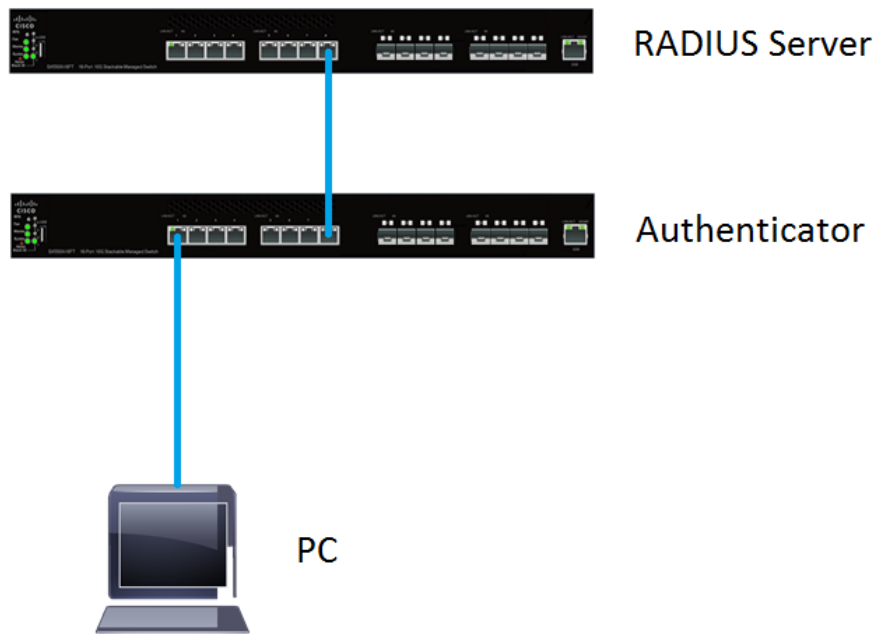
En MAC-gebaseerde verificatie?

In MAC-gebaseerde verificatie, wanneer de aanvrager niet begrijpt hoe hij met de authenticator moet praten of niet kan, gebruikt hij het MAC-adres van de host om te authenticeren. Op MAC gebaseerde leveranciers worden geauthentiseerd met pure RADIUS (zonder EAP te gebruiken). De RADIUS-server heeft een speciale host-database die alleen de toegestane MAC-adressen bevat. In plaats van het behandelen van het MAC-gebaseerde Verificatieverzoek als een PAP-verificatie (Wachtwoord Verificatieprotocol), herkennen de servers een dergelijk verzoek door kenmerk 6 [Service-Type] = 10. Ze zullen het MAC-adres in de eigenschap Calling-ID vergelijken met de MAC-adressen die in de host-database zijn opgeslagen.

De release van versie 2.4 voegt de mogelijkheid toe om het formaat van de gebruikersnaam te configureren dat voor op MAC gebaseerde leveranciers wordt verzonden en die ofwel de MAP-verificatiemethode of pure RADIUS wordt gedefinieerd. In deze versie kunt u ook het formaat van de gebruikersnaam configureren en een specifiek wachtwoord configureren, anders dan

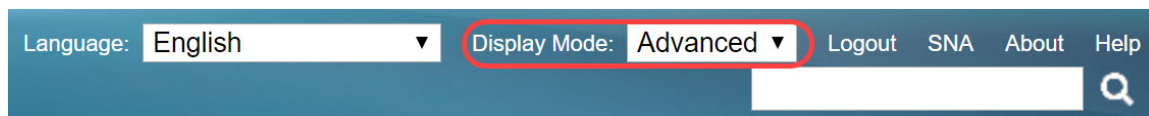
gebruikersnaam, voor MAC-gebaseerde leveranciers.

Topologie:



Opmerking: In dit artikel gebruiken we de SG550X-24 voor zowel de RADIUS-server als de authenticator. De RADIUS-server heeft een statisch IP-adres van 192.168.1.100 en de authenticator heeft een statisch IP-adres van 192.168.1.101.

De stappen in dit document worden uitgevoerd onder de modus **Geavanceerd**. Als u de modus in geavanceerde modus wilt wijzigen, gaat u naar de rechterbovenhoek en selecteert u **Geavanceerd** in de vervolgkeuzelijst *Weergavemodus*.



Inhoud

1. [Global Settings RADIUS-server](#)
2. [RADIUS-servertoetsen](#)
3. [RADIUS-servergroepen](#)
4. [Gebruikers van RADIUS-servers](#)
5. [RADIUS-client](#)
6. [802.1X verificatieeigenschappen](#)
7. [802.1X op MAC-gebaseerde verificatie-instellingen](#)
8. [802.1X verificatie en host- en sessieverificatie](#)
9. [802.1X poortverificatie](#)
10. [Conclusie](#)

Toepasselijke apparaten

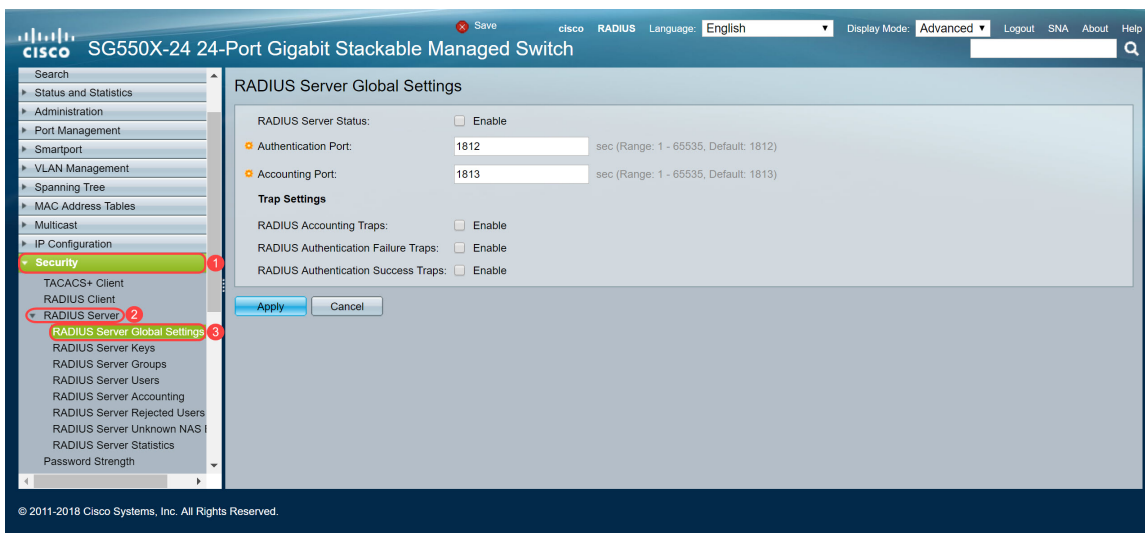
- SX350X Series-switches
- SG350XG Series
- Sx550X Series
- SG550XG Series

Softwareversie

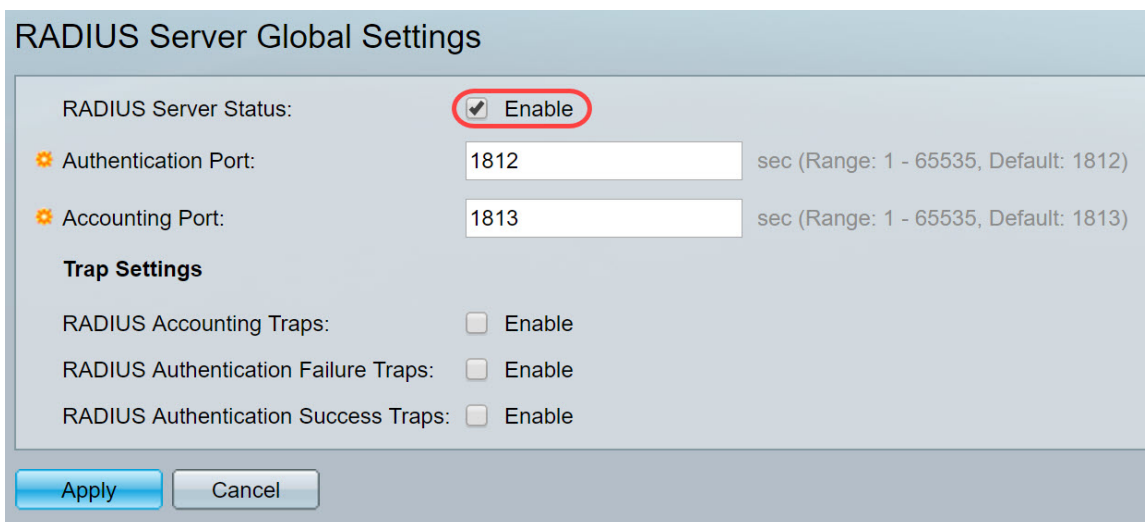
- 2.4.0.94

Global Settings RADIUS-server

Stap 1. Meld u aan bij het op web gebaseerde hulpprogramma van uw switch dat u als RADIUS-server hebt ingesteld en navigeer naar **Security > RADIUS Server > RADIUS Server Global Settings**.



Stap 2. Controleer de status van de RADIUS-serverfunctie in het veld *RADIUS-serverstatus* in het veld *RADIUS-serverstatus*.



Stap 3. Om vallen voor de boekhoudingsgebeurtenissen van de RADIUS te genereren, logins die mislukt zijn, of voor logins die geslaagd zijn, controleer het gewenste selectieteken **Enable** om vallen te genereren. Traps zijn systeemgebeurtenissen die via Simple Network Management Protocol (SNMP) zijn gegenereerd. Er wordt een val naar de SNMP-beheerder van de switch

gestuurd wanneer er sprake is van een schending. De volgende val-instellingen zijn:

- RADIUS-accounting Traps — Controleer om vallen te genereren voor RADIUS-accounting gebeurtenissen.
- RADIUS-verificatiestekens - Controleer om vallen te genereren voor mislukte logins.
- RADIUS-verificatietraps - Controleer om vallen te genereren voor logins die zijn geslaagd.

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

Apply Cancel

Stap 4. Klik op **Toepassen** om uw instellingen op te slaan.

RADIUS-servertoetsen

Stap 1. Navigeer naar **Security > RADIUS-server > RADIUS-servertoetsen**. De pagina *RADIUS-serversleutel* wordt geopend.

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
TACACS+ Client
RADIUS Client
RADIUS Server
RADIUS Server Global Settings
RADIUS Server Keys
RADIUS Server Groups
RADIUS Server Users
RADIUS Server Accounting
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:

Apply Cancel

Secret Key Table

NAS Address	Secret Key's MD5
0 results found.	

Add... Edit... Delete

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

Stap 2. Klik in het gedeelte *Tabel* geheim op **Toevoegen...** om een geheime sleutel toe te voegen.

RADIUS Server Keys

Default Key: Keep existing default key

Encrypted

Plaintext

(0/128 characters used)

MD5 Digest:

Apply

Cancel

Secret Key Table

NAS Address

Secret Key's MD5

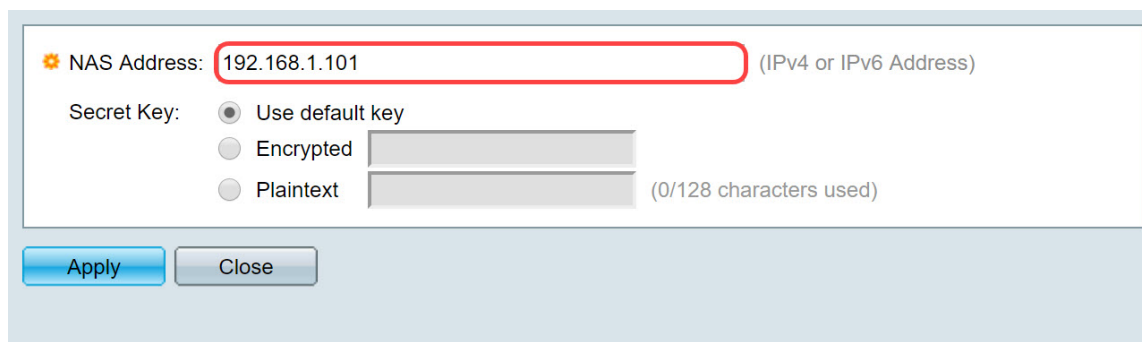
0 results found.

Add...

Edit...

Delete

Stap 3. Het venster *Geheime sleutel toevoegen* wordt geopend. Voer in het veld *NAS-adres* het adres in van de switch die RADIUS-client bevat. In dit voorbeeld zullen we het IP-adres 192.168.1.101 als onze RADIUS-client gebruiken.



NAS Address: 192.168.1.101 (IPv4 or IPv6 Address)

Secret Key: Use default key

Encrypted

Plaintext (0/128 characters used)

Apply Close

Stap 4. Selecteer een van de radioknop die als een *geheime sleutel* wordt gebruikt. De volgende opties zijn:

- Gebruik de standaardtoets — Voor gespecificeerde servers probeert het apparaat de RADIUS-client te authentifieren door de bestaande, standaard Key String te gebruiken.
- Versleuteld — Voor het versleutelen van communicatie met behulp van Message-Digest Algorithm 5 (MD5), voert u de sleutel in een versleuteld formulier in.
- Plaintext — Voer de sleutelstring in in klaagtekstmodus.

In dit voorbeeld selecteren we *Plaintext* en gebruiken we het woord **voorbeeld** als onze *Secret Key*. Nadat u op de toets drukt, wordt uw sleutel in een gecodeerd formulier geplaatst.

Opmerking: We raden niet aan het woord **voorbeeld** te gebruiken als de geheime sleutel. Gebruik een sterkere toets. Er kunnen maximaal 128 tekens worden gebruikt. Als je wachtwoord te complex is om het te onthouden, is het een goed wachtwoord, maar nog beter als je het wachtwoord kunt veranderen in een gedenkwaardig wachtwoord met speciale tekens en nummers die klinken vervangen — "P@55w0rds@reH@rdT0Remember". U kunt het beste geen woord gebruiken dat in een woordenboek voorkomt. U kunt het beste een zin kiezen en een aantal letters omruilen voor speciale tekens en getallen. Raadpleeg dit [Cisco](#)-blogartikel voor meer informatie.

NAS Address: (IPv4 or IPv6 Address)

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

Stap 5. Klik op **Toepassen** om de configuratie op te slaan. De geheime sleutel is nu versleuteld met MD5. MD5 is een cryptografische hashfunctie die een stuk gegevens neemt en een uniek hexadecimale uitvoer maakt die doorgaans niet reproduceerbaar is. MD5 gebruikt een hashwaarde van 128 bit.

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

RADIUS-servergroepen

Stap 1. Navigeer naar **Security > RADIUS-server > RADIUS-servergroepen**.

The screenshot shows the Cisco IOS configuration interface for a SG550X-24 24-Port Gigabit Stackable Managed Switch. The left sidebar shows the navigation tree with 'Security' expanded and 'RADIUS Server' selected. The main area shows the 'RADIUS Server Groups' configuration page. The 'RADIUS Server Group table' is currently empty, showing '0 results found.' The 'Add...' button is highlighted with a red circle. The top of the interface shows the 'Save' button and various system information like 'Language: English' and 'Display Mode: Advanced'.

Stap 2. Klik op **Add...** om een nieuwe RADIUS-servergroep toe te voegen.

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"/>						

Stap 3. De pagina *RADIUS-servergroep toevoegen* wordt geopend. Voer een naam in voor de groep. In dit voorbeeld zullen we **MAC802** gebruiken als onze groepsnaam.

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)

Stap 4. Voer het niveau van de beheerstoegangsrechten van de groep in in het veld *Priviveau*. Het bereik loopt van 1 tot 15, 15 is de meest bevoorrechte en de standaardwaarde is 1. In dit voorbeeld verlaten we het voorkeursniveau als 1.

Opmerking: We zullen in dit artikel geen *tijdbereik* of *VLAN* configureren.

Group Name: (6/32 characters used)

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

Time Range: Enable

Time Range Name:

VLAN:

None

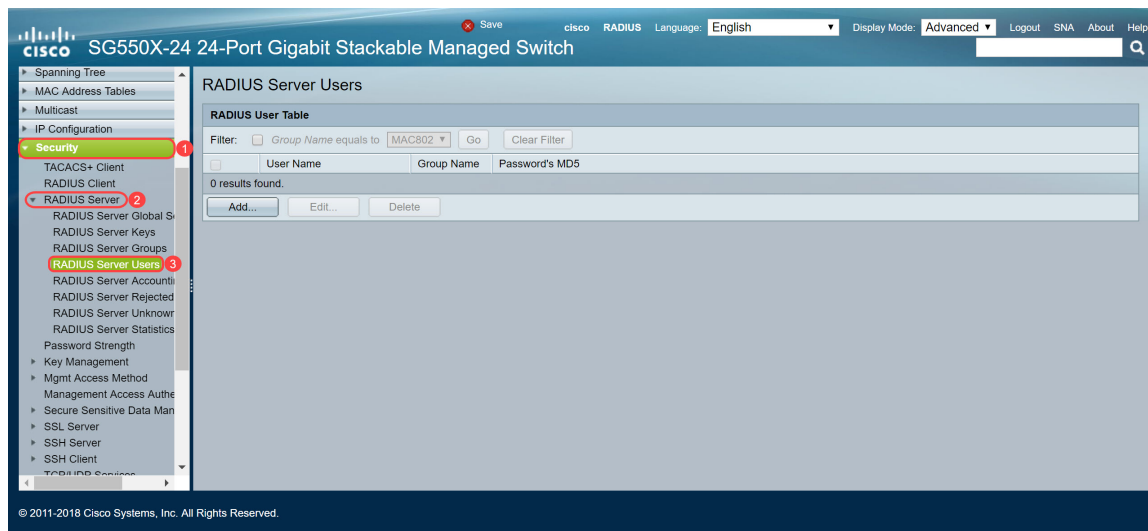
VLAN ID (Range: 1 - 4094)

VLAN Name (0/32 characters used)

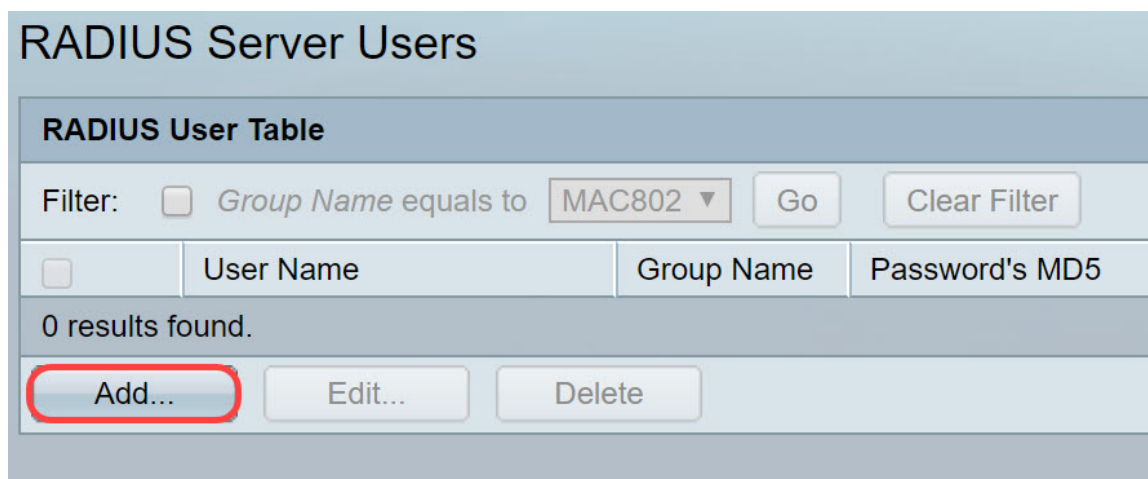
Stap 5. Klik op **Toepassen** om uw instellingen op te slaan.

Gebruikers van RADIUS-servers

Stap 1. Navigeer naar **Security > RADIUS-server > RADIUS-servergebruikers** om gebruikers voor RADIUS te configureren.



Stap 2. Klik op **Add...** om een nieuwe gebruiker toe te voegen.



Stap 3. De pagina *met gebruiker van RADIUS-server toevoegen* wordt geopend. Voer in het veld *Gebruikersnaam* het MAC-adres van een gebruiker in. In dit voorbeeld zullen we ons Ethernet MAC-adres op onze computer gebruiken.

Opmerking: Een deel van het MAC-adres is vervaagd.

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

Group Name: MAC802 ▼

Password: Encrypted
 Plaintext (0/32 characters used)

Apply Close

Stap 4. Selecteer een groep in de vervolgkeuzelijst *Naam van de groep*. Zoals aangegeven in [stap 3](#) van het gedeelte [RADIUS-servergroep](#), selecteren we **MAC802** als onze groepsnaam voor deze gebruiker.

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

Group Name: MAC802 ▼

Password: Encrypted
 Plaintext (0/32 characters used)

Apply Close

Stap 5. Selecteer een van de volgende radioknoppen:

- Versleuteld — Er wordt een sleutel gebruikt om communicatie te versleutelen met de MD5. Voer de sleutel in een versleuteld formulier in om encryptie te gebruiken.
- Plaintext — Als u geen gecodeerde key string hebt (van een ander apparaat), voer dan de key string in plaintext mode in. De gecodeerde key string wordt gegenereerd en weergegeven.

We selecteren *Plaintext* als ons wachtwoord voor deze gebruiker en typen **een** voorbeeldwachtwoord.

Opmerking: Het wordt niet aanbevolen het **voorbeeld** als het helderheidswachtwoord te gebruiken. We raden aan een sterker wachtwoord te gebruiken.

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

Group Name: MAC802 ▼

Password: Encrypted Plaintext example (32 characters used)

Apply Close

Stap 6. Klik op **Toepassen** zodra u het configureren hebt uitgevoerd.

U hebt nu de RADIUS-server configureren. In het volgende hoofdstuk zullen we de tweede schakelaar configureren om een authenticator te zijn.

RADIUS-client

Stap 1. Meld u aan bij het op web gebaseerde hulpprogramma van uw switch dat als authenticator is ingesteld en navigeer naar **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

Stap 2. Scrollt naar het gedeelte *RADIUS-tabel* en klik vervolgens op **Add...** om een RADIUS-server toe te voegen.

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.

Step 3. (Optioneel) Selecteer of u de RADIUS-server wilt specificeren via IP-adres of via de naam in het veld *Server Definition*. In dit voorbeeld, zullen we de standaardselectie van **Door IP adres** houden.

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

Step 4. (Optioneel) Selecteer de versie van het IP-adres van de RADIUS-server in het veld *IP-versie*. We houden de standaardselectie van **versie 4** voor dit voorbeeld.

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

Step 5. Voer in de RADIUS-server in via IP-adres of -naam. We voeren het IP-adres van **192.168.1.100** in het veld *IP-adres/naam van de server in*.

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

Stap 6. Voer de prioriteit van de server in. De prioriteit bepaalt de volgorde waarin het apparaat probeert om contact op te nemen met de servers om een gebruiker te authenticeren. Het apparaat start eerst met de hoogste prioriteit RADIUS-server. Nul is de hoogste prioriteit.

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

Stap 7. Voer de sleutelstring in die wordt gebruikt voor het authenticeren en versleutelen van communicatie tussen het apparaat en de RADIUS-server. Deze toets moet overeenkomen met de toets die op de RADIUS-server is ingesteld. U kunt dit formulier invoeren in de indeling **Encrypted** of **Plaintext**. Als **Use Default** wordt geselecteerd, probeert het apparaat om authenticatie aan de RADIUS server te geven door de standaard Key String te gebruiken. We zullen de **door gebruiker gedefinieerde (Plaintext)** gebruiken en in het belangrijke **voorbeeld** invoeren.

Opmerking: We laten de rest van de configuratie standaard over. U kunt ze zo nodig configureren.

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

Stap 8. Klik op **Toepassen** om de configuratie op te slaan.

802.1X verificatieeigenschappen

De eigenschappen pagina wordt gebruikt om wereldwijd poort/apparaatverificatie mogelijk te maken. Om de authenticatie te laten functioneren, moet deze zowel mondiaal als individueel op elke poort worden geactiveerd.

Stap 1. Navigeer naar **Security > 802.1X verificatie > Eigenschappen**.

The screenshot shows the Cisco configuration interface for a SG550X-24 switch. The left sidebar shows the navigation tree with 'Security' expanded and '802.1X Authentication' selected. The main area shows the 'Properties' page for 802.1X authentication. The 'Port-Based Authentication' checkbox is checked and highlighted with a red circle. Other settings like 'Authentication Method' (RADIUS) and 'Trap Settings' are visible.

Stap 2. Controleer het selectieteken **Enable** om poortgebaseerde verificatie mogelijk te maken.

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)
Trap Settings	
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

Stap 3. Selecteer de methoden voor gebruikersverificatie. We kiezen RADIUS als onze authenticatiemethode. De volgende opties zijn:

- RADIUS, geen — Voer eerst poortverificatie uit door gebruik te maken van de RADIUS-server. Als er geen respons wordt ontvangen van RADIUS (bijvoorbeeld als de server is ingedrukt) wordt er geen verificatie uitgevoerd en is de sessie toegestaan. Als de server beschikbaar is maar de gebruikersreferenties niet correct zijn, wordt de toegang geweigerd en de sessie beëindigd.
- RADIUS — Verifieer de gebruiker op de RADIUS-server. Als er geen verificatie wordt uitgevoerd, is de sessie niet toegestaan.
- Geen — echt van de gebruiker. Geef de sessie toe.

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)
Trap Settings	
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

Stap 4. (Optioneel) Controleer het aanvinkvakje **Enable** for *MAC-verificatie-fouten* en *MAC-verificatie-Succeszoekingen*. Dit zal een val genereren als de MAC-verificatie faalt of slaagt. In dit voorbeeld, zullen we zowel *MAC-verificatie-fouten* als *MAC-verificatietraps* inschakelen.

Properties

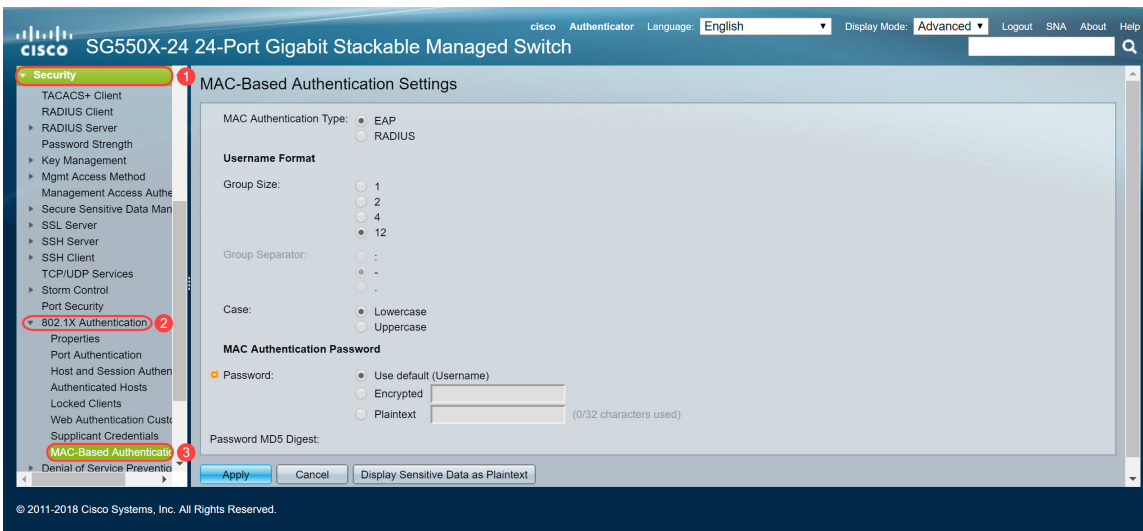
Port-Based Authentication:	<input checked="" type="checkbox"/> Enable
Authentication Method:	<input type="radio"/> RADIUS, None <input checked="" type="radio"/> RADIUS <input type="radio"/> None
Guest VLAN:	<input type="checkbox"/> Enable
Guest VLAN ID:	1 ▾
Guest VLAN Timeout:	<input checked="" type="radio"/> Immediate <input type="radio"/> User Defined <input type="text"/> sec (Range: 30 - 180)
Trap Settings	
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

Stap 5. Klik op **Toepassen**.

802.1X op MAC-gebaseerde verificatie-instellingen

Deze pagina stelt u in staat om verschillende instellingen te configureren die van toepassing zijn op MAC-gebaseerde verificatie.

Stap 1. Navigeer naar **Security > 802.1X verificatie > MAC-gebaseerde verificatie-instellingen**.



Stap 2. Selecteer in het *type MAC-verificatie* een van de volgende opties:

- EAP — Gebruik RADIUS met EAP-insluiting voor het verkeer tussen de switch (RADIUS-client) en de RADIUS-server, die een MAC-gebaseerde applicatie authentiek maakt.
- RADIUS — Gebruik RADIUS zonder EAP-insluiting voor het verkeer tussen de switch (RADIUS-client) en de RADIUS-server, die een MAC-gebaseerde applicatie authentiek maakt.

In dit voorbeeld kiezen we RADIUS als ons MAC-verificatietype.

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:

Stap 3. In het *formaat* van de *naam* van de *gebruiker* selecteert u het aantal ASCII-teken tussen de grenzen van het MAC-adres dat als een gebruikersnaam wordt verzonden. In dit geval kiezen wij 2 als onze fractie.

Opmerking: Zorg ervoor dat de gebruikersnaam dezelfde is als de manier waarop u het MAC-adres in de sectie [Radius Server Gebruikers](#) invoert.

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:

Stap 4. Selecteer het teken dat als scheidingsteken tussen de gedefinieerde groepen tekens in het MAC-adres wordt gebruikt. In dit voorbeeld selecteert u: als groepsscheidingsteken.

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:

Stap 5. Selecteer in het veld *Case* en **Case of Uppercase** om de gebruikersnaam in de onderste of bovenste case te verzenden.

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:

Stap 6. Wachtwoord definieert hoe de schakelaar voor verificatie via de RADIUS-server zal worden gebruikt. Selecteer een van de volgende opties:

- Gebruik standaard (Gebruikersnaam) - Selecteer dit item om de gedefinieerde gebruikersnaam voor het wachtwoord te gebruiken.
- Versleuteld — Definieer een wachtwoord in gecodeerde indeling.
- Plaintext — Definieer een wachtwoord in plaintext-indeling.

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:

N.B.: *Wachtwoord: algoritme 5 (MD5) Digest* geeft het MD5 Digest-wachtwoord weer. MD5 is een cryptografische hashfunctie die een stuk gegevens neemt en een unieke hexadecimale uitvoer maakt die doorgaans niet reproduceerbaar is. MD5 gebruikt een hashwaarde van 128 bit.

Stap 7. Klik op **Toepassen** en de instellingen worden opgeslagen in het actieve configuratiebestand.

802.1X verificatie en host- en sessieverificatie

De pagina *Host and Session Authentication* stelt het definiëren van de modus waarin 802.1X actief is in de poort en de actie om uit te voeren als er een schending is gedetecteerd.

Stap 1. Navigeer naar **Security > 802.1X verificatie > Host and Session Authentication**.

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

SG550X-24 24-Port Gigabit Stackable Managed Switch

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

Security

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)			

Showing 1-28 of 28 All per page

Stap 2. Selecteer de poort die u host-verificatie wilt configureren. In dit voorbeeld, zullen we GE1 configureren aangezien het is aangesloten op een eindhost.

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)			

Stap 3. Klik op **Bewerken...** om de poort te configureren.

<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...

Stap 4. Selecteer in het veld *Host Verificatie* een van de volgende opties:

1. Single Host Mode

- Een haven is toegestaan als er een geautoriseerde cliënt is. Slechts één host kan worden geautoriseerd in een haven.
- Wanneer een poort niet is geautoriseerd en het gastVLAN is geactiveerd, wordt untagged verkeer opnieuw in kaart gebracht aan de gast VLAN. Verkeersverkeer met tag wordt verbroken tenzij het van de gast VLAN of van een niet-echt VLAN is gemaakt. Als een gast VLAN niet op de haven wordt toegelaten, wordt slechts het gelabelde verkeer dat tot niet echt bevonden VLANs behoort overbrugd.
- Wanneer een poort is geautoriseerd, wordt untagged en tagged verkeer van de geautoriseerde host overbrugd op basis van de statische VLAN-lidmaatschapspoortconfiguratie. Verkeer van andere gastheren is gedaald.
- Een gebruiker kan specificeren dat niet-gelabeld verkeer van de geautoriseerde host opnieuw in kaart wordt gebracht aan een VLAN dat door een RADIUS-server wordt toegewezen tijdens het verificatieproces. Verkeer met tag wordt verbroken tenzij het behoort tot het door RADIUS toegewezen VLAN of de niet-geauthentiseerde VLAN's. De taak van Radius VLAN op een poort wordt ingesteld in de pagina *Port Verificatie*.

2. Multi-Host Mode

- Een haven is toegestaan indien er ten minste één geautoriseerde cliënt is.
- Wanneer een poort niet is geautoriseerd en een gast VLAN is geactiveerd, wordt untagged verkeer opnieuw in kaart gebracht aan de gast VLAN. Verkeersverkeer met tag wordt

verbroken tenzij het van de gast VLAN of van een niet-echt VLAN is gemaakt. Als de gast VLAN niet op een haven wordt toegelaten, wordt slechts het gelabelde verkeer dat tot niet echt bevonden VLANs behoort aangesloten.

- Wanneer een poort is toegestaan, wordt untagged en gelabeld verkeer van alle hosts die met de poort zijn verbonden, overbrugd op basis van de configuratie van de statische VLAN-poort.
- U kunt specificeren dat niet-gelabeld verkeer van de geautoriseerde poort opnieuw in kaart wordt gebracht aan een VLAN dat door een RADIUS-server wordt toegewezen tijdens het authenticatieproces. Verkeer met tag wordt verbroken tenzij het behoort tot het door RADIUS toegewezen VLAN of tot de niet-geauthentiseerde VLAN's. De taak van Rus VLAN op een poort wordt ingesteld in de pagina *Port Verificatie*.

3. Modus met meerdere sessies

- Anders dan de single-host- en multi-host-modi heeft een poort in de multi-sessie-modus geen verificatiestatus. Deze status wordt toegewezen aan elke client die is aangesloten op de poort.
- Gevangen verkeer dat tot een niet-echt VLAN behoort wordt altijd overbrugd ongeacht of de host is geautoriseerd.
- Gevangen en niet getagd verkeer van niet-geautoriseerde hosts die niet tot een niet-echt VLAN behoren, wordt opnieuw in kaart gebracht aan de gast VLAN als dit op het VLAN is gedefinieerd en ingeschakeld, of als het gastVLAN niet op de poort is geactiveerd.
- U kunt specificeren dat niet-gelabeld verkeer van de geautoriseerde poort opnieuw in kaart wordt gebracht aan een VLAN dat door een RADIUS-server wordt toegewezen tijdens het authenticatieproces. Verkeer met tag wordt verbroken tenzij het behoort tot het door RADIUS toegewezen VLAN of tot de niet-geauthentiseerde VLAN's. De radiale VLAN-toewijzing op een poort wordt ingesteld in de pagina *Port Verificatie*.

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)

Stap 5. Klik op **Toepassen** om de configuratie op te slaan.

Opmerking: *Instellingen kopiëren* gebruiken... dezelfde configuratie van GE1 op meerdere poorten toepassen. Laat de poort die op de RADIUS-server is aangesloten als *meerdere host (802.1X)*.

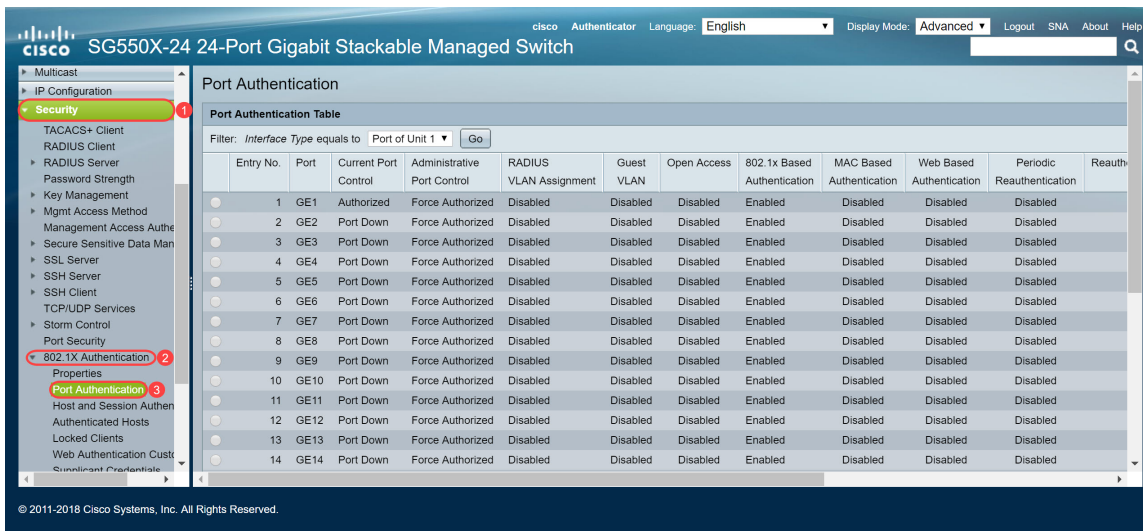
802.1X poortverificatie

De pagina *Port Verificatie* maakt het mogelijk de parameters voor elke poort te configureren.

Aangezien sommige van de configuratieveranderingen slechts mogelijk zijn terwijl de haven in de geautoriseerde staat van kracht is, zoals de authenticatie van de gastheer, wordt aanbevolen om de havencontrole in Macht te veranderen alvorens veranderingen door te voeren. Wanneer de configuratie is voltooid, moet u de poortcontrole terugbrengen naar de vorige status.

Opmerking: We zullen alleen instellingen configureren die vereist zijn voor MAC-gebaseerde verificatie. De rest van de configuratie blijft standaard over.

Stap 1. Navigeer naar **Security > 802.1X verificatie > Port-verificatie**.



Stap 2. Selecteer de poort waar u de poortadapter voor wilt configureren.

Opmerking: Configureer de poort waarop de schakelaar is aangesloten niet. De schakelaar is een betrouwbaar apparaat zodat laat die poort zoals *Gedwongen Geautomatiseerd*.

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		

Stap 3. Ga dan naar beneden en klik op **Bewerken...** om de poort te configureren.

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...

In de pagina *Port Verificatie bewerken* geeft het veld *Huidige poortcontrole* de huidige status van de poortautorisatie weer. Als de staat *toestemming* heeft *gekregen*, is de haven ofwel geauthentiseerd ofwel is de *administratieve havencontrole toestemming* verleend. Als de staat daarentegen *onbevoegd* is, is de haven niet echt bevonden of is de *administratieve havencontrole niet toegestaan*. Als de applicatie op een interface is ingeschakeld, zal de huidige poortcontrole *Suppliciet* zijn.

Stap 4. Selecteer de staat van de vergunning van de administratieve poort. Configureer de poort **automatisch**. De beschikbare opties zijn:

- Gedwongen onbevoegd — ontkent de interfacetoegang door de interface naar de onbevoegde staat te verplaatsen. Het apparaat verleent geen authenticatiediensten aan de cliënt door middel van de interface.
- Auto — schakelt verificatie en autorisatie op de haven in. De interface beweegt tussen een geautoriseerde of niet-geautoriseerde staat op basis van de authenticatie-uitwisseling tussen het apparaat en de client.
- Gedwongen geautoriseerd — autoriseert de interface zonder verificatie.

Opmerking: *Gedwongen toestemming* is de standaardwaarde.

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

Stap 5. In het veld *802.1X gebaseerde verificatie*, schakelt u het selectieteken *Inschakelen* uit omdat we 802.1X niet als onze verificatie gaan gebruiken. De standaardwaarde van *802.1x gebaseerde verificatie* is ingeschakeld.

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

Stap 6. Controleer het selectieteken **Enable** for *MAC Based Verificatie* omdat we poortverificatie op basis van het aangevoerde MAC-adres willen inschakelen. Alleen 8 MAC-gebaseerde authenticaties kunnen in de poort worden gebruikt.

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

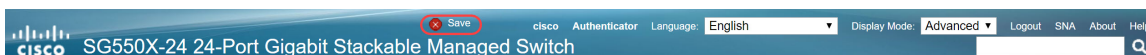
Maximum WBA Login Attempts:

- Infinite
- User Defined (Range: 3 - 10)

Maximum WBA Silence Period: Infinite

Stap 7. Klik op **Toepassen** om uw wijzigingen op te slaan.

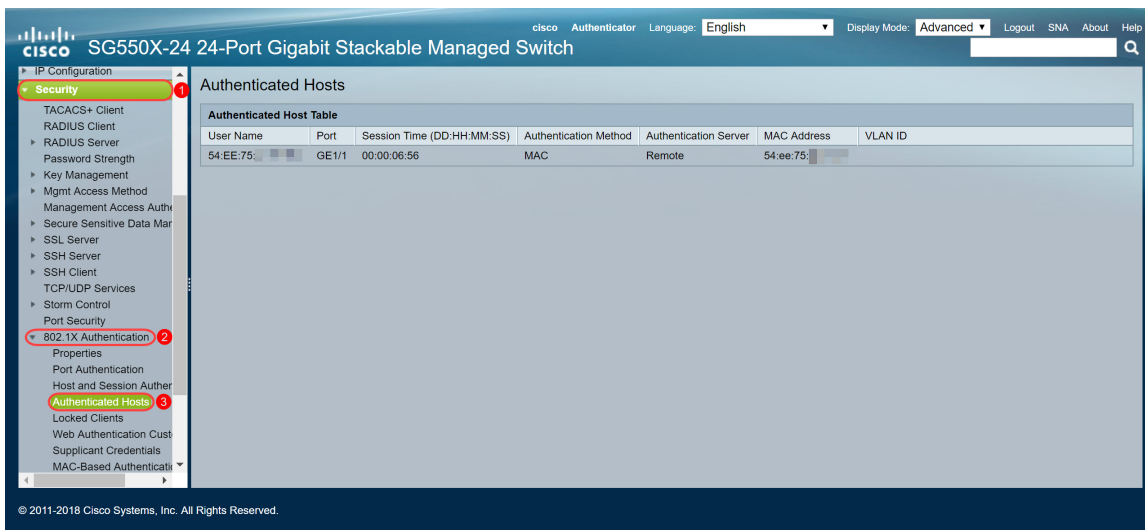
Druk op de knop **Opslaan** bovenin het scherm als u de configuratie wilt opslaan.



Conclusie

U hebt nu met succes MAC-gebaseerde verificatie op uw switch ingesteld. Om te verifiëren dat de MAC-gebaseerde verificatie werkt, volgt u de onderstaande stappen.

Stap 1. Navigeer naar **Security > 802.1X Verificatie > Verificeerde hosts** om details over geauthenticeerde gebruikers te bekijken.



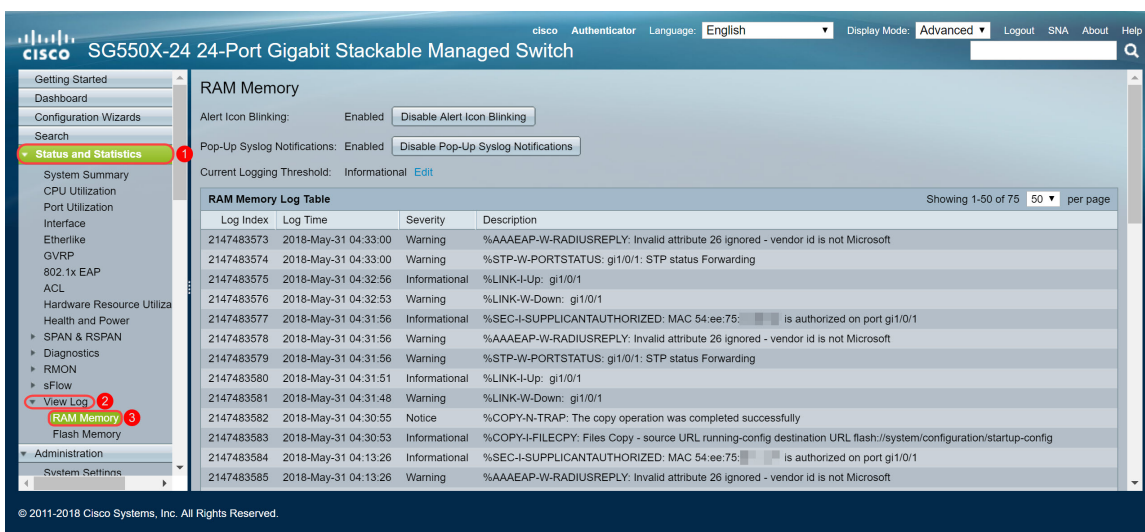
Stap 2. In dit voorbeeld, kunt u ons Ethernet MAC-adres zien dat in de *verklaard Host Tabel* authentiek was. De volgende velden worden gedefinieerd als:

- Gebruikersnaam — Leveranciersnamen die voor elke poort zijn geauthentiseerd.
- Poorten — Nummer van de haven.
- Sessietijd (DD:UU:MM:SS) — Hoeveelheid tijd dat de aanvrager gewaarmerkt werd en geautoriseerde toegang in de poort.
- Verificatiemethode — Methode waarmee de laatste sessie is geauthentiseerd.
- Authenticated Server — RADIUS server.
- MAC-adres — Hiermee wordt het opgegeven MAC-adres weergegeven.
- VLAN-id - Port is VLAN.

Authenticated Hosts

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]	

Stap 3. (Optioneel) navigeren naar **Status en Statistieken > Log bekijken > RAM geheugen**. De pagina *RAM Geheugen* geeft alle berichten weer die zijn opgeslagen in RAM (cache) in chronologische volgorde. Vermeldingen worden opgeslagen in het RAM-logbestand volgens de configuratie in de pagina *Log instellingen*.



Stap 4. In de *RAM-logtabel* moet u een informatief logbericht zien waarin staat dat uw MAC-adres is toegestaan op poort gi1/0/1.

Opmerking: Een deel van het MAC-adres is onduidelijk.

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

Bekijk de videoversie van dit artikel...

[Klik hier om andere Tech Talks uit Cisco te bekijken](#)