

SNMP-Konfiguration (Simple Network Management Protocol) auf RV215W

Ziel

Simple Network Management Protocol (SNMP) ist ein Protokoll auf Anwendungsebene, das zur Verwaltung und Überwachung eines Netzwerks verwendet wird. SNMP wird von Netzwerkadministratoren verwendet, um die Netzwerkleistung zu verwalten, Netzwerkprobleme zu erkennen und zu beheben und Netzwerkstatistiken zu erfassen. Ein verwaltetes SNMP-Netzwerk besteht aus verwalteten Geräten, Agenten und einem Netzwerkmanager. Verwaltete Geräte sind Geräte, die die SNMP-Funktion unterstützen. Ein Agent ist SNMP-Software auf einem verwalteten Gerät. Ein Netzwerkmanager ist eine Einheit, die Daten von den SNMP-Agenten empfängt. Der Benutzer muss ein SNMP v3-Manager-Programm installieren, um SNMP-Benachrichtigungen anzuzeigen.

In diesem Artikel wird beschrieben, wie SNMP auf der RV215W konfiguriert wird.

Anwendbare Geräte

RV215W

Softwareversion

·1.1.0.5

SNMP-Konfiguration

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Administration > SNMP** aus. Die Seite *SNMP* wird geöffnet:

SNMP

SNMP System Information

SNMP:	<input checked="" type="checkbox"/> Enable
Engine ID:	80000009033CCE738E0126
SysContact:	<input type="text" value="contact contact@email.com"/>
SysLocation:	<input type="text" value="3rd floor Rack #3"/>
SysName:	<input type="text" value="router8E0126"/>

SNMPv3 User Configuration

UserName:	<input type="radio"/> guest <input checked="" type="radio"/> admin
Access Privilege:	Read Write User
Security level:	<input type="text" value="Authentication and Privacy"/>
Authentication Algorithm Server:	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Authentication Password:	<input type="password" value="••••••••"/>
Privacy Algorithm:	<input type="radio"/> DES <input checked="" type="radio"/> AES
Privacy Password:	<input type="password" value="••••••••••"/>

Trap Configuration

IP Address:	<input type="text" value="192.168.1.100"/> (Hint: 192.168.1.100 or fec0::64)
Port:	<input type="text" value="162"/> (Range: 162 or 1025 - 65535, Default: 162)
Community:	<input type="text" value="community1"/>
SNMP Version:	<input type="text" value="v1"/>

Save

Cancel

SNMP-Systeminformationen

SNMP System Information

SNMP:	<input checked="" type="checkbox"/> Enable
Engine ID:	80000009033CCE738E0126
SysContact:	<input type="text" value="contact contact@email.com"/>
SysLocation:	<input type="text" value="3rd floor Rack #3"/>
SysName:	<input type="text" value="router8E0126"/>

Schritt 1: Aktivieren Sie im Feld **SNMP Aktivieren**, um die SNMP-Konfiguration für den RV215W zuzulassen.

Hinweis: Die Engine-ID für den Agenten des RV215W wird im Feld Engine ID (Engine-ID) angezeigt. Engine-IDs werden verwendet, um Agenten auf verwalteten Geräten eindeutig zu

identifizieren.

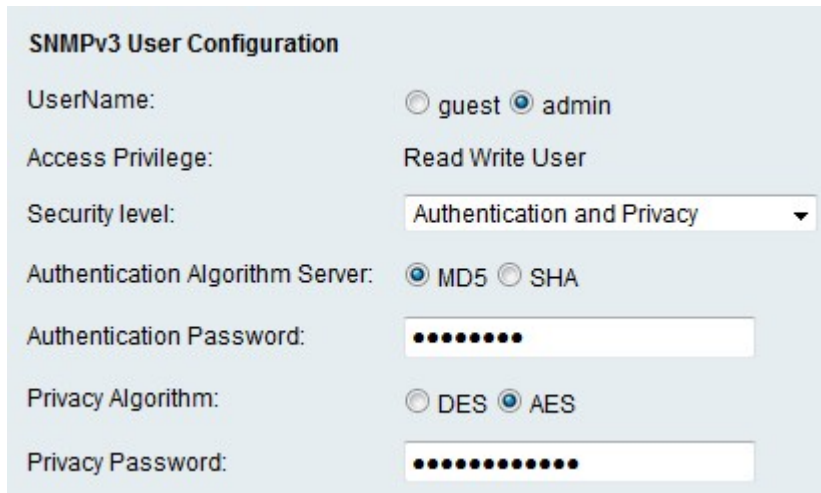
Schritt 2: Geben Sie im Feld SysContact einen Namen für den Systemkontakt ein. Es ist gängige Praxis, Kontaktdaten für den Systemkontakt einzuschließen.

Schritt 3: Geben Sie im Feld SysLocation den physischen Standort des RV215W ein.

Schritt 4: Geben Sie im Feld SysName einen Namen zur Identifizierung des RV215W ein.

Schritt 5: Klicken Sie auf **Speichern**.

SNMPv3-Benutzerkonfiguration



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:

Schritt 1: Klicken Sie auf das Optionsfeld für das gewünschte Konto, das im Feld UserName konfiguriert werden soll. Die Zugriffsberechtigung des Benutzers wird im Feld Zugriffsberechtigung angezeigt.

·Guest (Gast): Ein Gastbenutzer hat nur Leseberechtigungen.

·Admin - Ein Admin-Benutzer hat Lese- und Schreibrechte.

Schritt 2: Wählen Sie aus der Dropdown-Liste Security Level (Sicherheitsstufe) die gewünschte Sicherheit aus. Die Authentifizierung dient zur Authentifizierung und zum Anzeigen oder Verwalten der SNMP-Funktionen. Datenschutz ist ein weiterer Schlüssel, mit dem die Sicherheit der SNMP-Funktion erhöht werden kann.

·Keine Authentifizierung und kein Datenschutz - Der Benutzer benötigt keine Authentifizierung oder kein Datenschutzkennwort.

·Authentifizierung und "Kein Datenschutz" - Nur Authentifizierung ist vom Benutzer erforderlich.

·Authentifizierung und Datenschutz - Der Benutzer benötigt sowohl eine Authentifizierung als auch ein Datenschutzkennwort.

Schritt 3: Wenn die Sicherheitsstufe Authentifizierung umfasst, klicken Sie im Feld Authentifizierungsalgorithmus-Server auf das Optionsfeld für den gewünschten Server. Dieser Algorithmus ist eine Hashfunktion. Hashfunktionen werden verwendet, um Schlüssel in eine bestimmte Bitnachricht zu konvertieren.

·MD5 — Message-Digest 5 (MD5) ist ein Algorithmus, der eine Eingabe akzeptiert und

einen 128-Bit-Message-Digest der Eingabe erzeugt.

·SHA - Secure Hash Algorithm (SHA) ist ein Algorithmus, der eine Eingabe annimmt und einen 160-Bit-Message-Digest der Eingabe erstellt.

Schritt 4: Geben Sie im Feld Authentifizierungskennwort ein Kennwort für die Benutzer ein.

Schritt 5: Wenn die Sicherheitsstufe Datenschutz beinhaltet, klicken Sie im Feld Privacy Algorithm (Datenschutzalgorithmus) auf das Optionsfeld für den gewünschten Algorithmus.

·DES - Data Encryption Standard (DES) ist ein Verschlüsselungsalgorithmus, der dieselbe Methode zur Verschlüsselung und Entschlüsselung einer Nachricht verwendet. Der DES-Algorithmus verarbeitet schneller als AES.

·AES - Advanced Encryption Standard (AES) ist ein Verschlüsselungsalgorithmus, der verschiedene Methoden zum Verschlüsseln und Entschlüsseln von Nachrichten verwendet. Dies macht AES zu einem sichereren Verschlüsselungsalgorithmus als DES.

Schritt 6: Geben Sie im Feld Privacy Password (Datenschutzkennwort) ein Datenschutzkennwort für die Benutzer ein.

Schritt 7: Klicken Sie auf **Speichern**.

Trap-Konfiguration

Traps werden zum Melden von Systemereignissen verwendet. Ein Trap zwingt ein verwaltetes Gerät, eine SNMP-Nachricht an den Netzwerkmanager zu senden, die den Netzwerkmanager über ein Systemereignis benachrichtigt.



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	

Schritt 1: Geben Sie die IP-Adresse ein, an die die Trap-Benachrichtigungen gesendet werden sollen.

Schritt 2: Geben Sie die Portnummer der IP-Adresse ein, an die die Trap-Benachrichtigungen im Feld Port gesendet werden.

Schritt 3: Geben Sie im Community-Feld den Community-String ein, zu dem der Trap-Manager gehört. Ein Community String ist eine Zeichenfolge, die als Kennwort fungiert. SNMP wird verwendet, um Nachrichten zu authentifizieren, die zwischen einem Agenten und einem Netzwerkmanager gesendet werden.

Hinweis: Dieses Feld ist nur gültig, wenn die SNMP-Trap-Version nicht Version 3 ist.

Schritt 4: Wählen Sie aus der Dropdown-Liste SNMP Version (SNMP-Version) die SNMP Manager-Version für die SNMP-Trap-Meldungen aus.

·v1 - Verwendet einen Community-String, um Trap-Nachrichten zu authentifizieren.

·v2c - Verwendet einen Community-String, um Trap-Nachrichten zu authentifizieren.

·v3 - Verwendet verschlüsselte Kennwörter, um Trap-Nachrichten zu authentifizieren.

Schritt 5: Klicken Sie auf **Speichern**.