Configuration de Protocole SNMP (Simple Network Management Protocol) sur RV215W

Objectif

Le Protocole SNMP (Simple Network Management Protocol) est un protocole de la couche applicative qui est utilisé pour gérer et surveiller un réseau. Le SNMP est utilisé par des administrateurs réseau pour traiter des performances du réseau, pour les détecter et des problèmes de réseau approprié, et pour recueillir des statistiques de réseau. Un réseau administré SNMP se compose des périphériques gérés, des agents, et d'un gestionnaire de réseau. Les périphériques gérés sont des périphériques qui sont capables de la caractéristique SNMP. Un agent est 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 gestionnaire SNMP v3 pour visualiser des notifications SNMP.

Cet article explique comment configurer le SNMP sur le RV215W.

Périphériques applicables

- RV215W

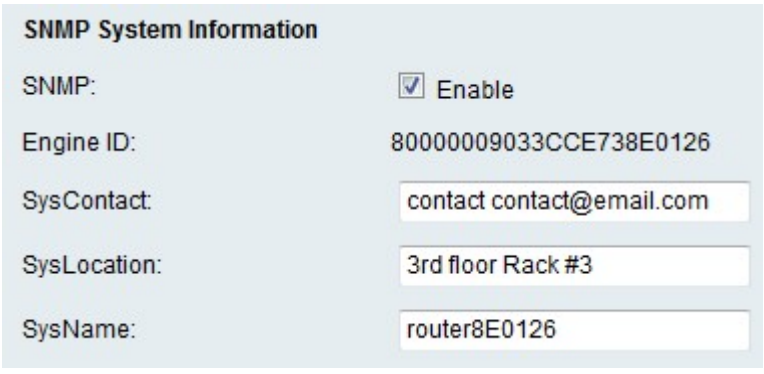
Version de logiciel

- 1.1.0.5

Configuration SNMP

Étape 1. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **gestion > le SNMP**. La page *SNMP* s'ouvre :

Les informations système SNMP



Étape 1. **Enable de** contrôle dans le domaine SNMP pour permettre la configuration SNMP sur le RV215W.

Remarque: L'ID d'engine pour l'agent du RV215W est affiché dans le domaine d'ID du

moteur. Des id d'engine sont utilisés pour identifier seulement des agents sur des périphériques gérés.

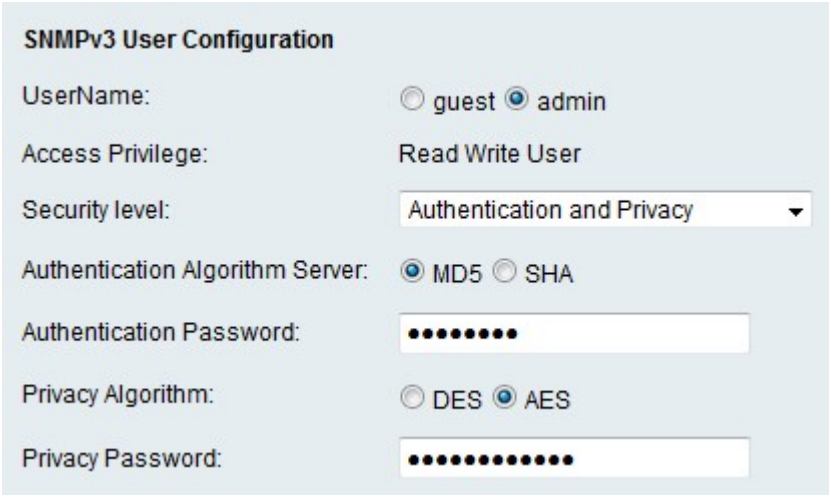
Étape 2. Écrivez un nom pour la personne-ressource du système dans le domaine de SysContact. Il est dans pratique commune d'inclure l'information de contact pour la personne-ressource du système.

Étape 3. Entrez l'emplacement physique du RV215W dans le domaine de SysLocation.

Étape 4. Écrivez un nom pour l'identification du RV215W dans le domaine de SysName.

Étape 5. **Sauvegarde de** clic.

Configuration utilisateur SNMPv3



Étape 1. Cliquez sur la case d'option qui correspond au compte désiré pour configurer dans le domaine de nom d'utilisateur. Le privilège d'accès de l'utilisateur est affiché dans le domaine de privilège d'accès.

- Invité — Un utilisateur d'invité seulement a lu des privilèges.
- Admin — Un utilisateur d'admin a lu et écrit des privilèges.

Étape 2. De la liste déroulante de niveau de Sécurité choisissez la Sécurité désirée. L'authentification est utilisée pour authentifier et permettre à des utilisateurs pour visualiser ou gérer les caractéristiques SNMP. L'intimité est une autre clé qui peut être utilisée pour augmenter la Sécurité sur la caractéristique SNMP.

- Aucune authentification et aucune intimité — Aucun mot de passe d'authentification ou d'intimité n'est exigé par l'utilisateur.
- Authentification et aucune intimité — Seulement l'authentification est exigée par l'utilisateur.
- Authentification et intimité — L'authentification et un mot de passe d'intimité est exigée par l'utilisateur.

Étape 3. Si le niveau de Sécurité inclut l'authentification, cliquez sur la case d'option qui correspond au serveur désiré dans le champ de serveur d'algorithme d'authentification. Cet algorithme est une fonction d'informations parasites. Des fonctions d'informations parasites sont utilisées pour convertir des clés en message indiqué de bit.

• MD5 — Le Message Digest 5 (MD5) est un algorithme qui prend une entrée et produit un condensé de message de 128 bits de l'entrée.

• SHA — L'Algorithme de hachage sûr (SHA) est un algorithme qui prend une entrée et produit un condensé de message de 160 bits de l'entrée.

Étape 4. Entrez un mot de passe pour les utilisateurs dans le domaine de mot de passe d'authentification.

Étape 5. Si le niveau de Sécurité inclut l'intimité, cliquez sur la case d'option qui correspond à l'algorithme désiré dans le domaine d'algorithme d'intimité.

• DES — Le Norme de chiffrement de données (DES) est un algorithme de chiffrement qui emploie la même méthode pour chiffrer et déchiffrer un message. L'algorithme DES traite plus rapide qu'AES.

• AES — Le Norme AES (Advanced Encryption Standard) est un algorithme de chiffrement qui emploie des différentes méthodes pour chiffrer et déchiffrer un message. Ceci fait à AES un algorithme de chiffrement plus sécurisé que le DES.

Étape 6. Entrez un mot de passe d'intimité pour les utilisateurs dans le domaine de mot de passe d'intimité.

Étape 7. **Sauvegarde de** clic.

Configuration de déroutement

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

Étape 1. Écrivez l'adresse IP à laquelle les avis de déroutement seront introduits le champ d'adresse IP.

Étape 2. Introduisez le numéro de port de l'adresse IP à laquelle les avis de déroutement seront introduits le champ de port.

Étape 3. Écrivez la chaîne de la communauté à laquelle le gestionnaire des déroutements appartient à dans le champ de la Communauté. Une chaîne de la communauté est une chaîne de texte qui agit en tant que mot de passe. Il est utilisé par SNMP pour authentifier des messages envoyés entre un agent et un gestionnaire de réseau.

Remarque: Ce champ s'applique seulement si la version de déroutement SNMP n'est pas version 3.

Étape 4. De la liste déroulante de version SNMP choisissez la version de SNMP Manager pour les messages de déroutement SNMP.

- v1 — Emploie une chaîne de la communauté pour authentifier des messages déroutés.
- v2c — Emploie une chaîne de la communauté pour authentifier des messages déroutés.
- v3 — Emploie des mots de passe chiffré pour authentifier des messages déroutés.

Étape 5. **Sauvegarde de** clic.