

## Cisco Prime Security Manager

**Q.** What is Cisco Prime™ Security Manager?

**A.** 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

**Q.** Who should deploy Cisco Prime Security Manager?

**A.** Cisco Prime Security Manager is designed to meet the needs of small to large enterprise environments that use Cisco ASA 5500-X Series NGFW. In particular, customers looking to manage core firewall capabilities and Network Address Translation (NAT) are encouraged to deploy this management tool.

**Q.** What are the features of Cisco Prime Security Manager?

**A.** Cisco Prime Security Manager provides a range of features for the Cisco ASA 5500-X NGFW platform:

- Preloaded on-box single-device management
- Offered as a Central Management Application for multi-device management
- Top-*n* traffic-pattern reports (on sources, destinations, devices, and so on) with multiple levels of drill-down
- Object import from the Cisco ASA 5500-X Series NGFW appliances
- Behavior-based policy management for the Cisco ASA 5500-X NGFW solution
- Event analysis for the Cisco ASA 5500-X NGFW
- Proactive health monitoring for the Cisco ASA 5500-X NGFW
- License management for the Cisco ASA 5500-X NGFW

For a detailed summary of Cisco Prime Security Manager features and benefits, please refer to the data sheet available at: <http://www.cisco.com/go/prsm>.

**Q.** What is new in the latest release of Cisco Prime Security Manager?

**A.** The following features are new to the latest Prime Security Manager release.

<b>New Policy Model</b>	Users can now view, create, and modify policies using the 5-tuple policy table for both NGFW Services and ASA-X.
<b>Per-Device Configuration</b>	The group-device configuration has been removed. Users can now import devices and manage them individually.
<b>Repository View</b>	Users can see all their devices and configurations from a single inventory view.
<b>Policy Sharing</b>	Users can share policy sets (for example, Human Resource Servers) and configurations such as syslogs across multiple devices.
<b>ASA-X Device Support</b>	Users can manage core fundamentals of the ASA-X device (firewall, NAT, and events).

<b>ASA-X Command-Line Interface Preview</b>	ASA-X users can also now preview CLI configurations before they deploy the changes to the devices.
<b>ASA-X and NGFW Services High-Availability Dashboard</b>	Device high-availability support has been added to the user interface with dedicated dashboard widgets.
<b>Import Workflow</b>	Users now have more control over the import of NGFW Services in ASA deployments.

**Q.** How is Cisco Prime Security Manager delivered, and what are the licensing considerations?

**A.** Every Cisco ASA 5500-X NGFW comes with a preloaded on-box, single-device management version of Cisco Prime Security Manager. This version also has limited storage available for event logging and reporting purposes. In all but the simplest Cisco ASA NGFW deployments, it is recommended that customers purchase the Cisco Prime Security Manager centralized management solution.

The multidevice version of Cisco Prime Security Manager is designed for centralized management of multiple ASA NGFW appliances. This version is available as a VMware ESX-based virtual appliance and in physical appliance form factors.

Licensing in both cases is based on the number of Cisco ASA NGFW appliances that need to be managed. Customers who already have Cisco Prime Security Manager to manage a specific number of devices, but who find that they now need to manage a greater number of devices, can procure licenses to manage the additional devices. Note that these licenses can be applied to existing Prime Security Manager installations, whether they are based on virtual or physical appliance form factors.

**Q.** What kind of literature is available for Cisco Prime Security Manager?

**A.** Visit <http://www.cisco.com/go/prsm> for the most recent information on Cisco Prime Security Manager. User guides, an installation guide, and other technical information can be found at: [http://www.cisco.com/en/US/products/ps12635/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps12635/tsd_products_support_series_home.html). In addition, Cisco will provide related online videos and webinars. These training opportunities will be announced in Cisco security newsletters as well.

**Q.** Is Cisco Prime Security Manager supported on VMware?

**A.** Yes. Cisco Prime Security Manager is supported on VMWare ESX 4.1 and ESX 5.0.

**Q.** What support options are available for Cisco Prime Security Manager?

**A.** Cisco Prime Security Manager is eligible for technical support service coverage under Cisco Software Application Support plus Upgrades (SASU). For details on Cisco SASU coverage, visit: [http://www.cisco.com/en/US/products/svcs/ps3034/ps2827/ps2993/serv\\_group\\_home.html](http://www.cisco.com/en/US/products/svcs/ps3034/ps2827/ps2993/serv_group_home.html).

Cisco Software Application Support (SAS) is not available for Cisco Prime Security Manager.

**Q.** What options are available to evaluate Cisco Prime Security Manager?

**A.** Anybody with a valid Cisco.com account can download Cisco Prime Security Manager and use the software for up to 90 days in evaluation mode. Visit <http://www.cisco.com/go/prsm> and click the Download Software link. There is no separate evaluation license. The product operates automatically in evaluation mode in the absence of an installed permanent license file.

---

## Importing Cisco ASA Next-Generation Firewall Platform Settings

**Q.** What directory realm configuration settings are imported from the Cisco ASA NGFW platform?

**A.** The following settings are imported, but with certain restrictions:

- Lightweight Directory Access Protocol (LDAP) directory realms are imported.
- The Active Directory (AD) realm is imported only if no AD realm is defined in Prime Security Manager.
- If an AD realm is defined on both ASA Next-Generation Firewall and Prime Security Manager, they must be identical, or the device import will fail.

**Q.** What decryption configuration settings are imported from the Cisco ASA Next-Generation Firewall platform?

**A.** The following settings are imported, but with certain restrictions:

- If decryption is enabled on ASA Next-Generation Firewall or on Prime Security Manager but not both, it will be enabled on the other.
- If decryption is enabled on both ASA NGFW and Prime Security Manager, the certificate and settings must be identical or device import will fail.

**Q.** What license configuration settings are imported from the Cisco ASA Next-Generation Firewall platform?

**A.** The following settings are imported, but with certain restrictions:

- Valid licenses on a device are imported. Application services, URL filtering, and web reputation are the valid licenses on the Cisco ASA 5500-X NGFW.
- Invalid licenses, or licenses that are identical to ones already in Prime Security Manager, are replaced with the copies in Prime Security Manager.
- Evaluation licenses are not imported.

**Q.** What configuration settings are not imported from the Cisco ASA 5500-X Series Next-Generation Firewalls?

**A.** The following settings are not imported:

- AD agent
- Authentication settings
- Signature update settings
- Packet capture settings

## Importing Cisco ASA Next-Generation Firewall Services Settings

**Q.** What will be the response by Prime Security Manager if a user makes CLI changes on ASA-X?

**A.** Users have two options:

- **Abort and alert:** This aborts the current deployment and lets users investigate.
- **Overwrite:** This always overwrites the changes from Prime Security Manager over the out-of-band changes.

**Out-of-band settings**

Please select the default behavior in case an out-of-band conflict is detected.

<b>Abort and alert</b>	In case of out-of-band change conflict, abort the current deployment and alert me to investigate and redeploy.
<b>Overwrite</b>	Do not alert and abort deployment, always overwrite the changes from PRSM to the out-of-band changes.

- Q.** How many devices will Prime Security Manager support?
- A.** Prime Security Manager will support up to 100 devices (NGFW Services and ASA 5500-X), as long as they fall under these limits:
- 10,000 objects
  - 5000 policies
  - 15,000 events/sec
- Q.** What does “100-device support” mean?
- A.** Prime Security Manager will support any one of the following:
- 100 NGFW Services devices
  - 100 ASA 5500-X devices
  - 100 ASA 5500-X and NGFW Services devices in combination
- Q.** What ASA-X models do this application support?
- A.** This tool will support all ASA-X devices with ASA Software Release 9.0 or later. Note that ASA 5505 is not supported by this tool.
- Q.** Can I manage firewall and NAT policies with this new release and everything else with Cisco Adaptive Security Device Manager?
- A.** Yes. You can manage policies with this tool and let the device-specific configurations be carried out by ASDM. Here are examples:
- Firewall policies by Cisco Prime Security Manager
  - NAT policies by Cisco Prime Security Manager
  - Syslog configuration by Cisco Prime Security Manager
  - Interface Roles by Cisco Prime Security Manager
  - Interface configuration by ASDM
  - Routing by ASDM
  - VPN by ASDM
  - Packet tracer by ASDM

**Q.** How does policy sharing work in the new Prime Security Manager?

**A.** Users can import policies and then share policy sets across multiple devices. Although policy rules (within a policy set) cannot be shared across devices, users can create universal policies that can apply either to a single device or to multiple devices. These then become mandatory rules that only an administrator can change.

**Q.** Is there a single policy rule for both ASA 5500-X hardware platform and NGFW Services?

**A.** No. These are managed by separate configurations. This separation helps ensure that the ASA-X policies are configured first, followed by the NGFW Services policies.

**Q.** What built-in PDF reports do we get in this new release?

**A.** The chart below outlines the reports.

<b>Administrative</b>	<ol style="list-style-type: none"><li>1. Policy changes</li><li>2. Top 25 policies by number of transactions</li><li>3. Traffic summary</li></ol>
<b>Users and Devices</b>	<ol style="list-style-type: none"><li>1. Top 25 users</li><li>2. Top 25 devices</li></ol>
<b>Threat Analyses</b>	<ol style="list-style-type: none"><li>1. Top 25 threats</li><li>2. Top 25 attackers</li><li>3. Top 25 targets</li><li>4. Top 25 policies with maximum threats</li></ol>
<b>Applications and Web Destinations</b>	<ol style="list-style-type: none"><li>1. Top 25 applications</li><li>2. Top 25 application types</li><li>3. Top 25 web destinations</li><li>4. Top 25 web categories</li></ol>

**Q.** Which ASA-X features are and are not supported in Cisco Prime Security Manager?

**A.** The following chart lists these features.

ASA-X Features Supported in Prime Security Manager	ASA-X Features Not Supported in Prime Security Manager
Firewall policies	Multicontext
Basic reports	Site-to-site VPN
Policy objects	Remote access VPN
NAT policies	Routing (all types)
Routed mode	Classic IPS module
Interface/VLAN	Certificates
Transparent mode	Syslog export
Device management	Protocol inspection
Basic events	Identity firewall
High availability	Cisco TrustSec




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](http://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](http://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)