

Configurazione delle impostazioni SNMP (Simple Network Management Protocol) sulla serie SPA100

Obiettivo

L'SNMP (Simple Network Management Protocol) è uno strumento utilizzato per monitorare e regolare i dispositivi in una rete e per mantenere le configurazioni. La raccolta, le prestazioni e la protezione delle statistiche consentono di risolvere rapidamente i problemi di rete. Una rete gestita SNMP è costituita da dispositivi gestiti, agenti e un gestore di rete. I dispositivi gestiti sono dispositivi che supportano la funzione SNMP. Un agente è un software SNMP su un dispositivo gestito. Un gestore di rete è un'entità che riceve i dati dagli agenti SNMP. È necessario installare un programma di gestione SNMP v3 per visualizzare le notifiche SNMP. Sul dispositivo, l'utente può regolare le impostazioni di configurazione della trap. I trap sono messaggi di errore inviati a un indirizzo IP specifico quando si verifica un errore nella rete.

L'obiettivo di questo documento è mostrare come configurare le impostazioni SNMP sull'adattatore per telefono analogico (ATA) serie SPA100.

Dispositivi interessati

·Serie SPA100 Analog Telephone Adapter

Versione del software

·v1.1.0

Configurazione SNMP

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Amministrazione > Gestione > SNMP**. Viene visualizzata la pagina *SNMP*:

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

Passaggio 2. A destra del campo *SNMP*, fare clic sul pulsante di opzione **Enabled** (Abilitato) per abilitare il protocollo SNMP oppure sul pulsante di opzione **Disabled** (Disabilitato) per disabilitare il protocollo SNMP sul dispositivo.

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

Passaggio 3. Nel campo *Trusted IP*, fare clic su **Any** (Qualsiasi) per consentire l'accesso ai dati da qualsiasi indirizzo IP tramite SNMP, oppure fare clic su **Address** (Indirizzo) per consentire a un intervallo di indirizzi IP di accedere ai dati tramite SNMP.

Passaggio 4. Nel campo *Get Community*, immettere una frase che agisca come password per i comandi GET nella community SNMP.

Passaggio 5. Nel campo *Set Community*, immettere una frase che agisca come password per i comandi SET nella community SNMP.

SNMPV3: Enabled Disabled

R/W User: v3rwuser

Auth- Protocol: HMAC-SHA

Auth- Password :

PrivProtocol: CBC-DES

Privacy Password:

Passaggio 6. SNMPV3 è un'implementazione di SNMP più sicura. Consente l'utilizzo di meccanismi di autenticazione e crittografia più avanzati per garantire che solo i dispositivi autorizzati siano in grado di leggere e scrivere sui dispositivi di rete tramite SNMP. Fare clic sul pulsante di scelta **Abilitato** per utilizzare SNMPv3 o fare clic sul pulsante di scelta **Disabilitato** per disabilitarlo.

Passaggio 7. Nel campo *Utente R/W*, immettere un nome utente per l'autenticazione SNMPv3.

Passaggio 8. Dall'elenco a discesa *Auth-Protocol*, scegliere un protocollo di autenticazione per SNMPv3. Le opzioni disponibili sono definite come segue:

- MD5 — Message-Digest 5 (MD5) è un algoritmo che accetta un input e produce un digest del messaggio a 128 bit dell'input.

- SHA — Secure Hash Algorithm (SHA) è un algoritmo che accetta un input e produce un digest del messaggio a 160 bit dell'input.

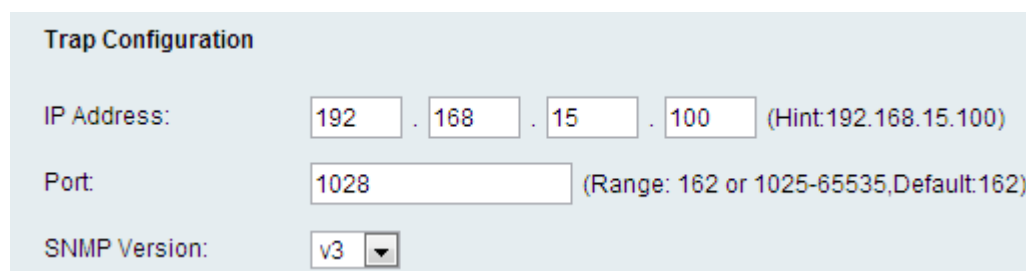
Nota: HMAC-SHA è considerato più sicuro di HMAC-MD5 ed è consigliato.

Passaggio 9. Nel campo *Auth-Password*, immettere una password per l'autenticazione.

Passaggio 10. Dall'elenco a discesa *PrivProtocol*, scegliere un protocollo di autenticazione della privacy. È consigliabile che l'utente disponga di una caratteristica di privacy per la protezione dei dati. Le opzioni disponibili sono definite come segue:

- Nessuno: non viene utilizzato alcun algoritmo di privacy. I dati di un messaggio verranno inviati senza crittografia.
- CBC-DES: questa opzione consente di crittografare i dati di un messaggio utilizzando la crittografia DES.

Passaggio 11. Nel campo *Password privacy*, immettere una password per il protocollo di autenticazione della privacy.



The image shows a 'Trap Configuration' form with three main fields:

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

Passaggio 12. Nel campo *IP Address* (Indirizzo IP), immettere un indirizzo IP che riceverà i messaggi trap.

Passaggio 13. Nel campo *Port* (Porta), immettere il numero della porta che riceverà i messaggi trap. La porta predefinita è 162.

Passaggio 14. Dall'elenco a discesa *SNMP Version*, scegliere la versione di SNMP da utilizzare per trovare i messaggi trap. Le opzioni disponibili sono le seguenti:

- v1: utilizza trap SNMPv1. I trap SNMPv1 utilizzano una stringa della community per autenticare i messaggi trap e non crittografano i dati.
- v2: utilizza trap SNMPv2. I trap SNMPv2 utilizzano una stringa della community per autenticare i messaggi trap e non crittografano i dati.
- v3: utilizza trap SNMPv3. Le trap SNMPv3 possono essere impostate in modo da utilizzare un nome utente e una password per autenticare l'origine di una trap e possono crittografare i dati di una trap. Per utilizzare questa opzione, SNMPv3 deve essere abilitato e configurato come descritto nel passaggio 6.

Passaggio 15. Fare clic su **Sottometti** per applicare le modifiche oppure su **Annulla** per annullarle.