



Supported Devices and Software Versions for Cisco Security Manager 3.3

Revised: October 12, 2010

Cisco Security Manager 3.3 supports the devices and operating system versions listed in these sections:

- [Supported Devices](#)
- [Supported Software](#)
- [Software Supported in Downward Compatibility Mode](#)

Supported Devices

The following table lists the devices you can manage in Cisco Security Manager 3.3.

Table 1 *Cisco Security Manager 3.3 Supported Devices*

Series	Supported Device Models
Routers, Switches	
Cisco SOHO 70 Series Router	<ul style="list-style-type: none">• 71• 76 ADSL• 77 ADSL• 77 H ADSL• 78 G.SHDSL
Cisco SOHO 90 Series Secure Broadband Routers	<ul style="list-style-type: none">• 91• 96• 97



Table 1 Cisco Security Manager 3.3 Supported Devices (continued)

Series	Supported Device Models
Cisco 800 Series Routers	<ul style="list-style-type: none"> • 801 • 803 • 805 • 811 • 813 • 828 • 831 • 836 • 837 • 851 • 857 • 861, 861W • 871 • 876 • 877 • 878 • 881, 881B, 881G, 881F, 881SRST • 887 • 888, 888G, 888F, 888SRST • 891 • 892
Cisco ASR 1000 Series Aggregation Services Routers Note Support is limited to the following Cisco IOS XE Software consolidated packages: Advanced IP Services, Advanced Enterprise Services. The IP Base packages are not supported.	<ul style="list-style-type: none"> • 1002 • 1004 • 1006
Cisco 1600 Series Routers	<ul style="list-style-type: none"> • 1601 • 1602 • 1603 • 1604 • 1605

Table 1 Cisco Security Manager 3.3 Supported Devices (continued)

Series	Supported Device Models
Cisco 1700 Series Modular Access Routers	<ul style="list-style-type: none"> • 1701 • 1710 • 1711 • 1712 • 1720 • 1721 • 1750 • 1751 • 1760
Cisco 1800 Series Routers	<ul style="list-style-type: none"> • 1801 • 1802 • 1803 • 1805 • 1811 • 1812 • 1841 • 1861
Cisco 2600 Series Multiservice Platforms	<ul style="list-style-type: none"> • 2610 • 2610XM • 2611 • 2611XM • 2612 • 2613 • 2620 • 2620XM • 2621 • 2621XM • 2650 • 2650XM • 2651 • 2651XM • 2691

Table 1 Cisco Security Manager 3.3 Supported Devices (continued)

Series	Supported Device Models
Cisco 2800 Series Integrated Services Routers	<ul style="list-style-type: none"> • 2801 • 2811 • 2821 • 2851
Cisco 3200 Series Mobile Access Routers	<ul style="list-style-type: none"> • 3251 • 3270
Cisco 3600 Series Multiservice Platforms	<ul style="list-style-type: none"> • 3620 • 3631 • 3640 • 3660 • 3661 • 3662
Cisco 3700 Series Multiservice Access Routers	<ul style="list-style-type: none"> • 3725 • 3745
Cisco 3800 Series Integrated Services Routers	<ul style="list-style-type: none"> • 3825 • 3845
Cisco 7100 Series VPN Routers	<ul style="list-style-type: none"> • 7120 • 7140 • 7160
Cisco 7200 Series Routers	<ul style="list-style-type: none"> • 7201 • 7202 • 7204 • 7204VXR • 7206 • 7206VXR • VPN Services Adapter (VSA)
Cisco 7300 Series Routers	<ul style="list-style-type: none"> • 7301 • 7304
Cisco 7500 Series Routers	<ul style="list-style-type: none"> • 7505 • 7506 • 7507 • 7513 • 7576

Table 1 Cisco Security Manager 3.3 Supported Devices (continued)

Series	Supported Device Models
Cisco 7600 Series Routers	<ul style="list-style-type: none"> • 7603 • 7604 • 7606 • 7609 • 7613
Cisco Catalyst 3550 Series Switches	<ul style="list-style-type: none"> • 3550 12G • 3550 12T • 3550 24 DC SMI • 3550 24 FX SMI • 3550 24 PWR • 3550 24 • 3550 48
Cisco Catalyst 3560 Series Switches	<ul style="list-style-type: none"> • 3560-24PS • 3560-24TS • 3560-48PS • 3560-48TS • 3560-8PC • 3560G-24PS • 3560G-24TS • 3560G-48PS • 3560G-48TS
Cisco Catalyst 3560-E Series Switches	<ul style="list-style-type: none"> • 3560E-12D-S • 3560E-12SD-E • 3560E-24PD-E • 3560E-24TD-E • 3560E-48PD-E • 3560E-48TD-E
Cisco Catalyst 3750 Metro Series Switches	<ul style="list-style-type: none"> • 3750 Metro 24-DC

Table 1 Cisco Security Manager 3.3 Supported Devices (continued)

Series	Supported Device Models
Cisco Catalyst 3750 Series Switches	<ul style="list-style-type: none"> • 3750 Stack • 3750-24FS • 3750-24PS • 3750-24TS • 3750-48PS • 3750G-12S • 3750G-12S-SD • 3750G-16TD • 3750G-24 • 3750G-24PS • 3750G-24T • 3750G-24TS-1U • 3750G-24WS • 3750G-48 • 3750G-48PS • 3750G-48TS
Cisco Catalyst 3750-E Series Switches	<ul style="list-style-type: none"> • 3750E-24PD-E • 3750E-24TD-E • 3750E-48PD-E • 3750E-48TD-E
Cisco Catalyst 4500 Series Switches	<ul style="list-style-type: none"> • 4503 • 4503-E • 4506 • 4506-E • 4507R • 4507R-E • 4510R • 4510R-E
Cisco Catalyst 4900 Series Switches	<ul style="list-style-type: none"> • 4900M • 4948 • 4948-10 GE

Table 1 Cisco Security Manager 3.3 Supported Devices (continued)

Series	Supported Device Models
Cisco Catalyst 6500 Series Switches	<ul style="list-style-type: none"> • 6503 • 6503-E • 6504-E • 6506 • 6506-E • 6509 • 6509-E • 6509-NEB • 6509-NEB-A • 6509-V-E • 6513
Cisco 7600/Catalyst 6500 IPSec VPN Services Module (VPNSM) ¹	
Cisco 7600 Series/Catalyst 6500 Series IPSec VPN Shared Port Adapter (VPN SPA) ¹	
Cisco Catalyst 6500 Series VPN Services Port Adapter (VSPA) ¹	
Adaptive Security Appliances and Firewalls	
Cisco PIX 500 Series Firewalls	<ul style="list-style-type: none"> • 501 • 506 • 506E • 515 • 515E • 520 • 525 • 535
Cisco ASA-5500 Series Adaptive Security Appliance	<ul style="list-style-type: none"> • 5505 • 5510 • 5520 • 5540 • 5550 • 5580-20 • 5580-40
Cisco Catalyst 6500 Series Firewall Services Module (FWSM) ¹	

Table 1 Cisco Security Manager 3.3 Supported Devices (continued)

Series	Supported Device Models
IPS Sensors	
Cisco IPS 4200 Series Sensors	<ul style="list-style-type: none"> • 4210 • 4215 • 4235 • 4240 • 4250 TX • 4250 SX • 4250 XL • 4255 • 4260 • 4270
Cisco ASA 5500 Series Advanced Inspection and Prevention (AIP) Security Services Module	<ul style="list-style-type: none"> • 10 (AIP-SSM-10) • 20 (AIP-SSM-20) • 40 (AIP-SSM-40)
Cisco ASA Advanced Inspection and Prevention Security Services Card (SSC)	<ul style="list-style-type: none"> • 5 (SSC-5)
Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Services Module ¹	
Cisco IDS Network Module (NM-CIDS)	
Cisco Intrusion Prevention System Advanced Integration Module (AIM) for Cisco 1841, 2800, and 3800 Series Integrated Services Routers	
Cisco Intrusion Prevention System Network Module Enhanced (NME) for Cisco 2811, 2821, 2851, 3800 Series Integrated Services Routers	
Routers running IOS IPS feature	<ul style="list-style-type: none"> • 85x • 86x • 87x • 88x • 89x • 18xx • 26xx • 28xx • 37xx • 38xx • 72xx • 7301

1. Cisco Security Manager Professional Edition is required to manage this services module.

Supported Software

You can use the following software applications with Security Manager 3.3:

- Cisco Secure ACS (Windows) 4.1(3, 4) and 4.2(0) and Cisco Secure ACS Solution Engine 4.1(4) for AAA functions.
- Cisco Configuration Engine 3.0 for managing configuration updates. You cannot use older releases of this product.

Security Manager supports the software on the devices that it manages as described in the following sections:

- [Cisco IOS Software Supported Versions, page 9](#)
- [Other Supported Software, page 11](#)

Cisco IOS Software Supported Versions

The following list describes the minimum supported Cisco IOS Software versions plus the specific release numbers that have additional support in Security Manager for standard routers. You must use a software version that meets at least the minimum. If you use a version that is not listed, Security Manager will treat it as one of these versions (the most closely-matching version, which is typically the release number nearest to it but lower). Any features that are unique to the version you are using are not supported in Security Manager.

- 12.4T—Other versions include 12.4(2)T, 12.4(4)T, 12.4(6)T, 12.4(8)T, 12.4(9)T, 12.4(11)T, 12.4(11)T1, 12.4(11)T2, 12.4(15)T, 12.4(20)T, 12.4(22)T.
- 12.4—Other versions include 12.4(1), 12.4(1a), 12.4(3).
- 12.3(2)T—Other versions include 12.3(2)T1-9, 12.3(4)T, 12.3(4)T1-11, 12.3(7)T, 12.3(7)T1-7, 12.3(8)T, 12.3(8)T1-7, 12.3(11)T, 12.3(11)T1-3, 12.3(13)T, 12.3(14)T, 12.3(14)T2.
- 12.3—Other versions include:
 - 12.3(1), including 12.3(1a)B.
 - 12.3(2), including the XA3, XB3, XC2, XE2, and XF versions.
 - 12.3(3), including the B and B1 versions.
 - 12.3(4), including the XD4, XG3, XK2, and XQ1 versions.
 - 12.3(5), including the 12.3(5a)B, 12.3(5a)B0a, and 12.3(5a)B1-4 versions.
 - 12.3(6).
 - 12.3(7), including the XI6, XR, XR2, XR4, XJ2, and XS2 versions.
 - 12.3(8), including the XU4, XW3, XX1, YA1, YD1, YG2, YH, YI, and YI1 versions.
 - 12.3(9), including the 12.3(9a)BC, BC1, and BC2 versions.
 - 12.3(10).
 - 12.3(11), including the XL1, YK1, and YS versions.
 - 12.3(12).
 - 12.3(13).

- 12.2. Specific support is also available for the following versions:
 - 12.2(8)T and ZB8.
 - 12.2(11)YU, YX, YZ, and YZ2.
 - 12.2(13)T, T12, ZD2, and ZE.
 - 12.2(14)S, SU, SU2, SX, SY, and SZ.
 - 12.2(15)BX, JK, and ZJ.
 - 12.2(17b)SXA.
 - 12.2(17d)SXB.
 - 12.2(18)SE, SW, SXD, SXE, and SXF.
 - 12.2(20)EW, EWA, EX, and S8.
 - 12.2(23)SW1.
 - 12.2(25)EY, EZ, FX, FY, JA, SEA, SEB, SEC, SED, SEE, and SG.
 - 12.2(27)SBC
- 12.1—Other versions include 12.1(4)E3 and 12.1(5)T9.

Cisco routers and switches have these software restrictions:

- For routers running Release 12.1 and 12.2, there is limited support for Layer 3 access rules, interfaces, and FlexConfigs, but not for any other features.
- The Cisco ASR 1000 Series Aggregation Services Routers software releases use a different numbering scheme, but these releases are mapped to more standard IOS release numbers in Security Manager. The following are the supported releases and their Cisco IOS software equivalent releases:
 - Version 2.1.x—Called 12.2(33)XNA in Security Manager.
 - Version 2.2.x—Called 12.2(33)XNB in Security Manager.
 - Version 2.3.x—Called 12.2(33)XNC in Security Manager. Security Manager treats this release as equivalent to 12.2(33)XNB except for the addition of GET VPN support.



Note Although the ASR releases are mapped to IOS 12.2 releases, you must select IOS 12.3+ as the operating system type when adding the device to the Security Manager inventory.

- For the Catalyst 6500/7600, you can use Cisco IOS Software Release 12.1, 12.2 and these versions at the specified point release and later: 12.1(13)E, 12.1(17B)SXA, 12.1(19)E, 12.1(20)E, 12.1(22)E, 12.1(23)E, 12.1(26)E, 12.2(14)SX, 12.2(14)SY, 12.2(17a)SX, 12.2(17d)SXB, 12.2(18)SXD, 12.2(18)SXE, 12.2(18)SXE1, 12.2(18)SXE2, 12.2(18)SXE4, 12.2(18)SXF2, 12.2(18)SXF4, 12.2(33)SRA, 12.2(33)SRB, 12.2(33)SXH, and 12.2(33)SXI.



Note You cannot use the Catalyst Operating System on a device managed by Security Manager.

- For the Catalyst 3500/4500, you can use Cisco IOS Software Release 12.1 and 12.2 and the following versions at the specified point release and later. Note that specific devices support a subset of the listed versions:
 - 12.2(37)SE, SG
 - 12.2(31)SGA
 - 12.2(25)EWA, FZ, EZ, EY, SE, EW, SEA, SEB, SEC, SED, SEE, SEG

- 12.2(20)EU
- 12.1(26)E
- 12.1(20)EW, EU, E
- 12.1(19)EA1, EA1d
- 12.1(14)AX
- 12.1(11)AX
- To configure and manage VPNs on Catalyst 6500/7600 devices, the earliest software release is Cisco IOS Software Release 12.2(17b)SXA.
- To configure and manage IDSM settings on Catalyst 6500/7600 devices, the earliest software release is Cisco IOS Software Release 12.2(18)SXF4.
- For routers running an IPS-enabled version of Cisco IOS Software, the earliest supported Cisco IOS Software release is 12.4(11)T2.

Other Supported Software

The following list describes the minimum supported software versions plus the specific release numbers that have additional support in Security Manager for devices that run operating system other than Cisco IOS Software. You must use a software version that meets at least the minimum. If you use a version that is not listed, Security Manager will treat it as one of these versions (the most closely-matching version, which is typically the release number nearest to it but lower). Any features that are unique to the version you are using are not supported in Security Manager.

- Cisco PIX 500 Series Firewalls—PIX Firewall Software Release 6.3(1-5), 7.0(1, 2, 4-8), 7.1(1-2), 7.2(1-3), 8.0(2-3), and 8.1(1-2).
- Cisco ASA-5500 Series Adaptive Security Appliances (ASA)—ASA Software Release 7.0(1, 2, 4-8), 7.1(1-2), 7.2(1-4), 8.0(2-3), 8.1(1-2), and 8.2(1), with the following exceptions:
 - Do not use this version of Security Manager to manage ASA 8.3 devices. This version of Security Manager configures ASA 8.3 devices in downward-compatibility mode, meaning that the device configuration does not use the new features introduced in version 8.3. Because of the extensive changes introduced with version 8.3, it is not downwardly-compatible with older ASA releases. If you want to manage ASA 8.3 devices with Security Manager, you must upgrade to Security Manager 4.0.
 - You cannot use Security Manager to manage SSL VPNs on ASA 7.x. ASA Software Release 7.2(4) is supported only on the ASA 5505 platform.
- Cisco Catalyst 6500 Series Firewall Services Module (FWSM)—FWSM Software Release 2.2, 2.2(1), 2.3(1-4), 3.1(1, 3-9), 3.2(1-4), and 4.0(1).
- IPS sensors and modules—IPS Software 5.1, 6.0, 6.1, 6.2, and 7.0, with these restrictions:
 - IPS signature updates are supported only on IPS Software 5.1(5)E1 and later.
 - You cannot configure any IPv6 features that are available with version 6.2 and higher. If you configure IPv6 features directly on the device, Security Manager does not disturb your configuration. Consider using Security Manager's FlexConfig feature to manage IPv6 configurations.

Software Supported in Downward Compatibility Mode

Security Manager directly supports many individual point releases for the various operating systems you can use with the supported devices. When Security Manager supports a specific point release, it means that you can configure some features new to that release using the product.

Some point releases are supported in “downward compatibility mode.” In this mode, you can use the product to configure devices running that point release, but you cannot configure features that are new in the release unless you use FlexConfigs. Thus, the point release is treated as being the same as the nearest point release to it, and Security Manager maps the release number to that supported release.

Table 2 lists the releases that are specifically supported in Security Manager, and the point releases that are supported as downward equivalents to the release. The table might not include information about every downward compatible release. In general, if a version is not listed here or in [Supported Software, page 9](#), Security Manager will treat it as one of the supported versions (the most closely-matching version, which is typically the release number nearest to it but lower).

Table 2 Software Releases Supported in Downward Compatibility Mode

Releases Supported in Downward Compatibility Mode	Supported As These Releases
ASA Software Releases	
8.0(4-5)	8.0(3)
FWSM Software Releases	
4.1(1-2)	4.0(1)
4.0(2-11)	4.0(1)
3.2(5-17)	3.2(4)
3.1(10-18)	3.1(9)
Cisco IOS Software Releases	
12.4(24)T, 12.4(22)T1, 12.4(22)YB, 12.4(22)YB1	12.4(22)T
12.4(20)T1-3	12.4(20)T
12.4(15)T1, 3-9	12.4(15)T
Cisco IOS Software Releases for Cisco ASR 1000 Series Aggregation Services Routers	
2.1.x releases: 12.2(33)XNA1, 12.2(33)XNA2	12.2(33)XNA
2.2.x releases: 12.2(33)XNB1-3	12.2(33)XNB
2.3.x releases: 12.2(33)XNC1	12.2(33)XNC
Cisco IOS Software Releases for Catalyst switches and 7600 series routers	
12.2(33)SXI1	12.2(33)SXI