Release Notes for Cisco Security Manager 4.20

Originally Published: June 29, 2020

This document contains the following topics:

Introduction

Note Use this document in conjunction with the documents identified in Communications, Services, and Additional Information, page 15. The online versions of the user documentation are also occasionally updated after the initial release. As a result, theJ information contained in the Cisco Security Manager end-user guides on Cisco.com supersedes any information contained in the context-sensitive help included with the product. For latest Cisco Security Manager 4.20 updates, refer Cisco.com.

This document contains release note information for the following:

- **Cisco Security Manager 4.20**—Cisco Security Manager enables you to manage security policies on Cisco security devices. Security Manager supports integrated provisioning of firewall, VPN, ASA security appliances, and several other services modules. (You can find complete device support information under Cisco Security Manager Compatibility Information on Cisco.com.) Security Manager also supports provisioning of many platform-specific settings, for example, interfaces, routing, identity, QoS, logging, and so on.

Cisco Systems, Inc.
www.cisco.com

Security Manager efficiently manages a wide range of networks, from small networks consisting of a few devices to large networks with thousands of devices. Scalability is achieved through a rich feature set of device grouping capabilities and objects and policies that can be shared.

Note From version 4.21 onwards, Cisco Security Manager terminates whole support, including support for any bug fixes or enhancements, for all Aggregation Service Routers, Integrated Service Routers, Embedded Service Routers, and any device operating on Cisco IOS software, including the following devices:

- Cisco Catalyst 6500 and 7600 Series Firewall Services Modules (EOL8184)
- Cisco Catalyst 6500 Series Intrusion Detection System Services Module 2 (EOL8843)
- Cisco Intrusion Prevention System: IPS 4200, 4300, and 4500 Series Sensors (EOL9916)
- Cisco SR 500 Series Secure Routers (EOL7687, EOL7657)
- PIX Firewalls (EOL)

- **Auto Update Server 4.20**—The Auto Update Server (AUS) is a tool for upgrading ASA software images, Adaptive Security Device Manager (ASDM) images, and ASA configuration files. Security appliances with dynamic IP addresses that use the auto update feature connect to AUS periodically to upgrade device configuration files and to pass device and status information.

Note Before using Cisco Security Manager 4.20, we recommend that you read this entire document. In addition, it is critical that you read the Important Notes, page 9, the Installation Notes, page 6, and the *Installation Guide for Cisco Security Manager 4.20* before installing Cisco Security Manager 4.20.

Supported Component Versions and Related Software

The Cisco Security Management Suite of applications includes several component applications plus a group of related applications that you can use in conjunction with them. The following table lists the components and related applications, and the versions of those applications that you can use together for this release of the suite. For a description of these applications, see the *Installation Guide for Cisco Security Manager 4.20*.

Note For information on the supported software and hardware that you can manage with Cisco Security Manager, see the *Supported Devices and Software Versions for Cisco Security Manager* online document under Cisco Security Manager Compatibility Information on Cisco.com.

Table 1 Supported Versions for Components and Related Applications

Application	Support Releases
Component Applications	
Cisco Security Manager	4.20
Auto Update Server	4.20
CiscoWorks Common Services	4.2.2

Table 1 Supported Versions for Components and Related Applications (Continued)

Application	Support Releases
Related Applications	
Cisco Security Monitoring, Analysis and Response System (CS-MARS)	6.0.7, 6.1.1
Cisco Secure Access Control Server (ACS) for Windows **Notes** • Cisco Secure ACS Solution Engine 4.1(4) is also supported. • Cisco Secure ACS 5.x is supported for authentication. • You can use other versions of Cisco Secure ACS if you configure them as non-ACS TACACS+ servers. A non-ACS configuration does not provide the granular control possible when you configure the server in ACS mode.	4.2(0), 5.x
Cisco Configuration Engine	3.5, 3.5(1)

What's New

Cisco Security Manager 4.20 Service Pack 2

This release includes bug fixes. Refer Resolved Caveats, page 14 for more information.

Cisco Security Manager 4.20 Service Pack 1

This release includes the following new features and enhancements:

- **Speed nonegotiate enhancement**—The following enhancements have been made in Cisco Security Manager 4.20 Service Pack1 release, pertaining to speed nonegotiate enhancement:
  - The support for "nonegotiate" Speed option has been removed for FPR-4K and 9K devices, owing to ASA limitations. However, it is recommended to use Firepower Device Management (FDM), if in need to avail the support.
  - For devices whose 1G SFP modules are already part of the device hardware and their PIDs are not part of the 16 default PIDs ("**fwsvc.PIDsFor1GSFP**=GLC-SX-MMD,GLC-LH-SMD,GLC-EX-SMD,GLC-ZX-SMD,GLC-SX-MMD=,GLC-LH-SMD=,GLC-EX-SMD=,GLC-ZX-SMD=,GLC-LH-SM,GLC-LH-SM=,GLC-SX-MM,GLC-SX-MM=,SFP-GE-L,SFP-GE-L=,SFP-GE-S,SFP-GE-S=") in the "csm.properties" file, add the corresponding PIDs to the "**fwsvc.PIDsFor1GSFP**" property as shown in the image below.

```
multicontext(config)# sh inventory
Name: "module 0", DESCR: "ASA 5585-X Security Services Processor-10 with 8GE"
PID: ASA5585-SSP-10    , VID: V05     , SN: JAD1804000A

Name: "module 1", DESCR: "ASA 5585-X CX Security Services Processor-10 with 8GE"
PID: ASA5585-SSP-CX10  , VID: V02     , SN: JAD17510444

Name: "Chassis", DESCR: "ASA 5585-X"
PID: ASA5585           , VID: V04     , SN: JMX18058052

Name: "TenGigabitEthernet0/9", DESCR: "1000Based-SX"
PID: GLC-SX-MMD        , VID: V01 , SN: AGJ1807RRHM

Name: "TenGigabitEthernet1/8", DESCR: "1000Based-SX"
PID: FTRJ-8519-7D-CS4A , VID: A   , SN: FNS0917B0D1

Name: "TenGigabitEthernet1/9", DESCR: "10G Based-SR"
PID: SFP-10G-SR-S      , VID: V01 , SN: FNS194727MK

Name: "power supply 0", DESCR: "ASA 5585-X AC Power Supply"
PID: ASA5585-PWR-AC    , VID: V05     , SN: POG17470051

Name: "fan", DESCR: "ASA 5585-X Fan Module"
PID: ASA5585-FAN       , VID: V04     , SN: POG163000HZ
```

- For other devices whose SFP module hardware has been externally added and their module PIDs are not part of the 6 default PIDs ("**fwsvc.PIDsForSFPModule**=ASA-IC-6GE-SFP-A,ASA-IC-6GE-SFP-A=,ASA-IC-6GE-SFP-B,ASA-IC-6GE-SFP-B=,ASA-IC-6GE-SFP-C,ASA-IC-6GE-SFP-C=") in the "csm.properties" file, add the corresponding module PIDs to the "**fwsvc.PIDsForSPFModule**" property as shown in the image below.

```
ASA5525-K9(config)# sh inventory
Name: "Chassis", DESCR: "ASA 5525-X with SW, 8 GE Data, 1 GE Mgmt, AC"
PID: ASA5525           , VID: V06     , SN: FGL200240PS

Name: "module 1", DESCR: "ASA 5525-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-B  , VID: N/A     , SN: N/A

Name: "GigabitEthernet1/0", DESCR: "1000BaseT"
PID: SFP-GE-T          , VID: V02 , SN: MTC19420C10

Name: "GigabitEthernet1/1", DESCR: "1000BaseT"
PID: GLC-TE            , VID: V01 , SN: AVC2251291Y
```

Note After adding new PIDs to the "csm.properties" file, ensure you restart the Security Manager and rediscover the device, for the changes to take effect.

Cisco Security Manager 4.20

This release includes the following new features and enhancements:

Support for ASA 9.13 (1) version

- **Support for Customer Success Network**—Beginning with version 4.20, Cisco Security Manager provides an option to enable Customer Success Network. Customer Success Network helps to avail the features enabled on ASA devices and leverage the same mechanism of Smart Call Home (SCH). The data SCH collects are mostly outdated and the features added since the release of SCH do not report the exact status. Hence, Customer Success Network is being introduced. This feature is supported on ASA 9.13(1) and later devices.
- **Support for CGNAT MAP domains**—Beginning with version 4.20, Cisco Security Manager supports Carrier-Grade NAT Mapping of Address and Port (CGNAT MAP) domains for ASA 9.13(1) devices operating in single, multi-context, and routed modes. This feature helps to configure MAP domains using default or basic mapping rules and is not supported in transparent mode.
- **Support for GTP location logging**—Beginning with version 4.20, Cisco Security Manager supports GTP location logging. When enabled, you can obtain the device location information through a syslog message. The syslog message contains the mobile country code and mobile network code of the device. This syslog message is displayed when activating/updating a PDP context on Gn/Gp in GTPv0/v1 or S5/S8 in GTPv2. You can also add an optional cell ID to the syslog message.
- **NTP server configuration enhancement**—Earlier, only md5 authentication type was supported for configuring NTP server. Beginning with version 4.20, Cisco Security Manager enables support for the following new authentication types for NTP Server Configuration—sha1, sha256, sha512, and cmac.
- **VLAN interface support**—Beginning with version 4.20, Cisco Security Manager supports L2 hardware switching. The L2 switching support is provided by adding a new interface type called VLAN Interface under the Interface Policy Type and a new Switch Port tab. Security Manager supports this feature on Cisco FPR-1010 Adaptive Security Appliance.
- **PoE enhancement**—Beginning with Cisco Security Manager 4.20, Power over Ethernet (PoE) is supported for ASA 9.13(1) or higher devices. This feature comes as part of the physical interface for Ethernet1/7 and Ethernet 1/8 ports. The PoE support is provided by introducing a new Power Over Ethernet tab under Interface Policy. This feature is supported on Cisco FPR-1010 Adaptive Security Appliance.
- **Deprecation of DH groups 2, 5, and 24**—Cisco Security Manager supports numerous DH group algorithms in various policies. DH groups determine the strength of the key used in the key exchange process. DH groups 2, 5, and 24 are no longer considered to be secure against modern threats. Hence, beginning from Cisco Security Manager 4.20, the support for DH groups 2, 5, and 24 is removed in ASA 9.13(1) or higher devices.
- **DH group 14 support for IKEv1**—Beginning with Cisco Security Manager 4.20, DH group 14 is supported for IKEv1, for ASA 9.13(1) and higher devices. This support is added to all relevant RAVPN and site-to-site VPN policies.
- **DH groups 15, 16 support for IKEv2**—Beginning with Cisco Security Manager 4.20, DH groups 15 and 16 are supported for IKEv2, for ASA 9.13(1) and higher devices.
- **New platform support**—Beginning with version 4.20, Cisco Security Manager supports the following Firepower 1000 series devices—Cisco FPR-1010, Cisco FPR-1120, Cisco FPR-1140, and Cisco FPR-1150.
- **Appliance mode for FP1000 and FP2100 series**—Beginning with version 4.20, Cisco Security Manager enables a new option to select the FXOS mode in which the device is operating. The Appliance Mode lets you to configure devices from the CLI, an on-box device such as ASDM, or a multi-device manager such as Cisco Security Manager. The Appliance Mode is supported for existing Firepower 2100 series and new 1000 series appliances on ASA 9.13(1) or higher devices.

- **Support for NBAPI Hitcount Feature**—Beginning with Cisco Security Manager 4.20, you can make API calls at any time to obtain the current or live hitcount values from devices without any manual intervention.
- **Support for Veritas Cluster 7.4**—Beginning with version 4.20, Cisco Security Manager supports Veritas Cluster 7.4 in addition to the existing Veritas support.

Installation Notes

Please refer to the *Installation Guide for Cisco Security Manager 4.20* for specific installation instructions and for important information about client and server requirements. Before installing Cisco Security Manager 4.20, it is critical that you read the notes listed in this section and the Important Notes, page 9.

- The "Licensing" chapter in the installation guide enables you to determine which license you need. (The license you need depends upon whether you are performing a new installation or upgrading from one of several previous versions.) It also describes the various licenses available, such as standard, professional, and evaluation.
- The STD-TO-PRO upgrade converts an ST25 license to a PRO50 license and will result in support for 50 devices. If additional devices need to be supported, you need to buy the necessary incremental licenses.
- Beginning with Version 4.7 of Security Manager, a temporary license for the API is available from Cisco.
- Beginning with Version 4.7 of Security Manager, you can apply incremental licenses to the evaluation version of the Security Manager license.
- Do not modify casuser (the default service account) or directory permissions that are established during the installation of the product. Doing so can lead to problems with your being able to do the following:
  - Logging in to the web server
  - Logging in to the client
  - Performing successful backups of all databases
- Supported operating systems for the server machine are the following:
  - Microsoft Windows Server 2016 Standard— 64-bit
  - Microsoft Windows Server 2016 Datacenter—64-bit
  - Microsoft Windows Server 2012 R2 Standard—64-bit
  - Microsoft Windows Server 2012 Standard—64-bit
  - Microsoft Windows Server 2012 R2 Datacenter—64-bit
  - Microsoft Windows Server 2012 Datacenter—64-bit
- Supported operating systems for the client machine are the following:
  - Microsoft Windows 7
  - Microsoft Windows 8.1 Enterprise Edition—64-bit and 32-bit
  - Microsoft Windows 10 —64-bit and 32-bit
  - Microsoft Windows Server 2016 Standard— 64-bit
  - Microsoft Windows Server 2016 Datacenter— 64-bit

  - Microsoft Windows Server 2012 R2 Standard—64-bit
  - Microsoft Windows Server 2012 Standard—64-bit
  - Microsoft Windows Server 2012 R2 Datacenter—64-bit
  - Microsoft Windows Server 2012 Datacenter—64-bit
- Supported browsers are the following for both the server machine and the client machine:
  - Internet Explorer 8.x, 9.x, 10.x, or 11.x, but only in Compatibility View
  - Firefox 15.0.1 and above supported and recommended
- You can install Security Manager server software directly, or you can upgrade the software on a server where Security Manager is installed. The *Installation Guide for Cisco Security Manager 4.20* explains which previous Security Manager releases are supported for upgrade and provides important information regarding server requirements, server configuration, and post-installation tasks.
- Before you can successfully upgrade to Security Manager 4.20 from a prior version of Security Manager, you must make sure that the Security Manager database does not contain any pending data, in other words, data that has not been committed to the database. If the Security Manager database contains pending data, you must commit or discard all uncommitted changes, then back up your database before you perform the upgrade. The *Installation Guide for Cisco Security Manager 4.20* contains complete instructions on the steps required for preparing the database for upgrade.
- We do not support installation of Security Manager on a server that is running any other web server or database server (for example, IIS or MS-SQL). Doing so might cause unexpected problems that may prevent you from logging into or using Cisco Security Manager.
- Be aware of the following important points before you upgrade:
  - Ensure that all applications that you are upgrading are currently functioning correctly, and that you can create valid backups (that is, the backup process completes without error). If an application is not functioning correctly before an upgrade, the upgrade process might not result in a correctly functioning application.

    Note It has come to Cisco's attention that some users make undocumented and unsupported modifications to the system so that the backup process does not back up all installed CiscoWorks applications. The upgrade process documented in the installation guide assumes that you have not subverted the intended functioning of the system. If you are creating backups that back up less than all of the data, you are responsible for ensuring you have all backup data that you require before performing an update. We strongly suggest that you undo these unsupported modifications. Otherwise, you should probably not attempt to do an inline upgrade, where you install the product on the same server as the older version; instead, install the updated applications on a new, clean server and restore your database backups.

  - Inline upgrades are not supported for Cisco Security Manager 4.12 SP2. If you are upgrading from 4.12SP2 to 4.13 or 4.14, follow the remote upgrade procedure and refer to the steps given in "Resolving database errors while upgrading from Cisco Security Manager 4.12 SP2" section of the *Installation Guide for Cisco Security Manager 4.20* to resolve the database migration issues.

    Note This exception is not applicable if you are upgrading from Cisco Security Manager 4.12.

- If you log in to a Security Manager server that is running a higher version than your client, a notification will be displayed and you will have the option of downloading the matching client version.
- Beginning with Security Manager 4.12, AUS and the Security Manager client are installed in parallel to improve installation time.
- CiscoWorks Common Services 4.2.2 is installed automatically when you install Security Manager or AUS.
- An error message will pop up if there is any database migration error; this will be at a point where installation can be taken forward without stopping.
- It is recommended to do disk defragmentation for every 50 GB increase in the disk size for optimal performance.

Caution Frequent defragmentation will also contribute to bad sectors, eventually leading to disk failure.

- Beginning with Version 4.4, Security Manager includes a Windows Firewall configuration script in the server installer. This script automates the process of opening and closing the ports necessary for Windows Firewall to work correctly and securely; its purpose is to harden your Security Manager server.

Service Pack 2 Download and Installation Instructions

To download and install Security Manager 4.20 Service Pack 2, follow these steps:

Note You must install the Cisco Security Manager 4.20 FCS build on your server before you can apply this service pack.

Caution Before installing this service pack, please back up the following files:

MDC\ips\etc\sensorupdate.properties
MDC\eventing\config\communication.properties

If you have previously modified these files, you will need to reconfigure them after installing the service pack.

Step 1 Go to http://www.cisco.com/go/csmanager, and then click **Download Software for this Product** under the Support heading on the right side of the screen.

Step 2 Enter your user name and password to log in to Cisco.com.

Step 3 Click **Security Manager 4.20** in the rightmost column.

Step 4 Click **Security Manager (CSM) Software** and then click **4.20sp2** under **Latest**.

Step 5 Download the file CSM4.20.0Service_Pack2.exe.

Step 6 To install the service pack, close all open applications, including the Cisco Security Manager Client.

Step 7 If Cisco Security Agent is installed on your server, manually stop the Cisco Security Agent service from **Start > Settings > Control Panel > Administrative Tools > Services**.

Step 8 Run the CSM4.20.0Service_Pack2.exe file that you previously downloaded.

Step 9 In the Install Cisco Security Manager 4.20 Service Pack 2 dialog box, click **Next** and then click **Install** in the next screen.

Step 10 After the updated files have been installed, click **Finish** to complete the installation.

Step 11 On each client machine that is used to connect to the Security Manager server, you must perform the following steps to apply the service pack before you can connect to the server using that client:

a. If Cisco Security Agent is installed on the client, manually stop the Cisco Security Agent service from **Start > Settings > Control Panel > Administrative Tools > Services**.

b. Launch the Security Manager client.

   You will be prompted to “Download Service Pack”.

c. Download the service pack and then launch the downloaded file to apply the service pack.

Step 12 (Optional) Go to the client installation directory and clear the cache, for example, <Client Install Directory>/cache.

Step 13 (Optional) Configure SSL Certificates or self-signed certificates for Open SSL:

a. Stop the CSM Daemon service [net stop crmdmgtd]

b. If you have your own SSL certificates configured, you can reconfigure the certificates as per the steps outlined in the link below:

   http://www.cisco.com/c/en/us/td/docs/net_mgmt/ciscoworks_lan_management_solution/4-2/user/guide/admin/admin/appendixcli.html#wp1016314

c. For self-signed certificates, from the command prompt navigate to the <CSCOpx>\MDC\Apache directory, and then execute the gencert.bat file.
(where <CSCOpx> is your installation directory)

d. Start the CSM Daemon service [net start crmdmgtd].

Important Notes

The following notes apply to the Security Manager 4.20 release:

- The following patches are required to run the critical Cisco Security Manager services on the Microsoft Windows Server 2012 R2. Failing to install the patches will bring down the services. Ensure that you have these patches installed on your server, else install the patches in the same order as follows:

  a. KB2919442

  b. Run the clearcompressionflag.exe

  Note The clearcompressionflag.exe file is part of the cumulative set of security updates. This tool prepares the computer for the Windows Updates in the background. The executable file can be downloaded from the Microsoft site: https://support.microsoft.com/en-in/kb/2919355.

  c. KB2919355, KB2932046, KB2959977, KB2937592, KB2938439, and KB2934018

  d. KB2999226

You can also install these patches after installing the Cisco Security Manager to bring up the critical services. To register the services with the windows services, you must run the "RegisterApache.bat" script which is located in "<CSMInstalledDirectory>\CSCOpx\bin", and then restart the server.

Note It might take a minimum of 30 minutes for these Windows patches to get installed, and the installation duration might vary based on the Windows servers. Errors, if any, while installing these patches pertain to Miscrosoft and not to Cisco Security Manager.

- For remote access VPN in multi-context ASA devices running the software version 9.6(2) or later, the device modifies the storage-url configured with flash:/ directory into disk0:/. Since the device modifies the configuration, Security Manager negates the device configuration and pushes the configuration into the device again. This is a limitation of Security Manager version 4.12.
- In Policy Object Manager > Access Control List > Unified ACL, if you right-click the ACL which is used in any of the device configuration and select "Find Usage", the Find Usage option does not show the list of devices that are configured with the Unified Access List.
- Cisco Security Manager was using OpenSSL for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. Beginning with version 4.13, Cisco Security Manager replaced OpenSSL version 1.0.2 with Cisco SSL version 6.x. Cisco SSL enables FIPS compliance over full FIPS Validation which results in fast and cost-effective connectivity. The Common Criteria mode in Cisco SSL allows easier compliance. Cisco SSL is feature-forward when compared to OpenSSL. The product Security Baseline (PSB) requirements for Cisco SSL ensures important security aspects such as credential and key management, cryptography standards, anti-spoofing capabilities, integrity and tamper protection, and session, data, and stream management and administration are taken care of. In version 4.20, the SSL 1.0.2S is being used.
- Security Manager sends only the delta configuration to the Configuration Engine, where the particular device retrieves it. The full configuration is not pushed to the device. Therefore, the following behaviors are encountered for OSPF, VLAN, and failover for devices.
  - OSPF for IOS routers—Security Manager supports OSPF policy for routers running the IOS Software version 12.2 and later. However, Security Manager does not support OSPF policy for Catalyst devices. Therefore when you configure the OSPF policy in a Catalyst device and perform the discovery in Security Manager, the latter removes the 'no passive-interface <*interface number*>' command from the full configuration. Therefore you will see a difference in the Security Manager-generated configuration and the configuration on the device.
  - VLAN—Security Manager supports discovery of VLAN command in IOS devices but does not support dynamic behavior of the VLAN command. If there are user driven changes in VLAN policy, Security Manager generates the command in delta and full configuration. In other words, in normal preview or deployment, Security Manager does not generate VLAN command in full configuration. Therefore you will see a difference in the Security Manager-generated configuration and the configuration on the device.
  - Failover policy for firewall devices, such as ASA and FWSM, and IOS devices—Security Manager does not support dynamic behavior of failover devices. That is, the primary unit in HA has 'failover lan unit primary' command and secondary unit has 'failover lan unit secondary' command. When there is a switchover, Security Manager tries to compare with the 'failover lan unit primary' and generates the delta configuration. This leads to a failure in deployment.

    Note Security Manager does not support 'dynamic' CLI commands. If the syntax of a CLI command is modified, for example, the 'primary' keyword is changed to 'secondary'; it will not be supported by Security Manager.

- The following ASA policies are supported in Security Manager version 4.8 and higher:
  - SSL
  - EIGRP

  Therefore these policies are managed by default in a fresh 4.8 version, or higher, installation. However, if you are upgrading Security Manager from version 4.7 to 4.8, or from version 4.7 to 4.9, by default the said policies will be unmanaged for both inline and remotely upgraded servers.

  If you are upgrading from Security Manager 4.7 to 4.9, in addition to the SSL and EIGRP ASA policies, the following ASA policies will also be unmanaged:
  - Route-Map
  - CLI Prompt
  - Virtual Access
  - AAA Exec Authorization

  If you have a device that uses commands that were unsupported in previous versions of Security Manager, these commands are not automatically populated into Security Manager as part of the upgrade to this version of Security Manager. If you deploy back to the device, these commands are removed from the device because they are not part of the target policies configured in Security Manager. We recommend that you set the correct values for the newly added attributes in Security Manager so that the next deployment will correctly provision these commands. You can also rediscover the platform settings from the device; however, you will need to take necessary steps to save and restore any shared Security Manager policies that are assigned to the device.

Note If a route-map is configured on the ASA and the same route-map is used in OSPF policy, after upgrading to Security Manager 4.9 from Security Manager 4.7, the OSPF page will show a red-banner. To overcome this issue, you must rediscover the ASA.

- You can also create the Unified ACL object on-the-fly in certain Remote Access VPN policies, such as the Dynamic Access Policy. However, when you create the Unified ACL object on-the-fly, Cisco Security Manager displays an error message. You must add again the created ACL in the Selector window and save the policy.
- If PKI specification is chosen for IKEv2 authentication in Site to Site VPN, created using S2S manager and if a trustpoint is chosen for PKI specification. Then the corresponding Trustpoint should be selected in: Remote Access VPN > Public Key Infrastructure also.
- If you upgrade an ASA managed by Security Manager to release 8.3(x) or higher from 8.2(x) or lower, you must rediscover the NAT policies using the NAT Rediscovery option (right-click on the device, select Discover Policies on Device(s), and then select NAT Policies as the only policy type to discover). This option will update the Security Manager configuration so that it matches the device configuration while preserving any existing shared policies, inheritance, flex-configs, and so on.

  When upgrading an ASA device from 8.4.x to 9.0.1, the device policies will be converted to the unified format. You can rediscover the unified NAT rules using the NAT Rediscovery option or you can convert the existing NAT policies to unified NAT policies with the help of the rule converter in Security Manager. For more information, see http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-6/user/guide/CSMUserGuide/porules.html#pgfId-161507 or the “Converting IPv4 Rules to Unified Rules” topic in the online help.

You can also use the rule converter for the other firewall rules like access rules, AAA rules, and inspection rules if you want to manage these policies in unified firewall rules format.

- 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 4.20* at the following URL:

  http://www.cisco.com/c/en/us/support/security/security-manager/products-user-guide-list.html
- ASA 8.3 ACLs use the real IP address of a device, rather than the translated (NAT) address. During upgrade, rules are converted to use the real IP address. All other device types, and older ASA versions, used the NAT address in ACLs.
- The device memory requirements for ASA 8.3 are higher than for older ASA releases. Ensure that the device meets the minimum memory requirement, as explained in the ASA documentation, before upgrade. Security Manager blocks deployment to devices that do not meet the minimum requirement.
- For ASA devices in cluster mode, Security Manager treats the entire cluster as a single node and manages the cluster using the main cluster IP address. The main cluster IP address is a fixed address for the cluster that always belongs to the current control unit. If the control node changes, the SNMP engine ID for the cluster also changes. In such a case, Security Manager will regenerate the CLI for all SNMP Server Users that are configured with a Clear Text password. Security Manager will not regenerate the CLI for users that are configured using an Encrypted password.

  You can use the Get SNMP Engine ID button on the SNMP page to retrieve the engine ID from the device currently functioning as the cluster control unit.
- The Rollback feature is not supported with ASA clusters. Hence, do not attempt to rollback ASA cluster configurations.
- You cannot use Security Manager to manage an IOS or 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.
- Device and Credential Repository (DCR) functionality within Common Services is not supported in Security Manager 4.8 and later versions.
- LACP configuration is not supported for the IPS 4500 device series.
- A Cisco Services for IPS service license is required for the installation of signature updates on IPS 5.x+ appliances, Catalyst and ASA service modules, and router network modules.
- Do not connect to the database directly, because doing so can cause performance reductions and unexpected system behavior.
- Do not run SQL queries against the database.

- If an online help page displays blank in your browser view, refresh the browser.
- Beginning with version 4.9, Security Manager only supports Cisco Secure ACS 5.x for authentication. ACS 4.1(3), 4.1(4), or 4.2(0) is required for authentication and authorization.
- If you do not manage IPS devices, consider taking the following performance tuning step. In *$NMSROOT*\MDC\ips\etc\sensorupdate.properties, change the value of packageMonitorInterval from its initial default value of 30,000 milliseconds to a less-frequent value of 600,000 milliseconds. Taking this step will improve performance somewhat. [*$NMSROOT* is the full pathname of the Common Services installation directory (the default is C:\Program Files (x86)\CSCOpx).]
- The IPS packages included with Security Manager do not include the package files that are required for updating IPS devices. You must download IPS packages from Cisco.com or your local update server before you can apply any updates. The downloaded versions include all required package files and replace the partial files that are included in the Security Manager initial installation.
- From Cisco Security Manager 4.4, the "License Management" link on the CiscoWorks Common Services home page has been removed.
- CsmReportServer and CsmHPMServer are now supported with 64-bit JRE.
- The "rsh" service has been changed to manual start mode. You can start it manually if you need it.
- To be PCI compliant, in Cisco Security Manager 4.15 and 4.16, TLS 1.0 and TLS 1.1 were disabled respectively. Hence from 4.16, Cisco Security Manager was using only TLS 1.2 version. However, the ISE 1.3 server and its lower versions does not support TLS 1.2. This impacts the legacy ISE settings with Cisco Security Manager from release 4.15. This incompatibility prevents integration of ISE server with Cisco Security Manager. If you are required to integrate ISE 1.3 and lower versions with Cisco Security Manager successfully, refer "Resolving errors while integrating ISE server with Cisco Security Manager" section in *User Guide for Cisco Security Manager 4.19*.
- Beginning from version 4.19, Cisco Security Manager does not support cross-launch of Cisco Adaptive Security Device Manager 7.12.1 for ASA 9.12.1 devices. However, the Security Manager supports cross-launch of ASDM for ASA 9.10.1 and earlier versions. Hence, beginning with version 4.19, you must install ASDM separately for ASA 9.12.1 devices in Cisco Security Manager client machine.
- Beginning with version 4.19, Cisco Security Manager does not support the device SSL Certificates using DES algorithms. If the device SSL uses DES algorithms, Security Manager throws up an error when you try to add the device. This happens because the JRE, by default, disables the DES algorithms due to security vulnerability.

Caveats

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Open Caveats

There are no open bugs with severity 3 and higher for version 4.20. All open bugs with severity 3 and higher for 4.20 Service Pack 1, and all versions prior to 4.20 are included in the following search:

- Open caveats—Release 4.20 Service Pack 1
- Open caveats—Releases prior to 4.20

Resolved Caveats

- Resolved caveats—Release 4.20 Service Pack 2
- Resolved caveats—Release 4.20 Service Pack 1
- Resolved caveats—Release 4.20
- For the list of caveats resolved in releases prior to this one, see the following documents:

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

Where to Go Next

Note The links in the following table pertain to Cisco Security Manager version 4.20 and earlier.

If you want to:	Do this:
Install Security Manager server or client software.	See *Installation Guide for Cisco Security Manager*.
Understand the basics.	See the interactive JumpStart guide that opens automatically when you start Security Manager.
Get up and running with the product quickly.	See "Getting Started with Security Manager" in the online help, or see Chapter 1 of *User Guide for Cisco Security Manager*.
Complete the product configuration.	See "Completing the Initial Security Manager Configuration" in the online help, or see Chapter 1 of *User Guide for Cisco Security Manager*.
Manage user authentication and authorization.	See the following topics in the online help, or see Chapter 7 of *Installation Guide for Cisco Security Manager*. • Setting Up User Permissions • Integrating Security Manager with Cisco Secure ACS
Bootstrap your devices.	See "Preparing Devices for Management" in the online help, or see Chapter 2 of *User Guide for Cisco Security Manager*.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

This document is to be used in conjunction with the documents listed in the "Communications, Services, and Additional Information" section.