Administración del dominio en RV220W y RV120W

Objetivos

Utilizan los dominios y a los grupos para aerodinamizar la Administración de las configuraciones del usuario de VPN SSL. En vez de tener que especificar las configuraciones para cada usuario individualmente, usted puede especificar el dominio y las configuraciones de grupo una vez y después asignar a los usuarios a los grupos. Las configuraciones del dominio determinan el método de autentificación. Un usuario puede agregar un nuevo dominio así como editar o borrar los dominios existentes del lista de dominio.

Este documento explica cómo configurar la lista de dominios configurados en el RV120W y el RV220W.

Dispositivos aplicables

- RV120W
- RV220W

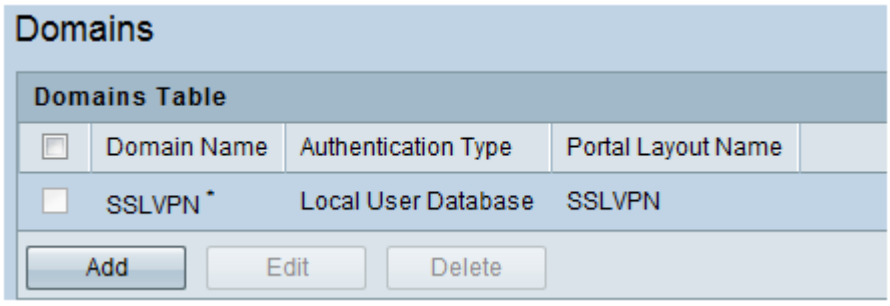
Versión del software

- v1.0.5.8

Configuración del dominio de administración de los usuarios

Agregue un dominio

Paso 1. Inicie sesión a la utilidad de configuración de la red y elija la **administración > User Management (Administración de usuario) > los dominios**. La página de los *dominios* se abre:

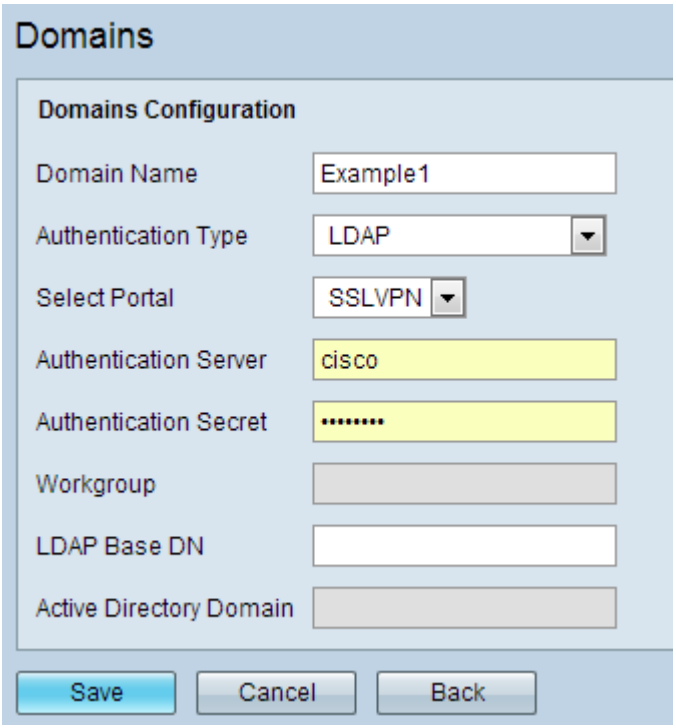


La siguiente información se puede ver en esta página:

- Domain Name — Un Identificador único para el Domain Name.
- Tipo de autenticación — El tipo de autenticación para el dominio creado.
- Nombre porta de la disposición — La disposición porta para el dominio.

Paso 2. El tecleo **agrega** para agregar un nuevo dominio. *La página de configuración de los*

dominios se abre:



Paso 3. Ingrese el Domain Name deseado que se utilizará en el campo del *Domain Name*.

Paso 4. Elija el tipo de servidor de autenticación que se utilizará por el dominio de la lista desplegable del *tipo de autenticación*.

Se describen las opciones como sigue:

• Base de datos de usuarios locales — Utiliza la base de datos de usuarios encontrada localmente.

• RADIUS-PAP — Una implementación del RADIUS donde el cliente se autentica enviando un Nombre de usuario y una contraseña al servidor, que el servidor compara a su base de datos.

• RADIUS-CHAP — Una implementación del RADIUS donde el servidor envía una cadena aleatoriamente generada al cliente, junto con su nombre de host. El cliente utiliza el nombre de host para mirar para arriba la cadena apropiada, lo combina con el desafío, y cifra la cadena usando una función de troceo unidireccional. El resultado se vuelve al servidor para confirmar junto con el nombre de host del cliente.

• RADIUS-MSCHAP — La implementación de Microsoft de RADIUS-CHAP que incluye un cambio controlado por autenticador de la contraseña y los mecanismos de reintentos de la autenticación.

• RADIUS-MSCHAPv2 — La segunda versión de la implementación de Microsoft de RADIUS-CHAP que incluye la autenticación recíproca entre los pis llevando a cuestas un desafío del par.

• Dominio de NT — El dominio de NT es definido teniendo por lo menos un controlador de dominio primario (PDC) donde toda la información sobre seguridad centralmente se guarda el hacer de él fácil para que a los administradores mantengan. En un par a mirar red no se guarda ningún controlador de dominio, toda la información de cuenta de usuario en cada máquina del cliente individual.

• Active Directory — Un servicio de directorio que Microsoft desarrolló para las redes del Dominio de Windows. El controlador de dominio autentica y autoriza a todos los usuarios y los ordenadores en un Dominio de Windows teclean la red, asignando y aplicando las políticas de seguridad y instalar/que ponen al día el software a todos los ordenadores.

• LDAP — El Lightweight Directory Access Protocol (LDAP) es un protocolo del servicio de directorio que se ejecuta en una capa sobre la pila de TCP/IP. Proporciona un mecanismo usado para conectar con, para buscar, y para modificar los directorios de Internet.

Paso 5. Elija el portal que los usuarios utilizarán para conectar de la lista desplegable *porta selecta*. Solamente los usuarios de los dominios asociados a ciertos portales pueden utilizar esos portales para iniciar sesión.

Nota: El portal SSLVPN se selecciona por abandono. Para la información sobre agregar las disposiciones porta se refieren *configurando al servidor VPN SSL* en el *capítulo 5 de la* guía Admin.

Paso 6. Ingrese el nombre del servidor usado para autenticar a los usuarios en el campo del *servidor de autenticación*.

Paso 7. Ingrese la contraseña de autenticación para acceder al servidor del dominio en el campo del *secreto de autenticación*.

El paso 8. (opcional) si la *autenticación de dominio NT* fue elegida en el paso 4, ingresa el nombre o el ID del grupo de trabajo NT en el campo del *grupo de trabajo*.

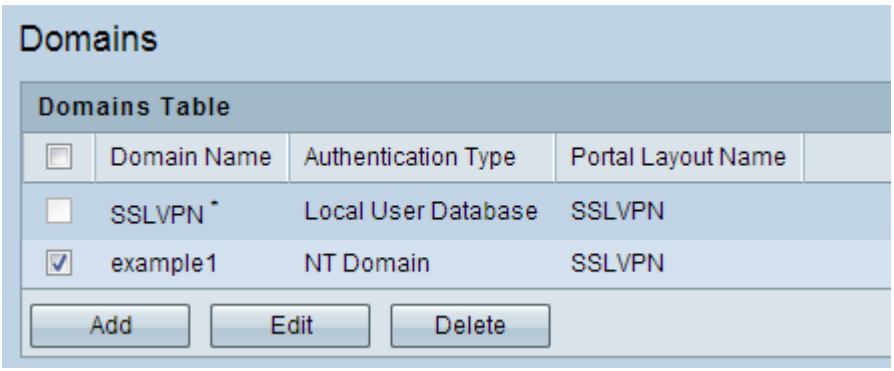
El paso 9. (opcional) si el *LDAP* fue elegido en el paso 4, ingresa el Domain Name bajo en el campo de la *base DN del LDAP*.

El paso 10. (opcional) si el *Active Directory* fue elegido en el paso 4, ingresa el Domain Name del Active Directory en el campo del *dominio del Active Directory*. Los usuarios que se registran en la base de datos del Active Directory pueden acceder el portal VPN SSL.

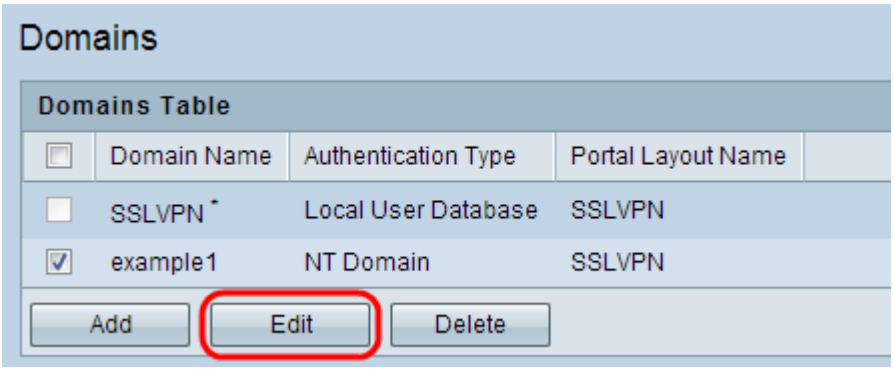
Paso 11 **Salvaguardia del** tecleo para aplicar todas las configuraciones.

Edite un dominio

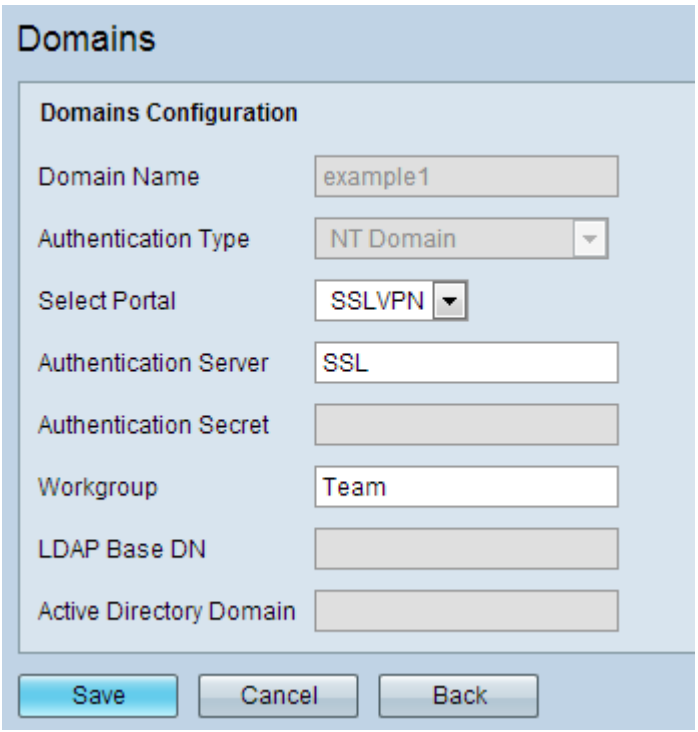
Paso 1. Inicie sesión a la utilidad de configuración de la red y elija la **administración > User Management (Administración de usuario) > los dominios**. La página de los *dominios* se abre:



Paso 2. Marque la casilla de verificación de la entrada deseada para editar.



Paso 3. El tecleo **edita** y la *página de configuración de los dominios* se abre:



Paso 4. Ingrese el Domain Name deseado que se utilizará en el campo del *Domain Name*.

Paso 5. Elija el tipo de servidor de autenticación que se utilizará por el dominio de la lista desplegable del *tipo de autenticación*.

Se describen las opciones como sigue:

• Base de datos de usuarios locales — Utiliza la base de datos de usuarios encontrada localmente.

• RADIUS-PAP — Una implementación del RADIUS donde el cliente se autentica enviando un Nombre de usuario y una contraseña al servidor, que el servidor compara a su base de datos.

• RADIUS-CHAP — Una implementación del RADIUS donde el servidor envía una cadena aleatoriamente generada al cliente, junto con su nombre de host. El cliente utiliza el nombre de host para mirar para arriba la cadena apropiada, lo combina con el desafío, y cifra la cadena usando una función de troceo unidireccional. El resultado se vuelve al servidor para confirmar junto con el nombre de host del cliente.

• RADIUS-MSCHAP — La implementación de Microsoft de RADIUS-CHAP que incluye un cambio controlado por autenticador de la contraseña y los mecanismos de reintentos de la

autenticación.

• RADIUS-MSCHAPv2 — La segunda versión de la implementación de Microsoft de RADIUS-CHAP que incluye la autenticación recíproca entre los pis llevando a cuestas un desafío del par.

• Dominio de NT — El dominio de NT es definido teniendo por lo menos un controlador de dominio primario (PDC) donde toda la información sobre seguridad centralmente se guarda el hacer de él fácil para que a los administradores mantengan.

• Active Directory — Un servicio de directorio que Microsoft desarrolló para las redes del Dominio de Windows. El controlador de dominio autentica y autoriza a todos los usuarios y los ordenadores en un Dominio de Windows teclean la red, asignando y aplicando las políticas de seguridad y instalar/que ponen al día el software a todos los ordenadores.

• LDAP — El Lightweight Directory Access Protocol (LDAP) es un protocolo del servicio de directorio que se ejecuta en una capa sobre la pila de TCP/IP. Proporciona un mecanismo usado para conectar con, para buscar, y para modificar los directorios de Internet.

Paso 6. Elija el portal que los usuarios utilizarán para conectar de la lista desplegable *porta selecta*. Solamente los usuarios de los dominios asociados a ciertos portales pueden utilizar esos portales para iniciar sesión.

Nota: El portal SSLVPN se selecciona por abandono. Para la información sobre agregar las disposiciones porta se refieren *configurando al servidor VPN SSL* en el *capítulo 5 de la* guía Admin.

Paso 7. Ingrese el nombre del servidor usado para autenticar a los usuarios en el campo del *servidor de autenticación*.

Paso 8. Ingrese la contraseña de autenticación para acceder al servidor del dominio en el campo del *secreto de autenticación*.

El paso 9. (opcional) si la *autenticación de dominio NT* fue elegida en el paso 5, ingresa el nombre o el ID del grupo de trabajo NT en el campo del *grupo de trabajo*.

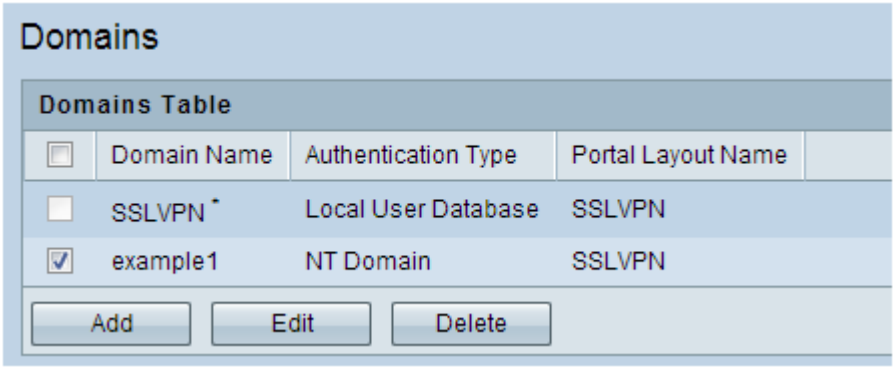
El paso 10. (opcional) si el *LDAP* fue elegido en el paso 5, ingresa el Domain Name bajo en el campo de la *base DN del LDAP*.

El paso 11 (opcional) si el *Active Directory* fue elegido en el paso 5, ingresa el Domain Name del Active Directory en el campo del *dominio del Active Directory*. Los usuarios que se registran en la base de datos del Active Directory pueden acceder el portal VPN SSL.

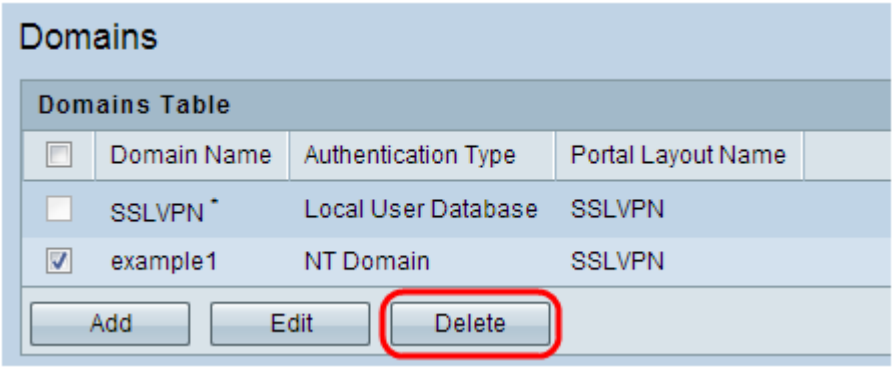
Paso 12. **Salvaguardia del** tecleo para aplicar todas las configuraciones.

Borre un dominio

Paso 1. Inicie sesión a la utilidad de configuración de la red y elija la **administración > User Management (Administración de usuario) > los dominios**. La página de los *dominios* se abre:



Paso 2. Marque la casilla de verificación de la entrada deseada para borrar.



Paso 3. **Cancelación del** tecleo. Se borra el dominio.