

# Configurare il protocollo SNMPv3 sui router WAP125 e WAP581

## Obiettivo

Il protocollo SNMPv3 (Simple Network Management Protocol versione 3) è un modello di protezione in cui viene impostata una strategia di autenticazione per un utente e il gruppo in cui risiede l'utente. Il livello di protezione è il livello di protezione consentito in un modello di protezione. La combinazione di un modello di sicurezza e di un livello di sicurezza determina il meccanismo di sicurezza da utilizzare quando si gestisce un pacchetto SNMP.

In SNMP, il MIB (Management Information Base) è un database di informazioni gerarchico contenente OID (Object Identifier) che funge da variabile leggibile o impostabile tramite SNMP. Il MIB è organizzato in una struttura ad albero. Una sottostruttura all'interno della struttura di denominazione degli oggetti gestiti è una sottostruttura della vista. Una vista MIB è una combinazione di sottostrutture di una vista o di una famiglia di sottostrutture di vista. Le viste MIB vengono create per controllare l'intervallo OID a cui gli utenti SNMPv3 possono accedere. La configurazione delle viste SNMPv3 è essenziale per fare in modo che un utente visualizzi solo il MIB limitato. Un punto di accesso remoto può avere fino a 16 visualizzazioni, incluse le due visualizzazioni predefinite.

L'obiettivo di questo documento è mostrare come raccogliere, visualizzare e scaricare l'attività della CPU/RAM sui modelli WAP125 e WAP581.

## Dispositivi interessati

- WAP125
- WAP581

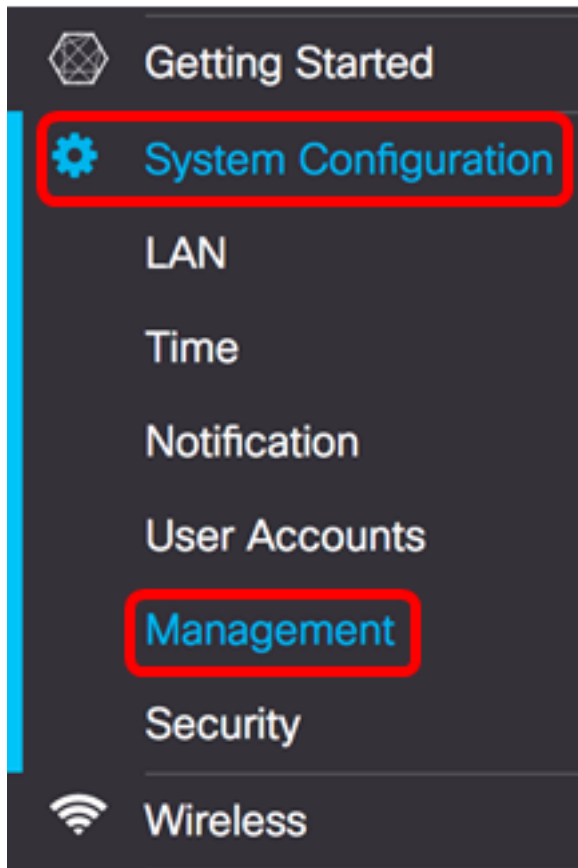
## Versione del software

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

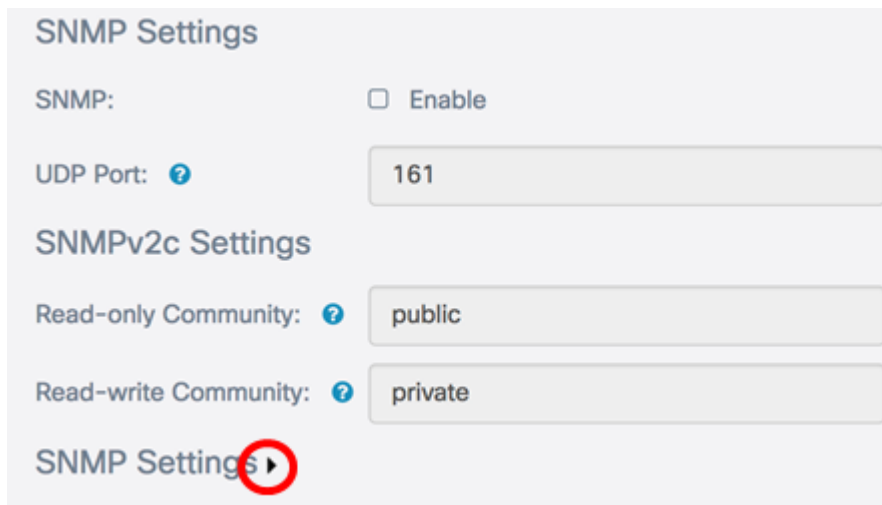
## Configurazione delle impostazioni SNMPv3

### Configurazione delle viste SNMPv3

Passaggio 1. Accedere all'utility basata sul Web e scegliere **Configurazione di sistema > Gestione**.



Passaggio 2. Fare clic sulla freccia destra **Impostazioni SNMP**.



Passaggio 3. Fare clic sulla scheda **SNMPv3**.

SNMPv2c **SNMPv3**

### SNMPv3 Views

+ ✎ 🗑

<input type="checkbox"/>	View Name	Type	OID	Mask
<input type="checkbox"/>	view-all	included	.1	
<input type="checkbox"/>	view-none	excluded	.1	

---

### SNMPv3 Groups

+ ✎ 🗑

<input type="checkbox"/>	Group Name	Security Level	Write Views	Read Views
<input type="checkbox"/>	RO	authPriv	view-none	view-all
<input type="checkbox"/>	RW	authPriv	view-all	view-all

Passaggio 4. Fare clic sul pulsante + per creare una nuova voce in Viste SNMPv3.

SNMPv3 Views

**+** ✎ 🗑

<input type="checkbox"/>	View Name	Type	OID	Mask
<input type="checkbox"/>	view-all	included	.1	
<input type="checkbox"/>	view-none	excluded	.1	
<input checked="" type="checkbox"/>	view-new	included		

Passaggio 5. Nel campo *Nome vista*, inserire un nome che identifichi la vista MIB.

**Nota:** In questo esempio, il nome della vista è view-new. View-all e view-none vengono creati per default e contengono tutti gli oggetti di gestione supportati dal sistema. Non è possibile modificarli né eliminarli.

## SNMPv3 Views

<input type="checkbox"/>	View Name	Type	OID	Mask
<input type="checkbox"/>	view-all	included	.1	
<input type="checkbox"/>	view-none	excluded	.1	
<input checked="" type="checkbox"/>	view-new	included		

Passo 6: dall'elenco a discesa Tipo, scegliere un'opzione se escludere o includere la vista.

- inclusa - include la vista nella sottostruttura o nella famiglia di sottostrutture dalla vista MIB.
- escluso - esclude la vista nella sottostruttura o nella famiglia di sottostrutture dalla vista MIB.

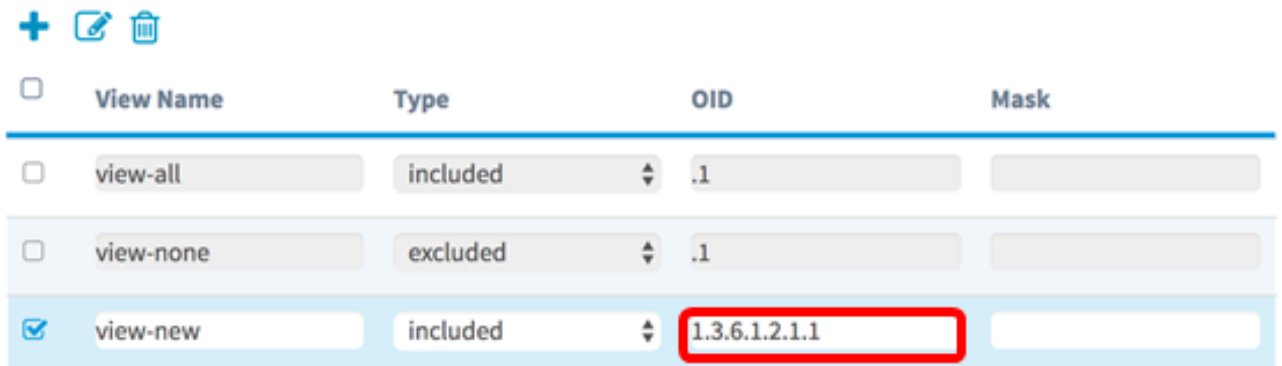
## SNMPv3 Views

<input type="checkbox"/>	View Name	Type	OID	Mask
<input type="checkbox"/>	view-all	included	.1	
<input type="checkbox"/>	view-none	excluded	.1	
<input checked="" type="checkbox"/>	view-new	<input checked="" type="checkbox"/> included <input type="checkbox"/> excluded		

Passaggio 7. Nel campo *OID*, immettere una stringa OID per la sottostruttura da includere o escludere dalla vista. Ogni numero viene utilizzato per individuare le informazioni e ogni numero corrisponde a una sezione specifica della struttura OID. Gli OID sono identificatori univoci degli oggetti gestiti nella gerarchia MIB. Gli ID oggetto MIB di livello superiore appartengono a organizzazioni di standard diversi, mentre gli ID oggetto di livello inferiore vengono allocati dalle organizzazioni associate. Le filiali private possono essere definite dai fornitori per includere oggetti gestiti per i propri prodotti. I file MIB eseguono il mapping dei numeri OID in un formato leggibile. Per convertire il numero OID nel nome dell'oggetto, fare clic [qui](#).

**Nota:** nell'esempio si usa il punto 1.3.6.1.2.1.1.

## SNMPv3 Views

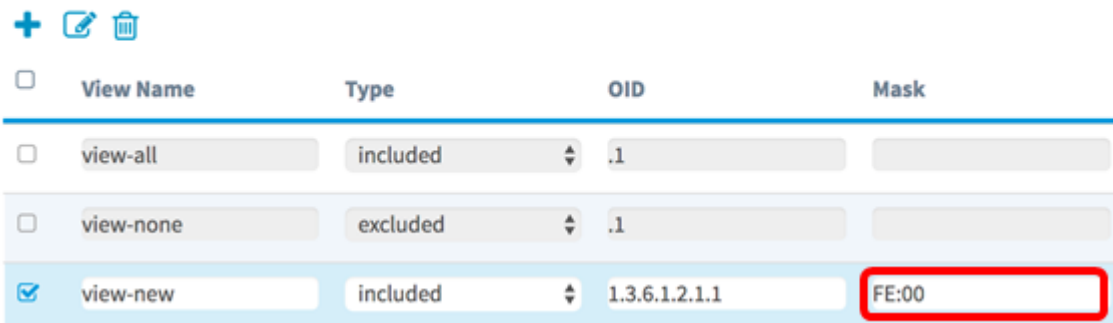


<input type="checkbox"/>	View Name	Type	OID	Mask
<input type="checkbox"/>	view-all	included	.1	
<input type="checkbox"/>	view-none	excluded	.1	
<input checked="" type="checkbox"/>	view-new	included	1.3.6.1.2.1.1	

Passaggio 8. Inserire una maschera OID nel campo *Maschera*. Il campo *Maschera* viene utilizzato per controllare gli elementi della sottostruttura OID che devono essere considerati rilevanti quando si determina la vista in cui si trova un OID e la lunghezza massima è 47 caratteri. Il formato è lungo 16 ottetti e ogni ottetto contiene due caratteri esadecimali separati da un punto o due punti. Per determinare la maschera, contate il numero di elementi OID e impostate il numero di bit su uno. In questo campo sono accettati solo i formati esadecimali. Si consideri l'esempio di OID 1.3.6.1.2.1.1, che ha sette elementi, quindi se si impostano sette 1s consecutivi seguiti da uno 0 nel primo ottetto e tutti gli zeri nel secondo ottetto, si ottiene FE:00 come maschera.

**Nota:** Nell'esempio viene utilizzato FE:00.

## SNMPv3 Views



<input type="checkbox"/>	View Name	Type	OID	Mask
<input type="checkbox"/>	view-all	included	.1	
<input type="checkbox"/>	view-none	excluded	.1	
<input checked="" type="checkbox"/>	view-new	included	1.3.6.1.2.1.1	FE:00

Passaggio 9. Fare clic su [Save](#).

A questo punto, è necessario aver configurato correttamente le visualizzazioni SNMPv3 su WAP125.

## Configurazione dei gruppi SNMPv3

Passaggio 1. Fare clic sul pulsante + per creare una nuova voce in Gruppi SNMPv3.

<input type="checkbox"/>	Group Name	Security Level	Write Views	Read Views
<input type="checkbox"/>	RO	authPriv	view-none	view-all
<input type="checkbox"/>	RW	authPriv	view-all	view-all

Passaggio 2. Inserire un nome utilizzato per identificare il gruppo nel campo *Nome gruppo*. Non è possibile riutilizzare i nomi predefiniti RO e RW. I nomi dei gruppi possono contenere fino a 32 caratteri alfanumerici.

**Nota:** Nell'esempio viene utilizzato CC.

<input type="checkbox"/>	Group Name	Security Level	Write Views	Read Views
<input type="checkbox"/>	RO	authPriv	view-none	view-all
<input type="checkbox"/>	RW	authPriv	view-all	view-all
<input checked="" type="checkbox"/>	CC	noAuthNoPriv	view-none	view-none

Passaggio 3. Dall'elenco a discesa Livello di protezione, scegliere un livello di autenticazione appropriato.

- noAuthNoPriv: non fornisce alcuna autenticazione e nessuna crittografia dei dati (nessuna protezione).
- authNoPriv: fornisce l'autenticazione ma non la crittografia dei dati (nessuna protezione). L'autenticazione viene fornita da una passphrase SHA (Secure Hash Authentication).
- authPriv: autenticazione e crittografia dei dati. L'autenticazione viene fornita da una passphrase SHA. La crittografia dei dati viene fornita dalla passphrase DES.

**Nota:** Nell'esempio viene utilizzato authPriv.

SNMPv3 Groups

<input type="checkbox"/>	Group Name	Security Level	Write Views	Read Views
<input type="checkbox"/>	RO	authPriv	view-none	view-all
<input type="checkbox"/>	RW	noAuthNoPriv authNoPriv	view-all	view-all
<input checked="" type="checkbox"/>	CC	✓ authPriv	view-new	view-none

Passaggio 4. Dall'elenco a discesa Vista scrittura, scegliere l'accesso in scrittura a tutti gli oggetti di gestione (MIB) per il nuovo gruppo. Definisce l'azione che un gruppo può eseguire sui MIB. L'elenco includerà inoltre tutte le nuove visualizzazioni SNMP create sul WAP.

**Nota:** Nell'esempio viene utilizzato view-new.

SNMPv3 Groups

Group Name	Security Level	Write Views	Read Views
RO	authPriv	view-none	view-all
RW	authPriv	view-all	view-all
<input checked="" type="checkbox"/> CC	authPriv	view-new	view-none

Passaggio 5. Scegliere l'accesso in lettura per tutti gli oggetti di gestione (MIB) per il nuovo gruppo dall'elenco a discesa Viste di lettura. Le opzioni di default riportate di seguito vengono visualizzate insieme a tutte le altre viste create sul piano WAP.

- view-all: consente ai gruppi di visualizzare e leggere tutti i MIB.
- view-none: limita il gruppo in modo che nessuno possa visualizzare o leggere i MIB.
- view-new - Vista creata dall'utente.

**Nota:** Nell'esempio viene utilizzato view-none.

SNMPv3 Groups

Group Name	Security Level	Write Views	Read Views
RO	authPriv	view-none	view-all
RW	authPriv	view-all	view-all
<input checked="" type="checkbox"/> CC	authPriv	view-new	view-none

Passaggio 6. Fare clic su .

A questo punto, è necessario configurare correttamente i gruppi SNMPv3.

## Configurazione degli utenti SNMPv3

Un utente SNMP è definito dalle relative credenziali di accesso (nome utente, password e metodo di autenticazione) e viene gestito in associazione a un gruppo SNMP e a un ID motore. Solo SNMPv3 utilizza utenti SNMP. Gli utenti con privilegi di accesso vengono associati a una visualizzazione SNMP.

Passaggio 1. Fare clic sul pulsante + per creare una nuova voce in Utenti SNMPv3.

## SNMPv3 Users



<input type="checkbox"/>	User Name	Group	Authenticati... Type	Authenticati... Pass Phrase	Encryption Type	Encryption Pass Phrase
<input checked="" type="checkbox"/>	<input type="text"/>	CC	SHA	****	DES	<input type="text"/>

Passaggio 2. Nel campo *User Name* (Nome utente), creare un nome utente che identifichi un utente SNMP.

**Nota:** Nell'esempio viene utilizzato AdminConan.

## SNMPv3 Users



<input type="checkbox"/>	User Name	Group	Authentication Type	Authentication Pass Phrase	Encryption Type	Encryption Pass Phrase
<input checked="" type="checkbox"/>	AdminConan	CC	SHA	<input type="text"/>	DES	<input type="text"/>

Passaggio 3. Dall'elenco a discesa Gruppo, scegliere un gruppo da mappare all'utente. Le opzioni sono:

- RO — gruppo di sola lettura, creato per impostazione predefinita. Questo gruppo consente a un utente solo di visualizzare la configurazione.
- RW — gruppo di lettura/scrittura, creato per impostazione predefinita. Questo gruppo consente a un utente di visualizzare e apportare le modifiche necessarie alla configurazione.
- CC: CC, un gruppo definito dall'utente. Il gruppo definito dall'utente viene visualizzato solo se è stato definito un gruppo.

**Nota:** In questo esempio, si sceglie CC come definito nel Passaggio 2 in Configurazione dei gruppi SNMPv3.

## SNMPv3 Users



<input type="checkbox"/>	User Name	Group	Authentication Type	Authentication Pass Phrase	Encryption Type	Encryption Pass Phrase
<input checked="" type="checkbox"/>	AdminConan	RO RW ✓ CC	SHA	<input type="text"/>	DES	<input type="text"/>

Passaggio 4. Dall'elenco a discesa Autenticazione, scegliere **Agente integrità sistema**.

**Nota:** Quest'area è disattivata se il livello di protezione del gruppo scelto nel passaggio 3 è stato impostato su noAuthNoPriv.



SNMPv3 Users

User Name	Group	Authentication Type	Authentication Pass Phrase	Encryption Type	Encryption Pass Phrase
<input checked="" type="checkbox"/> AdminConan	CC	SHA		DES	

Passaggio 5. Nel campo *Frase di accesso autenticazione*, immettere la passphrase associata per l'utente. Questa è la password SNMP che deve essere configurata per autenticare i dispositivi e consentire loro di connettersi tra loro.

SNMPv3 Users

User Name	Group	Authentication Type	Authentication Pass Phrase	Encryption Type	Encryption Pass Phrase
<input checked="" type="checkbox"/> AdminConan	CC	SHA	*****	DES	

Passaggio 6. Dal menu a discesa Tipo di crittografia, scegliere un metodo di crittografia per crittografare le richieste SNMPv3. Le opzioni sono:

- DES: Data Encryption Standard (DES) è una cifratura a blocchi simmetrica che utilizza una chiave segreta condivisa a 64 bit.
- AES128 — Advanced Encryption Standard che utilizza una chiave a 128 bit.

**Nota:** Nell'esempio riportato di seguito viene scelto DES.

SNMPv3 Users

User Name	Group	Authentication Type	Authentication Pass Phrase	Encryption Type	Encryption Pass Phrase
<input checked="" type="checkbox"/> AdminConan	CC	SHA	*****	DES	*****

Passaggio 7. Nel campo *Frase password crittografia*, immettere la passphrase associata per l'utente. Questa opzione viene utilizzata per crittografare i dati inviati ad altri dispositivi nella rete. Questa password viene utilizzata anche per decrittografare i dati sull'altra estremità. La passphrase deve corrispondere nei dispositivi in comunicazione. La passphrase può avere una lunghezza compresa tra 8 e 32 caratteri.

SNMPv3 Users

User Name	Group	Authentication Type	Authentication Pass Phrase	Encryption Type	Encryption Pass Phrase
<input checked="" type="checkbox"/> AdminConan	CC	SHA	*****	DES	*****

Passaggio 8. Fare clic su .

A questo punto, è necessario aver configurato correttamente gli utenti SNMPv3 su WAP125.

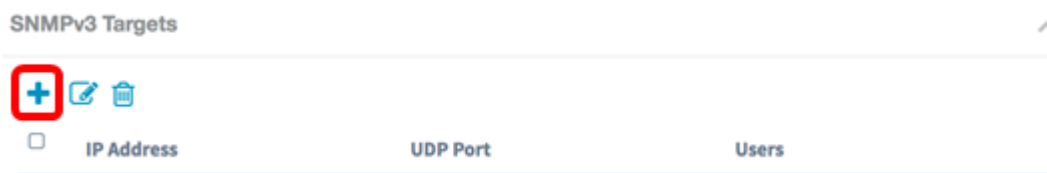
## Configurazione delle destinazioni SNMPv3

Una destinazione SNMP fa riferimento sia al messaggio inviato che al dispositivo di gestione a cui vengono inviate le notifiche dell'agente. Ogni destinazione è identificata da nome, indirizzo IP, porta UDP e nome utente.

SNMPv3 invia le notifiche di destinazione SNMP come messaggi Inform a SNMP Manager invece che come trap. In questo modo viene garantito il recapito del target poiché le trap non utilizzano la conferma ma le informazioni la utilizzano.

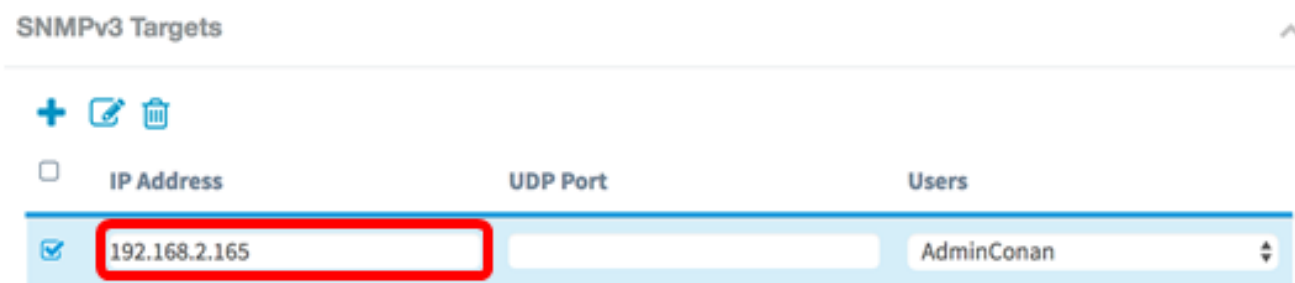
Passaggio 1. Fare clic sul pulsante **+** per creare una nuova voce in Destinazioni SNMPv3.

**Nota:** È possibile configurare fino a 16 destinazioni.



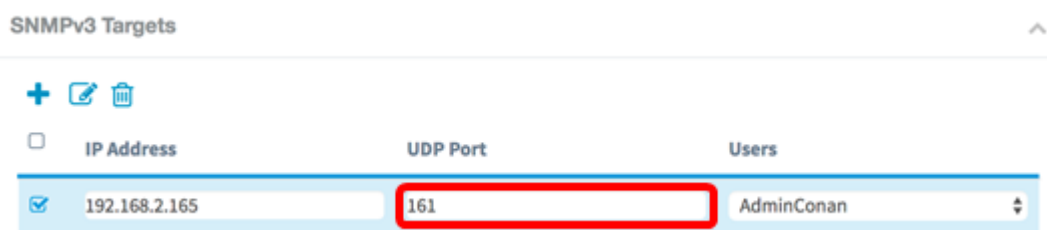
Passaggio 2. Nel campo *IP Address* (Indirizzo IP), immettere l'indirizzo IP di destinazione a cui verranno inviate tutte le trap SNMP. Si tratta in genere dell'indirizzo del sistema di gestione di rete. Può essere un indirizzo IPv4 o IPv6.

**Nota:** nell'esempio viene usato 192.168.2.165.



Passaggio 3. Immettere un numero di porta UDP (User Datagram Protocol) nel campo *Porta UDP*. L'agente SNMP controlla questa porta per individuare eventuali richieste di accesso. Il valore predefinito è 161. L'intervallo valido è compreso tra 1025 e 65535.

**Nota:** Nell'esempio viene utilizzato 161.



Passaggio 4. Scegliere l'utente da associare alla destinazione dall'elenco a discesa Utenti. In questo elenco sono elencati tutti gli utenti creati nella pagina Utenti.

**Nota:** AdminConan viene scelto come User.

SNMPv3 Targets ^

+ ✎ 🗑

<input type="checkbox"/>	IP Address	UDP Port	Users
<input checked="" type="checkbox"/>	192.168.2.165	161	<input checked="" type="checkbox"/> AdminConan

Passaggio 5. Fare clic su Save.

A questo punto, le destinazioni SNMPv3 sui modelli WAP125 e WAP581 devono essere configurate correttamente.