Supported Devices and Software Versions for Cisco Security Manager 4.11

First Published: April 1, 2016

Cisco Security Manager and its related applications support the devices and operating system versions listed in these sections:

General Device to Feature Support for Security Manager

Broadly speaking, Security Manager has these main features: device configuration, event management, report management, health and performance monitor, and image management. Table 1 explains which classes of device are supported for each feature. The exact models and software versions supported in each device class are listed in subsequent sections.

Cisco Systems, Inc.
www.cisco.com

Table 1 Features Supported By Device Class in Security Manager

Device Class	Device Configuration	Event Management	Report Management	Health and Performance Monitor	Image Manager
Adaptive Security Appliance (ASA), including the Cisco Adaptive Security Virtual Appliance (ASAv) and service modules	Yes	Yes (ASA 8.0+ only)	Yes (ASA 8.0+ only)	Yes	• ASAs—Yes • Cisco Catalyst 6500 Series ASA Services Modules—Yes • ASA-SM on 7600 Series Routers—Yes • Other ASA service modules—No
Intrusion Prevention System (IPS) appliances and service modules[1]	Yes[1]	Yes (IPS 6.1+ only)	Yes (IPS 6.1+ only)	Yes	No[1]
Firewall Services Modules (FWSM)	Yes	Yes (FWSM 3.1.17+, 3.2.17+, 4.0.10+, and 4.1.1+ only)	No	No	No
PIX Firewalls	Yes	No	No	No	No
Cisco IOS routers	Yes	No	No	No	No
Cisco IOS IPS in supported routers	Yes	No	No	No	No
Catalyst switches	Yes	No	No	No	No

1. Signature and sensor image update is already available in Configuration Manager, although it is not available in Image Manager.

IPv6 Support Summarized by Device Class and Application

Security Manager provides some support for IPv6, but only for configuring policies on a device (for example, firewall rules and IPS rules). Support is for traffic through the device; it is not for communication from Security Manager to the device.

Table 2 summarizes IPv6 support by device class in each Security Manager application (for example, Configuration Manager).

If a particular device class has no policies that use IPv6 (for example, Cisco IOS IPS in supported routers), then the table lists “Not applicable.” The table also lists “Not applicable” for devices that are not supported at all by a particular application (for example, Image Manager supports only ASAs and ASAv’s).

For the specific policies that you can configure, see the Getting Started chapter in the *User Guide for Cisco Security Manager*.

Table 2 IPv6 Support By Device Class in Each Security Manager Application

Device Class	Configuration Manager	Event Viewer	Report Manager	Health and Performance Monitor	Image Manager
Adaptive Security Appliance (ASA), including the Cisco Adaptive Security Virtual Appliance (ASAv) and service modules (Single or multiple security context configurations)	Yes (ASA 7.0+ in router mode; 8.2+ transparent mode)	Yes (ASA 8.0+ only)	Yes (ASA 8.0+ only)	Yes	No
Intrusion Prevention System (IPS) appliances and service modules	Yes	Yes (IPS 6.1+ only)	Yes (IPS 6.1+ only)	Yes	Not applicable
Firewall Services Modules (FWSM) (Single or multiple security context configurations)	Yes (FWSM 3.1+ router mode; not supported in transparent mode)	Yes (FWSM 3.1.17+, 3.2.17+, 4.0.10+, and 4.1.1+ only)	No	No	Not applicable
PIX Firewalls	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Cisco IOS routers	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Cisco IOS IPS on supported routers	No applicable	No applicable	No applicable	No applicable	Not applicable
Catalyst switches	No applicable	No applicable	No applicable	No applicable	Not applicable

Explicitly Supported Devices for Security Manager

The following table lists the devices you can manage in Cisco Security Manager. These specific models are explicitly supported, that is, Security Manager is aware of the features available on the device and recognizes the device module.

Tip If a device model is not listed in this table, you might still be able to manage it as a generic device type. For more information, see Generically Supported Devices for Security Manager.

Table 3 Cisco Security Manager Supported Devices

Series	Supported Device Models
Adaptive Security Appliances and Firewalls	
Cisco Firepower 4000 Series [support for ASA Version 9.6.1 and above]	• FPR4K-SM-12, FPR4K- SM24, FPR4K- SM-36
Cisco Firepower 9000 Series [support for ASA Version 9.5.2 and above]	• FPR9K-SM-24, FPR9K-SM-36

Table 3 Cisco Security Manager Supported Devices (continued)

Series	Supported Device Models
ISA 3000 [support for ASA Version 9.4.1, 9.5.1, 9.5.2 and 9.6.1]	• ISA 3000 4C, ISA 3000 2C2F
Cisco 1783 Industrial Security Appliance [support for ASA Version 9.5.2 and above]	• 1783-SAD2T2S • 1783-SAD4T0S
Cisco ASA-5500 Series Adaptive Security Appliance [support for ASA Version 9.4.1, 9.5.1, 9.5.2 and 9.6.1]	• 5506Wireless • Ruggedized 5506 • 5508 • 5516
Cisco ASA-5500 Series Adaptive Security Appliance [support for ASA Version 9.4.1 and above]	• 5506W-X • 5516-X (Rackmount) • 5508-X (Rackmount) • 5506H-X
Cisco ASA-5500 Series Adaptive Security Appliance [support for ASA Version 9.2 and earlier]	• 5505
Cisco ASA-5500 Series Adaptive Security Appliance [support for ASA Version 9.3(2) and later]	• 5506-X
Cisco ASA-5500 Series Adaptive Security Appliance [support for ASA Version 9.1 and earlier]	• 5510 • 5520 • 5540 • 5550 • 5580-20, -40
Cisco ASA-5500 Series Adaptive Security Appliance [support for ASA versions 8.6(1), 9.0(1), and later]	• 5512-X • 5515-X • 5525-X • 5545-X • 5555-X
Cisco ASA-5500 Series Adaptive Security Appliance [support for ASA versions 8.2(3), 8.4(1-6), 9.0(1), and later]	• 5585-X with SSP-10, SSP-20, SSP-40, and SSP-60
Cisco Adaptive Security Virtual Appliance (ASAv) [support for ASA version 9.2(1) and later]	
Cisco Catalyst 6500 Series ASA Services Module	
ASA-SM on 7600 Series Routers **Note** You must select Cisco Catalyst 6500 Series ASA Services Module as the device type to manage the ASA Services Module on a 7600 Series Router.	
Cisco Catalyst 6500 Series Firewall Services Module (FWSM)[1]	

Table 3 Cisco Security Manager Supported Devices (continued)

Series	Supported Device Models
Cisco PIX 500 Series Firewalls	• 501 • 506 • 506E • 515 • 515E • 520 • 525 • 535
IPS Sensors	
Cisco IPS 4200 Series Sensors [IPS version 7.1 and earlier]	• 4210 • 4215 • 4235 • 4240 • 4250 SX • 4250 XL • 4255 • 4260 • 4270
Cisco IPS 4300 Series Sensors [IPS Version 7.1(4) onwards]	• 4345 • 4360
Cisco IPS 4500 Series Sensors [IPS version 7.1(6) onwards]	• 4510 • 4520
Cisco ASA 5500 Series IPS Security Services Processor [IPS Version 7.1(4) onwards]	• 5512-X • 5515-X • 5525-X • 5545-X • 5555-X
Cisco ASA 5585 Series IPS Security Services Processor [IPS Version 7.1(1) onwards]	• IPS SSP-10 • IPS SSP-20 • IPS SSP-40 • IPS SSP-60
Cisco ASA 5500 Series Advanced Inspection and Prevention (AIP) Security Services Module	• 10 (AIP-SSM-10) • 20 (AIP-SSM-20) • 40 (AIP-SSM-40)
Cisco ASA Advanced Inspection and Prevention Security Services Card (SSC)	• 5 (SSC-5)

Table 3 Cisco Security Manager Supported Devices (continued)

Series	Supported Device Models
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 Cisco1841, 2800, and 3800 Series Integrated Services Routers	
Cisco Intrusion Prevention System Network Module Enhanced (NME)	
Routers running the IOS IPS feature	• 85x, 86x, 87x, 88x, 89x • 18xx • 19xx • 26xx • 28xx • 29xx • 37xx • 38xx • 39xx • 72xx • 7301
Routers, Switches	
Cisco SOHO 70 Series Router	• 71 • 76 ADSL • 77 ADSL • 77 H ADSL • 78 G.SHDSL
Cisco SOHO 90 Series Secure Broadband Routers	• 91 • 96 • 97

Table 3 Cisco Security Manager Supported Devices (continued)

Series	Supported Device Models
Cisco 800 Series Routers	• 801 • 803 • 805 • 811 • 813 • 828 • 831 • 836 • 837 • 851 • 857 • 861, 861W • 866 • 867 • 871 • 876 • 877 • 878 • 881, 881SRST, 881SRSTW, 881W • 886, 886SRST, 886SRSTW, 886W • 887, 887SRST, 887SRSTW, 887Vdsl2, 887W • 888, 888SRST, 888SRSTW, 888W • 891 • 892
Cisco IAD880 Series Integrated Access Devices	• IAD 881(B, F), IAD 881W • IAD 886(B, F), IAD 886W • IAD 887(B, F), IAD 887W • IAD 888(B, F), IAD 888W

Table 3 Cisco Security Manager Supported Devices (continued)

Series	Supported Device Models
Cisco ASR 1000 Series Aggregation Services Routers Support includes all Ethernet (all speeds), Serial, ATM, and Packet over Sonet (POS) shared port adapters (SPA), but not services SPAs. **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.	• 1002 Fixed Router • 1002 • 1004 • 1006
Cisco 1600 Series Routers	• 1601 • 1602 • 1603 • 1604 • 1605
Cisco 1700 Series Modular Access Routers	• 1701 • 1710 • 1711 • 1712 • 1720 • 1721 • 1750 • 1751 • 1760
Cisco 1800 Series Routers	• 1801 • 1802 • 1803 • 1805 • 1811 • 1812 • 1841 • 1861
Cisco 1900 Series Integrated Services Routers	• 1905 • 1921 • 1941 • 1941W

Table 3 Cisco Security Manager Supported Devices (continued)

Series	Supported Device Models
Cisco 2600 Series Multiservice Platforms	• 2610, 2610XM • 2611, 2611XM • 2612 • 2613 • 2620, 2620XM • 2621, 2621XM • 2650, 2650XM • 2651, 2651XM • 2691
Cisco 2800 Series Integrated Services Routers	• 2801 • 2811 • 2821 • 2851
Cisco 2900 Series Integrated Services Routers	• 2901 • 2911 • 2921 • 2951
Cisco 3200 Series Mobile Access Routers	• 3251 • 3270
Cisco 3600 Series Multiservice Platforms	• 3620 • 3631 • 3640 • 3660 • 3661 • 3662
Cisco 3700 Series Multiservice Access Routers	• 3725 • 3745
Cisco 3800 Series Integrated Services Routers	• 3825 • 3825 NOVPN • 3845 • 3845 NOVPN
Cisco 3900 Series Integrated Services Routers	• 3925 • 3925E • 3945 • 3945E

Table 3 Cisco Security Manager Supported Devices (continued)

Series	Supported Device Models
Cisco 7100 Series VPN Routers	• 7120 • 7140 • 7160
Cisco 7200 Series Routers	• 7201 • 7202 • 7204 • 7204VXR • 7206 • 7206VXR • VPN Services Adapter (VSA)
Cisco 7300 Series Routers	• 7301 • 7304
Cisco 7500 Series Routers	• 7505 • 7506 • 7507 • 7513 • 7576
Cisco 7600 Series Routers	• 7603 • 7604 • 7606 • 7606-S • 7609 • 7609S • 7613
Cisco Catalyst 3550 Series Switches	• 3550 12G • 3550 12T • 3550 24 DC SMI • 3550 24 FX SMI • 3550 24 PWR • 3550 24 • 3550 48

Table 3 Cisco Security Manager Supported Devices (continued)

Series	Supported Device Models
Cisco Catalyst 3560 Series Switches	• 3560-24PS • 3560-24TS • 3560-48PS • 3560-48TS • 3560-8PC • 3560G-24PS • 3560G-24TS • 3560G-48PS • 3560G-48TS
Cisco Catalyst 3560-E Series Switches	• 3560E-12D-S • 3560E-12SD-E • 3560E-24PD-E • 3560E-24TD-E • 3560E-48PD-E • 3560E-48TD-E
Cisco Catalyst 3750 Metro Series Switches	• 3750 Metro 24-DC
Cisco Catalyst 3750 Series Switches	• 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

Table 3 Cisco Security Manager Supported Devices (continued)

Series	Supported Device Models
Cisco Catalyst 3750-E Series Switches	• 3750E-24PD-E • 3750E-24TD-E • 3750E-48PD-E • 3750E-48TD-E
Cisco Catalyst 4500 Series Switches	• 4503 • 4503-E • 4506 • 4506-E • 4507R • 4507R-E • 4510R • 4510R-E
Cisco Catalyst 4900 Series Switches	• 4900M • 4948 • 4948E • 4948-10 GE
Cisco Catalyst 6500 Series Switches **Note** The virtual switching system (VSS) mode is not supported.	• 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]	

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

Generically Supported Devices for Security Manager

Security Manager can manage some device models even if the model does not appear in the supported device list. This type of generic device support relies on the fact that device features are controlled more by the software running on the device than the device model.

If you have a device that does not appear in the explicitly supported device list, you can try to manage it as a generic device using the device modules listed in the following table.

Tips

- This type of generic support works best for new models of series that are already explicitly supported. For example, a new model in the ASR 1000 series, or in the ISR 88x or 89x series. Generic support does not work with carrier-class routers (the CRS) or for Catalyst switches.
- Because this support is generic, Security Manager cannot determine if a particular feature is not available on the specific model you are managing. You are responsible for determining if a feature that you are allowed to configure in Security Manager is not supported on the device. If you configure an unsupported feature, you will see errors when you deploy the configuration to the device.
- If the device contains an explicitly supported module, such as an AIM-IPS module, the module is also supported. However, the module's model must be explicitly supported: there is no generic module support.
- If a particular ASR is not listed as being explicitly supported in Table 3 on page 3, but a previous version is, that particular ASR is supported generically in Security Manager with "Generic Router Backward Compatibility Support."

Table 4 Cisco Security Manager Generically Supported Devices

Generic Device Type	When To Use
Cisco Generic Aggregation Services Router	For devices running Cisco IOS XE Software.
Cisco Generic Integration Services Router	For devices running Cisco IOS Software.

The following table lists the device models that have been tested for generic support:

Table 5 Device Models Tested for Generic Support

Series	Tested Device Models
Cisco 800 Series Routers	• 812-G, 812-S, 812-V, 812-B, 812-CT, 812+R7 • 819-G, 819-S, 819-V, 819-B, 819-CT, 819+R7 • 866VA, 866VAE • 867VA, 867VAE • 881G, 881G+7 • 886G, 886VA, 886VA-W, 886VAG+7 • 887G, 887M, 887MVA-W, 887VA, 887VA-M, 887VA-W, 887VAG-S, 887VAG+7, 887VAMG+7 • 888E, 888G, 888EG+7 • 891W • 892W • 893FG
Cisco ASR 1000 Series Aggregation Services Routers	1001
Cisco 4400 Series Integrated Services Routers	4451, 4452
Cisco 5940 Series Embedded Services Router	5940

Supported Software for Security Manager

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

- ASA, FWSM, PIX, and IPS Supported Software Versions, page 14
- Cisco IOS Software Supported Versions, page 17

ASA, FWSM, PIX, and IPS Supported Software Versions

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 systems 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.

Tip The primary software support that is new in Version 4.11 of Security Manager is support for ASA 9.6(1).

- Cisco ASA-5500 Series Adaptive Security Appliances (ASA)—ASA Software Release 7.0(1-2, 4-8), 7.1(1-2), 7.2(1-5), 8.0(2-3, 5), 8.1(1-2), 8.2(1-3), 8.3(1-2), 8.4(1-6), 8.5(1), 8.6(1), 9.0(1), 9.1(1-5), 9.2(1), 9.2(2), 9.2(3), 9.3(1-2), 9.4.1, 9.5.1, 9.5.2 and 9.6.1.

  The following special cases and exceptions apply to ASA software support:

  - If you upgrade a device that you are already managing in Security Manager from 8.x to 9.0(1) or higher, you must rediscover the device inventory so that Security Manager starts interpreting the device as a 9.x device and then you must rediscover the policies on the device to ensure that Security Manager looks for and discovers the appropriate policy types. Alternatively, you can delete the device from Security Manager and then add the device again.
  - If you perform one of the following upgrades to a device that you are already managing in Security Manager:

    —from 7.x to 8.x

    —from any lower version to 8.3(1) or higher

    —from 8.3(x) to 8.4(2) or higher

    you must rediscover the device in Security Manager. This is required due to significant policy changes between the two releases.

    For detailed information on these scenarios, refer to the section titled "Validating a Proposed Image Update on a Device" in the *User Guide for Cisco Security Manager 4.8* at the following URL:

    http://www.cisco.com/c/en/us/support/security/security-manager/products-user-guide-list.html
  - Although 8.2(4) is supported in downward compatibility mode as 8.2(3), Security Manager does support ASA 5585-X models with SSP-10 and SSP-40 running 8.2(4).
  - You cannot use Security Manager to manage SSL VPNs on ASA 7.x.
  - You cannot use Security Manager to manage an ASA 8.3+ device if you enable password encryption using the **password encryption aes** command. You must turn off password encryption before you can add the device to the Security Manager inventory.
  - Release 8.5(1) applies to the Catalyst 6500 Series ASA Services Module (ASA-SM) only. The ASA-SM does not support any type of VPN configuration for this version. However, starting from the 9.0(1) version, ASA-SM supports VPN configurations.
  - Release 8.6(1) applies to the following Cisco ASA 5500-X based Adaptive Security Appliance models only: 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X.
  - Security Manager 4.8 supports ASAv's when you are using ASA 9.2(1) or other versions of ASA that support ASAv's.
  - Table 6 provides the details of the ASA platforms that are supported and not supported for ASA 9.2(1) and above.

Table 6 ASA platforms that are supported and not supported for ASA 9.2(1) and above

ASA Version	Supported	Not Supported
9.2(1)	ASA 5505, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X; ASASM; ASAv	ASA 1000V, 5510, 5520, 5540, 5550, 5580-20, 5580-40
9.2(2)	ASA 5505, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X; ASASM; ASAv	ASA 1000V, 5510, 5520, 5540, 5550, 5580-20, 5580-40

Table 6 ASA platforms that are supported and not supported for ASA 9.2(1) and above

ASA Version	Supported	Not Supported
9.2(3)	ASA 5505, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X; ASASM; ASAv	ASA 1000V, 5510, 5520, 5540, 5550, 5580-20, 5580-40
9.3(1)	ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X; ASASM; ASAv	ASA 1000V, 5505, 5510, 5520, 5540, 5550, 5580-20, 5580-40
9.3(2)	ASA 5506-X, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X; ASASM; ASAv	ASA 1000V, 5505, 5510, 5520, 5540, 5550, 5580-20, 5580-40
9.4(1)	ASA 5506-X, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X; ASASM; ASAv, ASA 5506W-X, 5506H-X, 5508-X, 5516-X, FPR9K-SM-36, FPR9K-SM-24	ASA 1000V, 5505, 5510, 5520, 5540, 5550, 5580-20, 5580-40
9.5(1)	ASA 5506-X, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X; ASASM; ASAv, ASA 5506W, 5506-H, 5508, 5516, FPR9K-SM-36, FPR9K-SM-24	ASA 1000V, 5505, 5510, 5520, 5540, 5550, 5580-20, 5580-40
9.5(2)	ASA 5506-X, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X; ASASM; ASAv, ASA 5506W, 5506-H, 5508, 5516, FPR9K-SM-36, FPR9K-SM-24	ASA 1000V, 5505, 5510, 5520, 5540, 5550, 5580-20, 5580-40
9.6(1)	ASA 5506-X, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X; ASASM; ASAv, ASA 5506W, 5506-H, 5508, 5516, FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-12, FPR4K- SM-24, FPR4K-SM-36	ASA 1000V, 5505, 5510, 5520, 5540, 5550, 5580-20, 5580-40

- Cisco Catalyst 6500 Series Firewall Services Module (FWSM)—FWSM Software Release 2.2(1), 2.3(1-4), 3.1(1, 3-9), 3.2(1-4), 4.0(1), and 4.1(1).
- 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(1-4), and 8.0(2-4).
- IPS sensors and modules—IPS Software 5.1, 6.0, 6.1, 6.2, 7.0, 7.1 [7.1(1), 7.1(2), 7.1(3), 7.1(4), 7.1(8), 7.1(9)], IPS 7.2(1), IPS 7.2(2), 7.3(1), 7.3(2), and 7.3(3) with these restrictions:
  - Release 5.1(5)E1 and later *only* support IPS signature updates.
  - Release 7.1 is supported on the following platforms: Cisco ASA 5585 Series IPS Security Services Processor; IPS 4300 series sensors; IPS 4500 series sensors; IPS 4270; and Cisco ASA 5500 Series IPS Security Services Processor.
  - Release 7.1(6) is supported on six hardware platforms: IPS 4240; IPS 4255; IPS 4260; ASA 5500 AIP SSM-10; ASA 5500 AIP SSM-20; and ASA 5500 AIP SSM-40.
  - Release 7.3(1)E4 is supported on four hardware platforms: IPS-4345 (standalone IPS sensor); IPS-4360 (standalone IPS sensor); IPS-4510 (standalone IPS sensor); and IPS-4520 (standalone IPS sensor).

- Release 7.3(2)E4 is supported on the following platforms: IPS 4345, IPS 4360, IPS 4510, IPS 4520, IPS 4520-XL, ASA 5512-X IPS SSP, ASA 5515-X IPS SSP, ASA 5525-X IPS SSP, ASA 5545-X IPS SSP, ASA 5555-X IPS SSP, ASA 5585-X IPS SSP-10, ASA 5585-X IPS SSP-20, ASA 5585-X IPS SSP-40, and ASA 5585-X IPS SSP-60.
- Release 7.3(3)E4 is supported on the following platforms: IPS 4345, IPS 4360, IPS 4510, IPS 4520, IPS 4520-XL, ASA 5512-X IPS SSP, ASA 5515-X IPS SSP, ASA 5525-X IPS SSP, ASA 5545-X IPS SSP, ASA 5555-X IPS SSP, ASA 5585-X IPS SSP-10, ASA 5585-X IPS SSP-20, ASA 5585-X IPS SSP-40, and ASA 5585-X IPS SSP-60.

Cisco IOS Software Supported Versions

The following sections explain the basic versions supported for Cisco IOS Software and the limitations and restrictions that apply to managing Cisco IOS Software devices:

Basic Cisco IOS Software Support

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. Note that the device model might limit the versions you are allowed to install; this is not controlled by Security Manager.

Note Security Manager provides limited support for features in routers running the Cisco IOS Software releases. The Eventing, Monitoring, Reporting, and Image Management functionalities are not supported on IOS devices. For Security Manager to manage IOS routers, you must make sure that the IOS versions comply with the list of supported versions.

- 15.3T—Versions include 15.3(1)T, 15.3(2)T, and 15.3(2)S.
- 15.2T—Versions include 15.2(1)T1 and 15.2(2)T.

  Note Security Manager supports 15.2(1)T1 on 88x, 89x, 19xx, 29xx, and 39xx routers only. ScanSafe is the only supported new feature in this version.

- 15.1T—Versions include 15.1(1)T.
- 15.0—Versions include 15.0(1)M.
- 12.4T—Versions include 12.4(2)T, 12.4(4)T, 12.4(6)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(24)T.
- 12.4—Versions include 12.4(1), 12.4(1a), 12.4(3).
- 12.3(2)T—Versions include 12.3(2)T, 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—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—Versions include:
  - 12.2(8)T and ZB8.
  - 12.2(11)YU, YX, YX1, 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—Versions include 12.1(4)E3 and 12.1(5)T9.

Basic Cisco IOS XE Software Support

The Cisco ASR 1000 Series Aggregation Services Routers use Cisco IOS XE Software, which uses a different numbering scheme from standard Cisco IOS Software. However, these release numbers are mapped to standard IOS release numbers in Security Manager. The following are the supported Cisco IOS XE Software releases and the Cisco IOS software equivalent releases used in Security Manager:

- 2.1.x—Called 12.2(33)XNA.
- 2.2.x—Called 12.2(33)XNB.
- 2.3.x—Called 12.2(33)XNC. Security Manager treats this release as equivalent to 2.2 (12.2(33)XNB) except for the addition of GET VPN support.

- 2.4.x—Called 12.2(33)XND. No features that are new in this release are supported. This is the lowest release supported on the ASR 1002 Fixed Router.
- 2.5.x—Called 12.2(33)XNE. Security Manager treats this release as equivalent to 2.4 (12.2(22)XND) except for the addition of DMVPN phase 3 support (for direct spoke-to-spoke communications).
- 2.6.x—Called 12.2(33)XNF. No features that are new in this release are supported.
- 3.1.x—Called 15.0(1)S. No features that are new in this release are supported.
- 3.5.x—Called 15.2(1)S. No features that are new in this release are supported.
- 3.8.x—Called 15.3(1)S. No features that are new in this release are supported.
- 3.9.x—Called 15.3(2)S. No features that are new in this release are supported.

Tip Although the 2.x 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.

Restrictions for Cisco IOS Software Devices

Cisco routers and switches have these software restrictions:

- Security Manager ***does not*** support Cisco IOS Software Release 15.x for Catalyst switches.
- 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 software release you can use on a device is always limited to those releases that the hardware supports. For example, the 1900, 2900, and 3900 series ISRs require 15.0(1)M as a minimum release.
- The Cisco ASR 1000 Series Aggregation Services Routers require Cisco IOS XE Software. For more detailed information, see Basic Cisco IOS XE Software Support, page 18.
- 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. In addition, to perform signature updates on routers running Cisco IOS Software release 15.0, you need a a separate ios-ips-update license, which you must manually apply to the device.
- The IPS subsystem has a separate numbering scheme, which you can view in the device properties in Security Manager. The 3.x subsystems are equivalent to IPS 5.x. The subsystems are:
  - 3.000.001, supported in 12.4(11)T to 12.4(11)T4.
  - 3.001.001, supported in 12.4(15)T to 12.4(15)T2.
  - 3.001.002, supported in 12.4(15)T3 to 12.4(24)T.
  - 3.002.001, supported in 15.0(1)M+.

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.

The following table 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 for Security Manager, page 14, 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 7 Software Releases Supported in Downward Compatibility Mode

Releases Supported in Downward Compatibility Mode	Supported As These Releases
ASA Software Releases	
8.2(5), 8.2(4.4), 8.2(4.1), 8.2(4), 8.2(3.9)	8.2(3)
8.0(4)	8.0(3)
PIX Software Releases	
7.2(5)	7.2(4)
FWSM Software Releases	
4.1(2-6)	4.1(1)
4.0(2-15)	4.0(1)

Table 7 Software Releases Supported in Downward Compatibility Mode (continued)

Releases Supported in Downward Compatibility Mode	Supported As These Releases
3.2(5-21)	3.2(4)
3.1(10-20)	3.1(9)
3.1(2)	3.1(1)
Cisco IOS Software Releases	
15.1(3)T	15.1(1)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
12.4(15)XZ	12.4(20)T
Cisco IOS XE Software Releases for Cisco ASR 1000 Series Aggregation Services Routers	
2.1(x) releases: 12.2(33)XNA1,2	12.2(33)XNA
2.2(x) releases: 12.2(33)XNB1-3	12.2(33)XNB
2.3(x), 2.3.xt releases: 12.2(33)XNC1-2, XNC0t, XNC1t	12.2(33)XNC
2.4(x) releases: 12.2(33)XND1-4	12.2(33)XND
2.5(x) releases: 12.2(33)XNE1-2	12.2(33)XNE
2.6(x) releases: 12.2(33)XNF1-2	12.2(33)XNF
3.1(x) releases: 3.1(1-4)S (in running configs, 15.0(1)S1-4)	15.0(1)S
3.2(x) releases: 3.2(0-2)S (in running configs, 15.1(1)S-S2)	15.0(1)S
3.3(x) releases: 3.3(0-1)S (in running configs, 15.1(2)S-S1)	15.0(1)S
3.4(x) releases: 3.4(0)S	15.0(1)S
3.6(x) releases	15.2(1)S
3.7(x) releases	15.2(1)S
3.10(x) releases	15.3(2)S
Cisco IOS Software Releases for Catalyst switches and 7600 series routers	
12.2(33)SXI1	12.2(33)SXI

Supported Devices and Software Versions for Auto Update Server

You can use the Auto Update Server application with any Cisco ASA-5500 Series Adaptive Security Appliance, Catalyst 6500 Series ASA Services Module, or Cisco PIX 500 Series Firewall and the ASA or PIX software versions supported by Security Manager.

Note You cannot use devices configured in multiple-context mode with Auto Update Server.

Product Documentation

For the complete list of documents supporting this release, see the release-specific document roadmap:

- *Guide to User Documentation for Cisco Security Manager*

  http://www.cisco.com/c/en/us/support/security/security-manager/products-documentation-roadmaps-list.html

  Lists document set that supports the Security Manager release and summarizes contents of each document.

- For general product information, see:

  http://www.cisco.com/go/csmanager

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Product Documentation" section.