

Configurazione SNMP (Simple Network Management Protocol) su RV215W

Obiettivo

Il protocollo SNMP (Simple Network Management Protocol) è un protocollo a livello di applicazione utilizzato per gestire e monitorare una rete. L'SNMP viene utilizzato dagli amministratori di rete per gestire le prestazioni, rilevare e correggere problemi e raccogliere statistiche sulla rete. Una rete gestita SNMP è costituita da dispositivi gestiti, agenti e un gestore di rete. I dispositivi gestiti sono dispositivi che supportano la funzione SNMP. Un agente è un software SNMP su un dispositivo gestito. Un gestore di rete è un'entità che riceve i dati dagli agenti SNMP. L'utente deve installare un programma di gestione SNMP v3 per visualizzare le notifiche SNMP.

Questo articolo spiega come configurare il protocollo SNMP sull'RV215W.

Dispositivi interessati

RV215W

Versione del software

•1.1.0.5

Configurazione SNMP

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Amministrazione > SNMP**. Viene visualizzata la pagina *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

Informazioni di sistema SNMP

SNMP System Information

SNMP: Enable

Engine ID: 80000009033CCE738E0126

SysContact:

SysLocation:

SysName:

Passaggio 1. Selezionare **Enable** (Abilita) nel campo SNMP per consentire la configurazione SNMP sull'RV215W.

Nota: Nel campo ID motore viene visualizzato l'ID motore per l'agente RV215W. Gli ID dei motori vengono utilizzati per identificare in modo univoco gli agenti sui dispositivi gestiti.

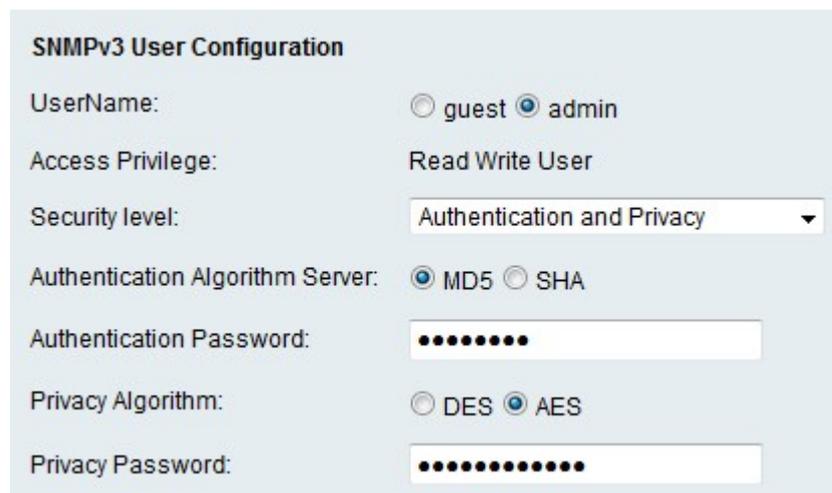
Passaggio 2. Inserire un nome per il contatto di sistema nel campo SysContact. È prassi comune includere informazioni di contatto per il contatto di sistema.

Passaggio 3. Inserire l'ubicazione fisica della RV215W nel campo SysLocation.

Passaggio 4. Inserire un nome per l'identificazione della RV215W nel campo SysName.

Passaggio 5. Fare clic su **Salva**.

Configurazione utente 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:

Passaggio 1. Fare clic sul pulsante di opzione corrispondente all'account desiderato da configurare nel campo UserName. Il privilegio di accesso dell'utente viene visualizzato nel campo Privilegio di accesso.

·Guest: un utente guest dispone solo dei privilegi di lettura.

·Amministratore: un utente amministratore dispone di privilegi di lettura e scrittura.

Passaggio 2. Dall'elenco a discesa Livello di protezione scegliere la protezione desiderata. L'autenticazione viene utilizzata per autenticare e consentire agli utenti di visualizzare o gestire le funzionalità SNMP. La privacy è un'altra chiave che può essere utilizzata per aumentare la sicurezza sulla funzione SNMP.

·Nessuna autenticazione e nessuna privacy: l'utente non richiede alcuna password di autenticazione o privacy.

·Autenticazione e nessuna privacy: l'utente richiede solo l'autenticazione.

·Autenticazione e privacy: l'utente richiede sia l'autenticazione che una password per la privacy.

Passaggio 3. Se il livello di protezione include l'autenticazione, fare clic sul pulsante di opzione corrispondente al server desiderato nel campo Server algoritmo di autenticazione. Questo algoritmo è una funzione hash. Le funzioni hash vengono utilizzate per convertire le chiavi in un messaggio di bit designato.

·MD5 — Message-Digest 5 (MD5) è un algoritmo che accetta un input e produce un digest del messaggio a 128 bit dell'input.

·SHA — Secure Hash Algorithm (SHA) è un algoritmo che accetta un input e produce un

digest del messaggio a 160 bit dell'input.

Passaggio 4. Immettere una password per gli utenti nel campo Password di autenticazione.

Passaggio 5. Se il livello di protezione include la privacy, fare clic sul pulsante di opzione corrispondente all'algoritmo desiderato nel campo Algoritmo di privacy.

·DES: Data Encryption Standard (DES) è un algoritmo di crittografia che utilizza lo stesso metodo per crittografare e decrittografare un messaggio. L'algoritmo DES viene elaborato più rapidamente di AES.

·AES - Advanced Encryption Standard (AES) è un algoritmo di crittografia che utilizza metodi diversi per crittografare e decrittografare un messaggio. Ciò rende AES un algoritmo di crittografia più sicuro di DES.

Passaggio 6. Immettere una password di privacy per gli utenti nel campo Password privacy.

Passaggio 7. Fare clic su **Salva**.

Configurazione trap

I trap sono messaggi SNMP generati utilizzati per segnalare gli eventi di sistema. Una trap forzerà un dispositivo gestito a inviare un messaggio SNMP al gestore della rete che notifica al gestore della rete un evento di sistema.



The screenshot 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	

Passaggio 1. Immettere l'indirizzo IP a cui verranno inviate le notifiche di trap nel campo Indirizzo IP.

Passaggio 2. Immettere il numero di porta dell'indirizzo IP a cui verranno inviate le notifiche di trap nel campo Porta.

Passaggio 3. Inserire nel campo Community la stringa della community a cui appartiene il gestore di trap. Una stringa della community è una stringa di testo che funge da password. Viene utilizzato dal protocollo SNMP per autenticare i messaggi inviati tra un agente e un gestore di rete.

Nota: Questo campo è applicabile solo se la versione della trap SNMP non è la versione 3.

Passaggio 4. Dall'elenco a discesa SNMP Version (Versione SNMP), selezionare la versione di SNMP Manager per i messaggi trap SNMP.

·v1 — Utilizza una stringa della community per autenticare i messaggi trap.

·v2c: utilizza una stringa della community per autenticare i messaggi trap.

·v3: utilizza password crittografate per autenticare i messaggi trap.

Passaggio 5. Fare clic su **Salva**.