

Cisco Prime Security Manager

An evolving global workforce and the proliferation of applications and devices have amplified network complexity, requiring firewall administrators to choose between enabling the anytime, anywhere, any device access required for employee productivity, and the degree of security required to protect the business. Cisco® ASA Next-Generation Firewalls address this issue by enabling access control based on applications, devices, and users.

Cisco Prime Security Manager is the management tool for the Cisco ASA 5500-X Series Next-Generation Firewalls (NGFW). This application is built on Web 2.0 technologies and supports both single-device and multidevice manager form factors to help manage the following capabilities:

- Application Visibility and Control to help block applications, users and devices
- Web Security Essentials, which includes URL filtering and Web reputation
- Intrusion Prevention on the Cisco Next-Generation Firewalls
- Stateful inspection capabilities to configure layer 3/Layer 4 access control rules

Unprecedented Network Visibility

Cisco Prime Security Manager provides security administrators with end-to-end visibility across the security network, including top-level traffic patterns, granular logs, and the health and performance of ASA Next-Generation Firewalls and Cisco Next-Generation Firewall Services.

This application also provides reports that give administrators a better understanding of the traffic flows throughout the network. For example, the Network Dashboard report (Figure 1) highlights the top ASA Next-Generation Firewall sources and destinations along with traffic by location. It also shows the policies that have been hit from web and nonweb requests.

Figure 1. Report on Top Sources, Destinations, Policies, Traffic, and Applications



In addition to the top-level reports, Cisco Prime Security Manager enables administrators to access detailed information about users, applications, devices, and other contextual elements for exceptional visibility and control. Figures 2 through 5 provide examples. Table 1 describes all the reports offered by Cisco Prime Security Manager.

Figure 2. Report on Facebook Microapplications Accessed from Within the Network

	Application	Transactions	Transactions allowed	Transactions denied	Data usage	Bytes sent	Bytes received
1	Facebook General	2.8 K	2.8 K	0	16 MB	1.9 MB	14.1 MB
2	Facebook Photos	865	865	0	3.1 MB	716.2 KB	2.4 MB
3	Facebook Applications: Games	614	0	614	852.3 KB	84.8 KB	767.5 KB
4	Facebook Chat & Video Chat	403	403	0	983.8 KB	237.9 KB	745.9 KB

Figure 3. Report of Facebook Access by User

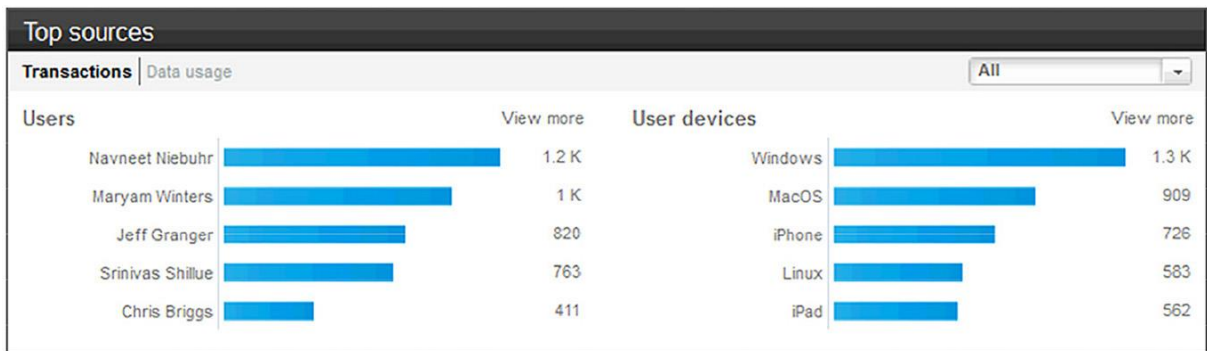


Figure 4. Overview of Device-Level View

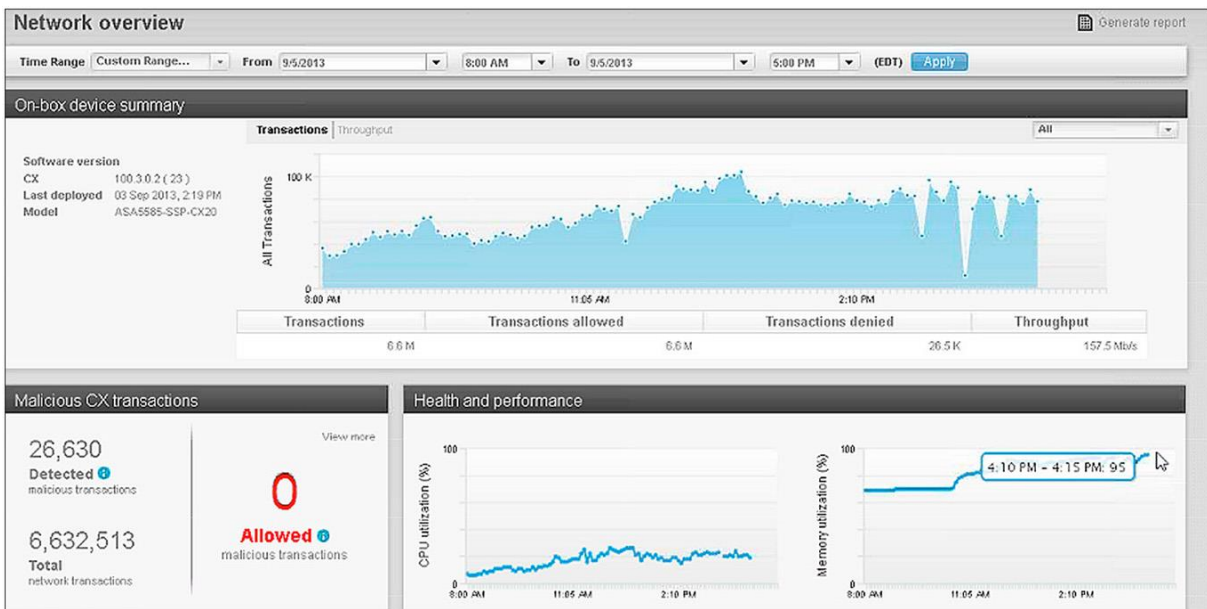


Figure 5. View of New ASA Next-Generation Firewall Policies

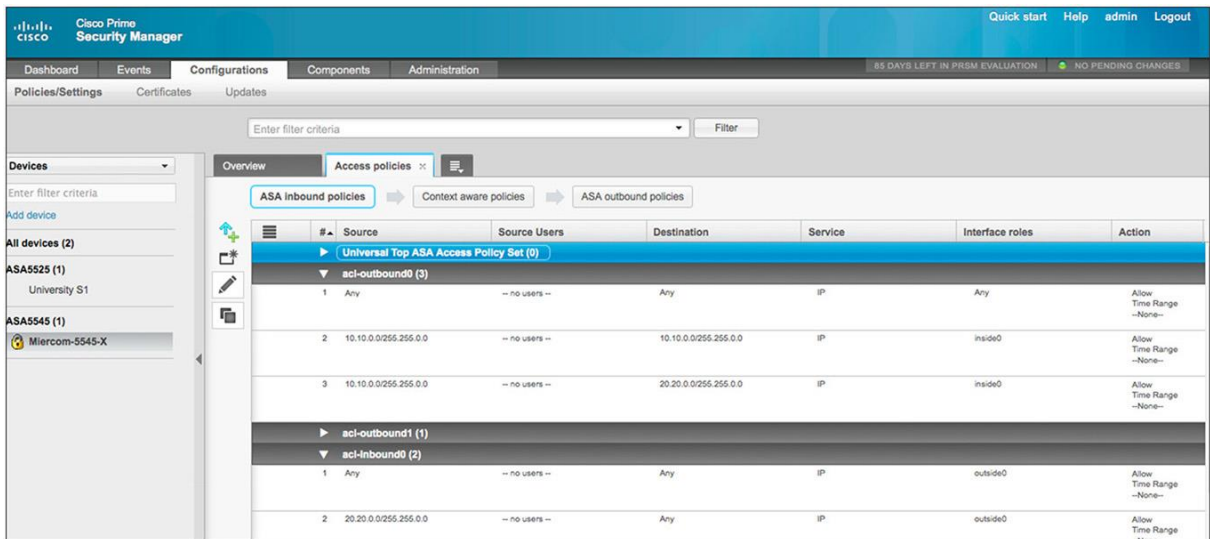


Table 1. Reports Available in Cisco Prime Security Manager

Report Category	Description	Specific Reports
Traffic Summary Reports	Provides a high-level summary of network traffic	<ul style="list-style-type: none"> Traffic summary by transactions: details which transactions were permitted or denied Traffic summary by bytes: gives a summary of received and transmitted data Web versus non-web traffic summary, by transactions and bytes
Application Reports	Enables network applications to be monitored	<ul style="list-style-type: none"> Top applications by transactions Top applications by blocked transactions Detailed application table
User Reports	Enables user activity to be monitored	<ul style="list-style-type: none"> Top users by transactions Top users by blocked transactions Detailed user table
Endpoint Reports	Provides visibility into which endpoints and operating systems are accessing the network	<ul style="list-style-type: none"> Top operating systems by transactions Top operating systems by blocked transactions Detailed operating systems table Location-based traffic: details which traffic comes from directly connected devices versus remote-access mechanisms
URL Reports	Enables web activity to be monitored	<ul style="list-style-type: none"> Top URL categories by transactions Top URL categories by blocked transactions Detailed URL table
Device Reports	Analyzes the usage of network security devices	<ul style="list-style-type: none"> Top devices by transactions: shows the firewalls that are most frequently used Top devices by blocked transactions: shows the firewalls that block the most traffic Detailed devices table: detailed list of the firewalls, transactions processed, and total throughput
Threat Reports	Provides more visibility into the threat profiles in a network	<ul style="list-style-type: none"> Top 25 threats affecting the business environment Top 25 attackers and top 25 targets that are vulnerable Top 25 policies that are affected with the maximum number of threats

Management of Cisco ASA 5500-X Series Next-Generation Firewalls

The latest update of Cisco Prime Security Manager helps manage many features of the ASA 5500-X Series:

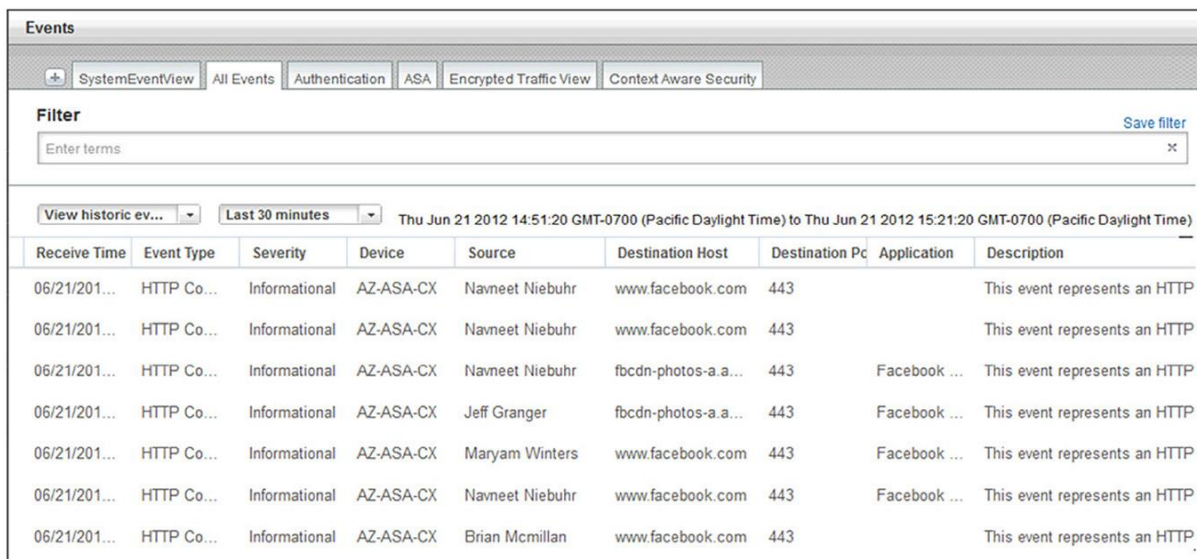
- Users can preview various command-line interface (CLI) configurations before they deploy the changes to the devices.
- Cisco Prime Security Manager can help manage core fundamentals such as firewall, Network Address Translation (NAT), and events.
- Device high availability can be monitored, and dashboard widgets for high availability are supported as well.
- Workflows from ASA deployments can be imported to provide better integration between ASA 5500-X Series devices and other devices running ASA Next-Generation Firewall Services.

Event Analysis and Proactive Monitoring

While the top-n reports provide high-level information regarding traffic patterns throughout the network, Cisco Prime Security Manager also enables detailed information about specific users, applications, URLs, and devices, which simplifies any next-level analysis that may be required for anomalous traffic.

Log monitoring for troubleshooting and longer-term security analysis is also critical for security administrators. Cisco Prime Security Manager provides intuitive access to raw events from the reporting dashboard to support administrators in scenarios that require deeper analysis. A view of the policies that have been deployed provides more information on the effects of various policy rules. Figure 6 shows the Cisco Prime Security Manager Event Monitor, which supports real-time and historical event analysis, as well as intuitive filtering capabilities.

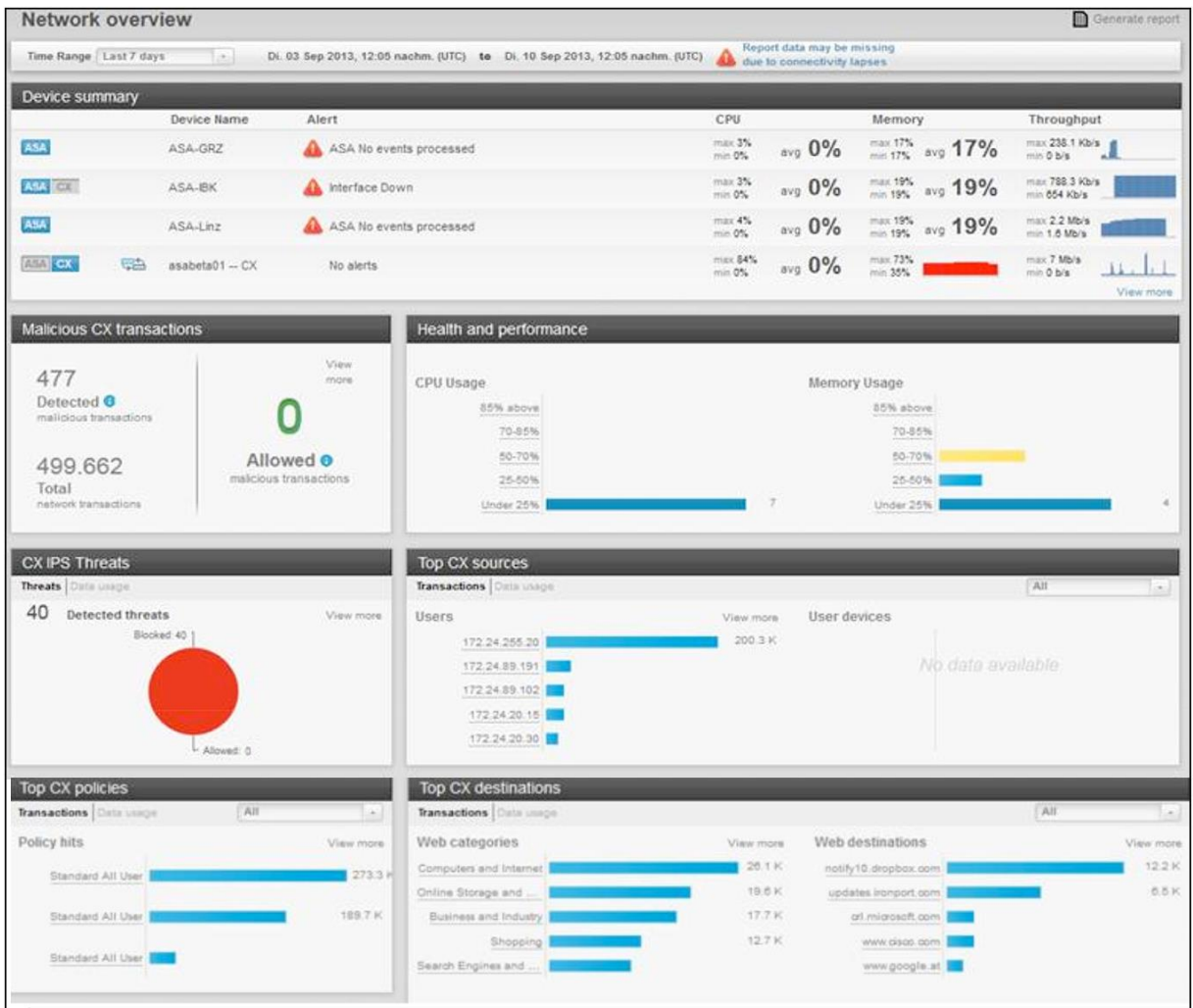
Figure 6. Cisco Prime Security Manager Event Monitor



Receive Time	Event Type	Severity	Device	Source	Destination Host	Destination Pc	Application	Description
06/21/201...	HTTP Co...	Informational	AZ-ASA-CX	Navneet Niebuhr	www.facebook.com	443		This event represents an HTTP
06/21/201...	HTTP Co...	Informational	AZ-ASA-CX	Navneet Niebuhr	www.facebook.com	443		This event represents an HTTP
06/21/201...	HTTP Co...	Informational	AZ-ASA-CX	Navneet Niebuhr	fbcdn-photos-a.a...	443	Facebook ...	This event represents an HTTP
06/21/201...	HTTP Co...	Informational	AZ-ASA-CX	Jeff Granger	fbcdn-photos-a.a...	443	Facebook ...	This event represents an HTTP
06/21/201...	HTTP Co...	Informational	AZ-ASA-CX	Maryam Winters	www.facebook.com	443	Facebook ...	This event represents an HTTP
06/21/201...	HTTP Co...	Informational	AZ-ASA-CX	Navneet Niebuhr	www.facebook.com	443	Facebook ...	This event represents an HTTP
06/21/201...	HTTP Co...	Informational	AZ-ASA-CX	Brian Mcmillan	www.facebook.com	443		This event represents an HTTP

By providing health, performance, and license expiration information, Cisco Prime Security Manager enables the security team to proactively manage any issues that can adversely affect operations. The device inventory view in Figure 7 shows general health information of all the network security devices, along with malicious transactions and IPS threats.

Figure 7. Cisco Prime Security Manager Health Monitor



Granular Application, User, and Device Control

Cisco Prime Security Manager enables policies to be based on a rich set of contextual elements, including applications, microapplications, users, devices, and locations. For example, instead of a policy that allows or denies the entire Facebook application, microapplications within Facebook that are used for business purposes can be enabled, while nonbusiness microapplications such as Facebook Games can be disabled. The embedded application browser enables administrators to quickly find applications and microapplications of interest, and user-based access capabilities enable individual- and group-based access policies to control the use of applications. This process is further simplified through the intuitive directory search functionality.

Figure 8 illustrates how common access policy parameters such as source, destination, and service can be extended to include such contextual elements as user, user group, website and web category, application and application category, and device type. In addition, behaviors within an application or microapplication can also be controlled. For example, administrators may want to allow marketing and sales access to the Facebook Messages microapplication, but disable downloads (see Figure 9).

Figure 8. Granular Context-Based Access Control




Access			
Used by device groups: Default device group, California Branch Office, Arizona Branch Office			Policy set type: Access
Features enabled:   			Number of Policies: 4
Source	Destination	Application/Service	Action/Conditions
1 ANY	Gambling Websites		Deny
2 All Authenticated Users	ANY	Facebook Excluding Games	Allow
3 ANY	ANY	Instant Messaging	Allow
4 ANY	ANY		Conditional Allow Profiles: Low Reputation Websites

Figure 9. Behavior-Based Policy Control

Application / Service: [Create new object](#)

▼ **Set application behaviors**

Set global behavior to Allow all Deny all

Facebook Events

Post

Tag

Facebook General

Install

Post

Tag

Facebook Messages

Attachment Download

Attachment Upload

Post

The hit count of each policy is dynamically presented, clearly displaying the actual usage of each policy in the table. Policies can be shared across multiple firewalls, enabling administrators to maintain policy consistency across the network infrastructure.

Flexible Management Architecture

Built from the ground up for intuitive usability, Cisco Prime Security Manager provides administrators with a consistent management interface for single-device and multidevice management. When multiple devices are managed, all access requests are redirected to the primary manager to help ensure efficient, centralized control. In the event of an emergency, administrators can manually reset Cisco Prime Security Manager for single-device management.

To serve a range of deployment needs, Cisco Prime Security Manager is available either as a physical appliance or as a virtual VMware ESXi-based appliance.

Table 2 lists features and benefits of Cisco Prime Security Manager.

Table 2. Features and Benefits of Cisco Prime Security Manager

Feature	Benefit
Granular Application Control	Enables access policies to be developed and enforced for more than 1,000 commonly used applications and 75,000 microapplications as well as application behaviors (for example, file uploads and posts on a social networking site). Port- and protocol-hopping applications can also be effectively blocked with fewer policies.
User Identity	Supports common identity mechanisms such as Active Directory agent, Lightweight Directory Access Protocol (LDAP), Kerberos, and Windows NT LAN Manager (NTLM) for user- and role-based differentiated access control.
Device-Type-Based Enforcement	Enables administrators to clearly identify the types of devices that are attempting to access the network, and to control which of those devices will be permitted or denied.
URL Filtering	Includes an enterprise-class, full-featured URL filtering solution that enables granular control of Internet traffic.
Global Intelligence	Employs Cisco Security Intelligence Operations (SIO) to protect against zero-day malware and provide safe access to applications by using regularly updated threat intelligence feeds from the global footprint of Cisco security deployments.
Use of Existing Network Definitions	Enables existing object definitions to be imported from other ASA security devices and used to construct newer policy rules.
Shared Policy Rules	Enables easy sharing of policies across multiple firewalls. Users can import devices and manage them individually, or they can share policies and configuration across multiple devices.
Administrative Role-Based Access Control (RBAC)	Provides differentiated role-based access to the management application (for example, a help desk user can have read-only access to troubleshoot issues, whereas a security administrator can be granted the ability to manage security policies).
ASA 5500-X Support	Allows users to manage ASA 5500-X Series devices (firewall, NAT, events) along with the ability to preview CLI configurations before deployment.

Ordering Information

Every Cisco ASA Next-Generation Firewall Services solution comes preloaded with an on-box single-device management version of Cisco Prime Security Manager. Central management of multiple appliances running Cisco ASA Next-Generation Firewall Services can be achieved using the multidevice version of Cisco Prime Security Manager. This version is available either as a physical appliance or as a VMware ESXi-based virtual appliance. In either case, licensing is based on the number of appliances to be managed (Table 3).

Table 3. Cisco Prime Security Manager Licensing Information

Product ID Number	Description	Form Factor
PRSMv9-SW-5-K9	Prime Security Manager - Software - 5-Device Management	Virtual Appliance
PRSMv9-SW-10-K9	Prime Security Manager - Software - 10-Device Management	Virtual Appliance
PRSMv9-SW-25-K9	Prime Security Manager - Software - 25-Device Management	Virtual Appliance
PRSMv9-SW-50-K9	Prime Security Manager - Software - 50-Device Management	Virtual Appliance
PRSMv9-SW-100-K9	Prime Security Manager - Software - 100-Device Management	Virtual Appliance

Product ID Number	Description	Form Factor
R-PRSMv9-SW-5-K9	Prime Security Manager - SW (eDelivery) - 5-Device Manager	Virtual Appliance
R-PRSMv9-SW-10-K9	Prime Security Manager - SW (eDelivery) - 10-Device Manager	Virtual Appliance
R-PRSMv9-SW-25-K9	Prime Security Manager - SW (eDelivery) - 25-Device Manager	Virtual Appliance
R-PRSMv9-SW-50-K9	Prime Security Manager - SW (eDelivery) - 50-Device Manager	Virtual Appliance
R-PRSMv9-SW-100-K9	Prime Security Manager - SW (eDelivery) - 100-Device Manager	Virtual Appliance
PRSM-HW1-25-K9	Prime Security Manager - Appliance - 25-Device Management	Physical Appliance
PRSMv9-HW1-50-K9	Prime Security Manager - Appliance - 50-Device Management	Physical Appliance
PRSMv9-HW1-100-K9	Prime Security Manager - Appliance - 100-Device Management	Physical Appliance

Additional licenses can be purchased for existing installations, as necessary, and can be applied to both virtual and physical appliances (Table 4).

Table 4. Additional Licenses for Cisco Prime Security Manager

Product ID Number	Description
PRSM-DEV-5=	PRSM - License - Manage 5 Additional Devices
PRSM-DEV-10=	PRSM - License - Manage 10 Additional Devices
PRSM-DEV-25=	PRSM - License - Manage 25 Additional Devices
PRSM-DEV-50=	PRSM - License - Manage 50 Additional Devices
PRSM-DEV-100=	PRSM - License - Manage 100 Additional Devices
L-PRSM-DEV-5=	PRSM - License (eDelivery) - Manage 5 Additional Devices
L-PRSM-DEV-10=	PRSM - License (eDelivery) - Manage 10 Additional Devices
L-PRSM-DEV-25=	PRSM - License (eDelivery) - Manage 25 Additional Devices
L-PRSM-DEV-50=	PRSM - License (eDelivery) - Manage 50 Additional Devices
L-PRSM-DEV-100=	PRSM - License (eDelivery) - Manage 100 Additional Devices

Once the product ID numbers are selected, the next step is to identify the support services for Cisco Prime Security Manager. Note that the virtual appliance version of Cisco Prime Security Manager is covered by Software Application Support plus Upgrades (SASU), and the physical appliance version is covered by Cisco SMARTnet[®]. Cisco highly recommends obtaining support services along with product purchases to simplify product use and upgrade experience. See Table 5 to find the most appropriate service.

Table 5. Service Licenses for Cisco Prime Security Manager

Prime Security Manager Product ID Number	Corresponding Support Product ID Number
PRSMv9-SW-5-K9	R-PRSMv9-SW-5-K9 CON-SAU-PRSM5
PRSMv9-SW-10-K9	R-PRSMv9-SW-10-K9 CON-SAU-PRSM10
PRSMv9-SW-25-K9	R-PRSMv9-SW-25-K9 CON-SAU-PRSM25
PRSMv9-SW-50-K9=	R-PRSMv9-SW-50-K9 CON-SAU-PRSM50
PRSMv9-SW-100-K9=	R-PRSMv9-SW-100-K9 CON-SAU-PRSM100
PRSM-DEV-5=	L-PRSM-DEV-5= CON-SAU-PRSM5A
PRSM-DEV-10=	L-PRSM-DEV-10= CON-SAU-PRSM10A
PRSM-DEV-25=	L-PRSM-DEV-25= CON-SAU-PRSM25A
PRSM-DEV-50=	L-PRSM-DEV-50= CON-SAU-PRSM50A
PRSM-DEV-100=	L-PRSM-DEV-100= CON-SAU-PRSM100A

For More Information

- Cisco ASA Next-Generation Firewall Services: <http://www.cisco.com/go/asacx>
- Cisco Prime Security Manager: <http://www.cisco.com/go/prsm>
- Cisco ASA 5500-X Series Next Generation Firewalls: <http://www.cisco.com/go/asa>
- Cisco Security Services: http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html




Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)