Configuración de autenticación de host y sesión 802.1X en switches de la serie 200/220/300

Objetivo

802.1X es un estándar IEEE para el control de acceso a la red (PNAC) basado en puertos que proporciona un método de autenticación a los dispositivos que están conectados a los puertos. La página Host and Session Authentication (Autenticación de sesión y host) de la GUI de administración del switch se utiliza para definir el tipo de autenticación que se utiliza por puerto. La autenticación por puerto es una función que permite que un administrador de red divida los puertos del switch según el tipo de autenticación deseado. La página Hosts Autenticados muestra información sobre los hosts que se han autenticado.

En este artículo se explica cómo configurar la autenticación de sesión y host por puerto y cómo ver los hosts autenticados en los parámetros de seguridad de 802.1X en los switches gestionados de las series 200/220/300.

Dispositivos aplicables

- Serie Sx200
- Serie Sx220
- Serie Sx300

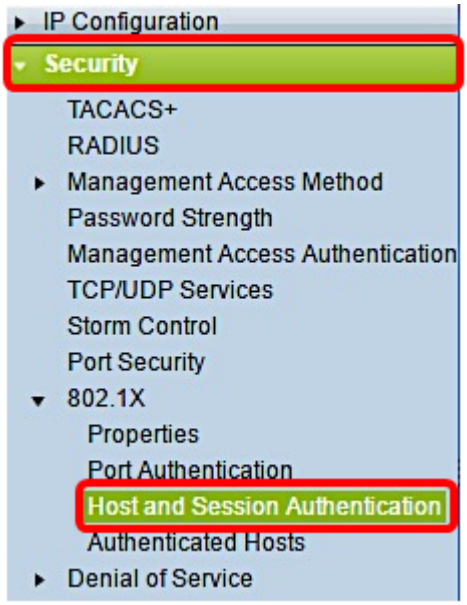
Versión del software

- 1.4.5.02 — Serie Sx200, Serie Sx300
- 1.1.0.14 — Serie Sx220

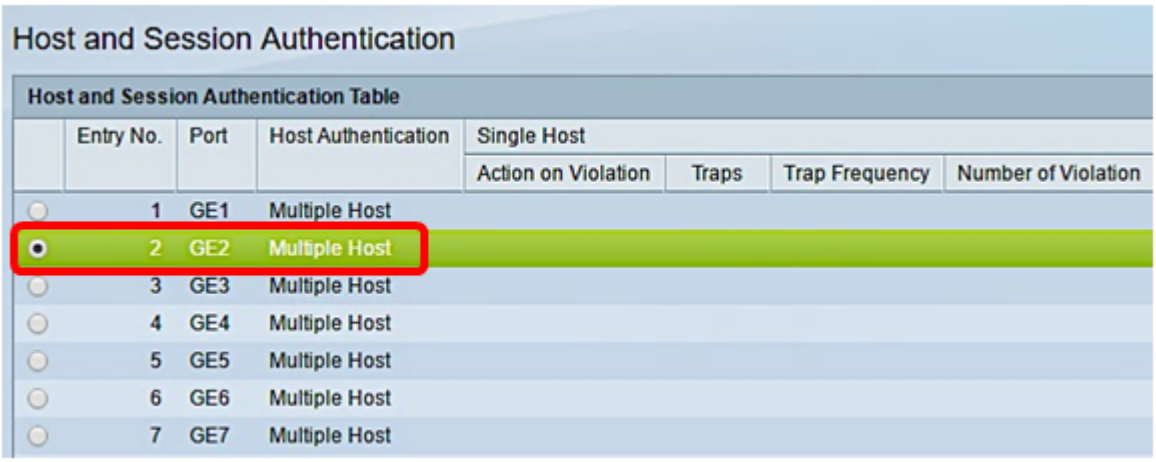
Autenticación de Host y Sesión

Paso 1. Inicie sesión en la utilidad basada en web y elija **Security > 802.1X > Host and Session Authentication**.

Nota: Las imágenes siguientes se han tomado del conmutador inteligente SG220-26P.

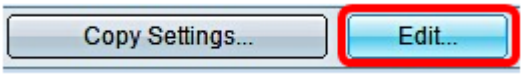


Paso 2. Haga clic en el botón de opción del puerto que desea editar.

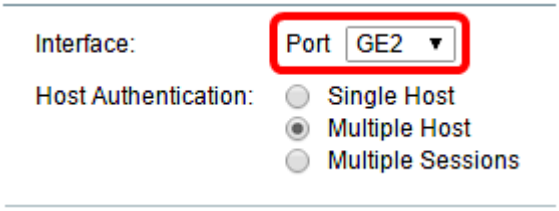


Nota: En este ejemplo, se elige el puerto GE2.

Paso 3. Haga clic en **Edit** para editar la autenticación de host y de sesión para el puerto especificado.



Paso 4. Aparecerá la ventana Editar autenticación de puerto. En la lista desplegable Interface (Interfaz), asegúrese de que el puerto especificado es el elegido en el paso 2. De lo contrario, haga clic en la flecha desplegable y elija el puerto correcto.



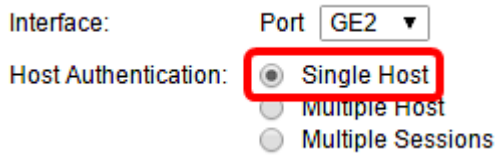
Nota: Si utiliza las series 200 o 300, aparecerá la ventana Editar Autenticación de Host y Sesión.

Paso 5. Haga clic en el botón de opción correspondiente al modo de autenticación deseado

en el campo *Host Authentication*. Las opciones son:

- Host único: el switch solo concede acceso al puerto a un solo host autorizado.
- Varios hosts (802.1X): varios hosts pueden obtener acceso al único puerto. Este es el modo predeterminado. El switch sólo requiere que se autorice el primer host. A partir de ese momento, todos los demás clientes conectados al puerto tendrán acceso a la red. Si la autenticación falla, se deniega el acceso a la red al primer host y a todos los clientes conectados.
- Sesiones Múltiples: Varios hosts pueden obtener acceso al puerto único; sin embargo, cada host debe autenticarse.

Nota: En este ejemplo, se elige Host único.

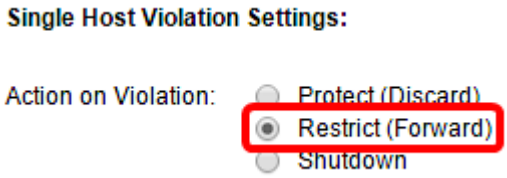


Nota: Si selecciona Host Múltiple o Sesiones Múltiples, vaya al paso 9.

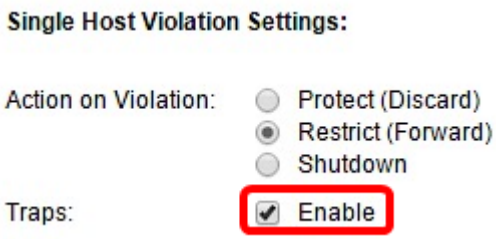
Paso 6. En el área Configuración de una sola violación de host, haga clic en el botón de opción correspondiente a la acción deseada en caso de violación. Una violación ocurre si los paquetes llegan de un host que tiene una dirección MAC que no coincide con la dirección MAC del solicitante original. Cuando esto ocurre, la acción determina qué sucede con los paquetes que llegan de los hosts que no se consideran el suplicante original. Las opciones son:

- Proteger (descartar): descarta los paquetes. Ésta es la acción predeterminada.
- Restringir (reenviar): concede acceso y reenvía los paquetes.
- Shutdown — Bloquea los paquetes y apaga el puerto. El puerto permanece inactivo hasta que se reactiva o hasta que se reinicia el switch.

Nota: En este ejemplo, se elige Restringir (reenviar).



Paso 7. (Opcional) Marque **Enable** en el campo *Traps* para habilitar las trampas. Las trampas son mensajes generados por el Protocolo simple de administración de red (SNMP) que se utilizan para informar sobre eventos del sistema. Cuando se produce una infracción, se envía una trampa al administrador SNMP del switch.



Paso 8. Ingrese el tiempo deseado permitido en segundos entre las trampas enviadas en el campo *Frecuencia de Trampa*. Esto define la frecuencia con que se envían las trampas.

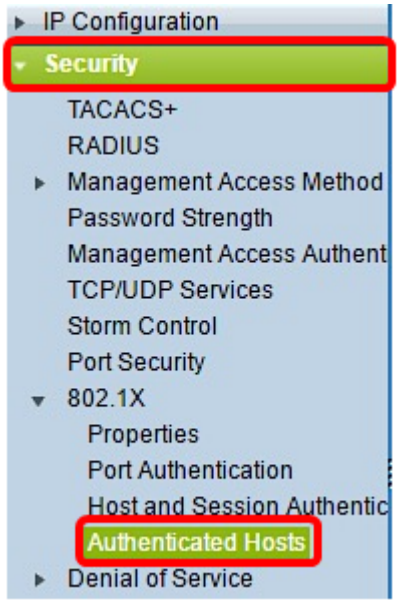
Nota: En este ejemplo, se utilizan 30 segundos.

Paso 9. Haga clic en Apply (Aplicar).

Ahora debería haber configurado la autenticación de host y de sesión en su switch.

Visualización de Hosts Autenticados

Paso 1. Inicie sesión en la utilidad basada en Web y seleccione **Security > 802.1X > Authenticated Host**.



La Tabla Hosts Autenticados muestra la siguiente información para los hosts autenticados.

- Nombre de usuario: especifica el nombre del solicitante autenticado en el puerto.
- Puerto: especifica el número de puerto al que está conectado el solicitante.

- Tiempo de sesión: especifica el tiempo completo que el solicitante estuvo conectado al puerto. El formato es DD:HH:MM:SS (Día:Hora:Minuto:Segundo).
- Método de autenticación: especifica el método utilizado para autenticar. Los valores posibles son:
- Ninguno: especifica que el solicitante no se autenticó.
- Radius — Especifica que el suplicante fue autenticado por el servidor RADIUS.
- Dirección MAC: especifica la dirección MAC del solicitante.
- ID de VLAN: especifica a qué VLAN pertenece el host. La columna VLAN ID solo está disponible en los switches Smart Plus de la serie 220.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).