

Konfigurieren der SNMP-Einstellungen (Simple Network Management Protocol) auf der SPA100-Serie

Ziel

Simple Network Management Protocol (SNMP) ist ein Tool zur Überwachung und Regulierung von Geräten in einem Netzwerk sowie zum Verwalten von Konfigurationen. Mithilfe der Statistikerfassung, der Leistung und der Sicherheit können Sie Netzwerkprobleme schnell beheben. 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. Sie müssen ein SNMP v3-Manager-Programm installieren, um SNMP-Benachrichtigungen anzuzeigen. Auf dem Gerät kann ein Benutzer die Einstellungen für die Trap-Konfiguration anpassen. Traps sind Fehlermeldungen, die an eine bestimmte IP-Adresse gesendet werden, wenn im Netzwerk ein Fehler auftritt.

In diesem Dokument wird erläutert, wie Sie die SNMP-Einstellungen für den analogen Telefonadapter (ATA) der Serie SPA100 konfigurieren.

Anwendbare Geräte

- Analoger Telefonadapter der Serie SPA100

Softwareversion

- v1.1.0

SNMP-Konfiguration

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

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

Schritt 2: Klicken Sie rechts neben dem Feld *SNMP* auf das **Optionsfeld Aktiviert**, um SNMP zu aktivieren, oder klicken Sie auf das **Optionsfeld Deaktiviert**, um SNMP auf dem Gerät zu deaktivieren.

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

Schritt 3: Klicken Sie im Feld *Trusted IP (Vertrauenswürdige IP)* auf **Any (Beliebig)**, um den Zugriff auf den ATA von einer beliebigen IP-Adresse über SNMP zu ermöglichen, oder klicken Sie auf **Address (Adresse)**, um einem Bereich von IP-Adressen den Zugriff auf den ATA über SNMP zu ermöglichen.

Schritt 4: Geben Sie im Feld *Get Community (Community abrufen)* eine Phrase ein, die als Kennwort für GET-Befehle in der SNMP-Community dient.

Schritt 5: Geben Sie im Feld *Set Community (Community festlegen)* eine Phrase ein, die als Kennwort für SET-Befehle in der SNMP-Community dient.

SNMPV3: Enabled Disabled

R/W User: v3rwuser

Auth- Protocol: HMAC-SHA

Auth- Password :

PrivProtocol: CBC-DES

Privacy Password:

Schritt 6: SNMPV3 ist eine sicherere Implementierung von SNMP. Es ermöglicht die Verwendung erweiterter Authentifizierungs- und Verschlüsselungsmechanismen, um sicherzustellen, dass nur autorisierte Geräte über SNMP lesen und auf Ihre Netzwerkgeräte schreiben können. Klicken Sie auf das Optionsfeld **Aktiviert**, um SNMPv3 zu verwenden, oder klicken Sie auf das Optionsfeld **Deaktiviert**, um die Funktion zu deaktivieren.

Schritt 7: Geben Sie im Feld *R/W User (R/W-Benutzer)* einen Benutzernamen für die SNMPv3-Authentifizierung ein.

Schritt 8: Wählen Sie aus der Dropdown-Liste *Auth-Protocol* ein Authentifizierungsprotokoll für SNMPv3 aus. Die verfügbaren Optionen sind wie folgt definiert:

- 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.

Hinweis: HMAC-SHA gilt als sicherer als HMAC-MD5 und wird empfohlen.

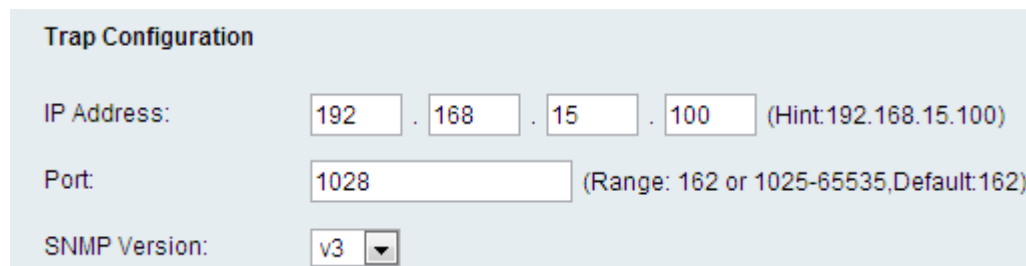
Schritt 9: Geben Sie im Feld *Auth-Passwort* ein Kennwort für die Authentifizierung ein.

Schritt 10: Wählen Sie aus der Dropdown-Liste *PrivProtocol* ein Protokoll zur Authentifizierung der Privatsphäre aus. Es wird empfohlen, dass der Benutzer über eine Datenschutzfunktion verfügt, um Daten zu schützen. Die verfügbaren Optionen sind wie folgt definiert:

·Keine - Es wird kein Datenschutzalgorithmus verwendet. Die Daten einer Nachricht werden unverschlüsselt gesendet.

·CBC-DES: Diese Option verschlüsselt die Daten einer Nachricht mit DES-Verschlüsselung.

Schritt 11: Geben Sie im Feld *Privacy Password* (Datenschutzkennwort) ein Kennwort für das Datenschutzauthentifizierungsprotokoll ein.



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

- IP Address:** A dotted decimal IP address field with values 192, 168, 15, and 100. A hint '(Hint:192.168.15.100)' is shown to the right.
- Port:** A text input field containing the value 1028. A range '(Range: 162 or 1025-65535,Default:162)' is shown to the right.
- SNMP Version:** A dropdown menu with 'v3' selected.

Schritt 12: Geben Sie im Feld *IP-Adresse* eine IP-Adresse ein, die Trap-Nachrichten empfängt.

Schritt 13: Geben Sie im Feld *Port* (Port) die Portnummer ein, die Trap-Meldungen empfangen soll. Der Standard-Port ist 162.

Schritt 14: Wählen Sie aus der Dropdown-Liste *SNMP Version* (SNMP-Version) eine SNMP-Version aus, mit der Trap-Meldungen gesucht werden sollen. Folgende Optionen sind verfügbar:

·v1 - Verwendet SNMPv1-Traps. SNMPv1-Traps verwenden einen Community-String, um Trap-Nachrichten zu authentifizieren, und verschlüsseln keine Daten.

·v2 - Verwendet SNMPv2-Traps. SNMPv2-Traps verwenden einen Community-String, um Trap-Nachrichten zu authentifizieren, und verschlüsseln keine Daten.

·v3 - Verwendet SNMPv3-Traps. SNMPv3-Traps können so eingestellt werden, dass sie einen Benutzernamen und ein Kennwort zur Authentifizierung der Quelle eines Traps verwenden und die Daten eines Traps verschlüsseln. SNMPv3 muss aktiviert und wie in Schritt 6 beschrieben konfiguriert werden, um diese Option verwenden zu können.

Schritt 15: Klicken Sie auf **Senden**, um Änderungen anzuwenden, oder auf **Abbrechen**, um sie zu verwerfen.