

# 802.1X configureren op SG300 Series-switches

## Doel

802.1X is een IEEE-standaard die poortgebaseerde verificatie implementeert. Als een haven 802.1X gebruikt, dan moet elke klant die die haven gebruikt (als de aanvrager genoemd) correcte geloofsbrieven voorleggen alvorens toegang tot het netwerk te krijgen. Een apparaat dat 802.1X implementeert (ook bekend als de authenticator) moet kunnen communiceren met een RADIUS-server (Remote Authentication Dial-In User Service) die elders op het netwerk is. Deze server bevat een lijst met geldige gebruikers die toegang tot het netwerk hebben; alle door de authenticator verzonden geloofsbrieven (die door de aanvrager worden verstrekt) moeten overeenkomen met die welke door de RADIUS-server worden bewaard. Zo ja, dan vertelt de server de authenticator om toegang te verlenen aan de gebruiker; anders zal de authenticator de toegang weigeren .

De 802.1X-standaard is een goede beveiligingsmaatregel om te voorkomen dat ongewenste gebruikers toegang krijgen tot het netwerk door ze aan te sluiten op een fysieke poort. Merk op dat een RADIUS-server, wil 802.1X kunnen werken, al elders op het netwerk moet zijn geconfigureerd en dat de authenticator ermee moet kunnen communiceren.

Dit document heeft tot doel u te laten zien hoe u 802.1X kunt instellen op de SG300 Series-switches.

## Toepasselijke apparaten

- SG300 Series-switches

## Softwareversie

- v1.4.1.3

## Instellen van 802.1X-verificatie

### Een RADIUS-server toevoegen

Stap 1. Meld u aan bij het web configuratieprogramma en kies **Security > RADIUS**. De pagina *RADIUS* wordt geopend.

## RADIUS

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:  (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)  
Source IPv4 Interface:   
Source IPv6 Interface:

Apply

Cancel

### 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.

Add...

Edit...

Delete

Stap 2. In het veld *RADIUS-accounting* selecteert u een radioknop om te selecteren welk type boekhoudkundige informatie de RADIUS-server wordt gegeven. Een RADIUS-server kan boekhoudkundige informatie krijgen die de sessietijd van een gebruiker, de middelen die hij gebruikt en andere dingen bijhoudt. De hier geselecteerde optie heeft geen invloed op de prestaties van 802.1X.

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:  (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)  
Source IPv4 Interface:   
Source IPv6 Interface:

Apply

Cancel

De opties zijn:

- Port-Based Access Control - Deze optie stuurt boekhoudkundige informatie over poortgebaseerde gewaarmerkte sessies naar de RADIUS-server.

- Management Access - Deze optie stuurt boekhoudkundige informatie over de beheersessies van de switch naar de RADIUS-server.
- Zowel Port-Based Access Control als Management-toegang - Met deze optie worden beide typen boekhoudkundige informatie naar de RADIUS-server verzonden.
- Geen - stuur geen boekhoudkundige informatie naar de RADIUS-server.

Stap 3. In het gebied *Default parameters* gebruiken, moet u de instellingen configureren die standaard worden gebruikt, tenzij een RADIUS-server met een eigen specifieke instelling wordt geconfigureerd. elke afzonderlijke server die u aan de schakelaar toevoegt, kan de standaardwaarden of afzonderlijke unieke instellingen gebruiken. Voor dit artikel gebruiken we de standaardinstellingen die in deze sectie worden gedefinieerd.

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:  (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  (6/128 characters used)

Source IPv4 Interface:    
 Source IPv6 Interface:

Configuratie van de volgende instellingen:

- Retries - Voer het aantal keer in dat de switch probeert om contact op te nemen met een RADIUS-server voordat u naar de volgende server gaat. De standaardinstelling is 3.
- Time-out bij antwoord - Voer het aantal seconden in dat de schakelaar op een antwoord van de RADIUS-server wacht voordat u verdere actie onderneemt (opnieuw proberen of opgeven). De standaardinstelling is 3.
- Dode tijd - Voer het aantal minuten in dat verstreken is voordat een RADIUS-server die niet reageert, wordt doorgegeven voor serviceaanvragen. De standaardinstelling is 0; deze waarde betekent dat de server niet wordt omzeild .
- Key String - Voer de geheime sleutel in die wordt gebruikt voor het authenticeren tussen de switch en de RADIUS-server. Als u een versleutelde sleutel hebt, voert u deze in met de radioknop **Encrypted**; anders voert u de Plaintext-toets in met de radioknop **Plaintext**.
- Bron IPv4/IPv6-interface - Gebruik deze vervolgkeuzelijsten om te kiezen welke IPv4/IPv6-broninterface zal worden gebruikt bij communicatie met de RADIUS-server. Deze

optie is Auto. Hiermee wordt het IP-adres standaard gebruikt dat op de uitgaande interface is gedefinieerd.

Stap 4. Klik op **Toepassen**. De standaardinstellingen worden toegepast.

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:  (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  (6/128 characters used)

Source IPv4 Interface:  ▼

Source IPv6 Interface:  ▼

**Apply** Cancel

Stap 5. De **RADIUS-tabel** toont de RADIUS-serveritems die momenteel op de switch zijn ingesteld. Klik op de knop **Toevoegen...** om een nieuw item toe te voegen. Het venster **Add RADIUS Server** wordt geopend.

Server	Priority	Key String (Encrypted)	Timeout for Reply	Authentication Port	Accounting Port	Retries	Dead Time	Usage Type
0 results found.								

**Add...** Edit... Delete

An \* indicates that the parameter is using the default global value.

Display Sensitive Data as Plaintext

Stap 6. In het veld *Server Definition*, kies of u contact opneemt met de RADIUS-server **door IP-adres** of **door naam** (hostname). Als u **per IP-adres** hebt geselecteerd, selecteert u IPv6 (**versie 6**) of IPv4 (**versie 4**). Als u **versie 6** hebt geselecteerd, gebruikt u het *IPv6-adrestype* en de *lokale interface voor link* om het IPv6-adres te specificeren dat gebruikt zal worden.

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 - 10, Default: 3)

✱ Dead Time:  Use Default  
 User Defined  min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  
 802.1x  
 All

Stap 7. In het veld *IP-adres/naam van de server* voert u het IP-adres of de hostnaam van de RADIUS-server in.

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 - 10, Default: 3)

**Dead Time:**  Use Default  
 User Defined  min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  
 802.1x  
 All

Stap 8. Voer in het veld *Prioriteit* de prioriteit in die u aan deze server wilt toewijzen; de switch zal proberen met de hoogste prioriteit contact op te nemen met de server en verder de lijst in te stellen totdat er een responsieve server optreedt. Het gaat om 0-65535, waarvan 0 de hoogste prioriteit heeft.

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 - 10, Default: 3)

Dead Time:  Use Default  
 User Defined  min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  
 802.1x  
 All

Stap 9. Selecteer de knop **Default** radio in de *Key String*, *Time-out voor antwoord*, *Retries* en *Dead Time*-velden om de instellingen te gebruiken die eerder in de *RADIUS*-pagina waren ingesteld. U kunt ook de **User Defined** radioknoppen selecteren om instellingen te configureren die anders zijn dan de standaardinstellingen; Als u dit doet, worden deze instellingen alleen gebruikt voor deze specifieke *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)   
 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 - 10, Default: 3)

Dead Time:  Use Default  
 User Defined  min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  
 802.1x  
 All

Stap 10. In het veld *Verificatiepoort* specificeert u de poort die wordt gebruikt voor authenticatie communicatie met de RADIUS-server. Aanbevolen wordt om dit op de standaardpoort 1812 te laten.



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 - 10, Default: 3)

Dead Time:  Use Default  
 User Defined  min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  
 802.1x  
 All

Stap 1. In het veld *Accounting Port* specificeert u de poort die wordt gebruikt voor accounting communicatie met de RADIUS-server. Aanbevolen wordt om dit op de standaardpoort 1813 te laten.

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 - 10, Default: 3)

Dead Time:  Use Default  
 User Defined  min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  
 802.1x  
 All

Stap 12. Selecteer in het veld *Gebruikstype* waarvoor de RADIUS-server wordt gebruikt. Bij het configureren van 802.1X selecteert u de **802.1x** of **Alle** radioknoppen om de RADIUS-server te gebruiken voor 802.1X poortverificatie.

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 - 10, Default: 3)

Dead Time:  Use Default  
 User Defined  min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  
 802.1x  
 All

Stap 13. Klik op **Toepassen**. De server wordt toegevoegd aan de *RADIUS-tabel*. Ga naar de volgende sectie om verificatie op basis van port-based 802.1X mogelijk te maken.

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 - 10, Default: 3)

✱ Dead Time:  Use Default  
 User Defined  min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  
 802.1x  
 All

## Port-gebaseerde verificatie inschakelen

Stap 1. Ga naar **Security > 802.1X/MAC/Web Verificatie > Properties** in het **web Configuration-hulpprogramma**. De pagina *Eigenschappen* wordt geopend.

## Properties

Port-Based Authentication:  Enable

Authentication Method:  RADIUS, None  
 RADIUS  
 None

Guest VLAN:  Enable

Guest VLAN ID:

✱ Guest VLAN Timeout:  Immediate  
 User Defined  sec (Range: 30 - 180)

### Trap Settings

802.1x Authentication Failure Traps:  Enable

802.1x Authentication Success Traps:  Enable

MAC Authentication Failure Traps:  Enable

MAC Authentication Success Traps:  Enable

Web Authentication Failure Traps:  Enable

Web Authentication Success Traps:  Enable

Web Authentication Quiet Traps:  Enable

Apply

Cancel

### VLAN Authentication Table

VLAN ID	VLAN Name	Authentication
---------	-----------	----------------

0 results found.

Edit...

Stap 2. In het veld *Port-gebaseerde verificatie* controleert u het selectieteken **Enable** om poortgebaseerde verificatie mogelijk te maken. Dit is standaard ingeschakeld.

Port-Based Authentication:  Enable

Authentication Method:  RADIUS, None  
 RADIUS  
 None

Guest VLAN:  Enable

Guest VLAN ID:

✱ Guest VLAN Timeout:  Immediate  
 User Defined  sec (Range: 30 - 180)

**Trap Settings**

802.1x Authentication Failure Traps:  Enable

802.1x Authentication Success Traps:  Enable

MAC Authentication Failure Traps:  Enable

MAC Authentication Success Traps:  Enable

Web Authentication Failure Traps:  Enable

Web Authentication Success Traps:  Enable

Web Authentication Quiet Traps:  Enable

Stap 3. Kies in het veld *Verificatiemethode* een radioknop om te bepalen hoe poortgebaseerde verificatie zal werken.

Port-Based Authentication:  Enable

Authentication Method:  RADIUS, None  
 RADIUS  
 None

Guest VLAN:  Enable

Guest VLAN ID:

✱ Guest VLAN Timeout:  Immediate  
 User Defined  sec (Range: 30 - 180)

**Trap Settings**

802.1x Authentication Failure Traps:  Enable

802.1x Authentication Success Traps:  Enable

MAC Authentication Failure Traps:  Enable

MAC Authentication Success Traps:  Enable

Web Authentication Failure Traps:  Enable

Web Authentication Success Traps:  Enable

Web Authentication Quiet Traps:  Enable

De opties zijn:

- RADIUS, geen - De switch zal proberen contact op te nemen met de RADIUS-server(s) die op de *RADIUS*-pagina is gedefinieerd. Indien geen antwoord van de server(s) wordt

ontvangen, wordt geen echtheidscontrole uitgevoerd en is de sessie toegestaan. Als de server reageert en de aanmeldingsgegevens niet correct zijn, wordt de sessie ontkend.

- RADIUS - De switch zal proberen contact op te nemen met de RADIUS-server(s) die op de *RADIUS*-pagina is gedefinieerd. Indien geen antwoord van de server(s) is ontvangen, wordt de sessie geweigerd. Voor de meest beveiligde 802.1X-implementatie wordt deze optie aanbevolen.
- Geen - Er wordt geen verificatie uitgevoerd. Alle sessies zijn toegestaan. Deze optie implementeert 802.1X niet.

Stap 4. Klik op **Toepassen**.

Port-Based Authentication:  Enable

Authentication Method:  RADIUS, None  
 RADIUS  
 None

Guest VLAN:  Enable

Guest VLAN ID:

✱ Guest VLAN Timeout:  Immediate  
 User Defined  sec (Range: 30 - 180)

**Trap Settings**

802.1x Authentication Failure Traps:  Enable

802.1x Authentication Success Traps:  Enable

MAC Authentication Failure Traps:  Enable

MAC Authentication Success Traps:  Enable

Web Authentication Failure Traps:  Enable

Web Authentication Success Traps:  Enable

Web Authentication Quiet Traps:  Enable

**Apply** Cancel

Stap 5. Navigeer naar **security > 802.1X/MAC/Web verificatie > Port-verificatie**. De pagina *Poortverificatie* wordt geopend.

## Port Authentication

Port Authentication Table									
	Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment	Guest VLAN	Open Access	802.1x Based Authentication	MAC Based Authentication
<input type="radio"/>	1	FE1	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled
<input type="radio"/>	2	FE2	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled
<input type="radio"/>	3	FE3	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled
<input type="radio"/>	4	FE4	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled
<input type="radio"/>	5	FE5	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled
<input type="radio"/>	6	FE6	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled
<input type="radio"/>	7	FE7	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled
<input type="radio"/>	8	FE8	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled
<input type="radio"/>	9	GE1	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled
<input type="radio"/>	10	GE2	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled

Copy Settings... Edit...

Stap 6. Selecteer de poort die u wilt configureren door de radioknop ervan in de *Tabel voor poortverificatie* te selecteren en op de knop **Bewerken...** te klikken. Het venster *Portverificatie bewerken* wordt geopend.

Port Authentication										
Port Authentication Table										
	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
<input checked="" type="radio"/>	1	FE1	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
<input type="radio"/>	2	FE2	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
<input type="radio"/>	3	FE3	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
<input type="radio"/>	4	FE4	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
<input type="radio"/>	5	FE5	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
<input type="radio"/>	6	FE6	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
<input type="radio"/>	7	FE7	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
<input type="radio"/>	8	FE8	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
<input type="radio"/>	9	GE1	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
<input type="radio"/>	10	GE2	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled

Copy Settings... Edit...

Stap 7. Kies in het veld *Beheerpoortcontrole* een radioknop om te bepalen hoe de poort sessies zal autoriseren. Het veld *Huidige poortcontrole* geeft de huidige status van de geselecteerde poort weer.



Interface:	<input type="text" value="FE1"/>
Current Port Control:	<input type="text" value="Authorized"/>
Administrative Port Control:	<input type="radio"/> Force Unauthorized <input checked="" type="radio"/> Auto <input type="radio"/> Force Authorized
RADIUS VLAN Assignment:	<input checked="" type="radio"/> Disable <input type="radio"/> Reject <input type="radio"/> Static
Guest VLAN:	<input type="checkbox"/> Enable
Open Access:	<input type="checkbox"/> Enable
802.1x Based Authentication:	<input checked="" type="checkbox"/> Enable
MAC Based Authentication:	<input type="checkbox"/> Enable
Web Based Authentication:	<input type="checkbox"/> Enable
Periodic Reauthentication:	<input type="checkbox"/> Enable
Reauthentication Period:	<input type="text" value="3600"/> sec (Range: 300 - 4294967295, Default: 3600)
Reauthenticate Now:	<input type="checkbox"/>
Authenticator State:	Force Authorized
Time Range:	<input type="checkbox"/> Enable
Time Range Name:	<input type="text" value=""/> <a href="#">Edit</a>

De opties zijn:

- Macht onbevoegd - Verplaats de interface in een onbevoegde staat. Het apparaat biedt geen authenticatie aan cliënten die met deze poort zijn verbonden en ontkent toegang.
- Auto - schakelt poortgebaseerde verificatie in voor de geselecteerde poort. Verplaatst de interface tussen geautoriseerd en onbevoegd afhankelijk van de uitkomst van de authenticatieprocedure. Kies deze optie om 802.1X te implementeren.
- Force Authorized - Verplaatst de interface in een geautoriseerde status. Het apparaat zal toegang verlenen tot elke client die verbinding maakt met deze poort zonder verificatie.

Stap 8. Controleer het selectieteken **Enable** in het veld *802.1X-gebaseerde verificatie* om 802.1X-verificatie voor de geselecteerde poort mogelijk te maken.

Interface:	FE1
Current Port Control:	Authorized
Administrative Port Control:	<input type="radio"/> Force Unauthorized <input checked="" type="radio"/> Auto <input type="radio"/> Force Authorized
RADIUS VLAN Assignment:	<input checked="" type="radio"/> Disable <input type="radio"/> Reject <input type="radio"/> Static
Guest VLAN:	<input type="checkbox"/> Enable
Open Access:	<input type="checkbox"/> Enable
802.1x Based Authentication:	<input checked="" type="checkbox"/> Enable
MAC Based Authentication:	<input type="checkbox"/> Enable
Web Based Authentication:	<input type="checkbox"/> Enable
Periodic Reauthentication:	<input type="checkbox"/> Enable
Reauthentication Period:	3600 sec (Range: 300 - 4294967295, Default: 3600)
Reauthenticate Now:	<input type="checkbox"/>
Authenticator State:	Force Authorized
Time Range:	<input type="checkbox"/> Enable
Time Range Name:	<input type="text"/> Edit

Stap 9. Klik op **Toepassen**. De poort moet nu volledig zijn ingesteld voor 802.1X poortgebaseerde authenticatie en is klaar om alle clients die er op aansluiten te authenticeren. Gebruik het veld *Interface* om een andere poort te selecteren voor configuratie zonder terug te gaan naar de pagina *Port Verificatie*.

802.1x Based Authentication:  Enable

MAC Based Authentication:  Enable

Web Based Authentication:  Enable

Periodic Reauthentication:  Enable

Reauthentication Period:  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  
 User Defined  sec (Range: 60 - 65535)

Max Hosts:  Infinite  
 User Defined  sec (Range: 1 - 4294967295)

Quiet Period:  sec (Range: 10 - 65535, Default: 60)

Resending EAP:  sec (Range: 30 - 65535, Default: 30)

Max EAP Requests:  (Range: 1 - 10, Default: 2)

Supplicant Timeout:  sec (Range: 1 - 65535, Default: 30)

Server Timeout:  sec (Range: 1 - 65535, Default: 30)

Stap 10. Als u de instellingen van een poort snel wilt kopiëren naar een andere poort of reeks poorten, klikt u op de radioknop van de poort die u in de *Tabel voor poortverificatie* wilt kopiëren en vervolgens klikt u op de knop **Kopie-instellingen....** Het venster *Instellingen kopiëren* wordt geopend.

Port Authentication

Port Authentication Table											
	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	
<input checked="" type="radio"/>	1	FE1	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	
<input type="radio"/>	2	FE2	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	
<input type="radio"/>	3	FE3	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	
<input type="radio"/>	4	FE4	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	
<input type="radio"/>	5	FE5	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	
<input type="radio"/>	6	FE6	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	
<input type="radio"/>	7	FE7	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	
<input type="radio"/>	8	FE8	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	
<input type="radio"/>	9	GE1	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	
<input type="radio"/>	10	GE2	N/A	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	

Stap 1. Voer in het tekstveld de poort of poorten (gescheiden door komma's) in waarop u de instellingen wilt kopiëren. U kunt ook een reeks poorten instellen. Klik vervolgens op **Toepassen** om de instellingen te kopiëren.

Copy configuration from entry 1 (FE1)

to:  (Example: 1,3,5-10 or: FE1,FE3-FE5)

**Bekijk een video gerelateerd aan dit artikel...**

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