

Configuración de la Autenticación de Puerto 802.1x en un Switch

Objetivo

IEEE 802.1x es un estándar que facilita el control de acceso entre un cliente y un servidor. Antes de que una red de área local (LAN) o un switch puedan proporcionar servicios a un cliente, el servidor de autenticación que ejecuta el servicio de usuario de acceso telefónico de autenticación remota (RADIUS) debe autenticar al cliente conectado al puerto del switch.

La autenticación 802.1x impide que los clientes no autorizados se conecten a una LAN a través de puertos accesibles a través de la publicidad. La autenticación 802.1x es un modelo cliente-servidor. En este modelo, los dispositivos de red tienen las siguientes funciones específicas:

Cliente o suplicante: un cliente o suplicante es un dispositivo de red que solicita acceso a la LAN. El cliente está conectado a un autenticador.

Authenticator: un autenticador es un dispositivo de red que proporciona servicios de red y a los que se conectan los puertos de suplicante. Se admiten los siguientes métodos de autenticación:

basado en 802.1x: compatible con todos los modos de autenticación. En la autenticación basada en 802.1x, el autenticador extrae los mensajes del protocolo de autenticación extensible (EAP) de los mensajes 802.1x o de los paquetes EAP sobre LAN (EAPoL) y los pasa al servidor de autenticación mediante el protocolo RADIUS.

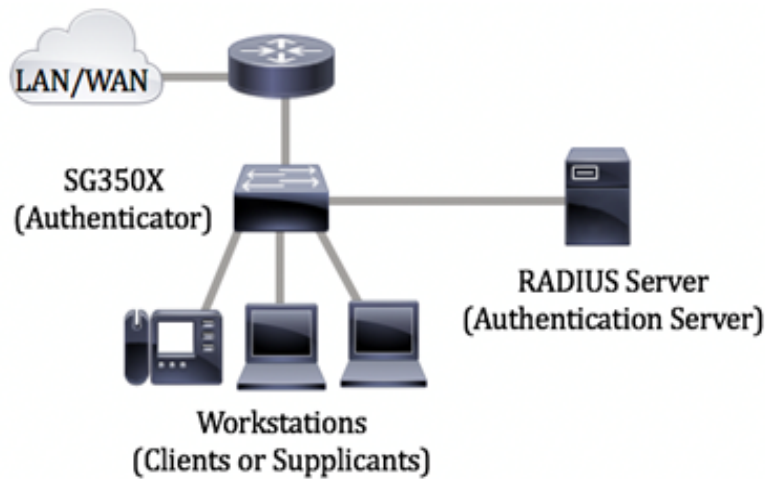
basado en MAC: compatible en todos los modos de autenticación. Con el control de acceso a medios (MAC) basado, el autenticador ejecuta la parte de cliente EAP del software en nombre de los clientes que buscan acceso a la red.

Basado en Web: solo se admite en modos multisesión. Con la autenticación basada en web, el autenticador ejecuta la parte de cliente EAP del software en nombre de los clientes que buscan acceso a la red.

Servidor de autenticación: un servidor de autenticación realiza la autenticación real del cliente. El servidor de autenticación para el dispositivo es un servidor de autenticación RADIUS con extensiones EAP.

Nota: Un dispositivo de red puede ser un cliente o suplicante, autenticador o ambos por puerto.

La siguiente imagen muestra una red que ha configurado los dispositivos según las funciones específicas. En este ejemplo, se utiliza un switch SG350X.



Pautas para configurar 802.1x:

Cree una red de acceso virtual (VLAN). Para crear VLAN utilizando la utilidad basada en web de su switch, haga clic [aquí](#). Para obtener instrucciones basadas en CLI, haga clic [aquí](#).

Configure los parámetros de puerto a VLAN en su switch. Para configurar mediante la utilidad basada en web, haga clic [aquí](#). Para utilizar la CLI, haga clic [aquí](#).

Configure las propiedades 802.1x en el switch. 802.1x debe habilitarse globalmente en el switch para habilitar la autenticación basada en puertos 802.1x. Para obtener instrucciones, haga clic [aquí](#).

(Opcional) Configure el rango de tiempo en el switch. Para aprender a configurar los parámetros de rango de tiempo en su switch, haga clic [aquí](#).

Configure la autenticación de puerto 802.1x. En este artículo se proporcionan instrucciones sobre cómo configurar los parámetros de autenticación de puertos 802.1x en el switch.

Para saber cómo configurar la autenticación basada en mac en un switch, haga clic [aquí](#).

Dispositivos aplicables

Serie Sx300

Serie Sx350

Serie SG350X

Serie Sx500

Serie Sx550X

Versión del software

1.4.7.06 — Sx300, Sx500

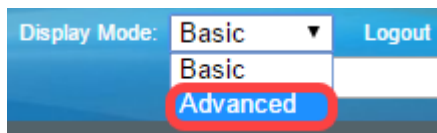
2.2.8.04: Sx350, SG350X, Sx550X

Configuración de los parámetros de autenticación de puerto 802.1x en un switch

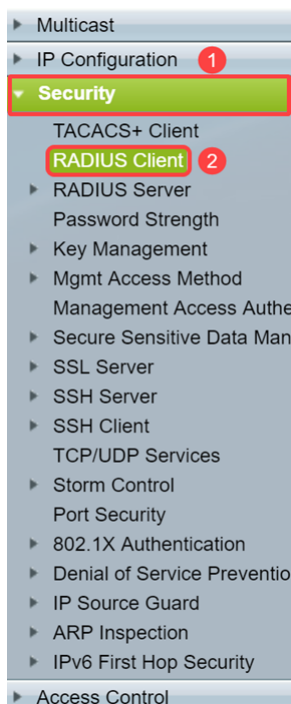
Configuración de los parámetros del cliente RADIUS

Paso 1. Inicie sesión en la utilidad basada en Web del switch y, a continuación, seleccione **Avanzado** en la lista desplegable Modo de visualización.

Nota: Las opciones de menú disponibles pueden variar en función del modelo de dispositivo. En este ejemplo, se utiliza SG550X-24.



Paso 2. Vaya a **Seguridad > Cliente RADIUS**.



Paso 3. Desplácese hacia abajo hasta la sección *Tabla RADIUS* y haga clic en **Agregar...** para agregar un servidor RADIUS.

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

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

Paso 4. Seleccione si desea especificar el servidor RADIUS por dirección IP o nombre en el campo *Definición de servidor*. Seleccione la versión de la dirección IP del servidor RADIUS en el campo *IP Version*.

Nota: En este ejemplo, usaremos **By IP address** y **Version 4**.

Add RADIUS Server - Google Chrome

Not secure | https://192.168.1.125/cs30a6baef/mts/mgmtauthen/security_authen_radius_a_jq.htm

Server Definition: **1** By IP address By name

IP Version: Version 6 **Version 4** **2**

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 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

Paso 5. Introduzca en el servidor RADIUS por dirección IP o nombre.

Nota: Entraremos la dirección IP de **192.168.1.146** en el campo *Server IP Address/Name*.

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: 192.168.1.146

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

Paso 6. Introduzca la prioridad del servidor. La prioridad determina el orden en que el dispositivo intenta ponerse en contacto con los servidores para autenticar a un usuario. El dispositivo comienza con el servidor RADIUS de mayor prioridad primero. 0 es la prioridad más alta.

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: 192.168.1.146

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

Paso 7. Introduzca la cadena de clave utilizada para autenticar y cifrar la comunicación entre el dispositivo y el servidor RADIUS. Esta clave debe coincidir con la clave configurada en el servidor RADIUS. Se puede ingresar en el formato **Cifrado** o **Texto sin formato**. Si se selecciona **Usar valor predeterminado**, el dispositivo intenta autenticarse en el servidor RADIUS mediante la cadena de clave predeterminada.

Nota: Utilizaremos el **texto definido por el usuario (texto sin formato)** e introduciremos el **ejemplo clave**.

Para saber cómo configurar los parámetros del servidor RADIUS en su switch, haga clic [aquí](#).

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: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) example (7/128 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

Paso 8. En el campo *Timeout for Reply*, seleccione **Use Default** o **User Defined**. Si **User Defined** fue seleccionado, ingrese el número de segundos que el dispositivo espera una respuesta del servidor RADIUS antes de reintentar la consulta, o conmutando al siguiente servidor si se realiza el número máximo de reintentos. Si se selecciona **Usar valor predeterminado**, el dispositivo utiliza el valor de tiempo de espera predeterminado.

Nota: En este ejemplo, se seleccionó **Usar valor predeterminado**.

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) example (7/128 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

Paso 9. Ingrese el número de puerto UDP del puerto del servidor RADIUS para la solicitud de autenticación en el campo *Puerto de autenticación*. Ingrese el número de puerto UDP del puerto del servidor RADIUS para las solicitudes de contabilización en el campo *Puerto de Contabilización*.

Nota: En este ejemplo, utilizaremos el valor predeterminado tanto para el puerto de autenticación como para el puerto de contabilidad.

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) example (7/128 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

Paso 10. Si el campo **Definido por el usuario** está seleccionado para *Reintentos*, introduzca el número de solicitudes que se envían al servidor RADIUS antes de que se considere que se ha producido una falla. Si se seleccionó **Usar valor predeterminado**, el dispositivo utiliza el valor predeterminado para el número de reintentos.

Si **User Defined** está seleccionado para *Dead Time*, ingrese el número de minutos que deben pasar antes de que se omita un servidor RADIUS no receptivo para las solicitudes de servicio. Si se seleccionó **Usar valor predeterminado**, el dispositivo utiliza el valor predeterminado para el tiempo muerto. Si ha introducido 0 minutos, no habrá tiempo muerto.

Nota: En este ejemplo, seleccionaremos **Usar valor predeterminado** para ambos campos.

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) example (7/128 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: 1 Use Default User Defined Default (Range: 1 - 15, Default: 3)

Dead Time: 2 Use Default User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type: Login 802.1x All

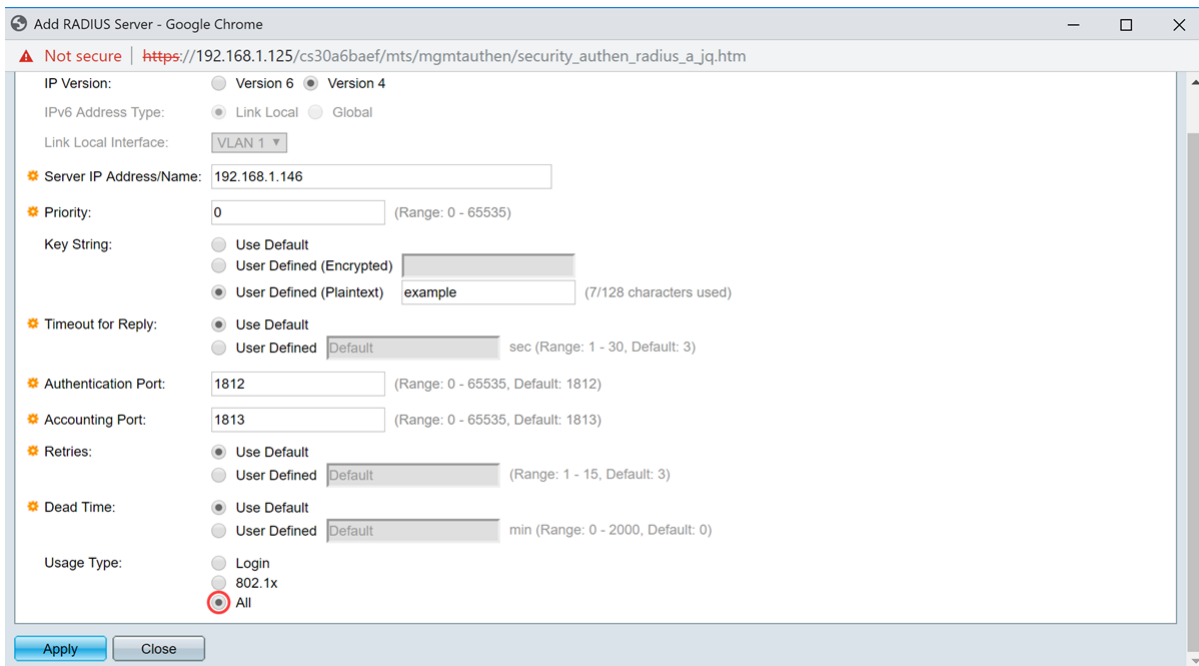
Apply Close

Paso 11. En el campo *Tipo de uso*, ingrese el tipo de autenticación del servidor RADIUS. Las opciones son:

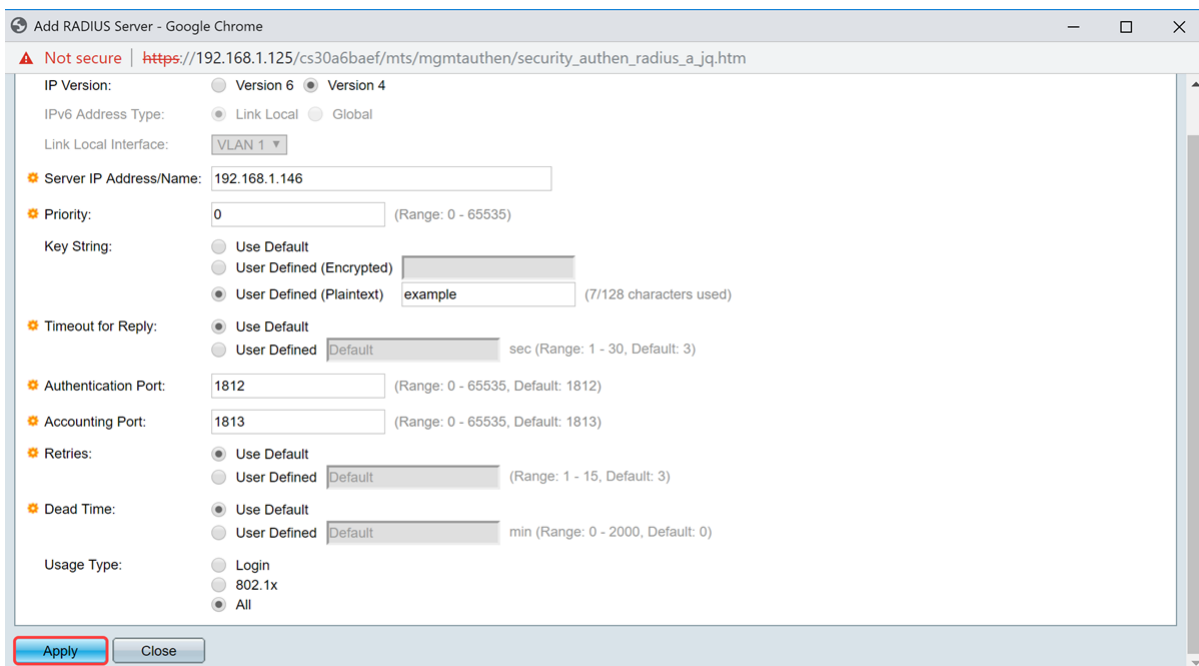
Login - El servidor RADIUS se utiliza para autenticar a los usuarios que solicitan administrar el dispositivo.

802.1x: el servidor RADIUS se utiliza para la autenticación 802.1x.

All - El servidor RADIUS se utiliza para autenticar al usuario que solicita administrar el dispositivo y para la autenticación 802.1x.



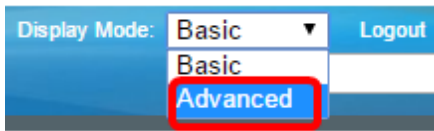
Paso 12. Haga clic en Apply (Aplicar).



Configuración de los parámetros de autenticación de puerto 802.1x

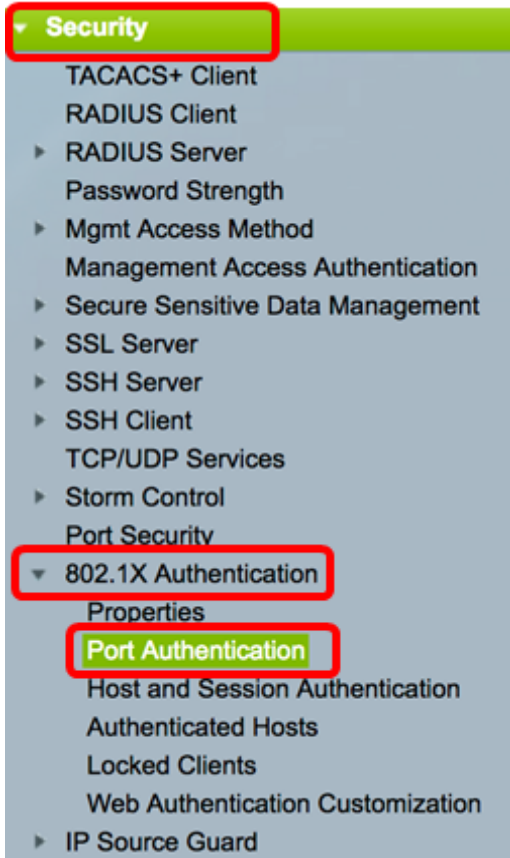
Paso 1. Inicie sesión en la utilidad basada en Web del switch y, a continuación, seleccione **Avanzado** en la lista desplegable Modo de visualización.

Nota: Las opciones de menú disponibles pueden variar en función del modelo de dispositivo. En este ejemplo, se utiliza SG350X-48MP.



Nota: Si tiene un switch Sx300 o Sx500 Series, vaya directamente al [Paso 2](#).

Paso 2. Elija **Security > 802.1X Authentication > Port Authentication**.

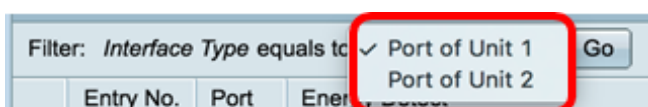


Paso 3. Elija una interfaz de la lista desplegable *Tipo de interfaz*.

Puerto: desde la lista desplegable *Tipo de Interfaz*, elija **Puerto** si sólo se necesita elegir un puerto único.

LAG: en la lista desplegable *Tipo de interfaz*, elija el LAG que desea configurar. Esto afecta al grupo de puertos definido en la configuración LAG.

Nota: En este ejemplo, se elige el puerto de la unidad 1.



Nota: Si tiene un switch no apilable como un switch Sx300 Series, vaya directamente al [Paso 5](#).

Paso 4. Haga clic en **Ir** para mostrar una lista de puertos o LAG en la interfaz.

Port Authentication

Port Authentication Table

Filter: *Interface Type* equals to Port of Unit 1

Paso 5. Haga clic en el puerto que desea configurar.

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
1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
2	GE2	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
3	GE3	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
4	GE4	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
6	GE6	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled

Nota: En este ejemplo, se elige GE4.

Paso 6. Desplácese hacia abajo por la página y haga clic en **Editar**.

46	GE46	Port Down	Force Authorized	Disabled	Disabled
47	GE47	Port Down	Force Authorized	Disabled	Disabled
48	GE48	Port Down	Force Authorized	Disabled	Disabled
49	XG1	Authorized	Force Authorized	Disabled	Disabled
50	XG2	Port Down	Force Authorized	Disabled	Disabled
51	XG3	Port Down	Force Authorized	Disabled	Disabled
52	XG4	Authorized	Force Authorized	Disabled	Disabled

Paso 7. (Opcional) Si desea editar otra interfaz, elija entre las listas desplegables Unidad y Puerto.

Interface: Unit 1 Port GE4
Current Port Control: Authorized

Nota: En este ejemplo, se elige el puerto GE4 de la unidad 1.

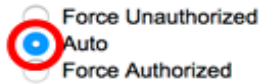
Paso 8. Haga clic en el botón de opción correspondiente al control de puerto deseado en el área Administrative Port Control (Control de puerto administrativo). Las opciones son:

Force Unauthorized: niega el acceso a la interfaz al mover el puerto al estado no autorizado. El puerto descartará el tráfico.

Auto: el puerto se mueve entre un estado autorizado o no autorizado basado en la autenticación del suplicante.

Force Authorized: autoriza el puerto sin autenticación. El puerto reenviará el tráfico.

Administrative Port Control:



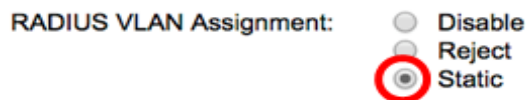
Nota: En este ejemplo, se elige Auto (Automático).

Paso 9. Haga clic en el botón de opción RADIUS VLAN Assignment (Asignación de VLAN RADIUS) para configurar la asignación de VLAN dinámica en el puerto seleccionado. Las opciones son:

Disable (Desactivar): la función no está activada.

Rechazar: si el servidor RADIUS autorizó el solicitante, pero no proporcionó una VLAN de suplicante, se rechaza el suplicante.

Estático: si el servidor RADIUS autorizó el solicitante, pero no proporcionó una VLAN de suplicante, se acepta el suplicante.



Nota: En este ejemplo, se elige Estático.

Paso 10. Marque **Enable** en la casilla de verificación Guest VLAN para habilitar la VLAN de invitado para los puertos no autorizados. La VLAN de invitado hace que el puerto no autorizado se una automáticamente a la VLAN elegida en el área ID de VLAN de invitado de las propiedades 802.1.



Paso 11. (Opcional) Marque la casilla de verificación **Enable** Open Access para habilitar el acceso abierto. Open Access le ayuda a entender los problemas de configuración de los hosts que se conectan a la red, monitorea las situaciones incorrectas y permite solucionar estos problemas.

Nota: Cuando se habilita el acceso abierto en una interfaz, el switch trata todos los fallos recibidos de un servidor RADIUS como éxitos y permite el acceso a la red para las estaciones conectadas a interfaces, independientemente de los resultados de autenticación. En este ejemplo, Open Access está desactivado.



Paso 12. Marque la casilla de verificación **Enable 802.1x Based Authentication** para habilitar la autenticación 802.1X en el puerto.

Guest VLAN: Enable
Open Access: Enable
802.1x Based Authentication: Enable

Paso 13. Marque la casilla de verificación **Enable** MAC Based Authentication para habilitar la autenticación de puerto basada en la dirección MAC del solicitante. Sólo se pueden utilizar ocho autenticaciones basadas en MAC en el puerto.

Nota: Para que la autenticación MAC se realice correctamente, el nombre de usuario y la contraseña del solicitante del servidor RADIUS deben ser la dirección MAC del solicitante. La dirección MAC debe estar en minúsculas y debe introducirse sin . o - separadores (como 0020aa00bcc).

802.1x Based Authentication: Enable
MAC Based Authentication: Enable

Nota: En este ejemplo, la autenticación basada en MAC está inhabilitada.

Paso 14. Marque la casilla de verificación **Enable** Web Based Authentication para habilitar la autenticación basada en Web en el switch. En este ejemplo, la autenticación basada en web está inhabilitada.

802.1x Based Authentication: Enable
MAC Based Authentication: Enable
Web Based Authentication: Enable

Nota: En este ejemplo, la autenticación basada en web está inhabilitada.

Paso 15. (Opcional) Marque la casilla de verificación **Enable** Periodic Reauthentication para forzar al puerto a volver a autenticarse después de un tiempo determinado. Esta hora se define en el campo *Periodo de Reautenticación*.

Web Based Authentication: Enable
Periodic Reauthentication: Enable

Nota: En este ejemplo, se habilita la reautenticación de período.

Paso 16. (Opcional) Introduzca un valor en el campo *Periodo de Reautenticación*. Este valor representa la cantidad de segundos antes de que la interfaz vuelva a autenticar el puerto. El valor predeterminado es 3600 segundos y el rango es de 300 a 4294967295 segundos.

Periodic Reauthentication: Enable
Reauthentication Period: sec

Nota: En este ejemplo, se configuran 6000 segundos.

Paso 17. (Opcional) Marque la casilla de verificación **Enable** Reauthenticate Now para forzar una reautenticación inmediata del puerto. En este ejemplo, se inhabilita la reautenticación inmediata.

Periodic Reauthentication: Enable

Reauthentication Period: sec

Reauthenticate Now:

Authenticator State: Force Authorized

El área Estado del autenticador muestra el estado de autorización del puerto.

Paso 18. (Opcional) Marque la casilla de verificación **Enable** Time Range para habilitar un límite en el tiempo que el puerto está autorizado.

Time Range: Enable

Time Range Name: [Edit](#)

Nota: En este ejemplo, se habilita Time Range . Si prefiere omitir esta función, vaya al [Paso 20](#).

Paso 19. (Opcional) En la lista desplegable Nombre del rango de tiempo, elija un rango de tiempo para usar.

Time Range: Enable

Time Range Name: Dayshift NightShift

Maximum WBA Login Attempts:

Nota: En este ejemplo, se elige el turno de día.

Paso 20. En el área Máximo de intentos de inicio de sesión de WBA, haga clic en Infinite for no limit o User Defined para establecer un límite. Si se selecciona User Defined (Definido por el usuario), introduzca el número máximo de intentos de inicio de sesión permitidos para la autenticación basada en web.

Maximum WBA Login Attempts: Infinite User Defined

Nota: En este ejemplo, se elige Infinite.

Paso 21. En el área Maximum WBA Silence Period (Período de silencio máximo de WBA), haga clic en Infinite for no limit (Infinito para no limitar) o User Defined (Definido por el usuario) para establecer un límite. Si se selecciona User Defined (Definido por el usuario), introduzca la duración máxima del período de silencio para la autenticación basada en web permitida en la interfaz.

Maximum WBA Silence Period: Infinite User Defined sec

Nota: En este ejemplo, se elige Infinite.

Paso 22. En el área Max Hosts (Máximo de hosts), haga clic en Infinite for no limit (Infinito sin límite) o User Defined (Definido por el usuario) para establecer un límite. Si se elige User Defined (Definido por el usuario), introduzca el número máximo de hosts autorizados permitidos en la interfaz.

Max Hosts:

Infinite
 User Defined

Nota: Establezca este valor en 1 para simular el modo de host único para la autenticación basada en Web en el modo de sesiones múltiples. En este ejemplo, se elige Infinite.

Paso 23. En el campo *Período silencioso*, ingrese el tiempo que el switch permanece en estado silencioso después de un intercambio de autenticación fallido. Cuando el switch se encuentra en estado silencioso, significa que el switch no está escuchando nuevas solicitudes de autenticación del cliente. El valor predeterminado es 60 segundos y el intervalo es de uno a 65535 segundos.

Quiet Period:

Nota: En este ejemplo, el período de inactividad se establece en 120 segundos.

Paso 24. En el campo *Resending EAP*, ingrese el tiempo que el switch espera un mensaje de respuesta del solicitante antes de reenviar una solicitud. El valor predeterminado es 30 segundos y el intervalo es de uno a 65535 segundos.

Quiet Period:

Resending EAP:

Nota: En este ejemplo, el reenvío de EAP se establece en 60 segundos.

Paso 25. En el campo *Max EAP Requests*, ingrese el número máximo de solicitudes EAP que se pueden enviar. EAP es un método de autenticación utilizado en 802.1X que proporciona intercambio de información de autenticación entre el switch y el cliente. En este caso, las solicitudes EAP se envían al cliente para la autenticación. A continuación, el cliente debe responder y coincidir con la información de autenticación. Si el cliente no responde, se establece otra solicitud EAP en función del valor EAP de reenvío y se reinicia el proceso de autenticación. El valor predeterminado es 2 y el intervalo es de uno a 10.

Quiet Period:

Resending EAP:

Max EAP Requests:

Nota: En este ejemplo, se utiliza el valor predeterminado de 2.

Paso 26. En el campo *Supplicant Timeout*, ingrese el tiempo antes de que las solicitudes EAP se envíen al solicitante. El valor predeterminado es 30 segundos y el intervalo es de uno a 65535 segundos.

Max EAP Requests:

(Rar

Supplicant Timeout:

sec |

Nota: En este ejemplo, el tiempo de espera del solicitante se establece en 60 segundos.

Paso 27. En el campo *Server Timeout*, ingrese el tiempo que transcurre antes de que el switch envíe una solicitud nuevamente al servidor RADIUS. El valor predeterminado es 30 segundos y el intervalo es de uno a 65535 segundos.

☛ Max EAP Requests:	<input type="text" value="2"/>	(Ran
☛ Supplicant Timeout:	<input type="text" value="60"/>	sec (
☛ Server Timeout:	<input type="text" value="60"/>	sec (

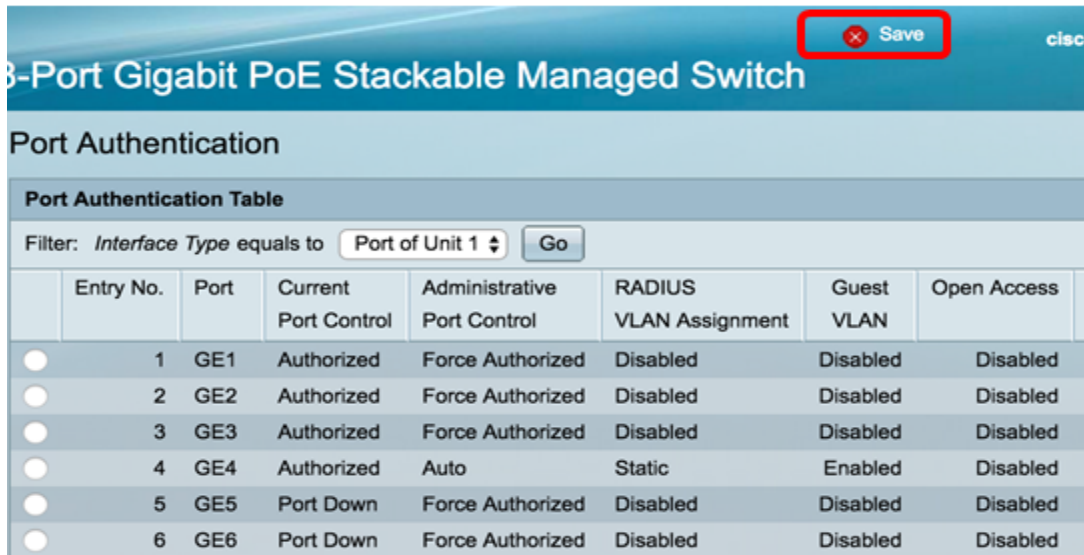
Nota: En este ejemplo, el tiempo de espera del servidor se establece en 60 segundos.

Paso 28. Haga clic en **Aplicar** y luego haga clic en **Cerrar**.

Interface:	Unit <input type="text" value="1"/>	Port <input type="text" value="GE4"/>
Current Port Control:	Unauthorized	
Administrative Port Control:	<input type="radio"/> Force Unauthorized <input checked="" type="radio"/> Auto <input type="radio"/> Force Authorized	
RADIUS VLAN Assignment:	<input type="radio"/> Disable <input type="radio"/> Reject <input checked="" type="radio"/> Static	
Guest VLAN:	<input checked="" 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 checked="" type="checkbox"/> Enable	
☛ Reauthentication Period:	<input type="text" value="6000"/>	sec (Range: 300 - 4294967295, Default: 3600)
Reauthenticate Now:	<input type="checkbox"/>	
Authenticator State:	Connecting	
Time Range:	<input type="checkbox"/> Enable	
Time Range Name:	<input type="text" value="Dayshift"/> Edit	
☛ Maximum WBA Login Attempts:	<input checked="" type="radio"/> Infinite <input type="radio"/> User Defined <input type="text"/> (Range: 3 - 10)	
☛ Maximum WBA Silence Period:	<input checked="" type="radio"/> Infinite <input type="radio"/> User Defined <input type="text"/> sec (Range: 60 - 65535)	
☛ Max Hosts:	<input checked="" type="radio"/> Infinite <input type="radio"/> User Defined <input type="text"/> sec (Range: 1 - 4294967295)	
☛ Quiet Period:	<input type="text" value="120"/>	sec (Range: 10 - 65535, Default: 60)
☛ Resending EAP:	<input type="text" value="60"/>	sec (Range: 30 - 65535, Default: 30)
☛ Max EAP Requests:	<input type="text" value="2"/>	(Range: 1 - 10, Default: 2)
☛ Supplicant Timeout:	<input type="text" value="60"/>	sec (Range: 1 - 65535, Default: 30)
☛ Server Timeout:	<input type="text" value="60"/>	sec (Range: 1 - 65535, Default: 30)

Paso 29. (Opcional) Haga clic en **Guardar** para guardar la configuración en el archivo de

configuración de inicio.



3-Port Gigabit PoE Stackable Managed Switch

Port Authentication

Port Authentication Table

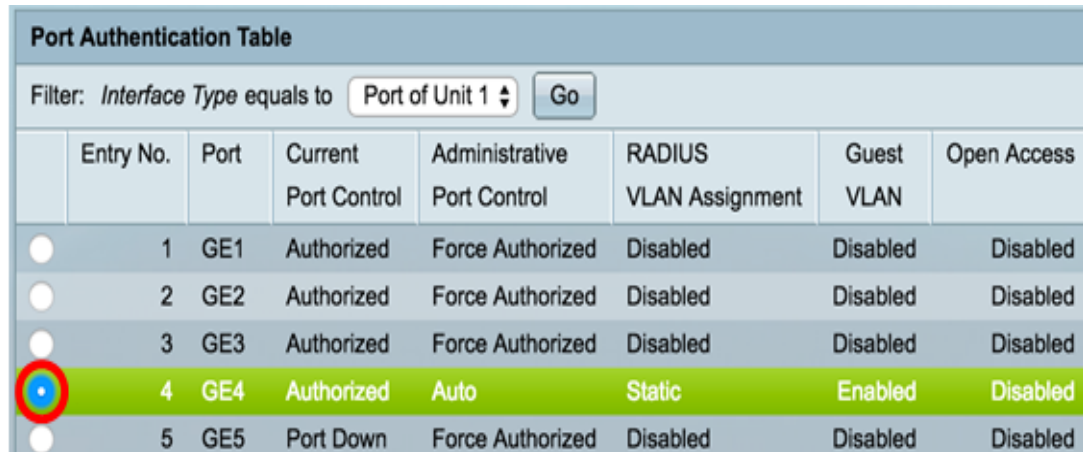
Filter: Interface Type equals to Port of Unit 1 Go

	Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment	Guest VLAN	Open Access
<input type="radio"/>	1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	2	GE2	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	3	GE3	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	4	GE4	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	6	GE6	Port Down	Force Authorized	Disabled	Disabled	Disabled

Ahora debería haber configurado correctamente los parámetros de autenticación de puerto 802.1x en su switch.

Aplicar configuración de interfaz a varias interfaces

Paso 1. Haga clic en el botón de opción de la interfaz que desea aplicar la configuración de autenticación a varias interfaces.



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
<input type="radio"/>	1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	2	GE2	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	3	GE3	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input checked="" type="radio"/>	4	GE4	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled

Nota: En este ejemplo, se elige GE4.

Paso 2. Desplácese hacia abajo y haga clic en **Copiar configuración**.

<input type="radio"/>	43	GE43	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	44	GE44	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	45	GE45	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	46	GE46	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	47	GE47	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	48	GE48	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	49	XG1	Authorized	Force Authorized	Disabled	Disabled
<input type="radio"/>	50	XG2	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	51	XG3	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	52	XG4	Authorized	Force Authorized	Disabled	Disabled

Copy Settings... Edit...

Paso 3. En el campo *to*, ingrese el rango de interfaces que desea aplicar la configuración de la interfaz elegida. Puede utilizar los números de interfaz o el nombre de las interfaces como entrada. Puede ingresar cada interfaz separada por una coma (como 1, 3, 5 o GE1, GE3, GE5) o puede ingresar un rango de interfaces (como 1-5 o GE1-GE5).

Copy configuration from entry 4 (GE4)

to: (Example: 1,3,5-10 or: GE1,GE3-XG4)

Nota: En este ejemplo, la configuración se aplicará a los puertos 47 a 48.

Paso 4. Haga clic en **Aplicar** y luego haga clic en **Cerrar**.

Copy configuration from entry 4 (GE4)

to: (Example: 1,3,5-10 or: GE1,GE3-XG4)

Apply Close

La siguiente imagen muestra los cambios después de la configuración.

Port Authentication Table

Filter: *Interface Type* equals to

	Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment	Guest VLAN	Open Access
<input type="radio"/>	1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	2	GE2	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	3	GE3	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	4	GE4	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	6	GE6	Port Down	Force Authorized	Disabled	Disabled	Disabled

<input type="radio"/>	45	GE45	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	46	GE46	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	47	GE47	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	48	GE48	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	49	XG1	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	50	XG2	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	51	XG3	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	52	XG4	Authorized	Force Authorized	Disabled	Disabled	Disabled

Ahora debería haber copiado correctamente los parámetros de autenticación 802.1x de un puerto y aplicarlos a otros puertos del switch.