

RV215WでのSimple Network Management Protocol(SNMP)の設定

目的

Simple Network Management Protocol(SNMP)は、ネットワークの管理と監視に使用されるアプリケーション層プロトコルです。SNMPは、ネットワーク管理者がネットワークパフォーマンスの管理、ネットワークの問題の検出と修正、およびネットワーク統計情報の収集に使用します。SNMP管理ネットワークは、管理対象デバイス、エージェント、およびネットワークマネージャで構成されます。管理対象デバイスは、SNMP機能を使用できるデバイスです。エージェントは、管理対象デバイス上のSNMPソフトウェアです。ネットワークマネージャは、SNMPエージェントからデータを受信するエンティティです。SNMP通知を表示するには、SNMP v3マネージャプログラムをインストールする必要があります。

この記事では、RV215WでSNMPを設定する方法について説明します。

該当するデバイス

- RV215W

[Software Version]

- 1.1.0.5

SNMP の設定 (SNMP Configuration)

ステップ1:Web構成ユーティリティにログインし、[Administration] > [SNMP]を選択します。
。[SNMP]ページが開きます。

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

SNMPシステム情報

SNMP System Information

SNMP: Enable

Engine ID: 80000009033CCE738E0126

SysContact:

SysLocation:

SysName:

ステップ1:RV215WでSNMP設定を許可するには、SNMPフィールドの**Enable**をオンにします。

注：RV215WのエージェントのエンジンIDが[Engine ID]フィールドに表示されます。エンジンIDは、管理対象デバイス上のエージェントを一意に識別するために使用されます。

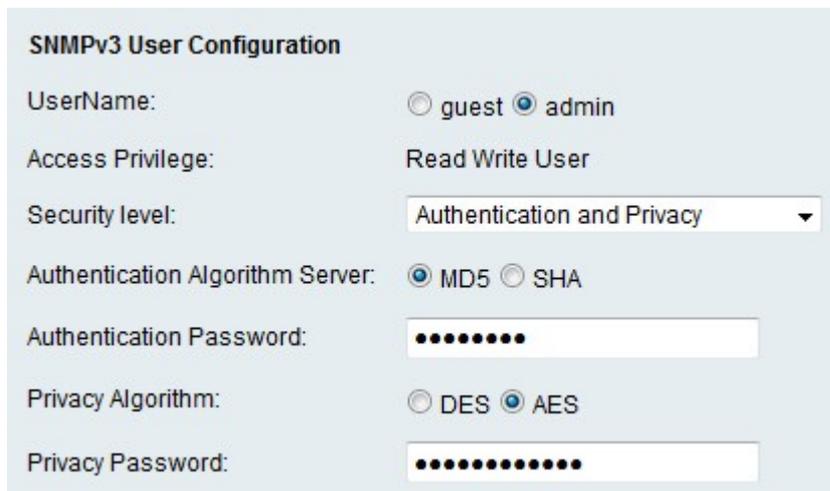
ステップ2:[SysContact]フィールドにシステム担当者の名前を入力します。システム担当者の連絡先情報を含めることは一般的です。

ステップ3:[SysLocation]フィールドにRV215Wの物理的な場所を入力します。

ステップ4:[SysName]フィールドにRV215Wの識別用の名前を入力します。

ステップ5:[Save]をクリックします。

SNMPv3ユーザ設定



ステップ1:[UserName]フィールドで、設定するアカウントに対応するオプションボタンをクリックします。ユーザのアクセス権限が[Access Privilege]フィールドに表示されます。

- ・ Guest – ゲストユーザには読み取り権限しかありません。
- ・ Admin – 管理者ユーザーには読み取り/書き込み権限があります。

ステップ2:[Security level]ドロップダウンリストから、目的のセキュリティを選択します。認証は、SNMP機能の表示や管理をユーザに許可するために使用されます。プライバシーは、SNMP機能のセキュリティを強化するために使用できるもう1つのキーです。

- ・ No Authentication and No Privacy : ユーザは認証またはプライバシーパスワードを要求しません。
- ・ 認証とプライバシーなし : ユーザが必要とする認証のみ。
- ・ 認証とプライバシー : 認証とプライバシーパスワードの両方がユーザに必要です。

ステップ3 : セキュリティレベルに認証が含まれている場合は、[Authentication Algorithm Server]フィールドで、目的のサーバに対応するオプションボタンをクリックします。このアルゴリズムはハッシュ関数です。ハッシュ関数は、キーを指定ビットメッセージに変換するために使用されます。

- ・ MD5:Message-Digest 5(MD5)は、入力を取得し、入力の128ビットのメッセージダイジェストを生成するアルゴリズムです。
- ・ SHA : セキュアハッシュアルゴリズム(SHA)は、入力を受け取り、入力の160ビットのメッセージダイジェストを生成するアルゴリズムです。

ステップ4:[Authentication Password]フィールドにユーザのパスワードを入力します。

ステップ5：セキュリティレベルにプライバシーが含まれている場合は、[Privacy Algorithm]フィールドで、目的のアルゴリズムに対応するオプションボタンをクリックします。

- ・ DES:Data Encryption Standard (DES ; データ暗号規格) は、メッセージの暗号化と復号化に同じ方法を使用する暗号化アルゴリズムです。DESアルゴリズムはAESより高速に処理する。
- ・ AES : 高度暗号化規格(AES)は、メッセージの暗号化と復号化に異なる方法を使用する暗号化アルゴリズムです。これにより、AESはDESよりも安全な暗号化アルゴリズムになります。

ステップ6:[Privacy Password]フィールドにユーザのプライバシーパスワードを入力します。

ステップ7:[Save]をクリックします。

トラップの設定

トラップは、システムイベントのレポートに使用されるSNMPメッセージを生成します。トラップは、管理対象デバイスにシステムイベントをネットワークマネージャに通知するSNMPメッセージをネットワークマネージャに強制的に送信させます。



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	

ステップ1：トラップ通知の送信先IPアドレスを[IP address]フィールドに入力します。

ステップ2：トラップ通知の送信先IPアドレスのポート番号を[Port]フィールドに入力します。

ステップ3：トラップマネージャが属するコミュニティ文字列を[Community]フィールドに入力します。コミュニティストリングは、パスワードとして機能するテキスト文字列です。エージェントとネットワークマネージャの間で送信されるメッセージを認証するために、SNMPによって使用されます。

注：このフィールドは、SNMPトラップバージョンがバージョン3でない場合にのみ適用されます。

ステップ4:[SNMP Version]ドロップダウンリストから、SNMPトラップメッセージのSNMPマネージャバージョンを選択します。

- ・ v1 : コミュニティストリングを使用してトラップメッセージを認証します。
- ・ v2c : コミュニティストリングを使用してトラップメッセージを認証します。
- ・ v3 : 暗号化されたパスワードを使用してトラップメッセージを認証します。

ステップ5:[Save]をクリックします。