Configuración de la autenticación 802.1x en los switches Cisco Business de la serie 220

Objetivo

El objetivo de este artículo es mostrarle cómo configurar la autenticación 802.1x en los switches inteligentes Cisco Business serie 220.

Dispositivos aplicables | Versión del firmware

- Serie CBS220 (Ficha técnica) |2.0.0.17

Introducción

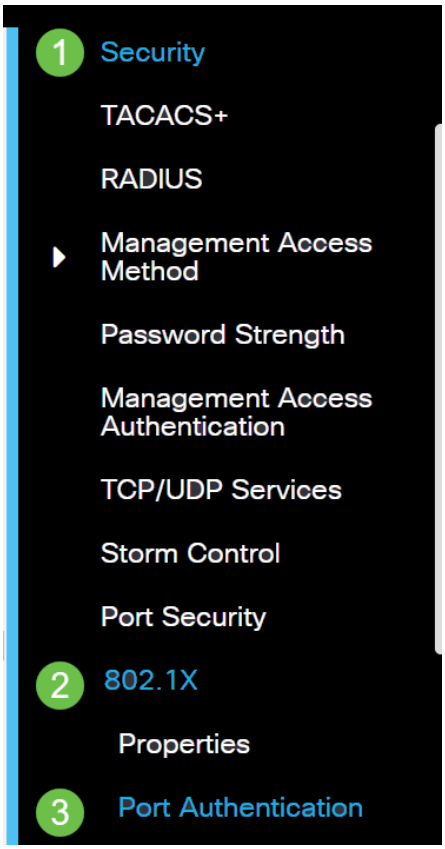
La autenticación de puerto habilita la configuración de parámetros para cada puerto. Dado que algunos de los cambios de configuración sólo son posibles mientras el puerto se encuentra en estado Forzar autorizado, como la autenticación de host, se recomienda cambiar el control de puerto a Forzar autorizado antes de realizar cambios. Cuando se complete la configuración, devuelva el control de puerto a su estado anterior.

Un puerto con 802.1x definido en él no puede convertirse en miembro de un LAG. 802.1x y Port Security no se pueden habilitar en el mismo puerto al mismo tiempo. Si habilita la seguridad de puerto en una interfaz, el Control de puerto administrativo no se puede cambiar al modo automático.

Configuración de la autenticación de puerto

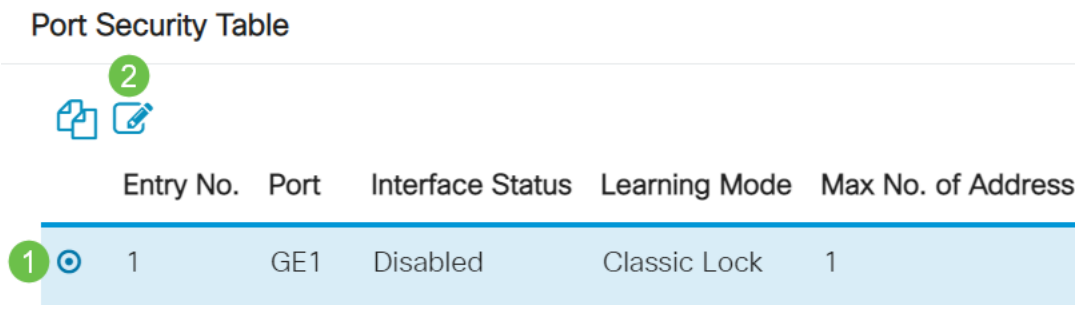
Paso 1

Inicie sesión en el switch Web User Interface (UI) y elija **Security > 802.1x > Port Authentication**.



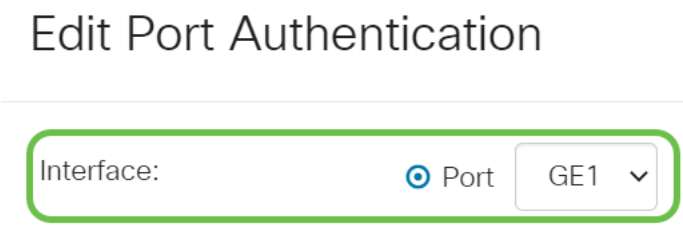
Paso 2

Haga clic en el botón de opción del puerto que desea configurar y luego haga clic en el **icono de edición**.



Paso 3

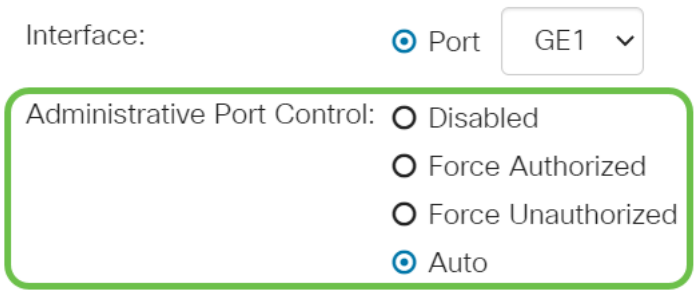
A continuación, aparecerá la ventana *Edit Port Authentication* . En la lista desplegable Interfaz, asegúrese de que el puerto especificado es el que eligió en el Paso 2. De lo contrario, haga clic en la flecha desplegable y elija el puerto derecho.



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**: inhabilita 802.1x. Este es el estado predeterminado.
- **Forzar no autorizado**: 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.
- **Auto**: habilita la autenticación y autorización basadas en puerto 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.

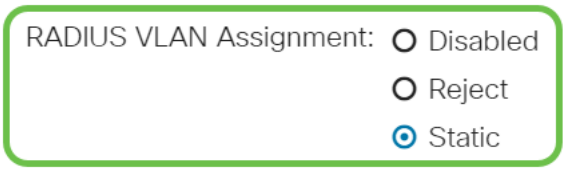


Paso 5 (opcional)

Elija un botón de radio para la Asignación de VLAN RADIUS. Esto habilitará la asignación de VLAN dinámica en el puerto especificado. Las opciones son:

- **Deshabilitado**: 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 información autorizada de VLAN, utilizará la información. Sin embargo, si no hay información de VLAN autorizada, conservará la VLAN original del host.

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.



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.

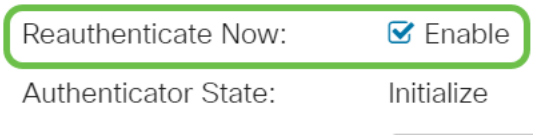
Paso 8

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

Paso 9 (opcional)

Marque la casilla de verificación **Reautenticar ahora** para habilitar la reautenticación inmediata del puerto.

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



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 multisesión.

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.

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.

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.

Paso 14

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

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.

Paso 16

Haga clic en Apply (Aplicar).

Ahora debería haber configurado correctamente la autenticación 802.1x en su switch.

Para obtener más configuraciones, refiérase a la Guía de Administración de Switches Cisco Business 220 Series.

Si desea ver otros artículos, consulte la página de soporte de switches Cisco Business serie 220