SAMM

دليل التنصيب

تنصيب SAMM خطوةً بخطوة على Windows أو Ubuntu أو MikroTik (RouterOS) أو على سيرفر جاهز

ثم ربط الترخيص والدفع والتجديد وربط الراوترات وتفعيل الميزات

الإصدار الثاني · تشرين الثاني 2026

samm.securytik.com

المحتويات

1. اختيار طريقة التنصيب المناسبة
2. قبل البدء: عناوين IP (لا يجوز تكرار العنوان نفسه)
3. التنصيب على Windows (حاسوب محمول أو مكتبي)
4. تفعيل خاصية Virtualization (Intel VT-x / AMD-V) من إعدادات BIOS
5. التنصيب على Ubuntu Server (سيرفر خاص أو VPS)
6. التنصيب على راوتر MikroTik (Container)
7. طلب سيرفر جاهز (تجهيز تلقائي)
8. تسجيل الدخول لأول مرة
9. الترخيص: إنشاء الحساب، ربط SAMM، الدفع، التجديد
10. ربط الراوترات (NAS) محلياً أو عبر VPN
11. تفعيل الميزات الإضافية (Data Log و SAMM Fallback و Health والنسخ الاحتياطي والتحديثات)
12. المشكلات الشائعة وحلولها

طريقة استخدام هذا الدليل

نفّذ الخطوات بالترتيب، وانسخ الأوامر كما هي تماماً (المربعات الداكنة)، ولا تتجاوز أي خطوة. عند ظهور العلامة ✅ انتقل إلى الخطوة التالية، وعند ظهور العلامة ❌ توقّف وعالج المشكلة أولاً.

1. اختيار طريقة التنصيب المناسبة

الحالة	الطريقة	القسم
لديك حاسوب يعمل بنظام Windows 10/11 بنسخة **Pro** ويبقى قيد التشغيل باستمرار	Windows	3 و 4
لديك سيرفر أو Virtual Machine أو VPS (سيرفر سحابي مستأجر)	Ubuntu Server	5
لديك راوتر MikroTik قوي (RB5009 أو CCR2004 أو CCR2116 أو CCR2216 أو hAP ax² أو L009 أو CHR) مع ذاكرة USB أو microSD	MikroTik Container	6
لا ترغب في تنصيب أي شيء بنفسك	سيرفر جاهز	7

توصيتنا

للشبكات الفعلية التي تضم عدداً كبيراً من المشتركين نوصي باستخدام **Ubuntu Server** أو **سيرفر جاهز**.
أما Windows فيناسب الشبكات الصغيرة والتجربة. ويُعدّ MikroTik Container الخيار الأحدث والأخف.

2. قبل البدء: عناوين IP

يحتاج كل جهاز على الشبكة إلى عنوان IP **خاص به وحده**. يشبه عنوان IP رقم الهاتف: إذا حمل جهازان الرقم نفسه، وصلت البيانات إلى الجهاز الخطأ وتعطّل العمل.

> ⚠️ **القاعدة الأساسية**
>
> الراوتر والحاسوب و SAMM هي **ثلاثة عناوين مختلفة**. لا تمنح SAMM عنوان الراوتر ولا عنوان الحاسوب، ولا تستخدم أبداً عنواناً يستخدمه جهاز آخر.

اختر أحد الخيارات التالية وانسخ أرقامه

الخيار	راوتر MikroTik	حاسوب Windows	SAMM	Subnet
1 ⭐ الأفضل	`10.10.10.1`	`10.10.10.10`	`10.10.10.20`	`/24 = 255.255.255.0`
2	`10.20.30.1`	`10.20.30.10`	`10.20.30.20`	`/24`
3	`172.16.50.1`	`172.16.50.10`	`172.16.50.20`	`/24`

يعتمد هذا الدليل **الخيار 1**. إذا اخترت خياراً آخر، فاستبدل الأرقام فقط.

التحقق من أن العناوين غير مستخدمة

1. افتح برنامج **WinBox** وادخل إلى الراوتر، ثم اضغط **New Terminal**.
2. الصق الأمر التالي:

```
/ip address print
```

✅ لا يوجد أي سطر يبدأ بـ `10.10.10.`: الخيار 1 مناسب.

❌ يوجد سطر يبدأ بـ `10.10.10.`: استخدم الخيار 2، ثم الخيار 3.

3. الصق الأمر التالي:

```
/ping 10.10.10.20 count=3
```

✅ ظهرت الكلمة `timeout`: العنوان غير مستخدم.

❌ ظهر رد: العنوان مستخدم، فاختر خياراً آخر.

تعيين عنوان للراوتر على منفذ غير مستخدم

مثال: الحاسوب (أو سيرفر SAMM) موصول بالمنفذ **ether5**، ولا يوجد أي جهاز آخر على هذا المنفذ.

```
/interface bridge port remove [find interface=ether5]
/ip address add address=10.10.10.1/24 interface=ether5 comment=SAMM
/ip service set api disabled=no
```

⚠️ تنبيه

يفصل السطر الأول المنفذ ether5 عن الشبكة الداخلية (Bridge)، لذا لا تنفّذه إلا إذا كان المنفذ غير مستخدم. ويشغّل السطر الأخير خدمة API في الراوتر، وهي الخدمة التي يستخدمها SAMM لإدارة الراوتر.

3. التنصيب على Windows

المتطلبات

- Windows 10 أو 11 بنسخة **Pro** أو Enterprise أو Education، أو Windows Server 2019 وما بعده.
  نسخة Home غير مدعومة لأنها لا تتضمن Hyper-V.
- ذاكرة RAM بسعة 8 GB أو أكثر (يستخدم SAMM منها 4 GB)، ومساحة فارغة لا تقل عن 40 GB.
- **كابل شبكة** من الحاسوب إلى الراوتر، إذ إن الاتصال عبر Wi-Fi لا يعمل في أغلب الحالات.
- تفعيل خاصية Virtualization في BIOS (يشرح القسم 4 طريقة ذلك).

كيف أعرف نسخة Windows؟

اضغط Windows + R واكتب `winver` ثم اضغط Enter. إذا ظهرت كلمة **Home** فيجب ترقية النسخة إلى Pro أولاً.

الخطوة 1: تعيين عنوان IP ثابت للحاسوب

1. اضغط Windows + R واكتب `ncpa.cpl` ثم اضغط Enter.
2. انقر بالزر الأيمن على **Ethernet** واختر **Properties**.
3. انقر نقراً مزدوجاً على **Internet Protocol Version 4 (TCP/IPv4)**.
4. اختر **Use the following IP address** واكتب القيم التالية:

IP address	**10.10.10.10**
Subnet mask	**255.255.255.0**
Default gateway	**10.10.10.1**
Preferred DNS	**8.8.8.8**
Alternate DNS	**1.1.1.1**

5. اضغط **OK** ثم **OK**.
6. للتحقق: اضغط Windows + R واكتب `cmd` ثم نفّذ:

```
ping 10.10.10.1
```

✅ ظهرت العبارة `Reply from 10.10.10.1`: الاتصال سليم.
❌ ظهرت العبارة `Request timed out`: تحقّق من الكابل ومن توصيله بالمنفذ ether5.

الخطوة 2: تشغيل أداة التنصيب

1. انقر بالزر الأيمن على زر **Start** واختر **Terminal (Admin)** أو **Windows PowerShell (Admin)**، ثم وافق بالضغط على **Yes**.
   (لا تستخدم Command Prompt).
2. الصق السطر التالي واضغط Enter:

```
irm https://samm.securytik.com/install-windows.ps1 | iex
```

إذا تعذّر الوصول إلى الموقع، فاستخدم الرابط البديل:

```
irm https://dl.securytik.com/install-windows.ps1 | iex
```

الخطوة 3: الإجابة عن أسئلة أداة التنصيب

السؤال	الإجابة
بطاقة الشبكة (Adapter)	رقم بطاقة **Ethernet** الموصولة بالراوتر
عنوان SAMM	**10.10.10.20/24**، ولا تكتب أبداً **.10** (الحاسوب) أو **.1** (الراوتر)
Gateway (عنوان الراوتر MikroTik)	**10.10.10.1**
DNS servers	اضغط Enter
CPU / RAM / Disk	اضغط Enter لكل منها
Continue? [y/N]	اكتب y ثم اضغط Enter

إذا ظهرت الرسالة already answers on the network

فهذا يعني أن العنوان مستخدم من جهاز آخر. اكتب عنواناً مختلفاً، مثل **10.10.10.30/24**.

إذا طُلبت إعادة تشغيل Windows

يحدث ذلك مرة واحدة لتشغيل Hyper-V. أعد تشغيل الحاسوب، وبعد تسجيل الدخول يتابع التنصيب تلقائياً. وإذا لم يتابع، فافتح PowerShell (Admin) مجدداً والصق السطر نفسه.

يستغرق التنصيب **من 10 إلى 20 دقيقة** مع شريط يوضّح التقدّم. لا تغلق النافذة ولا تطفئ الحاسوب.

الخطوة 4: فتح SAMM

عند الانتهاء يظهر على سطح المكتب اختصاران: **SAMM Admin** و **SAMM Info**. افتح **SAMM Admin**، أو اكتب في المتصفح:

```
http://10.10.10.20/admin
```

نوع الدخول	اسم المستخدم / كلمة المرور
لوحة SAMM	`admin` / `admin` (يجب تغييرها فوراً)
SSH إلى جهاز SAMM	`samm` / `samm`
Root (الشاشة)	`samm` / `root`

يجب أن يبقى الحاسوب قيد التشغيل

يعمل SAMM تلقائياً عند تشغيل Windows. في الحاسوب المحمول أبقِ الشاحن موصولاً، واضبط خيار إغلاق الغطاء على **Do nothing** من Control Panel ثم Power Options.

لإزالة SAMM لاحقاً: افتح **SAMM Info** من سطح المكتب واكتب `uninstall-samm`.

4. تفعيل Virtualization (VT-x / AMD-V)

نفّذ هذا القسم إذا أظهرت أداة التنصيب أن **Virtualization غير مفعّلة**، أو ظهر خطأ متعلق بـ **Intel VT-x**، أو تعذّر تشغيل **Hyper-V**.

أولاً: هل الخاصية مفعّلة؟

1. اضغط Ctrl + Shift + Esc لفتح Task Manager.
2. اختر **Performance** ثم **CPU**.
3. انظر أسفل الرسم البياني إلى عبارة **Virtualization**:

✅ **Enabled**: الخاصية مفعّلة ولا حاجة لأي إجراء.

❌ **Disabled**: يجب تفعيلها من BIOS كما هو موضح أدناه.

ما نوع المعالج لديك؟

في Task Manager ثم **Performance** ثم **CPU** يظهر اسم المعالج أعلى يمين الصفحة، ويبدأ إما بـ **Intel** (مثل Intel Core i5) أو بـ **AMD** (مثل AMD Ryzen 5). دوّن النوع، لأن اسم الخيار في BIOS يختلف بحسبه.

المعالج	الخيار الذي يجب ضبطه على Enabled	هل هو ضروري؟
Intel	**Intel Virtualization Technology** (أو VT-x أو Vanderpool)	نعم، ضروري
	Execute Disable Bit (أو XD bit أو No-Execute Memory Protection)	نعم، يحتاجه Hyper-V (ويكون مفعّلاً عادةً)
	Intel VT-d (Virtualization for Directed I/O)	اختياري
AMD	**SVM Mode** (أو AMD-V أو Secure Virtual Machine)	نعم، ضروري
	NX Mode (No-Execute)	نعم، يحتاجه Hyper-V (ويكون مفعّلاً عادةً)
	IOMMU (AMD-Vi)	اختياري

> **لا تغيّر أي إعداد آخر**
>
> لا تعدّل Secure Boot ولا ترتيب الإقلاع ولا نمط القرص (AHCI/RAID) ولا الساعة. غيّر فقط الخيارات الواردة في الجدول أعلاه.

التفعيل من BIOS

1. احفظ عملك وأعد تشغيل الحاسوب.

2. فور ظهور الشاشة، اضغط مفتاح الدخول إلى BIOS عدة مرات متتالية:

الشركة المصنّعة	المفتاح	موقع الخيار غالباً
Dell	F2	Virtualization Support ثم Enable Intel Virtualization Technology
HP	Esc ثم F10	System Configuration أو Advanced ثم Virtualization Technology (VTx)
Lenovo	F1 أو F2 (أو زر Novo الصغير)	Security أو Configuration ثم Intel Virtualization Technology أو AMD SVM
ASUS	F2 أو Del	Advanced Mode (F7) ثم Advanced ثم CPU Configuration
Acer	F2	Advanced أو Main ثم Intel Virtualization Technology
MSI	Del	OC ثم CPU Features
Gigabyte	Del	Tweaker ثم Advanced CPU Settings
حاسوب مكتبي آخر	Del	Advanced ثم CPU Configuration

3. اضبط الخيار على **Enabled**:
   - معالج **Intel**: الخيار **Intel Virtualization Technology** (ويُسمّى أيضاً **VT-x**).
   - معالج **AMD**: الخيار **SVM Mode** (ويُسمّى أيضاً **AMD-V**).
4. طريقة التنقل في BIOS: استخدم مفاتيح الأسهم ↑ ↓ ← → للتنقل، واضغط Enter لفتح الخيار، ثم اختر **Enabled** واضغط Enter مرة أخرى. في واجهات BIOS الرسومية يمكن استخدام الفأرة. وإذا كانت القائمة مخفية، فابحث عن **Advanced Mode** (غالباً بالمفتاح F7).
5. اضغط F10 ثم اختر **Yes** للحفظ والخروج.
6. افتح Task Manager مجدداً، ويجب أن تظهر العبارة **Virtualization: Enabled**. بعد تشغيل Hyper-V قد تظهر بدلاً منها العبارة **A hypervisor has been detected**، وهي تعني أيضاً أن الخاصية مفعّلة.

> **إذا لم يعمل أي مفتاح**
>
> من داخل Windows: افتح Settings ثم System ثم Recovery ثم Advanced startup واضغط **Restart now**، ثم اختر Troubleshoot ثم Advanced options ثم **UEFI Firmware Settings** ثم Restart.

تشغيل Hyper-V (إذا لم تشغّله أداة التنصيب)

افتح PowerShell (Admin) والصق الأمر التالي:

```
Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -All
```

اكتب `Y` لإعادة التشغيل، ثم شغّل أداة تنصيب SAMM مرة أخرى.

مشكلات شائعة

- لا يوجد خيار Virtualization في BIOS: حدّث BIOS من موقع الشركة المصنّعة؛ فالأجهزة القديمة جداً لا تدعم تشغيل SAMM.
- ظهرت الرسالة Feature name not found: نسخة Windows لديك هي Home، ويجب ترقيتها إلى Pro.
- يعمل Windows نفسه داخل VMware أو Proxmox أو Hyper-V: فعّل **Nested Virtualization** في النظام الخارجي (في VMware: الخيار Virtualize Intel VT-x/EPT والجهاز مُطفأ).

5. التنصيب على Ubuntu Server (سيرفر خاص أو VPS)

المتطلبات

- Ubuntu Server **جديد** بالإصدار 22.04 أو 24.04 أو 26.04 (أو Debian 12 / 13)، بنسخة Server وليس Desktop.
- معالج بنواتين وذاكرة 4 GB ومساحة 40 GB على الأقل، مع اتصال بالإنترنت.
- كلمة مرور المستخدم **root** أو مستخدم يملك صلاحية `sudo`.

الخطوة 1: الدخول إلى السيرفر

من Windows افتح PowerShell (أو برنامج Termius أو PuTTY) واكتب الأمر التالي مع عنوان السيرفر لديك:

```
ssh root@10.10.10.20
```

الخطوة 2: تعيين عنوان IP ثابت (للسيرفرات المحلية فقط)

في حالة VPS تمنحك الشركة المزوّدة عنواناً ثابتاً مسبقاً، فتجاوز هذه الخطوة. أما في السيرفر الموجود ضمن شبكتك، فعدّل ملف إعدادات الشبكة:

```
sudo nano /etc/netplan/50-cloud-init.yaml
```

واجعل محتواه كما يلي (قد يكون اسم بطاقة الشبكة لديك `eth0` أو `ens18`، ويمكن معرفته بالأمر `ip a`):

```
network:
  version: 2
  ethernets:
    eth0:
      addresses: [10.10.10.20/24]
      routes:
        - to: default
          via: 10.10.10.1
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1]
```

احفظ الملف (`Ctrl` + `O` ثم `Enter` ثم `Ctrl` + `X`) ثم طبّق الإعدادات:

```
sudo netplan apply
```

الخطوة 3: تنصيب SAMM بسطر واحد

```
curl -fsSL https://samm.securytik.com/install.sh | sudo bash
```

إذا كان GitHub أو الموقع محجوباً في بلدك، فاستخدم الرابط البديل:

```
curl -fsSL https://dl.securytik.com/install.sh | sudo bash
```

السؤال	الإجابة
Cloudflare token	اضغط Enter للتجاوز (يمكن إضافته لاحقاً)
HTTP port (فقط إذا كان المنفذ 80 مستخدماً)	اضغط Enter لاعتماد المنفذ 8080

بعد بضع دقائق تظهر الرسالة **SAMM is installed and running**. افتح العنوان التالي:

```
http://10.10.10.20/admin
```

اسم المستخدم وكلمة المرور: `admin` / `admin`. في حالة VPS استخدم عنوان IP العام الخاص به بدلاً من 10.10.10.20.

> **هل يحتوي VPS على Firewall؟**
>
> اسمح من لوحة الشركة المزوّدة بالمنافذ التالية: TCP 80 و 443 (لوحة التحكم)، و UDP 51820 (شبكة WireGuard للراوترات)، و UDP 500 و 4500 و 1701 (L2TP/IPsec)، و TCP 443 (SSTP).

6. التنصيب على راوتر MikroTik (Container)

المتطلبات

- RouterOS بالإصدار **7.23 أو أحدث**.
- راوتر بمعالج arm64 أو x86، مثل RB5009 أو hAP ax² أو L009 أو CCR2004 أو CCR2116 أو CCR2216 أو x86 أو CHR. **لا يعمل** على hEX أو RB750 أو الطرازات القديمة.
- ذاكرة USB أو microSD بسعة **30 GB أو أكثر** بتنسيق **ext4**.

الخطوة 1: تفعيل Container Mode

1. من WinBox اضغط **New Terminal** والصق:

```
/system device-mode update container=yes
```

2. ينتظر الراوتر تأكيدك: خلال **5 دقائق افصل التيار الكهربائي ثم أعد توصيله** (أو اضغط زر Reset ضغطة قصيرة واحدة كما تشير الرسالة). إعادة التشغيل العادية لا تكفي.

الخطوة 2: تجهيز الذاكرة

```
/disk print
```

حدّد اسم ذاكرة USB أو microSD (مثل `usb1`)، ثم نفّذ التهيئة (Format)، علماً بأنها تمسح كل محتوى الذاكرة:

```
/disk format usb1 file-system=ext4 label=samm
```

الخطوة 3: سطر واحد ينصّب كل شيء

```
/tool fetch url="https://samm.securytik.com/install-routeros.rsc" dst-path=samm-instal
l.rsc; /import samm-install.rsc
```

يفحص هذا السطر الراوتر، ويثبّت حزمة **container**، ويحدّد الذاكرة، ثم ينزّل SAMM ويشغّله. وعندما يُطلب منك ذلك (بعد إعادة التشغيل أو فصل التيار) **الصق السطر نفسه مرة أخرى**، فيتابع من حيث توقّف.

الخطوة 4: تشغيل SAMM تلقائياً بعد إعادة التشغيل

```
/container set [find where name~"^app-samm"] start-on-boot=yes restart-policy=always
/system scheduler remove [find name=samm-watchdog]
/system scheduler add name=samm-watchdog start-time=startup interval=1m on-event=":for
each c in=[/container find where name~\"^app-samm\" and stopped] do={/container start
\$c}"
```

افتح لوحة التحكم عبر `http://<router IP>:8000/admin` باسم المستخدم وكلمة المرور `admin` / `admin`. يتصل الراوتر بـ SAMM المثبّت عليه عبر العنوان **`127.0.0.1`**.

> ⚠️ **تحديث SAMM على MikroTik يحذف البيانات**
>
> قبل أي تحديث: افتح SAMM ثم Tools ثم Backup، وأنشئ نسخة احتياطية و**نزّلها إلى حاسوبك**. بعد ذلك احذف التطبيق وأضفه من جديد، ثم استرجع النسخة الاحتياطية.

> **ظهرت الرسالة could not download أو رُفض أمر fetch؟**
>
> إعدادات device-mode في الراوتر تمنع التنزيل. نفّذ `/system device-mode print`، وإذا ظهر `fetch: no` فنفّذ `/system device-mode update fetch=yes` ثم افصل التيار وأعد توصيله مرة أخرى.

7. طلب سيرفر جاهز

لا حاجة إلى أي تنصيب: نتولّى استئجار السيرفر وشراء نطاق **com.** باسمك، وتنصيب SAMM باسم شركتك، وربط الترخيص.

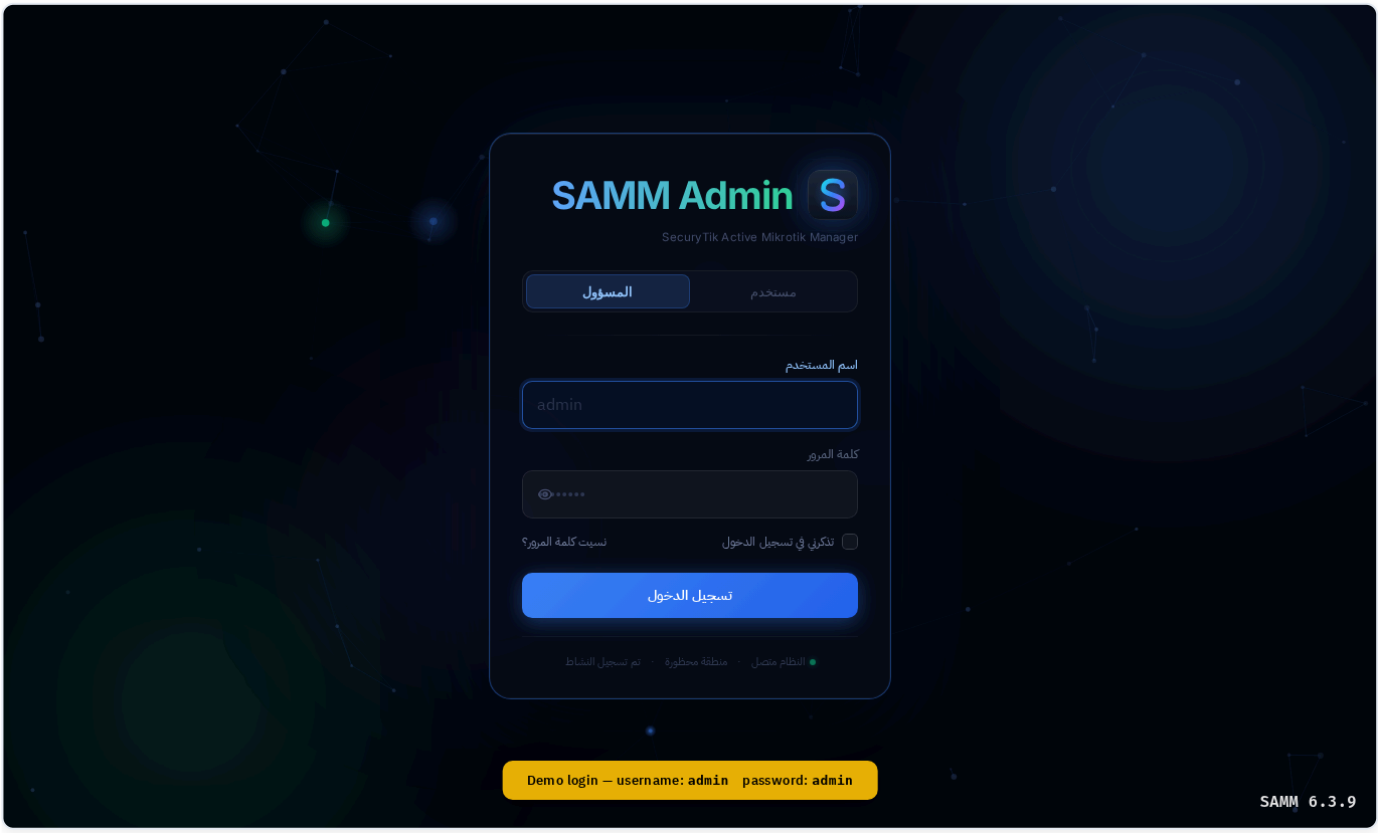
الحجم	مواصفات السيرفر	السعر السنوي
صغير	6 cores · 12 GB RAM · 200 GB SSD	$100
متوسط	8 cores · 24 GB RAM · 300 GB SSD	$200
كبير	12 cores · 48 GB RAM · 400 GB SSD	$300

1. ادخل إلى **samm.securytik.com** وسجّل الدخول (أو أنشئ حساباً جديداً).
2. افتح **Dashboard** ثم **Get a server**.
3. اختر الحجم واسم السيرفر وعدد المشتركين.
4. ابحث عن نطاق **com.** المطلوب، أو اختر أحد الاقتراحات.
5. اضغط زر الدفع واختر طريقة الدفع. **يجب إتمام الدفع خلال ساعتين**، وإلا يُلغى الطلب.
6. تتم بقية العملية تلقائياً، ويصلك **بريد إلكتروني** يتضمن رابط لوحة التحكم (`https://your-domain/admin`) وكلمة مرور قوية.

> **التجديد**
>
> يُتاح التجديد قبل 7 أيام من نهاية السنة. يجب التجديد قبل تاريخ الانتهاء بـ **يوم واحد على الأقل**، وإلا يُحذف السيرفر والنطاق والبيانات. احرص دائماً على الاحتفاظ بنسخ احتياطية لديك.

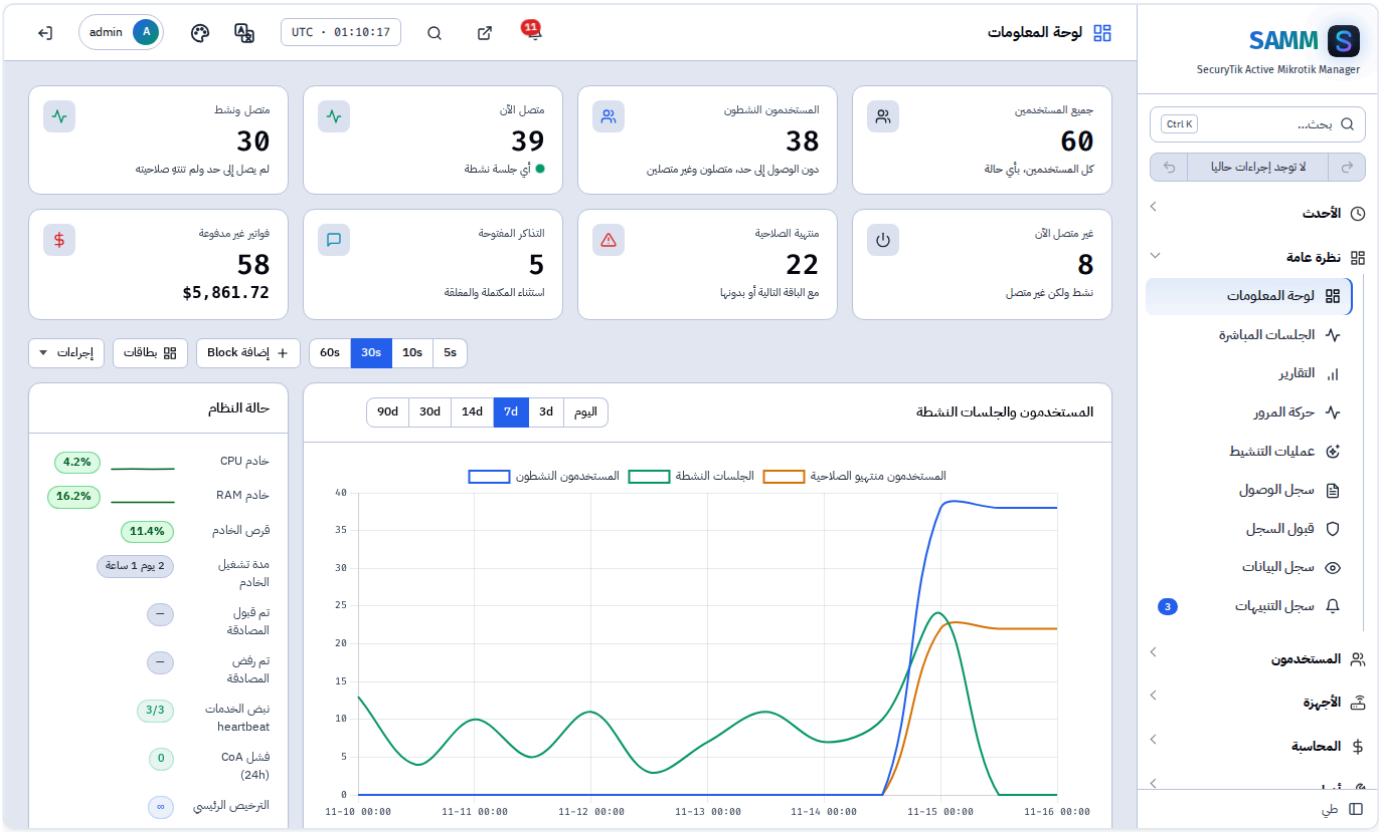
الدخول عبر SSH: يمكنك إنشاء حساب SSH خاص بك من **Dashboard** ثم **Servers**.

8. تسجيل الدخول لأول مرة



صفحة تسجيل الدخول إلى SAMM

1. افتح `http://<SAMM IP>/admin` (مثال: `http://10.10.10.20/admin`).
2. سجّل الدخول باسم المستخدم وكلمة المرور `admin` / `admin`.
3. غيّر كلمة المرور فوراً من قائمة الحساب أعلى الشاشة ثم **Profile**، أو من **النظام** ثم **المسؤولون**.



لوحة التحكم بعد تسجيل الدخول

9. الترخيص: الحساب، الربط، الدفع، التجديد

يعمل SAMM الجديد **دون ترخيص** بحدود منخفضة (25 مشتركاً وراوتر واحد). وللحصول على حدود أعلى، اربطه بحسابك في SecuryTik واختر باقة.

الباقة	المشتركون	بطاقات Hotspot	الراوترات
Unregistered	25	25	1
Free	100	50	2
Lite	500	1,500	4
Plus	1,000	3,000	6
Pro	2,000	6,000	12
Mega	5,000	15,000	24
Max	10,000	30,000	غير محدود
Unlimited	غير محدود	غير محدود	غير محدود

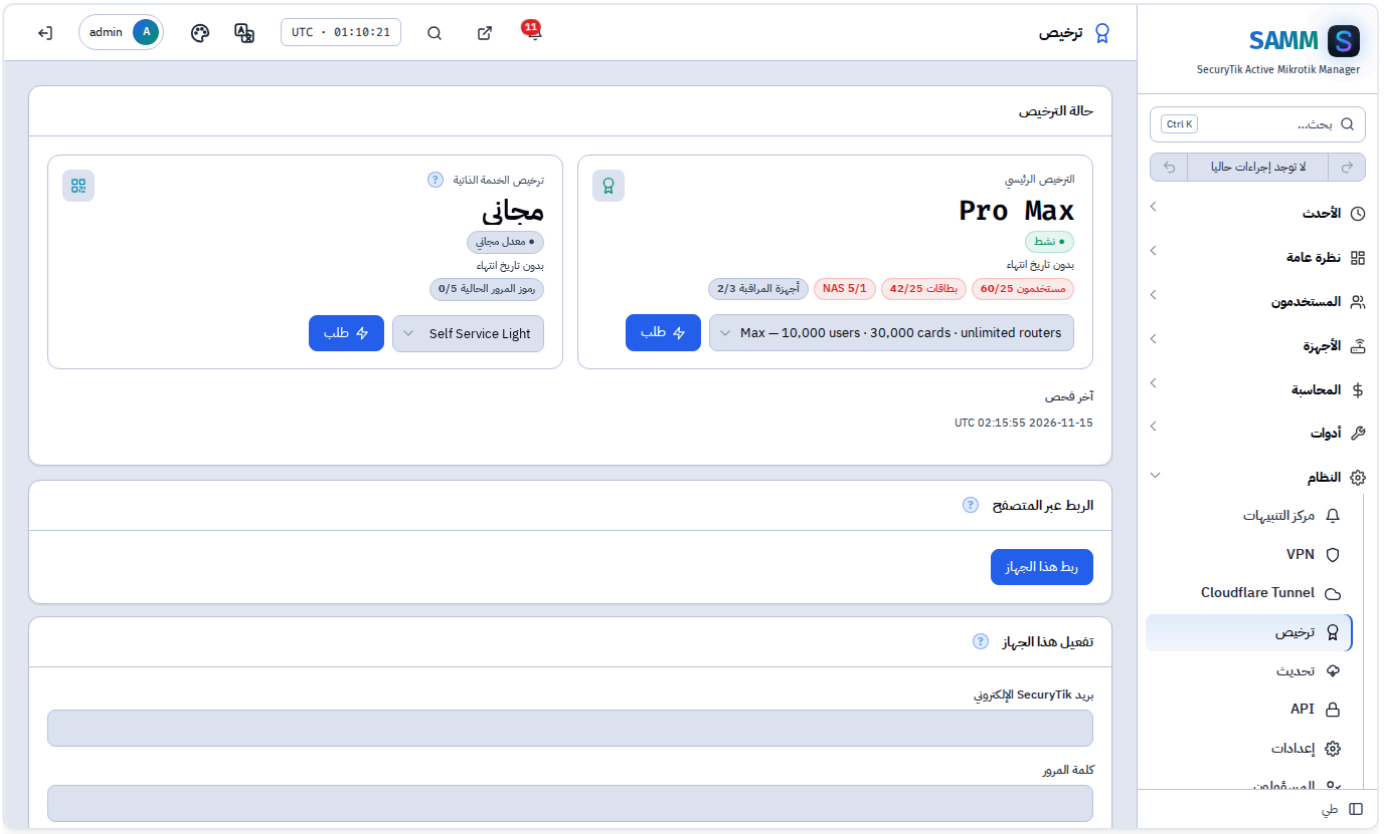
الأسعار متاحة على **`samm.securytik.com/pricing`**. تتضمن جميع الباقات كل الميزات، وتختلف فقط في الحدود العددية.

الخطوة 1: إنشاء الحساب

ادخل إلى **samm.securytik.com** واضغط **Sign up**. استخدم بريدك الإلكتروني الحقيقي وأكّده.

الخطوة 2: ربط SAMM بحسابك

1. في SAMM افتح **النظام** ثم **ترخيص**.
2. اضغط **Link this device**، فيظهر **رمز (Code)**.
3. من الهاتف أو الحاسوب افتح **samm.securytik.com**، وسجّل الدخول، ثم وافق على الرمز من **Dashboard** ثم **Link a device**.
4. ينتقل SAMM تلقائياً إلى باقة **Free**.



النظام ← ترخيص

الخطوة 3: شراء باقة والدفع

1. في samm.securytik.com افتح **Dashboard** ثم **Devices** واختر جهاز SAMM الخاص بك (أو اختر الباقة من صفحة الترخيص داخل SAMM).
2. اختر الباقة والمدة (مثل سنة واحدة).
3. اضغط **Continue to payment** واختر إحدى طرق الدفع المعروضة.
4. أتمّ الدفع، فيُفعَّل الترخيص تلقائياً خلال دقائق. تظهر الباقة الجديدة في صفحة الترخيص داخل SAMM (اضغط زر إعادة الفحص عند الحاجة).

> **الدفع بالبطاقة المصرفية**
>
> للدفع بالبطاقة المصرفية، راسلنا عبر واتساب على الرقم **+961 81 507 933** مع رقم الترخيص (License ID)، وسنرسل إليك رابط الدفع.

الخطوة 4: التجديد

- افتح **Dashboard** ثم **Devices** ثم جهازك واضغط **Renew**، وادفع بالطريقة نفسها.
- فعّل خيار **Auto-renew** للتجديد التلقائي.
- تصلك رسائل تذكير قبل تاريخ الانتهاء.

في حال عدم التجديد

المرحلة	ما يحدث
تنبيه	يظهر شريط أحمر، ويستمر كل شيء في العمل.
مهلة (Grace)	فترة قصيرة للتجديد، ويبقى المشتركون متصلين.
إيقاف جزئي	تتوقف التعديلات، ويستمر دخول المشتركين نحو 7 أيام.
إيقاف كامل	لا تعمل سوى صفحة التجديد.

لا تُحذف بياناتك أبداً. عند التجديد في أي مرحلة، يعود كل شيء إلى العمل تلقائياً.

10. ربط الراوترات (NAS)

NAS هو راوتر MikroTik الذي يتصل عبره المشتركون (PPPoE / Hotspot). يجب أن يصل SAMM إلى الراوتر، وأن يصل الراوتر إلى SAMM.

موقع SAMM	موقع الراوتر	الطريقة
الشبكة نفسها (Windows أو سيرفر محلي أو MikroTik)	الشبكة نفسها	الحالة (أ): الإضافة بعنوان IP
VPS أو سيرفر جاهز (على الإنترنت)	أي مكان	الحالة (ب): رابط VPN بسطر واحد
محلي	مدينة أخرى أو خلف NAT	الحالة (ب)، مع تحويل منافذ VPN إلى SAMM على الراوتر الرئيسي

الحالة (أ): الراوتر على الشبكة نفسها

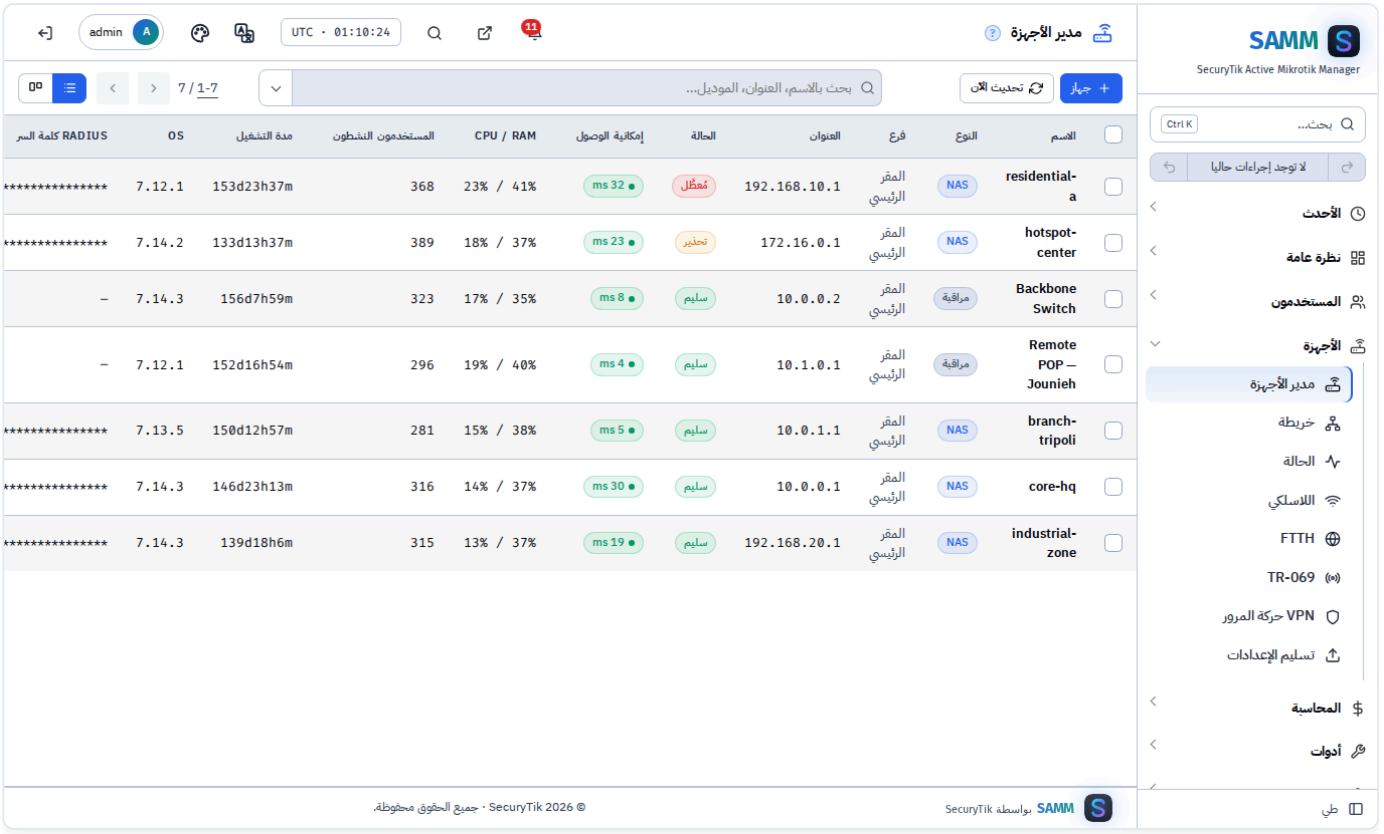
1. تأكّد من تشغيل خدمة API على الراوتر:

```
/ip service set api disabled=no
```

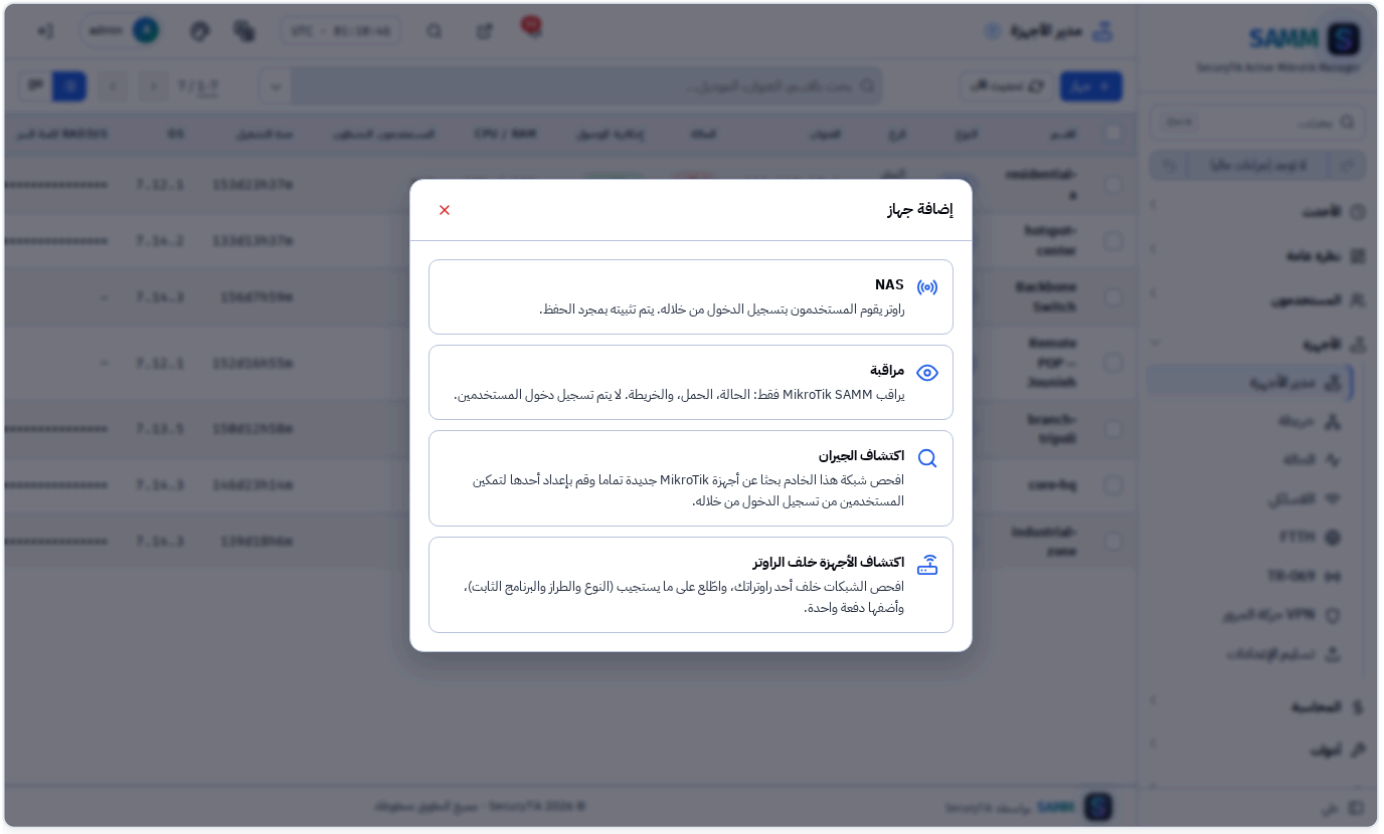
2. في SAMM افتح **الأجهزة** ثم **مدير الأجهزة**، واضغط **+ جهاز**، ثم اختر **NAS**.
3. املأ نموذج **New Router**:

NAS IP or hostname	**10.10.10.1**
Shortname	أي اسم، مثل `Main`
Type	MikroTik
RADIUS shared secret	كلمة سر تختارها (حروف وأرقام دون مسافات)
CoA port / API port	اتركهما على القيم الافتراضية
API user / API password	بيانات الدخول إلى الراوتر عبر WinBox

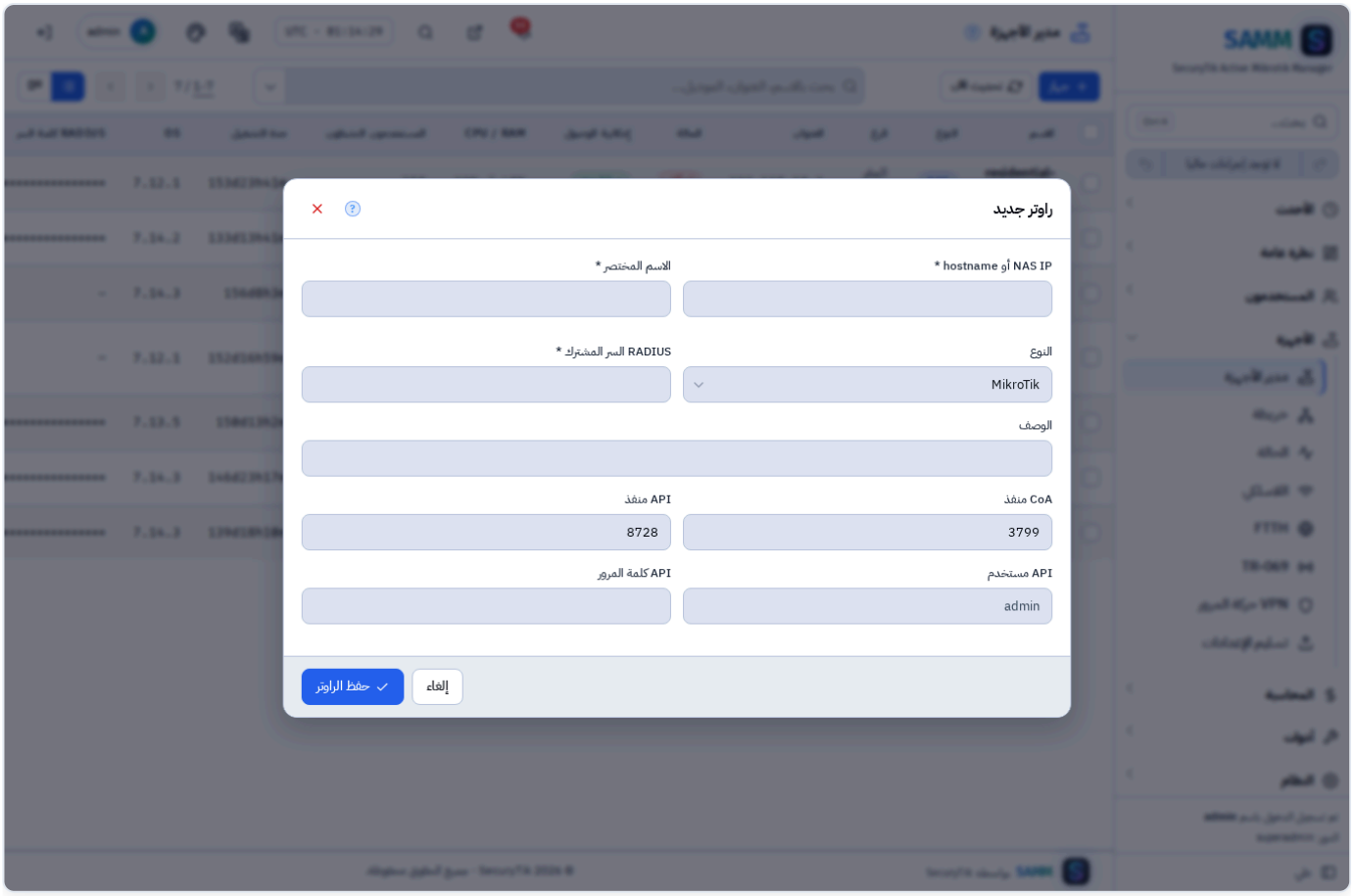
4. اضغط **Save Router**.
5. حدّد الراوتر في القائمة ثم اختر **Actions** ثم **Push RADIUS**، فيكتب SAMM إعدادات RADIUS في الراوتر تلقائياً (ويمكن ذلك أيضاً من القائمة ⋮ الخاصة بالراوتر).
6. انتظر حتى تظهر حالة الراوتر **سليم**.



الأجهزة ← مدير الأجهزة: كل راوتر مع حالته



+ جهاز ← اختر NAS



نموذج New Router

الحالة (ب): الراوتر في موقع بعيد أو SAMM على VPS (رابط VPN)

يتضمن SAMM خادم VPN خاصاً به. يفتح الراوتر نفقاً (Tunnel) إلى SAMM، فيعمل الاتصال خلف NAT أو عبر شبكة 4G أو من أي مكان.

اختيار نوع VPN

إصدار الراوتر	النوع المناسب
RouterOS 7	**WireGuard** (الأسرع والأبسط) ⭐
RouterOS 6	**L2TP/IPsec** (لأن RouterOS 6 لا يدعم WireGuard)
راوتران أو أكثر خلف عنوان IP عام واحد	**SSTP**

الخطوة 1: تشغيل خوادم VPN (مرة واحدة)

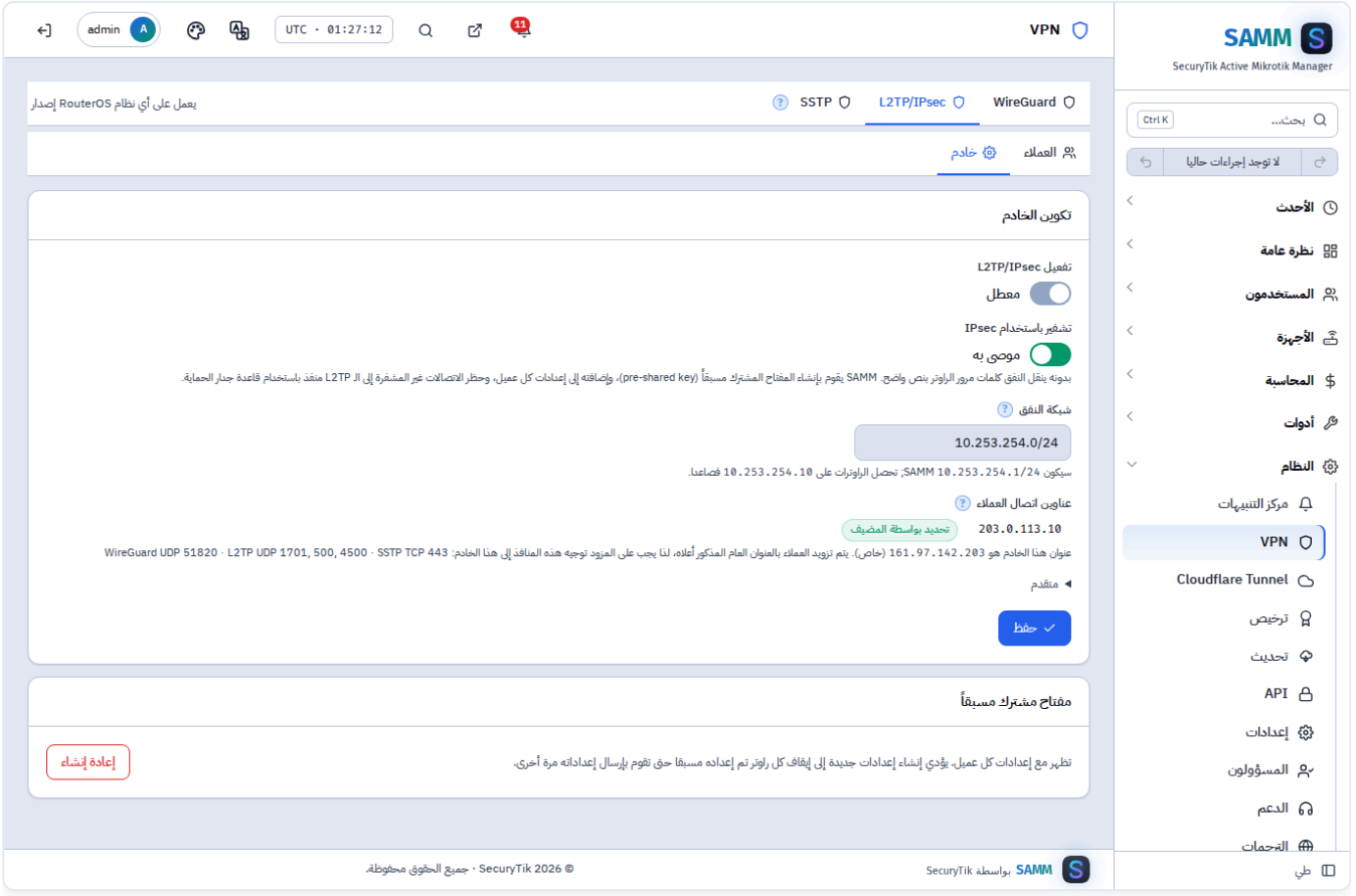
> ⚠️ **خوادم VPN الثلاثة متوقفة في SAMM الجديد**
>
> تأتي خوادم WireGuard و L2TP/IPsec و SSTP جاهزة لكنها متوقفة افتراضياً، ولا يمكن لأي راوتر الاتصال قبل تشغيل الخادم المناسب له. شغّل الخوادم التي تحتاجها راوتراتك، ونوصي بتشغيل الثلاثة.

WireGuard (RouterOS 7)

1. في SAMM افتح **النظام** ثم **VPN** ثم تبويب **WireGuard** ثم **خادم**.
2. اضغط **Generate Keys** لإنشاء مفاتيح الخادم (في المرة الأولى فقط).
3. اترك المنفذ `51820` والعناوين على القيم الافتراضية.
4. شغّل الخادم (**On**) واضغط **Save** ثم أكّد.

L2TP/IPsec (RouterOS 6 و 7)

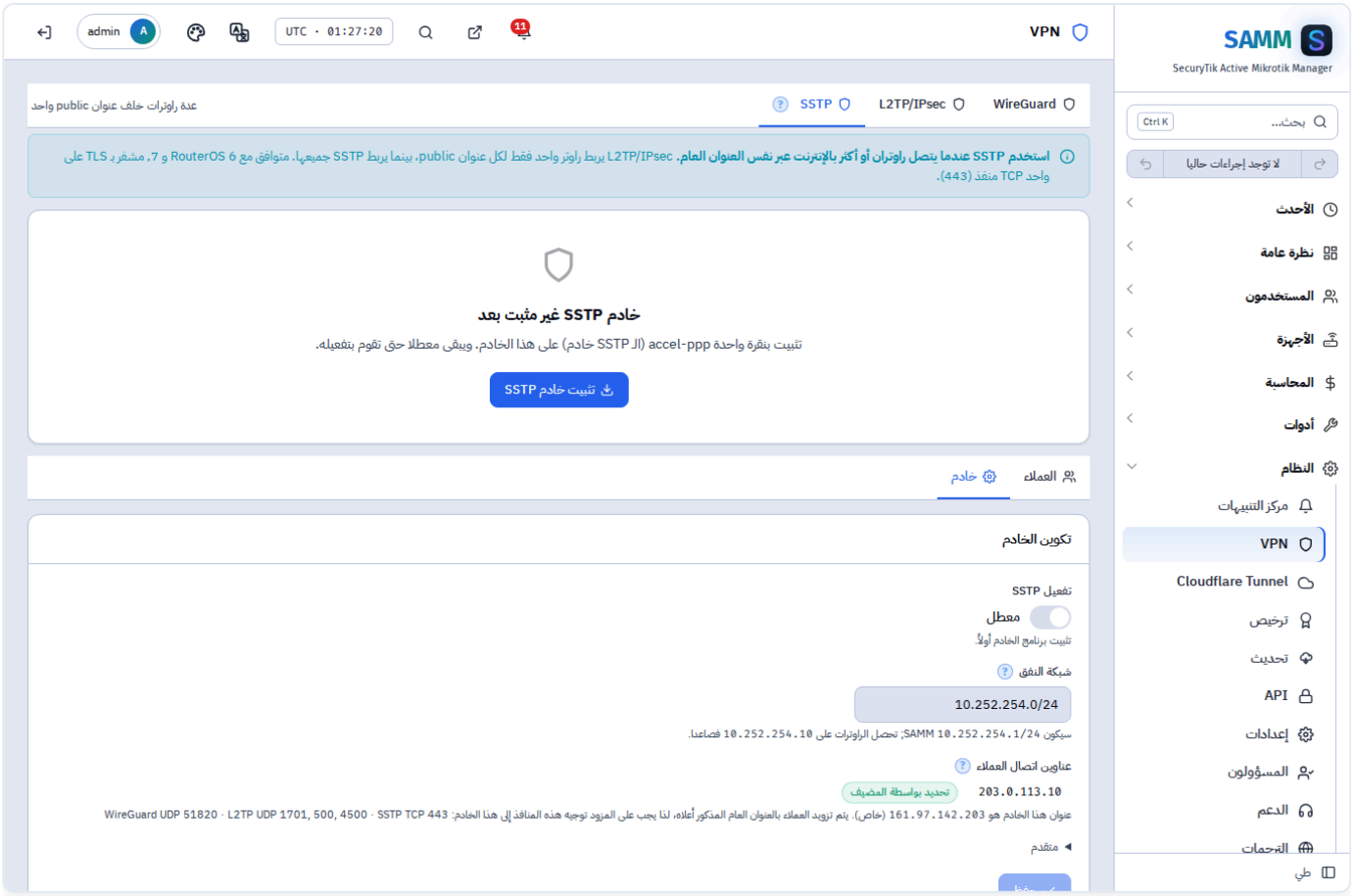
1. افتح **النظام** ثم **VPN** ثم تبويب **L2TP/IPsec** ثم **خادم**.
2. فعّل الخيار **Enable L2TP/IPsec** (تظهر حالته *Disabled* قبل التفعيل).
3. أبقِ الخيار **Encrypt with IPsec** مفعّلاً (موصى به؛ فبدونه تنتقل كلمات مرور الراوترات دون تشفير). يُنشئ SAMM المفتاح المشترك (Pre-shared key) ويضيفه إلى إعدادات كل راوتر.
4. اترك شبكة النفق على القيمة الافتراضية واضغط **Save**.



النظام ← L2TP/IPsec ← VPN ← خادم: فعّل Enable L2TP/IPsec ثم اضغط Save

SSTP (عدة راوترات خلف عنوان IP عام واحد)

1. افتح **النظام** ثم **VPN** ثم تبويب **SSTP** ثم **خادم**.
2. فعّل الخيار **Enable SSTP**، واترك المنفذ كما هو، ثم اضغط **Save**.



النظام ← SSTP ← VPN ← خادم

فتح المنافذ أو تحويلها

نوع VPN	المنفذ
WireGuard	UDP 51820
L2TP/IPsec	UDP 1701 و 500 و 4500
SSTP	TCP 443

في حالة VPS: اسمح بهذه المنافذ في Firewall لدى الشركة المزوّدة. وإذا كان SAMM في المنزل أو المكتب (خلف NAT): حوّل هذه المنافذ من الراوتر الرئيسي إلى عنوان SAMM. يعرض تبويب الخادم المنافذ المطلوبة والعنوان العام الذي يُعطى للراوترات.

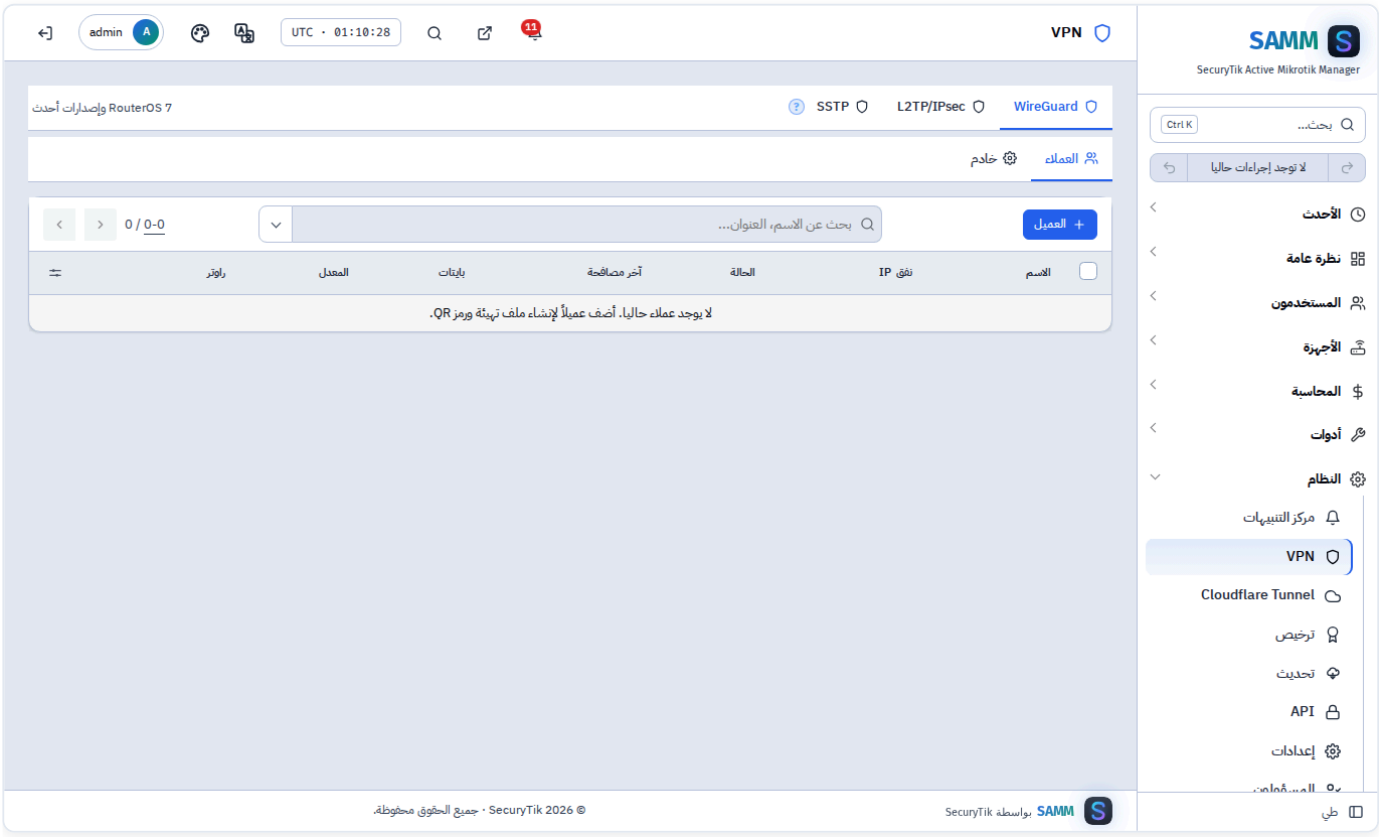
> ⚠️ **لا تضغط Regenerate Keys بعد ذلك**
>
> فهذا الإجراء يقطع اتصال جميع الراوترات المتصلة. أنشئ المفاتيح مرة واحدة فقط عند البداية.

الخطوة 2: الحصول على رابط التنصيب للراوتر

1. افتح تبويب **العملاء** ثم اضغط **+ العميل**.

2. اكتب اسم الراوتر، واختر **Managed NAS** (يدخل المشتركون عبره)، أو **Monitor only** لأجهزة البث (Access Points).

3. احفظ، فيعرض SAMM **رابط تنصيب من سطر واحد**. اضغط زر النسخ.



النظام ← VPN ← العملاء

الخطوة 3: لصق الرابط في الراوتر

1. افتح WinBox وادخل إلى الراوتر، ثم اضغط **New Terminal**.
2. الصق السطر واضغط Enter. يُنشئ هذا السطر النفق، وحساب SAMM على الراوتر، وإعدادات RADIUS، وصفحة المشتركين المنتهية اشتراكاتهم، دفعة واحدة.
3. يتحوّل لون العميل في SAMM إلى الأخضر، ويظهر الراوتر في **الأجهزة** ثم **مدير الأجهزة**.

التحقق النهائي على الراوتر

يجب أن تستخدم خدمتا PPPoE و Hotspot نظام RADIUS. يتولّى SAMM ذلك تلقائياً، وللتحقق يدوياً:

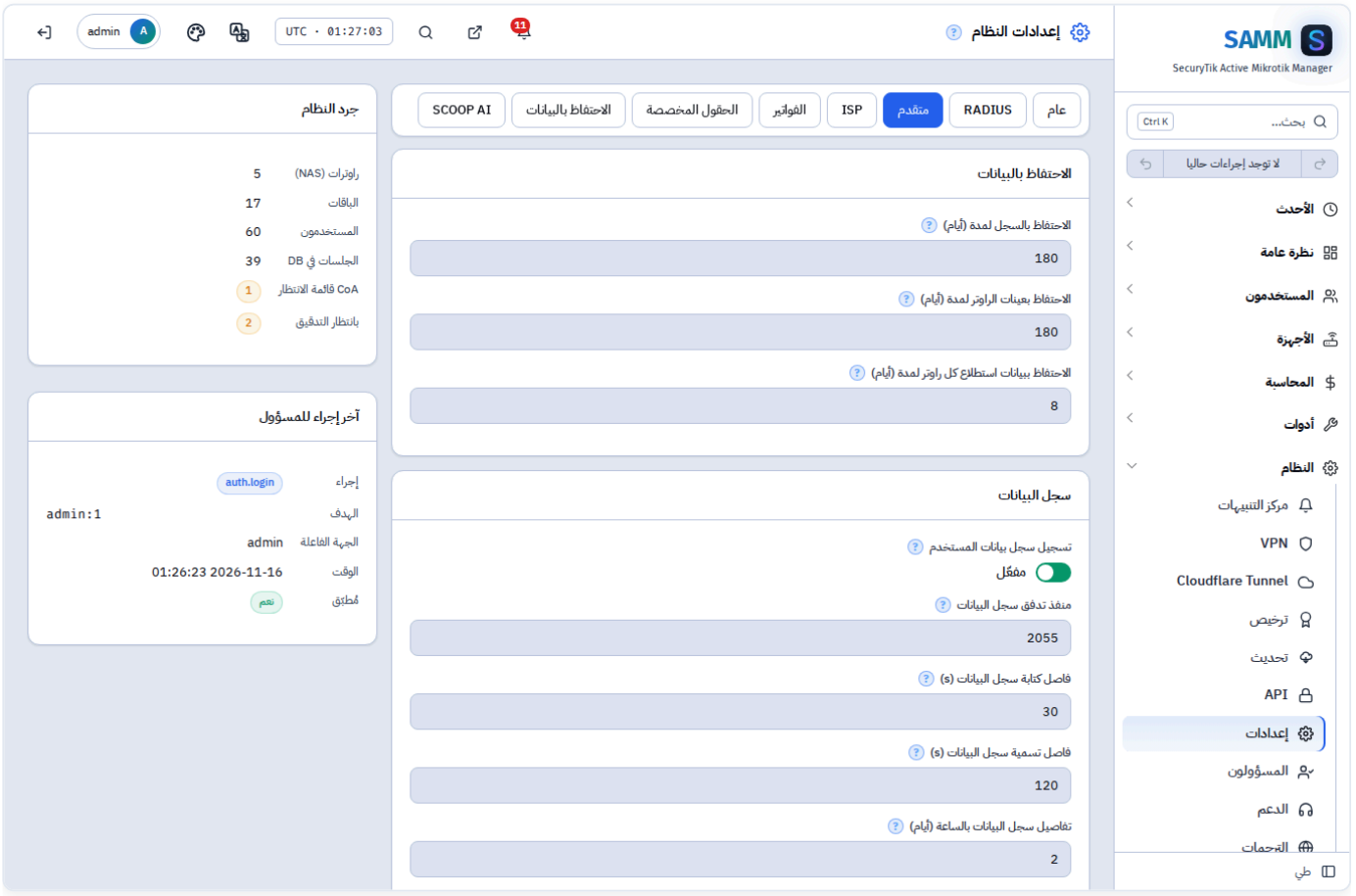
```
/radius print
/ppp aaa print
```

يجب أن يُظهر الأمر `/radius` عنوان SAMM مع الخدمة `ppp,hotspot`، وأن تظهر القيمة `use-radius:` `yes`.

الخطوة التالية: إنشاء الباقات من **المستخدمون** ثم **Plans**، وإضافة المشتركين من **المستخدمون** ثم **New customer**.

11. تفعيل الميزات الإضافية

بعض الميزات متوقفة في SAMM الجديد لأنها تستهلك مساحة تخزين أو تُجري تعديلات على الراوتر. فعّل ما تحتاجه منها. توجد معظم هذه الإعدادات في **النظام** ثم **إعدادات** ثم تبويب **متقدم**.



النظام ← إعدادات ← متقدم

Data Log (وجهات حركة كل مشترك)

1. افتح **النظام** ثم **إعدادات** ثم **متقدم** ثم قسم **سجل البيانات** (Data Log).
2. فعّل الخيار **تسجيل سجل بيانات المستخدم** (Record user Data Log).
3. حدّد عدد أيام الاحتفاظ بالتفاصيل الساعية ومدة الاحتفاظ، واترك بقية القيم على وضعها الافتراضي.
4. احفظ. بعد ذلك افتح صفحة أي مشترك واختر **سجل البيانات** (Data Log) لعرض أكثر المواقع والتطبيقات استخداماً (YouTube و Facebook و WhatsApp وغيرها) مع حجم الرفع والتنزيل.

> **معلومة مفيدة**
>
> يقرأ Data Log بيانات التدفق (Flow) من الراوتر نفسه، ولا يقع SAMM أبداً في مسار حركة البيانات. الأرقام تقريبية، أما الفوترة فتعتمد دائماً على محاسبة RADIUS. ويتطلب ذلك أن يكون الراوتر مُداراً من SAMM عبر API.

SAMM Fallback (استمرار دخول المشتركين عند توقف SAMM)

1. افتح **النظام** ثم **إعدادات** ثم **متقدم** ثم قسم **SAMM Fallback**.
2. فعّله لكل راوتر ترغب في حمايته.
3. حدّد مدة الانتظار (المدة التي يمكن أن يبقى فيها SAMM دون استجابة قبل أن يتولّى الراوتر المهمة).
4. احفظ. يحتفظ SAMM بنسخة معطّلة من كل مشترك نشط على ذلك الراوتر، فإذا توقّف SAMM عن الاستجابة، يتولّى الراوتر تسجيل دخول المشتركين بنفسه، وعند عودة SAMM يعود الجميع إلى الاتصال عبره.

يعرض جدول الحالة في الصفحة نفسها حالة المزامنة لكل راوتر، وأي مشترك تعذّرت مزامنته.

Network Health (سلامة الشبكة)

من **النظام** ثم **إعدادات** ثم **متقدم** ثم **Network Health**: يفحص الراوترات بحثاً عن الأخطاء الشائعة (خطوط احتياطية معطّلة، أو DNS مفتوح على الإنترنت، أو تداخل في Pools...) ويرسل التنبيهات. هذه الميزة مفعّلة في التنصيبات الجديدة، ويُنصح بإبقائها مفعّلة.

الاحتفاظ بالبيانات (السجلات القانونية)

من **النظام** ثم **إعدادات** ثم تبويب **الاحتفاظ بالبيانات** (Data retention): يحتفظ بسجلات الاتصال (سنتان افتراضياً)، ويوفّر صفحة **Lookup** لمعرفة المشترك الذي استخدم عنواناً معيّناً في وقت محدد. هذه الميزة متوقفة إلى أن تفعّلها.

النسخ الاحتياطي

من **أدوات** ثم **Backup**: أنشئ نسخة احتياطية و**نزّلها إلى حاسوبك** بشكل دوري (ودائماً قبل أي تحديث على MikroTik).

التحديثات

من **النظام** ثم **تحديث**: يتحقق SAMM يومياً من وجود إصدار جديد موقَّع. اختر **notify** (يظهر شريط مع زر **Apply now**، وهو الخيار الافتراضي) أو **auto** (يُطبَّق التحديث تلقائياً).

نشر لوحة التحكم على الإنترنت (Cloudflare Tunnel)

من **النظام** ثم **Cloudflare Tunnel**: الصق رمز Cloudflare Zero Trust لفتح SAMM من أي مكان عبر HTTPS دون فتح أي منافذ.

لكل مشترك: الرقابة الأبوية و VPN عبر SAMM

افتح صفحة المشترك ثم **Edit**: فعّل **Parental control** (تتمكن العائلات من حجب الفئات والتطبيقات من بوابة المشترك)، و/أو **VPN through SAMM** (تخرج حركة المشترك عبر سيرفر SAMM، ويتطلب ذلك نفق VPN عاملاً إلى الراوتر). ولتطبيق ذلك على عدة مشتركين دفعة واحدة: من قائمة المستخدمين حدّدهم ثم استخدم الإجراءات الجماعية.

12. المشكلات الشائعة وحلولها

المشكلة	الحل
Windows: خاصية Virtualization غير مفعّلة أو خطأ VT-x	راجع القسم 4.
Windows بنسخة Home	رقّ النسخة إلى Pro، أو استخدم Ubuntu أو سيرفراً جاهزاً.
ظهرت الرسالة already answers on the network	العنوان مستخدم من جهاز آخر. اختر عنواناً آخر غير مستخدم (القسم 2).
لوحة التحكم لا تفتح	نفّذ ping إلى عنوان SAMM، وتحقّق من الكابل. في Windows افتح SAMM Info وتحقّق من الحالة، وفي VPS تحقّق من Firewall (TCP 80/443).
يبقى الراوتر Offline في SAMM	هل خدمة API مفعّلة؟ (`/ip service print`). هل اسم المستخدم وكلمة المرور صحيحان؟ في الحالة (ب): هل خادم VPN مفعّل من النظام ثم VPN؟ وهل منافذه مفتوحة أو محوّلة (UDP 1701 / UDP 51820 و 500 و 4500 / TCP 443)؟
لا يستطيع المشتركون تسجيل الدخول	تحقّق بالأمر `/radius print`، وتأكّد من تطابق RADIUS secret في SAMM والراوتر تماماً. وتعرض صفحة Accept log في SAMM سبب الرفض.
ما زال الترخيص Unregistered	من النظام ثم ترخيص اضغط Link this device، ثم وافق على الرمز في samm.securytik.com.
حاسوب محمول عبر Wi-Fi: الراوتر لا يصل إلى SAMM	استخدم كابل شبكة؛ فكثير من بطاقات Wi-Fi لا تستطيع ربط Virtual Machine بالشبكة.

هل تحتاج إلى مساعدة؟

افتح SAMM ثم **النظام** ثم **الدعم**، أو راسلنا عبر samm.securytik.com.