Configuraciones remotas del servicio de usuario de acceso telefónico de la autorización (RADIUS) en el Switches manejado serie ESW2 350G

Objetivo

El Remote Authentication Dial-In User Service (RADIUS) es un protocolo del cliente o del servidor que proporciona un mecanismo de autenticación para que los dispositivos conecten y utilicen los servicios de red. Estos servicios se extienden del acceso a los archivos compartidos a la impresión compartida. Un servidor de RADIUS es un mecanismo que regula el acceso del usuario a una red informática vía los credenciales de usuario. Por ejemplo, una red inalámbrica pública (de WiFi) está instalada en un campus de la universidad, cualquier usuario NON-autorizado no puede utilizar esta red, sólo las a quién la universidad ha dado a contraseña pueden accederla. El servidor de RADIUS marca las contraseñas ingresadas por los usuarios y concede o niega el acceso como apropiado. Esta característica es útil para asegurar la red contra el acceso no autorizado.

Este artículo explica cómo configurar las configuraciones RADIUS en el Switches manejado serie ESW2 350G.

Dispositivos aplicables

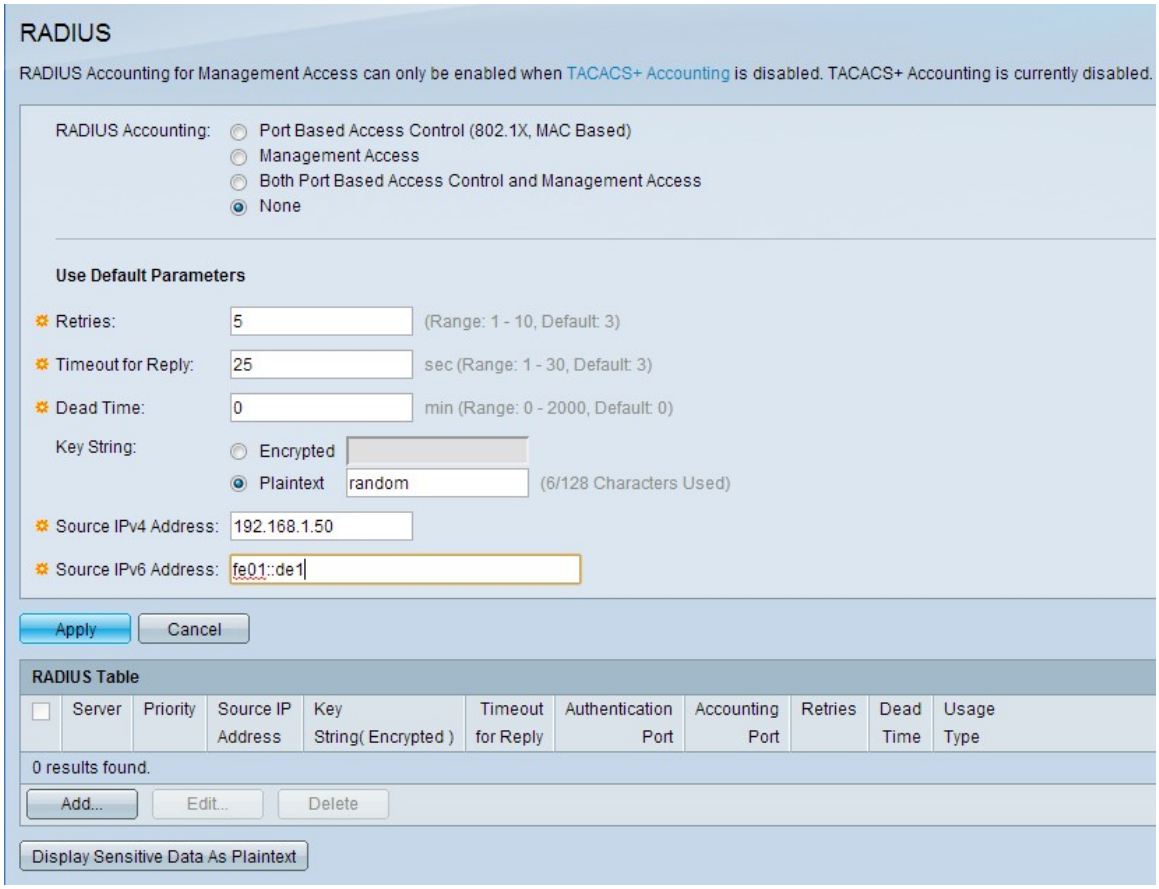
- ESW2-350G-52
- ESW2-350G-52DC

Versión del software

- 1.3.0.62

Configuraciones RADIUS

Paso 1. Inicie sesión a la utilidad de configuración de la red y elija la **Seguridad > el RADIUS** . La página *RADIUS* se abre:



Nota: El Acceso de administración que explica RADIUS puede ser habilitado solamente cuando se inhabilitan las estadísticas TACACS. Refiera a la *configuración del* artículo de los *parámetros TACACS+ y del servidor TACACS+ en el Switches ESW2-350G* para más información sobre esto.

Paso 2. Haga clic un botón de radio para que el tipo de las estadísticas RADIUS sea utilizado en el campo de las estadísticas RADIUS.

Las estadísticas RADIUS permiten que la información sea compartida entre el cliente y el servidor. Los datos se envían al principio de la sesión y en el final de la sesión que indica los recursos usados durante la sesión.

- El puerto basó el control de acceso — Esta opción especifica que utilizan al servidor de RADIUS para el puerto del 802.1x que explica la interacción del servidor/del cliente.
- Acceso de administración — Esta opción especifica que utilizan al servidor de RADIUS para el ingreso del usuario al sistema que explica la interacción del servidor/del cliente.
- Ambos viran el control de acceso y el Acceso de administración hacia el lado de babor basados — Esta opción especifica que utilizan al servidor de RADIUS para ambos las estadísticas y ingreso del usuario al sistema del puerto del 802.1x que explican la interacción del servidor/del cliente.
- Ninguno — Esta opción no permite considerar en el servidor de RADIUS.

Paso 3. En el campo del Retries, ingrese el número de recomprobaciones que una petición pueda ser enviada antes de que se dé un aviso del incidente.

Paso 4. En el descanso para el campo de la contestación, ingrese el tiempo (en los segundos) antes de que se vuelva a enviar una petición por contestar.

Paso 5. En el campo del tiempo muerto, ingrese el tiempo (en los minutos) antes de un servidor de RADIUS insensible se desvía y se mueve al servidor disponible siguiente para intentar la conexión. Un valor de 0 significa que no desvían al servidor de RADIUS.

Paso 6. En el campo dominante de la cadena, haga clic el botón de radio deseado para elegir el tipo de cadena dominante entonces para utilizar ingresan una cadena dominante que las ayudas cifren los mensajes entre el servidor y el cliente. La cadena dominante debe hacer juego la cadena dominante del servidor de RADIUS. Usted puede ingresar la cadena dominante de las maneras siguientes:

• Cifrado — Usted puede ingresar la cadena dominante en la forma encriptada.

• Plaintext — Si usted no ha cifrado la cadena dominante de otro dispositivo, después ingrese como plaintext.

Paso 6 (opcional). En el campo de dirección del IPv4 de la fuente, ingrese el direccionamiento del IPv4 de la fuente que se utilizará.

Paso 7 (opcional). En el campo de dirección del IPv6 de la fuente, ingrese el direccionamiento del IPv6 de la fuente que se utilizará.

Nota: El IPv4 de la fuente y los campos del IPv6 de la fuente están solamente disponibles si el Switch está en el modo de la capa 3. Para conmutar para acodar el modo 3, refiera a los *ajustes de sistema de la configuración del* artículo *en el Switches ESW2-350G.*

Paso 7. El tecleo **se aplica**. Un prompt se visualiza en la cima de la página para indicar si la configuración es acertada o no. Hay también copiar/salvaguardia del prompt la configuración en el archivo.

Nota: Para copiar/configuración de la salvaguardia en el archivo, referir a la *copia o salvar la configuración en el Switch ESW2-350G.*

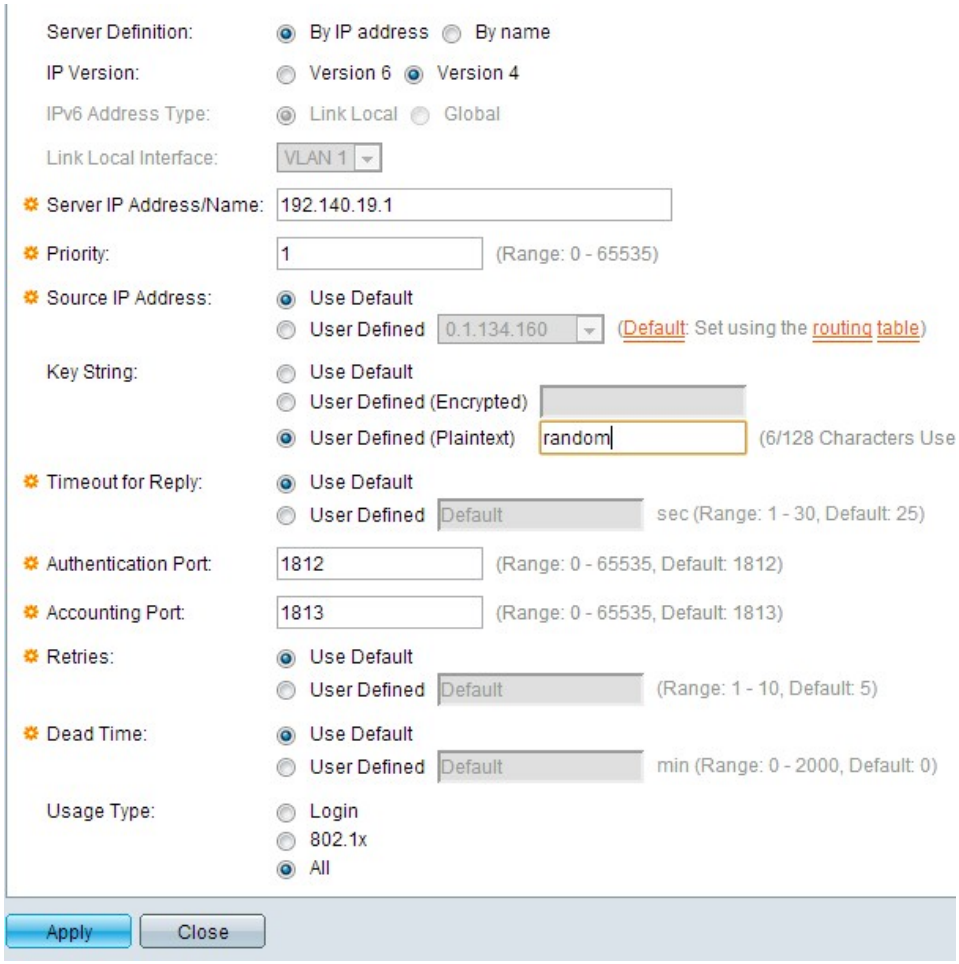
Paso 8. **Datos vulnerables de la visualización del** tecleo **como texto simple** para visualizar los datos vulnerables en el sólo texto.

Maneje a los servidores de RADIUS

La tabla RADIUS permite que un usuario agregue o edite a un servidor Radius configurado.

Este procedimiento muestra cómo agregar a un servidor de RADIUS.

Paso 1. En la tabla RADIUS, el tecleo **agrega** para agregar a un servidor de RADIUS. La ventana del servidor de RADIUS del agregar aparece.



Nota: Para editar a un servidor de RADIUS actual, el tecleo **edita** y edita las propiedades del servidor de RADIUS.

Paso 2. En el campo de definición del servidor, haga clic el botón de radio deseado para elegir si el nombre especifica al servidor de RADIUS la dirección IP o.

- Por la dirección IP — Esta opción define al servidor de RADIUS por la dirección IP.
- Por nombre — Esta opción define al servidor de RADIUS por el nombre.

Paso 3. En versión IP el campo, haga clic el botón de radio deseado para elegir si la dirección IP del servidor de RADIUS es versión 6 o versión 4.

- Versión 6 — Esta opción fija la dirección IP del servidor de RADIUS al direccionamiento sabido del IPv6.
- Versión 4 — Esta opción fija la dirección IP del servidor de RADIUS al direccionamiento sabido del IPv4.

Nota: Si se elige el IPv4, se amortiguan el campo del tipo de dirección del IPv6 y el campo de la interfaz local del link.

Paso 4. Si usted ha hecho clic el botón de radio de la versión 6 en el paso 3, después elija el tipo de dirección del IPv6. Las opciones son:

- Local del link — Los host en una red única se identifican únicamente en el direccionamiento del IPv6. FE80 es el prefijo de una dirección local del link. Este direccionamiento no es routable desde fuera de la red. Soportan a solamente una dirección local del link.

• Global — El direccionamiento global del IPv6 es un direccionamiento de la unidifusión global que es routable desde fuera de la red local.

Paso 5. De la lista desplegable de la interfaz local del link elija la interfaz local deseada del link de las interfaces disponibles del IPv6 creadas en el Switch.

Paso 6. En el dirección IP del servidor/el campo de nombre, ingrese el nombre o el IP Address para el servidor de RADIUS basado en su opción en el paso 2.

Paso 7. En el campo de prioridad, ingrese un nivel de prioridad para el servidor de RADIUS. Para autenticar a un usuario, la prioridad determina la orden que el Switch intenta conectar con los servidores de RADIUS. El valor 0 es la prioridad máxima.

Nota: Si el Switch no puede conectar con el servidor de RADIUS con la prioridad más alta entonces el Switch intenta conectar con el servidor más prioritario siguiente.

Paso 8. En el campo dominante de la cadena, ingrese una cadena dominante que las ayudas cifren los mensajes entre el servidor y el cliente. La cadena dominante debe hacer juego la cadena dominante del servidor de RADIUS. Usted puede ingresar la cadena dominante de diversas maneras como sigue:

• Valor por defecto del uso — Fija la cadena dominante del servidor de RADIUS a la cadena predeterminada.

• Definido por el usario — Permite que un usuario ingrese la cadena dominante en el campo adyacente. Usted puede ingresar los valores definidos por el usuario en uno las dos maneras como sigue:

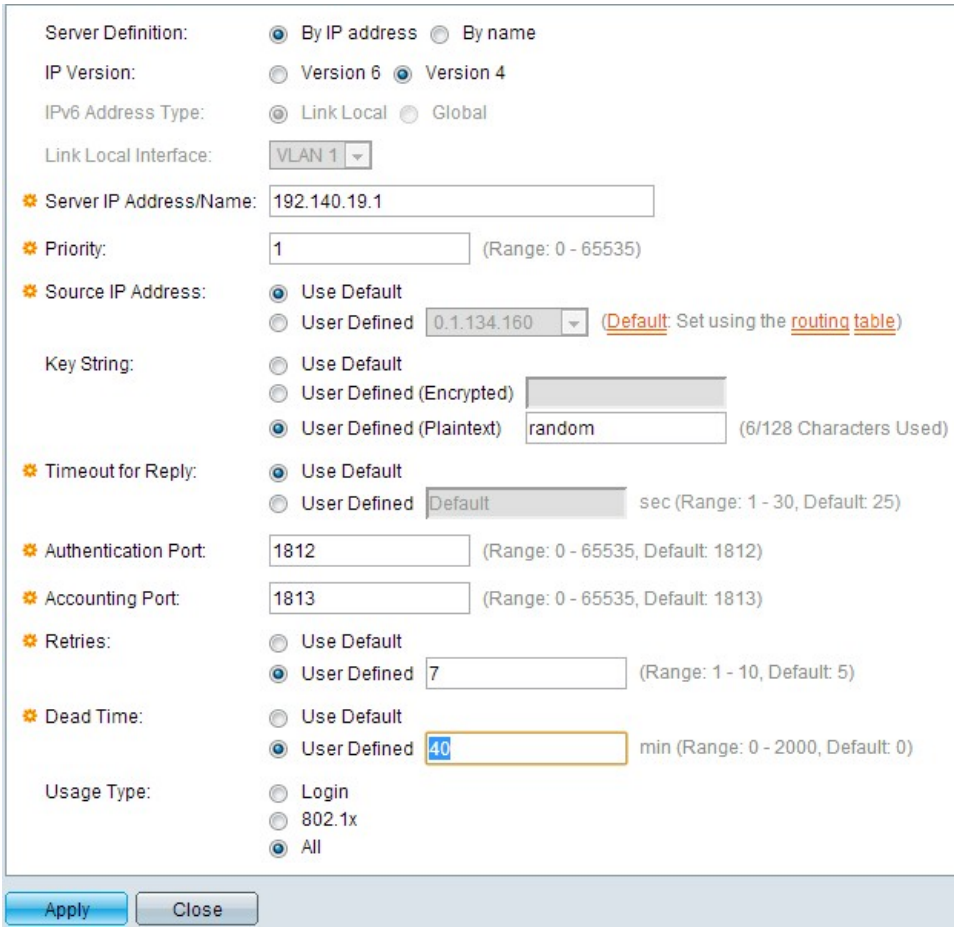
– Cifrado — Usted puede ingresar la cadena dominante en la forma encriptada.

– Plaintext — Si usted no tiene la cadena dominante cifrada de otro dispositivo, después usted puede ingresar como plaintext.

Paso 9. En el descanso para el campo de la contestación, haga clic el botón de radio para fijar la hora (en los segundos) para los cuales el Switch espera el servidor de RADIUS para responder.

• Valor por defecto del uso — Fija el tiempo al valor predeterminado.

• Definido por el usario — Permite que un usuario ingrese el tiempo en el campo adyacente.



Paso 10. En el campo de puerto de autenticación, ingrese el número del puerto usado por el servidor de RADIUS para los pedidos de autenticación.

Paso 11. En el campo de puerto de contabilidad, ingrese el número del puerto usado por el servidor de RADIUS para las peticiones que consideran.

Paso 12. En el campo del Retries, haga clic el botón de radio para el número de peticiones que se envíen al servidor de RADIUS antes de que ocurra un aviso del error.

- Valor por defecto del uso — Utiliza el número predeterminado de recomprobaciones.
- Definido por el usario — Permite que un usuario ingrese el número de recomprobaciones en el campo adyacente.

Paso 13. En el campo del tiempo muerto, haga clic el botón de radio por el tiempo en los minutos antes de que desvíen a un servidor de RADIUS para ser insensible.

- Valor por defecto del uso — Utiliza el tiempo predeterminado.
- Definido por el usario — Permite que un usuario ingrese el tiempo en el campo adyacente.

Nota: Si usted selecciona la opción predeterminada del uso en el paso 8, el paso 9, el paso 12 y el paso 13, se utiliza la configuración del RADIUS predeterminado. Vea la *configuración del* artículo de las *configuraciones del RADIUS predeterminado.*

Paso 14. En el campo del tipo del uso, elija una opción para el tipo de autenticación de servidor de RADIUS.

- Login — Autentica al usuario para el servidor de RADIUS.

- 802.1x — Utiliza la autenticación del 802.1x.
- Todos — Realiza ambas autenticaciones.

Paso 15. Haga clic los **datos vulnerables de la visualización como texto simple** para visualizar los datos vulnerables en el sólo texto.

Paso 16. Haga clic en Apply (Aplicar). Un prompt se visualiza en la cima de la página para indicar si la configuración es acertada o no. Hay también copiar/salvaguardia del prompt la configuración en el archivo. La ventana se cierra y la tabla RADIUS es actualizada.

Nota: Para copiar/configuración de la salvaguardia en el archivo, referir a la *copia o salvar la configuración en el Switch ESW2-350G.*