Configureer 802.1x poortverificatie-instelling op een switch

Doel

IEEE 802.1x is een standaard die toegangscontrole tussen een client en een server vergemakkelijkt. Voordat services aan een client kunnen worden geleverd door een LAN (Local Area Network) of switch, moet de client die is aangesloten op de switchpoort worden geauthentificeerd door de verificatieserver die Remote Authentication Dial-User Service (RADIUS) uitvoert.

802.1x-verificatie beperkt niet-geautoriseerde clients tot het aansluiten op een LAN door middel van openbaarheidspoorten. 802.1x-verificatie is een client-server-model. In dit model hebben netwerkapparaten de volgende specifieke rollen:

Een client of leverancier — Een client of leverancier is een netwerkapparaat dat toegang tot het LAN vraagt. De client is verbonden met een authenticator.

Authenticator - Een authenticator is een netwerkapparaat dat netwerkservices aanbiedt en waarmee aanvoerpoorten worden aangesloten. De volgende authenticatiemethoden worden ondersteund:

802.1x-gebaseerd — Ondersteund in alle verificatiemodi. In 802.1x-gebaseerde verificatie haalt de authenticator de MAP-berichten uit de 802.1x-berichten of EAP-over-LAN-pakketten (EAPoL) van het Extensible Authentication Protocol (EAP), en geeft ze door aan de verificatieserver, met behulp van het RADIUS-protocol.

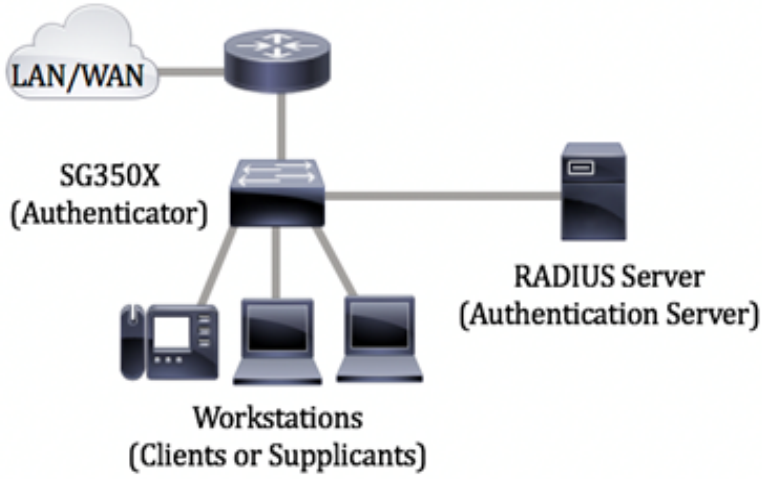
MAC-gebaseerd — Ondersteund in alle verificatiemodi. Met Media Access Control (MAC)-gebaseerde, voert de authenticator zelf het MAP-clientgedeelte van de software uit namens de klanten die netwerktoegang zoeken.

Web-gebaseerd - uitsluitend ondersteund in multi-sessiemodi. Met webgebaseerde authenticatie voert de authenticator zelf het MAP-clientgedeelte van de software uit namens de klanten die netwerktoegang zoeken.

Verificatieserver - Een verificatieserver voert de eigenlijke authenticatie van de client uit. De authenticatieserver voor het apparaat is een RADIUS-verificatieserver met EAP-extensies.

Opmerking: Een netwerkapparaat kan een client of applicator zijn, authenticator of beide poorten.

Het beeld hieronder toont een netwerk dat de apparaten volgens de specifieke rollen heeft gevormd. In dit voorbeeld wordt een SG350X-schakelaar gebruikt.



Richtsnoeren voor de configuratie van 802.1x:

Maak een Virtual Access Network (VLAN). Om VLAN's te maken die het web-based hulpprogramma van uw switch gebruiken, klik hier. Klik hier voor instructies met de opdrachtregel.

Configureer poort naar VLAN-instellingen op uw switch. Klik hier om te configureren met behulp van het webgebaseerde hulpprogramma. Klik hier om de CLI te gebruiken.

Configuratie van 802.1x eigenschappen op de schakelaar. 802.1x zou wereldwijd op de switch moeten worden ingeschakeld om 802.1x op poorten gebaseerde verificatie mogelijk te maken. Klik hier voor meer informatie.

(Optioneel) Het instellen van tijdbereik op de schakelaar. Klik hier om te leren hoe u de instellingen voor het tijdbereik van uw schakelaar kunt configureren.

Configureer 802.1x poortverificatie. Dit artikel bevat instructies over de manier waarop u 802.1x-instellingen voor poortverificatie op uw switch kunt configureren.

Om te leren hoe te om op mac gebaseerde authenticatie op een schakelaar te configureren klikt u hier.

Toepasselijke apparaten

Sx300 Series

Sx350 Series

SG350X Series

Sx500 Series

Sx550X Series

Softwareversie

1.4.7.06 — SX300, SX500

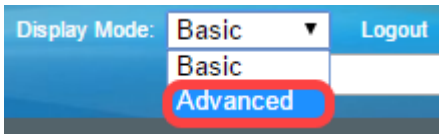
2.2.8.04 — SX350, SG350X, SX550X

Configureer 802.1x poortverificatie-instellingen op een switch

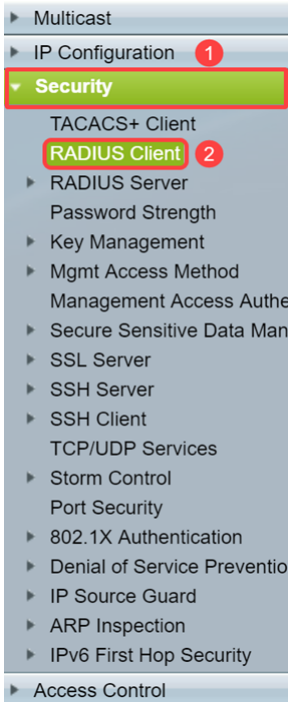
RADIUS-clientinstellingen configureren

Stap 1. Meld u aan bij het op web gebaseerde hulpprogramma van uw switch en kies vervolgens **Geavanceerd** in de vervolgkeuzelijst Weergavemodus.

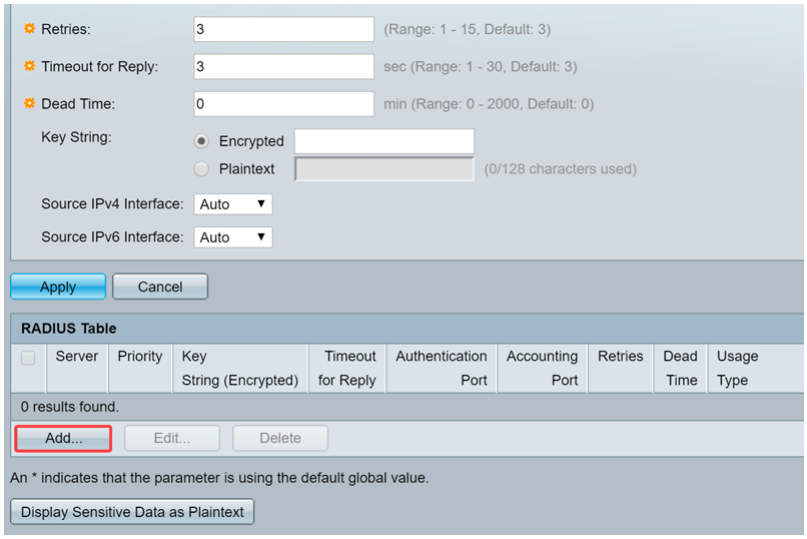
Opmerking: De beschikbare menu-opties kunnen afhankelijk van het apparaatmodel verschillen. In dit voorbeeld wordt SG550X-24 gebruikt.



Stap 2. Navigeer naar **security > RADIUS-client**.

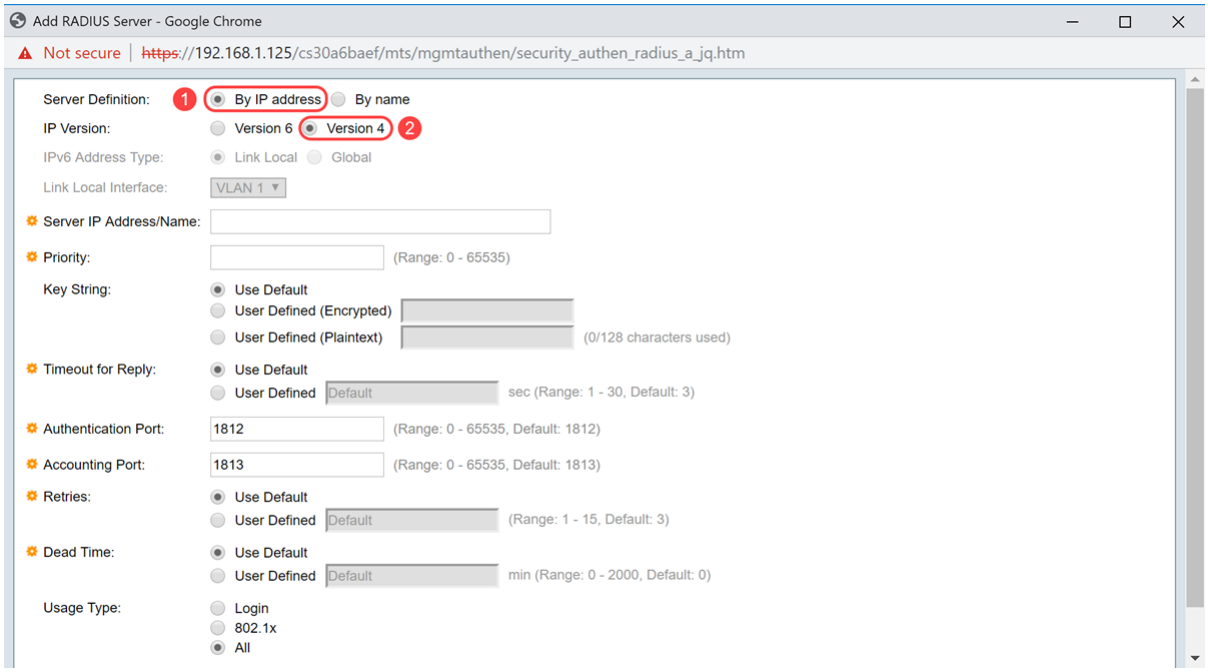


Stap 3. Scrolt naar het gedeelte *RADIUS-tabel* en klik op **Add...** om een RADIUS-server toe te voegen.



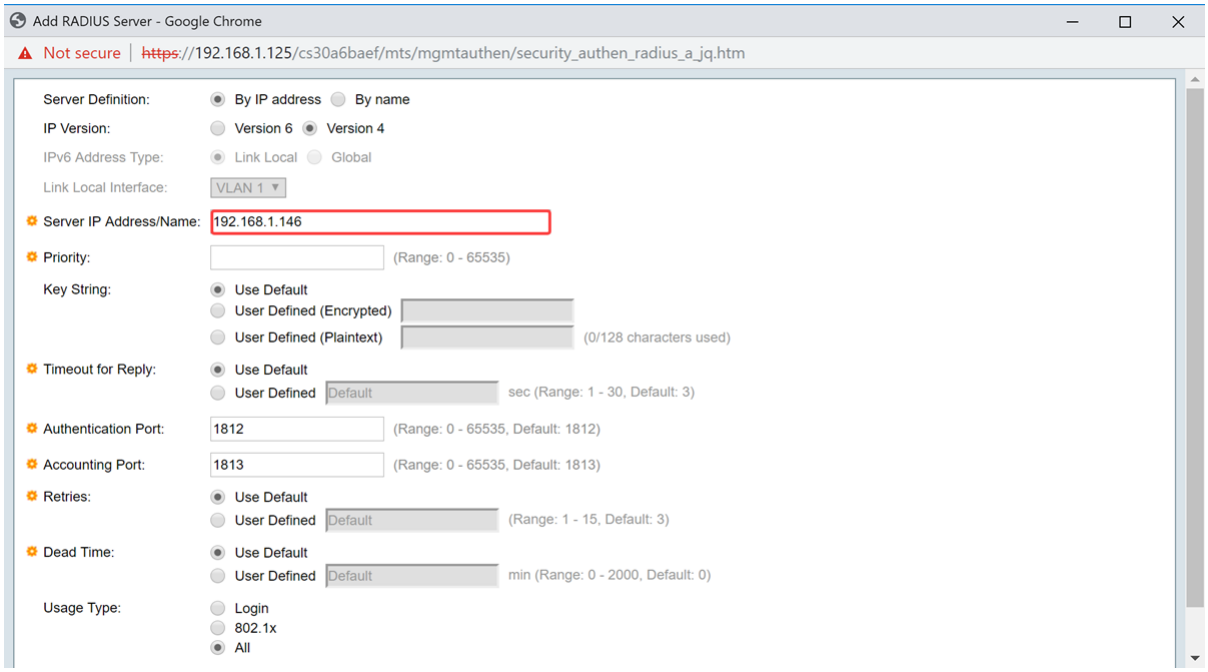
Stap 4. Selecteer of u de RADIUS-server wilt specificeren per IP-adres of naam in het veld *Server Definition*. Selecteer de versie van het IP-adres van de RADIUS-server in het veld *IP-versie*.

Opmerking: We zullen **per IP-adres** en **versie 4** in dit voorbeeld gebruiken.

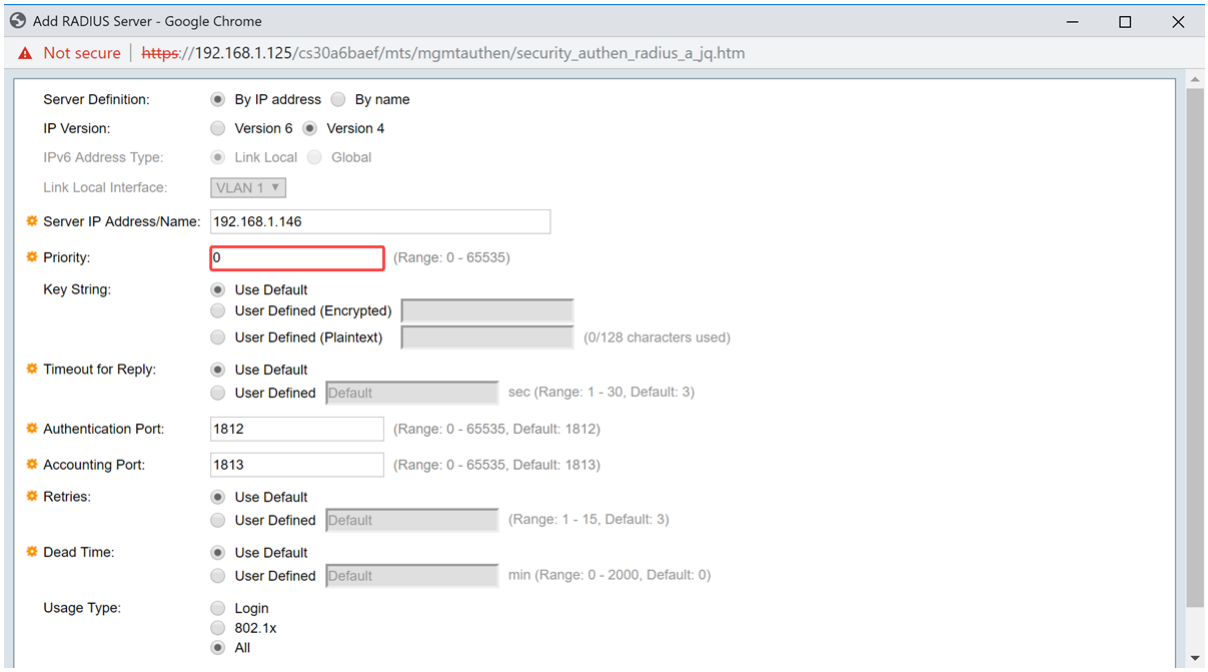


Stap 5. Voer in de RADIUS-server in via IP-adres of -naam.

Opmerking: We voeren het IP-adres van **192.168.1.146** in het veld *IP-adres/naam van de server in*.



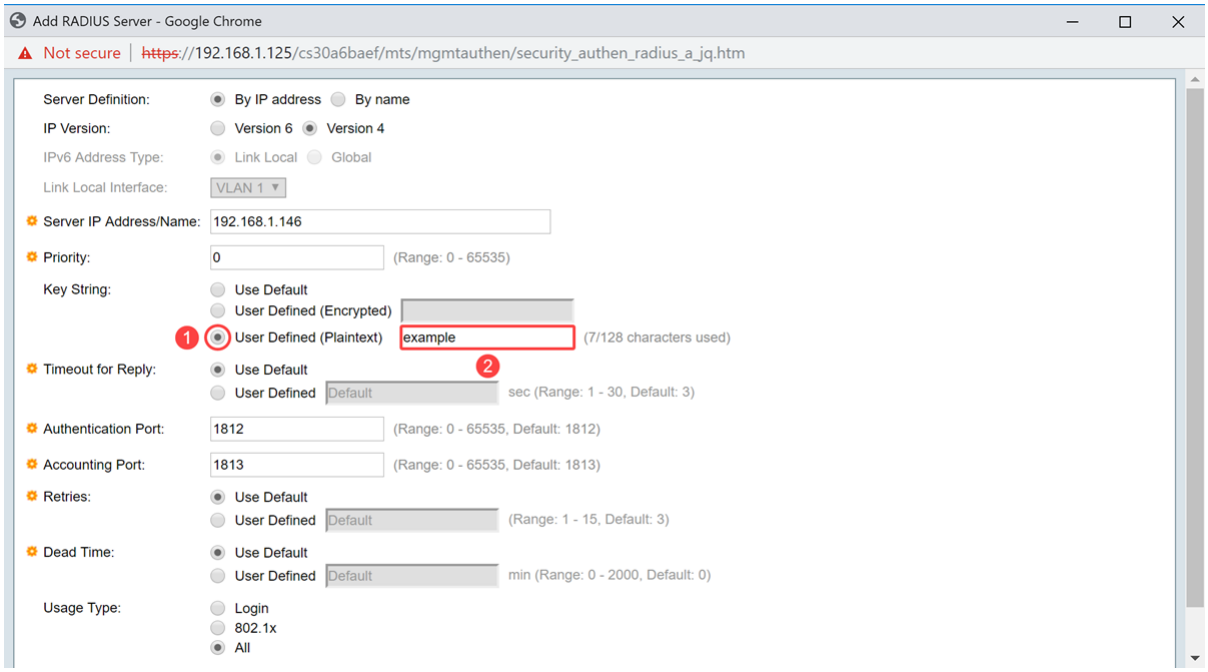
Stap 6. Voer de prioriteit van de server in. De prioriteit bepaalt de volgorde waarin het apparaat probeert om contact op te nemen met de servers om een gebruiker te authentiseren. Het apparaat start eerst met de hoogste prioriteit RADIUS-server. 0 is de hoogste prioriteit.



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.

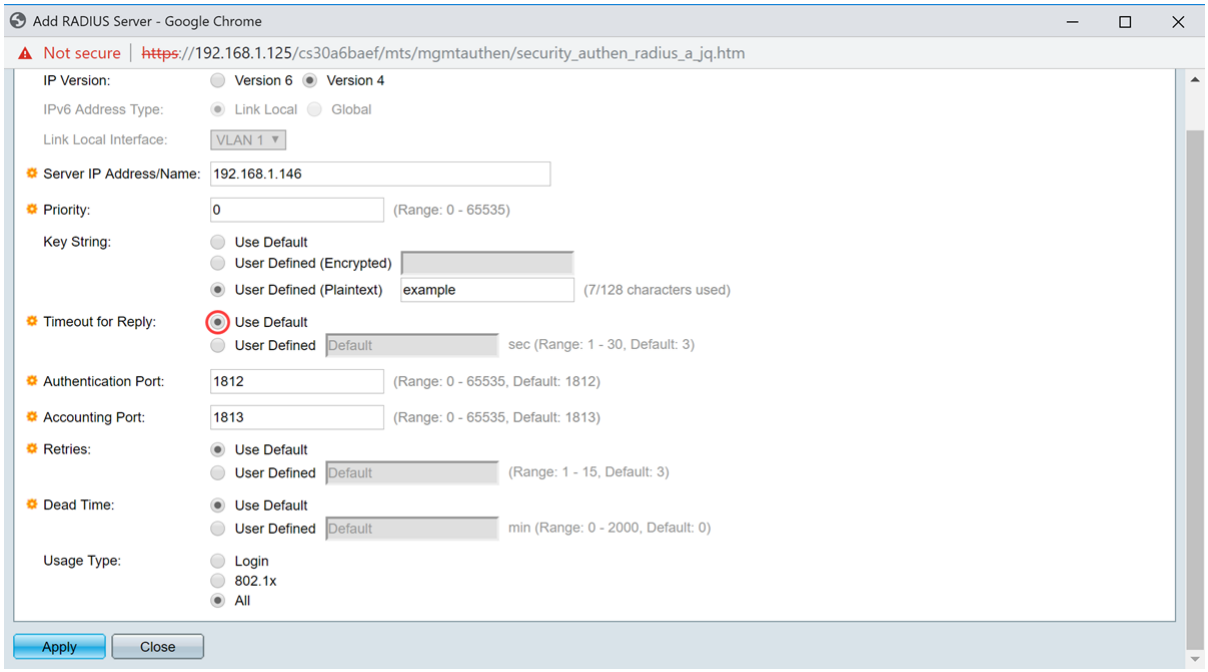
Opmerking: We zullen de **door gebruiker gedefinieerde (Plaintext)** gebruiken en in het belangrijke **voorbeeld** invoeren.

Klik hier voor informatie over het configureren van de RADIUS-serverinstellingen op de schakelaar.



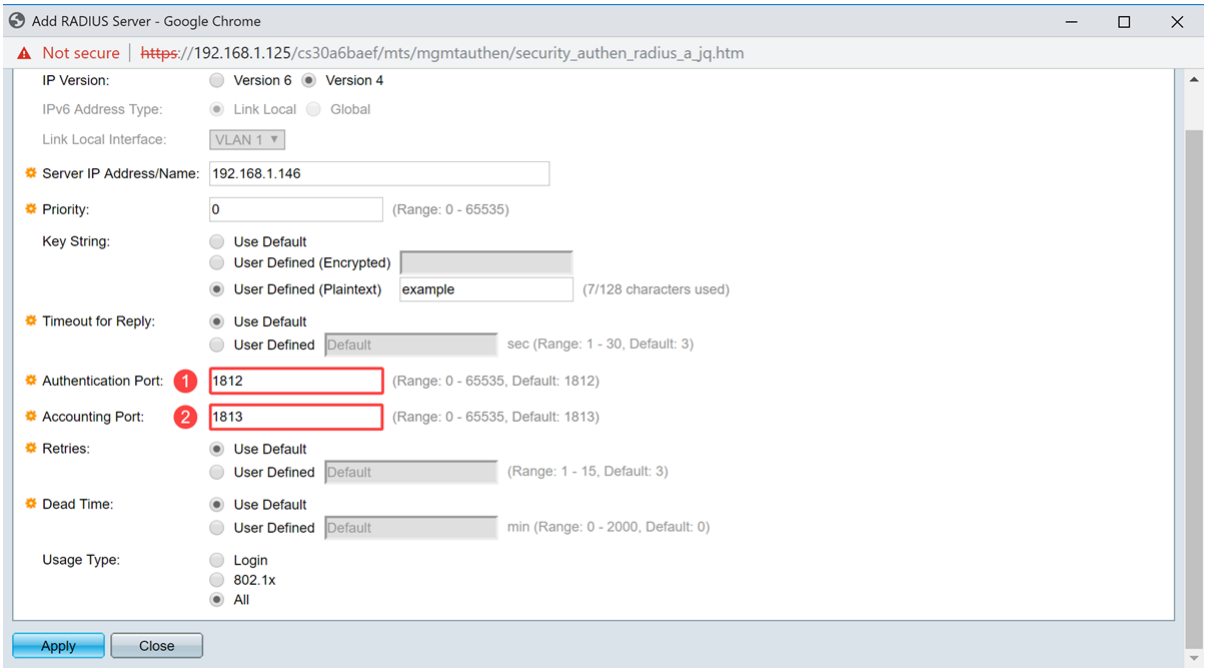
Stap 8. Selecteer in het veld *Time-out voor antwoorden* de optie **Standaard** of **door de gebruiker gedefinieerde** optie. Als **Gebruiker Defined** werd geselecteerd, voer het aantal seconden in dat het apparaat op een antwoord van de RADIUS-server wacht alvorens de query opnieuw uit te proberen, of schakel naar de volgende server als het maximale aantal herhalingen heeft plaatsgevonden. Als **Standaard** wordt **gebruikt**, gebruikt het apparaat de standaardwaarde voor de tijd.

Opmerking: In dit voorbeeld is **Default** geselecteerd.



Stap 9. Voer het UDP-poortnummer van de RADIUS-serverpoort in voor een verificatieaanvraag in het veld *Verificatiepoort*. Voer het UDP-poortnummer van de RADIUS-serverpoort in voor accounting verzoeken in het veld *Accounting Port*.

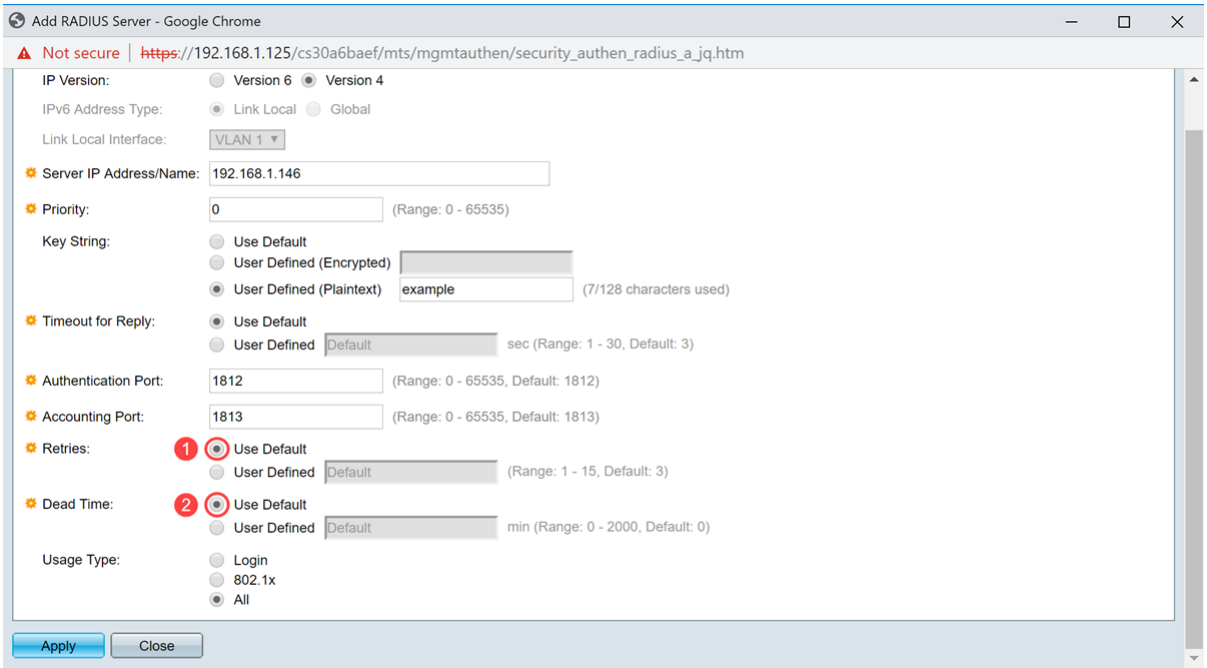
Opmerking: In dit voorbeeld gebruiken we de standaardwaarde voor zowel de authenticatiepoort als de accounting poort.



Stap 10. Als **User Defined** is geselecteerd voor het veld *Retries*, specificeert u het aantal verzoeken dat naar de RADIUS-server is verzonden voordat er een storing wordt geacht te zijn opgetreden. Als **Default** is geselecteerd, gebruikt het apparaat de standaardwaarde voor het aantal meldingen.

Als de **door gebruiker gedefinieerde** is geselecteerd voor *Dode Time*, moet u het aantal minuten invoeren dat moet doorgeven voordat een niet-reagerende RADIUS-server wordt omzeild voor serviceaanvragen. Als **Standaard** is **gebruikt** het apparaat de standaardwaarde voor de dode tijd. Als je 0 minuten binnenkwam, is er geen dode tijd.

Opmerking: In dit voorbeeld selecteren we **Default** voor beide velden.

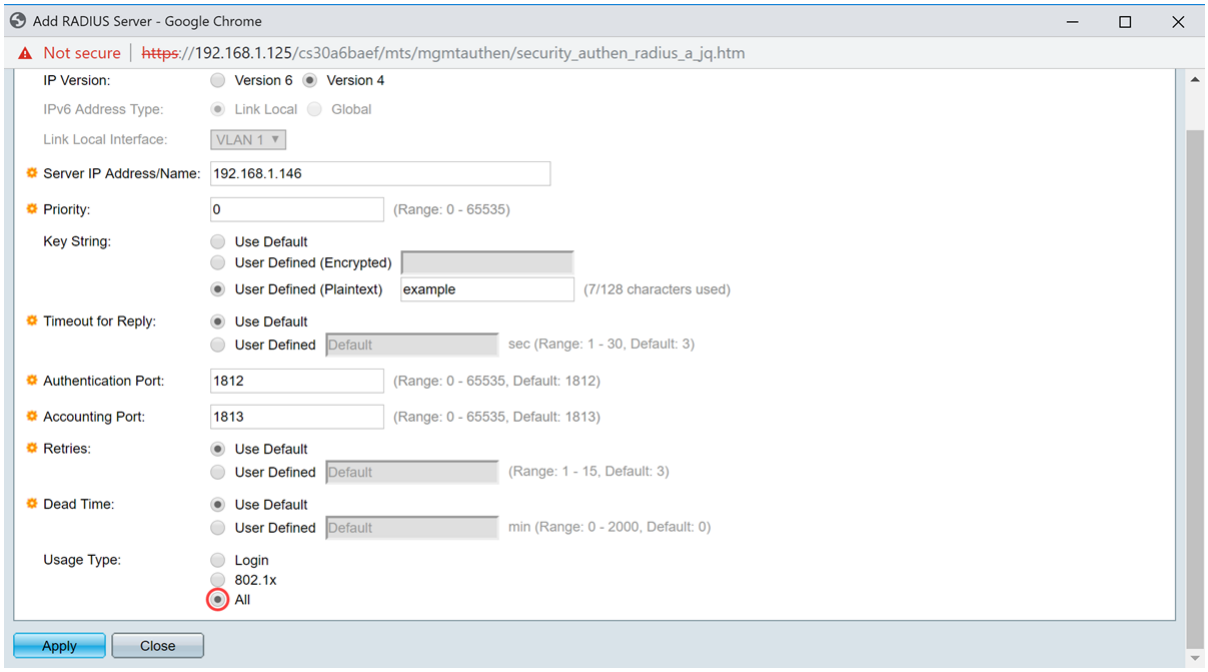


Stap 11. Voer in het veld *Gebruikstype* in het type RADIUS-serververificatie. De opties zijn:

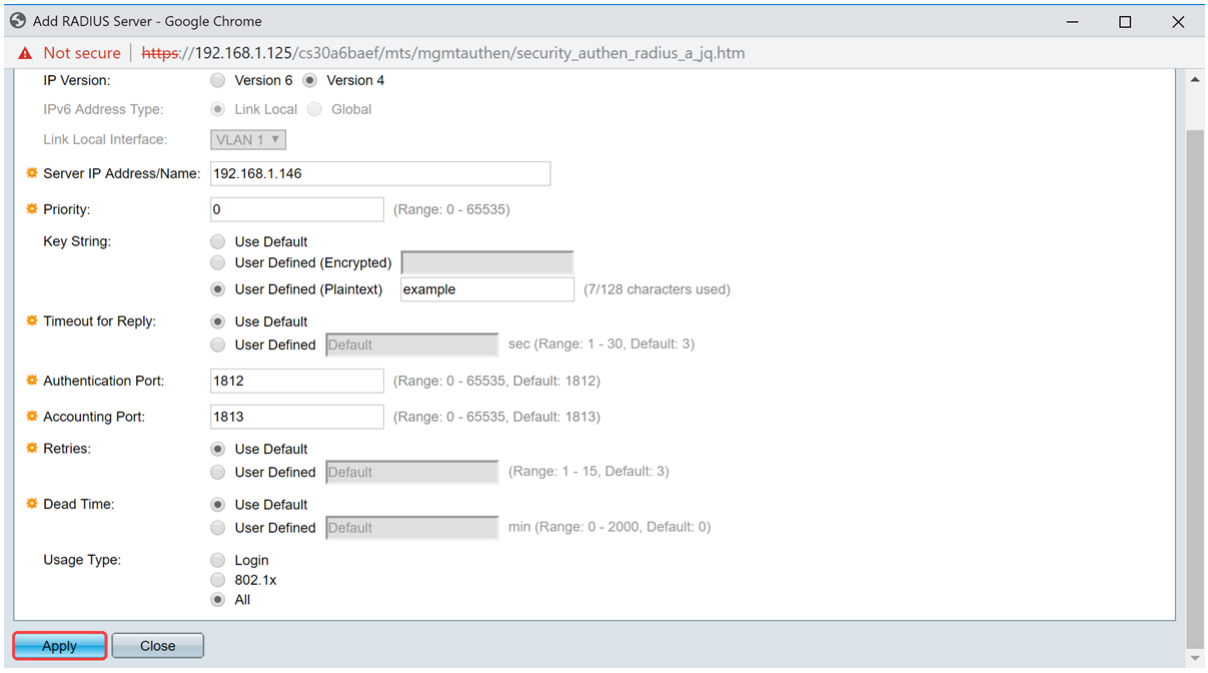
Aanmelden - De RADIUS-server wordt gebruikt voor het authenticeren van gebruikers die om het apparaat vragen.

802.1x - RADIUS-server wordt gebruikt voor 802.1x-verificatie.

All - RADIUS-server wordt gebruikt voor het authentificeren van gebruiker die om het apparaat en voor 802.1x-verificatie vraagt.



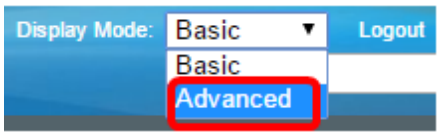
Stap 12. Klik op **Toepassen**.



Instellen 802.1x-poortverificatie-instellingen

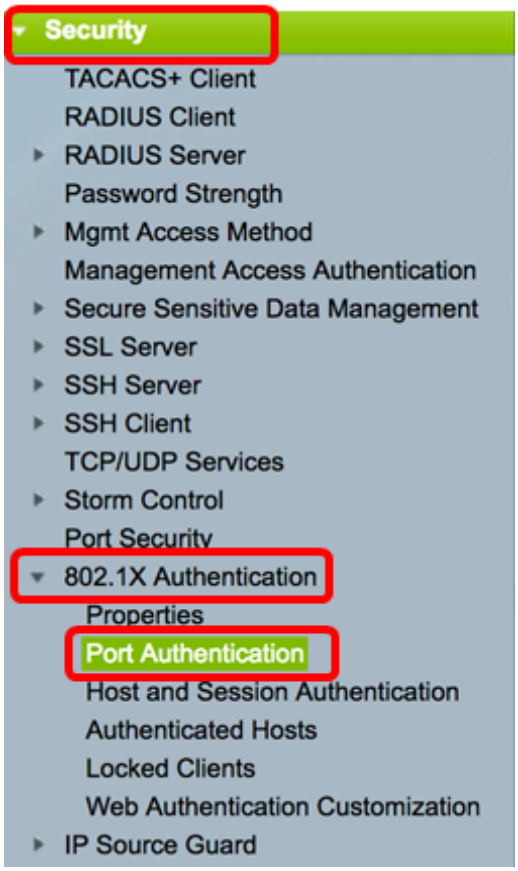
Stap 1. Meld u aan bij het op web gebaseerde hulpprogramma van uw switch en kies vervolgens **Geavanceerd** in de vervolgkeuzelijst Weergavemodus.

Opmerking: De beschikbare menu-opties kunnen afhankelijk van het apparaatmodel verschillen. In dit voorbeeld wordt SG350X-48MP gebruikt.



Opmerking: Als u een SX300- of SX500 Series-switch hebt, slaat u over naar Stap 2.

Stap 2. Kies **Security > 802.1X verificatie > Port-verificatie**.

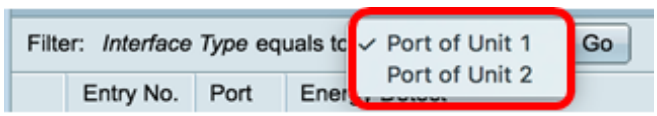


Stap 3. Kies een interface uit de vervolgkeuzelijst *Interfacetype*.

Port - Van de vervolgkeuzelijst *Interfacetype*, kies **Port** als u slechts één poort hoeft te selecteren.

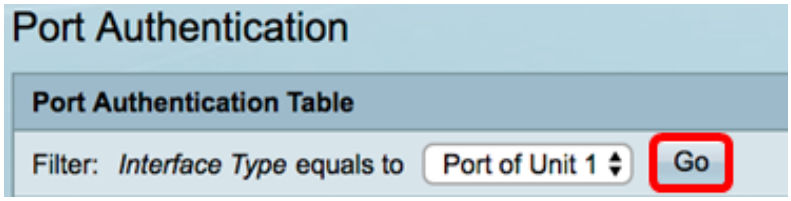
LAG — Kies in de vervolgkeuzelijst *Interfacetype* de LAG die u wilt configureren. Dit beïnvloedt de groep havens die in de configuratie van de LAG wordt gedefinieerd.

Opmerking: In dit voorbeeld wordt de Port of Unit 1 gekozen.

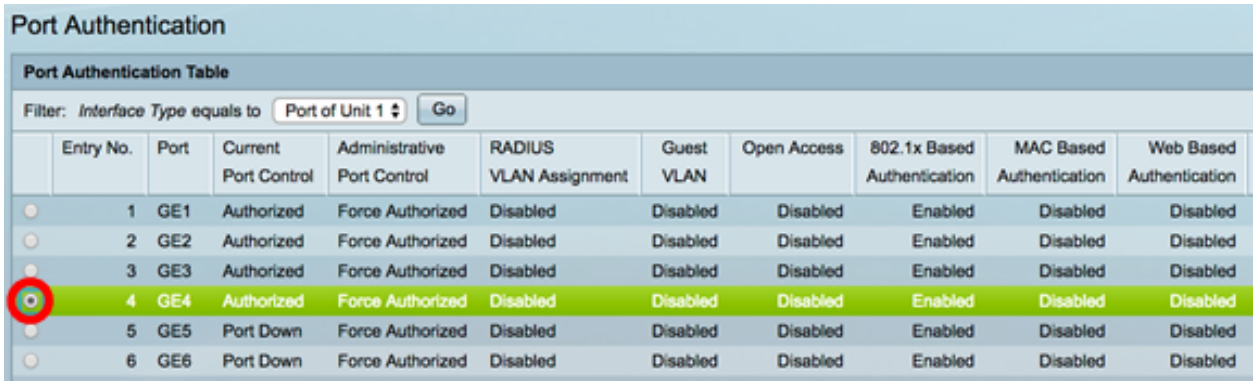


Opmerking: Als u een niet-stapelbare switch hebt zoals een SX300 Series-switch, slaat u de overtrek over naar Stap 5.

Stap 4. Klik op **Ga** om een lijst met poorten of LAG's op de interface te uploaden.



Stap 5. Klik op de poort die u wilt configureren.



Opmerking: In dit voorbeeld wordt GE4 gekozen.

Stap 6. Scrolt neer de pagina en klik op **Bewerken**.

Stap 7. (Optioneel) Als u een andere interface wilt bewerken, kiest u uit de vervolgkeuzelijsten Eenheid en Port.

Opmerking: In dit voorbeeld wordt poort GE4 van eenheid 1 geselecteerd.

Stap 8. Klik op de radioknop die overeenkomt met de gewenste poortcontrole in het beheergebied van poortcontrole. De opties zijn:

Macht onbevoegd — Ontkent de interface toegang door de haven in de onbevoegde staat te verplaatsen. De haven zal verkeer weggooien.

Auto — De haven beweegt tussen een geautoriseerde of niet-geautoriseerde staat op basis van de echtheidscontrole van de aanvrager.

Macht goedgekeurd — geeft toestemming voor de haven zonder echtheidscontrole. De haven zal verkeer door sturen.

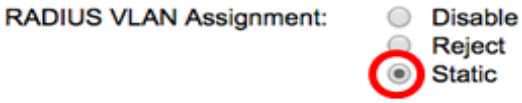
Opmerking: In dit voorbeeld wordt Auto geselecteerd.

Stap 9. Klik op een radioknop van RADIUS VLAN-toewijzing om de dynamische VLAN-toewijzing op de geselecteerde poort te configureren. De opties zijn:

Uitschakelen — Functie is niet ingeschakeld.

Afwijzen — Als de RADIUS-server de aanvrager toestemming heeft gegeven, maar geen VLAN heeft opgegeven, wordt de aanvrager afgewezen.

Statisch — Als de RADIUS-server de aanvrager toestemming heeft gegeven maar geen aanleverend VLAN heeft geleverd, wordt de aanvrager geaccepteerd.



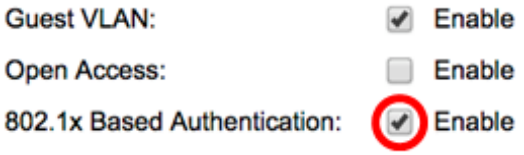
Opmerking: In dit voorbeeld wordt Static geselecteerd.

Stap 10. Controleer het aanvinkvakje Guest VLAN in om Guest VLAN in te schakelen voor onbevoegde poorten. Gast VLAN maakt de onbevoegde poort automatisch tot het VLAN toetreden dat in het gebied van de Gast VLAN ID van de 802.1 eigenschappen is geselecteerd.

Stap 1. (Optioneel) Controleer het vakje Toegang openen **inschakelen** om open toegang mogelijk te maken. Open Access helpt u de configuratieproblemen van hosts te begrijpen die met het netwerk verbonden zijn, controleert slechte situaties en stelt deze problemen in staat om vast te zetten.

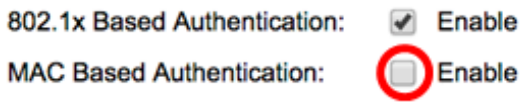
Opmerking: Wanneer Open Access op een interface is ingeschakeld, behandelt de switch alle fouten die van een RADIUS-server zijn ontvangen als successen en geeft hij toegang tot het netwerk voor stations die zijn aangesloten op interfaces, ongeacht de resultaten van de verificatie. In dit voorbeeld wordt Open Access uitgeschakeld.

Stap 12. Controleer de optie 802.1x gebaseerde verificatie **inschakelen** om verificatie op de poort op 802.1X mogelijk te maken.



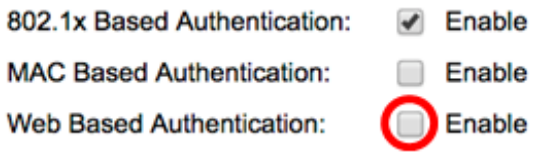
Stap 13. Controleer het selectieteken MAC **inschakelen** om poortverificatie mogelijk te maken op basis van het opgegeven MAC-adres. Slechts acht MAC-gebaseerde authenticaties kunnen in de poort worden gebruikt.

Opmerking: Om te slagen moet de MAC-verificatie van de RADIUS-server voorzien van een gebruikersnaam en een wachtwoord zijn: het opgegeven MAC-adres. Het MAC-adres moet in kleine letters zijn en zonder het wachtwoord zijn ingevoerd. of - scheidingstekens (zoals 0020aa00bbcc).



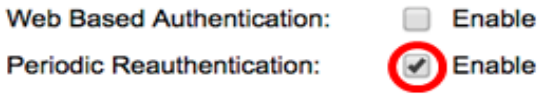
Opmerking: In dit voorbeeld is MAC-gebaseerde verificatie uitgeschakeld.

Stap 14. Controleer het aanvinkvakje Webgebaseerde verificatie **inschakelen** om op het web gebaseerde verificatie op de switch mogelijk te maken. In dit voorbeeld is op internet gebaseerde authenticatie uitgeschakeld.



Opmerking: In dit voorbeeld is op internet gebaseerde authenticatie uitgeschakeld.

Stap 15. (Optioneel) Controleer het aanvinkvakje Periodieke herkenning **inschakelen** om de poort na een bepaalde tijd opnieuw te bevestigen. Deze tijd wordt gedefinieerd in het veld *Reauthenticatieperiode*.

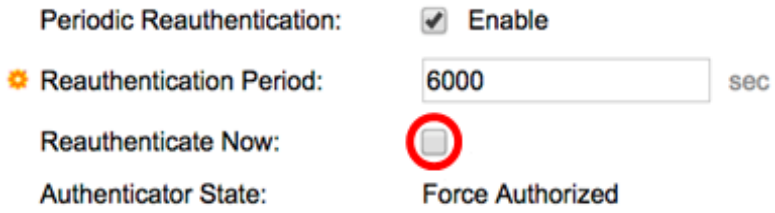


Opmerking: In dit voorbeeld is herauthenticatie van de periode ingeschakeld.

Stap 16. (Optioneel) Voer een waarde in het veld *Verificatieperiode in*. Deze waarde vertegenwoordigt de hoeveelheid seconden voordat de interface de poort opnieuw echt maakt. De standaardwaarde is 3600 seconden en het bereik loopt van 300 tot 4294967295 seconden.

Opmerking: In dit voorbeeld wordt 6000 seconden ingesteld.

Stap 17. (Optioneel) Controleer het aanvinkvakje Nu **activeren** om een onmiddellijke poort opnieuw te bevestigen. In dit voorbeeld is onmiddellijke herauthenticatie uitgeschakeld.



Het Statusgebied van de Authenticator toont de machtigingsstaat van de haven.

Stap 18. (Optioneel) Controleer het aanvinkvakje Tijdbereik **inschakelen** om een limiet op de tijd dat de poort is geautoriseerd, in te schakelen.

Opmerking: In dit voorbeeld wordt het bereik van de tijd ingeschakeld. Als u deze functie liever niet overslaat, gaat u naar Stap 20.

Stap 19. (Optioneel) Kies in de vervolgkeuzelijst Naam tijdbereik een tijdbereik om te gebruiken.

Opmerking: In dit voorbeeld wordt Dayshift gekozen.

Stap 20. Klik in het gedeelte Maximum aantal WBA-inlogmeldingen op Infinite voor geen limiet of door de gebruiker gedefinieerd om een limiet in te stellen. Als de door de gebruiker gedefinieerde optie is geselecteerd, voert u het maximale aantal inlogpogingen in dat is toegestaan voor op het web gebaseerde verificatie.

Opmerking: In dit voorbeeld wordt Infinite gekozen.

Stap 21. Klik in het gebied met de maximale WBA-tijd op Infinite voor geen limiet of door de gebruiker gedefinieerd om een limiet in te stellen. Als de door de gebruiker gedefinieerde definitie is gekozen, specificeert u de maximale lengte van de stille periode voor op het web gebaseerde verificatie die op de interface is toegestaan.

Opmerking: In dit voorbeeld wordt Infinite gekozen.

Stap 2. In het gebied Max Hosts, klik op Infinite voor geen limiet of door gebruiker gedefinieerde om een limiet in te stellen. Als de door gebruiker gedefinieerde selectie is geselecteerd, specificeert u het maximale aantal geautoriseerde hosts dat op de interface is toegestaan.

Opmerking: Stel deze waarde in op 1 om single-host modus te simuleren voor web-gebaseerde verificatie in multi-sessiemodus. In dit voorbeeld wordt Infinite gekozen.

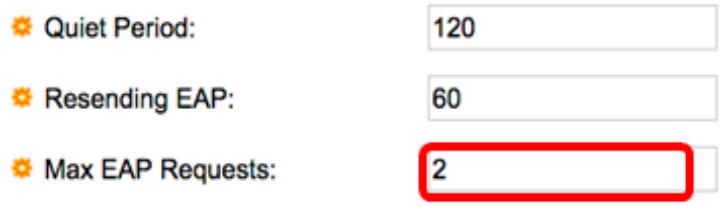
Stap 23. Voer in het veld *Quiet Period* de tijd in dat de switch in stille toestand blijft na een mislukte authenticatie-uitwisseling. Wanneer de schakelaar in rustige staat is, betekent het dat de schakelaar niet naar nieuwe authentificatieverzoeken van de cliënt luistert. De standaardwaarde is 60 seconden en het bereik is van één tot 65535 seconden.

Opmerking: In dit voorbeeld wordt de stille periode ingesteld op 120 seconden.

Stap 24. Voer in het veld *Resending EAP* de tijd in waarop de switch wacht op een antwoordbericht van de aanvrager voordat hij een verzoek doorgeeft. De standaardwaarde is 30 seconden en het bereik is van één tot 6535 seconden.

Opmerking: In dit voorbeeld wordt het doorlopen van EAP ingesteld op 60 seconden.

Stap 25. In het veld *MAP-aanvragen* vermeldt u het maximale aantal MAP-verzoeken dat kan worden verstuurd. EAP is een in 802.1X gebruikte authenticatiemethode die informatie-uitwisseling tussen de switch en de cliënt over authenticatie mogelijk maakt. In dit geval worden MAP-verzoeken naar de cliënt gestuurd voor echtheidscontrole. De cliënt moet dan reageren en de authenticatieinformatie matchen. Indien de cliënt niet reageert, wordt een ander MAP-verzoek ingesteld op basis van de terugkerende MAP-waarde en wordt het verificatieproces hervat. De standaardwaarde is 2 en het bereik is van 1 tot 10.



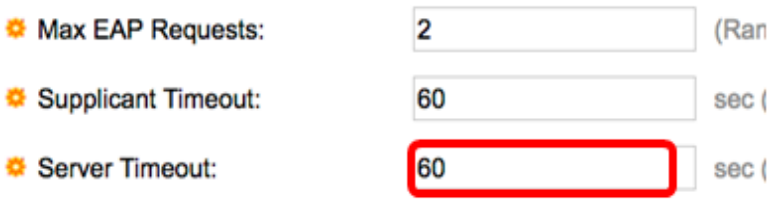
Opmerking: In dit voorbeeld wordt de standaardwaarde van 2 gebruikt.

Stap 26. In het veld *Leverancier Time-out* voert u de tijd in voordat de MAP-verzoeken aan de aanvrager worden gericht. De standaardwaarde is 30 seconden en het bereik is van één tot 6535 seconden.

Opmerking: In dit voorbeeld wordt de pluizend tijd ingesteld op 60 seconden.

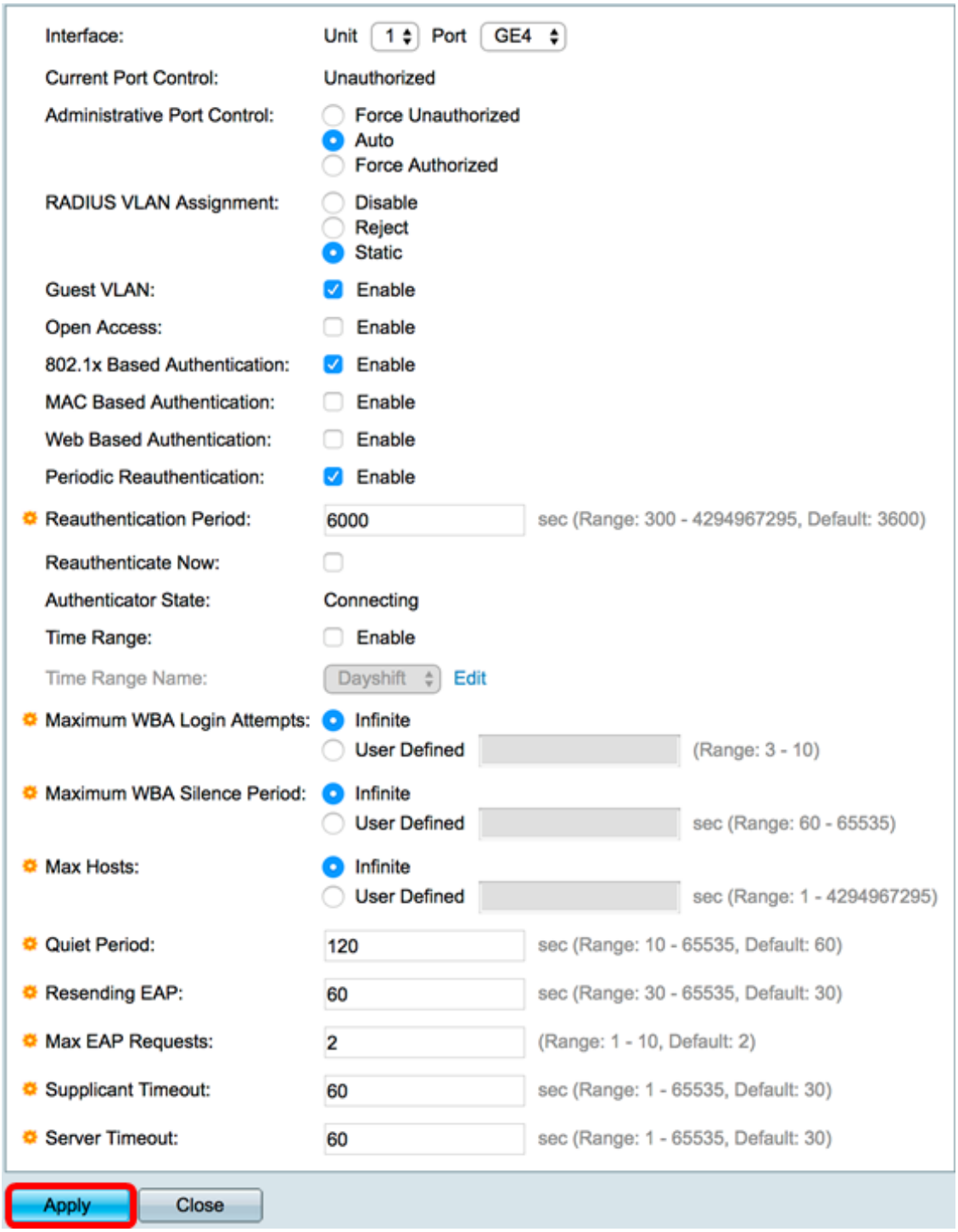
Stap 27. In het veld *Time-out voor servers* specificeert u de tijd die verloopt voordat de

switch een verzoek opnieuw naar de RADIUS-server stuurt. De standaardwaarde is 30 seconden en het bereik is van één tot 6535 seconden.

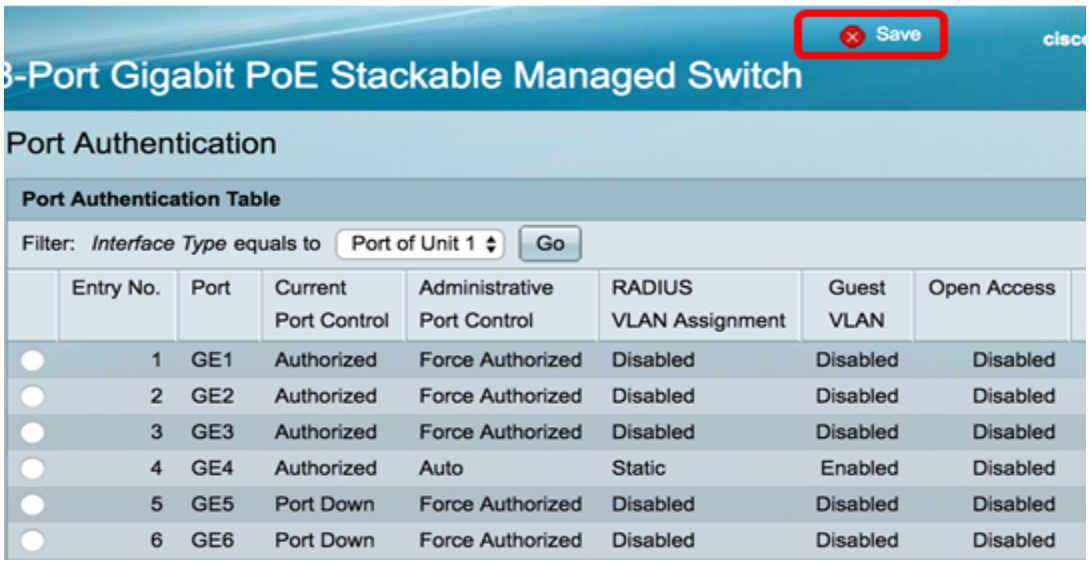


Opmerking: In dit voorbeeld wordt de server timeout ingesteld op 60 seconden.

Stap 2. Klik op **Toepassen** en vervolgens op **Sluiten**.



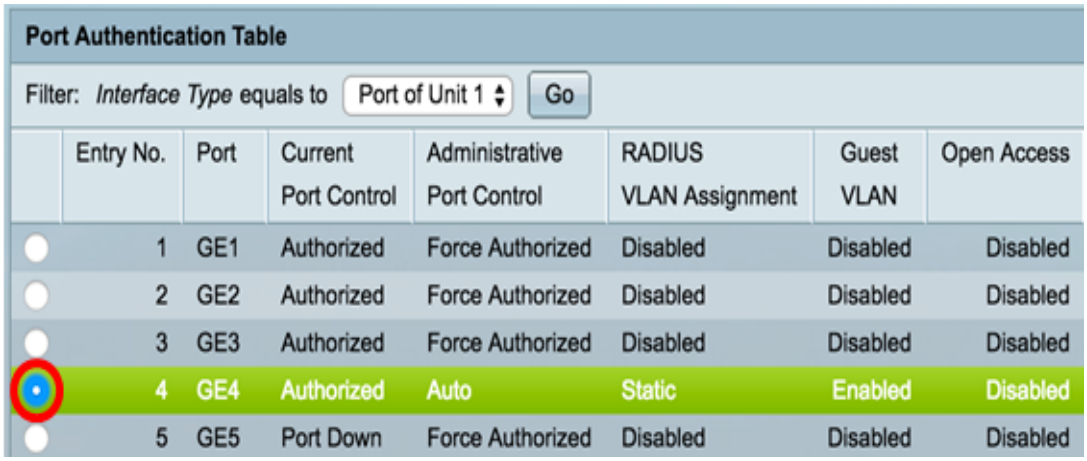
Stap 29. (Optioneel) Klik op **Opslaan** om instellingen op te slaan in het opstartconfiguratiebestand.



U had nu met succes de 802.1x instellingen voor poortverificatie op uw switch moeten configureren.

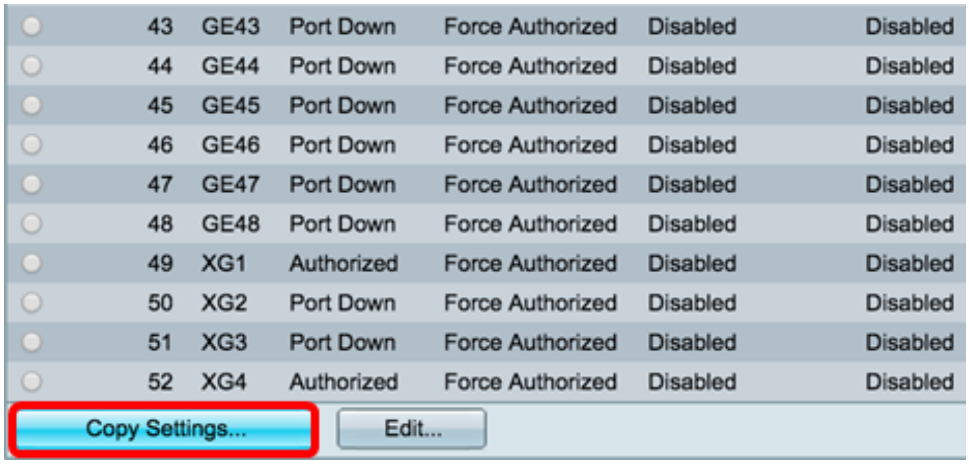
Instellingen interfaceconfiguratie op meerdere interfaces toepassen

Stap 1. Klik op de radioknop van de interface die u de authenticatie configuratie op meerdere interfaces wilt toepassen.



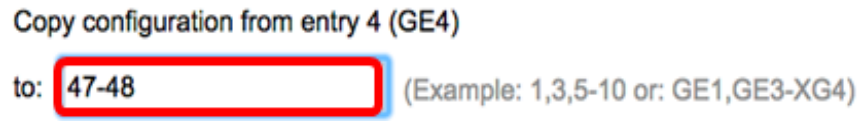
Opmerking: In dit voorbeeld wordt GE4 gekozen.

Stap 2. Scrolt neer en klik op **Instellingen kopiëren**.



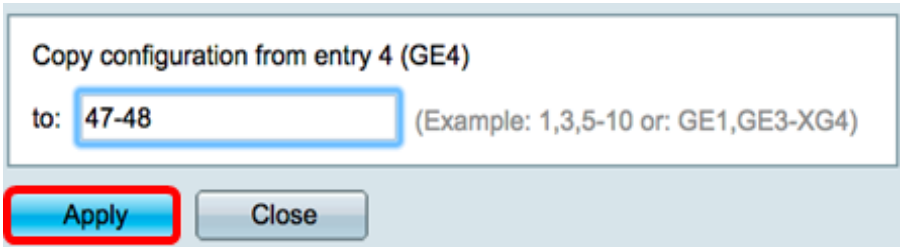
Stap 3. In het veld *naar*, specificeert u het bereik van de interfaces dat u de configuratie van

de gekozen interface wilt toepassen. U kunt de interfacenummers of de naam van de interfaces als invoer gebruiken. U kunt elke interface invoeren die wordt gescheiden door een komma (zoals 1, 3, 5 of GE1, GE3, GE5) of u kunt een reeks interfaces invoeren (zoals 1-5 of GE1-GE5).

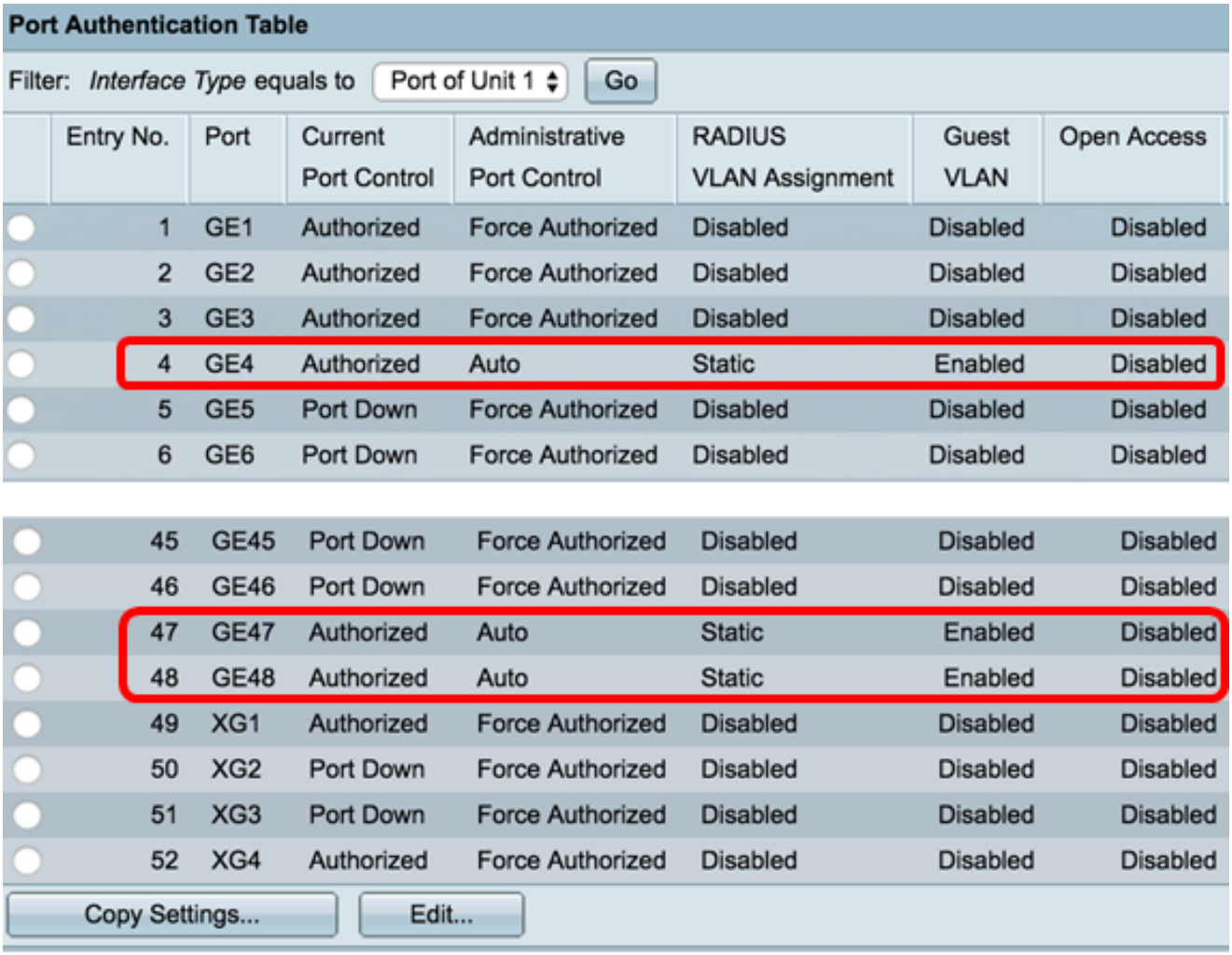


Opmerking: In dit voorbeeld zullen de configuratie instellingen worden toegepast op poorten 47 tot 48.

Stap 4. Klik op **Toepassen** en vervolgens op **Sluiten**.



In het onderstaande beeld worden de wijzigingen na de configuratie weergegeven.



U had nu met succes de 802.1x authenticatie instellingen van één poort moeten hebben gekopieerd en toegepast op andere poort of poorten op uw switch.