

RADIUS-configuratie op de 200/300 Series beheerde Switches

Doel

Remote Authorisation Dial-In User Service (RADIUS) is een beveiligingsservice die wordt gebruikt voor de verificatie van gebruikers in netwerken met een gecentraliseerde beveiligingsarchitectuur. De 200/300 Series beheerde Switches kunnen fungeren als een RADIUS-client in uw netwerk en, in combinatie met een RADIUS-server, kunt u een gecentraliseerd systeem opzetten voor verificatie van gebruikers in uw netwerk. In dit artikel wordt uitgelegd hoe u een RADIUS-server kunt configureren en verificatiemethoden kunt toepassen op de 200/300 Series beheerde Switches.

Toepasselijke apparaten | Softwareversie

- SF/SG 200 Series - 1.2.9.x
- SF/SG 300 Series - 1.2.9.x

Standaardconfiguratie RADIUS

Deze sectie begeleidt u door de standaardconfiguratie van een RADIUS-server. Deze standaardwaarden kunnen worden gebruikt voor elke RADIUS-server die u aan een switch wilt toevoegen.

Stap 1

Log in op het hulpprogramma voor webconfiguratie en kies **Beveiliging > RADIUS**. De pagina *RADIUS* wordt geopend:

RADIUS

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

Use Default Parameters

IP Version: Version 6 Version 4

Retries: (Range: 1 - 10, 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)

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.									

De afbeeldingen in dit artikel zijn van een SG300 model switch.

Stap 2

Klik in het veld RADIUS-accounting op een van de volgende opties:

- Poortgebaseerde toegangscontrole (802.1x, MAC-gebaseerd) - voor gebruik van de RADIUS-server voor 802.1x-poortaccounting.
- Management Access - voor gebruik van de RADIUS-server voor login accounting.
- Zowel poortgebaseerde toegangscontrole als beheertoegang - voor gebruik van de RADIUS-server voor zowel 802.1x- als inlogaccounting.
- Geen - De RADIUS-server niet gebruiken voor boekhouddoeleinden.

Radius Accounting is niet beschikbaar op de SG200 reeks switches.

Stap 3

In de sectie Standaardparameters gebruiken, voert u in het veld Opnieuw proberen het aantal keren in dat de switch opnieuw probeert om de RADIUS-server te verifiëren.

Stap 4

Voer in het veld Time-out voor antwoord de tijd in seconden in voor elke verificatiepoging op de RADIUS-server.

Stap 5

Voer in het veld Tijd dode de tijd in minuten in voordat de switch een niet-reagerende RADIUS-server dood verklaart en verhuist naar de volgende beschikbare server voor verbinding.

Stap 6

Voer in het veld Toetsenreeks de sleutel in die wordt gebruikt voor verificatie en codering tussen de switch en de RADIUS-server. Deze sleutel moet overeenkomen op zowel de RADIUS-server als de switch. Klik op een van de volgende opties:

- Versleuteld - Als u een versleutelde sleutel van een ander apparaat hebt, voert u de sleutel in.
- Plaintext - Als u geen versleutelde sleutel van een ander apparaat hebt, voert u de sleutel in als onbewerkte tekst.

Stap 7

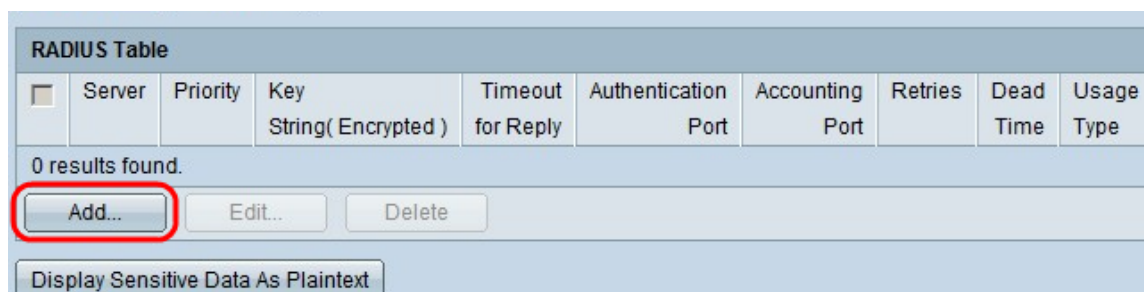
Klik op **Toepassen** om deze standaardwaarden op te slaan en ze beschikbaar te maken voor een RADIUS-server.

Een RADIUS-server toevoegen/bewerken

In deze sectie wordt een stapsgewijze procedure gegeven die uitlegt hoe u een RADIUS-server kunt toevoegen of bewerken met een 200/300 Series beheerde Switch.

Stap 1

Log in op het hulpprogramma voor webconfiguratie en kies **Beveiliging > RADIUS**. De pagina *RADIUS* wordt geopend:



<input type="checkbox"/>	Server	Priority	Key String(Encrypted)	Timeout for Reply	Authentication Port	Accounting Port	Retries	Dead Time	Usage
0 results found.									
<input type="button" value="Add..."/> <input type="button" value="Edit..."/> <input type="button" value="Delete"/>									
<input type="button" value="Display Sensitive Data As Plaintext"/>									

Stap 2

Klik in het gedeelte RADIUS-tabel op **Toevoegen**. Het venster *Add Radius Server* verschijnt.

Als u een huidige RADIUS-server wilt bewerken, klikt u op **Bewerken** en bewerkt u de gewenste eigenschappen van de RADIUS-server.



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)

Stap 3

Klik in het veld Serverdefinitie op een van de volgende opties:

- Op naam - Als de RADIUS-server is gedefinieerd met een naam.
- Op IP-adres - als de RADIUS-server is gedefinieerd met een IP-adres.

Stap 4

Klik in het veld IP Version op **versie 6** of **versie 4** als het type IP-adres van de RADIUS-server.

Stap 5

Als **versie 6** in het IPv6-adrestype als IP-adres wordt gekozen, klikt u op een van de volgende opties:

- Link Local - Een IPv6-adres dat alleen hosts op één netwerklink identificeert.
- Wereldwijd - Een IPv6-adres dat via andere netwerken kan worden bereikt.

Stap 6

Als Link Local is gekozen als het IPv6-adrestype, kiest u in de vervolgkeuzelijst Link Local Interface de juiste interface.

Stap 7

Voer in het veld IP-adres/naam van server het IP-adres of de naam van de RADIUS-server in.

Stap 8

Voer in het veld Prioriteit de prioriteit in van de RADIUS-server die de switch zal gebruiken. De server met de hoogste prioriteit wordt het eerst in de switch gevraagd. Nul (0) geeft de hoogste prioriteit.

Stap 9

Klik in het veld Key String op een van de volgende opties:

- Standaard gebruiken - Hiermee gebruikt u de standaardtoets voor verificatie.
- Door gebruiker gedefinieerd (versleuteld) - Indien beschikbaar, voer de versleutelde sleutel in.
- Door gebruiker gedefinieerd (onbewerkte tekst) - Indien niet beschikbaar, voert u de toets in als onbewerkte tekst.

Stap 10

Klik in het veld Time-out voor antwoord op een van de volgende opties:

- Standaardwaarde gebruiken - De standaardwaarde gebruiken.
- Gebruiker gedefinieerd - Voer het aantal in seconden in dat de switch wacht op elke poging om verbinding te maken met de RADIUS-server.

Stap 11

Voer in het veld Verificatiepoort de UDP-poort in die de RADIUS-server gebruikt voor verificatie.

Stap 12

Voer in het veld Accounting Port de UDP-poort in die de RADIUS-server voor accounting gebruikt.

Stap 13

Klik in het veld Opnieuw proberen op een van de volgende opties:

- Standaardwaarde gebruiken - De standaardwaarde gebruiken.
- Door gebruiker gedefinieerd - Een andere waarde gebruiken. Voer het aantal pogingen in dat de switch uitvoert voordat een foutverbinding met de RADIUS-server geacht wordt te hebben plaatsgevonden.

Stap 14

Klik in het veld Dood tijd op een van de volgende opties:

- Standaardwaarde gebruiken - De standaardwaarde gebruiken.
- Door gebruiker gedefinieerd - Een andere waarde gebruiken. Geef de tijd op in minuten voordat de switch een niet-reagerende RADIUS-server dood verklaart en verhuist naar de volgende beschikbare server voor verbinding.

Stap 15

Klik in het veld Type gebruik op een van de volgende opties:

- Login - Verifieert de beheerders van de switch.
- 802.1x - De RADIUS-server controleert de beveiligingsreferenties van gebruikers die netwerktoegang aanvragen op basis van de 802.1x-regeling (PNAC-regeling) voor poortgebaseerde netwerktoegangscontrole.
- Alle - Hiervoor worden beide soorten verificatie gebruikt.

Stap 16

Klik op **Apply** (Toepassen).

RADIUS

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

Use Default Parameters

IP Version: Version 6 Version 4

Retries: (Range: 1 - 10, 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)

Stap 17

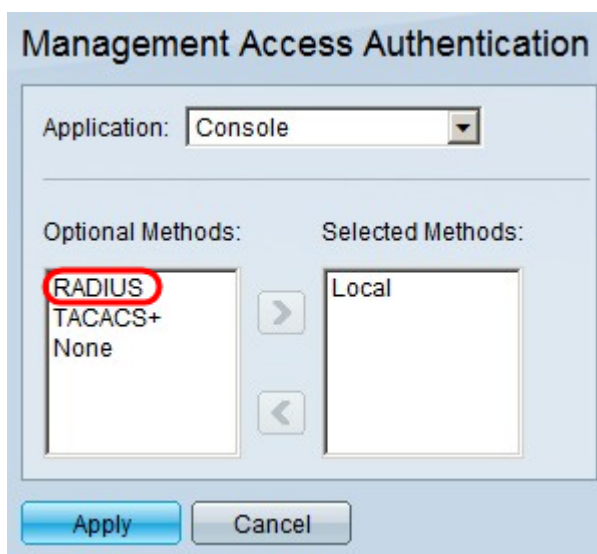
(Optioneel) Als u een RADIUS-server wilt verwijderen, schakelt u in het gedeelte RADIUS-tabel het aanvinkvakje in van de RADIUS-server die u wilt verwijderen en klikt u op **Verwijderen**.

RADIUS-verificatie

Zodra de RADIUS-server correct is geconfigureerd, moet u deze op de switch verifiëren. In deze sectie wordt uitgelegd hoe u een RADIUS-server op de 200/300 Series beheerde Switches kunt verifiëren.

Stap 1

Log in op het web configuratie hulpprogramma en kies **Security > Management Access Verification**. De pagina *Beheertoegangsverificatie* wordt geopend:



Management Access Authentication

Application: Console

Optional Methods: Selected Methods:

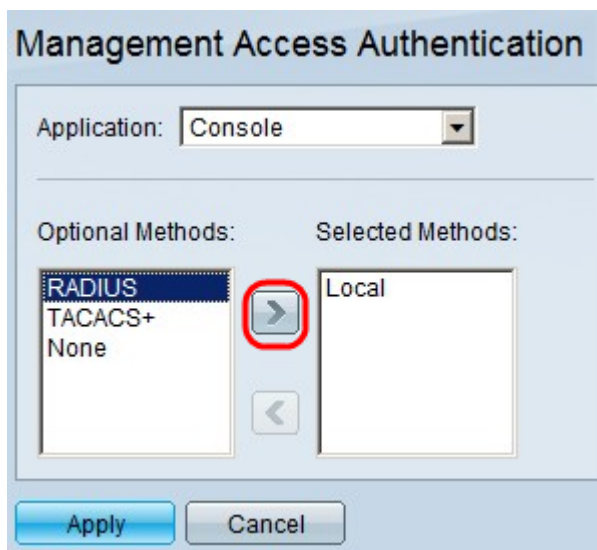
RADIUS
TACACS+
None

Local

Apply Cancel

Stap 2

Kies RADIUS in de lijst Optionele methoden.



Management Access Authentication

Application: Console

Optional Methods: Selected Methods:

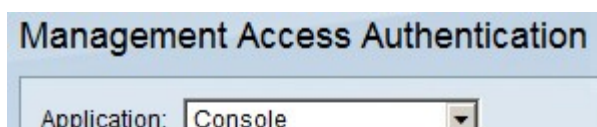
RADIUS
TACACS+
None

Local

Apply Cancel

Stap 3

Klik op de knop >.



Management Access Authentication

Application: Console

Stap 4

Klik op **Apply** (Toepassen).

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.