

Configuración del protocolo simple de administración de red (SNMP) en RV215W

Objetivo

El protocolo simple de administración de red (SNMP) es un protocolo de capa de aplicación que se utiliza para administrar y supervisar una red. Los administradores de red utilizan SNMP para administrar el rendimiento de la red, detectar y corregir los problemas de red y recopilar estadísticas de red. Una red administrada SNMP consta de dispositivos, agentes y un administrador de red administrados. Los dispositivos administrados son dispositivos capaces de la función SNMP. Un agente es software SNMP en un dispositivo administrado. Un administrador de red es una entidad que recibe datos de los agentes SNMP. El usuario debe instalar un programa de administrador SNMP v3 para ver las notificaciones SNMP.

Este artículo explica cómo configurar SNMP en el RV215W.

Dispositivos aplicables

- RV215W

Versión del software

- 1.1.0.5

Configuración SNMP

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Administration > SNMP**. Se abre la página *SNMP*:

SNMP

SNMP System Information

SNMP: Enable

Engine ID: 80000009033CCE738E0126

SysContact:

SysLocation:

SysName:

SNMPv3 User Configuration

UserName: guest admin

Access Privilege: Read Write User

Security level:

Authentication Algorithm Server: MD5 SHA

Authentication Password:

Privacy Algorithm: DES AES

Privacy Password:

Trap Configuration

IP Address: (Hint: 192.168.1.100 or fec0::64)

Port: (Range: 162 or 1025 - 65535, Default: 162)

Community:

SNMP Version:

Save

Cancel

Información del sistema SNMP

SNMP System Information

SNMP: Enable

Engine ID: 80000009033CCE738E0126

SysContact:

SysLocation:

SysName:

Paso 1. Marque **Enable** en el campo SNMP para permitir la configuración SNMP en el RV215W.

Nota: El ID de motor del agente del RV215W se muestra en el campo Engine ID. Los ID de motor se utilizan para identificar de forma única a los agentes de los dispositivos

administrados.

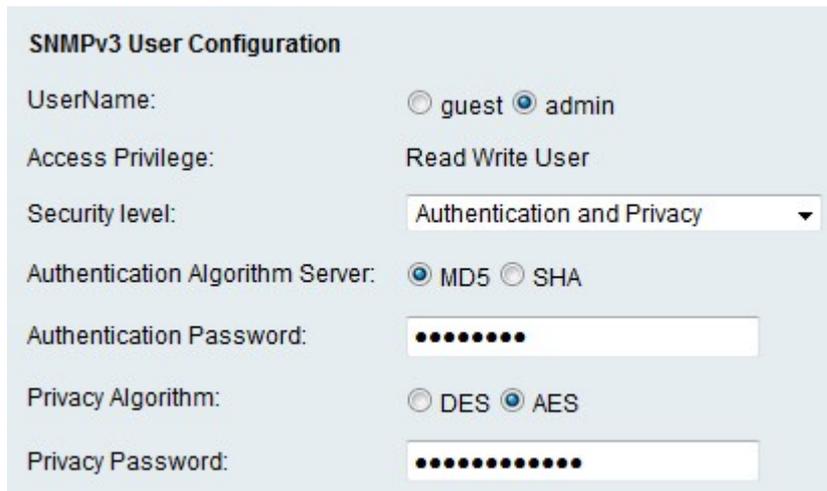
Paso 2. Introduzca un nombre para el contacto del sistema en el campo SysContact (Contacto del sistema). Es práctica habitual incluir información de contacto para el contacto del sistema.

Paso 3. Introduzca la ubicación física del RV215W en el campo SysLocation.

Paso 4. Introduzca un nombre para la identificación del RV215W en el campo SysName.

Paso 5. Click **Save**.

Configuración del usuario SNMPv3



SNMPv3 User Configuration

UserName: guest admin

Access Privilege: Read Write User

Security level: Authentication and Privacy

Authentication Algorithm Server: MD5 SHA

Authentication Password: ●●●●●●●●

Privacy Algorithm: DES AES

Privacy Password: ●●●●●●●●●●●●

Paso 1. Haga clic en el botón de opción correspondiente a la cuenta deseada para configurarla en el campo UserName. El privilegio de acceso del usuario se muestra en el campo Privilegio de acceso.

·invitado: un usuario invitado solo tiene privilegios de lectura.

·Admin: un usuario administrador tiene privilegios de lectura y escritura.

Paso 2. En la lista desplegable Nivel de seguridad, elija la seguridad deseada. La autenticación se utiliza para autenticar y permitir a los usuarios ver o administrar las funciones SNMP. La privacidad es otra clave que se puede utilizar para aumentar la seguridad de la función SNMP.

·Sin autenticación y Sin privacidad: el usuario no necesita autenticación ni contraseña de privacidad.

Autenticación · y Sin privacidad: el usuario sólo requiere autenticación.

Autenticación y privacidad ·: el usuario requiere tanto la autenticación como una contraseña de privacidad.

Paso 3. Si el nivel de seguridad incluye la autenticación, haga clic en el botón de opción correspondiente al servidor deseado en el campo Servidor de algoritmo de autenticación. Este algoritmo es una función hash. Las funciones hash se utilizan para convertir las claves en un mensaje de bit designado.

·MD5: Message-Digest 5 (MD5) es un algoritmo que toma una entrada y produce un

resumen de mensaje de 128 bits de la entrada.

·SHA: Secure Hash Algorithm (SHA) es un algoritmo que toma una entrada y produce un resumen de mensaje de 160 bits de la entrada.

Paso 4. Introduzca una contraseña para los usuarios en el campo Contraseña de autenticación.

Paso 5. Si el nivel de seguridad incluye la privacidad, haga clic en el botón de opción correspondiente al algoritmo deseado en el campo Algoritmo de privacidad.

·DES: el estándar de cifrado de datos (DES) es un algoritmo de cifrado que utiliza el mismo método para cifrar y descifrar un mensaje. El algoritmo DES procesa más rápido que AES.

·AES: el estándar de cifrado avanzado (AES) es un algoritmo de cifrado que utiliza diferentes métodos para cifrar y descifrar un mensaje. Esto hace que AES sea un algoritmo de cifrado más seguro que DES.

Paso 6. Introduzca una contraseña de privacidad para los usuarios en el campo Contraseña de privacidad.

Paso 7. Click **Save**.

Configuración de trampa

Las trampas son mensajes SNMP generados que se utilizan para informar de eventos del sistema. Una trampa obligará a un dispositivo administrado a enviar un mensaje SNMP al administrador de red que notifica al administrador de red un evento del sistema.



The image shows a 'Trap Configuration' form with the following fields and values:

Field	Value	Hint/Range
IP Address:	192.168.1.100	(Hint: 192.168.1.100 or fec0::64)
Port:	162	(Range: 162 or 1025 - 65535, Default: 162)
Community:	community1	
SNMP Version:	v1	

Paso 1. Introduzca la dirección IP a la que se enviarán las notificaciones de trampa en el campo Dirección IP.

Paso 2. Introduzca el número de puerto de la dirección IP a la que se enviarán las notificaciones de trampa en el campo Puerto.

Paso 3. Introduzca la cadena de comunidad a la que pertenece el administrador de capturas en el campo Comunidad. Una cadena de comunidad es una cadena de texto que actúa como contraseña. SNMP lo utiliza para autenticar los mensajes enviados entre un agente y un administrador de red.

Nota: Este campo sólo se aplica si la versión de trampa SNMP no es la versión 3.

Paso 4. En la lista desplegable Versión SNMP, elija la versión del administrador SNMP para los mensajes de trampa SNMP.

·v1: utiliza una cadena de comunidad para autenticar los mensajes de trampa.

·v2c: utiliza una cadena de comunidad para autenticar los mensajes de trampa.

·v3: utiliza contraseñas cifradas para autenticar mensajes de trampa.

Paso 5. Click **Save**.