

# لبقي يدل ESA نأ نم دكأت لآ يننكمي فيك نيذلا عالمعلآ نم طقف SSH اتالاصتإ SSH v2؟ نومدختسي

## المحتويات

### [المقدمة](#)

[كيف يمكنني التأكد من أن ESA لدي يقبل اتصالات SSH فقط من العملاء الذين يستخدمون SSH v2؟](#)  
[معلومات ذات صلة](#)

## المقدمة

يوضح هذا المستند كيفية مراجعة إصدارات مصادقة SSH وتكوينها على جهاز أمان البريد الإلكتروني (ESA) من Cisco.

## كيف يمكنني التأكد من أن ESA لدي يقبل اتصالات SSH فقط من العملاء الذين يستخدمون SSH v2؟

يمكن تكوين ESA للسماح باتصالات SSH (Secure Shell). تقوم اتصالات SSH بتشفير حركة مرور البيانات بين المضيف المتصل و ESA. يحمي هذا معلومات المصادقة مثل اسم المستخدم وكلمات المرور. هناك إصداران رئيسيان من بروتوكول SSH: الإصدار 1 (SSH v1) والإصدار 2 (SSH v2). فالإصدار SSH v2، نظرا لأنه أحدث، أكثر أمانا من الإصدار الأول من بروتوكول SSH، وبالتالي فإن العديد من مسؤولي ESA يفضلون السماح فقط بالاتصالات من العملاء الذين يستخدمون الإصدار الثاني من بروتوكول SSH.

في إصدارات نظام التشغيل AsyncOS من خلال 7.6.3، يمكن القيام بتعطيل اتصالات SSH v1 من واجهة سطر الأوامر مع `sshconfig`:

```
mail3.example.com> sshconfig
:Currently installed keys for admin
:Choose the operation you want to perform
.NEW - Add a new key -
.USER - Switch to a different user to edit -
.SETUP - Configure general settings -
setup <[]
.SSH v1 is currently ENABLED
:Choose the operation you want to perform
.DISABLE - Disable SSH v1 -
.DISABLE <[]
```

في إصدارات AsyncOS 8.x والإصدارات الأحدث، لا يوجد خيار تعطيل SSH v1 مع `sshconfig`. إذا تم تمكين SSH v1 قبل ترقيته x.8، فسيظل الإصدار SSH v1 ممكنا ويمكن الوصول إليه على ESA، حتى بعد اكتمال الترقيّة على الرغم من إزالة جميع دعم SSH v1. قد تكون هذه مشكلة للمسؤولين الذين يقومون بإجراء عمليات تدقيق أمنية منتظمة واختبار الاختراق.

بما أنه قد تمت إزالة جميع دعم SSH v1، فيجب فتح طلب دعم لتعطيل SSHv1.

قم بتشغيل الأمر التالي من مضيف Linux/Unix خارجي، أو أي اتصال CLI آخر قابل للتطبيق يختاره، لتأكيد تمكين SSH v1 أو تعطيله إلى ESA المعني:

```
robert@my_ubuntu:~$ ssh -1 admin@192.168.0.199
Protocol major versions differ: 1 vs. 2
```

الناتج المتوقع هو "تختلف الإصدارات الرئيسية للبروتوكول: 1 مقابل 2"، مما يشير إلى تعطيل SSH v1. إذا لم تكن هناك مساحة، وكان SSH v1 لا يزال ممكناً، فسوف ترى:

```
robert@my_ubuntu:~$ ssh -1 admin@192.168.0.199
:Password
:Response
Last login: Thu Oct 30 14:53:40 2014 from 192.168.0.3
.Copyright (c) 2001-2013, Cisco Systems, Inc
```

```
AsyncOS 8.0.1 for Cisco IronPort C360 build 023
```

```
Welcome to the Cisco IronPort C360 Messaging Gateway(tm) Appliance
<myesa.local
```

سيشير هذا الناتج إلى أن SSH v1 لا يزال قيد الاستخدام ويمكن أن يتسبب في انعدام الأمان مع ESA بعد ترقية إلى x.8 أو أحدث. ويمكن لفت الانتباه إلى ذلك باختبار اختراق أو مراجعة أمنية، وتحديد ثغرة كبيرة. لإجراء تصحيح، سيتعين عليك [فتح حالة دعم](#) وطلب تصحيح هذا الأمر. ستحتاج إلى أن تكون قادراً على توفير نفق دعم من ESA لدعم Cisco الغني.

## معلومات ذات صلة

- [CSCuo46017: يظل SSHv1 ممكناً بعد الترقية ولا يمكن تعطيله](#)
- [جهاز أمان البريد الإلكتروني من Cisco - أدلة المستخدم النهائي](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت  
م ل ا ل ا ا ن ا ع مچ م ف ن م دخت س م ل م عد و ت م م م دقت ل ة م ش ب ل و  
م ك ة ق م ق د ن و ك ت ن ل ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م م چ ر م . ة ص ا خ ل م ه ت غ ل ب  
Cisco مچرت م ا م د ق م م ا ل ة م ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه  
ل ا م ا د ا د ع و چ ر ل ا ب م ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت م ل و ئ م س م  
Systems (ر ف و ت م ط ب ا ر ل ا) م ل ص ا ل ا م ل م چ ن ل ا دن ت س م ل ا