

Konfigurieren des SNMPv3 auf dem WAP125 und WAP581

Ziel

Simple Network Management Protocol Version 3 (SNMPv3) ist ein Sicherheitsmodell, in dem eine Authentifizierungsstrategie für einen Benutzer und die Gruppe, in der sich der Benutzer befindet, eingerichtet wird. Die Sicherheitsstufe ist der zulässige Sicherheitsgrad innerhalb eines Sicherheitsmodells. Eine Kombination aus Sicherheitsmodell und Sicherheitsstufe bestimmt, welcher Sicherheitsmechanismus bei der Verarbeitung eines SNMP-Pakets verwendet wird.

In SNMP ist die Management Information Base (MIB) eine hierarchische Informationsdatenbank mit OID (Object Identifiers), die als Variable fungiert, die über SNMP gelesen oder festgelegt werden kann. MIB ist in einer baumähnlichen Struktur organisiert. Eine Unterstruktur in der Struktur für die Benennung verwalteter Objekte ist eine Ansichtunterstruktur. Eine MIB-Ansicht ist eine Kombination aus einer Reihe von View-Unterbäumen oder einer Familie von View-Unterbäumen. MIB-Ansichten werden erstellt, um den OID-Bereich zu steuern, auf den SNMPv3-Benutzer zugreifen können. Die Konfiguration von SNMPv3-Ansichten ist erforderlich, um die Anzeige von Benutzern auf die limitierte MIB zu beschränken. Ein WAP kann bis zu 16 Ansichten einschließlich der beiden Standardansichten enthalten.

In diesem Dokument wird erläutert, wie Sie die CPU/RAM-Aktivität auf dem WAP125 und dem WAP581 erfassen, anzeigen und herunterladen.

Anwendbare Geräte

- WAP125
- WAP581

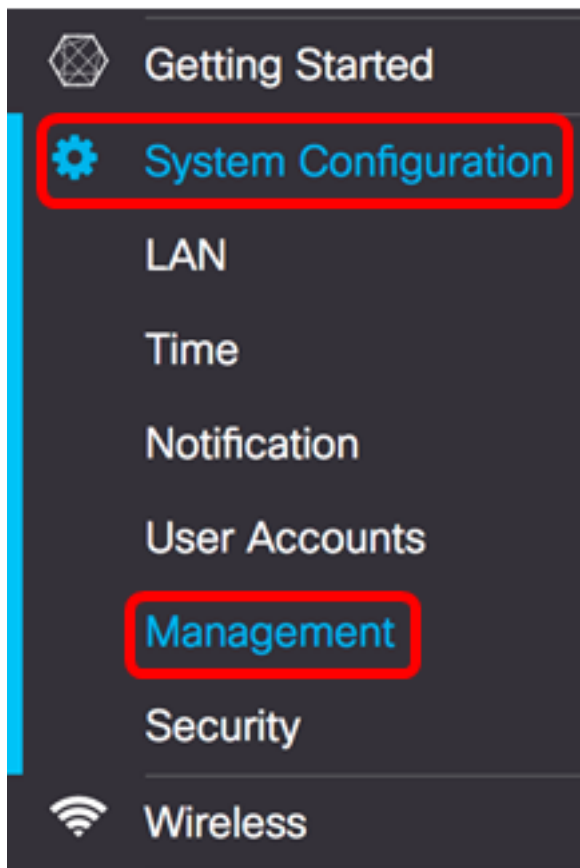
Softwareversion

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

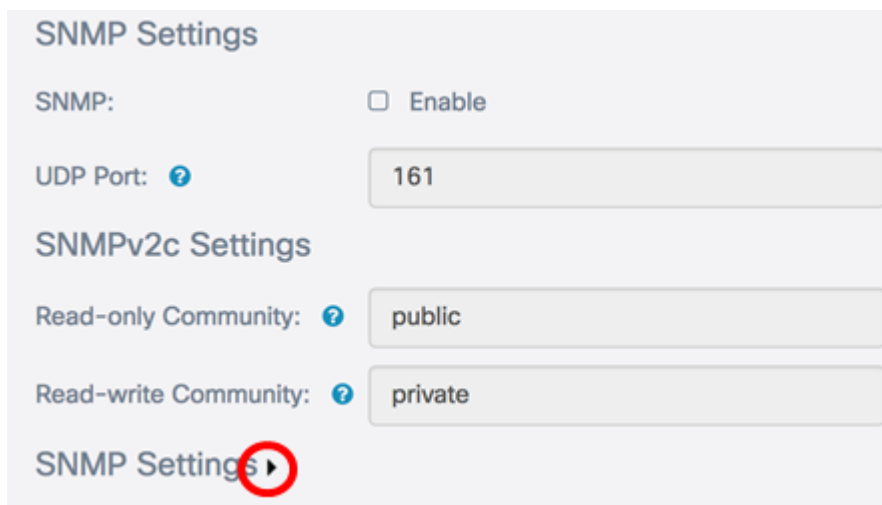
Konfigurieren der SNMPv3-Einstellungen

Konfigurieren von SNMPv3-Ansichten

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **Systemkonfiguration > Verwaltung** aus.



Schritt 2: Klicken Sie auf den Pfeil nach rechts **SNMP Settings**.



Schritt 3: Klicken Sie auf die Registerkarte **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

Schritt 4: Klicken Sie auf die +-Schaltfläche, um unter SNMPv3 Views einen neuen Eintrag zu erstellen.

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		

Schritt 5: Geben Sie im Feld *View Name (Anzeigename)* einen Namen ein, der die MIB-Ansicht identifiziert.

Hinweis: In diesem Beispiel wird view-new als View Name erstellt. View-all und view-none werden standardmäßig erstellt und enthält alle vom System unterstützten Verwaltungsobjekte. Diese können weder geändert noch gelöscht werden.

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		

Schritt 6: Wählen Sie in der Dropdown-Liste Type (Typ) eine Option aus, bei der die Ansicht ausgeschlossen oder eingeschlossen werden soll.

- Include - Beinhaltet die Ansicht in der Unterstruktur oder der Unterbaumfamilie aus der MIB-Ansicht.
- excluded - Schließt die Ansicht in der Unterstruktur oder der Familie von Unterstrukturen aus der MIB-Ansicht aus.

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		

Schritt 7: Geben Sie im Feld *OID* eine OID-Zeichenfolge für die Unterstruktur ein, die die Ansicht einschließen oder davon ausschließen soll. Jede Nummer wird zum Auffinden von Informationen verwendet, und jede Nummer entspricht einem bestimmten Zweig der OID-Struktur. OIDs sind eindeutige Bezeichner verwalteter Objekte in der MIB-Hierarchie. Die Objekt-IDs der obersten MIB-Ebene gehören zu verschiedenen Standardisierungsorganisationen, während Objekt-IDs der unteren Ebene von zugeordneten Organisationen zugewiesen werden. Private Zweigstellen können von Anbietern definiert werden, um verwaltete Objekte für ihre eigenen Produkte einzuschließen. MIB-Dateien ordnen OID-Nummern einem für Menschen lesbaren Format zu. Um die OID-Nummer in den Objektnamen zu übersetzen, klicken Sie [hier](#).

Hinweis: In diesem Beispiel wird 1.3.6.1.2.1.1 verwendet.

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	

Schritt 8: Geben Sie eine OID-Maske in das Feld *Maske* ein. Das *Maskenfeld* wird verwendet, um die Elemente der OID-Unterstruktur zu steuern, die bei der Bestimmung der Ansicht, in der eine OID angezeigt wird, als relevant betrachtet werden sollten. Die maximale Länge beträgt 47 Zeichen. Das Format ist 16 Oktette lang, und jedes Oktett enthält zwei Hexadezimalzeichen, die durch einen Punkt oder Doppelpunkt getrennt sind. Um die Maske zu bestimmen, zählen Sie die Anzahl der OID-Elemente, und legen Sie für viele Bits eine Zahl fest. In diesem Feld werden nur Hexadezimalformate akzeptiert. Betrachten wir das Beispiel OID 1.3.6.1.2.1.1, das sieben Elemente enthält. Wenn Sie also sieben aufeinander folgende 1s gefolgt von einer 0 im ersten Oktett und allen Nullen im zweiten setzen, erhalten Sie FE:00 als Maske.

Hinweis: In diesem Beispiel wird FE:00 verwendet.

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

Schritt 9: Klicken Sie .

Sie sollten jetzt die SNMPv3-Ansichten auf dem WAP125 erfolgreich konfiguriert haben.

Konfigurieren von SNMPv3-Gruppen

Schritt 1: Klicken Sie auf die +-Schaltfläche, um unter SNMPv3 Groups einen neuen Eintrag zu erstellen.

<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

Schritt 2: Geben Sie im Feld *Gruppenname* einen Namen für die Gruppe ein. Die Standardnamen RO und RW können nicht wiederverwendet werden. Gruppennamen können bis zu 32 alphanumerische Zeichen enthalten.

Hinweis: In diesem Beispiel wird CC verwendet.

<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

Schritt 3: Wählen Sie aus der Dropdown-Liste Security Level (Sicherheitsstufe) eine geeignete Authentifizierungsstufe aus.

- noAuthNoPriv: Bietet keine Authentifizierung und keine Datenverschlüsselung (keine Sicherheit).
- authNoPriv: Stellt Authentifizierung, aber keine Datenverschlüsselung (keine Sicherheit) bereit. Die Authentifizierung wird durch eine Secure Hash Authentication (SHA)-Passphrase bereitgestellt.
- authPriv - Authentifizierung und Datenverschlüsselung. Die Authentifizierung erfolgt über eine SHA-Passphrase. Die Datenverschlüsselung erfolgt über DES-Passphrase.

Hinweis: In diesem Beispiel wird authPriv verwendet.

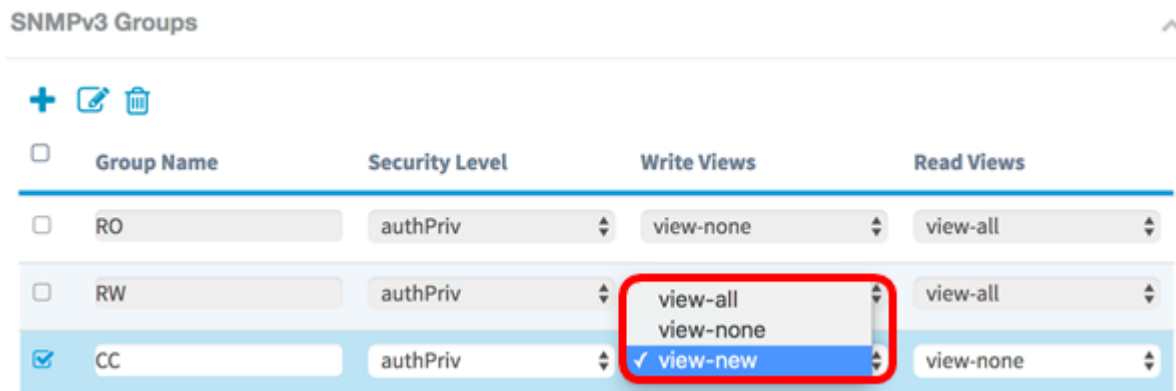
SNMPv3 Groups

<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

Schritt 4: Wählen Sie in der Dropdown-Liste Write Views (Ansichten schreiben) den Schreibzugriff auf alle Management-Objekte (MIBs) für die neue Gruppe aus. Dadurch wird

die Aktion definiert, die eine Gruppe für MIBs ausführen darf. Diese Liste enthält auch alle neuen SNMP-Ansichten, die auf dem WAP erstellt wurden.

Hinweis: In diesem Beispiel wird view-new verwendet.



Schritt 5: Wählen Sie in der Dropdown-Liste Leseansichten den Lesezugriff für alle Management-Objekte (MIBs) für die neue Gruppe aus. Die unten angegebenen Standardoptionen werden zusammen mit allen anderen auf dem WAP erstellten Ansichten angezeigt.

- view-all - Diese Funktion ermöglicht es Gruppen, alle MIBs anzuzeigen und zu lesen.
- view-none: Diese Funktion schränkt die Gruppe so ein, dass keine MIBs angezeigt oder gelesen werden können.
- view-new - Vom Benutzer erstellte Ansicht.

Hinweis: In diesem Beispiel wird view-none verwendet.



Schritt 6: Klicken Sie .

Sie sollten jetzt die SNMPv3-Gruppen erfolgreich konfiguriert haben.

Konfigurieren von SNMPv3-Benutzern

Ein SNMP-Benutzer wird durch seine Anmeldeinformationen (Benutzername, Kennwörter und Authentifizierungsmethode) definiert und in Verbindung mit einer SNMP-Gruppen- und Engine-ID betrieben. SNMPv3 verwendet nur SNMP-Benutzer. Benutzer mit Zugriffsberechtigungen sind einer SNMP-Ansicht zugeordnet.

Schritt 1: Klicken Sie auf die +-Schaltfläche, um unter SNMPv3-Benutzer einen neuen Eintrag zu erstellen.

SNMPv3 Users

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

Schritt 2: Erstellen Sie im Feld *User Name* (*Benutzername*) einen Benutzernamen, der einen SNMP-Benutzer angibt.

Hinweis: In diesem Beispiel wird AdminConan verwendet.

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		DES	

Schritt 3: Wählen Sie in der Dropdown-Liste Gruppe eine Gruppe aus, die dem Benutzer zugeordnet werden soll. Folgende Optionen stehen zur Verfügung:

- RO - Nur Lesezugriff, standardmäßig erstellt. Diese Gruppe ermöglicht es Benutzern, nur die Konfiguration anzuzeigen.
- RW - Lese-/Schreibgruppe, standardmäßig erstellt. Diese Gruppe ermöglicht es Benutzern, die Konfiguration anzuzeigen und notwendige Änderungen vorzunehmen.
- CC - CC, eine benutzerdefinierte Gruppe. Eine benutzerdefinierte Gruppe wird nur angezeigt, wenn eine Gruppe definiert wurde.

Hinweis: In diesem Beispiel wird CC wie in Schritt 2 unter Konfigurieren von SNMPv3-Gruppen definiert ausgewählt.

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		DES	

Schritt 4: Wählen Sie in der Dropdown-Liste Authentifizierung die Option **SHA**.

Hinweis: Dieser Bereich ist ausgegraut, wenn die in Schritt 3 gewählte Sicherheitsstufe der Gruppe auf noAuthNoPriv festgelegt wurde.

SNMPv3 Users

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

Schritt 5: Geben Sie im Feld *Authentifizierungs-Kennzeichenfolge* die zugeordnete Passphrase für den Benutzer ein. Dies ist das SNMP-Kennwort, das für die Authentifizierung der Geräte konfiguriert werden muss, damit diese miteinander verbunden werden können.

SNMPv3 Users

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

Schritt 6: Wählen Sie im Dropdown-Menü Verschlüsselungstyp eine Verschlüsselungsmethode aus, um die SNMPv3-Anforderungen zu verschlüsseln. Folgende Optionen stehen zur Verfügung:

- DES - Data Encryption Standard (DES) ist eine Verschlüsselung symmetrischer Blöcke, die einen 64-Bit-gemeinsamen geheimen Schlüssel verwendet.
- AES128 - Advanced Encryption Standard, der einen 128-Bit-Schlüssel verwendet.

Hinweis: In diesem Beispiel wird DES gewählt.

SNMPv3 Users

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

Schritt 7: Geben Sie im Feld *Encryption Pass-Phrase* die zugeordnete Passphrase für den Benutzer ein. Diese werden zur Verschlüsselung der Daten verwendet, die an die anderen Geräte im Netzwerk gesendet werden. Dieses Kennwort wird auch verwendet, um die Daten am anderen Ende zu entschlüsseln. Die Passphrase muss auf den kommunizierenden Geräten übereinstimmen. Die Passphrase kann zwischen acht und 32 Zeichen lang sein.

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	*****	DES	*****

Schritt 8: Klicken Sie .

Sie sollten jetzt die SNMPv3-Benutzer auf dem WAP125 erfolgreich konfiguriert haben.

Konfigurieren von SNMPv3-Zielen

Ein SNMP-Ziel bezieht sich sowohl auf die gesendete Nachricht als auch auf das Verwaltungsgerät, an das Agentenbenachrichtigungen gesendet werden. Jedes Ziel wird anhand des Zielnamens, der IP-Adresse, des UDP-Ports und des Benutzernamens identifiziert.

SNMPv3 sendet SNMP-Zielbenachrichtigungen nicht als Traps, sondern als Informative Nachrichten an den SNMP Manager. Dies stellt die Zielzustellung sicher, da Traps nicht Bestätigungen verwenden, sondern Informationen dies tun.

Schritt 1: Klicken Sie auf die +-Schaltfläche, um unter SNMPv3 Targets einen neuen Eintrag zu erstellen.

Hinweis: Es können insgesamt bis zu 16 Ziele konfiguriert werden.

SNMPv3 Targets

+ ✎ 🗑

<input type="checkbox"/>	IP Address	UDP Port	Users
--------------------------	------------	----------	-------

Schritt 2: Geben Sie im Feld *IP-Adresse* die Ziel-IP-Adresse ein, an die alle SNMP-Traps gesendet werden sollen. Dies ist in der Regel die Adresse des Netzwerkmanagementsystems. Dabei kann es sich um eine IPv4- oder eine IPv6-Adresse handeln.

Hinweis: In diesem Beispiel wird 192.168.2.165 verwendet.

SNMPv3 Targets

+ ✎ 🗑

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

Schritt 3: Geben Sie eine UDP-Portnummer (User Datagram Protocol) im Feld *UDP Port* ein. Der SNMP-Agent überprüft diesen Port auf Zugriffsanfragen. Der Standardwert ist 161. Der gültige Bereich liegt zwischen 1025 und 65535.

Hinweis: In diesem Beispiel wird 161 verwendet.

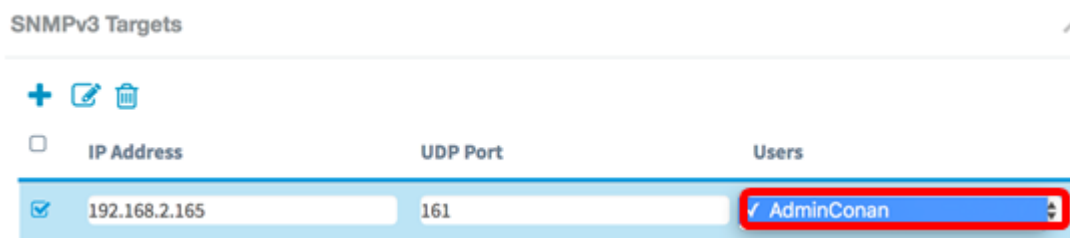


The screenshot shows the 'SNMPv3 Targets' configuration interface. At the top, there are icons for adding, editing, and deleting targets. Below is a table with columns for 'IP Address', 'UDP Port', and 'Users'. A single target is listed with IP address '192.168.2.165', UDP Port '161', and User 'AdminConan'. The '161' in the 'UDP Port' column is highlighted with a red rectangular box.

IP Address	UDP Port	Users
192.168.2.165	161	AdminConan

Schritt 4: Wählen Sie in der Dropdown-Liste Benutzer den Benutzer aus, der dem Ziel zugeordnet werden soll. Diese Liste enthält eine Liste aller Benutzer, die auf der Seite Benutzer erstellt wurden.

Hinweis: AdminConan wird als Benutzer ausgewählt.



The screenshot shows the 'SNMPv3 Targets' configuration interface. The 'Users' dropdown menu is open, and 'AdminConan' is selected and highlighted with a red rectangular box. The table below shows the target configuration with 'AdminConan' in the 'Users' column.

IP Address	UDP Port	Users
192.168.2.165	161	AdminConan

Schritt 5: Klicken Sie .

Sie sollten jetzt die SNMPv3-Ziele auf dem WAP125 und dem WAP581 erfolgreich konfiguriert haben.