

SPA100シリーズの簡易ネットワーク管理プロトコル(SNMP)設定の設定

目的

Simple Network Management Protocol (SNMP ; 簡易ネットワーク管理プロトコル) は、ネットワーク上のデバイスを監視および制御し、設定を維持するために使用されるツールです。統計情報の収集、パフォーマンス、セキュリティにより、ネットワークの問題を迅速に解決できます。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。デバイスで、ユーザはトラップの設定値を調整できます。トラップは、ネットワークでエラーが発生したときに特定のIPアドレスに送信されるエラーメッセージです。

このドキュメントの目的は、SPA100シリーズアナログ電話アダプタ(ATA)でSNMP設定を行う方法を示すことです。

該当するデバイス

- ・ SPA100シリーズアナログ電話アダプタ

[Software Version]

- ・ v1.1.0

SNMP の設定 (SNMP Configuration)

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

SNMP

SNMP Setting

SNMP: Enabled Disabled

Trusted IP: Any

Address: . . .

Netmask: . . .

Get / Trap Community:

Set Community:

SNMPV3: Enabled Disabled

R/W User:

Auth- Protocol: ▾

Auth- Password :

PrivProtocol: ▾

Privacy Password:

Trap Configuration

IP Address: . . . (Hint:192.168.15.100)

Port: (Range: 162 or 1025-65535,Default:162)

SNMP Version: ▾

Submit

Cancel

ステップ2:[SNMP]フィールドの右側にある[Enabled]ラジオボタンをクリックしてSNMPを有効にするか、[Disabled]オプションボタンをクリックしてデバイスのSNMPを無効にします。

SNMP Setting

SNMP: Enabled Disabled

Trusted IP: Any

Address: 192 . 168 . 10 . 1

Netmask: 255 . 255 . 255 . 0

Get / Trap Community: public

Set Community: private

ステップ3:[Trusted IP]フィールドで、[Any]をクリックしてSNMPを介した任意のIPアドレスからのATAへのアクセスを許可します。または、[Address]をクリックして、IPアドレスの範囲をATAにアクセスできます。

ステップ4:[Get Community]フィールドに、SNMPコミュニティのGETコマンドのパスワードとして機能するフレーズを入力します。

ステップ5:[Set Community]フィールドに、SNMPコミュニティのSETコマンドのパスワードとして機能するフレーズを入力します。

SNMPV3: Enabled Disabled

R/W User: v3rwuser

Auth- Protocol: HMAC-SHA

Auth- Password :

PrivProtocol: CBC-DES

Privacy Password:

ステップ6:SNMPV3は、SNMPのより安全な実装です。より高度な認証および暗号化メカニズムを使用して、許可されたデバイスだけがSNMPを介してネットワークデバイスに読み書きできるようにすることができます。SNMPv3を使用するには[有効]オプションボタンをクリックし、無効にするには[無効]ラジオボタンをクリックします。

ステップ7:[R/W User]フィールドに、SNMPv3認証のユーザ名を入力します。

ステップ8:[Auth-Protocol]ドロップダウンリストから、SNMPv3の認証プロトコルを選択します。使用可能なオプションは次のように定義されます。

- ・ 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。

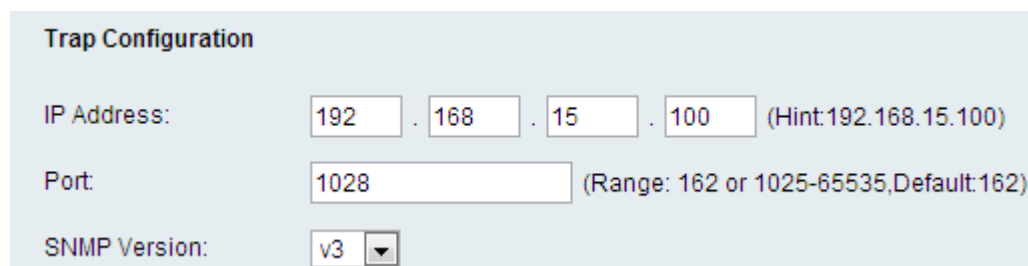
注 : HMAC-SHAはHMAC-MD5よりもセキュアであると見なされ、推奨されます。

ステップ9:[Auth-Password]フィールドに、認証用のパスワードを入力します。

ステップ10:[PrivProtocol] ドロップダウンリストからプライバシー認証プロトコルを選択します。データを保護するには、ユーザがプライバシー機能を持っている必要があります。使用可能なオプションは次のように定義されます。

- ・ なし：プライバシーアルゴリズムは使用されません。メッセージのデータは暗号化されずに送信されます。
- ・ CBC-DES：このオプションは、DES暗号化を使用してメッセージのデータを暗号化します。

ステップ11:[Privacy Password] フィールドに、プライバシー認証プロトコルのパスワードを入力します。



The image shows a 'Trap Configuration' form with the following fields:

- IP Address:** A field with four sub-inputs containing '192', '168', '15', and '100', followed by '(Hint:192.168.15.100)'. There are dots between the sub-inputs.
- Port:** A text input field containing '1028', followed by '(Range: 162 or 1025-65535,Default:162)'. There is a dot between the input and the hint.
- SNMP Version:** A dropdown menu with 'v3' selected.

ステップ12:[IP Address]フィールドに、トラップメッセージを受信するIPアドレスを入力します。

ステップ13:[ポート(Port)]フィールドに、トラップメッセージを受信するポート番号を入力します。デフォルトポートは162です。

ステップ14:[SNMP Version]ドロップダウンリストから、トラップメッセージの検索に使用するSNMPのバージョンを選択します。使用可能なオプションは次のとおりです。

- ・ v1:SNMPv1トラップを使用します。SNMPv1トラップは、トラップメッセージの認証にコミュニティストリングを使用し、データを暗号化しません。
- ・ v2:SNMPv2トラップを使用します。SNMPv2トラップは、トラップメッセージの認証にコミュニティストリングを使用し、データを暗号化しません。
- ・ v3:SNMPv3トラップを使用します。SNMPv3トラップは、ユーザ名とパスワードを使用してトラップの送信元を認証するように設定でき、トラップのデータを暗号化できます。このオプションを使用するには、ステップ6の説明に従ってSNMPv3を有効にして設定する必要があります。

ステップ15:[送信]をクリックして**変更を適用**するか、[キャンセル]をクリックして**変更を破棄**する場合があります。