

Configuration SNMP (Simple Network Management Protocol) sur RV215W

Objectif

Le protocole SNMP (Simple Network Management Protocol) est un protocole de couche application utilisé pour gérer et surveiller un réseau. Le protocole SNMP est utilisé par les administrateurs réseau pour gérer les performances réseau, détecter et corriger les problèmes réseau et collecter des statistiques réseau. Un réseau géré SNMP se compose de périphériques gérés, d'agents et d'un gestionnaire de réseau. Les périphériques gérés sont des périphériques capables de la fonctionnalité SNMP. Un agent est un logiciel SNMP sur un périphérique géré. Un gestionnaire de réseau est une entité qui reçoit des données des agents SNMP. L'utilisateur doit installer un programme de gestion SNMP v3 pour afficher les notifications SNMP.

Cet article explique comment configurer SNMP sur le RV215W.

Périphériques pertinents

- RV215W

Version du logiciel

- 1.1.0.5

Configuration SNMP

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Administration > SNMP**. La page *SNMP* s'ouvre :

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

Informations sur le système SNMP

SNMP System Information

SNMP: Enable

Engine ID: 80000009033CCE738E0126

SysContact:

SysLocation:

SysName:

Étape 1. Cochez **Enable** dans le champ SNMP pour autoriser la configuration SNMP sur le RV215W.

Note: L'ID de moteur de l'agent du RV215W s'affiche dans le champ ID de moteur. Les ID de moteur sont utilisés pour identifier de manière unique les agents sur les périphériques gérés.

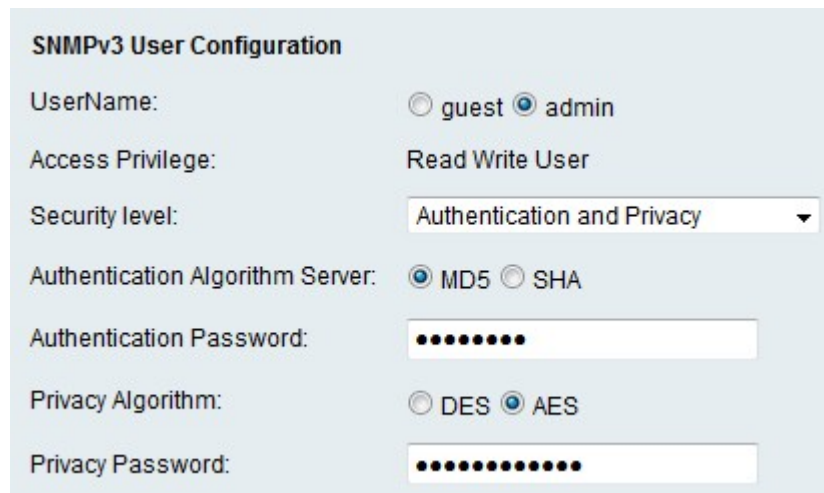
Étape 2. Entrez un nom pour le contact système dans le champ SysContact. Il est courant d'inclure les coordonnées du contact système.

Étape 3. Saisissez l'emplacement physique du RV215W dans le champ SysLocation.

Étape 4. Entrez un nom pour l'identification du RV215W dans le champ SysName.

Étape 5. Cliquez **Save**.

Configuration utilisateur 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:

Étape 1. Sélectionnez la case d'option correspondant au compte souhaité à configurer dans le champ UserName. Le privilège d'accès de l'utilisateur s'affiche dans le champ Privilège d'accès.

·invité : un utilisateur invité ne dispose que de privilèges de lecture.

·Admin : un utilisateur admin dispose de privilèges de lecture et d'écriture.

Étape 2. Dans la liste déroulante Niveau de sécurité, sélectionnez la sécurité souhaitée. L'authentification est utilisée pour authentifier et permettre aux utilisateurs d'afficher ou de gérer les fonctionnalités SNMP. La confidentialité est une autre clé qui peut être utilisée pour accroître la sécurité sur la fonctionnalité SNMP.

·Pas d'authentification et pas de confidentialité : aucune authentification ou mot de passe de confidentialité n'est requis par l'utilisateur.

Authentification · et absence de confidentialité : seule l'authentification est requise par l'utilisateur.

Authentification · et confidentialité : l'utilisateur doit utiliser à la fois l'authentification et un mot de passe de confidentialité.

Étape 3. Si le niveau de sécurité inclut l'authentification, cliquez sur la case d'option correspondant au serveur souhaité dans le champ Authentication Algorithm Server. Cet algorithme est une fonction de hachage. Les fonctions de hachage sont utilisées pour convertir des clés en message binaire désigné.

·MD5 — Message-Digest 5 (MD5) est un algorithme qui prend une entrée et produit un résumé de message de 128 bits de l'entrée.

·SHA — SHA (Secure Hash Algorithm) est un algorithme qui prend une entrée et produit un résumé de message de 160 bits de l'entrée.

Étape 4. Saisissez un mot de passe pour les utilisateurs dans le champ Authentication Password (Mot de passe d'authentification).

Étape 5. Si le niveau de sécurité inclut la confidentialité, cliquez sur la case d'option correspondant à l'algorithme souhaité dans le champ Privacy Algorithm.

·DES - Data Encryption Standard (DES) est un algorithme de chiffrement qui utilise la même méthode pour chiffrer et déchiffrer un message. L'algorithme DES traite plus rapidement qu'AES.

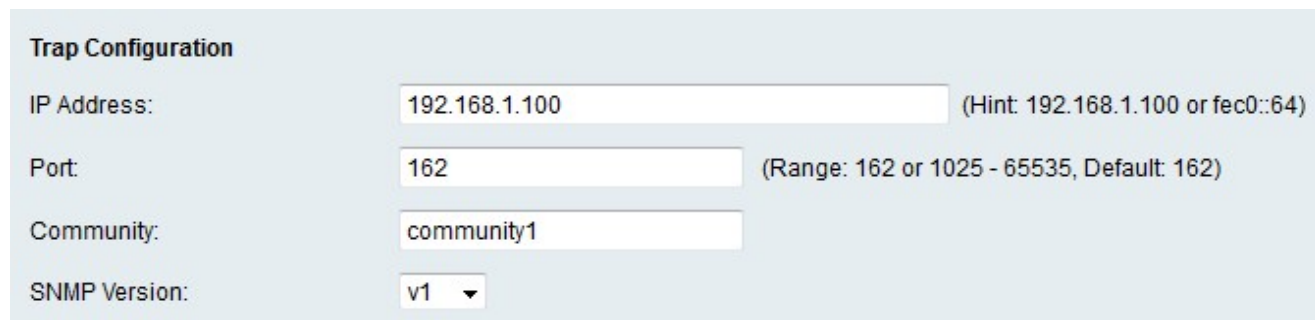
·AES - Advanced Encryption Standard (AES) est un algorithme de chiffrement qui utilise différentes méthodes pour chiffrer et déchiffrer un message. AES devient ainsi un algorithme de chiffrement plus sécurisé que DES.

Étape 6. Saisissez un mot de passe de confidentialité pour les utilisateurs dans le champ Privacy Password.

Étape 7. Cliquez **Save**.

Configuration du déROUTement

Les interruptions sont des messages SNMP générés utilisés pour signaler les événements système. Un déROUTement force un périphérique géré à envoyer un message SNMP au gestionnaire de réseau qui informe le gestionnaire de réseau d'un événement système.



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	

Étape 1. Saisissez l'adresse IP à laquelle les notifications de déROUTement seront envoyées dans le champ IP address.

Étape 2. Saisissez le numéro de port de l'adresse IP à laquelle les notifications de déROUTement seront envoyées dans le champ Port.

Étape 3. Entrez la chaîne de communauté à laquelle appartient le gestionnaire de déROUTements dans le champ Communauté. Une chaîne de communauté est une chaîne de texte qui agit comme un mot de passe. Il est utilisé par SNMP pour authentifier les messages envoyés entre un agent et un gestionnaire de réseau.

Note: Ce champ ne s'applique que si la version de déROUTement SNMP n'est pas la version 3.

Étape 4. Dans la liste déroulante Version SNMP, sélectionnez la version du gestionnaire SNMP pour les messages d'interruption SNMP.

·v1 : utilise une chaîne de communauté pour authentifier les messages de déROUTement.

·v2c : utilise une chaîne de communauté pour authentifier les messages de déroutement.

·v3 : utilise des mots de passe chiffrés pour authentifier les messages de déroutement.

Étape 5. Cliquez **Save**.