

在WAP125和WAP581上配置SNMPv3

目標

簡單網路管理協定第3版(SNMPv3)是一種安全模型，其中為使用者及使用者所在的組設定身份驗證策略。安全級別是安全模型中允許的安全級別。安全模型和安全級別的組合確定了在處理SNMP資料包時使用的安全機制。

在SNMP中，管理資訊庫(MIB)是一個包含對象識別符號(OID)的分層資訊資料庫，OID作為一個變數，可以通過SNMP讀取或設定。MIB以樹狀結構組織。託管對象命名樹內的子樹是檢視子樹。MIB檢視是一組檢視子樹或檢視子樹族的組合。建立MIB檢視以控制SNMPv3使用者可以訪問的OID範圍。SNMPv3檢視配置對於限制使用者只能檢視有限的MIB至關重要。一個WAP最多可以有16個檢視，包括兩個預設檢視。

本文檔旨在向您展示如何收集、檢視和下載WAP125和WAP581上的CPU/RAM活動。

適用裝置

- WAP125
- WAP581

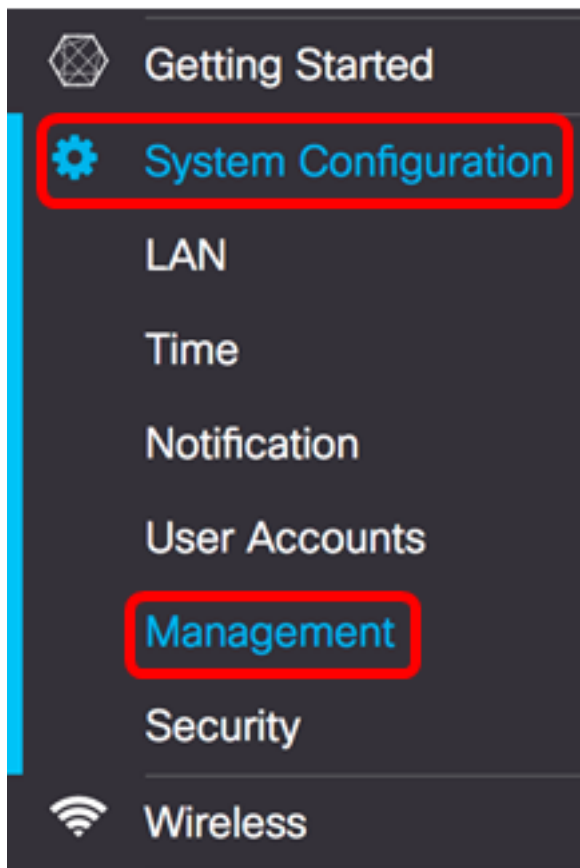
軟體版本

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

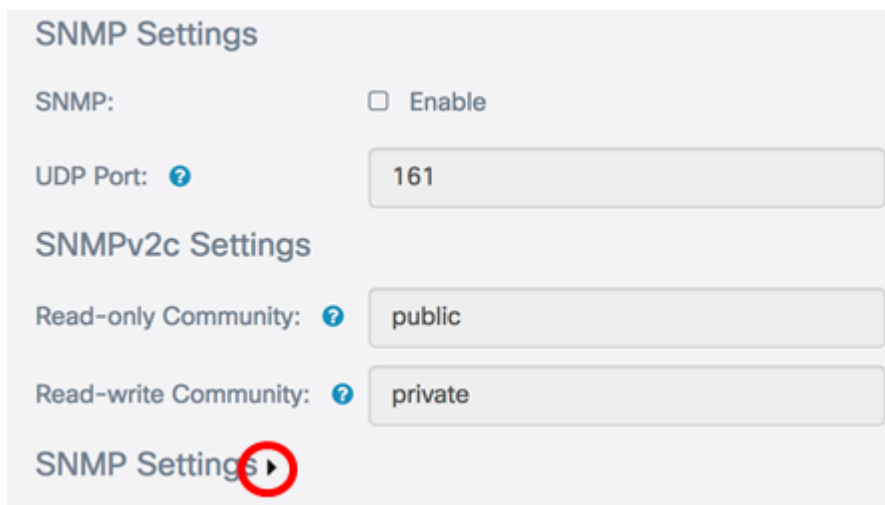
配置SNMPv3設定

配置SNMPv3檢視

步驟1. 登入到基於Web的實用程式，然後選擇**System Configuration > Management**。



步驟2.按一下SNMP設定右箭頭。



步驟3.按一下SNMPv3選項卡。

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

步驟4.按一下**+按鈕**，在SNMPv3檢視下建立一個新條目。

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		

步驟5.在 *View Name* 欄位中輸入標識MIB檢視的名稱。

附註：在此示例中，將view-new建立為View Name。預設情況下會建立「全部檢視」和「無檢視」，其中包含系統支援的所有管理對象。不能修改或刪除它們。

SNMPv3 Views

View Name	Type	OID	Mask
view-all	included	.1	
view-none	excluded	.1	
view-new	included		

步驟6.從「型別」下拉選單中，選擇是排除還是包括檢視的選項。

- included — 在MIB檢視的子樹或子樹族中包含檢視。
- excluded — 從MIB檢視中排除子樹或子樹族中的檢視。

SNMPv3 Views

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

步驟7.在OID欄位中，輸入子樹的OID字串，以便將其包含在檢視中或從檢視中排除。每個數字用於查詢資訊，每個數字對應於OID樹的特定分支。OID是MIB層次結構中託管對象的唯一識別符號。頂級MIB對象ID屬於不同的標準組織，而低級對象ID由相關組織分配。供應商可以定義專用分支，以包括他們自己的產品的託管對象。MIB檔案將OID號對映到使用者可讀的格式。要將OID編號轉換為對象名稱，請按一下[此處](#)。

附註：本示例中使用的是1.3.6.1.2.1.1。

SNMPv3 Views

View Name	Type	OID	Mask
view-all	included	.1	
view-none	excluded	.1	
view-new	included	1.3.6.1.2.1.1	

步驟8.在Mask欄位中輸入OID掩碼。Mask欄位用於控制確定OID所在的檢視時應被視為相關的OID子樹元素，最大長度為47個字元。格式為16個八位位元組，每個八位位元組包含兩個用句號或冒號分隔的十六進位制字元。要確定掩碼，請對OID元素的數量進行計數，並將該多個位設定為1。此欄位只接受十六進位制格式。以示例OID 1.3.6.1.2.1.1為例，它包含七個元素，因此，如果在第一個八位元中設定了七個連續的1後跟一個0，在第二個八位元中設定了全

部為零，則會獲得FE:00作為掩碼。

附註：本示例使用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

步驟9.單 **Save** 擊。

現在，您應該已經在WAP125上成功配置了SNMPv3檢視。

配置SNMPv3組

步驟1.按一下**+按鈕**，在SNMPv3 Groups下建立一個新條目。

<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

步驟2.在「組名稱」欄位中輸入用於標識組的名稱。不能重複使用RO和RW的預設名稱。組名稱最多可包含32個字母數字字元。

附註：在此示例中，使用CC。

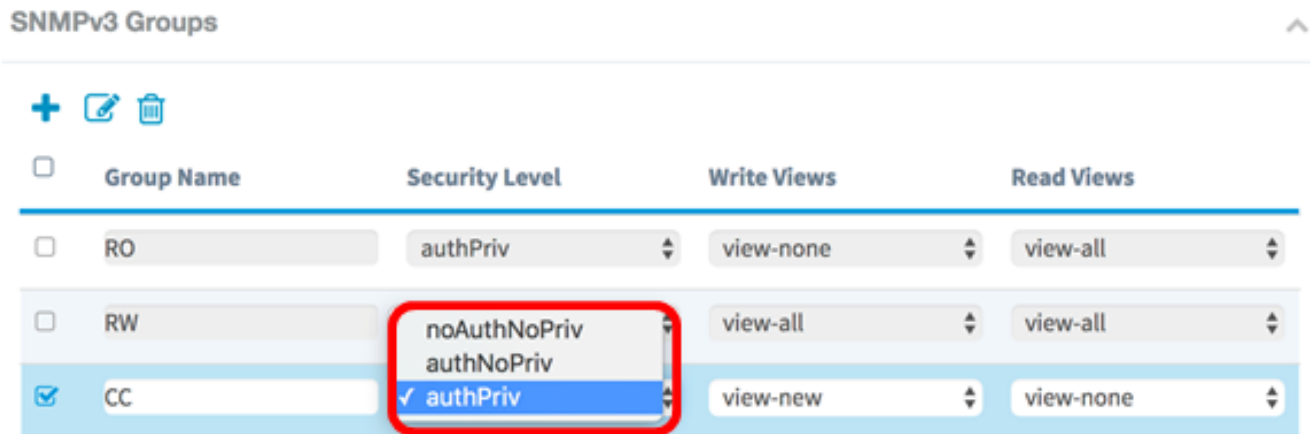
<input type="checkbox"/>	Group Name	Security Level	Write Views	Read Views
<input type="checkbox"/>	RO	authPriv	view-none	view-all
<input type="checkbox"/>	RW	authPriv	view-all	view-all
<input checked="" type="checkbox"/>	CC	noAuthNoPriv	view-none	view-none

步驟3.從「安全級別」下拉選單中，選擇適當的身份驗證級別。

- noAuthNoPriv — 不提供身份驗證和不資料加密（無安全性）。
- authNoPriv — 提供驗證但不提供資料加密（無安全性）。驗證由安全雜湊驗證(SHA)密碼提供。

- authPriv — 驗證和資料加密。身份驗證由SHA密碼提供。資料加密由DES密碼提供。

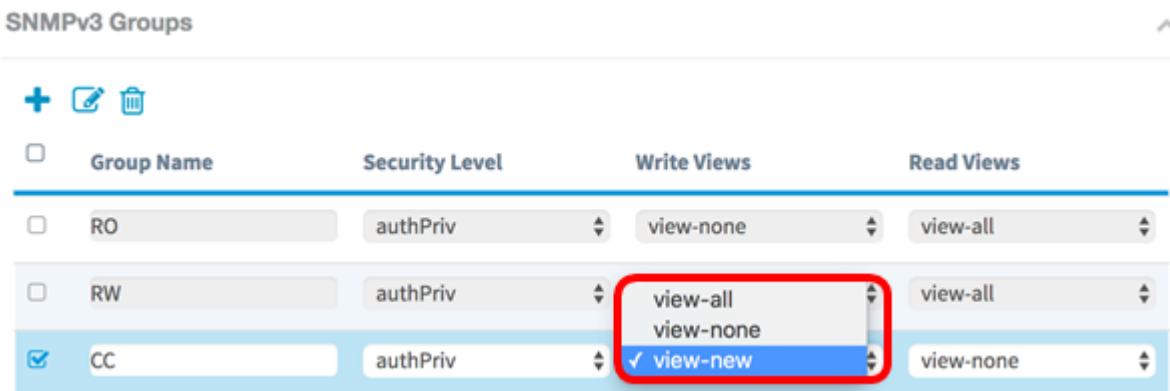
附註：在此範例中，使用authPriv。



Group Name	Security Level	Write Views	Read Views
RO	authPriv	view-none	view-all
RW	noAuthNoPriv authNoPriv	view-all	view-all
CC	authPriv	view-new	view-none

步驟4.從「寫入檢視」下拉選單中，為新組選擇對所有管理對象(MIB)的寫入訪問許可權。定義組可在MIB上執行的操作。此清單還將包括在WAP上建立的所有新SNMP檢視。

附註：在此示例中，使用view-new。



Group Name	Security Level	Write Views	Read Views
RO	authPriv	view-none	view-all
RW	authPriv	view-all view-none	view-all
CC	authPriv	view-new	view-none

步驟5.從「讀取檢視」下拉選單中選擇新組的所有管理對象(MIB)的讀取訪問許可權。下面給出的預設選項與在WAP上建立的任何其它檢視一起顯示。

- view-all — 這允許組檢視和讀取所有MIB。
- view-none — 這樣會限制組，以便任何人都無法檢視或讀取任何MIB。
- view-new — 使用者建立的檢視。

附註：在此示例中，使用view-none。



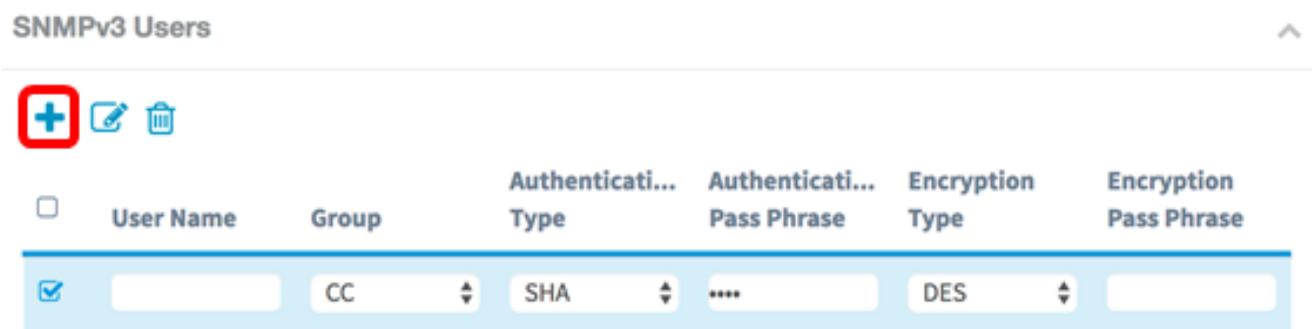
步驟6.單 **Save** 擊。

您現在應該已經成功配置了SNMPv3組。

配置SNMPv3使用者

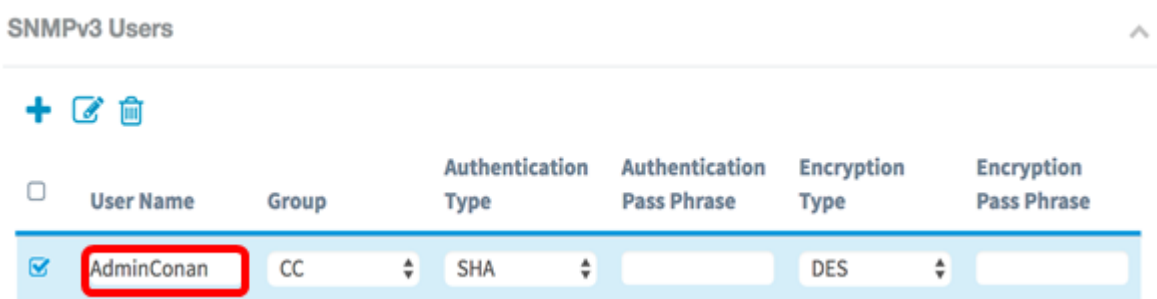
SNMP使用者由其登入憑證（使用者名稱、密碼和身份驗證方法）定義，並且與SNMP組和引擎ID關聯操作。只有SNMPv3使用SNMP使用者。具有訪問許可權的使用者與SNMP檢視相關聯。

步驟1.按一下+按鈕，在SNMPv3使用者下建立一個新條目。



步驟2.在 *User Name* 欄位中，建立一個表示SNMP使用者的使用者名稱。

附註：在本示例中，使用AdminConan。



步驟3.從Group下拉選單中，選擇要對映到使用者的組。選項包括：

- RO — 只讀組，預設建立。此組允許使用者僅檢視配置。
- RW — 讀/寫組，預設建立。此組允許使用者檢視配置並對配置進行必要的更改。
- CC - CC，使用者定義的組。僅當已定義組時才會顯示使用者定義的組。

附註：在此示例中，按照配置SNMPv3組下的步驟2中的定義選擇CC。

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

步驟4.從Authentication下拉選單中選擇SHA。

附註：如果在步驟3中選擇的組安全級別設定為noAuthNoPriv，此區域將呈灰色顯示。

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

步驟5.在Authentication Pass Phrase欄位中，輸入使用者的相關密碼短語。這是SNMP密碼，必須配置為對裝置進行身份驗證，才能使裝置相互連線。

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

步驟6.從Encryption Type下拉選單中，選擇加密SNMPv3請求的加密方法。選項包括：

- DES — 資料加密標準(DES)是使用64位共用金鑰的對稱分組密碼。
- AES128 — 使用128位金鑰的高級加密標準。

附註：在本示例中，選擇了DES。

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

步驟7.在加密口令欄位中，輸入使用者的關聯口令。這用於加密傳送到網路中其他裝置的資料。此密碼也用於解密另一端的資料。在通訊裝置中，密碼必須匹配。密碼長度範圍為8到32個字元。

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	*****

步驟8.單 **Save** 擊。

現在，您應該已經在WAP125上成功配置了SNMPv3使用者。

配置SNMPv3目標

SNMP目標是指傳送的消息和代理通知傳送到的管理裝置。每個目標由目標名稱、IP地址、UDP埠和使用者名稱標識。

SNMPv3將SNMP目標通知作為通知消息傳送到SNMP管理器，而不是陷阱。這可確保目標傳送，因為陷阱不使用確認，而是通知使用。

步驟1.按一下**+按鈕**，在SNMPv3 Targets下建立一個新條目。

附註：最多可以配置16個目標。

SNMPv3 Targets

+ ✎ 🗑

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

步驟2.在IP Address欄位中輸入將傳送所有SNMP陷阱的目標IP地址。這通常是網路管理系統地址。可以是IPv4或IPv6地址。

附註：本示例使用192.168.2.165。

SNMPv3 Targets

+ ✎ 🗑

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

步驟3.在UDP Port欄位中輸入使用者資料包協定(UDP)埠號。SNMP代理檢查此埠是否有訪問請求。預設值為161。有效範圍為1025到65535。

附註：在本示例中，使用161。

SNMPv3 Targets

+ ✎ 🗑

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

步驟4.從「使用者」下拉選單中選擇要與目標關聯的使用者。此清單顯示在「使用者」頁上建立的所有使用者的清單。

附註： AdminConan被選為使用者。

SNMPv3 Targets

+ ✎ 🗑

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

步驟5.單 **Save** 擊。

現在，您應該已經在WAP125和WAP581上成功配置了SNMPv3目標。