Configuratie van 802.1X-eigenschappen op de 200/300 Series beheerde Switches

Doel

De pagina *Properties* van de 802.1X IEEE-standaard in het Security gedeelte van de 200/300 Series beheerde Switches biedt verschillende mogelijkheden voor verificatie. De 802.1X IEEE-standaard maakt poortgebaseerde verificatie van gebruikers mogelijk. Een gebruiker in een bepaald netwerk met 802.1X ingeschakeld moet wachten op volledige verificatie om gegevens over het netwerk te verzenden. U kunt 802.1X inschakelen en de verificatiemethode voor poorten instellen. In dit artikel wordt uitgelegd hoe u de 802.1X-eigenschappen kunt configureren op de 200/300 Series beheerde Switches.

Toepasselijke apparaten

·SF/SG 200 en SF/SG 300 Series beheerde Switches

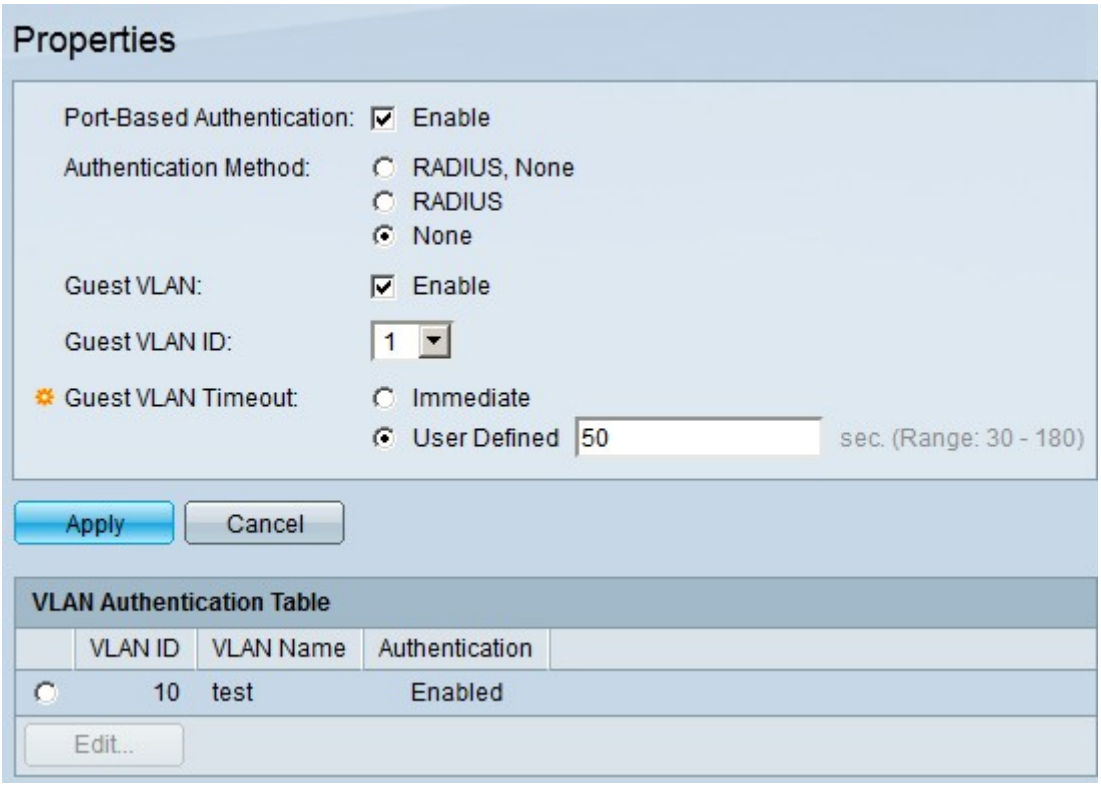
Softwareversie

•3.1.0.62

Configuratie 802.1X eigenschappen

Parameters voor 802.1X-eigenschappen definiëren

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies **Beveiliging > 802.1X > Eigenschappen.** De pagina *Eigenschappen* wordt nu geopend:



Stap 2. Als u poortgebaseerde 802.1x-verificatie wilt inschakelen, controleert u **Inschakelen** in het veld Poortgebaseerde verificatie.

Stap 3. Klik op het keuzerondje dat overeenkomt met de gewenste verificatiemethode in het veld Verificatiemethode. De beschikbare opties zijn:

·RADIUS, geen — Verifieer eerst met RADIUS-server. Als de RADIUS-server niet reageert, worden de aangesloten apparaten zonder verificatie toegestaan.

·RADIUS — Verifieer gebruikers alleen via een RADIUS-server. Als de RADIUS-server niet reageert, worden de services van gebruikers geweigerd.

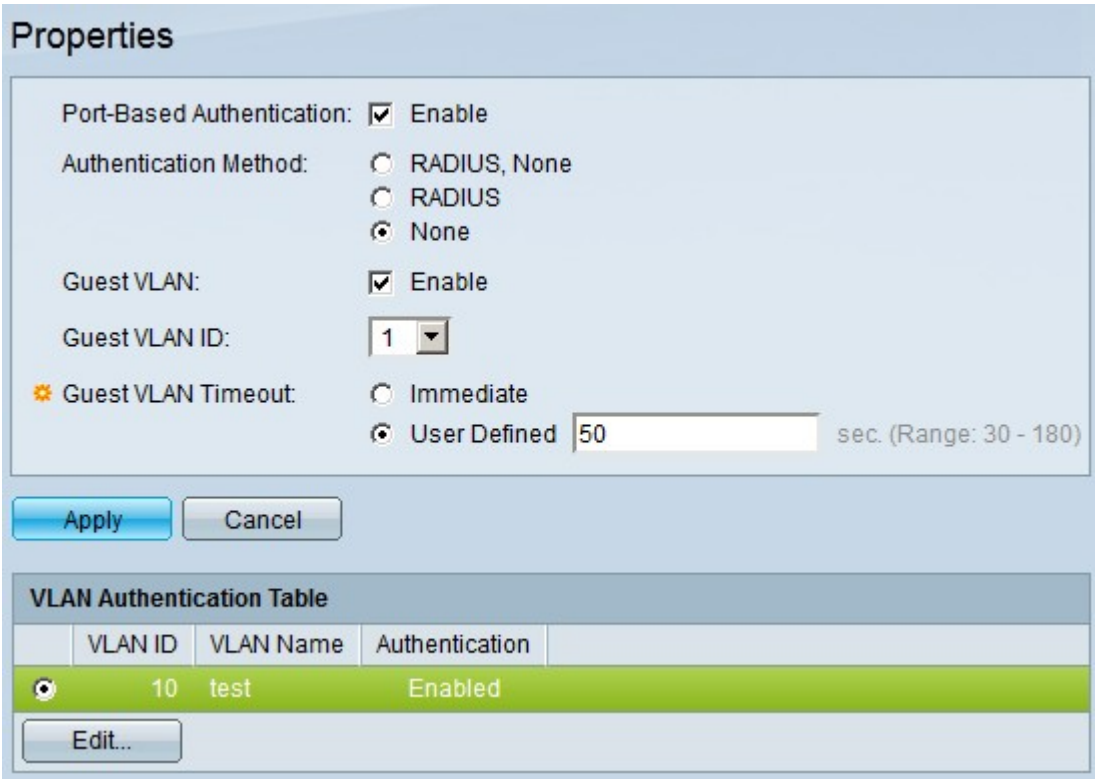
·Geen — Geen verificatie vereist voor gebruikers, alle gebruikers zijn toegestaan.

Stap 3. Klik op **Toepassen** om de configuratie op te slaan.

Configuratie van niet-geverifieerd VLAN

Een onbevoegde poort kan geen toegang tot een VLAN hebben tenzij dit VLAN de gast VLAN is. U kunt deze VLAN's verifiëren. Deze sectie verklaart hoe u VLAN's op de 200/300 Series beheerde Switches kunt verifiëren.

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies **Beveiliging > 802.1X > Eigenschappen.** De pagina *Eigenschappen* wordt nu geopend:



Stap 2. Klik onder de VLAN-verificatietabel op de radioknop van het VLAN dat u verificatie wilt inschakelen.

Stap 3. Klik op **Edit** (Bewerken). Het venster *Bewerken* verschijnt:

Stap 4. In het verificatieveld schakelt u het aanvinkvakje **Enable** in om verificatie van het gekozen VLAN in te schakelen.

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

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.