Supported Devices and Software Versions for Cisco Security Manager 4.1

First Published: March 2011
Revised: June 2011

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, and report management. The following table 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.

Table 1 Features Supported By Device Class in Security Manager

Device Class	Device Configuration	Event Management	Report Management
Adaptive Security Appliance (ASA)	Yes	Yes (ASA 8.0+ only.)	Yes (ASA 8.0+ only.)
Intrusion Prevention System (IPS) appliances and service modules	Yes	Yes (IPS 6.1+ only.)	Yes (IPS 6.1+ only.)
Firewall Services Modules (FWSM)	Yes	Yes (FWSM 3.1.17+, 3.2.17+, 4.0.10+, and 4.1.1+ only)	No

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table 1 Features Supported By Device Class in Security Manager (continued)

Device Class	Device Configuration	Event Management	Report Management
PIX Firewalls	Yes	No	No
Cisco IOS routers	Yes	No	No
Cisco IOS IPS in supported routers	Yes	No	No
Catalyst switches	Yes	No	No

IPv6 Support by Device Type

Security Manager provides some support for IPv6 configurations. The following table lists the general device support for IPv6 in Security Manager. For the specific policies that you can configure, see the Getting Started chapter in the *User Guide for Cisco Security Manager*.

Table 2 IPv6 Supported By Device Class in Security Manager

Device Class	Device Configuration	Event Management	Report Management
Adaptive Security Appliance (ASA) (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.)
Intrusion Prevention System (IPS) appliances and service modules	No	Yes (IPS 6.1+ only.)	Yes (IPS 6.1+ only.)
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
PIX Firewalls	No	No	No
Cisco IOS routers	No	No	No
Cisco IOS IPS in supported routers	No	No	No
Catalyst switches	No	No	No

Supported Devices for Security Manager

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

Table 3 Cisco Security Manager Supported Devices

Series	Supported Device Models
Adaptive Security Appliances and Firewalls	
Cisco ASA-5500 Series Adaptive Security Appliance	• 5505 • 5510 • 5520 • 5540 • 5550 • 5580-20, -40 • 5585-X with SSP-10, SSP-20, SSP-40, SSP-60
Cisco Catalyst 6500 Series Firewall Services Module (FWSM)[1]	
Cisco PIX 500 Series Firewalls	• 501 • 506 • 506E • 515 • 515E • 520 • 525 • 535
IPS Sensors	
Cisco IPS 4200 Series Sensors	• 4210 • 4215 • 4235 • 4240 • 4250 TX • 4250 SX • 4250 XL • 4255 • 4260 • 4270

Table 3 Cisco Security Manager Supported Devices (continued)

Series	Supported Device Models
Cisco ASA 5585 IPS Security Services Processor	• 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)
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, 881G, 881SRST, 881SRSTW, 881W • 886, 886G, 886SRST, 886SRSTW, 886W • 887, 887G, 887M, 887SRST, 887SRSTW, 887Vdsl2, 887W • 888, 888G, 888SRST, 888SRSTW, 888W • 891, 891W • 892, 892W
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 • 1941-W

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 • 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.

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

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.

- 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, 5), 8.1(1-2), 8.2(1-3), 8.3(1-2), 8.4(1).

  The following exceptions apply to ASA software support:

  - If you upgrade a device that you are already managing in Security Manager to 8.3(1) or higher, you must delete the device from the inventory and then add it back. This is required due to significant policy changes between the 8.3 release and lower releases. This requirement applies to all device models, including upgrades of a 5585-X from 8.2(3) to 8.4(1).
  - 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.
- 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(1-5), and 8.0(2-4).
- IPS sensors and modules—IPS Software 5.1, 6.0, 6.1, 6.2, 7.0, and 7.1 with these restrictions:
  - IPS signature updates are supported only on IPS Software 5.1(5)E1 and later.
  - Release 7.1 is supported on the Cisco ASA 5585 IPS Security Services Processor only.
  - 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.

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.

- 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)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, 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.

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 13.
- 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 11, 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 4 Software Releases Supported in Downward Compatibility Mode

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

Table 4 Software Releases Supported in Downward Compatibility Mode (continued)

Releases Supported in Downward Compatibility Mode	Supported As These Releases
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
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 or Cisco PIX 500 Series Firewall and ASA or PIX software versions supported by Security Manager.

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

Supported Devices and Software Versions for Performance Monitor

The following table lists the devices that you can monitor in Performance Monitor and describes supported software versions on those devices. The software versions that you can use on a device are limited in all cases by what can actually run on the device and are further limited in some cases by restrictions that Performance Monitor imposes.

Table 5 Cisco Performance Monitor Supported Devices

Series	Devices Supported	Software Versions Supported
Routers and Switches		
800	801, 802, 803, 804, 805, 811, 827, 828, 831, 836, 837, 851, 857, 861, 871, 876, 877, 878, 881, 887, 888, 891, 892	12.3(7)T and later.
1700	1701, 1710, 1711, 1712, 1720, 1721, 1750, 1751, 1760	12.3(7)T and later.
1800	1801, 1802, 1803, 1811, 1812, 1841, 1861	12.3(7)T and later.
1900	1905, 1921, 1941, 1941-W	15.0(1)M and later.
2600	2610, 2611, 2612, 2613, 2620, 2621, 2650, 2651, 2691	12.3(7)T and later.
2800	2801, 2811, 2821, 2851	12.3(7)T and later.

Table 5 Cisco Performance Monitor Supported Devices (continued)

Series	Devices Supported	Software Versions Supported
2900	2901, 2911, 2921, 2951	15.0(1)M and later.
3600	3620, 3640, 3660, 3661, 3662	12.3(7)T and later.
3700	3725, 3745	12.3(7)T and later.
3800	3825, 3845	12.3(7)T and later.
3900	3925, 3925E, 3945, 3945E	15.0(1)M and later.
7100	7100, UBR 7111, UBR 7114, 7120, 7140, 7150	12.3(7)T and later.
7200	7202, 7204, 7204VXR, 7206, 7206VXR, 7246, UBR 7223, UBR 7246Vxr, UBR7246	12.3(7)T and later.
7300	7301, 7304	12.3(7)T and later.
7400	7401	12.3(7)T and later.
Concentrators		
VPN 3000 Series Concentrators		4.1(x) or 4.7(x)
ASA and PIX Firewall Appliances		
PIX 500	501, 506, 506E, 515, 515E, 520, 525, 535	6.3(4+), 7.0(x), or 7.1(x)
ASA-5500	5505, 5510, 5520, 5540, 5550, 5580-20, 5580-40, 5585-X (all models)	7.0(x), 7.1(x), 7.2(x), 8.0(x), 8.1(x), 8.2(x), 8.3(x), 8.4(x)
Services Modules in Catalyst 6500 Switches		
Content Switching Modules		4.1(5) or 4.2(2)
Firewall Services Modules		2.2(1), 2.3(x), 3.1(x), 3.2(x), or 4.0(x)
IPSec VPN Services Modules		• 12.2(18)SX on Supervisor Engine 2 • 12.2(18)SX on Supervisor Engine 720
SSL Services Modules		1.2(2) or 2.1(6)
VPN Shared Port Adapters (VPN SPA)		12.2(18)SXE2 on Supervisor Engine 720
VPN Services Port Adapter (VSPA)		12.2(33) SXI on Supervisor Engine 720