Configuración de la Autenticación de Puerto 802.1X en los Cisco Sx220 Series Smart Switches

Objetivo

El objetivo de este artículo es mostrarle cómo configurar la autenticación de puerto en los switches inteligentes de la serie Sx220.

La autenticación de puerto 802.1X habilita la configuración de parámetros 802.1X para cada puerto del dispositivo. Un puerto que solicita autenticación se denomina suplicante. El autenticador es un switch o un punto de acceso que actúa como protector de red para los suplicantes. El autenticador reenvía los mensajes de autenticación al servidor RADIUS para que un puerto pueda ser autenticado y pueda enviar y recibir información.

Dispositivos aplicables

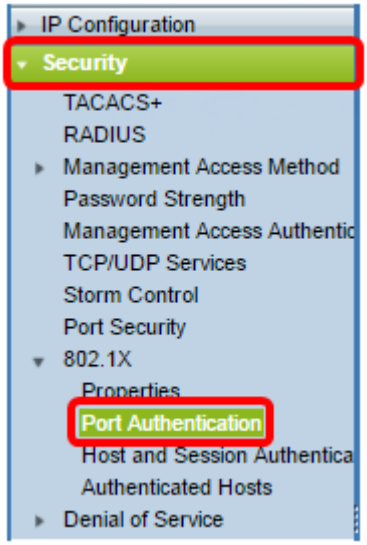
- Serie Sx220

Versión del software

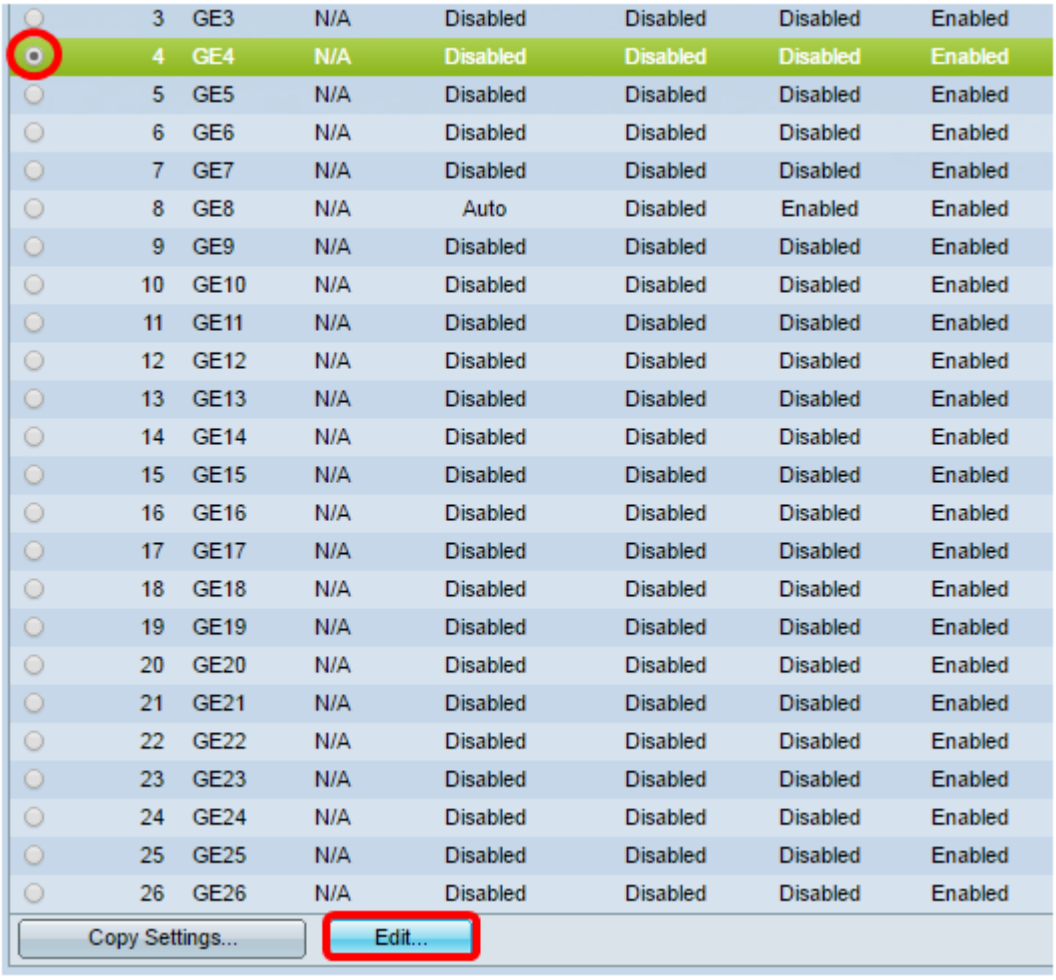
- 1.1.0.14

Configuración de la autenticación de puerto

Paso 1. Inicie sesión en la utilidad basada en web del switch y elija **Security > 802.1X > Port Authentication**.



Paso 2. Haga clic en el botón de opción del puerto que desea configurar y luego haga clic en **Editar**.

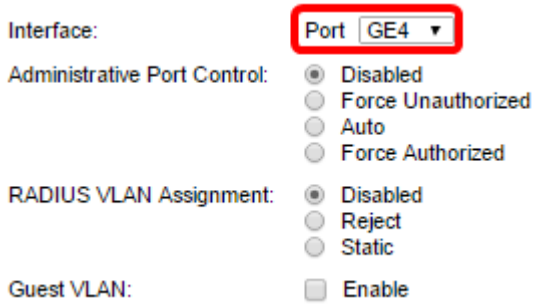


	3	GE3	N/A	Disabled	Disabled	Disabled	Enabled
◉	4	GE4	N/A	Disabled	Disabled	Disabled	Enabled
	5	GE5	N/A	Disabled	Disabled	Disabled	Enabled
	6	GE6	N/A	Disabled	Disabled	Disabled	Enabled
	7	GE7	N/A	Disabled	Disabled	Disabled	Enabled
	8	GE8	N/A	Auto	Disabled	Enabled	Enabled
	9	GE9	N/A	Disabled	Disabled	Disabled	Enabled
	10	GE10	N/A	Disabled	Disabled	Disabled	Enabled
	11	GE11	N/A	Disabled	Disabled	Disabled	Enabled
	12	GE12	N/A	Disabled	Disabled	Disabled	Enabled
	13	GE13	N/A	Disabled	Disabled	Disabled	Enabled
	14	GE14	N/A	Disabled	Disabled	Disabled	Enabled
	15	GE15	N/A	Disabled	Disabled	Disabled	Enabled
	16	GE16	N/A	Disabled	Disabled	Disabled	Enabled
	17	GE17	N/A	Disabled	Disabled	Disabled	Enabled
	18	GE18	N/A	Disabled	Disabled	Disabled	Enabled
	19	GE19	N/A	Disabled	Disabled	Disabled	Enabled
	20	GE20	N/A	Disabled	Disabled	Disabled	Enabled
	21	GE21	N/A	Disabled	Disabled	Disabled	Enabled
	22	GE22	N/A	Disabled	Disabled	Disabled	Enabled
	23	GE23	N/A	Disabled	Disabled	Disabled	Enabled
	24	GE24	N/A	Disabled	Disabled	Disabled	Enabled
	25	GE25	N/A	Disabled	Disabled	Disabled	Enabled
	26	GE26	N/A	Disabled	Disabled	Disabled	Enabled

Copy Settings... Edit...

Nota: En este ejemplo, se elige el puerto GE4.

Paso 3. A continuación, aparecerá la ventana Edit Port Authentication (Editar autenticación de puerto). En la lista desplegable Interfaz, asegúrese de que el puerto especificado es el que eligió en el Paso 2. De lo contrario, haga clic en la flecha desplegable y elija el puerto derecho.

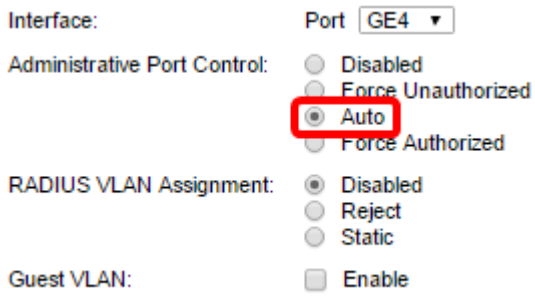


Paso 4. Elija un botón de opción para el control de puerto administrativo. Esto determinará el estado de autorización del puerto. Las opciones son:

- Desactivado: deshabilita 802.1X. Este es el estado predeterminado.
- Force Unauthorized: niega el acceso a la interfaz al mover la interfaz al estado no autorizado. El switch no proporciona servicios de autenticación al cliente a través de la interfaz.
- Automático: habilita la autenticación y autorización basadas en puertos en el switch. La interfaz se mueve entre un estado autorizado o no autorizado basado en el intercambio

de autenticación entre el switch y el cliente.

- Force Authorized: autoriza la interfaz sin autenticación.

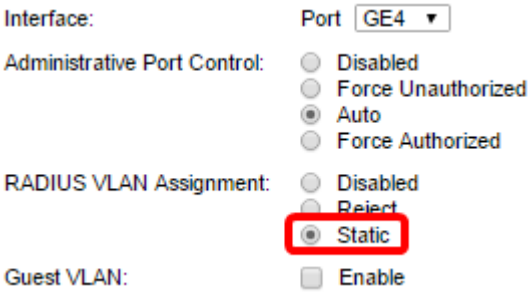


Nota: En este ejemplo, se elige Auto (Automático).

Paso 5. (Opcional) Elija un botón de opción para la Asignación de VLAN RADIUS. Esto habilitará la asignación de VLAN dinámica en el puerto especificado. Las opciones son:

- Desactivado: ignora el resultado de la autorización de VLAN y mantiene la VLAN original del host. Esta es la acción predeterminada.
- Rechazar: si el puerto especificado recibe una información autorizada de VLAN, utilizará la información. Sin embargo, si no hay información autorizada de VLAN, rechazará el host y lo hará no autorizado.
- Estático: si el puerto especificado recibe una información autorizada de VLAN, utilizará la información. Sin embargo, si no hay información de VLAN autorizada, conservará la VLAN original del host.

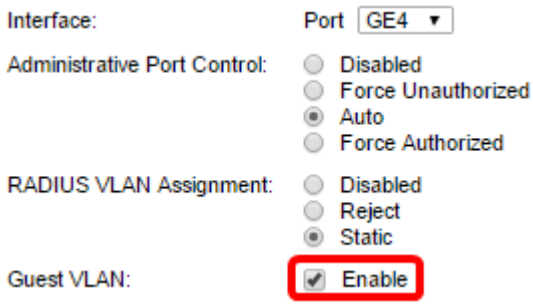
Nota: Si hay información de VLAN autorizada de RADIUS, pero la VLAN no se crea administrativamente en Device Under Test (DUT), la VLAN se creará automáticamente. En este ejemplo, se elige Estático.



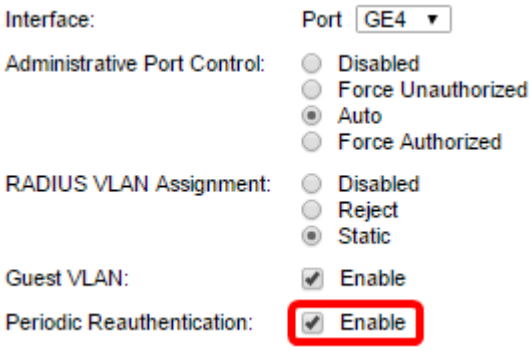
Sugerencia rápida: Para que la función Asignación de VLAN Dinámica funcione, el switch requiere que el servidor RADIUS envíe los siguientes atributos de VLAN:

- [64] Tipo de túnel = VLAN (tipo 13)
- [65] Túnel de tipo medio = 802 (tipo 6)
- [81] Tunnel-Private-Group-Id = ID de VLAN

Paso 6. (Opcional) Marque la casilla de verificación **Enable** para que la VLAN de invitado utilice una VLAN de invitado para puertos no autorizados.

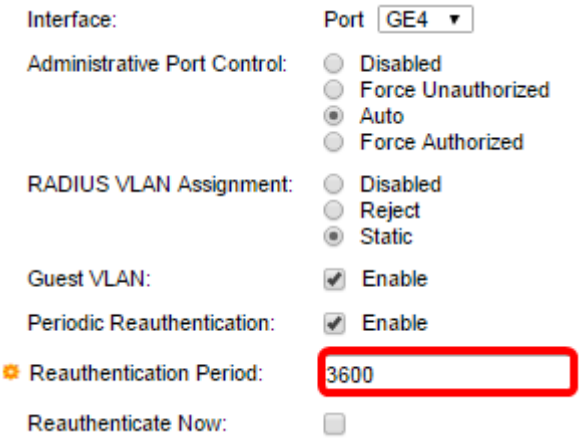


Paso 7. Marque la casilla de verificación **Enable** para la Reautenticación periódica. Esto habilitará los intentos de reautenticación del puerto después del periodo de reautenticación especificado.



Nota: Esta función está activada de forma predeterminada.

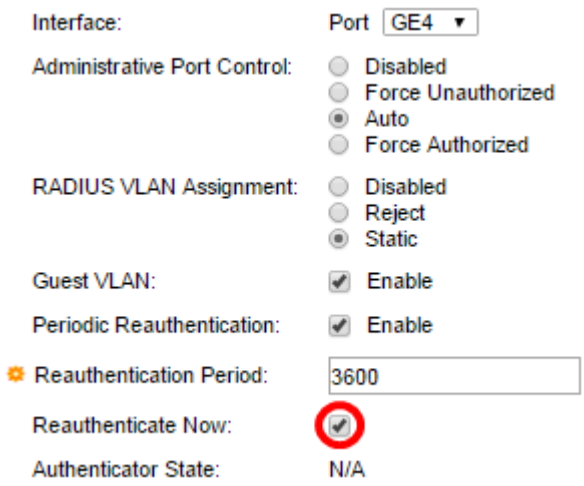
Paso 8. Introduzca un valor en el campo *Periodo de Reautenticación*. Este es el tiempo en segundos para volver a autenticar el puerto.



Nota: En este ejemplo, se utiliza el valor predeterminado 3600.

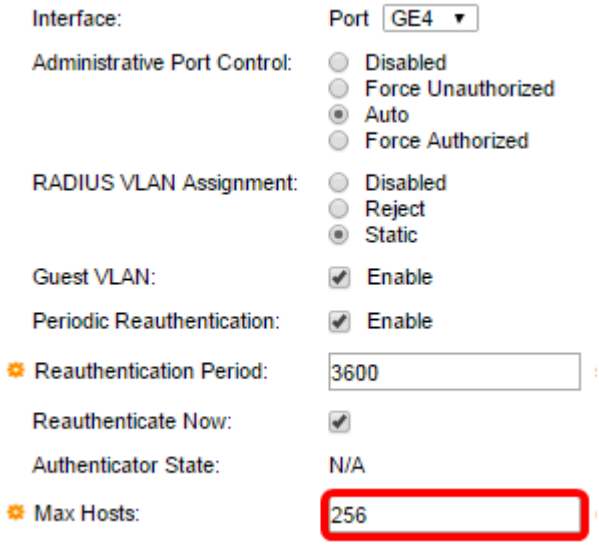
Paso 9. (Opcional) Marque la casilla de verificación **Reautenticar ahora** para habilitar la reautenticación inmediata del puerto.

Nota: El campo Estado del autenticador muestra el estado actual de la autenticación.



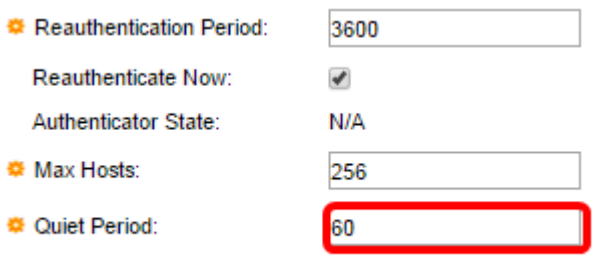
Nota: Si el puerto no se encuentra en el estado Forzar autorizado o Forzar no autorizado, se encuentra en el modo automático y el autenticador muestra el estado de la autenticación en curso. Después de autenticar el puerto, el estado se muestra como Autenticado.

Paso 10. En el campo *Max Hosts*, ingrese el número máximo de hosts autenticados permitidos en el puerto específico. Este valor sólo tiene efecto en el modo de sesiones múltiples.



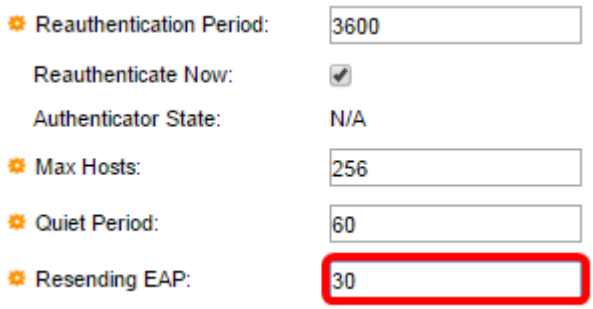
Nota: En este ejemplo, se utiliza el valor predeterminado 256.

Paso 11. En el campo *Período silencioso*, introduzca el número de segundos 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.



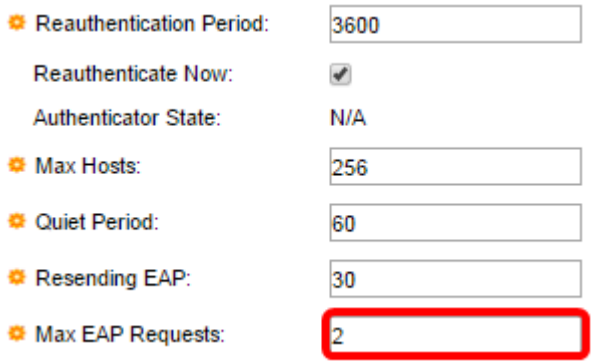
Nota: En este ejemplo, se utiliza el valor predeterminado 60.

Paso 12. En el campo *Resending EAP*, introduzca el número de segundos que el switch espera una respuesta a una solicitud de protocolo de autenticación extensible (EAP) o trama de identidad del suplicante (cliente) antes de volver a enviar la solicitud.



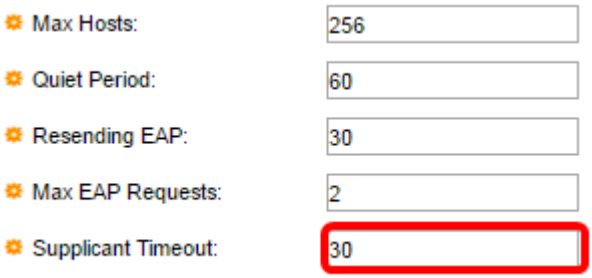
Nota: En este ejemplo, se utiliza el valor predeterminado 30.

Paso 13. En el campo *Max EAP Requests*, ingrese el número máximo de solicitudes EAP que se pueden enviar. Si no se recibe una respuesta después del período definido (tiempo de espera del solicitante), se reinicia el proceso de autenticación.



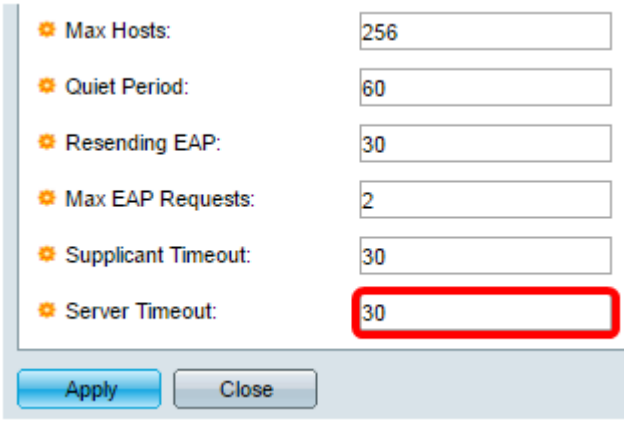
Nota: En este ejemplo, se utiliza el valor predeterminado 2.

Paso 14. En el campo *Supplicant Timeout*, ingrese el número de segundos que caducan antes de que las solicitudes EAP se envíen al suplicante.



Nota: En este ejemplo, se utiliza el valor predeterminado 30.

Paso 15. En el campo *Server Timeout*, ingrese el número de segundos que caducan antes de que el switch reenvíe una solicitud al servidor de autenticación.



Nota: En este ejemplo, se utiliza el valor predeterminado 30.

Paso 16. Haga clic en Apply (Aplicar).

Ahora debería haber configurado correctamente la autenticación de puerto en el switch.